MONITORUL OFICIAL AL ROMÂNIEI

Anul 194 (XXXVIII) — Nr. 712 bis

PARTEA I
LEGI, DECRETE, HOTĂRÂRI ȘI ALTE ACTE

Joi, 27 august 2026

SUMAR

ACTE ALE ORGANELOR DE SPECIALITATE ALE ADMINISTRAȚIEI PUBLICE CENTRALE

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

ORDIN
pentru aprobarea Măsurilor de gestionare a riscurilor de securitate cibernetică aferente rețelelor și sistemelor informatice utilizate de entitățile esențiale și importante și a Metodologiei de autoevaluare a maturității măsurilor de gestionare a riscurilor de securitate cibernetică și pentru modificarea Metodologiei privind evaluarea nivelului de risc al entităților, aprobată prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 2/2025 pentru aprobarea Criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și a Metodologiei privind evaluarea nivelului de risc al entităților*)

Având în vedere dispozițiile art. 10 alin. (2), art. 11 alin. (1), art. 12 alin. (1) și (4), art. 13, precum și ale art. 65 alin. (1) lit. b) din Ordonanța de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil, aprobată cu modificări și completări prin Legea nr. 124/2025, cu completările ulterioare, precum și dispozițiile art. 5 lit. b) și ale art. 7 alin. (3) și (4) din Ordonanța de urgență a Guvernului nr. 104/2021 privind înființarea Directoratului Național de Securitate Cibernetică, aprobată cu modificări și completări prin Legea nr. 11/2022, cu modificările ulterioare,

directorul Directoratului Național de Securitate Cibernetică emite prezentul ordin.

Art. I. — Se aprobă Măsurile de gestionare a riscurilor de securitate cibernetică aferente rețelelor și sistemelor informatice utilizate de entitățile esențiale și importante, prevăzute în anexa nr. 1 care face parte integrantă din prezentul ordin.

Art. II. — Se aprobă Metodologia de autoevaluare a maturității măsurilor de gestionare a riscurilor de securitate cibernetică, prevăzută în anexa nr. 2 care face parte integrantă din prezentul ordin.

Art. III. — (1) Atunci când este cazul, măsurile de gestionare a riscurilor de securitate cibernetică aplicabile entității se completează cu alte cerințe prevăzute în reglementări speciale sau sectoriale aplicabile acesteia.

(2) Cerințele implementate ca urmare a aplicării unor reglementări speciale sau sectoriale se evidențiază într-o declarație de aplicabilitate întocmită de entitate.

Art. IV. — Entitățile esențiale și importante implementează controalele aferente nivelului de asigurare corespunzător nivelului lor de risc, determinat potrivit Metodologiei privind evaluarea nivelului de risc al entităților, aprobată prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 2/2025 pentru aprobarea Criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și a Metodologiei privind evaluarea nivelului de risc al entităților.

Art. V. — Articolul 6 din Metodologia privind evaluarea nivelului de risc al entităților, aprobată prin Ordinul directorului Directoratului Național de Securitate Cibernetică nr. 2/2025 pentru aprobarea Criteriilor și pragurilor de determinare a gradului de perturbare a unui serviciu și a Metodologiei privind evaluarea nivelului de risc al entităților, publicat în Monitorul Oficial al României, Partea I, nr. 776 din 20 august 2025, se modifică și va avea următorul cuprins:

„Art. 6. — (1) Entitățile din sectorul 3 — Sectorul bancar și din sectorul 4 — Infrastructuri ale pieței financiare, prevăzute în anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024, aprobată cu modificări și completări prin Legea nr. 124/2025, cu completările ulterioare, cărora li se aplică Regulamentul (UE) 2022/2.554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1.060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1.011, denumit în continuare *Regulamentul (UE) 2022/2.554*, nu realizează evaluarea nivelului de risc al entității.

(2) Entitățile menționate la alin. (1) aplică măsurile de gestionare a riscurilor în materie de securitate cibernetică prevăzute de Regulamentul (UE) 2022/2.554.

(3) Atunci când entitățile din sectorul 8 — Infrastructură digitală și din sectorul 9 — Gestionarea serviciilor TIC (business-to-business), prevăzute în anexa nr. 1 la Ordonanța de urgență a Guvernului nr. 155/2024, aprobată cu modificări și completări prin Legea nr. 124/2025, cu completările ulterioare, sunt desemnate ca furnizori terți esențiali de servicii TIC potrivit Regulamentului (UE) 2022/2.554, acestea nu realizează evaluarea nivelului de risc al entității și aplică măsurile de gestionare a riscurilor în materie de securitate cibernetică prevăzute de același regulament.”

Art. VI. — Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

Directorul Directoratului Național de Securitate Cibernetică,
Dan-Petre Cîmpean

București, 6 august 2026.
Nr. 1.

*) Ordinul nr. 1/2026 a fost publicat în Monitorul Oficial al României, Partea I, nr. 712 din 27 august 2026 și este reprodus și în acest număr bis.

Anexa nr. 1

MĂSURILE

de gestionare a riscurilor de securitate cibernetică aferente rețelelor și sistemelor informatice utilizate de entitățile esențiale și importante

Art. 1 - Structura măsurilor de gestionare a riscurilor de securitate cibernetică

(1) Măsurile de gestionare a riscurilor de securitate cibernetică sunt organizate în șase Funcții, după cum urmează:

a) Guvernare (GV) - asigură tratarea securității cibernetice ca prioritate strategică și stabilește politicile, responsabilitățile și atribuțiile de autoritate, care sunt comunicate și revizuite la nivelul entității;

b) Identificare (ID) - asigură înțelegerea activelor, sistemelor, persoanelor și datelor relevante, precum și a riscurilor asociate, fundamentând deciziile privind gestionarea riscurilor de securitate cibernetică;

c) Protecție (PR) - cuprinde măsurile de protecție, de natură tehnică, procedurală și de conștientizare, menite să reducă probabilitatea producerii unui incident sau să îi limiteze impactul;

d) Detecție (DE) - susține detecția promptă a evenimentelor de securitate cibernetică, în vederea reducerii daunelor și a unui răspuns mai rapid;

e) Răspuns (RS) - cuprinde acțiunile întreprinse la producerea unui incident, pentru limitarea acestuia, coordonarea comunicării și reducerea perturbărilor;

f) Recuperare (RC) - vizează restabilirea serviciilor și a operațiunilor afectate de un incident, precum și valorificarea lecțiilor învățate pentru creșterea rezilienței.

(2) Fiecare Funcție prevăzută la alin. (1) se împarte în Categorii, fiecare Categorie se împarte în Subcategorii, iar fiecare Subcategorie cuprinde unul sau mai multe Controale.

(3) Controalele reprezintă cerințele de securitate cibernetică ce trebuie implementate de către entități și constituie, în ansamblul lor, măsurile de gestionare a riscurilor de securitate cibernetică prevăzute de prezentul ordin. Un Control poate consta într-un proces, o politică, un dispozitiv, o practică sau orice altă acțiune cu rol în gestionarea riscurilor.

(4) Fiecare Control este identificat printr-un cod alfanumeric unic, având forma „XX.YY-NN.MM”, în care „XX” desemnează Funcția, „YY” Categoria, „NN” Subcategoria, iar „MM” Controlul din cadrul Subcategoriei.

(5) Anumite Controale sunt marcate ca Măsuri cheie pe baza tipurilor comune de atacuri cibernetice. Măsurile cheie sunt obligatorii și trebuie tratate cu prioritate, conform nivelului de asigurare căruia le sunt aplicabile.

(6) Anumite Controale sunt marcate ca fiind aferente unor Aspecte de management, corespunzând principiilor sistemelor de management pe care standardul ISO/IEC 17021-1 le impune auditorilor să le evalueze, respectiv: imparțialitate, competență, responsabilitate, deschidere, confidențialitate, răspuns la plângeri și abordare bazată pe risc. Stadiul îndeplinirii acestor Controale se revizuiește în cadrul fiecărui audit de evaluare a nivelului de asigurare.

Art. 2 - Conținutul Controalelor

Conținutul integral al Controalelor, cuprinzând, pentru fiecare Control, codul de identificare, enunțul cerinței și ghidul de implementare, este prevăzut în continuare, în cuprinsul prezentei anexe.

Art. 3 - Nivelurile de asigurare

(1) Controalele se aplică pe trei niveluri de asigurare, denumite, în ordinea crescătoare a rigorii:

a) nivelul de Bază, care cuprinde Controale aplicabile tuturor entităților și asigură un nivel fiabil de protecție prin utilizarea unor tehnologii și procese, în general, deja disponibile;

b) nivelul Important, la care Controalele nivelului de Bază sunt consolidate pentru a contribui la reducerea riscurilor cibernetice cunoscute și la limitarea impactului atacurilor efectuate de actori de amenințare cu resurse și competențe limitate;

c) nivelul Esențial, la care Controalele nivelului Important sunt consolidate suplimentar pentru a îndeplini cele mai înalte cerințe de securitate cibernetică, incluzând caracteristici avansate de securitate și fiind destinate să reziste atacurilor cibernetice sofisticate efectuate de actori de amenințare cu resurse și expertiză semnificative.

(2) Nivelurile de asigurare se află în raport de incluziune ierarhică, astfel:

a) nivelul Important cuprinde toate Controalele aplicabile nivelului de Bază, precum și Controalele suplimentare prevăzute pentru acest nivel;

b) nivelul Esențial cuprinde toate Controalele aplicabile nivelului Important, precum și Controalele suplimentare prevăzute pentru acest nivel.

Art. 4 - Controalele și aplicabilitatea acestora sunt prevăzute în anexă la prezenta.

Anexă la Anexa nr. 1

GUVERNARE

[GV.OC] CONTEXT ORGANIZAȚIONAL

Sunt înțelese circumstanțele - misiunea, așteptările părților interesate, dependențele și cerințele legale, de reglementare și contractuale - aferente deciziilor organizației privind managementul riscului de securitate cibernetică.

GV.OC-01

Misiunea organizației este înțeleasă și se află la baza managementului riscului de securitate cibernetică.

GV.OC-01.1

Misiunea organizației trebuie stabilită, comunicată și trebuie să constituie baza pentru managementul riscului de securitate cibernetică sau a informației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că misiunea organizației este clar definită și comunicată și că servește drept bază pentru gestionarea riscurilor de securitate cibernetică sau a informației. Înțelegerea misiunii contribuie la identificarea riscurilor care ar putea interfera cu atingerea obiectivelor strategice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Misiunea organizației ar trebui comunicată prin intermediul unor materiale precum declarații de viziune și misiune, strategii de servicii sau documente de marketing. Aceasta contribuie la identificarea și prioritizarea riscurilor.
- Procesele organizației și obiectivele strategice ar trebui dezvoltate ținând seama de securitatea cibernetică sau a informației. Aceasta include înțelegerea modului în care riscurile pot afecta operațiunile, activele, persoanele fizice, partenerii sau interesele societății în general.
- Necesitatea de a proteja informațiile sensibile, inclusiv datele cu caracter personal, ar trebui evaluată pe baza misiunii organizației și a modului în care funcționează sistemele și serviciile sale.
- Misiunea și procesele conexe ale organizației ar trebui revizuite periodic, de exemplu anual, pentru a se asigura că rămân relevante și continuă să sprijine un management al riscului eficace.

GV.OC-02

Părțile interesate interne și externe sunt înțelese, iar nevoile și așteptările acestora în ceea ce privește managementul riscului de securitate cibernetică sunt înțelese și luate în considerare.

GV.OC-02.1

Organizația trebuie să demonstreze că înțelege și ia în considerare nevoile și așteptările părților interesate interne și externe în ceea ce privește managementul riscului de securitate cibernetică sau a informației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația înțelege și ia în considerare nevoile și așteptările părților interesate interne și externe în gestionarea riscurilor de securitate cibernetică sau a informației. Aceasta contribuie la alinierea eforturilor de securitate cibernetică la prioritățile organizației, obligațiile legale și încrederea părților interesate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Organizația ar trebui să identifice părțile interesate interne cheie, precum angajații, conducerea superioară, membri ai consiliului de administrație sau echivalent și auditorii interni. Rolurile, responsabilitățile și așteptările acestora în ceea ce privește securitatea cibernetică ar trebui înțelese și documentate.
- Ar trebui identificate părțile interesate externe cheie, inclusiv clienții, furnizorii, partenerii, autoritățile de reglementare, acționarii, furnizorii de servicii și auditorii externi, iar așteptările acestora în materie de conformitate, contracte și protecția datelor ar trebui luate în considerare.
- Nevoile și așteptările părților interesate ar trebui colectate prin metode precum interviuri, sondaje, revizuiri ale contractelor sau analize ale reglementărilor.
- Aceste informații ar trebui integrate în strategia de management al riscului de securitate cibernetică a organizației, pentru asigurarea alinierii cu prioritățile organizației și de reglementare.
- Ar trebui stabilite canale periodice de comunicare pentru a menține părțile interesate informate și implicate în chestiuni legate de securitatea cibernetică.
- Așteptările părților interesate ar trebui revizuite și actualizate periodic, în special atunci când apar modificări în operațiunile organizației, cerințele legale sau expunerea la risc.

GV.OC-03

Cerințele legale, de reglementare și contractuale privind securitatea cibernetică sunt înțelese și gestionate.

GV.OC-03.1

Cerințele legale și de reglementare privind securitatea cibernetică sau a informației trebuie identificate și implementate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că cerințele legale, de reglementare și contractuale referitoare la securitatea cibernetică sau a informației sunt identificate, monitorizate și implementate. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Ar trebui stabilit un proces pentru urmărirea și aplicarea cerințelor legale și de reglementare relevante legate de securitatea cibernetică sau a informației.
- Aceste cerințe ar trebui integrate în toate politicile, procedurile și practicile operaționale relevante.
- Domeniile care ar trebui acoperite includ, dar nu se limitează la:
    - Evaluarea riscurilor și protecția sistemelor informatice;
    - Răspunsul la incidente, continuitatea activității și managementul crizelor;
    - Securitatea lanțului de aprovizionare și dezvoltarea de sisteme securizate;
    - Managementul vulnerabilităților și configurarea securizată;
    - Conștientizarea și instruirea în materie de securitate;
    - Măsuri de control criptografic și comunicații securizate;
    - Sisteme de comunicare de urgență;
    - Controlul accesului, managementul activelor și autentificarea multifactor (MFA);
    - Divulgarea coordonată a vulnerabilităților (CVD).

GV.OC-03.2

Obligațiile legale, de reglementare și contractuale legate de securitatea cibernetică sau a informației trebuie gestionate în mod continuu pentru a se asigura că acestea rămân corecte, actualizate și aplicate în mod eficace.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că cerințele legale și de reglementare legate de securitatea cibernetică sau a informației sunt gestionate în mod continuu, actualizate și aplicate în mod eficace în cadrul organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Ar trebui să existe un proces structurat pentru gestionarea continuă a cerințelor legale și de reglementare legate de securitatea cibernetică sau a informației.
- Aceste cerințe ar trebui documentate, revizuite periodic și actualizate pentru a reflecta modificările legislației și reglementărilor.
- Abordarea organizației în materie de conformitate ar trebui să fie clar definită, incluzând rolurile, responsabilitățile și răspunderea.
- Ar trebui implementate mecanisme pentru monitorizarea modificărilor din peisajul legislativ și de reglementare. Astfel de modificări ar trebui să declanșeze o revizuire a politicilor, procedurilor și controalelor relevante pentru asigurarea conformității continue.
- Dovezile privind activitățile de conformitate ar trebui menținute pentru a sprijini auditurile și pentru a demonstra due diligence.

GV.OC-04

Obiectivele, capabilitățile și serviciile critice de care depind sau pe care le așteaptă părțile interesate externe de la organizație sunt înțelese și comunicate.

GV.OC-04.1

Organizația trebuie să identifice, să documenteze și să comunice obiectivele, capabilitățile și serviciile critice pe care se bazează părțile interesate externe, să le prioritizeze în funcție de criticitate și să integreze această prioritizare în procesul de evaluare a riscurilor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația înțelege care servicii, capabilități și obiective critice sunt esențiale pentru părțile interesate externe, le prioritizează în funcție de importanță și le include în procesul de evaluare a riscurilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Acest Control se concentrează pe ceea ce organizația oferă altora, cu alte cuvinte, serviciile și funcțiile de care depind părțile interesate externe (lanțul de aprovizionare din aval, precum clienții, partenerii sau utilizatorii finali).
- Serviciile critice și funcțiile interne care le susțin ar trebui identificate în mod clar.
- Ar trebui definite criterii pentru a determina importanța fiecărui serviciu sau capabilitate, atât din perspectivă internă, cât și externă.
- O analiză a impactului asupra activității (BIA) poate contribui la identificarea activelor și operațiunilor vitale pentru atingerea obiectivelor cheie și a consecințelor în cazul în care acestea ar fi întrerupte.
- Obiectivele de reziliență, cum ar fi viteza cu care serviciile critice trebuie recuperate în timpul perturbărilor, ar trebui stabilite și comunicate.

GV.OC-04.2

Organizația trebuie să definească și să documenteze cerințele de securitate cibernetică pentru operațiunile esențiale, să le valideze prin teste și audituri, să mențină înregistrări ale rezultatelor și măsurilor corective și să actualizeze periodic cerințele în funcție de evoluția riscurilor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că operațiunile esențiale sunt protejate prin măsuri de securitate clar definite și testate și că aceste măsuri rămân eficace și actualizate pe măsură ce riscurile evoluează.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea și documentarea
  - Definirea serviciilor critice și a dependențelor acestora (de exemplu, sisteme, furnizori) printr-o evaluare structurată a riscurilor.
  - Documentarea cerințelor de securitate și operaționale, inclusiv a cerințelor specifice reglementărilor și domeniului (de exemplu, CyFun®, ISO/IEC 27001, IEC 62443).
- Validarea și aprobarea
  - Stabilirea proceselor de guvernanță pentru revizuirea și aprobarea cerințelor de securitate identificate.
  - Atribuirea răspunderii părților interesate relevante (de exemplu, echipele de securitate, responsabilii cu conformitatea, conducerea superioară).
- Testarea și asigurarea
  - Efectuarea de teste de penetrare, evaluări ale vulnerabilităților și simulări de incidente pentru a valida implementarea.
  - Asigurarea efectuării de audituri pentru evaluarea eficacității și identificarea lacunelor în măsurile de securitate.
  - Implementarea unor măsuri corective în cazul în care sunt constatate deficiențe, asigurând îmbunătățirea continuă.
- Păstrarea înregistrărilor și conformitatea
  - Menținerea unei documentații detaliate a procedurilor de testare, a rezultatelor, a aprobărilor și a măsurilor corective.
  - Alinierea cadrelor de securitate la obligațiile de reglementare pentru asigurarea conformității și supravegherea guvernanței.

- Revizuirea şi adaptarea continue
  - Reevaluarea periodică a cerințelor ca răspuns la amenințările, incidentele şi modificările de reglementare în continuă evoluție.
  - Asigurarea faptului că organismele de guvernanță supraveghează actualizările și îmbunătățirile pentru menținerea rezilienței cibernetice pe termen lung.

GV.OC-04.3

Redundanța trebuie implementată pentru a îndeplini cerințele de disponibilitate definite de organizație, legislație și/sau reglementări.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura disponibilitatea sistemelor și serviciilor critice prin implementarea redundanței în conformitate cu cerințele organizaționale, legale și de reglementare privind disponibilitatea.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Acest Control se concentrează pe asigurarea continuității funcționării serviciilor esențiale, chiar și în cazul în care o parte a sistemului se defectează.
- Redundanța ar trebui integrată în componente cheie, precum stocarea datelor, infrastructura de rețea și sistemele critice. Exemplele includ:
  - Servere de rezervă, echilibratoare de sarcină, matrice redundante de discuri independente (RAID) și centre de date multiple;
  - Conexiuni internet de tip failover și mai mulți furnizori de servicii de internet (ISP).
- Echipamentele și serviciile critice ar trebui protejate împotriva întreruperilor de curent și a întreruperilor de utilități folosind:
  - Surse de alimentare neîntreruptibilă (UPS), generatoare de rezervă și cabluri de alimentare redundante, 2 furnizori diferiți de servicii de alimentare cu energie electrică;
  - Contracte de testare și mentenanță periodică pentru asigurarea fiabilității.

GV.OC-04.4

Obiectivele timpului de recuperare (RTO) și obiectivele punctului de recuperare (RPO) pentru reluarea proceselor esențiale ale sistemelor de tehnologia informației și comunicațiilor (TIC)/tehnologie operațională (OT) trebuie să fie definite și monitorizate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația definește și monitorizează obiective clare privind RTO și RPO pentru restabilirea proceselor esențiale ale sistemelor TIC și OT după o întrerupere.

Pentru definirea și monitorizarea RTO-urilor și RPO-urilor pentru sistemele TIC/OT critice, ar trebui luate în considerare următoarele elemente:

- Guvernanță și definirea politicilor
  - Stabilirea unor politici formale și a răspunderii pentru definirea și monitorizarea RTO/RPO.
  - Alinierea obiectivelor de recuperare la cadrele de continuitate a activității și de recuperare în caz de dezastru (de exemplu, ISO 22301, ISO/IEC 27031).
  - Asigurarea implicării conducerii și a conformității cu cerințele de reglementare.
- BIA
  - Identificarea interdependențelor dintre sistemele TIC și OT, precum și a efectelor lor în cascadă asupra operațiunilor organizației.
  - Determinarea pragurilor acceptabile de nefuncționare pentru diferite categorii de sisteme.
- Evaluarea riscurilor și amenințărilor
  - Efectuarea unor simulări de amenințări din lumea reală (de exemplu, exerciții de tip ransomware, testare la stres pentru atacuri DDoS).
  - Integrarea informațiilor privind amenințările în planificarea recuperării pentru anticiparea riscurilor în evoluție.
- Clasificarea și prioritizarea sistemelor
  - Definirea unor strategii de recuperare pe niveluri, în funcție de impactul asupra activității (de exemplu, Nivelul 1 = restaurare imediată, Nivelul 2 = recuperare întârziată).
  - Stabilirea mecanismelor de failover pentru procesele OT critice care trebuie să funcționeze continuu.

- Strategii de backup și recuperare
  - Implementarea de backup-uri imuabile pentru protecție împotriva ransomware-ului.
  - Asigurarea opțiunilor de recuperare la o locație externă și în cloud pentru reziliență geografică.
  - Efectuarea verificărilor periodice de validare și integritate ale backup-urilor pentru prevenirea eșecurilor în timpul recuperării.
- Testarea și validarea obiectivelor de recuperare
  - Efectuarea testelor de recuperare în caz de dezastru (exerciții teoretice, exerciții de restaurare completă).
  - Măsurarea eficacității RTO/RPO prin monitorizare în timp real și simulări de răspuns la incidente.
  - Stabilirea unei coordonări automate a recuperării pentru accelerarea reluării serviciilor.
- Monitorizarea continuă și îmbunătățirea
  - Utilizarea de analize în timp real pentru evaluarea abaterilor de la valorile RTO/RPO preconizate.
  - Adaptarea obiectivelor de recuperare pe baza lecțiilor învățate din incidente și audituri.

GV.OC-05

Rezultatele, capabilitățile și serviciile de care depinde organizația sunt înțelese și comunicate.

GV.OC-05.1

Organizația trebuie să identifice, să documenteze și să comunice rolul său în lanțul de aprovizionare, inclusiv capabilitățile externe, serviciile și dependențele de care depinde (din amonte), precum și interacțiunile sale cu părțile interesate din aval.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația identifică, documentează și comunică rolul său în cadrul lanțului de aprovizionare, prin înțelegerea capabilităților, serviciilor și dependențelor externe pe care se bazează (din amonte), recunoscând în același timp interacțiunile sale cu părțile interesate din aval.

Acest Control se concentrează în principal pe lanțul de aprovizionare din amonte, respectiv asupra elementelor de care organizația depinde din partea altor entități, menținând în același timp alinierea cu GV.OC-04, care abordează ceea ce organizația furnizează altor entități. Împreună, acestea oferă o imagine completă a dependențelor și responsabilităților lanțului de aprovizionare.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Rolul organizației în lanțul de aprovizionare ar trebui definit în mod clar, prin includerea atât a ceea ce este livrat altor părți (din aval), cât și a ceea ce este primit din surse externe (din amonte).
- Dependențele de resurse externe - precum incintele, furnizorii de servicii cloud și furnizorii de servicii, produse sau capabilități - ar trebui identificate și documentate.
- Aceste dependențe ar trebui corelate cu funcțiile operaționale conexe și cu activele organizației pentru a înțelege impactul lor asupra operațiunilor.
- O atenție deosebită ar trebui acordată dependențelor externe care reprezintă potențiale puncte de eșec pentru serviciile sau capabilitățile critice.
- Aceste informații ar trebui comunicate personalului relevant și părților interesate pentru sprijinirea managementului riscului, a planificării continuității și a coordonării răspunsului.
- Ar trebui stabilite canale de comunicare pentru a se asigura că rolurile și dependențele din lanțul de aprovizionare sunt înțelese în mod clar în cadrul organizației și de către partenerii cheie.

[GV.RM] STRATEGIA DE MANAGEMENT AL RISCULUI

Prioritățile, constrângerile, declarațiile privind toleranța și apetitul pentru risc ale organizației, precum și ipotezele sunt stabilite, comunicate și utilizate pentru sprijinirea deciziilor privind riscurile operaționale.

GV.RM-01

Obiectivele de management al riscului sunt stabilite și convenite de părțile interesate ale organizației.

GV.RM-01.1

Obiectivele privind securitatea cibernetică sau a informației trebuie identificate, convenite de părțile interesate ale organizației și aprobate de conducerea superioară.

GHID DE IMPLEMENTARE

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Respectarea principiilor de management al riscului descrise în ISO/IEC 27005, care oferă recomandări privind identificarea, evaluarea și atenuarea riscurilor de securitate a informației. Mai exact:
  - Clauza 6.1 ar trebui utilizată pentru stabilirea unui proces structurat de evaluare a riscurilor;
  - Clauza 6.3 ar trebui să ghideze definirea strategiilor adecvate de tratare a riscurilor.
- Actualizarea obiectivelor pe termen scurt și lung în materie de securitate cibernetică sau a informației în cadrul planificării strategice anuale și ca răspuns la modificările organizaționale majore.
- În organizațiile din sectorul OT, conducerea superioară ar trebui să ia în considerare factorii de sănătate, siguranță și mediu atunci când identifică riscurile.
- Stabilirea unor obiective specifice, măsurabile, realizabile, relevante și încadrate în timp (SMART) pentru securitatea cibernetică sau a informației (de exemplu, îmbunătățirea calității instruirii utilizatorilor, asigurarea unei protecții adecvate pentru sistemele de control industrial - ICS).
- Utilizarea acestor obiective pentru măsurarea și gestionarea riscului și performanței în cadrul organizației.

GV.RM-02

Declarațiile privind apetitul pentru risc și toleranța la risc sunt stabilite, comunicate și menținute.

GV.RM-02.1

Declarațiile privind apetitul pentru risc și toleranța la risc trebuie definite, documentate, aprobate de conducerea superioară, comunicate și menținute.

GHID DE IMPLEMENTARE

Obiectivul GV.RM-02.1 este de a asigura că organizația are o înțelegere clară și aplicabilă a limitelor sale de risc, ceea ce ajută la orientarea procesului decizional și a practicilor de management al riscului. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Apetitul pentru risc reprezintă cantitatea și tipul de risc pe care o organizație este dispusă să le asume sau să le accepte și are caracter strategic/calitativ (sursa: ISO/IEC 27005).
- Toleranța la risc reprezintă abaterea acceptabilă de la nivelul stabilit prin apetitul pentru risc și obiectivele organizației și are caracter tactic/cantitativ (sursa: ISACA).
- Apetitul pentru risc al organizației ar trebui să țină seama de rolul său în infrastructura critică și în sectorul său.
- Organizațiile din sectorul OT ar trebui să țină seama de prioritățile în materie de sănătate, siguranță și mediu în definirea apetitului lor pentru risc.
- Declarațiile privind apetitul pentru risc ar trebui traduse în declarații specifice, măsurabile și ușor de înțeles privind toleranța la risc (SMART).
- Obiectivele organizației și apetitul pentru risc ar trebui ajustate periodic pe baza expunerii cunoscute la riscuri și a riscului rezidual.
- Cu Awareness Raising in a Box (AR-in-a-Box), Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) oferă organizațiilor instrumentele și resursele esențiale pentru creșterea în mod eficace a gradului de conștientizare cu privire la securitatea cibernetică în cadrul operațiunilor lor. Acest set de instrumente Do-It-Yourself elaborat de către ENISA conține un ghid de nivel C.

GV.RM-03

Activitățile și rezultatele managementului riscului de securitate cibernetică sunt incluse în procesele de management al riscului la nivel de organizație (ERM).

GV.RM-03.1

Ca parte a strategiei de management al riscului la nivelul întregii organizații, trebuie elaborată o strategie cuprinzătoare de management al riscului de securitate cibernetică sau a informației, care trebuie actualizată atunci când apar modificări.

GHID DE IMPLEMENTARE

Acest Control se concentrează pe elaborarea și menținerea unei strategii specifice de gestionare a riscurilor de securitate cibernetică sau a informației. Aceasta asigură că organizația dispune de un plan dedicat și aplicabil, care evoluează odată cu peisajul amenințărilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- O strategie de management al riscului la nivelul întregii organizații include o exprimare a toleranței la riscul de securitate pentru organizație, strategii de atenuare a riscurilor de securitate, metodologii acceptabile de evaluare a riscurilor, un proces de evaluare a riscurilor de securitate în cadrul organizației în raport cu toleranța la risc a organizației și abordări pentru monitorizarea riscurilor în timp.
- Riscurile de securitate cibernetică sau a informației ar trebui agregate și gestionate alături de celelalte riscuri ale organizației (de exemplu, de conformitate, financiare, operaționale, de reglementare, de reputație, de siguranță).
- Strategia de management al riscului de securitate cibernetică sau a informației ar trebui să includă identificarea și alocarea resurselor necesare pentru protejarea activelor critice pentru activitatea organizației.
- Aceasta este implementarea specifică securității cibernetice a viziunii mai largi definite în GV.RM-04.1.

GV.RM-03.2

Riscurile de securitate cibernetică sau a informației trebuie documentate, ca parte a proceselor ERM, aprobate în mod formal de conducerea superioară și actualizate atunci când apar modificări.

GHID DE IMPLEMENTARE

Acest Control ar trebui să asigure punerea în aplicare a strategiei prin procese structurate. Se concentrează pe nivelul operațional și de guvernanță, asigură răspunderea și trasabilitatea riscurilor și pune accentul pe procesele formale și supravegherea.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea sistematică a riscurilor
  - Obiectiv:
    - Identificarea proactivă a riscurilor de securitate cibernetică sau a informației în cadrul organizației.
  - Măsuri:
    - Evaluări periodice ale riscurilor ar trebui efectuate utilizând metode precum modelarea amenințărilor, ateliere de lucru privind riscurile și scanări de vulnerabilități.
    - Riscurile legate de toate activele digitale și fizice (hardware, software, date, rețele) ar trebui incluse în inventarul activelor, împreună cu metadatele cheie (locație, proprietar, utilizare).
    - Utilizarea unor surse precum:
      → Jurnale de incidente de securitate.
      → Rezultatele testelor de penetrare.
      → Cerințe de reglementare.
      → Informații privind amenințările din domeniu.
  - Luarea în considerare a implicării echipelor interfuncționale (tehnologia informației - IT/OT, juridic, conformitate, unități organizaționale).
  - Instrumente de luat în considerare:
    - Șabloane de evaluare a riscurilor.
    - Platforme de informații privind amenințările (de exemplu, platformă de schimb de informații despre malware - MISP, Recorded Future).
    - Inventare de active și diagrame de fluxuri de date.

- Documentarea riscurilor în cadrul ERM
  - Obiectiv:
    - Asigurarea integrării riscurilor de securitate cibernetică în procesul ERM mai amplu.
  - Măsuri:
    - Luarea în considerare a utilizării unui registru centralizat de riscuri sau a unui instrument de guvernanță, risc și conformitate (GRC) pentru a documenta:
      - → Descrierea riscului.
      - → Probabilitatea și impactul.
      - → Responsabilul de risc.
      - → Controale existente.
      - → Riscul rezidual.
      - → Planul de tratare.
    - Managementul riscului de securitate cibernetică ar trebui să fie aliniat la obiectivele strategice ale organizației pentru a asigura relevanța și sprijinul.
  - Instrumente de luat în considerare:
    - Platforme GRC.
    - Foi de calcul/platforme de colaborare (de exemplu, Excel/SharePoint) pentru organizații mai mici.
- Aprobarea formală și implicarea conducerii superioare a organizației
  - Obiectiv:
    - Asigurarea supravegherii și a răspunderii conducerii în luarea deciziilor privind riscurile.
  - Măsuri:
    - Evaluările riscurilor și planurile de tratare a riscurilor ar trebui prezentate unui Comitet de risc sau unui Comitet executiv.
    - Luarea în considerare a includerii riscurilor de securitate cibernetică în rapoartele trimestriale de risc.
    - Ar trebui obținută aprobarea formală pentru:
      - → Acceptarea riscurilor.

→ Planuri de atenuare.

→ Alocările bugetare.

- Instrumente de luat în considerare:
  - Șabloane pentru raportarea către consiliul de administrație sau echivalent.
  - Tablouri de bord privind riscurile.
  - Procese-verbale ale ședințelor cu aprobări documentate.

- Comunicarea și conștientizarea
  - Obiectiv:
    - Asigurarea informării și implicării tuturor părților interesate relevante.
  - Măsuri:
    - Ar trebui stabilite linii clare de comunicare pentru riscurile de securitate cibernetică, inclusiv cele provenite de la furnizori și părți terțe.
    - Riscurile aprobate și strategiile de atenuare ar trebui comunicate echipelor relevante.
    - Conștientizarea ar trebui promovată prin instruire, sesiuni de informare și comunicări interne.
  - Instrumente de luat în considerare:
    - Platforme de comunicare internă (de exemplu, Teams, Slack).
    - Planuri de comunicare a riscurilor.
    - Liste ale părților interesate.

- Monitorizarea continuă și actualizările
  - Obiectiv:
    - Menținerea la zi a informațiilor privind riscurile și adaptarea acestora la modificări.
  - Măsuri:
    - Ar trebui implementată o monitorizare continuă pentru a detecta modificările în peisajul amenințărilor sau în mediul organizațional.
    - Luarea în considerare a definirii unor factori declanșatori pentru actualizări, precum:

→ Noi amenințări sau vulnerabilități.

→ Modificări în procesele organizației sau în sistemele IT.

→ Modificări ale reglementărilor.

- Ar trebui stabilit un proces de management al modificărilor care să includă actualizarea documentației privind securitatea cibernetică.
- Ar trebui efectuate revizuiri periodice (de exemplu, trimestrial sau de două ori pe an) ale riscurilor documentate.

- Instrumente de luat în considerare:
  - Sisteme de management al modificărilor.
  - Instrumente de monitorizare continuă.
  - Calendare de revizuire a riscurilor.

Acest Control pune în aplicare GV.RM-03.1 prin integrarea riscurilor de securitate cibernetică în cadrul ERM și prin asigurarea guvernanței și răspunderii.

GV.RM-04

Direcția strategică care descrie opțiunile adecvate de răspuns la riscuri este stabilită și comunicată.

GV.RM-04.1

Un plan sau o viziune la nivel înalt trebuie să fie stabilit în mod formal și comunicat în mod clar tuturor persoanelor implicate cu privire la modul de gestionare a riscurilor, inclusiv diferitele strategii pe care organizația le poate utiliza pentru a aborda riscurile identificate, în funcție de apetitul pentru risc sau de nivelul de toleranță la risc.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a stabili fundamentul strategic pentru managementul riscului, care include:

- Toleranța la risc și apetitul pentru risc.
- Direcția strategică pentru gestionarea riscurilor (de exemplu, atenuarea, transferul, acceptarea).
- Asigurarea alinierii între departamente.
- Asigurarea faptului că toți membrii organizației înțeleg imaginea de ansamblu a modului în care sunt abordate și gestionate riscurile.

Controlul se concentrează pe:

- Managementul riscului la nivel strategic și organizațional.
- Stabilirea unei viziuni sau a unui plan formal și cuprinzător.
- Comunicarea strategiilor de management al riscului (de exemplu, evitarea, atenuarea, transferul, acceptarea).
- Se aplică tuturor tipurilor de riscuri, nu doar securității cibernetice.

În raport cu Controalele GV.RM-03.1, GV.RM-03.2 și GV.RM-05.1, acest Control reprezintă punctul de plecare; el definește filosofia organizației în materie de risc, inclusiv apetitul și toleranța, care ghidează toate celelalte activități.

GV.RM-05

Liniile de comunicare în cadrul organizației sunt stabilite pentru riscurile de securitate cibernetică, inclusiv riscurile provenite de la furnizori și alte părți terțe.

GV.RM-05.1

Pentru a sprijini viziunea de nivel înalt privind managementul riscului, organizația trebuie să stabilească linii de comunicare clare pentru riscurile de securitate cibernetică, inclusiv cele provenite de la furnizori și părți terțe.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că informațiile privind riscurile de securitate cibernetică sau a informației sunt partajate în mod eficace în cadrul organizației și cu părți externe.

Acest Control axat pe comunicarea operațională și tactică este specific riscurilor de securitate cibernetică și pune accentul pe canalele de comunicare (de exemplu, raportarea, escaladarea, coordonarea), inclusiv riscurile externe provenite de la furnizori și părți terțe.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea rolurilor și responsabilităților în materie de comunicare
    - Atribuirea clară a răspunderii pentru raportarea, escaladarea și răspunsul la riscurile de securitate cibernetică între departamente și cu părți terțe.
- Stabilirea unor canale de comunicare
    - Utilizarea de canale structurate, precum grupuri de e-mail, sisteme de ticketing, platforme de răspuns la incidente sau instrumente de colaborare (de exemplu, Teams, Slack) pentru comunicarea la timp a riscurilor.
- Includerea părților terțe
    - Integrarea furnizorilor și partenerilor în procesul de comunicare prin clauze contractuale, protocoale comune de raportare sau planuri comune de răspuns la incidente (IRP).
- Documentarea și instruirea
    - Menținerea unui protocol de comunicare sau a unui manual și instruirea personalului relevant cu privire la modul și momentul în care trebuie raportate riscurile de securitate cibernetică.

- Revizuirea și îmbunătățirea
    - Testarea și revizuirea periodică a eficacității comunicării prin exerciții teoretice sau revizuiri post-incident.

Acest Control sprijină implementarea GV.RM-03.2, asigurând comunicarea riscurilor identificate și documentate către părțile interesate relevante, permițând un răspuns și o coordonare în timp util.

[GV.RR] ROLURI, RESPONSABILITĂȚI ȘI ATRIBUȚII DE AUTORITATE

Rolurile, responsabilitățile și atribuțiile de autoritate în materie de securitate cibernetică pentru a promova răspunderea, evaluarea performanței și îmbunătățirea continuă sunt stabilite și comunicate.

GV.RR-01

Conducerea organizației este responsabilă și răspunzătoare pentru riscul de securitate cibernetică și promovează o cultură conștientă de riscuri, etică și în continuă îmbunătățire.

GV.RR-01.1

Conducerea de vârf a organizației trebuie să fie responsabilă și răspunzătoare pentru riscul de securitate cibernetică și trebuie să promoveze o cultură conștientă de riscuri, etică și în continuă îmbunătățire.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că conducerea de vârf este răspunzătoare pentru riscul de securitate cibernetică și promovează o cultură conștientă de riscuri și în continuă îmbunătățire.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Conducerea de vârf a organizației ar trebui să convină asupra rolurilor și responsabilităților sale în elaborarea, implementarea și evaluarea strategiei de securitate cibernetică a organizației.
- Așteptările conducerii de vârf a organizației în ceea ce privește o cultură a securității, inclusiv evidențierea exemplelor pozitive sau negative de management al riscului de securitate cibernetică, ar trebui comunicate întregii organizații.
- Conducerea de vârf a organizației ar trebui să dispună ca managerul superior pentru securitatea informației (de exemplu, manager de securitate - CSO, manager securitatea informației - CISO) să mențină o strategie cuprinzătoare de management al riscului de securitate cibernetică și să o revizuiască și să o actualizeze cel puțin anual și după evenimente majore (a se vedea și GV.RR-02.2).
- Ar trebui efectuate revizuiri pentru a se asigura autoritatea și coordonarea adecvate între persoanele responsabile de gestionarea riscului de securitate cibernetică.

GV.RR-02

Rolurile, responsabilitățile și atribuțiile de autoritate legate de managementul riscului de securitate cibernetică sunt stabilite, comunicate, înțelese și puse în aplicare.

GV.RR-02.1

Rolurile, responsabilitățile și atribuțiile de autoritate în materie de securitate cibernetică sau a informației pentru angajați, furnizori, clienți și parteneri trebuie documentate, revizuite, autorizate, actualizate, comunicate și coordonate la nivel intern și extern.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate părțile interne și externe înțeleg și își îndeplinesc rolurile, responsabilitățile și atribuțiile de autoritate în materie de securitate cibernetică, reducând lacunele, suprapunerile și întârzierile în răspunsul la incidente și în conformitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Descrierea rolurilor, responsabilităților și atribuțiilor de autoritate în materie de securitate: cine din cadrul organizației ar trebui consultat, informat, considerat responsabil și tras la răspundere pentru toate sau o parte din activele organizației. Poate fi luată în considerare utilizarea modelului responsabil, răspunzător, consultat, informat (RACI). Ghidul poate fi găsit și în Profilurile de rol ale Cadrului european al competențelor în securitate cibernetică (ECSF) elaborate de către ENISA (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles).
- Includerea rolurilor, responsabilităților și atribuțiilor de autoritate în materie de management al riscului.
- Includerea responsabilităților și cerințelor de performanță în materie de securitatea cibernetică sau a informației în descrierile posturilor.
- Articularea în mod clar a responsabilităților în materie de securitatea cibernetică sau a informației în cadrul operațiunilor, funcțiilor de risc și funcțiilor de audit intern.
- Identificarea unuia sau mai multor roluri ori posturi specifice care vor fi responsabile și răspunzătoare de planificarea, alocarea resurselor și executarea activităților de management al riscului în lanțul de aprovizionare pentru securitate cibernetică (C-SCRM) sau a informației.
- Urmarea orientării anterioare, extinderea rolurilor, responsabilităților și atribuțiilor de autoritate de securitate internă la rolurile, responsabilitățile și atribuțiile de autoritate C-SCRM sau a informației.

- Dezvoltarea rolurilor, responsabilităților și atribuțiilor de autoritate pentru furnizori, clienți și parteneri ai organizației pentru abordarea responsabilităților comune pentru riscurile aplicabile de securitate cibernetică sau a informației și integrarea acestora în politicile organizației și în acordurile aplicabile părților terțe.
- Comunicarea internă a rolurilor și responsabilităților C-SCRM sau a informației pentru părți terțe.
- Stabilirea de reguli și protocoale pentru procesele de schimb de informații și de raportare între organizație și furnizorii săi.
- Luarea în considerare a stabilirii unei distincții clare între IT și OT în implementarea acestui Control, ținând cont de următoarele:
  - Roluri și responsabilități
    - IT
      - → Definirea de roluri precum administrator de sistem, analist de securitate a rețelelor, personal de răspuns la incidente.
    - OT
      - → Definirea de roluri precum inginer sisteme de control, coordonator securitate cibernetică OT, operator de instalație.
  - Documentare și revizuire
    - Asigurarea documentării separate, dar aliniate, a rolurilor IT și OT.
    - Ciclurile de revizuire pot diferi: IT (trimestrial/anual), OT (aliniat cu perioadele de mentenanță).
  - Autorizare și actualizări
    - Asigurarea aprobării documentației IT și OT de către conducerea relevantă (de exemplu, responsabilul pentru tehnologia informației - CIO pentru IT, director de fabrică pentru OT).
    - Actualizările în OT pot necesita proceduri de control al modificărilor din cauza implicațiilor asupra siguranței.

- Comunicare și coordonare
  - Intern
    - → Asigurarea existenței unor IRP-uri comune ale echipelor IT și OT.
  - Extern
    - → Includerea furnizorilor și partenerilor specifici OT (de exemplu, vânzătorii ICS) și IT (de exemplu, furnizorii de servicii cloud).

GV.RR-02.2

Organizația trebuie să numească un manager superior pentru securitatea informației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a stabili o răspundere executivă clară pentru securitatea cibernetică, prin numirea unui membru al conducerii superioare care să conducă strategia, supravegherea și alinierea la obiectivele organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Un membru al conducerii superioare este definit ca un membru de rang înalt al organizației, implicat în procesele importante de luare a deciziilor.
- Managerul superior pentru securitatea informației, care ar putea fi CISO, ar trebui să aibă autoritatea, responsabilitatea și resursele necesare pentru a coordona, dezvolta, implementa, monitoriza și menține o viziune, o strategie și un program la nivelul întregii organizații, pentru a se asigura că activele și tehnologiile informaționale sunt protejate în mod adecvat.

GV.RR-03

Resursele adecvate sunt alocate proporțional cu strategia, rolurile, responsabilitățile și politicile de management al riscului de securitate cibernetică.

GV.RR-03.1

Trebuie alocate resurse suficiente în conformitate cu strategia, rolurile, responsabilitățile și politicile de management al riscului de securitate cibernetică.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că securitatea cibernetică este susținută în mod eficace prin alinierea alocării resurselor (care pot include personal, buget, tehnologie) la prioritățile strategice, rolurile și politicile.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Ar trebui efectuate revizuiri periodice ale managementului pentru a asigura că persoanele responsabile de managementul riscului de securitate cibernetică dispun de autoritatea necesară.
- Alocarea resurselor și investițiile ar trebui stabilite în conformitate cu apetitul pentru risc al organizației.
- Ar trebui asigurate resurse umane, procese și resurse tehnice adecvate și suficiente pentru a sprijini strategia de securitate cibernetică.
- Personalul specializat ar trebui să dețină cunoștințele și competențele necesare pentru securitatea OT, pentru a permite colaborarea cu inginerii OT, astfel încât alertele să fie interpretate cu acuratețe și să se răspundă în mod eficace la amenințări.

GV.RR-03.2

Organizația trebuie să atribuie roluri și responsabilități pentru revizuirea și actualizarea planurilor de răspuns și recuperare, asigurându-se că acestea reflectă modificările din mediul de risc și rămân eficace.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura eficacitatea planurilor de răspuns și recuperare prin atribuirea de roluri și responsabilități pentru revizuirea și adaptarea periodică la riscurile în continuă evoluție.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea și atribuirea responsabilităților
  - Atribuirea de roluri clare pentru menținerea, revizuirea și actualizarea planurilor de răspuns și recuperare.
  - Asigurarea faptului că persoanele fizice responsabile au autoritatea și resursele necesare pentru a acționa în funcție de modificările identificate.
  - Desemnarea unui coordonator central sau a unei echipe pentru supravegherea procesului de actualizare și asigurarea răspunderii.
- Înțelegerea și monitorizarea contextului organizațional
  - Evaluarea periodică a factorilor interni și externi, precum:
    - Structura organizațională și sistemele critice.
    - Amenințările și vulnerabilitățile emergente.
    - Modificările reglementărilor și dinamica pieței.
    - Lecțiile învățate din incidente, teste sau exerciții.
- Actualizarea planurilor în funcție de modificările contextuale
  - Revizuirea planurilor pentru a reflecta:
    - Amenințările noi sau în evoluție.
    - Modificările tehnologiei sau infrastructurii.
    - Provocările operaționale sau lacunele identificate în timpul testării.
  - Actualizările pot include liste de contacte, protocoale de comunicare, căi de escaladare și alocări de resurse.

- Comunicarea și instruirea
  - Asigurarea informării părților interesate relevante cu privire la actualizări.
  - Furnizarea de instruire sau sesiuni de informare pentru a clarifica rolurile și responsabilitățile din planurile revizuite.
- Testare și îmbunătățire
  - Efectuarea de exerciții și simulări periodice pentru validarea eficacității planurilor actualizate.
  - Utilizarea rezultatelor pentru identificarea lacunelor și stimularea îmbunătățirii continue.
- Ciclul de revizuire continuă
  - Stabilirea unui calendar de revizuire (de exemplu, trimestrial sau după modificări majore).
  - Integrarea actualizărilor planului în procesele mai ample de management al riscului și de guvernanță.

GV.RR-04

Securitatea cibernetică este inclusă în practicile de resurse umane.

GV.RR-04.1

Personalul care are acces la informațiile sau tehnologiile cele mai critice ale organizației trebuie să fie autentificat.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a proteja activele critice prin asigurarea faptului că numai personalul autentificat poate avea acces la acestea.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- „Autentificat" înseamnă că utilizatorul trebuie să-și dovedească identitatea din punct de vedere tehnic la punctul de acces, în mod ideal utilizând MFA sau metode mai puternice, nu doar validat în timpul procesului de integrare organizațională.
- Accesul la informații sau tehnologii critice ar trebui luat în considerare în cadrul recrutării, în cadrul procesului de integrare organizațională, pe durata relațiilor contractuale, la modificarea funcției și în cadrul procesului de ieșire organizațională (încetarea relațiilor contractuale).
- Verificările de fond ar trebui efectuate înainte de integrarea noului personal în roluri sensibile, iar verificările de fond ar trebui repetate periodic pentru personalul care ocupă astfel de roluri. Verificările de fond ar trebui totuși să țină cont de legile, reglementările și principiile etice aplicabile, proporțional cu cerințele organizației, clasificarea informațiilor la care se va avea acces și riscurile percepute.
- Expertiza în domeniul securității cibernetice ar trebui recunoscută ca un atu valoros în deciziile de recrutare, instruire și retenție a personalului.

GV.RR-04.2

Trebuie elaborat și menținut un proces de securitate cibernetică pentru resurse umane, aplicabil la recrutare, pe durata angajării și la încetarea contractului de muncă.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura gestionarea riscurilor de securitate cibernetică pe tot parcursul ciclului de viață al angajaților, prin integrarea securității în procesele de resurse umane, de la angajare până la încetarea contractului de muncă.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Considerentele privind managementul riscului de securitate cibernetică ar trebui integrate în procesele de resurse umane (de exemplu, verificarea personalului, procesul de integrare organizațională, notificarea modificărilor și procesul de ieșire organizațională).
- Procesul de securitate cibernetică a resurselor umane ar trebui să includă accesul la informații sau tehnologii critice, verificări de fond, codul de conduită, roluri, atribuții de autoritate și responsabilități.
- Obligațiile personalului de a cunoaște, adera și respecta politicile de securitate în raport cu rolul lor ar trebui definite și puse în aplicare.

[GV.PO] POLITICI

Politica organizației privind securitatea cibernetică este stabilită, comunicată și pusă în aplicare.

GV.PO-01

Politica de gestionare a riscurilor de securitate cibernetică este stabilită pe baza contextului organizațional, a strategiei de securitate cibernetică și a priorităților și este comunicată și pusă în aplicare.

GV.PO-01.1

Politicile și procedurile pentru gestionarea securității cibernetice sau a informației trebuie stabilite, documentate, revizuite, aprobate, actualizate atunci când apar modificări, comunicate și puse în aplicare.

GHID DE IMPLEMENTARE

Acest Control stabilește baza modului în care ar trebui gestionate toate politicile și procedurile privind securitatea cibernetică sau a informației. Acesta pune accentul pe ciclul de viață al guvernanței, de la creare până la punerea în aplicare și asigură alinierea la direcția strategică a organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Elaborarea de politici, procese și proceduri clare și practice care:
  - Definesc comportamente și așteptări acceptabile pentru protejarea informațiilor și sistemelor organizației.
  - Precizează modul în care conducerea se așteaptă ca angajații să utilizeze și să protejeze resursele organizației.
- Asigurarea conștientizării angajaților prin comunicarea acestor politici, procese și proceduri:
  - La integrarea organizațională a noului personal;
  - Ori de câte ori se fac actualizări sau modificări semnificative;
  - Menținerea accesibilității, prin punerea cu ușurință la dispoziția angajaților a tuturor documentelor relevante.
- Revizuirea și actualizarea periodice (de exemplu, anual) pentru a reflecta:
  - Modificările organizaționale, precum fuziuni, achiziții sau noi obligații contractuale.
  - Evoluții tehnologice, precum adoptarea inteligenței artificiale sau a unor noi instrumente de securitate.

- Definirea criteriilor de evaluare a riscurilor în cadrul politicii de management al riscului a organizației:
  - Organizația ar trebui să stabilească și să documenteze criterii clare pentru determinarea probabilității și impactului riscurilor.
  - Aceste criterii ar trebui adaptate contextului specific al organizației și utilizate în mod consecvent pentru evaluarea și prioritizarea riscurilor de securitate cibernetică. Astfel se asigură că deciziile bazate pe risc sunt aliniate la strategia generală și la apetitul pentru risc al organizației.

GV.PO-01.2

Politicile și procedurile privind securitatea cibernetică sau a informației la nivelul întregii organizații trebuie să includă utilizarea criptografiei și, după caz, a criptării, să reflecte modificările în ceea ce privește cerințele, amenințările, tehnologia și rolurile organizației și să fie aprobate de conducerea superioară, care supraveghează punerea lor în aplicare.

GHID DE IMPLEMENTARE

Acest Control se bazează pe GV.PO-01.1 și se concentrează pe conținutul și supravegherea politicilor de securitate cibernetică sau a informației. Acesta asigură abordarea unor subiecte tehnice specifice (precum criptografia și criptarea), adaptarea politicilor la modificări și implicarea activă a conducerii superioare în procesul de aprobare și supraveghere.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea domeniului de aplicare și a obiectivelor
    - Asigurarea aplicării politicilor la nivelul întregii organizații și a alinierii acestora cu prioritățile organizației și cu cele de risc.
- Includerea criptografiei și a criptării
    - Abordarea criptării în repaus/în tranzit, managementul cheilor și algoritmii aprobați.
    - Definirea cazurilor când criptarea este necesară (de exemplu, date personale, acces la distanță).
- Menținerea politicilor actualizate
    - Actualizarea politicilor pentru a reflecta modificările în:
        - Cerințele legale/de reglementare;
        - Peisajul amenințărilor;
        - Tehnologie;
        - Structura organizațională.
- Supravegherea realizată de către conducerea superioară
    - Solicitarea aprobării formale a conducerii superioare a organizației.
    - Desemnarea unui responsabil de politici (de exemplu, CISO) pentru supravegherea implementării și conformității.

- Atribuirea rolurilor și responsabilităților
  - Utilizarea profilurilor de rol ECSF elaborat de către ENISA (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles) pentru:
    - Definirea rolurilor în domeniul securității cibernetice (de exemplu, responsabil de politici, manager de risc);
    - Alinierea sarcinilor, abilităților și competențelor.
- Comunicarea și instruirea
  - Diseminarea politicilor și furnizarea de instruire specifică rolului.
- Monitorizarea și punerea în aplicare
  - Utilizarea controalelor tehnice și auditurilor pentru a asigura conformitatea.

[GV.OV] SUPRAVEGHERE

Rezultatele activităților și performanțelor de management al riscului de securitate cibernetică la nivelul întregii organizații sunt utilizate pentru a informa, îmbunătăți și ajusta strategia de management al riscului.

GV.OV-02

Strategia de management al riscului de securitate cibernetică este revizuită și ajustată pentru a asigura acoperirea cerințelor și riscurilor organizației.

GV.OV-02.1

Strategia de management al riscului de securitate cibernetică sau a informației trebuie revizuită și ajustată pentru asigurarea acoperirii cerințelor și riscurilor organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că strategia de management al riscului de securitate cibernetică sau a informației este revizuită și actualizată periodic pentru a reflecta nevoile organizației, riscurile în evoluție și cerințele de conformitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Strategia ar trebui să definească direcția generală și obiectivele pentru gestionarea riscurilor de securitate cibernetică sau a informației.
- Politicile și procedurile de sprijin ar trebui să ghideze modul în care strategia este pusă în practică.
- Strategia ar trebui să abordeze riscurile pentru operațiunile organizației, activele, persoanele fizice și alte entități, inclusiv potențialele impacturi asupra vieții private.
- Revizuirile ar trebui efectuate la intervale planificate, inclusiv prin audituri interne, pe baza unui program de audit documentat care definește frecvența, metodele, responsabilitățile și raportarea.
- Auditurile ar trebui efectuate de personal competent și imparțial.
- Rezultatele auditului ar trebui revizuite pentru a evalua dacă strategia îndeplinește așteptările interne și respectă cerințele legale și de reglementare.
- Strategia ar trebui actualizată atunci când este necesar, în special după incidente sau constatări ale auditului.
- Dovezile activităților de audit și rezultatele acestora ar trebui documentate și raportate conducerii relevante.

GV.OV-03

Performanța organizației în materie de management al riscului de securitate cibernetică este evaluată și revizuită pentru identificarea ajustărilor necesare.

GV.OV-03.1

Performanța organizației în materie de management al riscului de securitate cibernetică trebuie evaluată, revizuită și ajustată atunci când este necesar.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că performanța organizației în materie de management al riscului de securitate cibernetică este evaluată, revizuită și ajustată în mod continuu, după cum este necesar.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Indicatorii cheie de performanță (KPI) ar trebui identificați, implementați și revizuiți periodic pentru a asigura că politicile și procedurile la nivelul întregii organizații ating obiectivele în materie de securitate cibernetică sau a informației.
- Indicatorii cheie de risc de securitate cibernetică sau a informației ar trebui evaluați periodic pentru identificarea riscurilor la care este expusă organizația, inclusiv probabilitatea și impactul potențial. Indicatorii de risc de securitate cibernetică sau a informației sunt, de exemplu:
  - Numărul de atacuri cibernetice detectate.
  - Numărul de scurgeri de date detectate.
  - Timpul necesar pentru detecție.
  - Timpul necesar pentru recuperare.
  - Numărul de dispozitive care nu sunt gestionate de organizație.
  - Nivelul de acces al diferiților utilizatori la datele sensibile.
  - Numărul de software și sisteme neactualizate.
  - Numărul conexiunilor de rețea negestionate.
- Indicatorii privind managementul riscului de securitate cibernetică sau a informației ar trebui colectați și comunicați conducerii superioare a organizației.

[GV.SC] C-SCRM

Procesele C-SCRM sunt identificate, stabilite, gestionate, monitorizate și îmbunătățite de către părțile interesate ale organizației.

GV.SC-01

Un program, o strategie, obiective, politici și procese C-SCRM sunt stabilite și convenite de părțile interesate ale organizației.

GV.SC-01.1

Un program, o strategie, obiective, politici și procese C-SCRM trebuie documentate, revizuite, actualizate atunci când apar modificări și aprobate de părțile interesate ale organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura gestionarea proactivă a riscurilor de securitate cibernetică ale lanțului de aprovizionare printr-un program de management al riscului documentat, aprobat de părțile interesate și actualizat periodic.

Organizațiile ar trebui să ia în considerare pașii de mai jos pentru stabilirea unui program C-SCRM care să fie aliniat la obiectivele lor strategice și susținut de toate părțile interesate relevante:

- Definirea programului și a strategiei
    - Identificarea obiectivelor
        - Definirea clară a ceea ce urmărește să realizeze organizația prin programul său C-SCRM. Obiectivele pot include protecția împotriva atacurilor în lanțul de aprovizionare, asigurarea conformității cu reglementările și menținerea continuității activității.
    - Dezvoltarea unei strategii
        - Conturarea unei strategii la nivel înalt, aliniată cu strategiile generale de securitate cibernetică și ale activității organizației. Aceasta ar trebui să includă planuri de evaluare a riscurilor, de atenuare a riscurilor și de monitorizare continuă.
- Implicarea părților interesate
    - Identificarea părților interesate
        - Determinarea părților interesate cheie, inclusiv echipele de conducere, IT, achiziții, juridic și conformitate.
    - Implicarea părților interesate
        - Implicarea părților interesate încă din faza incipientă a procesului pentru a asigura contribuția și acceptul acestora. Aceasta se poate realiza prin intermediul atelierelor, întâlnirilor și actualizărilor periodice.

- Stabilirea politicilor și proceselor
  - Elaborarea politicilor
    - Crearea unor politici documentate cuprinzătoare care să acopere toate aspectele C-SCRM, inclusiv managementul riscului vânzătorilor, răspunsul la incidente și cerințele de conformitate.
  - Implementarea proceselor
    - Definirea și documentarea proceselor de evaluare a riscurilor, evaluare a vânzătorilor, gestionare a contractelor și răspuns la incidente. Asigurarea integrării acestor procese în fluxurile de lucru existente ale organizației.
- Evaluarea și managementul riscului
  - Efectuarea evaluărilor riscurilor
    - Evaluarea periodică a riscurilor asociate lanțului de aprovizionare, inclusiv a potențialelor vulnerabilități și amenințări.
  - Atenuarea riscurilor
    - Elaborarea și implementarea unor strategii de atenuare a riscurilor pe baza rezultatelor evaluării. Acestea pot include diversificarea furnizorilor, îmbunătățirea controalelor de securitate și stabilirea planurilor de urgență.
- Monitorizarea și îmbunătățirea continue
  - Monitorizarea continuă
    - Implementarea monitorizării continue a lanțului de aprovizionare pentru detecția și răspunsul prompt la noile riscuri. Aceasta include monitorizarea performanței și conformității furnizorilor.
  - Revizuirea și îmbunătățirea
    - Revizuirea periodică a eficacității programului C-SCRM și îmbunătățirea după cum este necesar. Aceasta ar trebui să includă observațiile părților interesate și lecțiile învățate din incidente.

- Instruirea și conștientizarea
  - Educarea angajaților
    - Furnizarea unor programe de instruire și conștientizare pentru angajați, pentru ca aceștia să înțeleagă rolul lor în C-SCRM. Aceasta include recunoașterea riscurilor din lanțul de aprovizionare și respectarea politicilor și procedurilor stabilite.
- Documentarea și comunicarea
  - Documentarea tuturor elementelor relevante
    - Asigurarea că toate politicile, procesele, evaluările riscurilor și planurile de atenuare sunt bine documentate, actualizate, aprobate de către persoana din conducerea organizației cu atribuții în acest sens și accesibile părților interesate relevante.
  - Comunicarea eficace
    - Menținerea unor linii de comunicare deschise cu părțile interesate pentru a le ține la curent cu progresul programului, modificările și orice incidente care apar.

GV.SC-02

Rolurile și responsabilitățile în materie de securitate cibernetică pentru furnizori, clienți și parteneri sunt stabilite, comunicate și coordonate la nivel intern și extern.

GV.SC-02.1

Furnizorii terți trebuie să notifice orice transfer, încetare sau tranziție a personalului cu acces fizic sau logic la elementele sistemului critic pentru activitate ale organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura continuitatea și securitatea sistemelor critice, impunând furnizorilor terți să raporteze modificările de personal care afectează accesul.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Furnizorii terți includ, de exemplu, furnizori de servicii, contractori și alte organizații care furnizează servicii de dezvoltare de sisteme, servicii tehnologice, aplicații externalizate sau managementul rețelelor și securității.
- Regulile și protocoalele pentru schimbul de informații între organizație și furnizorii săi și furnizorii de nivel inferior ar trebui definite în acordurile contractuale.

GV.SC-03

C-SCRM este integrat în procesele de management al riscului de securitate cibernetică și procesele ERM, precum și în cele de evaluare a riscurilor și de îmbunătățire.

GV.SC-03.1

C-SCRM sau a informației trebuie integrat în procesele de management al riscului de securitate cibernetică sau a informației, în procesele ERM, în evaluarea riscurilor, precum și în procesele de îmbunătățire.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că riscurile de securitate cibernetică din lanțul de aprovizionare sunt identificate, evaluate și atenuate în mod consecvent, prin integrarea acestora în evaluările riscurilor organizației, revizuirile controalelor și ciclurile de îmbunătățire continuă.

Pentru integrarea în mod eficace a managementului riscului în lanțul de aprovizionare în cadrele mai largi de securitate cibernetică și de risc la nivel de organizație, organizațiile ar trebui să ia în considerare următoarele:

- Identificarea alinierii și suprapunerii
    - Identificarea proceselor existente de management al riscului de securitate cibernetică sau a informației și ERM.
    - Identificarea punctelor de contact în care riscurile lanțului de aprovizionare se intersectează cu:
        - Managementul vânzătorilor.
        - Achiziții.
        - Continuitatea activității.
        - Aspecte juridice și de conformitate.
    - Documentarea zonelor de suprapunere, duplicare sau lacune pentru a eficientiza integrarea.
- Stabilirea unor seturi de controale integrate
    - Dezvoltarea unui cadru de control unificat care să includă:
        - Controale specifice securității cibernetice a lanțului de aprovizionare (de exemplu, accesul părților terțe, gestionarea datelor, integritatea software-ului).
        - Controale din standardele existente de securitate cibernetică (de exemplu, ISO/IEC 27036).

- Asigurarea că controalele sunt bazate pe risc, scalabile și aliniate atât la mediile IT, cât și la cele OT.

- Integrarea în procesele de evaluare a riscurilor
  - Includerea scenariilor de amenințări specifice lanțului de aprovizionare în evaluările riscurilor (de exemplu, compromiterea furnizorilor, hardware contrafăcut, vulnerabilități software).
  - Evaluarea criticității furnizorilor și a expunerii la risc ca parte a registrului de riscuri ale organizației.
  - Utilizarea unei evaluări a riscurilor pe niveluri, bazată pe impactul furnizorului și sensibilitatea serviciilor/datelor.
- Integrarea în procesul de îmbunătățire continuă
  - Încorporarea informațiilor privind riscurile lanțului de aprovizionare în:
    - Lecțiile învățate din incidente și audituri.
    - Revizuirile post-mortem ale întreruperilor legate de furnizori.
    - Ciclurile de îmbunătățire a proceselor (de exemplu, planifică-execută-verifică-acționează - PDCA).
  - Actualizarea politicilor, procedurilor și controalelor pe baza amenințărilor în evoluție și a performanței furnizorilor.
- Escaladarea riscurilor semnificative la nivelul conducerii superioare a organizației
  - Definirea criteriilor de semnificație (de exemplu, impactul financiar, expunerea la reglementări, întreruperi operaționale).
  - Stabilirea unei căi formale de escaladare către conducerea superioară și comitetele de risc.
  - Asigurarea că riscurile semnificative din lanțul de aprovizionare sunt:
    - Reflectate în registrul de riscuri ale organizației.
    - Abordate în discuțiile strategice privind riscurile.
    - Luate în considerare în planificarea continuității activității și a managementului crizelor.

GV.SC-05

Cerințele privind abordarea riscurilor de securitate cibernetică în lanțurile de aprovizionare sunt stabilite, prioritizate și integrate în contracte și alte tipuri de acorduri cu furnizorii și alte părți terțe relevante.

GV.SC-05.1

Cerințele privind abordarea riscurilor de securitate cibernetică și schimbul de informații sensibile în lanțurile de aprovizionare trebuie stabilite, prioritizate, integrate în contracte și alte tipuri de acorduri formale și puse în aplicare.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a stabili și a pune în aplicare cerințele privind securitatea cibernetică și gestionarea datelor sensibile în acordurile privind lanțul de aprovizionare prin integrarea acestora în contracte și prioritizarea lor în funcție de risc.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Acordurile contractuale și alte tipuri de acorduri formale cu furnizorii și alte părți terțe relevante ar trebui să definească așteptările, responsabilitățile și cerințele de securitate.
- Elementele cheie ale acestor acorduri includ schimbul de informații între organizație și furnizorii săi și furnizorii de nivel inferior, controale de securitate, răspunsul la incidente și respectarea standardelor și reglementărilor.
- Cerințele de securitate pentru furnizori, produse și servicii ar trebui să fie proporționale cu criticitatea și consecințele potențiale în cazul compromiterii acestora.
- Toate cerințele privind securitatea cibernetică și lanțul de aprovizionare pe care părțile terțe trebuie să le respecte ar trebui incluse în limbajul contractual standard (adică termeni și clauze pre-redactate, utilizate în mod obișnuit, care asigură coerența, conformitatea și claritatea). Contractul ar trebui să specifice, de asemenea, modul în care va fi verificată conformitatea cu aceste cerințe.
- Luarea în considerare a includerii în punerea în aplicare a faptului că furnizorii și utilizatorii terți (de exemplu, furnizori, clienți, parteneri) ar trebui să poată demonstra înțelegerea rolurilor și responsabilităților lor.
- Luarea în considerare a definirii cerințelor de securitate în acordurile pentru nivelul serviciilor (SLA) pentru monitorizarea furnizorilor în ceea ce privește performanța acceptabilă în materie de securitate pe tot parcursul ciclului de viață al relației cu furnizorul.

- Luarea în considerare a posibilității de a impune contractual furnizorilor să își verifice angajații și să se protejeze împotriva amenințărilor din interior.
- Luarea în considerare a posibilității de a impune contractual furnizorilor să furnizeze dovezi ale aplicării unor practici de securitate acceptabile, de exemplu, prin autoevaluare (de exemplu, CyFun®), conformitate cu standardele cunoscute, verificări (de exemplu, CyFun®), certificări (de exemplu, CyFun®) sau inspecții.
- Reținerea faptului că cerințele Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE, denumit în continuare Regulamentul GDPR sau GDPR, trebuie respectate dacă informațiile aferente activității conțin date cu caracter personal (aplicabile la toate nivelurile), adică în cadrul contractual trebuie incluse măsuri de protecție.

GV.SC-05.2

Cerințele contractuale privind securitatea cibernetică sau a informației pentru furnizori și parteneri externi trebuie implementate pentru a asigura un proces verificabil de rezolvare a defectelor și pentru a garanta că deficiențele identificate în timpul testării și evaluării securității cibernetice sau a informației sunt remediate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control, care este corelat cu GV.SC-09.1, este de a integra cerințe care pot fi puse în aplicare în contractele cu furnizorii pentru a garanta rezolvarea în timp util a defectelor și rezolvarea problemelor de securitate cibernetică identificate prin testare și evaluare.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Sistemele informatice care conțin software (sau firmware) afectate de defectele software anunțate recent (și potențialele vulnerabilități rezultate din aceste defecte) ar trebui identificate.
- Patch-urile, pachetele de servicii și remedierile rapide relevante pentru securitate recent lansate ar trebui instalate, iar aceste patch-uri, pachete de servicii și remedieri rapide sunt testate în ceea ce privește eficacitatea și potențialele efecte secundare asupra sistemelor informatice ale organizației înainte de instalare. Deficiențele descoperite în timpul evaluărilor de securitate, monitorizării continue, activităților de răspuns la incidente sau gestionării erorilor sistemului informatic sunt, de asemenea, remediate cu promptitudine. Remedierea defectelor ar trebui încorporată în managementul configurației ca modificare de urgență.
- Luarea în considerare a posibilității de a impune contractual furnizorilor să divulge caracteristici de securitate cibernetică sau a informației, funcții și vulnerabilități ale produselor și serviciilor lor pe durata de viață a produsului sau pe durata serviciului.
- Luarea în considerare a posibilității de a impune contractual furnizorilor să furnizeze și să mențină un inventar actualizat al componentelor (de exemplu, Lista componentelor software - SBOM sau Lista componentelor hardware - HBOM) pentru produsele critice.

GV.SC-05.3

Organizația trebuie să stabilească cerințe contractuale care să îi permită să revizuiască programele de securitate cibernetică sau a informației implementate de furnizori și parteneri terți.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația poate evalua și verifica practicile de securitate cibernetică sau a informației ale furnizorilor și partenerilor terți prin acorduri contractuale. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Cerințe privind securitatea cibernetică sau a informației
    - Contractele ar trebui să definească așteptări clare în materie de securitate cibernetică sau a informației, inclusiv controale specifice OT, acolo unde este cazul.
- Drepturi de audit și revizuire
    - Acordurile ar trebui să acorde organizației dreptul de a audita, evalua sau revizui programele de securitate cibernetică sau a informației ale furnizorilor și partenerilor.
- Metode de verificare
    - Conformitatea ar trebui verificată prin autoevaluări, certificări ale unor părți terțe sau evaluări de securitate programate.
- Protocoale de schimb de informații
    - Contractele ar trebui să specifice ce informații legate de securitate cibernetică sau a informației trebuie partajate, cât de des și prin ce canale.
- Monitorizare continuă
    - Furnizorii ar trebui să raporteze periodic postura de securitate cibernetică sau a informației și să dezvăluie incidentele care ar putea afecta operațiunile, în special în mediile OT.
- Consecințele neconformității
    - Contractele ar trebui să precizeze consecințele nerespectării cerințelor privind securitatea cibernetică sau a informației, precum sancțiuni sau rezilierea contractului.

GV.SC-06

Planificarea și due diligence sunt efectuate pentru a reduce riscurile înainte de stabilirea unor relații formale cu furnizorii sau cu alte părți terțe.

GV.SC-06.1

Planificarea și due diligence trebuie efectuate pentru a reduce riscurile înainte de stabilirea unor relații formale cu furnizorii sau cu alte părți terțe.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscurile de securitate cibernetică și operaționale prin asigurarea faptului că planificarea și due diligence sunt efectuate în mod corespunzător înainte de stabilirea unor relații formale cu furnizorii sau cu părți terțe.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Due diligence bazat pe risc
    - Due diligence ar trebui efectuat asupra furnizorilor potențiali în conformitate cu politica de achiziții a organizației și ajustat la nivelul de risc, criticitate și complexitate al relației.
- Evaluarea capabilităților în materie de securitate cibernetică și de management al riscului
    - Maturitatea în materie de securitate cibernetică, practicile de management al riscului și capabilitățile specifice OT ale furnizorilor ar trebui evaluate din punct de vedere al adecvării.
- Evaluarea riscurilor furnizorilor
    - Evaluările riscurilor ar trebui efectuate pentru asigurarea alinierii la nevoile organizației și la cerințele aplicabile în materie de securitate cibernetică, inclusiv cele relevante pentru mediile OT.
- Integritatea și securitatea produselor
    - Autenticitatea, integritatea și securitatea produselor și componentelor critice ar trebui verificate înainte de achiziție și punere în funcțiune, în special în sistemele OT în care vulnerabilitățile pot afecta siguranța și operațiunile.

GV.SC-07

Riscurile prezentate de un furnizor, produsele și serviciile acestuia și alte părți terțe sunt înțelese, înregistrate, prioritizate, evaluate, gestionate și monitorizate pe parcursul relației.

GV.SC-07.1

Riscurile prezentate de un furnizor, produsele și serviciile sale și alte părți terțe trebuie identificate, documentate, prioritizate, atenuate și evaluate cel puțin anual și atunci când apar modificări în cursul relației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că riscurile legate de furnizori, produsele și serviciile acestora și alte părți terțe sunt identificate, evaluate, prioritizate și gestionate în mod continuu pe tot parcursul relației, în special atunci când apar modificări în sistemele critice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Evaluări ale riscurilor personalizate
    - Formatele și frecvențele evaluărilor ar trebui adaptate în funcție de reputația furnizorului și de criticitatea produselor sau serviciilor furnizate, inclusiv a componentelor OT.
- Considerații mai ample privind riscurile
    - Evaluările riscurilor ar trebui să includă potențiale întreruperi ale serviciilor și riscuri de concentrare care ar putea afecta operațiunile sau mediile OT.
- Dovezi de conformitate
    - Furnizorii ar trebui să furnizeze dovezi ale conformității cu cerințele contractuale privind securitatea cibernetică, precum autoevaluări (de exemplu, CyFun®), certificări, garanții, rezultate ale testelor, etichete sau rapoarte de audit realizate de părți terțe.
- Monitorizare continuă
    - Furnizorii critici ar trebui monitorizați pe tot parcursul relației prin inspecții, audituri, teste sau alte metode de evaluare pentru a se asigura că obligațiile de securitate sunt îndeplinite în continuare.

- Actualizări ale profilului de risc
    - Modificările serviciilor, produselor sau performanțelor furnizorilor ar trebui să determine o reevaluare a profilului de risc și a criticității, în special atunci când sunt implicate sisteme OT.
- Planificarea continuității activității
    - Ar trebui să existe un plan de acțiune pentru a face față întreruperilor neașteptate ale furnizorilor și pentru a menține continuitatea operațională.

GV.SC-07.2

Trebuie stabilită, actualizată și pusă la dispoziție online și offline o listă documentată a tuturor furnizorilor, vânzătorilor și partenerilor critici ai organizației care ar putea fi implicați într-un incident major, ținând seama în mod corespunzător de confidențialitate și securitate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura menținerea și accesibilitatea unei liste fiabile și actualizate a furnizorilor, vânzătorilor și partenerilor critici, atât online, cât și offline, pentru a sprijini răspunsul rapid în cazul incidentelor majore, protejând în același timp confidențialitatea și securitatea. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Menținerea unei înregistrări complete
    - Ar trebui menținută o listă completă a furnizorilor, vânzătorilor și partenerilor, ca bază pentru identificarea celor critici pentru operațiuni, inclusiv mediile OT.
- Definirea criteriilor de criticitate
    - Ar trebui stabilite criterii clare pentru clasificarea criticității furnizorilor pe baza unor factori precum:
        - Sensibilitatea datelor prelucrate.
        - Accesul la sisteme sau rețele.
        - Importanța pentru activitatea principală sau funcțiile OT.
- Documentarea informațiilor cheie
    - Pentru fiecare furnizor critic, lista ar trebui să includă:
        - Detalii de contact primare și secundare.
        - Descrierea serviciilor furnizate.
        - Căi de escaladare și disponibilitatea asistenței.
- Asigurarea disponibilității online și offline
    - Lista ar trebui să fie:
        - Actualizată periodic și stocată în mod securizat.
        - Accesibilă atât online, cât și offline (de exemplu, copii tipărite, dispozitive USB criptate) pentru asigurarea disponibilității în timpul incidentelor cibernetice sau al întreruperilor.

GV.SC-07.3

Organizația trebuie să auditeze furnizorii terți de servicii critice pentru activitate, în vederea conformității cu cerințele de securitate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că furnizorii terți de servicii critice pentru activitate sunt auditați periodic pentru a confirma conformitatea cu cerințele de securitate convenite, contribuind la gestionarea riscurilor privind operațiunile și sistemele critice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea furnizorilor critici
    - Criticitatea furnizorilor terți de servicii ar trebui evaluată pe baza impactului acestora asupra operațiunilor, inclusiv asupra sistemelor OT, și a nivelului de risc pe care îl introduc.
- Dovezi de audit acceptabile
    - Rezultatele auditurilor efectuate de părți terțe, precum certificările, evaluările independente sau atestările de securitate, ar trebui acceptate ca dovezi valabile ale conformității, acolo unde este cazul.
- Efectuarea auditurilor de securitate
    - Ar trebui efectuate audituri periodice asupra furnizorilor critici pentru a verifica dacă aceştia îndeplinesc obligațiile contractuale și de securitate bazate pe politici.

GV.SC-07.4

Organizația trebuie să asigure conformitatea cu obligațiile contractuale privind securitatea cibernetică sau a informației ale furnizorilor și partenerilor terți prin revizuiri periodice ale auditurilor independente, evaluărilor și a celor efectuate de părți terțe.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că furnizorii și partenerii terți respectă obligațiile contractuale privind securitatea cibernetică sau a informației, prin revizuirea periodică a auditurilor independente, a evaluărilor și a altor evaluări efectuate de părți terțe.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Fundamentarea pe controale conexe
    - Acest Control ar trebui implementat în conformitate cu GV.SC-05.3 și GV.SC-07.1 pentru a consolida supravegherea furnizorilor.
- Integrarea evaluărilor riscurilor
    - Auditurile independente și evaluările efectuate de părți terțe ar trebui să includă evaluări ale cerințelor corporative și ale cerințelor aplicabile în materie de securitate cibernetică, inclusiv riscurile specifice lanțului de aprovizionare și OT.
- Verificare înainte de inițierea colaborării
    - Înainte de angajarea furnizorilor critici, evaluările independente ar trebui revizuite pentru confirmarea conformității cu standardele și obligațiile convenite în materie de securitate cibernetică.
- Profunzimea revizuirii bazate pe risc
    - Profunzimea și frecvența revizuirilor ar trebui adaptate în funcție de criticitatea produselor sau serviciilor furnizorului. Furnizorii cu nivel mai ridicat de criticitate ar trebui să fie supuși unor evaluări mai aprofundate.

GV.SC-08

Furnizorii relevanți și alte părți terțe sunt incluși în activitățile de planificare, răspuns și recuperare în caz de incidente.

GV.SC-08.1

Organizația trebuie să identifice și să documenteze personalul cheie al furnizorilor relevanți și al altor părți terțe pentru a-i integra în activitățile de planificare, răspuns și recuperare în caz de incidente.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida pregătirea pentru incidente și recuperarea ulterioară, prin asigurarea identificării și integrării active a personalului cheie al furnizorilor critici și al altor părți terțe în planificarea și desfășurarea activităților de răspuns la incidente.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Stabilirea protocoalelor de comunicare
    - Ar trebui definite reguli și proceduri clare pentru raportarea stării incidentelor și coordonarea activităților de răspuns și recuperare între organizație și furnizorii săi critici pentru activitate.
- Definirea rolurilor și responsabilităților
    - Rolurile, responsabilitățile și autoritatea pentru răspunsul la incidente ar trebui documentate atât pentru echipele interne, cât și pentru participanții terți, inclusiv cei care susțin sistemele și infrastructura OT.
- Promovarea învățării comune
    - După incidente majore, ar trebui organizate, împreună cu furnizorii critici și părțile terțe, sesiuni de analiză a lecțiilor învățate, pentru a îmbunătăți coordonarea și reziliența în viitor.

GV.SC-09

Practicile de securitate a lanțului de aprovizionare sunt integrate în programele de securitate cibernetică și ERM, iar performanța acestora este monitorizată pe tot parcursul ciclului de viață al produselor și serviciilor tehnologice.

GV.SC-09.1

Practicile de securitate a lanțului de aprovizionare trebuie integrate în programele de securitate cibernetică sau a informației și ERM, iar performanța acestora trebuie monitorizată pe tot parcursul ciclului de viață al produselor și serviciilor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că practicile de securitate a lanțului de aprovizionare sunt integrate în programele de securitate cibernetică sau a informației și ERM, performanța acestora fiind monitorizată și îmbunătățită pe tot parcursul ciclului de viață al produselor și serviciilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Alinierea la controalele conexe
    - Acest Control se bazează pe GV.SC-05.2, asigurând că cerințele contractuale privind securitatea cibernetică sau a informației, precum rezolvarea defectelor și remedierea deficiențelor identificate, sunt gestionate în mod activ în cadrul programelor de risc mai ample.
- Stabilirea bazelor de guvernanță
    - Politicile de securitate ale lanțului de aprovizionare ar trebui documentate, acoperind așteptările în materie de securitate cibernetică sau a informației pentru furnizori și părți terțe.
- Integrarea în cadrele de risc
    - Riscurile lanțului de aprovizionare ar trebui integrate în cadrele de management al riscului la nivel de organizație și de securitate a informației, inclusiv riscurile și dependențele specifice OT.
- Formalizarea așteptărilor în materie de securitate
    - Contractele și SLA-urile ar trebui să includă clauze clare privind securitatea cibernetică sau a informației, drepturile de audit și indicatorii de performanță.
- Monitorizarea și evaluarea performanței
    - Evaluările riscurilor, rapoartele de audit și înregistrările incidentelor ar trebui revizuite periodic pentru evaluarea posturii furnizorului și identificarea domeniilor care necesită îmbunătățiri.

- Facilitarea monitorizării continue
    - Instrumentele de monitorizare și KPI-urile ar trebui utilizate pentru urmărirea performanței furnizorilor în materie de securitate pe parcursul întregului ciclu de viață, inclusiv timpul de răspuns la incidente și ratele de conformitate.
- Sprijinirea conștientizării și instruirii
    - Programele de instruire și conștientizare ar trebui să abordeze riscurile de securitate cibernetică sau a informației legate de lanțul de aprovizionare atât pentru echipele interne, cât și pentru furnizori.
- Asigurarea acoperirii ciclului de viață
    - Documentația ar trebui să demonstreze că securitatea lanțului de aprovizionare este luată în considerare de la achiziție până la scoatere din uz și dezafectare, în special pentru sistemele și componentele OT.

GV.SC-10

Planurile C-SCRM includ dispoziții pentru activitățile care au loc după încheierea unui parteneriat sau a unui contract de servicii.

GV.SC-10.1

Planurile C-SCRM trebuie să includă măsuri și responsabilități pentru gestionarea riscurilor care pot apărea după încheierea unei relații cu un furnizor sau a unui contract de servicii.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că riscurile reziduale de securitate cibernetică sau a informației sunt abordate în mod eficace după încetarea relațiilor cu furnizorii, prevenind astfel întreruperile, expunerea datelor și vulnerabilitățile în mediile operaționale și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Planificarea încetării relațiilor
    - Procedurile formale de încetare a relațiilor cu furnizorii ar trebui definite atât pentru condiții normale, cât și pentru condiții nefavorabile, inclusiv în caz de încălcare a contractului, insolvență sau incidente de securitate.
- Asigurarea unei tranziții sau a unei ieșiri securizate
    - Ar trebui elaborate planuri de tranziție pentru serviciile critice, pentru menținerea continuității și abordarea rezilienței lanțului de aprovizionare, inclusiv furnizori de rezervă sau alternative interne.
- Revocarea accesului și securizarea datelor
    - Accesul furnizorilor la sisteme, rețele și date ar trebui revocat imediat. Toate datele de autentificare și instrumentele de acces la distanță ar trebui dezactivate sau eliminate.
- Protejarea activelor organizației
    - Dispozitivele, suporturile de stocare și documentele care conțin date ale organizației ar trebui returnate în mod securizat sau sanitizate. Măsurile de control ar trebui să împiedice păstrarea neautorizată sau scurgerea de informații sensibile.
- Abordarea obsolescenței componentelor
    - Ar trebui să existe planuri pentru gestionarea componentelor sau serviciilor aflate la sfârșitul ciclului de viață (EOL), asigurând asistență continuă sau înlocuiri securizate, în special pentru sistemele OT.

- Monitorizarea riscurilor reziduale
    - Riscurile post-încetare ar trebui identificate, evaluate și escaladate către conducerea superioară, atunci când este necesar. Aceste riscuri ar trebui urmărite în cadrul procesului ERM.

IDENTIFICARE

[ID.AM] MANAGEMENTUL ACTIVELOR

Activele (de exemplu, date, hardware, software, sisteme, incinte, servicii, persoane) care permit organizației să își atingă scopurile activității sunt identificate și gestionate în concordanță cu importanța lor relativă pentru obiectivele organizației și strategia de management al riscului a organizației.

ID.AM-01

Menținerea inventarelor echipamentelor hardware gestionate de organizație.

ID.AM-01.1

Un inventar al activelor de infrastructură fizică și virtuală - precum hardware, dispozitive de rețea și medii găzduite în cloud - care susțin procesarea informațiilor trebuie documentat, revizuit și actualizat, pe măsură ce apar modificări.

GHID DE IMPLEMENTARE

În timp ce ID.AM-01.1 se concentrează pe nivelul infrastructurii, acest Control este strâns legat de ID.AM-02.1, care urmărește software-ul și serviciile care rulează peste aceasta, precum aplicații, platforme și instrumente digitale. Împreună, acestea oferă o imagine completă a mediului tehnologic al organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Organizațiile ar trebui să identifice și să documenteze toate activele fizice și virtuale ale infrastructurii care susțin procesarea informațiilor, inclusiv servere, stații de lucru, dispozitive de rețea, sisteme de stocare și resurse găzduite în cloud.
- Inventarul ar trebui să includă atribute cheie, precum tipul de activ, locația, proprietarul, configurația și starea ciclului de viață.
- Organizațiile ar trebui să ia în considerare utilizarea unor instrumente automatizate de identificare și management al activelor, acolo unde este posibil, pentru asigurarea acurateței și actualizării în timp real.
- Inventarul ar trebui revizuit și actualizat periodic, în special după modificări precum punerea în funcțiune, scoaterea din uz și dezafectarea sau relocări.
- Inventarul ar trebui să fie accesibil părților interesate relevante și ar trebui integrat în procesele de management al riscului și de răspuns la incidente.

ID.AM-01.2

Inventarul activelor organizației asociate cu informațiile și spațiile de procesare a informațiilor trebuie să reflecte modificările din contextul organizațional și să includă toate informațiile necesare pentru o răspundere efectivă.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că inventarele activelor susțin transparența operațională, permit o proprietate responsabilă și se adaptează la modificările din structura, tehnologia și peisajul de risc al organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Includerea detaliilor esențiale despre active
    - Inventarele ar trebui să cuprindă specificații cheie, precum producătorul, tipul dispozitivului, modelul, numărul de serie, numele mașinii, adresa de rețea și locația fizică. Activele OT ar trebui incluse acolo unde este cazul.
- Sprijinirea răspunderii
    - Înregistrările activelor ar trebui să permită trasabilitatea măsurilor și deciziilor, asigurând că părțile responsabile pot fi identificate și trase la răspundere pentru rezultate.
- Reflectarea modificărilor organizaționale
    - Inventarele ar trebui actualizate pentru a reflecta modificări precum relocarea activelor, actualizări sau scoaterea din uz și dezafectarea, inclusiv cele care afectează mediile OT.

ID.AM-01.3

Atunci când este detectat hardware neautorizat, acesta trebuie pus în carantină pentru o eventuală gestionare a excepțiilor, eliminat sau înlocuit, iar inventarul trebuie actualizat în consecință.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscurile de securitate prin identificarea, izolarea și remedierea promptă a echipamentelor neautorizate, menținând în același timp un inventar precis al activelor, care asigură răspunderea.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea hardware-ului neautorizat
    - Orice hardware neaprobat sau care nu are excepții documentate ar trebui desemnat ca neautorizat.
- Răspunsul la detecție
    - Hardware-ul neautorizat ar trebui pus în carantină pentru revizuire, eliminare sau înlocuire, după caz. Inventarul activelor ar trebui actualizat în consecință.
- Includerea considerentelor OT
    - Dispozitivele neautorizate în mediile OT ar trebui tratate cu precauție sporită datorită potențialului impact asupra siguranței și funcționării.

Exemple de hardware neautorizat pot include:

- Endpoint-uri neaprobate
    - Laptop-uri, desktop-uri sau dispozitive mobile, personale sau neînregistrate, conectate la rețea fără autorizare.
- Dispozitive de stocare externe
    - Dispozitive USB sau hard disk-uri externe neaprobate pentru utilizare, care pot introduce riscuri de malware sau de scurgere de date.
- Dispozitive de tip Internetul lucrurilor (IoT) și OT neverificate
    - Dispozitive inteligente, senzori sau componente industriale conectate fără o verificare adecvată, care prezintă riscuri atât pentru mediile IT, cât și pentru cele OT.
- Echipamente de rețea neautorizate
    - Puncte de acces wireless sau comutatoare instalate fără aprobare, care pot ocoli controalele de securitate ale rețelei.

ID.AM-01.4

Trebuie identificate mecanismele de detecție a prezenței componentelor hardware și firmware neautorizate în mediul TIC/OT al organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a identifica proactiv componentele hardware și firmware neautorizate în mediile TIC și OT, permițând astfel un răspuns prompt și reducând riscul de compromitere sau de întrerupere a operațiunilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Automatizarea acolo unde este fezabil
    - Mecanismele de detecție ar trebui automatizate acolo unde este sigur și posibil din punct de vedere tehnic, în special în medii complexe sau cu risc ridicat.
- Monitorizarea continuă a rețelelor
    - Rețelele ar trebui monitorizate continuu pentru detecția componentelor hardware și firmware noi sau neautorizate. Modificările detectate ar trebui să declanșeze actualizări automate ale inventarului activelor.
- Stabilirea unui proces de răspuns
    - Ar trebui să existe un proces definit pentru revizuirea și abordarea periodică a componentelor neautorizate:
        - Pentru hardware neautorizat, consultați ID.AM-01.3;
        - Pentru firmware neautorizat, consultați ID.AM-02.4.
- Includerea considerentelor specifice OT
    - Metodele de detecție în mediile OT ar trebui să ia în considerare siguranța, disponibilitatea și constrângerile specifice vânzătorului atunci când identifică componente neautorizate.

ID.AM-02

Inventarele software-ului, serviciilor și sistemelor gestionate de organizație sunt menținute.

ID.AM-02.1

Un inventar al software-ului, serviciilor digitale și sistemelor de gestiune a activității utilizate în cadrul organizației trebuie documentat, revizuit și actualizat pe măsură ce apar modificări.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura identificarea, urmărirea și actualizarea periodică a tuturor programelor software, serviciilor digitale și sistemelor de gestiune a activității utilizate în cadrul organizației. Se concentrează pe părțile funcționale și intangibile ale mediului tehnologic, precum aplicațiile, platformele și serviciile cloud, care funcționează pe infrastructura de bază sau interacționează cu aceasta. Menținerea actualizată a acestui inventar susține continuitatea operațională, consolidează securitatea și contribuie la îndeplinirea cerințelor de conformitate.

Este strâns legat de ID.AM-01.1, care acoperă infrastructura fizică și virtuală (precum servere, dispozitive de rețea și medii cloud) care susține aceste sisteme.

Împreună, ambele Controale oferă o imagine completă a peisajului tehnologic al organizației, de la infrastructura fundamentală până la aplicațiile și serviciile care aduc valoare pentru activitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea software-ului și a serviciilor
    - Inventarul ar trebui să includă toate aplicațiile, serviciile cloud, interfețele de programare a aplicațiilor (API) și sistemele de gestiune a activității (de exemplu, planificarea resurselor organizației - ERP, managementul relațiilor cu clienții - CRM, platforme de resurse umane).
- Înregistrarea informațiilor cheie
    - Fiecare intrare ar trebui să includă versiunea, proprietarul, scopul, tipul de licență și mediul de punere în funcțiune.
- Utilizarea automatizării acolo unde este posibil
    - Pentru detecția și actualizarea cu precizie a software-ului și serviciilor, ar trebui utilizate instrumente de detecție automată.
- Menținerea unui SBOM
    - Ar trebui menținut un SBOM pentru software-ul critic sau dezvoltat intern, pentru urmărirea componentelor și dependențelor.

- Menținerea inventarului actualizat
    - Inventarul ar trebui revizuit și actualizat periodic, în special după instalări, actualizări sau eliminări.
- Alinierea cu inventarul infrastructurii (ID.AM-01.1)
    - Înregistrările software ar trebui să fie corelate cu infrastructura pe care rulează pentru a oferi o imagine completă a mediului tehnologic.

ID.AM-02.2

Inventarul care reflectă software-ul, serviciile și sistemele utilizate în organizație trebuie să reflecte modificările din contextul organizațional și să includă toate informațiile necesare pentru o răspundere efectivă.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că inventarele de software, servicii și sisteme sunt menținute actualizate și complete, permițând trasabilitatea, o proprietate responsabilă și alinierea la modificările din contextul operațional și de risc al organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Includerea detaliilor cheie ale inventarului
    - Inventarele ar trebui să cuprindă atribute relevante precum titlul software-ului, editorul, data inițială de instalare sau de utilizare, scopul pentru activitate, versiunea, metoda de punere în funcțiune și data scoaterii din uz. Localizatorii uniformi de resurse (URL) sau sursele din magazinele de aplicații ar trebui incluse acolo unde este cazul.
- Sprijinirea răspunderii
    - Înregistrările inventarului ar trebui să permită trasabilitatea măsurilor și a deciziilor, asigurând identificarea persoanelor responsabile și tragerea acestora la răspundere pentru utilizarea și managementul software-ului și serviciilor.
- Reflectarea modificărilor organizaționale
    - Inventarele ar trebui actualizate pentru a reflecta modificările, precum noi puneri în funcțiune, actualizări sau eliminări, inclusiv cele care afectează sistemele OT și componentele software integrate.

ID.AM-02.3

Persoanele fizice responsabile și răspunzătoare de gestionarea platformelor software și a aplicațiilor din cadrul organizației trebuie identificate în mod formal.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura gestionarea corespunzătoare a platformelor și aplicațiilor software, prin identificarea clară a persoanelor responsabile de operațiunile zilnice și a celor răspunzătoare de supravegherea generală și de rezultate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea clară a rolurilor
    - Persoanele fizice responsabile de gestionarea software-ului ar trebui desemnate în mod formal. Acestea sunt persoanele care efectuează lucrările, iau decizii tehnice și îndeplinesc sarcini operaționale (de exemplu, dezvoltatori, administratori de sistem, personal de testare).
- Atribuirea răspunderii
    - Ar trebui atribuită în mod formal o funcție separată pentru supravegherea și aprobarea finalizării cu succes a sarcinilor legate de software. Aceasta ar putea include manageri de proiect, proprietari de produse sau conducători de echipe.
- Aplicarea principiului în toate mediile
    - Aceste roluri ar trebui definite atât pentru mediile IT, cât și pentru cele OT, asigurându-se că software-ul utilizat în sistemele industriale este, de asemenea, gestionat în mod corespunzător.

ID.AM-02.4

Atunci când este detectat software neautorizat, acesta trebuie pus în carantină pentru eventuala gestionare a excepțiilor, eliminare sau înlocuire, iar inventarul trebuie actualizat în consecință.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a minimiza riscurile de securitate, operaționale și de conformitate, asigurând că software-ul neautorizat este identificat prompt, gestionat în mod corespunzător și reflectat în inventarul de software al organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea software-ului neautorizat
    - Software-ul instalat sau utilizat fără licență, aprobare sau excepții documentate corespunzătoare ar trebui clasificat ca neautorizat.
- Înțelegerea riscurilor
    - Software-ul neautorizat poate introduce:
        - Vulnerabilități de securitate (de exemplu, malware sau backdoor-uri).
        - Riscuri legate de protecția datelor (de exemplu, prelucrarea neautorizată a datelor).
        - Ineficiențe operaționale (de exemplu, probleme de compatibilitate).
        - Pierderea controlului asupra utilizării și actualizării software-ului.
- Stabilirea procedurilor de răspuns
    - Software-ul neautorizat ar trebui pus în carantină pentru eventuala gestionare a excepțiilor, eliminat sau înlocuit. Inventarul software-ului ar trebui actualizat în consecință.
- Sprijin prin management centralizat
    - Ar trebui să existe un proces centralizat de management al software-ului pentru supravegherea selecției vânzătorilor vânzătorilor, software-ului vechi și controalelor de securitate.
- Utilizarea SBOM-urilor acolo unde este cazul
    - SBOM-urile ar trebui utilizate pentru urmărirea componentelor, bibliotecilor și modulelor, sprijinind conformitatea licențelor și managementul vulnerabilităților, în special în sistemele OT și integrate.

ID.AM-02.5

Trebuie identificate mecanisme pentru detecția prezenței software-ului neautorizat în mediul TIC/OT al organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura existența unor mecanisme pentru detecția software-ului neautorizat în mediile TIC și OT, permițând astfel un răspuns prompt și menținerea unui inventar software precis.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Automatizarea acolo unde este fezabil
    - Mecanismele de detecție ar trebui automatizate acolo unde este sigur și adecvat din punct de vedere tehnic, în special în medii complexe sau cu risc ridicat.
- Monitorizarea tuturor platformelor
    - Toate platformele, inclusiv sistemele fizice, mașinile virtuale (VM), containerele și sistemele OT integrate, ar trebui monitorizate continuu pentru detecția software-ului nou sau neautorizat. Modificările detectate ar trebui să declanșeze actualizări automate ale inventarului de software.
- Stabilirea unui proces de revizuire
    - Ar trebui instituit un proces pentru investigarea și abordarea periodică a software-ului neautorizat. Atunci când se detectează software neautorizat, ar trebui aplicat ID.AM-02.4.
- Adaptarea detecției la mediile OT
    - În mediile OT, mecanismele de detecție ar trebui adaptate pentru evitarea întreruperii operaționale. Pentru asigurarea siguranței și disponibilității sistemului, ar trebui considerată monitorizarea pasivă, instrumentele aprobate de vânzători și scanările programate.

ID.AM-03

Menținerea reprezentărilor comunicațiilor de rețea autorizate ale organizației și ale fluxurilor de date de rețea interne și externe.

ID.AM-03.2

Comunicarea în rețea și fluxurile de date interne ale organizației trebuie identificate, documentate, autorizate și actualizate atunci când apar modificări.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că comunicațiile interne de rețea și fluxurile de date sunt înțelese în mod clar, documentate corespunzător și actualizate, pentru a sprijini operațiuni securizate și luarea de decizii informate în mediile TIC și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Stabilirea unor valori de referință pentru rețea
    - Fluxurile de comunicații și date prin infrastructura cu fir, wireless și bazată pe cloud (de exemplu, infrastructură ca serviciu - IaaS) ar trebui identificate, documentate și autorizate. Actualizările ar trebui efectuate atunci când apar modificări.
- Documentarea detaliilor tehnice
    - Porturile de rețea, protocoalele și serviciile așteptate, utilizate între sistemele autorizate, ar trebui înregistrate pentru facilitarea monitorizării și depanării.
- Integrarea cu managementul configurației
    - Procesele de management al configurației ar trebui să sprijine menținerea și validarea documentației privind fluxul de rețea.
- Asigurarea unei documentații reziliente
    - Documentația privind fluxul de rețea ar trebui stocată în mod securizat și nu numai pe rețeaua pe care o descrie. Ar trebui menținută o copie offline protejată (de exemplu, unitate externă criptată sau copie tipărită) pentru asigurarea disponibilității în cazul întreruperilor sau incidentelor.

ID.AM-03.3

Comunicarea în rețea și fluxurile de date externe ale organizației trebuie identificate, documentate, autorizate și actualizate atunci când apar modificări.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că comunicațiile externe de rețea sunt înțelese în mod clar, controlate și monitorizate, pentru reducerea riscului de acces neautorizat, scurgeri de date sau întreruperea serviciilor în mediile TIC și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea și documentarea fluxurilor externe
    - Comunicarea și fluxurile de date între organizație și părțile externe ar trebui identificate, documentate și autorizate. Aceste înregistrări ar trebui actualizate atunci când apar modificări.
- Punerea în aplicare a controalelor de acces
    - Conexiunile de rețea ar trebui restricționate la interfețele autorizate în mod explicit, pentru reducerea suprafeței de atac și prevenirea transferurilor neautorizate de date.
- Intensificarea monitorizării atunci când este necesar
    - Monitorizarea ar trebui intensificată ca răspuns la nivelurile ridicate de risc. Aceasta ar putea include alerte în timp real, jurnalizare intensificată sau audituri mai frecvente ale activității rețelei externe.
- Prevenirea scurgerilor de informații
    - Riscul de scurgere de date prin emisii electromagnetice sau atacuri de tip side-channel ar trebui evaluat. După caz, ar trebui aplicate măsuri de atenuare, pentru securitatea emisiilor electromagnetice (EMSEC) sau TEMPEST, în special pentru sistemele care gestionează informații sensibile sau clasificate.

Cele două Controale - ID.AM-03.3 și ID.AM-04.2 - sunt strâns corelate, dar se concentrează pe domenii diferite ale fluxului de informații și ale activității rețelei. Controlul ID.AM-03.3 acoperă interacțiunile la nivel de rețea cu entități externe, inclusiv:

- Traficul de internet (de exemplu, accesul web de ieșire, interogări ale sistemului de nume de domenii - DNS, traficul de e-mail).

- Conexiunile de rețea virtuală privată (VPN), accesul la distanță și comunicațiile prin servicii cloud.
- Orice comunicare care traversează perimetrul organizațional, indiferent dacă implică un sistem extern specific.

ID.AM-04

Inventarele serviciilor furnizate de furnizori sunt menținute.

ID.AM-04.1

Organizațiile trebuie să păstreze o listă clară și actualizată a tuturor serviciilor externe pe care le utilizează, inclusiv modul în care acestea se conectează la sistemele lor. Aceste servicii trebuie revizuite și aprobate înainte de utilizare, iar lista trebuie actualizată ori de câte ori apar modificări.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate serviciile externe utilizate de organizație sunt identificate în mod clar, revizuite și actualizate, pentru reducerea riscului de acces neautorizat, dependențe față de părți terțe care nu sunt gestionate sau întreruperea serviciilor în mediile TIC și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Menținerea unui inventar al serviciilor externe
    - Toate serviciile externe pe care se bazează organizația ar trebui identificate și documentate. Aceasta include serviciile utilizate atât în mediile IT, cât și în cele OT. Inventarul ar trebui actualizat ori de câte ori sunt adăugate, modificate sau eliminate servicii.
- Descrierea și identificarea conexiunilor serviciilor
    - Modul în care fiecare serviciu extern se conectează la sistemele interne ar trebui descris și înregistrat în mod clar. Aceasta include instrumente de acces la distanță, platforme de control de supraveghere și achiziție de date (SCADA) bazate pe cloud și sisteme OT gestionate de vânzători.
- Revizuirea și aprobarea serviciilor înainte de utilizare
    - Serviciile externe ar trebui revizuite și aprobate înainte de a fi utilizate. Acest proces ar trebui să verifice dacă serviciul respectă cerințele interne de securitate, de conformitate și operaționale.
- Categorizarea și clasificarea serviciilor
    - Serviciile externe ar trebui categorizate în funcție de tip (de exemplu, IaaS, software ca serviciu - SaaS, API) și clasificate în funcție de criticitatea lor și de sensibilitatea datelor. Aceasta facilitează prioritizarea eforturilor de supraveghere și management al riscului.

- Integrarea cu managementul riscului și al modificărilor
    - Inventarul ar trebui integrat în procesele mai ample de management al riscului și al modificărilor. Orice modificare a serviciilor externe ar trebui să declanşeze o revizuire a riscurilor asociate și a controalelor necesare.

ID.AM-04.2

Organizația trebuie să identifice, să documenteze și să autorizeze fluxul de informații către/dinspre sistemele externe și să actualizeze fluxul atunci când apar modificări.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că fluxul de informații către și dinspre sistemele externe este înțeles în mod clar, gestionat în mod securizat și actualizat, pentru reducerea riscului scurgerii de date, al accesului neautorizat sau al întreruperilor în mediile TIC și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea și cartografierea căilor de acces la date
    - Toate căile prin care datele intră sau ies din sistemele organizației ar trebui identificate și documentate. Aceasta include funcțiile, porturile, protocoalele și serviciile utilizate atât în mediile IT, cât și în cele OT.
- Documentarea în detaliu a fluxurilor de date
    - Înregistrările ar trebui să descrie tipurile de date transferate, sistemele implicate și măsurile de securitate aplicate (de exemplu, criptare, autentificare, controale de acces). Aceasta contribuie la transparență și gestionarea securizată a datelor.
- Autorizarea și controlul accesului
    - Numai personalul desemnat și autorizat ar trebui să aibă dreptul de a aproba și gestiona transferurile de date. Aceasta contribuie la prevenirea accesului neautorizat și asigură răspunderea.
- Revizuirea și actualizarea periodică
    - Documentația privind fluxul de informații ar trebui revizuită și actualizată ori de câte ori se modifică sistemele, procesele sau conexiunile externe. Aceasta asigură menținerea eficacității controalelor și alinierea acestora la mediul actual.

Cele două Controale - ID.AM-03.3 și ID.AM-04.2 - sunt strâns legate, dar se concentrează pe domenii diferite ale fluxului de informații și activității rețelei. Acest Control se concentrează pe fluxurile de date granulare, specifice conținutului, între organizație și anumite sisteme externe. Acesta include:

- Transferuri de date către/de la platforme terțe, precum sisteme CRM, furnizori de servicii de stocare în cloud și API-uri externe.
- Transferuri de fișiere, apeluri API și sincronizarea bazelor de date cu sisteme externe.

ID.AM-05

Activele sunt prioritizate pe baza clasificării, criticității, resurselor și impactului asupra misiunii.

ID.AM-05.1

Activele organizației trebuie prioritizate în funcție de clasificare, criticitate și valoare pentru activitate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate activele organizației, precum dispozitivele, sistemele, serviciile, datele și procesele organizației, sunt prioritizate în funcție de clasificarea, criticitatea și valoarea pentru activitate.

Această prioritizare contribuie la direcționarea eforturilor de protecție către cele mai importante active, sprijinind continuitatea operațională, securitatea și conformitatea.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea activelor
    - Toate activele relevante, inclusiv dispozitivele, sistemele, software-ul, serviciile cloud, datele, angajații și procesele organizației, ar trebui identificate și înregistrate într-un inventar centralizat.
- Clasificarea activelor
    - Fiecare activ ar trebui clasificat în funcție de rolul său:
        - Activele primare ar trebui definite ca fiind cele care susțin în mod direct funcțiile de bază ale organizației.
        - Activele secundare ar trebui definite ca fiind cele care susțin, protejează sau permit funcționarea activelor primare.
- Evaluarea criticității
    - Organizația ar trebui să evalueze cât de critic este fiecare activ pentru continuitatea activității.
    - Evaluarea ar trebui să considere impactul potențial, precum întreruperea operațională, pierderile financiare, consecințele legale sau de reglementare, riscurile de siguranță și prejudiciile aduse reputației.
- Metoda de prioritizare
    - Ar trebui utilizată o metodă consecventă de notare sau ierarhizare pentru prioritizarea activelor în funcție de clasificare, criticitate și valoare pentru activitate.

- Atribuirea proprietății
  - Fiecare activ ar trebui să aibă un proprietar desemnat, responsabil cu menținerea informațiilor exacte și actualizate.
- Revizuirea periodică
  - Clasificările și prioritățile activelor ar trebui revizuite cel puțin anual sau atunci când apar modificări semnificative (de exemplu, sisteme noi, restructurarea organizației).
- Documentație și dovezi
  - Registrul activelor ar trebui să includă clasificarea, criteriile de prioritizare, proprietarii desemnați și dovezi ale revizuirilor periodice.
  - Definițiile activelor primare și secundare ar trebui documentate în mod clar.

ID.AM-07

Inventarele datelor și metadatelor corespunzătoare pentru tipurile de date desemnate sunt menținute.

ID.AM-07.1

Datele pe care organizația le stochează și le utilizează trebuie identificate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate datele stocate și utilizate de organizație sunt identificate în mod clar. Aceasta sprijină managementul și protecția corespunzătoare a datelor, precum și alinierea la cerințele organizaționale și de reglementare.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea datelor
    - Toate tipurile de date, indiferent de format, locație sau sistem, ar trebui identificate și înregistrate.
- Clasificarea datelor
    - Datele identificate ar trebui clasificate utilizând categorii standard, precum:
        - Publice.
        - Interne.
        - Confidențiale.
        - Restricționate.
- Corelarea datelor cu activele
    - Datele ar trebui să fie corelate cu activele care le stochează sau le prelucrează, inclusiv dispozitivele fizice, sistemele, software-ul și aplicațiile enumerate în inventarele din ID.AM-01 și ID.AM-02.
- Documentarea și menținerea
    - Tipurile de date, clasificările și activele asociate ar trebui documentate și actualizate periodic pentru reflectarea modificărilor din mediu.

ID.AM-07.2

Inventarele de date și metadatele asociate trebuie menținute pentru tipurile de date desemnate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura menținerea inventarelor de date și a metadatelor asociate pentru toate tipurile de date selectate sau desemnate în mod explicit prin politici sau orientări (de exemplu, datele clienților, informațiile financiare sau datele de producție), în vederea susținerii managementului securizat al datelor, conformității cu reglementările și integrității operaționale în mediile TIC și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea unei scheme de clasificare a datelor
    - Ar trebui stabilită o schemă de clasificare pentru categorizarea tipurilor de date în funcție de sensibilitate și de modul de utilizare. Această schemă ar trebui să ghideze modul în care datele sunt gestionate, protejate și păstrate.
- Aplicarea măsurilor de securitate în funcție de nivelul de clasificare
    - Pentru fiecare nivel de clasificare ar trebui implementate controale de securitate adecvate. Acestea ar putea include criptarea, control al accesului bazat pe roluri (RBAC) și politici personalizate de păstrare a datelor.
- Identificarea și protejarea tipurilor de date sensibile
    - Inventarele ar trebui să includă date sensibile, precum:
        - Informații de identificare a persoanei (PII).
        - Informații financiare și medicale.
        - Date confidențiale ale organizației.
        - Proprietate intelectuală.
        - Înregistrări guvernamentale și de personal.
    - Mediile OT ar trebui să includă și date operaționale critice pentru siguranță și fiabilitate.
- Urmărirea metadatelor pentru fiecare instanță de date
    - Metadatele ar trebui menținute pentru sprijinirea guvernanței datelor. Acestea includ:
        - Metadate descriptive (de exemplu, titlu, autor, cuvinte cheie).
        - Metadate structurale (de exemplu, format, schemă).

    - Metadate administrative (de exemplu, drepturi de acces, politică de păstrare).
    - Metadate tehnice (de exemplu, codificare, sumă de control).

- Monitorizarea provenienței și localizării datelor
    - Originea, proprietatea și localizarea geografică a fiecărei instanțe de date ar trebui documentate. Aceasta contribuie la înțelegerea locului și modului în care datele sunt stocate și prelucrate, în special în sistemele distribuite sau OT.
- Identificarea și analiza continuă a datelor ad-hoc
    - Ar trebui să existe procese pentru identificarea noilor instanțe de date sensibile care nu sunt capturate de inventarele inițiale. Aceasta contribuie la remedierea lacunelor în identificarea fluxului de date și sprijină protecția continuă a datelor.
- Considerarea utilizării Traffic Light Protocol (TLP)
    - TLP ar trebui luat în considerare ca metodă de clasificare și partajare a datelor legate de securitatea cibernetică, în special în contextul răspunsului la incidente și al informațiilor privind amenințările.

ID.AM-08

Sistemele, hardware-ul, software-ul, serviciile și datele sunt gestionate pe tot parcursul ciclului lor de viață.

ID.AM-08.2

Patch-urile și actualizările de securitate pentru sistemele de operare și componentele critice ale sistemului trebuie instalate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că sistemele de operare și componentele critice ale sistemelor sunt păstrate în mod securizat și actualizate prin instalarea de patch-uri și actualizări de securitate în timp util și în mod controlat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Actualizarea în timp util
    - Patch-urile și actualizările de securitate ar trebui instalate cât mai curând posibil, în special pentru sistemele critice.
- Sisteme industriale
    - Actualizările firmware pentru activele industriale (de exemplu, controler logic programabil - PLC, interfață om-mașină - HMI) ar trebui incluse în procesul de aplicare a patch-urilor.
- Management centralizat
    - Ar trebui utilizat un sistem centralizat de management al patch-urilor pentru automatizarea și eficientizarea punerii în funcțiune a acestora.
- Testare înainte de punerea în funcțiune
    - Patch-urile ar trebui testate într-un mediu controlat pentru evitarea întreruperilor.
    - Un mediu de testare ar trebui să reflecte cât mai fidel configurația de producție.
- Implementări etapizate
    - Acolo unde este cazul, ar trebui utilizate grupuri de testare, utilizatori pilot și implementări etapizate.
    - Ar trebui să existe o procedură de revenire la starea anterioară, în cazul în care apar probleme.
- Numai surse de încredere
    - Patch-urile ar trebui descărcate numai din surse verificate și de încredere.
    - Link-urile din e-mail-uri sau reclame ar trebui evitate.

- Amprentă software minimă
  - Ar trebui instalate numai aplicațiile esențiale. Acestora ar trebui să le fie aplicate patch-uri și să fie actualizate periodic.
- Practici sigure de actualizare
  - Actualizările automate ar trebui activate atunci când dispozitivul este conectat la rețele de încredere.
  - Actualizările nu ar trebui efectuate prin rețele nesigure (de exemplu, Wi-Fi public).
- Numai software susținut de furnizor
  - Ar trebui utilizate numai versiuni de software susținute de vânzători și actualizate.
  - Software-ul aflat la EOL ar trebui scos din uz cât mai curând posibil.
- Verificarea periodică
  - Dacă nu sunt posibile actualizările automate, ar trebui stabilit un program periodic (de exemplu, lunar) pentru verificarea manuală și instalarea actualizărilor.
- Instrumente de monitorizare a actualizărilor
  - Instrumentele care notifică actualizările disponibile ar trebui configurate pentru a monitoriza toate aplicațiile instalate.

ID.AM-08.3

Organizația trebuie să asigure răspunderea pentru toate activele sale critice pentru activitate pe parcursul ciclului de viață al sistemului, inclusiv eliminarea, transferurile și casarea.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura răspunderea pentru toate activele critice pentru activitate pe parcursul întregului lor ciclu de viață, inclusiv punerea în funcțiune, mutarea și casarea, pentru a reduce riscul de acces neautorizat, scurgere de date sau perturbare operațională în mediile TIC și OT. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Securizarea activelor înainte de punerea în funcțiune
    - Sistemele, hardware-ul, software-ul și serviciile ar trebui configurate și securizate corespunzător înainte de introducerea în mediile de producție.
- Identificarea și eliminarea activelor redundante
    - Sistemele, software-ul și serviciile redundante sau neutilizate care sporesc suprafața de atac ar trebui identificate și eliminate periodic.
- Monitorizarea și documentarea dinamicii activelor
    - Dinamica activelor critice pentru activitate ar trebui urmărite, iar documentația ar trebui menținută pentru asigurarea trasabilității și răspunderii.
- Autorizarea transferurilor de active
    - Activele critice pentru activitate ar trebui să poată intra sau ieși din incinte numai cu autorizația corespunzătoare, în special în mediile OT, unde controlul fizic al activelor este critic.
- Casarea activelor în mod securizat
    - Casarea activelor critice pentru activitate ar trebui efectuată în mod securizat, responsabil și auditabil, pentru a preveni scurgerea de date sau reutilizarea neautorizată.
- Actualizarea promptă a inventarelor
    - Inventarele activelor ar trebui actualizate ori de câte ori sistemele, hardware-ul, software-ul sau serviciile sunt mutate, transferate, eliminate, scoase din uz sau dezafectate.

ID.AM-08.4

Organizația trebuie să asigure luarea măsurilor necesare pentru a gestiona pierderea, utilizarea necorespunzătoare, deteriorarea sau furtul activelor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura luarea măsurilor adecvate pentru prevenirea și răspunsul la pierderea, utilizarea necorespunzătoare, deteriorarea sau furtul de active, în vederea protejării operațiunilor organizației și reducerii riscurilor de securitate în mediile TIC și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aplicarea măsurilor de securitate fizică
    - Pentru securizarea incintelor și a activelor critice, inclusiv a celor din mediile OT, ar trebui utilizate măsuri de protecție fizică, precum încuietori, camere de supraveghere și alarme.
- Implementarea măsurilor tehnice de protecție
    - Pentru protejarea datelor și sistemelor împotriva accesului neautorizat sau pierderii, ar trebui aplicate controale tehnice, precum criptarea, ștergerea securizată a datelor și efectuarea periodică a backup-urilor.
- Stabilirea controalelor organizaționale
    - Ar trebui să existe politici, proceduri și acorduri cu utilizatorii pentru definirea responsabilităților și așteptărilor. Pentru gestionarea utilizării activelor ar trebui utilizate instrumente de management al dispozitivelor mobile (MDM) și alte instrumente administrative.
- Efectuarea de audituri periodice și verificări ale inventarului
    - Ar trebui efectuate audituri periodice și inventarieri ale activelor pentru a verifica dacă toate activele sunt evidențiate și gestionate în mod corespunzător.
- Restricționarea accesului la activele sensibile
    - Accesul la sisteme, date și zone fizice critice ar trebui limitat doar la personalul autorizat, în special în medii în care continuitatea operațională este esențială.

- Furnizarea de conştientizare şi instruire angajaților
    - Personalul ar trebui instruit cu privire la practicile de protecție a activelor și încurajat să raporteze activități suspecte sau incidente care implică utilizarea necorespunzătoare sau pierderea activelor.
- Menținerea unei acoperiri adecvate de asigurare
    - Ar trebui să existe polițe de asigurare pentru a contribui la atenuarea pierderilor financiare rezultate din furtul, deteriorarea sau alte incidente care afectează activele.

ID.AM-08.5

Organizația trebuie să se asigure că acțiunile de casare sunt aprobate, urmărite, documentate și verificate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate acțiunile de casare care implică sisteme informatice, date sau active fizice sunt autorizate corespunzător, trasabile și verificabile, pentru a reduce riscurile, a menține conformitatea și a proteja informațiile sensibile, în special în mediile OT. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aprobarea
    - Acțiunile de casare ar trebui revizuite și aprobate de personalul autorizat înainte de execuție. Aceasta asigură alinierea cu politicile interne și cu reglementările externe.
- Urmărirea
    - Fiecare acțiune de casare ar trebui jurnalizată cu detalii cheie, inclusiv tipul activului sau mediului, metoda de casare, data și persoanele implicate.
- Documentarea
    - Toate etapele, de la aprobare până la verificare, ar trebui documentate în mod clar. Aceasta include înregistrările de aprobare, jurnalele de urmărire și orice dovezi justificative.
- Verificarea
    - Casarea ar trebui verificată pentru a confirma efectuarea corectă. Aceasta poate implica verificarea faptului că datele au fost șterse în mod securizat sau că distrugerea fizică a fost efectivă.

Această abordare structurată contribuie la menținerea răspunderii și a securității, în special în mediile OT, unde casarea necorespunzătoare poate duce la perturbări operaționale sau la riscuri de siguranță.

ID.AM-08.6

Organizația trebuie să planifice, să efectueze și să documenteze mentenanța preventivă și reparațiile componentelor critice ale sistemului său, în conformitate cu procesele și instrumentele aprobate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că mentenanța preventivă și reparațiile componentelor critice ale sistemului sunt planificate, efectuate și documentate într-un mod sigur și consecvent, pentru menținerea fiabilității sistemului și reducerea riscurilor operaționale în mediile TIC și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Documentarea procedurilor de mentenanță
    - Politicile și procedurile de mentenanță ar trebui să fie clar definite și incluse în planurile de securitate cibernetică și operaționale ale organizației. Supravegherea acestor proceduri ar trebui să facă parte din responsabilitățile conducerii.
- Autorizarea personalului de mentenanță
    - Ar trebui stabilit un proces de autorizare a persoanelor fizice sau a furnizorilor externi care efectuează operațiuni de mentenanță. Ar trebui menținută și revizuită periodic o listă a personalului sau a organizațiilor aprobate.
- Programarea și înregistrarea activităților de mentenanță
    - Mentenanța preventivă și reparațiile ar trebui programate, efectuate și documentate în conformitate cu cerințele organizaționale și specificațiile vânzătorului. Înregistrările ar trebui revizuite pentru a asigura completitudinea și acuratețea acestora.
- Monitorizarea tuturor activităților de mentenanță
    - Toate lucrările de mentenanță, indiferent dacă sunt efectuate la fața locului sau la distanță, ar trebui aprobate în prealabil și monitorizate în timpul executării. Aceasta include întreținerea componentelor scoase din incintă.
- Asigurarea unei mentenanțe sigure și fiabile a echipamentelor OT
    - Mentenanța sistemelor OT ar trebui planificată și efectuată într-un mod care să asigure siguranța operațiunilor, să evite perioadele de nefuncționare inutile și să respecte instrucțiunile sau cerințele specifice ale vânzătorilor de echipamente.

ID.AM-08.7

Organizația trebuie să împiedice îndepărtarea neautorizată a echipamentelor de mentenanță care conțin informații critice despre sistemul organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a preveni îndepărtarea neautorizată a echipamentelor de mentenanță care pot conține informații critice despre sistem, reducând riscul de scurgere sau furt de date, în special în mediile OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Verificarea
    - Echipamentele de mentenanță ar trebui verificate pentru a confirma că nu conțin informații ale organizației înainte de a fi îndepărtate.
- Sanitizarea sau distrugerea
    - Dacă sunt prezente date sensibile, echipamentul ar trebui sanitizat sau distrus în mod securizat, conform procedurilor aprobate.
- Păstrarea în incintă
    - Echipamentul ar trebui să rămână în incintă, cu excepția cazului în care îndepărtarea acestuia este strict necesară.
- Obținerea unei derogări
    - Dacă este necesară îndepărtarea, ar trebui obținută autorizarea explicită din partea personalului sau a persoanelor desemnate.

În acest context, echipamentele de mentenanță se referă la hardware-ul utilizat temporar pentru service sau diagnosticare, precum unități externe, servere temporare sau instrumente OT/ICS specializate și nu la instrumentele de mentenanță obișnuite acoperite de Controlul ID.AM-08.9.

ID.AM-08.8

Organizația trebuie să aprobe în prealabil, să monitorizeze și să pună în aplicare utilizarea instrumentelor de mentenanță pentru sistemele sale critice.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că instrumentele de mentenanță utilizate pe sistemele critice sunt aprobate în prealabil, monitorizate și puse în aplicare pentru protejarea integrității, siguranței și continuității operaționale a sistemului. În mediile OT, utilizarea necorespunzătoare a instrumentelor poate interfera cu procesele fizice, ceea ce face ca controlul asupra aprobării și utilizării instrumentelor să fie esențial pentru siguranța și fiabilitatea operațională.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea sistemelor critice
    - Sistemele care au impact asupra siguranței, calității, conformității cu reglementările sau randamentului operațional ar trebui clasificate ca fiind critice. Indicatori precum timpul mediu de reparare (MTTR) și timpul mediu între defecțiuni (MTBF) ar trebui să sprijine această clasificare.
- Instrumente aprobate în prealabil
    - Numai instrumentele de mentenanță care au fost revizuite și aprobate ar trebui să fie permise pentru utilizare pe sisteme critice. Aceasta include atât instrumente hardware, cât și software, precum dispozitive de diagnosticare, sniffere de pachete și laptopuri.
- Monitorizarea utilizării
    - Utilizarea instrumentelor de mentenanță pe sistemele critice ar trebui monitorizată activ pentru detecția activităților neautorizate sau nesigure.
- Punerea în aplicare a controalelor
    - Ar trebui să existe politici și controale tehnice pentru prevenirea utilizării instrumentelor neaprobate și pentru asigurarea conformității cu procedurile interne și respectarea legilor și reglementărilor aplicabile.

ID.AM-08.9

Instrumentele de mentenanță și dispozitivele de stocare portabile trebuie inspectate la intrarea în incintă și protejate cu soluții antimalware care le scanează în căutarea codurilor cu scop nelegitim înainte de a fi utilizate în sistemele organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a preveni introducerea de cod cu scop nelegitim în sistemele organizației, prin asigurarea faptului că toate instrumentele de mentenanță și dispozitivele de stocare portabile sunt inspectate și scanate înainte de utilizare. În mediile OT, introducerea de instrumente sau dispozitive de stocare neverificate poate compromite integritatea sistemului și perturba operațiunile fizice critice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Inspectarea la intrare
    - Instrumentele de mentenanță și dispozitivele de stocare portabile ar trebui inspectate la intrarea în incintă, pentru detecția elementelor neautorizate sau suspecte.
- Scanarea malware
    - Toate dispozitivele ar trebui scanate folosind soluții antimalware actualizate înainte de a fi conectate la sistemele organizației.
- Aplicarea asupra tuturor tipurilor de instrumente
    - Aceasta include instrumente software (de exemplu, software de diagnosticare, actualizări de firmware, instrumente de configurare, instrumente de acces la distanță), dispozitive de stocare portabile (de exemplu, dispozitive USB, hard disk-uri externe, carduri SD) și instrumente hardware (de exemplu, laptopuri, tablete, dispozitive portabile de diagnosticare).
- Utilizarea tehnicilor de sanitizare nedistructive
    - Atunci când dispozitivele sunt nou achiziționate sau nu au un lanț de custodie de încredere, înainte de prima utilizare ar trebui aplicate tehnici de sanitizare nedistructive.
- Asigurarea conformității și respectării normelor
    - Toate acțiunile ar trebui să fie conforme cu procedurile interne și să respecte reglementările aplicabile în materie de securitate cibernetică și standardele din domeniu.

ID.AM-08.10

Organizația trebuie să verifice controalele de securitate după mentenanță sau reparații/aplicare de patch-uri și să ia măsuri corespunzătoare.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că controalele de securitate rămân eficace după activitățile de mentenanță, reparații sau aplicare de patch-uri. În mediile OT, chiar și modificările minore de configurare pot avea consecințe semnificative asupra siguranței sau a operațiunilor, ceea ce face ca verificarea după mentenanță să fie critică.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Verificarea controalelor de securitate
    - După mentenanță, sistemele ar trebui evaluate pentru a confirma că nicio modificare nu a slăbit securitatea. Aceasta include verificarea configurațiilor, a permisiunilor de acces și a altor setări relevante pentru securitate.
- Actualizarea înregistrărilor
    - Orice modificări efectuate în timpul mentenanței ar trebui documentate, inclusiv actualizările controalelor de securitate sau implementarea de noi măsuri.
- Raportarea problemelor
    - Dacă în timpul verificării sunt identificate probleme de securitate, constatările ar trebui comunicate părților interesate relevante, pentru asigurarea conștientizării și coordonării răspunsului.
- Luarea măsurilor corective
    - Dacă se constată că măsurile de control sunt inadecvate sau compromise, ar trebui luate măsuri corective. Acestea ar putea include reconfigurarea setărilor, aplicarea de patch-uri suplimentare sau consolidarea controalelor existente.
- Asigurarea conformității și respectării normelor
    - Toate acțiunile de verificare și măsurile corective ar trebui să fie conforme cu procedurile interne și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.AM-08.11

Activitățile de mentenanță și diagnosticare la distanță ale activelor organizației trebuie să fie aprobate în prealabil, iar realizarea acestora trebuie jurnalizată.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că activitățile de mentenanță și diagnosticare la distanță sunt autorizate, trasabile și sigure. În mediile OT, mentenanța la distanță trebuie să fie strict controlată, deoarece modificările neautorizate pot afecta în mod direct siguranța și stabilitatea sistemelor fizice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aprobarea prealabilă a activităților
    - Toate activitățile de mentenanță și diagnosticare la distanță ar trebui revizuite și aprobate înainte de executare.
- Jurnalizarea performanței
    - Fiecare sesiune la distanță ar trebui jurnalizată în detaliu, inclusiv ora, durata, personalul implicat și acțiunile întreprinse.
- Stabilirea procedurilor de jurnalizare
    - Procedurile de jurnalizare și monitorizare ar trebui documentate, aprobate, comunicate, aplicate și revizuite periodic, ideal ar fi anual.
- Prevenirea modificărilor neautorizate
    - Ar trebui implementate măsuri tehnice și procedurale pentru detecția sau prevenirea modificărilor neautorizate ale sistemelor, configurațiilor, aplicațiilor sau infrastructurii în timpul accesului la distanță.
- Asigurarea conformității și respectării normelor
    - Toate activitățile ar trebui să fie conforme cu politicile interne și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.AM-08.12

Configurarea sesiunilor de mentenanță și diagnosticare non-locale prin conexiuni de rețea la distanță trebuie să necesite autentificatori puternici, iar aceste conexiuni trebuie întrerupte la finalizarea mentenanței non-locale.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că sesiunile de mentenanță și diagnosticare non-locale sunt stabilite în mod securizat și terminate corespunzător, pentru prevenirea accesului neautorizat sau conexiunilor persistente. În mediile OT, configurarea și terminarea securizată a sesiunilor sunt esențiale pentru prevenirea căilor de acces persistente care ar putea fi exploatate pentru perturbarea operațiunilor fizice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Utilizarea autentificării puternice
    - Sesiunile la distanță ar trebui protejate prin autentificatori puternici care rezistă atacurilor prin reluare. MFA ar trebui utilizată acolo unde este posibil.
- Protejarea comunicațiilor
    - Ar trebui implementate mecanisme criptografice pentru asigurarea confidențialității și integrității comunicațiilor de mentenanță la distanță.
- Închiderea sesiunilor
    - Conexiunile la distanță ar trebui închise imediat după finalizarea mentenanței pentru a reduce expunerea la potențiale amenințări.
- Verificarea deconectării
    - Verificarea deconectării la distanță ar trebui utilizată pentru a confirma că sesiunile au fost închise complet și nu mai sunt accesibile.
- Asigurarea conformității și respectării normelor
    - Toate activitățile de acces la distanță ar trebui să fie conforme cu procedurile interne de securitate și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.AM-08.13

Organizația trebuie să solicite ca serviciile de diagnosticare pentru mentenanța la distanță să fie efectuate de pe un sistem care implementează caracteristici de securitate similare cu cele implementate pe sistemul critic echivalent al organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că serviciile de mentenanță și diagnosticare la distanță sunt prestate de sisteme care implementează caracteristici de securitate echivalente cu cele ale sistemelor critice ale organizației. În mediile OT, această aliniere este esențială pentru menținerea unei posturi de securitate consecvente, pentru prevenirea introducerii vulnerabilităților și pentru protejarea siguranței, fiabilității și continuității operațiunilor fizice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Utilizarea autentificării puternice
    - Sistemele la distanță ar trebui să implementeze MFA pentru a asigura că accesul este restricționat la personalul autorizat.
- Menținerea înregistrărilor activităților
    - Ar trebui menținute și revizuite periodic jurnale detaliate ale tuturor activităților de mentenanță la distanță, pentru detecția anomaliilor sau acțiunilor neautorizate.
- Alinierea instrumentelor și procedurilor
    - Toate instrumentele și procedurile utilizate în timpul mentenanței la distanță ar trebui să fie aliniate la politicile organizației și documentate în planurile relevante de securitate cibernetică sau a informației.
- Închiderea sesiunilor
    - Sesiunile la distanță ar trebui închise corespunzător după finalizarea mentenanței, pentru prevenirea accesului prelungit.
- Asigurarea conformității și respectării normelor
    - Sistemele și activitățile la distanță ar trebui să respecte cerințele interne de securitate și să se conformeze legilor, reglementărilor și standardelor din domeniu aplicabile.

[ID.RA] EVALUAREA RISCURILOR

Înțelegerea riscului de securitate cibernetică pentru organizație, active și persoane fizice de către organizație.

ID.RA-01

Vulnerabilitățile activelor sunt identificate, validate și înregistrate.

ID.RA-01.1

Amenințările și vulnerabilitățile trebuie identificate în toate activele relevante, inclusiv software-ul, arhitecturile de rețea și de sistem, precum și incintele care găzduiesc active informatice critice.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a ajuta organizațiile să atenueze riscurile de securitate cibernetică prin identificarea amenințărilor și vulnerabilităților din activele lor critice. Acestea includ software-ul, rețelele, sistemele și incintele care susțin operațiunile informatice esențiale.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Înțelegerea conceptelor cheie
    - O vulnerabilitate este o slăbiciune a hardware-ului, software-ului sau procedurilor care ar putea fi exploatată.
    - O amenințare este un eveniment sau un actor care poate încerca să exploateze o vulnerabilitate.
    - Un risc este impactul posibil în cazul în care o amenințare exploatează cu succes o vulnerabilitate.
- Identificarea activelor relevante
    - Toate sistemele, aplicațiile, rețelele și incintele critice ar trebui enumerate și documentate.
- Răspunsul la vulnerabilități
    - Organizațiile ar trebui să ia măsuri în cazul vulnerabilităților raportate de surse de încredere (de exemplu, vânzătorilor, furnizori de servicii, avertizări guvernamentale).
    - La nivel de bază, scanarea activă nu este necesară, dar vulnerabilitățile cunoscute ar trebui remediate prompt.
- Conștientizarea amenințărilor
    - Organizațiile ar trebui să se informeze în permanență cu privire la amenințările comune relevante pentru sectorul lor (de exemplu, phishing, ransomware, riscuri legate de lanțul de aprovizionare).

ID.RA-01.2

Trebuie stabilit un proces pentru monitorizarea, identificarea și documentarea continuă a vulnerabilităților sistemelor critice pentru activitate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura identificarea, monitorizarea și documentarea continuă a vulnerabilităților sistemelor critice pentru activitate, pentru a sprijini atenuarea riscurilor în timp util și menținerea rezilienței operaționale.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Utilizarea scanării vulnerabilităților acolo unde este sigur
    - Scanarea vulnerabilităților ar trebui aplicată sistemelor IT și OT în cazul în care aceasta nu perturbă operațiunile și nu compromite siguranța. În mediile OT ar trebui preferate metodele pasive sau neintruzive.
- Punerea în funcțiune a instrumentelor de management al vulnerabilităților
    - Ar trebui utilizate instrumente pentru detecția software-ului neactualizat, a configurațiilor incorecte și a firmware-ului învechit atât în cadrul activelor IT, cât și OT.
- Evaluarea arhitecturilor pentru identificarea punctelor slabe
    - Arhitecturile de rețea și de sistem, inclusiv segmentarea, căile de acces la distanță și componentele vechi, ar trebui revizuite pentru identificarea defectelor de proiectare care ar putea expune sistemele OT la amenințări cibernetice.
- Monitorizarea surselor de informații privind amenințările
    - Sursele publice și private de informații privind amenințările cibernetice ar trebui monitorizate pentru identificarea vulnerabilităților care afectează produsele OT, ICS și tehnologiile specifice vânzătorilor.
- Revizuirea software-ului dezvoltat de organizație
    - Aplicațiile personalizate, inclusiv cele utilizate în medii OT (de exemplu, HMI-uri, logica PLC), ar trebui analizate și testate pentru identificarea practicilor de codificare nesigure și configurațiile implicite.
- Evaluarea procedurilor operaționale
    - Procesele și procedurile, în special cele care implică accesul la distanță, mentenanța și operațiunile de urgență, ar trebui revizuite pentru identificarea punctelor slabe care ar putea afecta integritatea sistemului OT.

ID.RA-01.3

Organizația trebuie să stabilească și să mențină un proces documentat care să permită ca vulnerabilitățile să fie revizuite, analizate și remediate în mod continuu și care să prevadă schimbul de informații, acolo unde este cazul.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că vulnerabilitățile sunt revizuite, analizate și remediate în mod continuu, printr-un proces documentat care sprijină, acolo unde este cazul, și schimbul de informații.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Încorporarea lecțiilor învățate și a amenințărilor emergente
    - Procesul ar trebui actualizat în funcție de incidente, modificări tehnologice și amenințări în continuă evoluție, inclusiv cele care vizează sistemele OT și protocoalele industriale.
- Utilizarea observațiilor interne și a indicatorilor
    - Rezultatele auditului, indicatorii și observațiile operatorilor ar trebui utilizate pentru rafinarea procesului de management al vulnerabilităților, în special în cazul în care procesele manuale sunt frecvente.
- Utilizarea SBOM
    - SBOM-urile ar trebui utilizate pentru a identifica componentele vulnerabile atât în stivele de software IT, cât și OT, inclusiv sistemele integrate și firmware-ul.
- Monitorizarea surselor de informații privind amenințările
    - Sursele de încredere, precum avizele vânzătorilor, echipa de răspuns la incidente cibernetice pentru sisteme de control industrial (ICS-CERT) și ENISA, ar trebui monitorizate pentru identificarea vulnerabilităților care afectează produsele OT, sistemele de control și dispozitivele de teren.
- Revizuirea proceselor și procedurilor
    - Procedurile operaționale, în special cele care implică accesul la distanță, mentenanța și funcțiile critice pentru siguranță, ar trebui revizuite pentru identificarea punctelor slabe care pot fi exploatate.
- Coordonarea cu departamentele de inginerie și operațiuni
    - Eforturile de remediere ar trebui planificate în coordonare cu echipele OT și de ingineri pentru evitarea perioadelor de nefuncționare neplanificate sau riscurilor de siguranță.

ID.RA-01.4

Pentru a asigura că operațiunile organizației nu sunt afectate negativ de procesul de testare, testele de performanță/încărcare și testele de penetrare asupra sistemelor organizației trebuie efectuate cu atenție.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că testele de performanță/încărcare și testele de penetrare sunt realizate cu atenție pentru evitarea perturbării operațiunilor sau a compromiterii stabilității sistemului, în special în mediile care includ sisteme critice pentru activitate sau pentru siguranță.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Stabilirea și menținerea programelor de testare
    - Programele de testare pentru testarea performanței/încărcării și testarea penetrării ar trebui adaptate la dimensiunea, complexitatea și maturitatea organizației, inclusiv la constrângerile specifice OT.
- Utilizarea mediilor de testare controlate
    - Testele de penetrare ar trebui efectuate în medii izolate sau controlate, acolo unde este posibil, pentru prevenirea impactului neintenționat asupra sistemelor OT active.
- Angajarea de hackeri etici calificați
    - Hackerii etici experimentați ar trebui folosiți pentru efectuarea testelor de penetrare, în special în medii OT complexe sau sensibile.
- Validarea măsurilor de securitate după testare
    - După testare, controalele de securitate ar trebui revalidate pentru a confirma că măsurile de protecție rămân eficace și că nu au avut loc modificări neintenționate.

Diferența față de ID.RA-01.5 (CyFun® Important)

În timp ce ID.RA-01.4 se concentrează asupra activităților de testare, precum testele de penetrare și testele de performanță/încărcare, care sunt de regulă planificate, realizate mai rar și adesea realizate în medii controlate, ID.RA-01.5 abordează efectuarea în condiții de siguranță a scanării vulnerabilităților, care este mai frecventă, adesea automatizată și trebuie gestionată cu atenție pentru evitarea perturbărilor neintenționate în sistemele OT aflate în producție.

ID.RA-01.5

Scanarea vulnerabilităților nu trebuie să afecteze negativ funcțiile sistemului.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că scanarea vulnerabilităților nu perturbă sau degradează performanța sistemelor critice pentru activitate, în special în mediile OT în care stabilitatea și disponibilitatea sistemului sunt critice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Programarea scanărilor în perioadele cu utilizare redusă
    - Scanările ar trebui efectuate în afara orelor de vârf sau în perioadele de mentenanță planificate, pentru minimizarea impactului operațional.
- Utilizarea instrumentelor de scanare neintruzive
    - Instrumentele ar trebui selectate în funcție de capacitatea lor de a scana fără a supraîncărca resursele sistemului sau a interfera cu operațiunile în timp real.
- Testarea inițială în medii de testare
    - Scanările ar trebui testate în medii care nu sunt de producție pentru identificarea potențialelor probleme înainte de punerea în funcțiune în sistemele aflate în producție.
- Aplicarea scanării incrementale
    - Scanarea ar trebui împărțită în segmente mai mici, ușor de gestionat, pentru reducerea încărcării sistemului și evitarea suprasolicitării componentelor critice.
- Monitorizarea performanței sistemului în timpul scanărilor
    - Comportamentul sistemului ar trebui monitorizat activ în timpul scanării pentru detecția și răspunsul la orice degradare a performanței sau anomalii.

Diferența față de ID.RA-01.4 (CyFun® Esențial)

În timp ce ID.RA-01.4 se concentrează asupra activităților de testare, precum testele de penetrare și testele de performanță/încărcare, care sunt de regulă planificate, realizate mai rar și adesea realizate în medii controlate, ID.RA-01.5 abordează efectuarea în condiții de siguranță a scanării vulnerabilităților, care este mai frecventă, adesea automatizată și trebuie gestionată cu atenție pentru evitarea perturbărilor neintenționate în sistemele OT aflate în producție.

ID.RA-01.6

Vulnerabilitățile trebuie identificate și gestionate în toate activele relevante, inclusiv software, arhitecturi de rețea și de sistem și incinte.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura identificarea și gestionarea sistematică a vulnerabilităților la nivelul tuturor activelor relevante, inclusiv software, arhitecturi de rețea și de sistem, precum și incintele. Aceasta se bazează pe Controlul ID.RA-01.1, care se concentrează pe identificarea atât a amenințărilor, cât și a vulnerabilităților, pentru sprijinirea reducerii riscurilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Extinderea domeniului de aplicare al managementului vulnerabilităților
    - Identificarea și remedierea vulnerabilităților ar trebui să acopere toate activele relevante, inclusiv sistemele IT și OT, aplicațiile, arhitecturile de rețea și incintele care susțin operațiunile critice.
- Menținerea unui proces dedicat de management al vulnerabilităților
    - Ar trebui să existe un proces structurat pentru urmărirea, evaluarea și atenuarea continuă a vulnerabilităților, distinct de activitățile de informații privind amenințările.
- Diferențierea între informațiile privind amenințările și managementul vulnerabilităților
    - Ar trebui menținute procese sau dovezi separate pentru a distinge între identificarea amenințărilor externe (de exemplu, actorii de amenințare, campaniile) și gestionarea punctelor slabe interne (de exemplu, sistemele neactualizate, configurațiile incorecte).
- Integrarea cu un proces mai amplu de management al riscului
    - Procesul de management al vulnerabilităților ar trebui să fie aliniat cu cadrul general de management al riscului al organizației și să sprijine luarea deciziilor în timp util.
- Asigurarea luării în considerare a aspectelor specifice OT
    - În mediile OT, managementul vulnerabilităților ar trebui să țină cont de sistemele vechi, dependențele de vânzători și constrângerile operaționale care ar putea limita opțiunile de aplicare a patch-urilor sau de scanare.

ID.RA-02

Informațiile privind amenințările cibernetice sunt obținute din forumuri și surse de schimb de informații.

ID.RA-02.1

Trebuie implementat un program de conștientizare a amenințărilor și vulnerabilităților care include o capabilitate de schimb de informații între organizații.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida capacitatea organizației de a anticipa și răspunde la amenințările cibernetice prin implementarea unui program de conștientizare a amenințărilor și vulnerabilităților, care include schimbul de informații între organizații.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Monitorizarea tacticilor actorilor de amenințare și vulnerabilitățile emergente
    - Informațiile privind amenințările cibernetice ar trebui să includă informații actualizate despre actorii de amenințare, tacticile, tehnicile și procedurile (TTP) ale acestora, precum și vulnerabilitățile tehnologiilor emergente (de exemplu, atacuri bazate pe inteligența artificială, otrăvirea datelor în învățarea automată).
- Stabilirea unei colaborări externe continue
    - Organizația ar trebui să mențină o participare activă în grupuri de securitate, forumuri și asociații profesionale pentru a primi alerte, avize și opinii ale colegilor relevante atât pentru mediile IT, cât și pentru cele OT.
- Facilitarea schimbului de informații
    - Programul ar trebui să sprijine schimbul de informații neclasificate și, acolo unde este cazul, clasificate, despre vulnerabilități și incidente între departamente și cu parteneri externi de încredere.
- Sprijinirea conștientizării specifice OT
    - Informațiile privind amenințările ar trebui să includă surse specifice OT (de exemplu, ICS-CERT, avize ale vânzătorilor) pentru a aborda vulnerabilitățile ICS, dispozitivele vechi și tehnologiile specifice sectorului.
- Diferențierea informațiilor privind amenințările de managementul vulnerabilităților
    - Programul de conștientizare ar trebui să completeze procesele de management al vulnerabilităților, dar să rămână distinct de acestea, concentrându-se pe evoluția amenințărilor externe și pe informații strategice.

ID.RA-02.2

Trebuie implementate mecanisme automatizate pentru difuzarea alertelor și avizelor de securitate către părțile interesate relevante ale organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că alertele și avizele de securitate sunt transmise prompt și în mod fiabil părților interesate relevante prin mecanisme automatizate, permițând conștientizarea și reacția în timp util în cadrul organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Implementarea platformelor de securitate centralizate
    - Soluții precum managementul informației și evenimentelor de securitate (SIEM), detecție și răspuns extinse (XDR), orchestrare, automatizare și răspuns în securitate (SOAR) sau analiza comportamentului utilizatorilor și entităților (UEBA) ar trebui utilizate pentru a colecta, analiza și corela alertele din mai multe surse, inclusiv sisteme OT și IT.
- Automatizarea distribuției alertelor
    - Alertele ar trebui configurate pentru notificarea automată a părților interesate prin e-mail, platforme de mesagerie sau alte canale, pentru asigurarea diseminării rapide a informațiilor critice.
- Utilizarea tablourilor de bord în timp real
    - Tablourile de bord ar trebui implementate pentru a oferi vizibilitate continuă asupra alertelor și avizelor de securitate, sprijinind conștientizarea situației și luarea deciziilor.
- Integrarea cu platformele de răspuns la incidente
    - Mecanismele automatizate ar trebui să sprijine distribuirea alertelor către echipele de răspuns la incidente, asigurând că acestea dispun de cele mai recente informații pentru a acționa în mod eficace.
- Extragerea din surse externe de informații privind amenințările
    - Instrumentele automatizate ar trebui să extragă date din surse externe de încredere pentru a îmbogăți alertele interne cu un context mai larg al amenințărilor, inclusiv avize specifice OT.

ID.RA-03

Amenințările interne și externe la adresa organizației sunt identificate și înregistrate.

ID.RA-03.1

Amenințările trebuie identificate și evaluate în raport cu toate activele relevante, inclusiv software-ul, arhitecturile de rețea și de sistem și incintele.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că amenințările sunt identificate și evaluate în mod sistematic în raport cu toate activele relevante, inclusiv software-ul, arhitecturile de rețea și de sistem, precum și incintele. Aceasta se bazează pe ID.RA-01.1, care stabilește fundamentul pentru identificarea atât a amenințărilor, cât și a vulnerabilităților la nivelul activelor critice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Extinderea identificării amenințărilor la toate activele
    - Amenințările ar trebui evaluate în raport cu toate activele relevante, inclusiv sistemele IT și OT, aplicațiile, arhitecturile de rețea și incintele care susțin operațiunile critice.
- Menținerea unui proces dedicat de informații privind amenințările
    - Ar trebui să existe un proces structurat pentru colectarea, analizarea și evaluarea informațiilor privind amenințările din surse interne și externe, inclusiv avize specifice sectorului și fluxuri de informații privind amenințările axate pe OT.
- Diferențierea informațiilor privind amenințările de managementul vulnerabilităților
    - Informațiile privind amenințările ar trebui gestionate separat de managementul vulnerabilităților, cu procese și dovezi distincte pentru a asigura claritatea și concentrarea. Amenințările se referă la potențiali actori sau evenimente, în timp ce vulnerabilitățile se referă la puncte slabe care ar putea fi exploatate.
- Integrarea cu analiza riscurilor
    - Amenințările identificate ar trebui corelate cu vulnerabilitățile cunoscute și înregistrate într-un registru central de riscuri pentru a sprijini stabilirea priorităților și planificarea măsurilor de atenuare, astfel cum se prevede în ID.RA-01.1.

- Includerea amenințărilor specifice OT
    - Evaluările amenințărilor ar trebui să considere riscurile specifice OT, precum compromiterea lanțului de aprovizionare, accesul la distanță neautorizat și exploatarea sistemelor vechi sau a protocoalelor proprietare.

ID.RA-05

Amenințările, vulnerabilitățile, probabilitățile și impacturile sunt utilizate pentru înțelegerea riscului inerent și pentru stabilirea priorităților în ceea ce privește răspunsul la riscuri.

ID.RA-05.1

Organizația trebuie să efectueze evaluări ale riscurilor în care riscul este determinat pe baza amenințărilor, vulnerabilităților și impactului asupra proceselor și activelor organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că evaluările riscurilor sunt realizate prin evaluarea amenințărilor, vulnerabilităților și impactului potențial al acestora asupra proceselor și activelor organizației. Acest obiectiv sprijină luarea de decizii informate și atenuarea eficace a riscurilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea amenințărilor și vulnerabilităților
    - Evaluările ar trebui să includă amenințările și vulnerabilitățile din arhitecturile software, de rețea și de sistem, precum și din incintele care găzduiesc active informatice critice.
- Evaluarea impactului asupra activității organizației
    - Impactul potențial asupra operațiunilor organizației, serviciilor și activelor organizației ar trebui analizat pentru a determina gravitatea fiecărui risc.
- Includerea factorilor umani
    - Comportamentul uman ar trebui luat în considerare la proiectarea și aplicarea politicilor de securitate, în special în mediile OT.
- Documentarea și revizuirea
    - Evaluările riscurilor ar trebui documentate, revizuite periodic și actualizate pentru a reflecta modificările survenite în sisteme, operațiuni sau peisajul amenințărilor.

ID.RA-05.2

Organizația trebuie să efectueze și documenteze evaluările riscurilor în cadrul cărora riscul este determinat pe baza amenințărilor, vulnerabilităților, impactului asupra proceselor și activelor organizației, precum și a probabilității de producere a acestora.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că evaluările riscurilor sunt realizate și documentate utilizând o abordare structurată care ia în considerare amenințările, vulnerabilitățile, impactul asupra activității organizației și probabilitatea de producere. Aceasta sprijină luarea de decizii informate și prioritizarea eforturilor de securitate cibernetică în mediile IT și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Includerea amenințărilor interne și externe
    - Evaluările riscurilor ar trebui să ia în considerare atât amenințările provenite din interiorul organizației, cât și pe cele provenite de la actori externi.
- Aplicarea metodelor recunoscute de analiză a riscurilor
    - Ar trebui utilizate metode calitative și/sau cantitative, precum modelul persoane, echipamente, software, date, organizație, mediu, servicii (MAPGOOD), ISO/IEC 27005 sau metoda de evaluare a riscurilor CIS. Aceste metode pot fi sprijinite de instrumente software de management al riscului.
- Prioritizarea pe baza probabilității și impactului
    - Resursele și investițiile în securitatea cibernetică ar trebui alocate pe baza probabilității estimate a amenințărilor și a impactului potențial asupra proceselor organizației și a activelor critice.
- Luarea în considerare a riscurilor specifice OT
    - Evaluările riscurilor ar trebui să țină cont de factori specifici OT, precum implicațiile asupra siguranței, disponibilitatea sistemului, tehnologiile vechi și constrângerile operaționale.

ID.RA-05.3

Rezultatele evaluării riscurilor trebuie comunicate părților interesate relevante.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că rezultatele evaluării riscurilor sunt comunicate în mod eficace părților interesate relevante, permițând luarea de decizii informate și adoptarea de răspunsuri coordonate în cadrul organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea unui plan sau a unei proceduri de comunicare
    - Un proces documentat ar trebui să specifice modul, momentul și destinatarii comunicării informațiilor legate de riscuri. Acesta ar trebui să includă atât părți interesate interne, cât și externe.
- Asigurarea unei comunicări clare și în timp util
    - Informațiile privind riscurile ar trebui comunicate prompt și într-un format ușor de înțeles, în special pentru părțile interesate fără cunoștințe tehnice, implicate în procesul decizional operațional sau strategic.
- Verificarea informațiilor de contact ale părților interesate
    - Datele de contact ale părților interesate ar trebui revizuite cel puțin anual pentru asigurarea acurateței și fiabilității comunicărilor.
- Sprijinirea nevoilor de comunicare specifice OT
    - Procedurile de comunicare ar trebui să țină cont de rolurile specifice OT, precum echipele de ingineri, mentenanță și operațiuni, asigurând că acestea primesc informații relevante privind riscurile legate de disponibilitatea, siguranța și continuitatea sistemului.

ID.RA-06

Răspunsurile la riscuri sunt selectate, prioritizate, planificate, urmărite şi comunicate.

ID.RA-06.1

Răspunsurile la riscuri trebuie identificate, prioritizate, planificate, urmărite şi comunicate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că răspunsurile la riscuri sunt identificate în mod clar, prioritizate, planificate, urmărite și comunicate, pentru sprijinirea atenuării eficace a riscurilor și luarea de decizii informate în cadrul organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aplicarea criteriilor de răspuns la riscuri
    - Deciziile de acceptare, transfer, atenuare sau evitare a riscurilor ar trebui să respecte criteriile de management al vulnerabilităților ale organizației, astfel cum sunt menționate în ID.RA-08.1.
- Selectarea cu atenție a controalelor compensatorii
    - În cazul în care atenuarea directă nu este fezabilă, controale compensatorii ar trebui selectate pe baza aceloraşi criterii pentru asigurarea unei reduceri consistente a riscurilor.
- Fundamentarea măsurilor pe rezultatele evaluărilor riscurilor
    - Toate deciziile privind răspunsul la riscuri ar trebui fundamentate pe rezultatele evaluărilor riscurilor documentate, asigurând alinierea cu amenințările, vulnerabilitățile și impactul real asupra activității.
- Urmărirea progresului implementării
    - Măsurile de răspuns la riscuri ar trebui urmărite folosind instrumente structurate, precum un registru de riscuri, un plan de acțiune și etape cheie sau rapoarte detaliate privind riscurile.
- Comunicarea în ordinea priorității
    - Răspunsurile planificate la riscuri ar trebui comunicate părților interesate afectate în ordinea priorității, asigurând conștientizarea și coordonarea în timp util.
- Includerea considerentelor specifice OT
    - Răspunsurile la riscuri în mediile OT ar trebui să țină seama de constrângerile operaționale, cerințele de siguranță și disponibilitatea sistemului, în special atunci când se planifică măsuri de atenuare sau de compensare.

ID.RA-08

Procesele pentru primirea, analizarea și răspunsul la divulgarea vulnerabilităților sunt stabilite.

ID.RA-08.1

Organizația trebuie să stabilească și să implementeze un plan de management al vulnerabilităților pentru identificarea, analizarea, evaluarea, atenuarea și comunicarea tuturor tipurilor de vulnerabilități, inclusiv sub forma unui CVD, în conformitate cu modalitățile legale aplicabile.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate tipurile de vulnerabilități sunt identificate, analizate, evaluate, atenuate și comunicate în mod sistematic, printr-un plan documentat de management al vulnerabilităților. Aceasta include gestionarea divulgărilor în conformitate cu practicile CVD și cu cerințele legale aplicabile.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Stabilirea unui plan cuprinzător de management al vulnerabilităților
    - Planul ar trebui să acopere vulnerabilitățile identificate în urma testelor interne, din surse externe, precum buletinele de securitate, precum și din informațiile divulgate de cercetători, vânzători, parteneri sau organisme guvernamentale responsabile cu securitatea cibernetică.
- Atribuirea responsabilităților și monitorizarea implementării
    - Ar trebui definite roluri clare pentru procesarea, analizarea și răspunsul la vulnerabilitățile divulgate. Implementarea procedurilor ar trebui monitorizată pentru asigurarea unei gestionări prompte și eficace.
- Sprijinirea CVD
    - Planul ar trebui să includă proceduri pentru primirea și răspunsul la rapoartele privind vulnerabilitățile din partea unor părți externe. Practicile CVD ar trebui să fie aliniate cu recomandările furnizate de cadrul CVD elaborat de către ENISA, care prezintă aspecte juridice, tehnice și de comunicare.
- Asigurarea acoperirii specifice OT
    - Planul ar trebui să abordeze vulnerabilitățile din mediile OT, inclusiv sistemele vechi, componentele gestionate de vânzători și firmware-ul integrat, unde aplicarea de patch-uri sau atenuarea vulnerabilităților ar necesita coordonarea cu echipele de ingineri.

ID.RA-08.2

Organizația trebuie să implementeze mecanisme automatizate pentru diseminarea și urmărirea măsurilor corective legate de informațiile privind vulnerabilitățile, care să gestioneze automat colectarea datelor privind vulnerabilitățile, să disemineze informații, să urmărească măsurile corective, să includă raportarea și răspunderea și să permită monitorizarea continuă.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că informațiile referitoare la vulnerabilități sunt colectate, diseminate, urmărite și tratate în mod automat, printr-un proces documentat și automatizat de management al vulnerabilităților. Aceasta include facilitarea monitorizării continue, raportării și răspunderii pentru sprijinirea remedierii prompte și eficace.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Automatizarea colectării și distribuirii datelor privind vulnerabilitățile
    - Informațiile privind vulnerabilitățile ar trebui colectate din surse interne (de exemplu, audituri, scanări OT/IT) și surse externe (de exemplu, avize ale ENISA, fluxuri de informații privind amenințările, buletine ale vânzătorilor). Aceste informații ar trebui distribuite automat părților interesate relevante utilizând tablouri de bord, alerte sau instrumente de comunicare integrate.
- Urmărirea măsurilor de remediere și monitorizarea progresului
    - Sistemele automatizate ar trebui să urmărească implementarea măsurilor de remediere, precum aplicarea de patch-uri, modificări de configurare sau controale compensatorii. Progresul ar trebui monitorizat pentru a asigura rezolvarea în timp util.
- Generarea de rapoarte și asigurarea răspunderii
    - Ar trebui generate rapoarte periodice pentru a oferi vizibilitate asupra stării vulnerabilităților, responsabilităților atribuite și progresului remediilor. Aceste rapoarte ar trebui să sprijine transparența și supravegherea managementului.
- Facilitarea monitorizării continue prin automatizare
    - Ar trebui instituite mecanisme automatizate pentru monitorizarea continuă a noilor vulnerabilități și pentru asigurarea actualizării corespunzătoare a fluxurilor de lucru de remediere.

- Evaluarea eficacității automatizării
    - Eficacitatea automatizării ar trebui evaluată periodic pentru determinarea îmbunătățirilor în ceea ce privește timpul de răspuns, eficiența și gradul de conștientizare al părților interesate. Dacă obiectivele nu sunt îndeplinite, ar trebui efectuate ajustări.
- Asigurarea acoperirii specifice OT
    - Procesul de automatizare ar trebui să includă mediile OT, abordând sistemele vechi, componentele gestionate de vânzători și firmware-ul integrat. Pentru remedierea problemelor din aceste medii poate fi necesară coordonarea cu echipele de ingineri.

[ID.IM] ÎMBUNĂTĂȚIRE

Îmbunătățirile aduse proceselor, procedurilor și activităților organizaționale de management al riscului de securitate cibernetică sunt identificate în toate funcțiile CyFun®.

ID.IM-02

Îmbunătățirile sunt identificate pe baza testelor și exercițiilor de securitate, inclusiv a celor efectuate în coordonare cu furnizorii și părțile terțe relevante.

ID.IM-02.1

Testele și exercițiile de securitate, inclusiv cele efectuate împreună cu furnizorii și părțile terțe relevante, trebuie utilizate pentru identificarea domeniilor care necesită îmbunătățiri.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a identifica oportunități de îmbunătățire a securității, a răspunsului la incidente și a rezilienței prin efectuarea de teste și exerciții de securitate - atât la nivel intern, cât și în colaborare cu furnizorii și părțile terțe. În mediile OT, aceste activități sunt esențiale pentru asigurarea pregătirii pentru incidente care ar putea afecta operațiunile fizice, siguranța sau continuitatea serviciilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Evaluarea gradului de pregătire pentru răspunsul la incidente
    - Teste de securitate, precum exerciții teoretice, simulări, revizuiri interne și audituri, ar trebui utilizate pentru a identifica îmbunătățiri în procedurile de răspuns la incidente.
- Coordonarea cu părțile externe
    - Ar trebui să se organizeze exerciții care să implice furnizorii de servicii critice și furnizorii de produse pentru a consolida continuitatea activității, recuperarea în caz de dezastru și capabilitățile de răspuns la incidente.
- Implicarea părților interesate interne
    - Rolurile interne relevante, inclusiv membri ai conducerii superioare, departamentul juridic și resursele umane, ar trebui să fie implicate în exerciții pentru a asigura conștientizarea și alinierea organizațională largă.
- Efectuarea de teste de penetrare
    - Sistemele cu risc ridicat ar trebui supuse testelor de penetrare pentru identificarea vulnerabilităților. Aceste teste ar trebui aprobate în prealabil de conducere.

- Testarea planurilor de urgență
    - Planurile de răspuns la produse sau servicii neautorizate sau falsificate ar trebui testate și perfecționate pentru asigurarea unei recuperări eficace.
- Asigurarea conformității și respectării normelor
    - Toate activitățile de testare ar trebui să fie conforme cu procedurile interne și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.IM-03

Îmbunătățirile sunt identificate în urma executării proceselor, procedurilor și activităților operaționale.

ID.IM-03.1

Organizația trebuie să realizeze evaluări post-incident pentru analizarea lecțiilor învățate din activitățile de răspuns la incidente și de recuperare și, în consecință, pentru îmbunătățirea proceselor/procedurilor/tehnologiilor în vederea consolidării rezilienței sale cibernetice.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida reziliența cibernetică prin învățarea din incidente. După fiecare incident, organizația ar trebui să analizeze ce s-a întâmplat, modul în care acesta a fost gestionat și ce poate fi îmbunătățit la nivelul proceselor, procedurilor sau tehnologiilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Realizarea revizuirilor post-incident
    - O evaluare structurată ar trebui realizată după fiecare incident, cu implicarea tuturor participanților relevanți.
- Reflectarea asupra întrebărilor cheie
    - Revizuirea ar trebui să cuprindă:
        - Ce s-a întâmplat și de ce.
        - Cum a fost gestionat răspunsul.
        - Ce a funcționat bine și ce nu.
        - Ce măsuri ar trebui luate pentru prevenirea recurenței.
- Documentarea lecțiilor învățate
    - Constatările rezultate în urma revizuirii ar trebui documentate și comunicate echipelor relevante.
- Actualizarea politicilor și procedurilor
    - Politicile, procesele și procedurile de securitate cibernetică ar trebui revizuite și actualizate periodic, cel puțin anual, pentru a reflecta lecțiile învățate.
- Îmbunătățirea instrumentelor și capacităților
    - Acolo unde este cazul, tehnologiile și instrumentele de răspuns ar trebui adaptate sau actualizate pe baza informațiilor obținute în urma incidentului.

ID.IM-03.2

Organizația trebuie să încorporeze lecțiile învățate din activitățile de gestionare a incidentelor în procesele și/sau procedurile actualizate sau noi de gestionare a incidentelor, care sunt încadrate de o instruire adecvată după revizuire, aprobare și testare.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a îmbunătăți capabilitățile organizației de gestionare a incidentelor prin încorporarea lecțiilor învățate din incidentele anterioare în procesele și procedurile actualizate sau noi. În mediile OT, unde incidentele pot afecta direct sistemele fizice și continuitatea operațională, aplicarea cunoștințelor din lumea reală contribuie la consolidarea eficacității răspunsului și la reducerea probabilității de eșecuri repetate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Acoperirea întregului ciclu de viață al incidentului
    - Lecțiile ar trebui extrase din toate etapele gestionării incidentelor, inclusiv identificarea, clasificarea, prioritizarea, investigarea, rezolvarea, recuperarea, închiderea și revizuirea post-incident.
- Demonstrarea optimizării proceselor
    - Actualizările procedurilor de gestionare a incidentelor ar trebui să reflecte informațiile obținute din incidentele anterioare și să fie documentate în mod clar.
- Colaborarea cu furnizorii
    - Sesiunile de analiză a lecțiilor învățate ar trebui desfășurate împreună cu furnizorii cheie pentru îmbunătățirea coordonării și răspunsului în cadrul lanțului de aprovizionare.
- Utilizarea indicatorilor de performanță
    - Indicatorii ar trebui utilizați pentru urmărirea și evaluarea eficacității gestionării incidentelor în timp și pentru ghidarea îmbunătățirilor.
- Asigurarea conformității și respectării normelor
    - Toate actualizările proceselor și procedurilor ar trebui să fie conforme cu cerințele interne de guvernanță și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.IM-03.3

Organizația trebuie să identifice îmbunătățiri rezultate din activitățile de monitorizare, măsurare, evaluare și din lecțiile învățate și să le transpună în procese/proceduri/tehnologii îmbunătățite pentru consolidarea rezilienței sale cibernetice (îmbunătățire continuă).

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida reziliența cibernetică a organizației prin identificarea îmbunătățirilor rezultate din monitorizare, măsurători, evaluări și lecții învățate și transpunerea acestora în procese, proceduri sau tehnologii actualizate. În mediile OT, în care fiabilitatea și siguranța sistemului sunt strâns legate de performanța cibernetică, îmbunătățirea continuă ajută la menținerea integrității operaționale și la adaptarea la amenințările în continuă evoluție.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Utilizarea indicatorilor de reziliență cibernetică
    - Indicatorii ar trebui utilizați pentru evaluarea capacității organizației de a rezista și de a se recupera în urma incidentelor cibernetice, sprijinind managementul riscului și luarea deciziilor informate.
- Aplicarea măsurilor de eficacitate (MOE)
    - MOE ar trebui utilizate pentru evaluarea și compararea eficacității diferitelor strategii de reziliență cibernetică și pentru ghidarea deciziilor de investiții sau proiectare.
- Implementarea indicatorilor orientați către obiective
    - Indicatorii ar trebui să acopere pregătirea, continuitatea operațională în timpul atacurilor, limitarea daunelor și capabilitățile de recuperare și restaurare.
- Efectuarea de evaluări independente
    - Echipe independente ar trebui angajate pentru efectuarea de evaluări și oferirea de informații obiective cu privire la domeniile care necesită îmbunătățiri.
- Utilizarea sistemelor de notare structurate
    - Ar trebui luate în considerare metodologii de notare, precum Situated Scoring Methodology for Cyber Resiliency (SSM-CR) elaborat de către MITRE, pentru a sprijini evaluarea structurată și prioritizarea îmbunătățirilor.
- Asigurarea conformității și respectării normelor
    - Toate îmbunătățirile ar trebui să fie aliniate cu cerințele interne de guvernanță și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.IM-03.4

Organizația trebuie să colaboreze și partajeze informații despre incidentele de securitate legate de sistemele sale critice și măsurile de atenuare cu partenerii desemnați.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida reziliența cibernetică prin schimbul de informații cu partenerii desemnați cu privire la incidentele de securitate și măsurile de atenuare legate de sistemele critice. În mediile OT, schimbul de informații coordonat și în timp util contribuie la prevenirea răspândirii amenințărilor, sprijină recuperarea mai rapidă și îmbunătățește apărarea colectivă în cadrul sistemelor interconectate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea rolurilor și atribuțiilor de autoritate
    - IRP-ul ar trebui să descrie în mod clar rolurile, responsabilitățile și autorizațiile pentru partajarea informațiilor legate de incidente cu partenerii desemnați.
- Instruirea echipei de răspuns
    - Personalul de răspuns la incidente ar trebui instruit periodic cu privire la procedurile de comunicare cu partenerii externi în timpul și după incidente.
- Coordonarea cu partenerii
    - Schimbul de informații ar trebui să includă detalii despre incidente, măsuri de atenuare și lecții învățate, în special cu furnizorii și prestatorii de servicii implicați în operațiunile critice ale sistemului.
- Consultarea recomandărilor de încredere
    - Practicile relevante ar trebui să se bazeze pe surse de încredere, precum Ghidul de securitate 22-001 elaborat de către ENISA/CERT-EU, care furnizează măsuri recomandate de atenuare a amenințărilor critice.
- Asigurarea conformității și respectării normelor
    - Toate activitățile de colaborare și partajare ar trebui să fie conforme cu politicile interne și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.IM-03.5

Comunicarea eficacității tehnologiilor de protecție trebuie împărtășită părților interesate relevante.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că eficacitatea tehnologiilor de protecție este comunicată în mod clar părților interesate relevante. În mediile OT, în care instrumentele de protecție asigură securitatea sistemelor fizice critice, o comunicare eficace sprijină luarea de decizii în cunoștință de cauză, conștientizarea riscurilor și alinierea între echipele tehnice și non-tehnice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Adaptarea comunicării cu părțile interesate
    - Informațiile ar trebui adaptate la nevoile diferitelor categorii de public; echipele tehnice ar putea avea nevoie de jurnale detaliate, în timp ce conducerea executivă ar putea avea nevoie de rezumate la nivel înalt legate de riscurile organizației.
- Depășirea indicatorilor tehnici
    - Comunicarea ar trebui să includă nu numai date (de exemplu, amenințări blocate, incidente detectate), ci și informații despre postura de risc, tendințele emergente și măsurile recomandate.
- Includerea tuturor rolurilor relevante
    - Părțile interesate, precum CISO, echipele de securitate IT, responsabilii cu conformitatea, auditorii interni și conducerea executivă, ar trebui să primească informațiile necesare pentru îndeplinirea responsabilităților.
- Monitorizarea și raportarea performanței
    - Performanța tehnologiilor de protecție (de exemplu, antivirus, firewall-uri, prevenția intruziunilor, detecția endpoint-urilor, prevenirea pierderii datelor - DLP) ar trebui monitorizată și raportată în mod continuu.
- Sprijinirea îmbunătățirii continue
    - Comunicarea ar trebui să contribuie la identificarea lacunelor, la informarea deciziilor strategice și la promovarea unei culturi a transparenței și a reziliență.
- Asigurarea conformității și respectării normelor
    - Toate practicile de comunicare ar trebui să fie aliniate cu politicile interne și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.IM-03.6

Organizația trebuie să implementeze, acolo unde este fezabil, mecanisme automatizate pentru facilitarea procesului de schimb de informații și colaborare.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a îmbunătăți eficiența, acuratețea și securitatea schimbului de informații și a colaborării prin implementarea de mecanisme automatizate acolo unde este fezabil. În mediile OT, automatizarea contribuie la reducerea erorilor manuale, la punerea în aplicare a controalelor de acces și la sprijinirea luării de decizii în timp util în cadrul sistemelor interconectate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Corelarea autorizațiilor de acces
    - Instrumentele automatizate ar trebui să verifice dacă drepturile de acces ale partenerilor care partajează informații sunt aliniate cu nivelul de sensibilitate a informațiilor. Neconcordanțele ar trebui semnalate înainte de partajare.
- Automatizarea punerii în aplicare a politicilor
    - Sistemele ar trebui să evalueze automat dacă informațiile pot fi partajate pe baza clasificării acestora și a drepturilor de acces ale destinatarului. Aceste verificări ar trebui integrate cu sistemele de managementul identității și accesului (IAM) pentru a asigura actualizarea datelor de autorizare.
- Controlul căutării și recuperării
    - Instrumentele de căutare și recuperare ar trebui să pună în aplicare restricții de acces utilizând etichetarea și clasificarea metadatelor, asigurându-se că utilizatorii pot accesa numai informațiile autorizate.
- Activități de monitorizare și audit
    - Jurnalizarea și monitorizarea automată ar trebui să urmărească toate acțiunile de schimb de informații. Jurnalele ar trebui revizuite periodic pentru detecția accesului neautorizat sau încălcările politicii.

- Promovarea utilizabilității și a instruirii
    - Instrumentele automate ar trebui să fie ușor de utilizat pentru a încuraja utilizarea corectă. Ar trebui furnizată instruire pentru ca utilizatorii să înțeleagă cum să folosească aceste instrumente în mod eficace și responsabil.
- Asigurarea conformității și respectării normelor
    - Toate mecanismele automatizate ar trebui să fie aliniate cu politicile interne și să respecte legile, reglementările și standardele din domeniu aplicabile.

ID.IM-03.7

Organizația trebuie să implementeze echipe independente pentru evaluarea proceselor sale, cele mai bune practici și soluțiile tehnologice pentru protejarea sistemelor și activelor critice.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida protecția sistemelor și activelor critice prin asigurarea unor evaluări obiective ale proceselor, practicilor și tehnologiilor organizației. În mediile OT, evaluările independente contribuie la identificarea vulnerabilităților, la reducerea prejudecăților și la susținerea îmbunătățirii continue a rezilienței și siguranței sistemului.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Implicarea echipelor independente
    - Evaluatorii independenți ar trebui să includă personal intern care nu este implicat în dezvoltarea sau funcționarea sistemului și experți externi care nu au legături financiare sau operaționale cu sistemul.
- Asigurarea imparțialității
    - Evaluatorii ar trebui să fie liberi de conflicte de interese. Rolurile de evaluare ar trebui rotite pentru evitarea prejudecăților legate de familiaritate. Independența și calificările ar trebui să fie documentate.
- Definirea clară a domeniului de aplicare și a criteriilor
    - Obiectivele, domeniul de aplicare și criteriile de evaluare ar trebui convenite în prealabil pentru a preveni influența nejustificată din partea părților interesate.
- Stabilirea liniilor de raportare independente
    - Rezultatele evaluării ar trebui raportate direct conducerii superioare a organizației sau unui organism de supraveghere, ocolind echipele responsabile de sistemele revizuite.
- Revizuirea periodică a eficacității evaluării
    - Independența și performanța echipelor de evaluare ar trebui revizuite periodic pentru menținerea obiectivității și relevanței.

ID.IM-03.8

Organizația trebuie să se asigure că planul de securitate pentru sistemele sale critice facilitează revizuirea, testarea și îmbunătățirea continuă a proceselor de protecție a securității.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că planul de securitate al organizației pentru sistemele critice sprijină revizuirea periodică, testarea și îmbunătățirea continuă a măsurilor de protecție. În mediile OT, aceasta contribuie la menținerea integrității sistemelor, la adaptarea la amenințările în continuă evoluție și la alinierea cu eforturile mai ample de management al riscului.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Elaborarea și menținerea unui plan de securitate
    - Un plan documentat ar trebui să descrie modul în care sistemele critice sunt protejate împotriva amenințărilor la adresa securității. Acesta ar trebui să fie distinct de planul de tratare a riscurilor, dar aliniat cu acesta.
- Concentrarea pe controale operaționale și tehnice
    - Planul ar trebui să includă obiective de securitate definite, responsabilități atribuite, arhitectura de securitate, măsuri de control și proceduri de monitorizare, testare și revizuire a controalelor.
- Facilitarea revizuirii și testării periodice
    - Planul ar trebui să sprijine revizuirile programate, evaluările vulnerabilităților și testele de penetrare pentru evaluarea eficacității măsurilor de securitate.
- Sprijinirea îmbunătățirii continue
    - Actualizările ar trebui să se bazeze pe lecțiile învățate, informațiile privind amenințările, rezultatele auditurilor și modificările în peisajul amenințărilor.
- Integrarea cu managementul riscului
    - Planul ar trebui să fie aliniat cu procesele de tratare a riscurilor și de guvernanță ale organizației, pentru asigurarea coerenței și răspunderii.
- Menținerea planului actualizat
    - Planul ar trebui revizuit și actualizat periodic pentru a reflecta modificările sistemului, noile amenințări și evoluția nevoilor operaționale.

ID.IM-03.9

Organizația trebuie să efectueze evaluări specializate, inclusiv monitorizare aprofundată, scanare a vulnerabilităților, testare a utilizatorilor rău intenționați, evaluare a amenințărilor din interior, testare a performanței/încărcării și testare de verificare și validare a sistemelor critice ale organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida securitatea sistemelor critice prin efectuarea de evaluări specializate care descoperă vulnerabilitățile, evaluează performanța și testează măsurile de apărare împotriva amenințărilor interne și externe. În mediile OT, aceste evaluări contribuie la validarea protecțiilor și susțin îmbunătățirea continuă.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Efectuarea de evaluări specializate
    - Evaluările ar trebui să includă monitorizare aprofundată, scanarea vulnerabilităților, testarea utilizatorilor rău intenționați, evaluarea amenințărilor din interior, testarea performanței/încărcării și testarea de verificare și validare.
- Externalizarea către furnizori acreditați
    - Evaluările specializate ar putea fi externalizate, de preferință către organizații acreditate. Acreditarea ar trebui să respecte standarde recunoscute, precum:
        - CREST pentru testarea de penetrare și evaluarea vulnerabilităților.
        - ISO/IEC 17025 pentru laboratoarele de testare.
    - Acreditarea ar trebui acordată de organisme recunoscute, precum CREST, autorități naționale de acreditare (de exemplu, Organismul de Acreditare Belgian - BELAC) sau organisme specifice industriei (de exemplu, PCI Security Standards Council). Aceasta garantează efectuarea evaluărilor cu competență tehnică, imparțialitate și în conformitate cu bunele practici.
- Integrarea constatărilor în procesul de remediere
    - Vulnerabilitățile identificate în timpul evaluărilor ar trebui abordate prin procese de remediere stabilite, astfel cum este prevăzut în Controlul ID.IM-03.3.
- Sprijinirea evaluării gradului de pregătire și maturitate
    - Rezultatele evaluării ar trebui să informeze despre nivelul de pregătire și performanță al organizației (de exemplu, maturitatea CyFun®), ghidând îmbunătățirile vizate.

ID.IM-04

IRP-urile și alte planuri de securitate cibernetică care afectează operațiunile sunt stabilite, comunicate, menținute și îmbunătățite.

ID.IM-04.1

Planurile de urgență și continuitate trebuie stabilite, comunicate, menținute, testate, validate și îmbunătățite.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura reziliența organizațională prin stabilirea, menținerea și îmbunătățirea planurilor de urgență și continuitate care permit un răspuns eficace și recuperarea în urma întreruperilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Stabilirea unor planuri cuprinzătoare
  - Planurile ar trebui să includă:
    - IRP.
    - Plan de continuitate a activității (BCP).
    - Plan de recuperare în caz de dezastru (DRP).
  - Acestea ar trebui să abordeze întreruperile operaționale, încălcările securității datelor și defecțiunile critice pentru misiune.
- Definirea conținutului clar al planului
  - Planurile ar trebui să includă:
    - Detalii de contact și comunicare.
    - Roluri, responsabilități și atribuții de autoritate (în conformitate cu GV.RR-02.1).
    - Proceduri pentru scenarii comune.
    - Criterii pentru stabilirea priorităților, escaladarea și luarea deciziilor.
  - IRP-urile ar trebui să acopere detecția, izolarea, răspunsul și recuperarea în urma incidentelor cibernetice.
- Comunicarea și instruirea
  - Planurile ar trebui comunicate întregului personal relevant. Ar trebui stabilită o Echipă de management al crizelor, formată din reprezentanți ai departamentelor cheie (de exemplu, IT, juridic, resurse umane, relații publice) și instruită să acționeze în situații de criză.

- Menținerea și revizuirea planurilor
    - Planurile ar trebui revizuite cel puțin anual sau după modificări sau incidente majore. Actualizările ar trebui să reflecte lecțiile învățate și riscurile în evoluție.
- Testarea și validarea periodică
    - Planurile ar trebui testate prin scenarii realiste. Validarea ar trebui să confirme funcționarea procedurilor conform așteptărilor și satisfacerea nevoilor operaționale. Rezultatele ar trebui documentate.
- Îmbunătățirea continuă
    - Observațiile obținute din teste, incidente și revizuiri ar trebui să conducă la îmbunătățiri. Îmbunătățirile ar trebui prioritizate în funcție de risc și impact, pentru asigurarea continuității funcțiilor esențiale.
- A se vedea: Șabloane de politici disponibile pe www.cyfun.eu.

ID.IM-04.2

Organizația trebuie să coordoneze elaborarea și testarea IRP-urilor și a altor planuri de securitate cibernetică care afectează operațiunile, împreună cu părțile interesate, pentru a asigura că aceste planuri sunt aliniate la obiectivele generale ale organizației și contribuie la consolidarea rezilienței.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că IRP-urile și alte planuri de securitate cibernetică care afectează operațiunile sunt aliniate la obiectivele organizației și consolidează reziliența prin dezvoltarea și testarea coordonată cu părțile interesate relevante.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Revizuirea și actualizarea periodică a planurilor
    - Planurile ar trebui revizuite și actualizate pentru a reflecta evoluția amenințărilor, modificările organizaționale și nevoile operaționale.
- Implicarea timpurie a părților interesate
    - Părțile interesate, inclusiv echipele interne, furnizorii și părțile terțe relevante, ar trebui să fie implicate încă din faza incipientă a procesului de planificare, pentru asigurarea alinierii și relevanței.
- Menținerea unei comunicări continue
    - Părțile interesate ar trebui să fie informate cu privire la progresul planului, actualizări și modificări, pentru menținerea unei înțelegeri comune și o stare de pregătire.
- Coordonarea activităților de testare
    - Testarea planurilor ar trebui coordonată împreună cu părțile interesate pentru validarea eficacității, clarificarea rolurilor și consolidarea capabilităților de răspuns colaborativ.

PROTECȚIE

[PR.AA] MANAGEMENTUL IDENTITĂȚII, AUTENTIFICAREA ȘI CONTROLUL ACCESULUI

Accesul la activele fizice și logice este limitat la utilizatorii, serviciile și hardware-ul autorizate și este gestionat proporțional cu riscul evaluat de acces neautorizat.

PR.AA-01

Identitățile și datele de acces ale utilizatorilor, serviciilor și echipamentelor autorizate sunt gestionate de către organizație.

PR.AA-01.1

Identitățile și datele de acces ale utilizatorilor, serviciilor și echipamentelor autorizate trebuie gestionate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că identitățile și datele de acces ale utilizatorilor, serviciilor și echipamentelor autorizate sunt gestionate corespunzător pentru prevenirea accesului neautorizat și pentru sprijinirea operațiunilor securizate atât în mediile TIC, cât și în cele OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Cereri de acces și autorizare
    - Accesul ar trebui solicitat în mod formal, documentat și aprobat de deținătorii sistemului sau ai datelor.
    - Drepturile de acces ar trebui să respecte principiul privilegiului minim.
- Managementul identității și a datelor de acces
    - Ar trebui utilizate conturi individuale de utilizator; ar trebui evitată partajarea parolelor.
    - Parolele implicite ar trebui modificate înainte de activarea sistemelor.
    - Conturile neutilizate ar trebui dezactivate imediat.
    - Conturile de administrator ar trebui limitate, revizuite periodic și să nu fie utilizate pentru sarcini zilnice.
- Politica privind parolele
    - Ar trebui puse în aplicare reguli stricte privind parolele.
    - Parolele ar trebui modificate periodic sau imediat după ce se suspectează compromiterea lor.
    - Ar trebui să existe o politică oficială privind parolele (a se vedea și: Setul de instrumente CyFun® pe www.cyfun.eu).

- Drepturile și privilegiile ar trebui atribuite prin intermediul grupurilor de utilizatori.

- Identitatea dispozitivului și a hardware-ului
  - Fiecare dispozitiv autorizat ar trebui să aibă un identificator unic (de exemplu, adresa MAC, numărul de serie).
  - Dispozitivele ar trebui etichetate fizic pentru a facilita inventarierea și mentenanța.
- Acces partajat la PLC-uri/HMI-uri (măsuri specifice OT)
  - Dacă conturile individuale nu sunt fezabile, principiul privilegiului minim ar trebui să fie aplicat în continuare.
  - Ar trebui utilizat un server jump securizat sau un frontend HMI pentru a controla accesul, a jurnaliza activitatea și a adăuga niveluri suplimentare de autentificare.
- Acces securizat la distanță
  - Cerințele tehnice pentru accesul la distanță ar trebui definite și documentate în mod clar.
  - Ar trebui utilizate metode securizate, precum VPN-uri, protocoale criptate (de exemplu, shell securizat - SSH, securitatea stratului de transport - TLS) și MFA (a se vedea și PR.AA-03.2).
  - Accesul la distanță ar trebui monitorizat și jurnalizat.

PR.AA-01.2

Identitățile și datele de acces pentru utilizatorii, serviciile și echipamentele autorizate trebuie gestionate prin mecanisme automatizate, ori de câte ori este fezabil.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul de utilizare abuzivă a datelor de acces și de acces neautorizat prin automatizarea proceselor de management al identității și al datelor de acces, asigurând consecvența, scalabilitatea și securitatea în mediile IT și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Automatizarea managementului datelor de acces
    - Ar trebui utilizate sistemele automatizate pentru emiterea, verificarea, revocarea și auditarea datelor de acces pentru utilizatori, servicii și hardware. Aceasta reduce erorile manuale și îmbunătățește eficiența operațională.
- Implementarea unor mecanisme puternice de autentificare
    - În conformitate cu Controlul PR.AA-03.2, MFA trebuie să fie obligatorie pentru toate accesările la distanță ale rețelelor organizației. MFA ar trebui să utilizeze cel puțin doi factori independenți:
        - Cunoștințe (de exemplu, parolă sau PIN).
        - Posesie (de exemplu, token sau smartphone).
        - Inerență (de exemplu, amprentă digitală sau recunoaștere facială).
    - Acești factori ar trebui să fie independenți pentru a asigura că compromiterea unuia dintre ei nu afectează ceilalți.
- Utilizarea soluțiilor criptografice și bazate pe token-uri
    - Certificatele digitale și token-urile de identitate ar trebui utilizate pentru autentificarea utilizatorilor, dispozitivelor și serviciilor, în special în mediile OT, unde gestionarea manuală a datelor de acces poate fi nepractică.
- Asigurarea integrării specifice OT
    - Soluțiile IAM ar trebui să suporte sistemele OT, inclusiv dispozitivele vechi și componentele gestionate de vânzători, cu întreruperi minime ale operațiunilor.

- În cazul în care nu sunt fezabile conturile individuale de utilizator (de exemplu, accesul partajat la PLC-uri sau HMI-uri), accesul ar trebui să fie redirecționat prin servere jump securizate, cu jurnalizare și straturi suplimentare de autentificare. Accesul la distanță la sistemele OT ar trebui să utilizeze protocoale securizate (de exemplu, VPN, SSH, TLS), să fie limitat în timp (Just-In-Time - JIT) și să fie monitorizat în totalitate.

PR.AA-01.3

Datele de acces ale sistemului trebuie dezactivate după o perioadă specifică de inactivitate, cu excepția cazului în care aceasta ar compromite funcționarea în condiții de siguranță a proceselor (critice).

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura dezactivarea datelor de acces ale sistemului după o perioadă definită de inactivitate, cu excepția cazului în care aceasta ar compromite funcționarea în condiții de siguranță a proceselor critice. Aceasta contribuie la reducerea riscului de acces neautorizat, menținând în același timp continuitatea operațională.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Utilizarea conturilor de serviciu pentru operațiuni automatizate
    - Conturile de serviciu ar trebui utilizate pentru rularea aplicațiilor, serviciilor sau sarcinilor automatizate. Aceste conturi ar trebui configurate cu permisiuni minime, izolate de conturile utilizatorilor și monitorizate separat pentru a sprijini auditabilitatea și automatizarea securizată.
- Aplicarea principiului privilegiului minim
    - Conturile de serviciu ar trebui să aibă doar permisiunile necesare pentru funcționarea lor. Aceasta limitează potențialele utilizări abuzive și sprijină operațiunile securizate atât în mediile IT, cât și în cele OT.
- Monitorizarea și auditarea activității conturilor de serviciu
    - Acțiunile efectuate de conturile de serviciu ar trebui jurnalizate și revizuite periodic. Aceasta îmbunătățește trasabilitatea și ajută la detecția anomaliilor sau a utilizării abuzive.
- Implementarea politicilor de inactivitate a datelor de acces
    - Datele de acces ale sistemului, inclusiv cele ale conturilor de serviciu și ale utilizatorilor, ar trebui dezactivate automat după o perioadă definită de inactivitate. Excepțiile ar trebui documentate și justificate, în special în mediile OT în care funcționarea continuă este critică.
- Stabilirea procedurilor formale de acces pentru părțile externe
    - Accesul extern ar trebui să respecte un proces definit, care să includă niveluri de acces bazate pe roluri, etape de autorizare, verificarea identității și instruire pentru conștientizare. Ar trebui să existe mecanisme de monitorizare și revocare pentru a gestiona încălcările accesului.

- Luarea în considerare a aspectelor specifice OT
    - În mediile OT, politicile de dezactivare a datelor de acces ar trebui să țină cont de cerințele privind timpul de funcționare a sistemului, componentele gestionate de vânzători și sistemele vechi. Poate fi necesară coordonarea cu echipele de ingineri pentru evitarea întreruperilor operaționale.

PR.AA-01.4

Pentru tranzacțiile din cadrul sistemelor critice ale organizației, organizația trebuie să implementeze MFA, certificate criptografice, token-uri de identitate, chei criptografice și alte date de acces, după caz și acolo unde este fezabil.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura aplicarea unor mecanisme puternice de autentificare pentru tranzacțiile din cadrul sistemelor critice. Aceasta include utilizarea MFA (PR.AA-03.2), a datelor de acces criptografice și a altor metode securizate pentru protejarea operațiunilor sensibile și a schimburilor de date.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aplicarea autentificării puternice tranzacțiilor critice
    - Tranzacțiile care implică accesul la date sensibile, modificări ale configurației sistemului, executarea de comenzi, autentificarea utilizatorilor/dispozitivelor sau transmiterea de date între sisteme ar trebui protejate utilizând MFA, token-uri de identitate, chei criptografice sau certificate, acolo unde este fezabil.
- Utilizarea autentificării bazate pe context și comportament
    - Autentificarea puternică ar trebui să includă verificări bazate pe context (de exemplu, locație, oră, dispozitiv) și date biometrice comportamentale (de exemplu, tipare de tastare) pentru detecția anomaliilor și îmbunătățirea securității.
- Combinarea MFA cu autentificare unică (SSO)
    - MFA ar trebui integrată cu soluții SSO pentru a simplifica accesul, menținând în același timp o protecție robustă pentru sistemele critice interne și externe.
- Gestionarea securizată a datelor de acces criptografice
    - Certificatele criptografice, token-urile de identitate și cheile ar trebui emise, stocate, rotite și revocate securizat. Aceasta susține implementarea securizată a mecanismelor de autentificare puternice cerute de acest Control și completează PR.AA-03.2, care impune MFA pentru accesul la distanță.

- Asigurarea fezabilității specifice OT
    - În mediile OT, metodele de autentificare ar trebui adaptate la constrângerile sistemului, echipamentele vechi și cerințele de continuitate operațională. Poate fi necesară coordonarea cu echipele de ingineri pentru a implementa soluții fezabile.

PR.AA-01.5

Sistemele critice ale organizației trebuie monitorizate pentru detecția utilizării atipice a datelor de acces de sistem. Datele de acces asociate cu un risc semnificativ trebuie dezactivate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a detecta și de a răspunde la utilizarea anormală sau cu risc ridicat a datelor de acces de sistem în sistemele critice, contribuind la prevenirea accesului neautorizat, a amenințărilor din interior și a atacurilor bazate pe date de acces.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Detecția utilizării atipice a datelor de acces
    - Sistemele ar trebui monitorizate pentru detecția abaterilor de la tiparele normale de utilizare a datelor de acces, precum orele de autentificare neobișnuite, accesul din locații necunoscute, utilizarea de sisteme necunoscute, autentificări simultane din locații îndepărtate sau accesul brusc la date sensibile.
- Limitarea și răspunsul la încercările eșuate de autentificare
    - Ar trebui să fie pus în aplicare un prag pentru încercările de autentificare eșuate. Conturile ar trebui să fie blocate automat după eșecuri repetate și să rămână inaccesibile până la expirarea unei perioade de blocare definite sau până când un administrator autorizat le resetează.
- Gestionarea ciclului de viață al datelor de acces
    - Emiterea, utilizarea și revocarea datelor de acces ar trebui să fie automatizate, acolo unde este posibil. Ar trebui menținut un inventar actualizat al datelor de acces active, iar conturile neutilizate sau abandonate ar trebui să fie revizuite și dezactivate periodic.
- Monitorizarea și corelarea evenimentelor
    - Ar trebui luate în considerare instrumente SIEM sau soluții echivalente pentru detecția anomaliilor și corelarea evenimentelor între sisteme. Ar trebui implementate referințe comportamentale pentru identificarea abaterilor de la utilizarea obișnuită.
- Dezactivarea automată a datelor de acces cu risc ridicat
    - Datele de acces asociate cu activități anomale confirmate sau cu risc ridicat ar trebui dezactivate imediat. Echipele de securitate ar trebui notificate pentru investigare și răspuns. Toate acțiunile ar trebui jurnalizate în scopuri de audit și criminalistică.

- Creşterea gradului de conştientizare a utilizatorilor
    - Utilizatorii ar trebui instruiți cu privire la practicile de utilizare securizată a datelor de acces şi încurajați să raporteze activități suspecte sau anomalii în comportamentul de acces.

PR.AA-02

Identitățile sunt verificate și legate de date de acces pe baza contextului interacțiunilor.

PR.AA-02.1

Organizația trebuie să implementeze proceduri documentate pentru verificarea identității persoanelor fizice înainte de emiterea datelor de acces care oferă acces la sistemele organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control, care se bazează pe GV.RR-04.1, este de a asigura că numai persoanele fizice verificate primesc date de acces, reducând astfel riscul de fraudă de identitate, acces neautorizat și amenințări din interior.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Stabilirea unor proceduri documentate de verificare a identității
    - Ar trebui elaborat și aprobat un proces formal de verificare a identității înainte de eliberarea datelor de acces. Acest proces ar trebui să asigure răspunderea, trasabilitatea și auditabilitatea.
- Verificarea identității folosind surse de încredere
    - Verificarea identității ar trebui să fie bazată pe documente oficiale, precum cărți de identitate, pașapoarte sau permise de conducere, eliberate de autorități. În ceea ce privește procesul de integrare organizațională la distanță sau digital, practicile ar trebui să fie aliniate cu bunele practici ale ENISA în materie de verificare a identității la distanță.
- Prevenirea fraudei de identitate și a utilizării abuzive
    - Procedurile ar trebui să includă controale pentru detecția și prevenirea furtului de identitate sau a uzurpării identității. Aceasta contribuie la reducerea riscului de pierderi financiare, de afectare a reputației și de acces neautorizat.
- Asigurarea adaptării relevante pentru OT
    - Procesele de verificare a identității ar trebui adaptate mediilor OT, în special în cazul în care tehnicienii terți sau personalul vânzătorilor necesită acces la sisteme critice.

PR.AA-02.2

Organizația trebuie să se asigure că utilizează date de acces unice pentru fiecare utilizator, dispozitiv și proces autentificat care interacționează cu sistemele critice ale organizației. Aceste date de acces trebuie verificate, iar identificatorii unici trebuie înregistrați în timpul interacțiunilor cu sistemul. Se pot face excepții pentru accesul de urgență (proceduri break-glass), cu condiția ca acest acces să fie strict controlat, jurnalizat și revizuit.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că fiecare utilizator, dispozitiv și proces care interacționează cu sistemele critice este identificabil și autentificat în mod unic. Aceasta sprijină răspunderea, trasabilitatea și accesul securizat, permițând în același timp excepții controlate în situații de urgență.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Atribuirea de date de acces unice
    - Fiecare utilizator, dispozitiv și proces automatizat ar trebui să aibă propriile date de acces unice. Conturile partajate ar trebui evitate. Toate datele de acces ar trebui verificate înainte de acordarea accesului.
- Implementarea autentificării puternice
    - MFA (PR.AA-03.2) trebuie utilizată ori de câte ori este fezabil. Mecanismele de autentificare ar trebui să fie rezistente la atacurile prin reluare și la reutilizarea datelor de acces. Aceste practici sunt aliniate cu Ghidul privind autentificarea securizată a utilizatorilor elaborat de către ENISA, care recomandă autentificarea stratificată și contextuală pentru sistemele critice.
- Punerea în aplicare a practicilor de management al datelor de acces
    - Politicile privind parolele și rotația datelor de acces ar trebui puse în aplicare. Datele de acces ar trebui revizuite și actualizate periodic, în special după modificări de rol sau după procesul de ieșire organizațională. Aceasta susține principiile prevăzute în Ghidul tehnic de implementare a NIS 2 (Technical Implementation Guidance On Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of NIS2 Directive as regards technical and methodological requirements of cybersecurity risk-management measures), ultima versiune, elaborat de către ENISA, care subliniază managementul securizat al ciclului de viață al identității.
- Aplicarea controlului accesului și monitorizarea
    - Accesul ar trebui să respecte principiul privilegiului minim. Jurnalele și pistele de audit ar trebui monitorizate continuu pentru detecția anomaliilor. Activitățile suspecte ar trebui investigate prompt.

- Controlul accesului de urgență (break-glass)
    - Accesul de urgență ar trebui acordat numai prin conturi break-glass desemnate. Aceste conturi ar trebui controlate strict, limitate în timp, jurnalizate integral și revizuite după utilizare. Pentru fiecare caz ar trebui să fie necesară justificarea și aprobarea.
- Promovarea conștientizării și instruirii utilizatorilor
    - Personalul ar trebui instruit cu privire la importanța utilizării datelor de acces individuale și a raportării accesului suspect. Conștientizarea ar trebui să includă riscurile asociate partajării și utilizării abuzive a datelor de acces.
- Asigurarea fezabilității specifice OT
    - În mediile OT, datele de acces unice ar trebui implementate într-un mod care să respecte constrângerile operaționale și limitările sistemului. Poate fi necesară coordonarea cu echipele de ingineri.

PR.AA-03

Utilizatorii, serviciile și hardware-ul sunt autentificate.

PR.AA-03.1

Toate punctele de acces wireless utilizate de organizație, inclusiv cele care oferă acces pentru vizitatori, trebuie configurate, gestionate și monitorizate în mod securizat pentru prevenirea accesului neautorizat și asigurarea integrității rețelei.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate punctele de acces wireless, inclusiv cele destinate utilizării de către vizitatori, sunt configurate, gestionate și monitorizate în mod securizat, pentru prevenirea accesului neautorizat și protejarea integrității rețelei.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Securitatea generală wireless
  - Datele de acces administrative implicite ar trebui modificate imediat după instalare.
  - Transmisia identificatorului setului de servicii (SSID) ar trebui dezactivată, cu excepția cazului în care este necesară operațional.
  - Ar trebui utilizate protocoale de criptare puternice (de exemplu, Wi-Fi Protected Access 2 - WPA2 sau Wi-Fi Protected Access 3 - WPA3 cu standard avansat de criptare - AES).
  - Accesul fizic la punctele de acces wireless ar trebui restricționat.
  - Firmware-ul ar trebui actualizat periodic pentru a remedia vulnerabilitățile cunoscute.
  - Rețelele wireless ar trebui monitorizate pentru detecția punctelor de acces neautorizate și activităților suspecte.
- Securitatea Wi-Fi pentru vizitatori
  - Rețelele pentru vizitatori ar trebui izolate de sistemele interne folosind rețele locale virtuale (VLAN) sau SSID-uri separate.
  - Limitările de lățime de bandă și restricțiile de acces ar trebui aplicate rețelelor pentru vizitatori.
  - Portalurile captive ar trebui utilizate pentru afișarea termenilor de utilizare și, opțional, pentru jurnalizarea accesului vizitatorilor.
  - Datele sensibile nu ar trebui stocate sau transmise prin rețelele pentru vizitatori.
  - Wi-Fi-ul pentru vizitatori ar trebui dezactivat când nu este utilizat sau în afara programului de lucru, dacă este fezabil.

- Practici privind endpoint-urile și utilizatorii
    - Dispozitivele care se conectează la rețelele wireless ar trebui să respecte politicile de securitate pentru endpoint-uri.
    - VPN-urile ar trebui utilizate atunci când se realizează conexiuni la rețele necunoscute sau nesecurizate.
    - Datele de acces Wi-Fi ar trebui să respecte politicile privind parolele care impun complexitate și actualizări periodice.

PR.AA-03.2

MFA trebuie să fie obligatorie pentru accesul la distanță la rețelele organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a proteja rețelele organizației prin solicitarea MFA pentru toate accesările la distanță, reducând astfel riscul accesului neautorizat și al atacurilor bazate pe date de acces.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Punerea în aplicare generală a MFA
  - MFA ar trebui pusă în aplicare pe toate sistemele expuse la internet, inclusiv pentru e-mail, VPN-uri, protocol desktop la distanță (RDP), servicii cloud și portaluri web.
  - Toate accesările la distanță, inclusiv accesul vânzătorilor și contractorilor terți, ar trebui să necesite MFA.
- Selectarea tehnologiei MFA
  - Metodele MFA ar trebui selectate pe baza nivelului de securitate, a rezistenței la phishing și a compatibilității operaționale.
  - Opțiunile obișnuite includ:
    - Token-uri hardware parolă unică bazată pe timp (TOTP) - securizate, rezistență limitată la phishing.
    - Aplicații de autentificare (software TOTP) - utilizate la scară largă, securitate moderată.
    - Chei de acces - fără parolă, ușor de utilizat, securizate din punct de vedere criptografic.
    - Fast Identity Online 2 (FIDO2) - bazat pe platformă sau hardware - autentificare criptografică puternică.
    - Aplicații capabile să trimită automat date către utilizator - convenabile, dar ar putea fi vulnerabile la oboseală cauzată de notificări push.
  - MFA bazată pe SMS și e-mail ar trebui evitată din cauza vulnerabilităților de securitate.
- Măsuri de securitate auxiliare
  - Politicile privind parolele puternice ar trebui puse în aplicare împreună cu MFA.
  - Utilizatorii ar trebui instruiți să se deconecteze în mod explicit din sesiuni.
  - Instrumentele și platformele antimalware ar trebui actualizate.
  - Ar trebui efectuată instruire periodică pentru conștientizare în privința atacurilor de phishing.

- Considerații specifice OT privind MFA (a se vedea și PR.AA-01.1)
  - Acces partajat la PLC-uri/HMI-uri.
    - Dacă conturile individuale nu sunt fezabile, ar trebui aplicat principiul privilegiului minim.
    - Trebuie utilizat un server jump securizat sau un frontend HMI pentru controlul accesului, jurnalizarea activității și adăugarea unui nivel de autentificare.
  - Acces securizat la distanță la sistemele OT
    - Cerințele tehnice și procedurale pentru accesul la distanță ar trebui definite în mod clar.
    - Ar trebui utilizate protocoale securizate (de exemplu, VPN, SSH, TLS).
    - MFA ar trebui impusă pentru toate accesările OT la distanță, în special pentru furnizorii terți.
    - Controalele de acces JIT ar trebui utilizate pentru a acorda acces temporar, limitat în timp.
    - Toate accesările la distanță ar trebui jurnalizate și monitorizate.
  - Integrare și compatibilitate.
    - Soluția MFA ar trebui să fie compatibilă atât cu sistemele IT, cât și cu cele OT.
    - Integrarea ar trebui testată în medii OT pentru a evita întreruperile.
    - În cazul în care integrarea directă nu este posibilă, ar trebui utilizate platforme intermediare securizate (de exemplu, servere jump).

PR.AA-03.3

Organizația trebuie să definească, documenteze și implementeze restricții de utilizare, cerințe de conectare și proceduri de autorizare pentru accesul la distanță la sistemele sale critice. Aceste controale trebuie să asigure că numai utilizatorii aprobați se pot conecta, folosind metode securizate, cu acces limitat la ceea ce este necesar pentru rolul lor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că accesul la distanță la sistemele critice este strict controlat prin restricții de utilizare definite, metode de conectare securizate și proceduri formale de autorizare. Aceasta ajută la prevenirea accesului neautorizat și limitează expunerea la amenințările cibernetice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea restricțiilor de utilizare
    - Identificarea sistemelor care sunt critice (de exemplu, sisteme OT, servere de producție, baze de date financiare). Definirea persoanelor sau rolurilor care pot avea acces la acestea la distanță (de exemplu, roluri specifice, vânzători terți). Limitarea accesului la intervalele de timp aprobate și restricționarea acestuia numai la sistemele și funcțiile necesare pentru rolul utilizatorului.
- Stabilirea unor cerințe de conectare securizată
    - Accesul la distanță ar trebui stabilit utilizând metode securizate, precum VPN-uri cu criptare puternică, TLS/SSH sau servere jump pentru medii OT. Tot accesul la distanță ar trebui protejat prin MFA, în conformitate cu PR.AA-03.2. Dispozitivele utilizate pentru accesul la distanță ar trebui să îndeplinească cerințele de securitate ale endpoint-urilor (de exemplu, antivirus, aplicarea de patch-uri).
- Documentarea și aprobarea accesului
    - O politică de acces la distanță ar trebui să definească procedurile de solicitare și aprobare, rolurile și cerințele tehnice. Ar trebui menținut un registru al utilizatorilor la distanță, care să includă domeniul de acces, datele de aprobare și termenele de revizuire.
- Monitorizarea și revizuirea accesului
    - Toate sesiunile la distanță ar trebui jurnalizate, capturând identitatea utilizatorului, ora, durata și sistemele accesate. Jurnalele ar trebui revizuite periodic pentru detecția anomaliilor. Permisiunile și configurațiile de acces la distanță ar trebui auditate periodic.

- Aplicarea controalelor specifice OT
    - Pentru sistemele OT, accesul ar trebui să fie direcționat prin interfețe frontend securizate sau servere jump. Dacă sunt necesare conturi partajate (de exemplu, pentru PLC-uri sau HMI-uri), accesul ar trebui să fie jurnalizat, limitat în timp, protejat prin MFA la nivelul serverului jump și să respecte principiul privilegiului minim.
- Alinierea la recomandările ENISA
    - Aceste practici sunt în conformitate cu Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA, care recomandă politici de acces securizat la distanță, autentificare puternică și monitorizare continuă ca parte a managementului riscului de securitate cibernetică pentru sistemele critice.

PR.AA-03.4

Accesul la distanță la sistemele critice ale organizației trebuie monitorizat, iar mecanisme criptografice trebuie implementate acolo unde se consideră necesar.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că accesul la distanță la sistemele critice nu este doar restricționat și aprobat (conform definiției din PR.AA-03.3), ci și monitorizat și protejat în mod activ folosind mecanisme criptografice pentru prevenirea accesului neautorizat și compromiterea datelor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Monitorizarea activităților de acces la distanță
    - Toate sesiunile de acces la distanță ar trebui jurnalizate, capturând identitatea utilizatorului, ora, durata și sistemele accesate. Instrumentele de monitorizare ar trebui să detecteze tiparele de acces neobișnuite sau neautorizate și să alerteze echipele de securitate în timp real. Jurnalele ar trebui revizuite periodic și păstrate în conformitate cu politica.
- Aplicarea protecțiilor criptografice
    - Conexiunile la distanță ar trebui să utilizeze protocoale de criptare puternice, precum TLS, SSH sau securitatea protocolului de internet (IPsec). Datele transmise în timpul sesiunilor la distanță ar trebui criptate în timpul transferului. În cazul accesării datelor sensibile, ar trebui luată în considerare criptarea end-to-end (E2EE).
- Punerea în aplicare a regulilor de acces din PR.AA-03.3
    - Setările de monitorizare și criptare ar trebui să reflecte restricțiile de acces definite în PR.AA-03.3. De exemplu, alertele ar trebui să se declanșeze în cazul accesului în afara programului sau al încercărilor de accesare a sistemelor neautorizate. Toate accesările ar trebui verificate în raport cu aprobările documentate.
- Sprijinirea îmbunătățirii continue
    - Datele de monitorizare ar trebui utilizate pentru rafinarea politicilor de acces, identificarea lacunelor în punerea în aplicare și sprijinirea răspunsului la incidente. Standardele criptografice ar trebui revizuite periodic pentru asigurarea alinierii la cele mai bune practici actuale.
- Asigurarea fezabilității specifice OT
    - În mediile OT, monitorizarea și criptarea ar trebui implementate într-un mod care să respecte constrângerile sistemului și continuitatea operațională. Pentru centralizarea controlului și jurnalizării ar trebui utilizate servere jump sau gateway-uri securizate.

- Alinierea la recomandările ENISA
    - Aceste practici sunt în conformitate cu Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA, care recomandă accesul securizat la distanță, criptarea comunicațiilor și monitorizarea continuă ca parte a managementului eficace al riscului de securitate cibernetică pentru sistemele critice.

PR.AA-03.5

Securitatea conexiunilor cu sistemele externe trebuie verificată și reglementată prin acorduri documentate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate conexiunile cu sistemele externe sunt securizate prin controale de securitate verificate și sunt guvernate de acorduri documentate. Aceasta reduce riscul de acces neautorizat, scurgerea de date și compromiterea lanțului de aprovizionare.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Controlarea și documentarea tuturor interacțiunilor externe
    - Toate interacțiunile dintre sistemele interne și părțile externe (de exemplu, vânzătorilor, parteneri, servicii cloud) ar trebui identificate, controlate și documentate pentru asigurarea trasabilității și răspunderii.
- Verificarea controalelor de securitate ale părților externe
    - Înainte de stabilirea oricărei conexiuni, postura de securitate a părții externe ar trebui verificată prin evaluări, audituri, certificări (de exemplu, CyFun®) efectuate de părți terțe sau prin documentație tehnică, precum M154. Aceste documente ar trebui să descrie arhitectura de securitate, controalele de acces, criptarea și monitorizarea.
- Stabilirea acordurilor documentate
    - Acordurile formale (de exemplu, contracte, SLA-uri, acorduri de prelucrare a datelor - DPA) ar trebui să definească cerințele de securitate, rolurile și responsabilitățile, protocoalele de schimb de date, procedurile de răspuns la incidente și condițiile de reziliere.
- Specificarea cerințelor de control al accesului
    - Acordurile ar trebui să includă restricții tehnice, precum lista albă de adrese IP, RBAC, reguli de gestionare a datelor și cerințe de criptare pentru datele în tranzit și stocate.
- Monitorizarea și revizuirea conexiunilor externe
    - Toate conexiunile externe ar trebui monitorizate continuu pentru detecția anomaliilor sau încălcările politicilor. Acordurile și documentația tehnică (de exemplu, M154) ar trebui revizuite periodic și actualizate atunci când este necesar. Orice modificare a posturii de securitate a sistemului extern ar trebui să declanșeze o reevaluare.

- Asigurarea luării în considerare a aspectelor specifice OT
    - În mediile OT, accesul extern ar trebui să fie direcționat prin gateway-uri securizate sau servere jump. Accesul partajat (de exemplu, pentru PLC-urile gestionate de vânzători) ar trebui jurnalizat, limitat în timp și protejat prin autentificare puternică.
- Alinierea la recomandările ENISA
    - Aceste practici sunt în conformitate cu Ghidul tehnic de implementare privind măsurile de management al riscului de securitate cibernetică elaborat de către ENISA, care recomandă verificarea securității părților terțe, formalizarea responsabilităților prin contracte și monitorizarea continuă a dependențelor externe.

PR.AA-04

Afirmațiile de identitate sunt protejate, transmise și verificate.

PR.AA-04.1

Afirmațiile de identitate trebuie să fie protejate, transmise și verificate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că afirmațiile privind identitatea - afirmații despre identitatea unui utilizator, dispozitiv sau proces - sunt protejate împotriva falsificării, transmise în mod securizat și verificate în mod fiabil înainte de acordarea accesului la sisteme sau date critice.

Definiție: O afirmație de identitate este o declarație digitală utilizată în timpul autentificării care confirmă identitatea unui utilizator, dispozitiv sau proces. Aceasta include de obicei informații precum furnizorul de identitate (IdP), metoda de autentificare și perioada de valabilitate și este utilizată pentru a acorda acces la sisteme sau servicii.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Protejarea afirmațiilor de identitate
    - Afirmațiile de identitate ar trebui protejate împotriva falsificării, furtului sau utilizării abuzive. Ar trebui aplicate criptarea puternică (de exemplu, TLS 1.2 sau o versiune superioară) și semnăturile digitale. IdP ar trebui să respecte Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE, denumit în continuare Regulamentul eIDAS sau eIDAS (de exemplu, itsme®, Belgia, Sistema Pubblico di Identità Digitale - SPID, Italia, FranceConnect, Franța). Aceste practici sunt în conformitate cu recomandările ENISA privind identitatea digitală și serviciile de încredere.
- Transmiterea afirmațiilor de identitate în mod securizat
    - Datele de identitate ar trebui transmise utilizând protocoale securizate, precum limbajul de marcare pentru aserțiuni de securitate (SAML) 2.0 sau OpenID Connect. Ar trebui evitată expunerea token-urilor în URL-uri; ar trebui utilizate anteturile protocolului de transfer hipertext (HTTP) sau metodele POST. Pentru federația transfrontalieră a identităților, ar trebui utilizate noduri eIDAS pentru asigurarea interoperabilității securizate între statele membre ale UE.
- Verificarea afirmațiilor de identitate
    - Toate afirmațiile ar trebui validate înainte de acordarea accesului. Aceasta include verificarea semnăturilor digitale utilizând autorități de certificare de încredere enumerate în Lista de

încredere a UE (EUTL), verificarea revendicărilor token (emitent, public, expirare) și validarea în raport cu metadatele eIDAS. Prestatorii de servicii de încredere calificați (QTSP) ar trebui utilizați pentru emiterea și verificarea datelor de acces de identitate.

- Asigurarea fezabilității specifice OT
  - În mediile OT, afirmațiile de identitate ar trebui integrate în gateway-uri de acces securizate sau servere jump. În cazul în care integrarea directă nu este fezabilă, verificarea identității ar trebui să aibă loc la nivelul stratului de interfață, cu jurnalizare și monitorizare.
- Alinierea la recomandările ENISA
  - Aceste practici sunt susținute de Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA și de activitatea sa privind cadrele de identitate digitală securizată în conformitate cu Regulamentul eIDAS și Regulamentul (UE) 2024/1183 al Parlamentului European și al Consiliului din 11 aprilie 2024 de modificare a Regulamentului (UE) nr. 910/2014 în ceea ce privește instituirea cadrului european pentru identitatea digitală.

PR.AA-05

Permisiunile de acces, drepturile și autorizațiile sunt definite într-o politică, gestionate, puse în aplicare și revizuite și încorporează principiile privilegiului minim și ale separării atribuțiilor (SoD).

PR.AA-05.1

Permisiunile de acces, drepturile și autorizațiile trebuie definite, gestionate, puse în aplicare și revizuite.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că permisiunile de acces, drepturile și autorizațiile sunt clar definite, gestionate corespunzător, puse în aplicare în mod consecvent și revizuite periodic pentru protejarea sistemelor și datelor împotriva accesului neautorizat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea și managementul accesului
    - Listele de acces pentru sisteme (de exemplu, fișiere, servere, software, baze de date) ar trebui create și revizuite periodic.
    - Revizuirile ar trebui să fie susținute de instrumente precum analiza Active Directory (AD).
    - Procedurile de management al permisiunilor ar trebui documentate și actualizate atunci când este necesar.
- Revizuirea și revocarea accesului
    - Drepturile de acces logic și fizic ar trebui revizuite periodic și ori de câte ori rolurile se modifică sau persoanele fizice părăsesc organizația.
    - Privilegiile inutile ar trebui revocate imediat.
- Practici privind conturile de utilizator
    - Fiecare utilizator, inclusiv contractorii, ar trebui să aibă un cont separat pentru asigurarea răspunderii.
    - Acolo unde este fezabil din punct de vedere tehnic, ar trebui aplicate măsuri de autentificare adecvate.
    - Conturile pentru vizitatori ar trebui să fie limitate la privilegiile minime necesare (de exemplu, numai acces la internet).
    - SSO ar trebui utilizat acolo unde este cazul.

- Criterii de autorizare
    - Deciziile de autorizare ar trebui să ia în considerare caracteristici precum localizarea geografică, ora accesului și postura de securitate a dispozitivului solicitant.
- Considerații specifice OT
    - În medii în care conturile individuale nu sunt fezabile din punct de vedere tehnic - precum accesul partajat la PLC-uri sau HMI-uri, accesul ar trebui să fie limitat numai la funcțiile esențiale și pus în aplicare prin metode securizate, precum un server jump sau un frontend HMI care jurnalizează activitatea, restricționează accesul în funcție de rol sau timp și adaugă un nivel suplimentar de autentificare (de exemplu, cartelă sau PIN).
    - Metodele de autentificare ar trebui să fie aliniate la capabilitățile sistemelor OT.
    - Accesul la sistemele OT ar trebui jurnalizat și monitorizat, acolo unde este posibil.

PR.AA-05.2

Trebuie stabilit cine are nevoie de acces la informațiile și tehnologiile critice pentru activitatea organizației și prin ce mijloace obține acest acces.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a determina cine are nevoie de acces la informațiile și tehnologia critice pentru activitatea organizației și de a defini mijloacele securizate prin care acest acces este acordat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Determinarea și restricționarea accesului
  - Drepturile de acces ar trebui limitate doar la persoanele fizice care au nevoie de ele pentru a-și îndeplini rolurile.
  - Ar trebui luat în considerare un model de zero trust atât pentru mediile IT, cât și pentru cele OT, care să necesite verificarea înainte de acordarea accesului.
- Mijloace de acces
  - Metodele de acces ar trebui să includă mecanisme securizate, precum chei, parole, coduri sau privilegii administrative.
  - Aceste metode ar trebui gestionate și monitorizate pentru prevenirea utilizării abuzive.
- Sănătatea cibernetică a endpoint-urilor
  - Dispozitive precum laptopuri, smartphone-uri și tablete ar trebui să îndeplinească standardele de securitate înainte de a se conecta la rețeaua de producție.
  - Sănătatea endpoint-urilor ar trebui verificată prin:
    - Software antivirus actualizat.
    - Absența malware-ului.
    - Instalarea celor mai recente patch-uri de securitate.
  - Numai dispozitivele conforme ar trebui să aibă acces la sistemele și datele critice.
- Considerații specifice OT
  - În mediile OT, accesul la sistemele de control ar trebui limitat la personalul esențial.
  - Metodele de acces securizate (de exemplu, servere jump, restricții bazate pe roluri) ar trebui utilizate în cazul în care conturile individuale nu sunt fezabile.

- Referință
    - Pentru instrumente și șabloane practice, consultați șablonul de Politică de acces din Setul de instrumente CyFun® pe www.cyfun.eu.

PR.AA-05.3

Drepturile de acces, privilegiile și autorizațiile trebuie restricționate la sistemele și informațiile specifice necesare pentru îndeplinirea sarcinilor (principiul privilegiului minim).

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura restricționarea drepturilor de acces, privilegiilor și autorizațiilor numai la sistemele și informațiile specifice necesare pentru îndeplinirea sarcinilor atribuite, respectând principiul privilegiului minim.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aplicarea principiului privilegiului minim
  - Drepturile de acces ar trebui limitate la minimul necesar pentru utilizatori, sisteme și servicii.
  - Conturile ar trebui să înceapă cu privilegii reduse și să fie ridicate doar atunci când este justificat.
  - Accesul JIT ar trebui utilizat pentru limitarea duratei privilegiilor ridicate.
- Definirea și gestionarea permisiunilor
  - Drepturile de acces ar trebui definite clar în funcție de roluri și responsabilități.
  - Un inventar al conturilor și permisiunilor asociate ar trebui menținut și actualizat.
  - Ar trebui utilizate conturi separate pentru contractori și părți terțe, pentru asigurarea trasabilității.
- Punerea în aplicare a controalelor de acces
  - Modelele de control al accesului bazate pe roluri sau atribute ar trebui implementate acolo unde este fezabil.
  - Punctele de acces la internet și conexiunile externe ar trebui limitate la strictul necesar.
- Întărirea sistemelor
  - Sistemele ar trebui întărite pentru a sprijini controlul accesului prin:
    - Dezactivarea porturilor și serviciilor neutilizate.
    - Restricționarea Bluetooth-ului acolo unde nu este necesar.
    - Limitarea protocoalelor vechi, precum protocol de transfer de fișiere (FTP), cu excepția cazului în care sunt configurate în mod securizat.

- Revizuirea şi adaptarea accesului
    - Drepturile de acces ar trebui revizuite periodic şi ajustate în funcție de modificările de rol, finalizarea proiectelor sau evaluările de securitate.
    - Accesul ar trebui revocat imediat când nu mai este necesar.
- Considerații specifice OT
    - În mediile OT, controlul accesului ar trebui să respecte în continuare principiul privilegiului minim. În cazul în care există limitări tehnice, ar trebui aplicate măsurile de control al accesului OT definite anterior (a se vedea PR.AA-01.1 şi PR.AA-05.1) pentru a asigura un acces securizat şi trasabil.

PR.AA-05.4

Nimeni nu trebuie să aibă privilegii administrative pentru sarcinile de rutină, zilnice.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a preveni utilizarea privilegiilor administrative pentru sarcinile de rutină, zilnice, reducând astfel riscul de utilizare abuzivă sau exploatare de către atacatori.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Separarea conturilor și gestionarea privilegiilor.
    - Conturile administrative și cele ale utilizatorilor obișnuiți ar trebui separate strict.
    - Conturile dedicate de administrator ar trebui utilizate numai pentru gestionarea sistemului și sarcinile administrative.
    - Conturile utilizatorilor nu ar trebui să aibă privilegii administrative.
- Restricții de acces și măsuri de securitate.
    - Ar trebui create parole locale unice de administrator pentru fiecare sistem.
    - Conturile neutilizate ar trebui dezactivate imediat.
    - Navigarea pe internet de pe conturile administrative ar trebui interzisă pentru a reduce expunerea la amenințări din mediul web.
- Considerații specifice OT
    - În mediile OT, accesul administrativ ar trebui limitat la personalul și funcțiile esențiale.
    - În cazul în care este necesar accesul partajat, ar trebui utilizate metode de acces securizat (de exemplu, servere jump, jurnalizarea sesiunilor) pentru asigurarea răspunderii și reducerea riscului.

PR.AA-05.5

Acolo unde este fezabil din punct de vedere tehnic, operațional și economic - fără a compromite integritatea, siguranța sau conformitatea sistemului - trebuie implementate mecanisme automatizate pentru gestionarea conturilor de utilizator pe sistemele critice TIC și OT. Fezabilitatea trebuie determinată pe baza capabilităților sistemului, potențialului de integrare, evaluării riscurilor și impactului asupra activității.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că conturile utilizatorilor pe sistemele critice TIC și OT sunt gestionate în mod securizat, eficient și consecvent prin mecanisme automatizate - acolo unde este fezabil din punct de vedere tehnic, operațional și economic - fără a compromite integritatea, siguranța sau conformitatea sistemului.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Evaluarea fezabilității automatizării
    - Fezabilitatea ar trebui să fie bazată pe capabilitățile sistemului, potențialul de integrare, evaluarea riscurilor și impactul asupra activității.
        - Pentru sistemele TIC, fezabilitatea depinde de disponibilitatea instrumentelor de automatizare, API-urilor sau opțiunilor de integrare și de absența unor obstacole tehnice sau financiare majore.
        - Pentru sistemele OT, fezabilitatea depinde de vechimea sistemului, de limitările vânzătorului, de cerințele de siguranță și de riscul de întrerupere a operațiunilor critice.
        - Fezabilitatea generală ar trebui să ia în considerare capabilitatea tehnică, siguranța operațională, rentabilitatea și conformitatea cu standardele de securitate și de reglementare.
- Automatizarea gestionării ciclului de viață al conturilor
    - Mecanismele automate ar trebui să gestioneze crearea, modificarea și ștergerea conturilor pe baza unor reguli predefinite. Aceasta asigură că numai utilizatorii autorizați au acces și că conturile sunt șterse imediat când nu mai sunt necesare.
- Dezactivarea conturilor inactive sau neautorizate
    - Conturile ar trebui dezactivate automat atunci când utilizatorii părăsesc organizația sau nu mai au nevoie de acces. Aceasta reduce riscul accesului neautorizat la sisteme critice.

- Monitorizarea și raportarea activității conturilor
  - Instrumentele automate ar trebui să monitorizeze continuu utilizarea contului și să genereze rapoarte pentru a detecta activități neobișnuite sau neautorizate. Ar trebui să fie declanșate alerte în cazul unor comportamente suspecte.
- Trimiterea de notificări pentru evenimente cheie
  - Notificările automate ar trebui să informeze administratorii cu privire la evenimente importante, precum crearea, modificarea sau ștergerea conturilor, permițând supravegherea în timp util.
- Menținerea pistelor de audit pentru conformitate
  - Toate activitățile legate de conturi ar trebui jurnalizate automat pentru a sprijini conformitatea cu politicile interne și reglementările externe.
- Asigurarea fezabilității specifice OT
  - În mediile OT, automatizarea ar trebui implementată doar în cazul în care nu compromite siguranța sau continuitatea operațională. În cazul în care automatizarea directă nu este fezabilă, managementul conturilor ar trebui realizat prin intermediul unor straturi de interfață securizate sau servere jump.
- Alinierea la recomandările ENISA
  - Aceste practici sunt susținute de Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA și de activitatea sa privind managementul accesului securizat în mediile de infrastructură critică.

PR.AA-05.6

SoD trebuie asigurată în managementul drepturilor de acces.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că nicio persoană fizică nu deține control deplin asupra sistemelor sau proceselor critice, prin aplicarea SoD. Aceasta ar trebui să reducă riscul de erori, fraudă și utilizarea abuzivă a drepturilor de acces.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea separării atribuțiilor
  - Responsabilitățile ar trebui împărțite astfel încât sarcinile cheie să fie îndeplinite de persoane fizice diferite.
  - SoD ar trebui să includă:
    - Rolurile operaționale și de asistență pentru sisteme ar trebui atribuite unor persoane fizice diferite.
    - Sarcinile de asistență sistemică ar trebui să necesite supraveghere sau control dublu.
  - O singură persoană nu ar trebui să inițieze și să aprobe aceeași tranzacție.
  - Funcțiile de control al accesului și de audit ar trebui gestionate de roluri separate.
- Gestionarea drepturilor de acces în mod adecvat
  - RBAC ar trebui utilizat pentru atribuirea permisiunilor în funcție de rolurile profesionale.
  - Principiul privilegiului minim ar trebui aplicat pentru limitarea accesului la ceea ce este strict necesar.
  - Drepturile de acces ar trebui revizuite periodic, în special pentru sistemele critice și rolurile cu risc ridicat.
  - Acolo unde este fezabil, pentru funcțiile administrative și de audit ar trebui utilizate instrumente sau conturi separate.
- Aplicarea controalelor pentru administratorii de sistem
  - Responsabilitățile administrative ar trebui împărțite pentru împiedicarea controlului total de către o singură persoană fizică.
  - Administratorii ar trebui să utilizeze conturi separate pentru sarcinile obișnuite și cele privilegiate.
  - Toate acțiunile administrative ar trebui jurnalizate și revizuite de o parte independentă.

- Administratorii care gestionează accesul nu ar trebui să fie responsabili pentru auditarea acestui acces.

- Asigurarea fezabilității în mediile OT
  - În sistemele OT, SoD ar trebui adaptată la constrângerile operaționale și de siguranță.
  - În cazul în care separarea completă nu este fezabilă, ar trebui implementate controale compensatorii, precum aprobarea dublă, jurnalizarea și revizuirea externă.

- Alinierea la recomandările ENISA
  - Aceste practici sunt aliniate cu Măsurile de securitate pentru operatorii de servicii esențiale (Reference document on security measures for Operators of Essential Services CG Publication 01/2018) elaborate de către ENISA, care subliniază importanța SoD și a RBAC în reducerea riscurilor legate de acces în mediile TIC și OT.

PR.AA-05.7

Utilizatorii cu drepturi privilegiate trebuie gestionați și monitorizați.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul de acces neautorizat, încălcări ale securității datelor și întreruperi operaționale, asigurându-se că utilizatorii cu drepturi privilegiate, care au acces ridicat la sisteme critice, sunt supuși unei gestionări stricte și unei supravegheri continue.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Monitorizarea activităților privilegiate
    - Activitățile utilizatorilor cu drepturi privilegiate ar trebui jurnalizate și revizuite periodic sau continuu, chiar dacă sunt efectuate de persoane fizice care nu sunt independente de proces.
- Protejarea datelor sensibile
    - Monitorizarea ar trebui să contribuie la prevenirea expunerii sau utilizării abuzive a informațiilor sensibile și a configurațiilor de sistem de către utilizatorii cu drepturi privilegiate.
- Prevenirea abuzului de privilegii
    - Conturile privilegiate ar trebui gestionate astfel încât să fie evitate modificările neautorizate, escaladarea privilegiilor sau ocolirea controalelor de securitate.
- Detecția comportamentului suspect
    - Anomaliile comportamentale și acțiunile neautorizate ar trebui identificate prin mecanisme automate de jurnalizare și alertare.
- Sprijinirea răspunsului la incidente
    - Datele de monitorizare ar trebui utilizate pentru a investiga și a răspunde la incidentele de securitate care implică conturi privilegiate.
- Gestionarea proactivă a drepturilor de acces
    - Drepturile de acces ar trebui definite clar, revizuite periodic și ajustate în funcție de modificările de roluri, necesitățile operaționale sau evaluările riscurilor.

- Asigurarea fezabilității specifice OT
    - În mediile OT, accesul privilegiat ar trebui gestionat ținând cont de stabilitatea și siguranța sistemului. În cazul în care monitorizarea completă nu este fezabilă, ar trebui implementate controale compensatorii, precum jurnalizarea la nivel de interfață[1] sau revizuirea externă.
- Alinierea la recomandările ENISA
    - Aceste practici sunt aliniate cu Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA, care subliniază importanța controlului și monitorizării accesului privilegiat în securizarea serviciilor esențiale și a infrastructurilor critice.

[1] Jurnalizarea la nivel de interfață înseamnă înregistrarea acțiunilor utilizatorilor în momentul în care se conectează la un sistem, de exemplu prin intermediul unui instrument de acces la distanță, al unui server jump sau al unui gateway securizat, fără a fi necesară jurnalizarea directă în interiorul sistemului (de exemplu, utilizând Splunk®). Aceasta contribuie la monitorizarea activităților privilegiate în medii în care jurnalizarea directă în sistem nu este posibilă, precum în sistemele OT.

PR.AA-05.8

Restricțiile de utilizare a conturilor pentru anumite perioade de timp și locații trebuie luate în considerare în politica de securitate a accesului organizației și aplicate în consecință.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul accesului neautorizat, asigurând că utilizarea contului este restricționată în funcție de timp, locație, dispozitiv și contextul utilizatorului. Aceste restricții ar trebui definite în politica de securitate a accesului organizației și aplicate în mod consecvent în mediile TIC și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aplicarea restricțiilor bazate pe timp
    - Accesul la sisteme ar trebui limitat la programul de lucru stabilit, pentru a reduce expunerea în afara programului.
    - Durata de utilizare a anumitor conturi ar trebui limitată pentru a preveni sesiunile excesive sau nesupravegheate.
- Aplicarea restricțiilor bazate pe locație
    - Geofencing ar trebui utilizat pentru a permite accesul numai din locații geografice de încredere.
    - Filtrarea adreselor IP ar trebui să restricționeze accesul la intervale de rețea cunoscute și aprobate.
- Aplicarea restricțiilor bazate pe dispozitiv
    - Accesul ar trebui permis numai de pe dispozitive gestionate care respectă politicile de securitate ale organizației.
    - Dispozitivele negestionate ar trebui restricționate sau ar trebui acordat acces limitat (de exemplu, acces numai pentru citire sau fără acces la date sensibile).
- Aplicarea restricțiilor bazate pe utilizator
    - RBAC ar trebui să asigure că utilizatorii accesează numai sistemele și datele relevante pentru activitatea lor.
    - Politicile de acces condiționat ar trebui să impună verificări suplimentare (de exemplu, MFA) în scenarii cu risc ridicat.
    - Evaluare continuă și adaptivă a riscului și încrederii (CARTA) ar trebui luată în considerare pentru evaluarea în mod dinamic a încrederii utilizatorilor și a dispozitivelor. Această abordare

este aliniată cu principiul zero trust, care presupune că nu există încredere implicită pentru niciun utilizator sau dispozitiv, chiar și în interiorul rețelei.

- Asigurarea fezabilității specifice OT
  - În mediile OT, restricțiile ar trebui adaptate la cerințele operaționale și de siguranță. În cazul în care există limitări tehnice, ar trebui implementate controale compensatorii, precum restricții de acces fizic sau servere jump monitorizate.
- Alinierea la recomandările ENISA
  - Aceste practici sunt aliniate cu Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA, care susține controlul contextual al accesului ca parte a managementului eficace al riscului de securitate cibernetică.

PR.AA-05.9

Utilizatorii cu drepturi privilegiate trebuie gestionați, monitorizați și auditați.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că conturile de utilizator cu drepturi privilegiate, cele cu acces ridicat la sisteme critice, sunt strict controlate, monitorizate continuu și auditate independent. Aceasta ar trebui să reducă riscul de utilizare abuzivă, să asigure răspunderea și să protejeze mediile critice IT, OT și IoT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Punerea în aplicare a unui management strict al accesului privilegiat
    - Conturile privilegiate ar trebui să aibă roluri clar definite, domenii de acces limitate și să fie supuse unor revizuiri periodice ale accesului.
- Implementarea monitorizării continue
    - Toate activitățile utilizatorilor cu drepturi privilegiate ar trebui jurnalizate și monitorizate continuu, utilizând instrumente automatizate acolo unde este posibil, pentru a sprijini trasabilitatea și răspunsul la incidente.
- Efectuarea de audituri independente
    - Auditurile ar trebui efectuate periodic de către persoane fizice independente de procesul de management al accesului.
    - Auditurile ar trebui să:
        - Verifice dacă accesul privilegiat este acordat în conformitate cu politica.
        - Confirme că mecanismele de monitorizare și jurnalizare funcționează corect.
        - Identifice utilizarea abuzivă, încălcările politicilor sau abaterile.
        - Producă rezultate documentate, precum rapoarte de audit sau planuri de acțiuni corective.
- Aplicarea principiului celor patru ochi
    - Nicio persoană fizică nu ar trebui să poată acorda, modifica sau revoca accesul privilegiat fără supravegherea sau aprobarea unei alte persoane autorizate.
- Diferențierea între monitorizare și audit
    - Monitorizarea zilnică a conformității ar trebui să se concentreze pe aspecte operaționale (de exemplu, alerte, anomalii).

- Auditurile periodice ar trebui să evalueze eficacitatea și integritatea generală a procesului de management al accesului privilegiat.

- Asigurarea fezabilității specifice OT
  - În mediile OT, controalele accesului privilegiat ar trebui adaptate la constrângerile operaționale și de siguranță. În cazul în care auditul complet nu este fezabil, ar trebui implementate controale compensatorii, precum jurnalizarea la nivel de interfață sau revizuirea externă.

- Alinierea la recomandările ENISA
  - Aceste practici ar trebui să fie aliniate cu Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA, care subliniază importanța controlului accesului privilegiat, a monitorizării și a auditului în securizarea serviciilor esențiale și a infrastructurii critice.

PR.AA-06

Accesul fizic la activele organizației este gestionat, monitorizat și pus în aplicare în mod proporțional cu riscul.

PR.AA-06.1

Accesul fizic la toate activele organizației, inclusiv zonele critice, trebuie gestionat, monitorizat și implementat în funcție de risc.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura gestionarea, monitorizarea și punerea în aplicare în funcție de riscuri a accesului fizic la toate activele organizației, în special în zonele critice, pentru a preveni intrarea neautorizată și a proteja sistemele sensibile.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Măsuri de control al accesului
  - Cheile, cartelele și codurile de alarmă ar trebui gestionate cu strictețe.
  - Datele de acces ale angajaților ar trebui colectate imediat după plecare.
  - Codurile de alarmă ar trebui modificate periodic.
  - Furnizorii externi de servicii (de exemplu, personalul de curățenie) ar trebui să aibă acces numai atunci când este necesar, iar acest acces ar trebui să fie:
    - limitat în timp, utilizând controale tehnice.
    - jurnalizat electronic pentru trasabilitate.
- Îmbunătățirea securității fizice
  - Zonele critice ar trebui protejate cu măsuri de control fizice, precum:
    - Camere de supraveghere.
    - Agenți de securitate.
    - Uși și porți încuiate.
    - Sisteme de alarmă.
  - Aceste măsuri de control ar trebui amplasate strategic pentru monitorizarea și restricționarea accesului.
- Protecția accesului la rețea
  - Porturile de rețea interne (de exemplu, Ethernet) nu ar trebui expuse în zone nesecurizate, precum săli de așteptare, coridoare sau zone de recepție.

- Considerații specifice OT
  - Accesul fizic la mediile OT (de exemplu, camere de control, dulapuri, dispozitive de teren) ar trebui limitat doar la personalul autorizat.
  - Accesul ar trebui jurnalizat și monitorizat, iar atunci când este fezabil, ar trebui utilizate bariere fizice.
- Referință
  - Pentru instrumente și șabloane practice, consultați Politica de acces din Setul de instrumente CyFun® pe www.cyfun.eu.

PR.AA-06.2

Controalele accesului fizic trebuie să includă proceduri specifice pentru situații de urgență, asigurând protecția continuă a activelor critice și non-critice în timpul unor astfel de evenimente.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că controalele accesului fizic rămân eficace și adaptabile în situații de urgență. Aceasta include menținerea securității activelor critice și non-critice, permițând în același timp accesul sigur, autorizat și trasabil pentru acțiuni de răspuns la urgențe, recuperare sau izolare - în special în medii în care siguranța fizică și operațională sunt strâns legate, precum sistemele OT și IoT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea unor scenarii de urgență
    - Procedurile de urgență ar trebui să acopere o serie de evenimente, printre care:
        - Incidente de mediu și de siguranță (de exemplu, incendii, inundații, urgențe medicale, evacuări).
        - Defecțiuni ale infrastructurii (de exemplu, întreruperi de curent, defecțiuni ale sistemului).
        - Incidente de securitate (de exemplu, intruziuni, defecțiuni ale sistemului de control al accesului).
        - Evenimente de securitate cibernetică (de exemplu, ransomware, încălcări ale securității datelor, amenințări din interior).
- Menținerea procedurilor de acces în caz de urgență
    - Accesul de urgență ar trebui să fie:
        - Jurnalizat
            → Înregistrarea a cine a accesat ce, când și de ce.
        - Monitorizat
            → Utilizarea sistemelor de supraveghere sau de control al accesului pentru urmărirea activității.
        - Revizuit
            → Efectuarea revizuirilor după eveniment pentru verificarea utilizării corespunzătoare și detecția utilizării necorespunzătoare.

- Sprijinirea pregătirii pentru situații de urgență cu controale fizice
  - Ar trebui menținute liste actualizate cu persoanele fizice care sunt autorizate cu drepturi de acces în situații de urgență.
  - Ar trebui utilizate documente de identitate (de exemplu, cartele de acces) și ar trebui definite zone de securitate.
  - Cerințe de escortă ar trebui aplicate vizitatorilor sau personalului temporar.
  - Ar trebui implementate bariere fizice, precum garduri, încuietori, turnicheți și puncte de control cu personal.
  - Sistemele de supraveghere ar trebui utilizate pentru monitorizarea punctelor de intrare și ieșire.
- Aplicarea de măsuri de siguranță suplimentare
  - Ar trebui luate în considerare sisteme de cartele cu niveluri de acces diferențiate pentru diverse zone.
  - Accesul fizic la servere și componente de rețea ar trebui restricționat numai la personalul autorizat.
  - Toate accesările la infrastructura critică ar trebui jurnalizate și revizuite periodic.
  - Menținerea și revizuirea - Înregistrările privind accesul vizitatorilor ar trebui menținute și revizuite. Dacă este necesar, ar trebui luate măsuri corective.
- Asigurarea fezabilității specifice OT
  - În mediile OT, procedurile de acces fizic ar trebui adaptate pentru evitarea perturbării siguranței sau a continuității operaționale. Accesul de urgență ar trebui proiectat astfel încât să permită atât o reacție rapidă, cât și protecția activelor.
- Alinierea la recomandările ENISA
  - Aceste practici sunt aliniate la Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA, care subliniază importanța controalelor de acces fizic și logic în menținerea rezilienței în situații de urgență.

PR.AA-06.3

Zonele critice trebuie să dispună de controale fizice suplimentare ale accesului, pe lângă cele aplicate incintelor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul accesului fizic neautorizat în zonele esențiale pentru continuitatea operațională, integritatea datelor și siguranța personalului și a echipamentelor, prin aplicarea unor măsuri de acces mai stricte decât cele utilizate în zonele generale ale incintelor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Zonele critice ar trebui identificate în timpul clasificării activelor. Acestea includ, de obicei:
  - Medii de producție și OT.
  - Săli de servere și centre de date.
  - Birourile financiare și de resurse umane.
  - Săli de control.
  - Locații în care sunt stocate informații sensibile sau clasificate.
- Ar trebui luate în considerare următoarele controale fizice îmbunătățite ale accesului:
  - Autentificarea cu doi factori (de exemplu, cartelă + date biometrice).
  - Supravegherea continuă (de exemplu, rețea video cu circuit închis - CCTV, senzori de mișcare).
  - Jurnalizarea accesului cu revizuire periodică.
  - Personal de securitate la fața locului sau de patrulare.
  - Sisteme de alarmă cu alerte în timp real.
  - Proceduri de gestionare a vizitatorilor:
    - Aprobare prealabilă și însoțire.
    - Acces limitat în timp.
    - Jurnale de vizitatori.
- Asigurarea coerenței cu politicile mai ample privind accesul fizic, inclusiv:
  - PR.AA-06.1 - Controlul accesului bazat pe risc.

- PR.AA-06.2 - Proceduri de acces în caz de urgență.
- PR.AA-06.4 - Protecția fizică a activelor.

- Adaptarea controalelor la criticitatea fiecărei zone și integrarea acestora în strategia generală de securitate fizică.

PR.AA-06.4

Activele situate în zone critice trebuie protejate fizic împotriva accesului neautorizat, deteriorării sau interferențelor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a proteja activele esențiale situate în zone critice împotriva accesului neautorizat, deteriorării sau interferențelor, intenționate sau accidentale, prin aplicarea unor măsuri de protecție fizică adaptate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Activele din zonele critice ar trebui protejate fizic în funcție de criticitatea și profilul lor de risc. Aceste active ar putea include:
  - Servere și sisteme de control.
  - Infrastructura electrică și cablarea.
  - Depozite de date sensibile.
  - Componente OT.
- Măsurile de protecție ar trebui să includă:
  - Bariere fizice și izolare:
    - Carcase încuiate, dulapuri securizate sau cuști pentru echipamente sensibile.
    - Sigilii inviolabile pentru detecția accesului neautorizat.
    - Măsuri de protecție a mediului (de exemplu, stingerea incendiilor, controlul temperaturii).
  - Protecția infrastructurii:
    - Securizarea cablurilor de alimentare și de rețea, a interfețelor de acces și a echipamentelor.
    - Sisteme de alimentare redundante și separate fizic pentru operațiuni critice.
  - Controlul accesului și supravegherea:
    - Însoțirea vizitatorilor, vânzătorilor și părților terțe în orice moment.
    - Menținerea și revizuirea periodică a jurnalelor de acces.
- Controalele ar trebui să fie aliniate cu cerințele aferente, inclusiv:
  - PR.AA-06.1 - Controlul accesului bazat pe risc.

- PR.AA-06.2 - Proceduri de acces în caz de urgență.
- PR.AA-06.3 - Controale de acces îmbunătățite pentru zonele critice.

- Protecția ar trebui să fie proactivă, inițiată în timpul clasificării activelor și proiectării incintelor și integrată în strategia mai amplă de securitate fizică.

[PR.AT] CONȘTIENTIZARE ȘI INSTRUIRE

Personalul organizației beneficiază de conștientizare și instruire în domeniul securității cibernetice, astfel încât să își poată îndeplini sarcinile legate de securitatea cibernetică.

PR.AT-01

Personalul beneficiază de activități de conștientizare și instruire, astfel încât să dețină cunoștințele și abilitățile necesare pentru îndeplinirea sarcinilor generale, ținând cont de riscurile de securitate cibernetică.

PR.AT-01.1

Organizația trebuie să stabilească și să mențină un program de conștientizare și instruire în domeniul securității cibernetice pentru a se asigura că tot personalul înțelege cum să își îndeplinească sarcinile în mod securizat și responsabil.

GHID DE IMPLEMENTARE

Obiectivul Controlului PR.AT-01.1 este de a asigura că toți membrii organizației înțeleg cum să lucreze în mod securizat, prin furnizarea de instruire periodică, clară și practică în domeniul securității cibernetice, care reduce riscul uman și susține un comportament sigur atât în mediile IT, cât și în cele OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Instruirea de bază ar trebui furnizată tuturor
    - Instruirea pentru conștientizarea în domeniul securității cibernetice ar trebui asigurată tuturor angajaților, contractorilor, partenerilor și furnizorilor, inclusiv celor din mediile OT.
- Instruirea ar trebui să acopere amenințările comune
    - Tematici precum phishing-ul, parolele slabe, ingineria socială și riscurile specifice OT (de exemplu, utilizarea necorespunzătoare a USB-urilor, amenințări legate de accesul la distanță) ar trebui incluse.
- Instruirea ar trebui să înceapă devreme și să fie repetată periodic
    - Instruirea ar trebui furnizată în timpul procesului de integrare organizațională și reînnoită cel puțin anual. Actualizările și memento-urile continue ar trebui să consolideze mesajele cheie.
- Ar trebui utilizate canale multiple
    - Conștientizarea ar trebui sporită prin sesiuni structurate, campanii, afișe, buletine informative și instrumente interactive.

- Consecințele neconformității ar trebui explicate
    - Impactul încălcării politicilor de securitate cibernetică ar trebui comunicat în mod clar, atât persoanelor fizice, cât și organizației.
- Instruirea ar trebui să fie aliniată cu politicile și bunele practici
    - Conținutul ar trebui să reflecte politicile interne de securitate cibernetică, comportamentele așteptate și măsurile de protecție. Cadrele recunoscute, precum AR-in-a-Box elaborat de către ENISA, ar trebui să ghideze proiectarea programului.
- Riscurile specifice OT ar trebui abordate
    - Instruirea ar trebui adaptată pentru a include responsabilitățile și riscurile specifice cu care se confruntă personalul care lucrează cu ICS și alte active OT.
- Conținutul ar trebui actualizat în permanență
    - Materialele de instruire ar trebui revizuite și actualizate periodic pentru a reflecta noile amenințări și lecțiile învățate din incidente.

PR.AT-01.2

Organizația trebuie să includă în instruirea sa pentru securitatea cibernetică, conștientizarea și raportarea amenințărilor din interior, pentru a ajuta personalul să recunoască și să răspundă la potențialele riscuri interne.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că tot personalul este instruit să recunoască și să raporteze potențialele amenințări interne, reducând astfel riscul incidentelor interne de securitate cibernetică. Acest Control se bazează pe conștientizarea generală din PR.AT-01.1, introducând scenarii specifice de amenințare și acțiuni de răspuns.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Instruirea ar trebui să includă modul de recunoaștere a semnelor comportamentale ale amenințărilor din interior, precum tiparele de acces neobișnuite, acumularea de date sau modificări bruște de comportament.
- Organizația ar trebui să definească în mod clar amenințările din interior (de exemplu, persoane din interior rău intenționate, neglijente sau compromise, inclusiv angajați și contractori).
- Personalul ar trebui instruit cu privire la modul și locul în care trebuie raportate activitățile suspecte și referitor la importanța raportării în timp util.
- Ar trebui utilizate studii de caz reale sau simulări pentru demonstrarea impactului amenințărilor din interior și pentru consolidarea procesului de învățare.
- Conștientizarea amenințărilor din interior ar trebui să facă parte din instruirea periodică de securitate și din procesul de integrare organizațională a întregului personal.
- Personalul care are acces la date sau sisteme sensibile ar trebui să beneficieze de instruire specializată, axată pe responsabilitățile specifice ale acestora.
- Ar trebui dezvoltate echipe de instruire interfuncționale, cu expertiză atât în domeniul securității IT, cât și în domeniul operațional OT (instruire încrucișată).
- Instruirea anuală de perfecționare ar trebui utilizată pentru a consolida mesajele cheie și a introduce actualizări.
- Organizația ar trebui să promoveze o cultură a securității în care angajații se simt în siguranță să raporteze problemele fără teama de represalii.

PR.AT-01.3

Personalul trebuie să primească instruire pentru a-și înțelege rolurile, responsabilitățile și prioritățile specifice în timpul unui incident de securitate cibernetică sau a informației, inclusiv pașii pe care trebuie să îi urmeze pentru a răspunde în mod eficace.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că întreg personalul își înțelege rolurile, responsabilitățile și prioritățile specifice pe care le are în timpul unui incident de securitate cibernetică sau a informației, permițându-le să răspundă în mod eficace și în coordonare cu planurile de răspuns la incidente și de urgență ale organizației. Acest Control se bazează pe conștientizarea specifică a amenințărilor din PR.AT-01.2, introducând instruirea bazată pe roluri și pregătirea pentru răspunsul la incidente.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Instruirea ar trebui adaptată diferitelor roluri (de exemplu, IT, resurse umane, cadre de conducere), astfel încât fiecare grup să își înțeleagă responsabilitățile sale specifice în cazul unui incident.
- Personalul ar trebui să fie familiarizat cu obiectivele sale, prioritățile de recuperare și ordinea corectă a acțiunilor care ar trebui întreprinse în timpul unui incident.
- Exercițiile teoretice sau simulările ar trebui utilizate pentru a exersa răspunsul la incidente într-un mediu realist, dar controlat.
- Ar trebui furnizată o documentație clară care să prezinte sarcinile și responsabilitățile fiecărui rol în timpul unui incident.
- Instruirea ar trebui să explice modul în care răspunsul la incidente se leagă de planificarea de urgență, asigurând că personalul înțelege când și cum să activeze măsurile de urgență (a se vedea și ID.IM-04.1).
- Ar trebui organizate sesiuni periodice de perfecționare pentru menținerea cunoștințelor actualizate și consolidarea pregătirii.

PR.AT-01.4

Organizația trebuie să evalueze dacă instruirea sa pentru conștientizare în domeniul securității cibernetice este eficace în îmbunătățirea cunoștințelor, comportamentului și pregătirii în cadrul organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că instruirea pentru conștientizare în domeniul securității cibernetice conduce la îmbunătățiri măsurabile în ceea ce privește cunoștințele personalului, comportamentul securizat și pregătirea pentru a răspunde la amenințările cibernetice la toate nivelurile organizației. Acest Control se bazează pe conștientizarea specifică amenințărilor din PR.AT-01.2 și pe instruirea bazată pe roluri din PR.AT-01.3, prin introducerea unei abordări structurate pentru măsurarea impactului eforturilor de conștientizare.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Organizația ar trebui să evalueze dacă instruirea pentru conștientizare este accesibilă întregului personal relevant și dacă influențează în mod eficace comportamentul, conștientizarea și atitudinile acestuia în materie de securitate cibernetică.
- Dacă organizația nu are experiență în evaluare, ar trebui să ia în considerare utilizarea cadrelor sau instrumentelor evaluate existente, precum AR-in-a-Box elaborat de către ENISA, care include îndrumări privind stabilirea obiectivelor, selectarea KPI-urilor și măsurarea impactului.
- În cazul elaborării unei metode de evaluare la nivel intern, organizația ar trebui să analizeze bunele practici și abordările bazate pe dovezi pentru evaluarea programelor de conștientizare.
- Metodele de evaluare ar trebui să includă o combinație de:
    - Evaluări sau teste înainte și după instruire.
    - Teste simulate de phishing sau inginerie socială.
    - Sondaje pentru măsurarea modificărilor în materie de conștientizare, încredere și comportament.
    - Observații de la participanți și instructori.
- Organizația ar trebui să documenteze lecțiile învățate și să utilizeze rezultatele pentru îmbunătățirea eforturilor viitoare de instruire.

PR.AT-02

Persoanele fizice care ocupă funcții specializate beneficiază de conștientizare și instruire, astfel încât să dețină cunoștințele și competențele necesare pentru îndeplinirea sarcinilor relevante, ținând seama de riscurile de securitate cibernetică.

PR.AT-02.1

Membrii organelor de conducere trebuie să poată demonstra că au urmat cursuri de instruire care le-au permis să dobândească cunoștințe solide în domeniul securității cibernetice sau a informației, precum și al managementului riscului, astfel încât să poată evalua riscurile de securitatea cibernetică sau a informației și consecințele acestora și să propună măsurile necesare de atenuare a riscurilor, ținând seama de rolurile, responsabilitățile și atribuțiile lor de autoritate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că membrii organelor de conducere sunt pregătiți să ia decizii informate cu privire la riscurile de securitate cibernetică și strategiile de atenuare a acestora, dezvoltând o înțelegere fundamentală a securității informației, a amenințărilor cibernetice și a principiilor de management al riscului relevante pentru rolurile lor de conducere.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Instruirea profesională ar trebui să furnizeze conducerii capacitatea de a evalua riscurile de securitate cibernetică, de a înțelege impactul potențial al acestora și de a propune măsuri de atenuare adecvate, în concordanță cu responsabilitățile și autoritatea lor.
- Conținutul instruirii ar trebui să ia în considerare:
  - Conceptele de bază ale securității cibernetice sau a informației;
  - Identificarea, evaluarea și atenuarea riscurilor;
  - Luarea deciziilor strategice în contextul amenințărilor cibernetice;
  - Recunoașterea potențialelor lacune de securitate și a responsabilităților de guvernanță.
- Instruirea ar trebui să fie adaptată rolurilor de conducere, utilizând recomandările ENISA privind profilurile de rol, inclusiv titlurile, misiunile, sarcinile, abilitățile și competențele (a se vedea profilurile de rol prevăzute în ECSF).
- Ar trebui luate în considerare sesiuni anuale de perfecționare pentru consolidarea practicilor existente și introducerea noilor evoluții în domeniul securității cibernetice și al managementului riscului.

PR.AT-02.2

Persoanelor fizice care ocupă funcții specializate trebuie să le fie furnizate conștientizare și instruire înainte de acordarea privilegiilor, astfel încât să dețină cunoștințele și competențele necesare pentru îndeplinirea sarcinilor relevante, ținând seama de riscurile de securitate cibernetică.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că persoanele fizice care ocupă funcții specializate beneficiază de conștientizare și instruire în domeniul securității cibernetice înainte de a primi acces privilegiat, permițându-le să își îndeplinească sarcinile cu o bună înțelegere a riscurilor de securitate cibernetică.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Rolurile specializate din cadrul organizației care necesită instruire suplimentară în domeniul securității cibernetice (de exemplu, personalul fizic și de securitate cibernetică, personalul financiar, persoanele cu funcții de conducere și orice persoană care are acces la date critice pentru activitate) ar trebui identificate în mod oficial.
- Toți cei care ocupă funcții specializate, inclusiv contractorii, partenerii, furnizorii și alte părți terțe, ar trebui să beneficieze de conștientizare și instruire în materie de securitate cibernetică, în funcție de rolul pe care îl ocupă.
- Ar trebui să se asigure că instruirea este furnizată înainte de acordarea accesului și că este adaptată riscurilor și responsabilităților specifice fiecărui rol.
- Persoanele fizice ar trebui să fie evaluate periodic și testate cu privire la înțelegerea practicilor de securitate cibernetică prin teste, simulări sau evaluări practice relevante pentru rolul lor.
- Luarea în considerare a organizării de cursuri anuale de perfecționare pentru consolidarea practicilor existente și introducerea unor noi practici.
- Ar trebui incluse atât contextul IT, cât și cel OT, în special pentru rolurile care interacționează cu sistemele industriale sau infrastructura critică.

PR.AT-02.3

Utilizatorii privilegiați trebuie calificați înainte de acordarea privilegiilor, iar acești utilizatori trebuie să poată demonstra înțelegerea rolurilor, responsabilităților și a atribuțiilor lor de autoritate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că persoanele fizice cărora li s-a acordat acces privilegiat, fie în medii IT, fie în medii OT, sunt în mod demonstrabil competente și pe deplin conștiente de responsabilitățile, riscurile și limitele autorității legate de rolul lor în domeniul securității cibernetice. Aceasta reduce probabilitatea utilizării accidentale sau a exploatării abuzive a privilegiilor ridicate, în special în sistemele critice în care continuitatea operațională și siguranța sunt în joc.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Utilizatorii cu drepturi privilegiate ar trebui să fie instruiți în diverse aspecte pentru a asigura că își utilizează drepturile de acces ridicate într-un mod sigur și responsabil. Ar putea fi considerate următoarele subiecte de instruire:
  - Conștientizarea securității
    - Este esențial ca utilizatorii cu drepturi privilegiate să fie conștienți de riscurile de securitate asociate drepturilor lor de acces ridicate. Aceasta include cunoștințe despre phishing, malware și alte amenințări cibernetice.
  - Managementul accesului
    - Utilizatorii ar trebui să înțeleagă cum să își gestioneze corect drepturile de acces, inclusiv utilizarea parolelor puternice, MFA și restricționarea accesului numai la ceea ce este necesar pentru rolul lor.
  - Conformitatea și reglementarea
    - Este important ca utilizatorii cu drepturi privilegiate să cunoască legile și reglementările relevante, precum GDPR, Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148, denumită în continuare Directiva NIS 2 sau NIS 2, Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011, și modul în care acestea le afectează activitatea.

- Răspunsul la incidente
  - Instruirea privind modul de răspuns la incidentele de securitate este esențială. Aceasta include recunoașterea activităților suspecte și cunoașterea modului și a persoanelor cărora trebuie să le fie raportate.
- Cele mai bune practici de management al datelor
  - Utilizatorii ar trebui instruiți cu privire la modul de stocare, prelucrare și transfer securizat al datelor sensibile.
- Etica și responsabilitatea
  - Este important ca utilizatorii cu drepturi privilegiate să fie conștienți de responsabilitățile lor etice și de posibilele consecințe ale utilizării abuzive a drepturilor lor de acces.

- Utilizatorii cu drepturi privilegiate ar trebui să fie evaluați și testați periodic cu privire la înțelegerea practicilor de securitate cibernetică pentru rolurile lor specializate.
- Luarea în considerare a organizării unor activități anuale de perfecționare pentru consolidarea practicilor existente și introducerea de noi practici.

[PR.DS] SECURITATEA DATELOR

Datele sunt gestionate în conformitate cu strategia de management al riscului a organizației pentru protejarea confidențialității, integrității și disponibilității informațiilor.

PR.DS-01

Confidențialitatea, integritatea și disponibilitatea datelor stocate sunt protejate.

PR.DS-01.1

Organizația trebuie să implementeze verificări ale integrității software-ului, firmware-ului și informațiilor pentru detecția modificărilor neautorizate ale componentelor critice ale sistemului său în timpul depozitării, transportului, pornirii și atunci când se consideră necesar.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura integritatea și fiabilitatea componentelor critice ale sistemului, precum software-ul, firmware-ul și datele de configurare, prin detecția modificărilor neautorizate care ar putea compromite siguranța, fiabilitatea sau securitatea operațională în toate etapele ciclului de viață, inclusiv depozitarea, transportul și punerea în funcțiune.

Pentru protejarea în mod eficace a integrității datelor stocate, organizația ar trebui să implementeze un set de controale stratificate, proiectate pentru detecția și prevenirea modificărilor neautorizate ale datelor stocate, ale software-ului și ale componentelor sistemului.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aplicarea mecanismelor de integritate criptografică
    - Utilizarea hash-urilor criptografice (de exemplu, SHA-256), a semnăturilor digitale sau a altor mecanisme criptografice (de exemplu, coduri de autentificare a mesajului - MAC) pentru verificarea integrității datelor stocate și fișierelor critice.
    - Valorile de integritate ar trebui generate în momentul stocării și verificate înainte de accesare sau executare.
- Implementarea monitorizării automate a integrității
    - Implementarea unor instrumente de monitorizare a integrității fișierelor (FIM) pentru a urmări continuu modificările aduse fișierelor, configurațiilor și aplicațiilor critice ale sistemului.
    - Ar trebui generate alerte pentru orice modificări neautorizate sau neașteptate, iar jurnalele ar trebui păstrate pentru audit și investigații.
- Validarea integrității software-ului și firmware-ului
    - Asigurarea validării software-ului și firmware-ului stocate pe sisteme, utilizând verificarea semnăturii sau mecanisme de pornire securizată înainte de execuție.

- Validarea integrității ar trebui să facă parte din procesul de pornire a sistemului și să fie pusă în aplicare prin controale tehnice.

- Punerea în aplicare a controlului modificărilor și restricțiilor de acces
  - Limitarea accesului de scriere la datele critice și componentele sistemului prin RBAC și principii de privilegii minime.
  - Toate modificările aduse datelor stocate ar trebui să fie supuse procedurilor formale de management al modificărilor și jurnalizate pentru a putea fi monitorizate.

- Protejarea integrității backup-urilor
  - Backup-urile ar trebui să includă mecanisme de verificare a integrității (de exemplu, sume de control sau semnături digitale) pentru a asigura că nu au fost modificate.
  - Ar trebui efectuate restaurări de testare periodice pentru a confirma integritatea și utilizabilitatea datelor de backup.

PR.DS-01.2

Organizația trebuie să implementeze instrumente automatizate, acolo unde este fezabil, pentru a furniza notificări în cazul descoperirii unor discrepanțe în timpul verificării integrității.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura detecția și raportarea automată a discrepanțelor în integritatea sistemului sau a datelor, permițând o reacție promptă și reducând riscul de manipulare nedetectată, în special în medii în care continuitatea operațională și siguranța sunt critice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Implementarea instrumentelor automatizate, acolo unde este fezabil, pentru a verifica în mod continuu integritatea datelor și sistemelor critice.
- Asigurarea faptului că aceste instrumente raportează prompt încălcările integrității, atunci când sunt detectate discrepanțe.
- Configurarea alertelor de notificare pentru personalul relevant, precum administratorii de sistem, responsabilii de proces și responsabilii cu securitatea informației, pentru a permite investigarea și răspunsul rapid.
- Utilizarea soluțiilor de verificare a integrității gestionate centralizat pentru eficientizarea monitorizării și raportării, atât în mediile IT, cât și în mediile OT.
- Urmarea recomandărilor ENISA, precum Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA, care prezintă bunele practici pentru monitorizarea automată a integrității și răspunsul la incidente.

PR.DS-01.3

Organizația trebuie să definească și să implementeze răspunsuri automate la încălcările de integritate detectate, utilizând măsuri de protecție predefinite, proporționale cu gravitatea și impactul încălcării.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a minimiza impactul încălcărilor integrității prin activarea unor răspunsuri rapide, proporționale și automate care contribuie la limitarea amenințărilor, la menținerea stabilității sistemului și la susținerea analizei criminalistice, în special în medii în care intervenția manuală poate fi întârziată sau nepractică.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Ar trebui definite nivelurile de gravitate și acțiunile de răspuns, încălcările integrității fiind clasificate (de exemplu, impact redus, mediu, ridicat) și corelate cu măsuri de protecție automate adecvate.
- Alertele și notificările ar trebui declanșate automat la detectarea încălcărilor integrității și integrate cu platformele SOAR pentru eficientizarea gestionării incidentelor.
- Componentele afectate ar trebui carantinate sau izolate, precum fișierele, aplicațiile sau sistemele compromise, pentru prevenirea deteriorării ulterioare.
- Toate evenimentele ar trebui să fie jurnalizate și auditabile, inclusiv încălcările detectate și acțiunile automate, pentru sprijinirea investigațiilor criminalistice și raportarea conformității.
- Automatizarea ușoară ar trebui utilizată acolo unde este posibil, precum:
    - Blocarea anumitor procese sau utilizatori.
    - Revenirea la o configurație cunoscută ca fiind bună.
    - Dezactivarea temporară a serviciilor afectate.
- Mecanismele de răspuns ar trebui testate și ajustate periodic în medii controlate pentru asigurarea eficacității și evitării întreruperilor inutile.
- Ar trebui consultate recomandările ENISA din Ghidul de implementare a măsurilor de securitate (pentru consultare publică, documentul nr. ENISA/2024/IGSM).

PR.DS-01.4

Organizația trebuie să definească și să pună în aplicare politici clare și măsuri practice de protecție pentru gestionarea și restricționarea utilizării suporturilor de stocare portabile, în vederea reducerii riscului de scurgeri de date, acces neautorizat și introducerea de malware.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul de scurgere de date, acces neautorizat și introducere de malware prin definirea și aplicarea unor politici și măsuri de protecție clare privind utilizarea suporturilor de stocare portabile.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea și comunicarea politicii
    - Ar trebui stabilită o politică documentată privind utilizarea acceptabilă a dispozitivelor de stocare portabile (de exemplu, dispozitive USB, carduri SD, hard disk-uri externe).
    - Politica ar trebui comunicată în timpul procesului de integrare organizațională și consolidată prin instruiri periodice pentru conștientizare în domeniul securității.
- Controlul utilizării dispozitivelor
    - Ar trebui permise doar dispozitivele de stocare portabile aprobate de organizație.
    - Ar trebui menținut un inventar al dispozitivelor aprobate asociat cu utilizatori sau departamente specifice.
- Aplicarea măsurilor de protecție practice
    - Controlul accesului: Dispozitivele ar trebui să solicite autentificarea utilizatorului (de exemplu, protecție prin parolă).
    - Criptarea: Datele de pe dispozitivele portabile ar trebui criptate folosind unități criptate hardware sau instrumente software precum BitLocker To Go sau VeraCrypt.
    - Modul numai pentru citire: Dispozitivele utilizate pentru distribuție (de exemplu, actualizări de software) ar trebui configurate doar pentru modul numai pentru citire.
    - Scanarea malware-ului: Dispozitivele ar trebui scanate pentru malware înainte și după utilizare.
    - Securitatea fizică: Dispozitivele ar trebui depozitate în mod securizat (de exemplu, în sertare sau dulapuri încuiate) atunci când nu sunt utilizate.

- Monitorizarea şi jurnalizarea utilizării
  - Pe sistemele gestionate, conexiunile dispozitivelor USB şi transferurile de fişiere ar trebui jurnalizate folosind instrumente de management al endpoint-urilor.
  - Jurnalele ar trebui revizuite periodic pentru detecția utilizării neautorizate sau a anomaliilor.
- Exemple
  - Un tehnician de teren ar trebui să utilizeze un dispozitiv USB criptat, furnizat de organizație, pentru colectarea datelor de la senzori la distanță. Unitatea ar trebui scanată înainte şi după utilizare, iar datele ar trebui încărcate pe un server securizat la întoarcere.
  - O echipă de marketing ar trebui să utilizeze un dispozitiv USB cu acces numai pentru citire pentru distribuirea materialelor promoționale la târguri şi expoziții, împiedicând astfel copierea datelor înapoi pe dispozitiv.

PR.DS-01.5

Organizația trebuie să permită utilizarea mediilor amovibile numai atunci când este absolut necesar și trebuie să pună în aplicare măsuri tehnice pentru a bloca executarea automată a fișierelor de pe aceste dispozitive.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a minimiza suprafața de atac în mediile operaționale și IT prin limitarea strictă a utilizării mediilor amovibile și prevenirea executării automate a fișierelor potențial dăunătoare.

Pentru a reduce riscul de infectare cu malware și de scurgere de date prin mediile amovibile (de exemplu, dispozitive USB, unități externe de memorie), organizația ar trebui să ia în considerare următoarele:

- Permiterea utilizării doar atunci când este necesar
    - Organizația ar trebui să precizeze în politica sa că mediile amovibile ar trebui utilizate doar atunci când nu există o alternativă mai securizată (de exemplu, transferul securizat de fișiere).
    - Ar trebui utilizate instrumente tehnice pentru limitarea accesului la porturile USB sau pentru solicitarea aprobării înainte de utilizare.
- Dezactivarea funcțiilor de rulare și execuție automată
    - Toate sistemele ar trebui configurate astfel încât să dezactiveze funcțiile de rulare automată și redare automată, pentru ca fișierele de pe mediile amovibile să nu fie executate automat.
    - Aceasta ar trebui să contribuie la prevenirea executării malware-ului fără acțiunea utilizatorului.
- Utilizarea instrumentelor de securitate pentru controlul accesului
    - Organizația ar trebui să utilizeze instrumente de protecție a endpoint-urilor pentru:
        - Blocarea sau limitarea accesului USB.
        - Permiterea utilizării doar a dispozitivelor aprobate.
        - Solicitarea aprobării administratorului pentru dispozitivele noi.
- Monitorizarea și revizuirea utilizării
    - Organizația ar trebui să monitorizeze utilizarea mediilor amovibile prin jurnalizarea conexiunilor dispozitivelor prin intermediul instrumentelor de protecție a endpoint-urilor sau al jurnalelor sistemului de operare. În mediile OT, ar trebui utilizate proceduri de jurnalizare

manuală sau de acces controlat. Jurnalele ar trebui revizuite periodic pentru detecția activităților neautorizate.

- Exemplu: Echipa financiară ar trebui să utilizeze dispozitive USB criptate, aprobate de organizație, pentru transferul rapoartelor confidențiale. Aceste unități ar trebui scanate înaintea utilizării, funcția de executare automată ar trebui dezactivată pe toate sistemele, iar accesul ar trebui jurnalizat și revizuit.

Clarificarea diferenței față de PR.DS-01.4

- PR.DS-01.4 se concentrează pe stabilirea regulilor și procedurilor privind modul în care ar trebui utilizate mediile amovibile (de exemplu, cine le poate utiliza, criptarea, protecția fizică).
- PR.DS-01.5 se concentrează pe punerea în aplicare tehnică a acestor norme - modul în care sistemele ar trebui configurate pentru reducerea riscurilor.

PR.DS-01.6

Organizația trebuie să protejeze confidențialitatea activelor sale critice în stare de repaus.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că datele operaționale și ale activității sensibile stocate pe sisteme, servere sau dispozitive rămân protejate împotriva accesului neautorizat, chiar și în cazul în care securitatea fizică sau logică este compromisă.

În mediile OT, unde sistemele vechi și infrastructura partajată sunt comune, protejarea datelor stocate este critică pentru prevenirea expunerii fișierelor de configurare, a datelor de proces sau a datelor de acces care ar putea fi exploatate pentru perturbarea operațiunilor sau pentru obținerea accesului lateral.

Acest Control se bazează pe PR.DS-01.1.

Pentru a permite protejarea activelor critice ale organizației în stare de repaus, ar trebui luate în considerare următoarele tehnici:

- Criptarea: Criptarea datelor stocate pe hard disk-uri, pe suporturi externe, în fișiere stocate, în fișiere de configurare și stocate în cloud, utilizând algoritmi de criptare puternici pentru prevenirea accesului neautorizat și protejarea datelor împotriva modificării.
- Controale de acces: Implementarea controalelor stricte de acces pentru a asigura că numai personalul autorizat poate accesa informațiile sensibile.
- Audituri periodice: Efectuarea de audituri de securitate periodice pentru identificarea și remedierea vulnerabilităților.
- Mascarea datelor: Utilizarea tehnicilor de mascare a datelor pentru ascunderea informațiilor sensibile în medii care nu sunt de producție (de exemplu, datele sensibile din punct de vedere al GDPR din mediul de producție nu pot fi copiate într-un mediu de testare fără randomizare, pentru prevenirea accesului neautorizat la date).

PR.DS-01.9

Activele organizației trebuie să fie casate în mod securizat.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate activele organizației sunt casate într-o manieră securizată și controlată, pentru a preveni accesul neautorizat la date sensibile referitoare la activitate, date personale sau date operaționale.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Sanitizarea datelor înainte de casare
    - Datele sensibile ar trebui eliminate în mod securizat („șterse în mod securizat") de pe toate activele, precum computere, servere, hard disk-uri, dispozitive USB, dispozitive mobile și documente pe hârtie, înainte de scoaterea din uz, reatribuire, reparare sau înlocuire.
- Utilizarea metodelor adecvate de distrugere
    - Ar trebui să existe metode adecvate pentru distrugerea documentelor pe hârtie, a suporturilor de stocare digitale și a altor suporturi fizice de date.
- Activarea ștergerii securizate la distanță pentru dispozitivele mobile
    - Capabilitățile de ștergere securizată la distanță ar trebui activate pe laptopuri, tablete, telefoane și alte dispozitive mobile pentru a proteja datele în cazul pierderii sau furtului.
- Gestionarea cu atenție a numelor de domenii expirate
    - Domeniile expirate ar trebui protejate, deoarece sunt adesea ținta infractorilor cibernetici. Ar trebui luate în considerare următoarele practici:
        - Activarea reînnoirii automate sau reînnoirea domeniilor pentru o perioadă de cel puțin zece ani.
        - Comunicarea clară a modificărilor de domeniu și gestionarea internă a tranzițiilor.
        - Setarea unor răspunsuri automate pentru e-mailurile trimise către domeniile vechi.
        - Actualizarea referințelor online și a setărilor din serviciile cloud.
        - Modificarea sau ștergerea conturilor înregistrate cu domenii vechi.
        - Menținerea actualizată a adreselor de e-mail folosite pentru autentificare și activarea MFA.
        - Evitarea utilizării unor soluții neaprobate de stocare în cloud pentru date sensibile.

- Respectarea bunelor practici de management al activelor
    - Pentru a sprijini casarea securizată, ar trebui utilizate recomandări din surse de încredere, precum șablonul de Politică pentru managementul activelor din Setul de instrumente CyFun ® de pe www.cyfun.eu.
- Includerea activelor OT în planificarea casării
    - Sistemele și dispozitivele OT ar trebui incluse în procedurile de casare, asigurându-se că datele operaționale și configurațiile sunt eliminate în mod securizat înainte de scoatere din uz și dezafectare.

PR.DS-02

Confidențialitatea, integritatea și disponibilitatea datelor în tranzit sunt protejate.

PR.DS-02.1

Dispozitivele de stocare portabile care conțin date de sistem trebuie controlate și protejate în timpul transportului și depozitării.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a preveni accesul neautorizat, modificarea sau pierderea datelor critice ale sistemului, atunci când dispozitivele de stocare portabile sunt mutate între locații sau stocate în afara mediilor securizate.

În mediile OT, unde datele pot fi transferate între sisteme izolate sau site-uri la distanță folosind suporturi fizice, protejarea acestor dispozitive este esențială pentru menținerea integrității și confidențialității sistemului.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Scanarea tuturor dispozitivelor de stocare portabile în căutarea de coduri cu scop nelegitim înainte de utilizarea în sistemele organizației.
- Criptarea datelor pentru asigurarea confidențialității în cazul pierderii sau furtului unui dispozitiv.
- Utilizarea sigiliilor inviolabile și containerelor încuiate în timpul transportului.
- Apelarea la curieri de încredere sau servicii de transport securizate și evitarea lăsării dispozitivelor nesupravegheate.
- Limitarea accesului la dispozitivele stocate la personalul autorizat, cu sprijinul politicilor documentate de control al accesului.
- Depozitarea dispozitivelor în medii securizate, cu climat controlat, pentru prevenirea deteriorării fizice.
- Efectuarea de audituri periodice și verificări ale inventarului pentru a asigura contabilizarea și securizarea corespunzătoare a dispozitivelor.

PR.DS-02.2

Organizația trebuie să protejeze informațiile sale critice și sensibile în timpul tranzitului.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura confidențialitatea și nealterarea informațiilor critice și sensibile în timpul transmiterii prin rețele sau între sisteme, în special în medii în care fluxurile de date circulă între straturile IT și OT sau între site-uri la distanță.

În contextele OT, în care datele pot traversa canale de comunicații mai puțin securizate sau vechi (de exemplu, între sisteme de control, dispozitive de teren sau stații de monitorizare la distanță), protecția în timpul tranzitului este esențială pentru prevenirea interceptării, manipulării sau scurgerii de informații. Acest Control se bazează în continuare pe PR.DS-01.1.

Pentru a permite protejarea informațiilor critice și sensibile ale organizației în timpul tranzitului, ar trebui luate în considerare următoarele tehnici:

- Criptarea
    - Utilizarea protocoalelor de criptare puternice, precum TLS sau stratul de socluri securizate (SSL), pentru criptarea datelor în timpul transmiterii. Astfel, chiar dacă datele sunt interceptate, ele rămân ilizibile pentru persoanele neautorizate.
- E2EE
    - Implementarea E2EE, care criptează datele pe dispozitivul expeditorului și le decriptează numai pe dispozitivul destinatarului.
- MFA
    - Solicitarea MFA pentru accesarea informațiilor sensibile.
- Politici de parole puternice
    - Punerea în aplicare a politicilor de parole puternice, inclusiv utilizarea de parole complexe și actualizări regulate.
- VPN
    - Utilizarea VPN - fie site-to-site, fie cu acces la distanță - pentru stabilirea unor tuneluri securizate pentru transmiterea datelor, în special în cazul conectării prin rețele nesigure, precum Wi-Fi-ul public.
- Audituri de securitate periodice
    - Efectuarea de audituri de securitate periodice pentru identificarea și remedierea vulnerabilităților din procesele de transmitere a datelor.

PR.DS-10

Confidențialitatea, integritatea și disponibilitatea datelor utilizate sunt protejate.

PR.DS-10.1

Sistemele critice ale organizației trebuie protejate împotriva atacurilor de tip denial-of-service (DoS) sau, cel puțin, efectul acestor atacuri trebuie limitat.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că sistemele critice rămân disponibile și operaționale chiar și atunci când sunt ținta unor atacuri de tip DoS, care au ca scop supraîncărcarea sau întreruperea serviciilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Limitarea impactului atacurilor DoS prin:
  - Implementarea de dispozitive sau servicii de protecție a granițelor care filtrează traficul cu scop nelegitim.
  - Asigurarea unei capacități și redundanțe suficiente a rețelei pentru a absorbi vârfurile de trafic.
- Restricționarea capacității de a lansa atacuri DoS prin:
  - Limitarea opțiunilor de conectivitate pentru prevenirea transmisiilor neautorizate prin conexiuni cu fir, wireless sau prin satelit.
  - Aplicarea limitelor de utilizare a resurselor pentru prevenirea supraîncărcării sistemului.
  - Aplicarea unei autentificări și autorizări puternice pentru a controla accesul la funcțiile critice.
- Consolidarea rezilienței sistemului prin:
  - Efectuarea de teste și audituri de securitate periodice pentru identificarea și remedierea vulnerabilităților.
  - Monitorizarea traficului de rețea pentru anomalii care ar putea indica semne timpurii ale unei tentative de DoS.
- Considerații specifice OT
  - În mediile OT, unde disponibilitatea afectează în mod direct siguranța și producția, chiar și întreruperile scurte pot avea consecințe grave. Protecțiile DoS trebuie adaptate protocoalelor industriale și sistemelor vechi, asigurând că măsurile de apărare nu interferează cu operațiunile în timp real.

PR.DS-11

Backup-urile datelor sunt create, protejate, menținute și testate.

PR.DS-11.1

Backup-urile datelor critice pentru activitatea organizației trebuie efectuate și stocate pe un sistem diferit de dispozitivul pe care se află datele originale.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că datele critice pentru activitate sunt salvate periodic și stocate în mod securizat pe un sistem separat, pentru a le proteja împotriva pierderii, defecțiunilor sistemului sau atacurilor cibernetice, precum ransomware.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Realizarea backup-urilor datelor și sistemelor critice
  - Backup-urile ar trebui să includă:
    - Date critice pentru activitate (de exemplu, înregistrări ale clienților, date financiare și operaționale).
    - Date de sistem, precum configurații software, setări ale dispozitivelor, documentație și backup-uri ale aplicațiilor.
- Definirea unei strategii de backup
  - Datele critice ar trebui să fie copiate în mod continuu sau aproape în timp real.
  - Alte date importante ar trebui să fie copiate la intervale regulate, convenite.
  - Backup-urile ar trebui stocate pe un sistem separat fizic sau logic de sursa originală de date. Aceasta înseamnă că nu trebuie să se afle pe același dispozitiv sau server de stocare ca datele originale. În mod ideal, backup-urile ar trebui stocate într-o zonă de securitate diferită, un segment de rețea diferit sau chiar într-o locație externă, pentru a asigura că rămân accesibile și necompromise în cazul unei defecțiuni a sistemului, al unui atac ransomware sau al altor incidente care afectează mediul principal.
- Asigurarea separării rețelei
  - Backup-urile nu ar trebui stocate în aceeași rețea cu sistemele originale.
  - Cel puțin o copie de backup ar trebui păstrată complet offline sau izolată fizic pentru a asigura recuperarea în cazul unei breșe de securitate a rețelei sau al unui atac ransomware.

- Planificarea procesului de recuperare
    - RTO (cât de repede trebuie restaurate sistemele) și RPO (cât de mare este pierderea acceptabilă de date) ar trebui definite și revizuite periodic pentru a asigura o restaurare rapidă și eficace.
- Includerea mediilor OT
    - Strategiile de backup ar trebui să acopere sistemele OT, inclusiv configurațiile sistemelor de control, datele operaționale și setările dispozitivelor critice pentru operațiunile industriale.

PR.DS-11.2

Fiabilitatea și integritatea backup-urilor trebuie verificate și testate periodic.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că datele de backup sunt fiabile și pot fi restaurate cu succes atunci când este necesar, sprijinind continuitatea operațională și reziliența.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Testarea procedurilor de recuperare
  - Procedurile de recuperare a backup-urilor ar trebui testate periodic pentru a confirma că datele pot fi restaurate cu acuratețe și în întregime.
- Verificarea integrității backup-urilor
  - Înainte de utilizare, backup-urile ar trebui verificate pentru detecția semnelor de compromitere, corupție sau manipulare.
  - Verificările de integritate ar trebui să se concentreze pe indicatorii de încălcare ai securității sau pierderi de date.
- Programarea testelor
  - Toate tipurile de surse de date ar trebui incluse în testele de backup și restaurare.
  - Testarea ar trebui să aibă loc cel puțin anual sau mai frecvent, pe bază de eșantion.
- Alinierea la controalele conexe
  - Acest Control ar trebui implementat în coordonare cu RC.RP-05.1 (Planificarea recuperării), asigurând coerența strategiilor de recuperare.

PR.DS-11.3

Organizația trebuie să mențină backup-uri securizate ale datelor critice pentru activitate într-o locație de stocare separată, pentru asigurarea disponibilității datelor în cazul unei defecțiuni a sistemului sau al pierderii datelor. Stocarea backup-urilor trebuie să aplice controale de securitate echivalente cu cele din mediul principal.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația poate recupera în mod fiabil datele sale critice pentru activitate, în două scenarii cheie:

- Dezastre naturale sau daune fizice ale sediului principal (care necesită backup-uri la o locație externă sau în cloud).
- Atacuri cibernetice avansate, inclusiv ransomware sau amenințări din interior, în care atacatorii pot încerca să corupă sau să șteargă backup-urile (necesitând backup-uri izolate sau protejate împotriva manipulării).

Acest Control contribuie la asigurarea faptului că o organizație poate recupera datele sale critice în cazul în care ceva nu funcționează corect. Se concentrează pe păstrarea backup-urilor separate și la fel de securizate ca datele originale, ceea ce îl face deosebit de util pentru organizațiile care încă își dezvoltă capabilitățile de securitate cibernetică (organizații cu o postură de securitate mai puțin matură).

- Strategia de backup de luat în considerare
  - Pentru îndeplinirea acestor obiective, organizația ar trebui să implementeze o abordare diversificată și rezilientă în materie de backup, precum Regula de backup 3-2-1:
    - Menținerea a trei copii ale datelor critice pentru activitate.
    - Stocarea acestor copii pe cel puțin două tipuri diferite de suporturi de stocare (de exemplu, disc local și cloud).
    - Asigurarea că cel puțin o copie este stocată la o locație externă sau în afara incintei, într-o locație fizic separată.
- Pentru protecție împotriva amenințărilor fizice și cibernetice, organizația ar trebui să ia în considerare următoarele tipuri de backup:
  - Backup-uri la o locație externă sau în cloud
    - Aceste backup-uri sunt stocate într-o locație separată geografic și contribuie la asigurarea recuperabilității în cazul unor dezastre naturale sau al deteriorării fizice a site-ului principal.

- Backup-uri imuabile
  - Acestea sunt backup-uri care nu pot fi modificate sau șterse pentru o perioadă determinată. Sunt deosebit de eficace împotriva ransomware-ului și a amenințărilor din interior și pot fi automatizate pentru reducerea efortului manual.
- Backup-uri offline sau izolate fizic
  - Acestea sunt backup-uri stocate pe dispozitive complet deconectate de la orice rețea, inclusiv de la internet. Această izolare asigură că, chiar dacă rețeaua organizației este compromisă, backup-ul rămâne intact.

- Considerații suplimentare
  - Separarea geografică
    - Locațiile backup-urilor ar trebui să fie situate în regiuni fizice diferite, pentru reducerea riscului unui impact simultan din cauza unor dezastre regionale.
  - Paritatea de securitate
    - Toate locațiile de backup ar trebui să implementeze același nivel de controale de securitate ca ale mediului principal (de exemplu, criptare, controlul accesului, monitorizare).
  - Testarea periodică
    - Procedurile de backup și recuperare ar trebui testate periodic pentru asigurarea integrității datelor și disponibilitatea operațională.

PR.DS-11.4

Organizația trebuie să verifice periodic integritatea și capacitatea de recuperare a backup-urilor, prin teste coordonate cu toate funcțiile relevante de continuitate și răspuns la incidente. Testarea backup-urilor trebuie integrată în planificarea mai largă a rezilienței, inclusiv continuitatea activității, recuperarea în caz de dezastru și răspunsul la incidente cibernetice.

GHID DE IMPLEMENTARE

Acest Control este o evoluție a PR.DS-11.3 și asigură că sistemele de backup nu sunt doar implementate, ci și testate periodic și aliniate la planurile mai ample de recuperare și continuitate ale organizației. Aceasta subliniază importanța coordonării între echipe și a planificării proactive, ajutând organizația să fie pregătită pentru recuperarea rapidă și eficace în urma incidentelor grave.

Pentru a asigura eficacitatea și integrarea în strategia generală de reziliență organizațională a capabilităților de backup și recuperare, ar trebui implementate următoarele practici:

- Coordonarea testării backup-urilor pentru toate planurile
    - Verificarea backup-urilor ar trebui planificată și executată în coordonare cu echipele responsabile pentru planurile cheie de continuitate și răspuns ale organizației. Acestea includ:
        - BCP-uri.
        - DRP-uri.
        - Planuri de urgență.
        - Planuri de continuitate a operațiunilor (COOP).
        - Planuri de comunicare de criză.
        - Planuri de protecție a infrastructurilor critice.
        - Planuri de răspuns la incidente cibernetice.
- Includerea recuperării backup-urilor în testarea scenariilor
    - În timpul exercițiilor sau simulărilor de incidente (de exemplu, atacuri cibernetice, defecțiuni ale sistemului sau dezastre naturale), recuperarea backup-urilor ar trebui testată în mod explicit. Aceasta garantează că backup-urile nu sunt doar disponibile, ci și utilizabile și aliniate la RTO/RPO.
- Documentarea și revizuirea rezultatelor
    - Rezultatele verificării backup-urilor și ale testelor de recuperare ar trebui documentate și revizuite împreună cu părțile interesate relevante pentru identificarea lacunelor și îmbunătățirea procedurilor.

PR.DS-11.5

Backup-urile sistemelor critice (precum sistemele de operare, configurațiile și aplicațiile) trebuie păstrate separat de backup-urile informațiilor critice (precum datele activității, documentele și bazele de date) pentru permiterea unei recuperări mai rapide și mai fiabile.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a sprijini o recuperare mai rapidă și mai fiabilă prin separarea backup-urilor sistemelor critice (de exemplu, sisteme de operare, configurații, aplicații) de backup-urile informațiilor critice (de exemplu, datele activității, documente, baze de date).

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Separarea domeniilor de aplicare ale backup-urilor
    - Backup-urile sistemului ar trebui să includă sistemele de operare, configurațiile, software-ul instalat și setările la nivel de sistem.
    - Backup-urile informațiilor ar trebui să includă date critice pentru activitate, precum baze de date, documente și date ale aplicațiilor.
- Utilizarea metodelor de backup personalizate
    - Backup-urile sistemului ar trebui să utilizeze imagini complete sau instantanee pentru a captura starea integrală a sistemului.
    - Backup-urile informațiilor ar trebui să utilizeze metode incrementale sau diferențiale pentru a captura în mod eficient modificările datelor.
- Criptarea datelor sensibile
    - Atât backup-urile sistemului, cât și cele ale informațiilor ar trebui criptate în timpul stocării și transmiterii, în special atunci când conțin date sensibile sau reglementate.
- Alinierea la obiectivele de recuperare
    - Separarea backup-urilor ar trebui să reflecte diferite RTO și RPO. De exemplu, recuperarea sistemului ar putea necesita o restaurare mai rapidă decât datele activității.
- Documentarea și automatizarea
    - Domeniile de aplicare și procedurile de backup ar trebui documentate în mod clar.
    - Procesele de backup ar trebui automatizate, acolo unde este fezabil, pentru reducerea erorilor umane și asigurarea consecvenței.

Considerații specifice OT

În mediile OT, separarea backup-urilor sistemului și ale datelor contribuie la restabilirea rapidă a sistemelor de control, fără a fi necesară recuperarea seturilor mari de date. Aceasta susține continuitatea operațională și reduce timpul de nefuncționare în procesele industriale critice.

Relația cu PR.DS-11.3 și PR.DS-11.4

PR.DS-11.5 este o evoluție - nu o repetare - a PR.DS-11.3 și PR.DS-11.4. În timp ce controalele anterioare se concentrează pe locul și modul în care sunt stocate și verificate backup-urile, PR.DS-11.5 se concentrează pe ceea ce este copiat și modul în care este separat logic pentru a optimiza recuperarea:

- PR.DS-11.3 asigură că backup-urile sunt securizate și stocate separat;
- PR.DS-11.4 asigură testarea backup-urilor și integrarea acestora în planificarea recuperării;
- PR.DS-11.5 asigură separarea funcțională între backup-urile sistemului și cele ale datelor pentru a permite o recuperare mai rapidă și mai precisă.

[PR.PS] SECURITATEA PLATFORMEI

Hardware-ul, software-ul (de exemplu, firmware, sisteme de operare, aplicații) și serviciile platformelor fizice și virtuale sunt gestionate în conformitate cu strategia de management al riscului a organizației pentru protejarea confidențialității, integrității și disponibilității.

PR.PS-01

Practicile de management al configurației sunt stabilite și aplicate.

PR.PS-01.1

Organizația trebuie să dezvolte, documenteze și mențină o configurație de bază pentru sistemele sale critice pentru activitate.

GHID DE IMPLEMENTARE

Acest Control asigură că toate sistemele critice pentru activitate funcționează într-o stare cunoscută, securizată și aprobată. O configurație de bază definește setarea standard pentru aceste sisteme, contribuind la detecția modificărilor neautorizate, punerea în aplicare a politicilor de securitate și susținerea operațiunilor consecvente.
În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea sintagmei critic pentru activitate
    - Sistemele critice pentru activitate ar putea include componente IT, OT și, potențial, IoT - dacă acestea susțin funcții esențiale ale organizației:
        - Sistemele IT sunt de obicei gestionate intern.
        - Sistemele OT ar putea include ICS.
        - Sistemele IoT (de exemplu, senzori, dispozitive inteligente) pot fi critice pentru activitate dacă defectarea lor perturbă operațiunile sau introduce riscuri de securitate.
- Stabilirea și menținerea configurațiilor de bază
    - Pentru fiecare sistem critic pentru activitate, linia de bază ar trebui să includă:
        - Componentele sistemului (de exemplu, software și hardware aprobat).
        - Versiunile sistemului de operare și ale aplicațiilor, inclusiv nivelurile de patch-uri.
        - Setări și parametri de configurare.
        - Topologia rețelei, care arată modul în care sunt conectate componentele, inclusiv:
            → Conexiuni externe.
            → Servere care găzduiesc date sau funcții sensibile.

→ Servicii DNS și de securitate.

→ Amplasarea logică a componentelor în cadrul arhitecturii sistemului.

- Aplicarea principiilor de securitate
  - Liniile de bază ar trebui să pună în aplicare principiul funcționalității minime - ar trebui activate numai funcțiile și serviciile necesare.
  - Setările implicite ar trebui revizuite și ajustate pentru reducerea riscurilor de securitate în timpul instalării sau actualizărilor.
- Monitorizarea și actualizarea liniei de bază
  - Monitorizarea continuă a sistemelor pentru detecția abaterilor de la linia de bază aprobată.
  - Actualizarea liniilor de bază în urma aplicării de patch-uri, a actualizărilor sau a reconfigurării sistemelor.
- Sisteme gestionate în cloud și de furnizori
  - Pentru sistemele gestionate de părți terțe (de exemplu, servicii cloud), organizația ar trebui să se asigure că așteptările privind linia de bază sunt definite contractual și că furnizorii oferă vizibilitate asupra configurației și a managementului modificărilor.

PR.PS-01.2

Organizația trebuie să configureze sistemele sale critice pentru activitate astfel încât să funcționeze doar cu funcțiile esențiale necesare scopului lor. Aceasta include revizuirea și actualizarea configurațiilor de bază pentru a dezactiva orice capabilități neesențiale.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscurile de securitate și complexitatea sistemului, asigurând că sistemele critice pentru activitate sunt configurate să execute numai funcțiile necesare pentru scopul pentru care au fost concepute.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Aplicarea principiului funcționalității minime prin dezactivarea caracteristicilor, serviciilor și componentelor neesențiale.
- Revizuirea și actualizarea periodică a configurațiilor de bază pentru reflectarea nevoilor operaționale și amenințărilor în continuă evoluție.
- Evaluarea și limitarea următoarelor elemente la ceea ce este strict necesar:
    - Software instalat;
    - Servicii activate;
    - Porturi deschise;
    - Protocoale permise;
    - Caracteristici ale sistemului.
- Alinierea configurațiilor la politicile de securitate pentru minimizarea expunerii la vulnerabilități și îmbunătățirea performanței sistemului.

PR.PS-01.3

Organizația trebuie să identifice și să dezactiveze funcțiile, porturile, protocoalele și serviciile specifice din cadrul sistemelor sale critice care nu sunt necesare pentru operațiunile organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce suprafața de atac a sistemelor critice prin dezactivarea funcțiilor, porturilor, protocoalelor și serviciilor care nu sunt esențiale pentru operațiunile organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Identificarea caracteristicilor sistemului care nu sunt necesare pe baza rolului sistemului și a riscurilor asociate.
- Dezactivarea elementelor inutile pentru limitarea potențialelor puncte de intrare și reducerea mișcării laterale în cadrul rețelei.
- Evaluarea și actualizarea periodică a configurațiilor pentru reflectarea nevoilor operaționale și amenințărilor în continuă evoluție.
- Elementele care trebuie luate în considerare pentru dezactivare includ:
    - Bluetooth;
    - FTP;
    - Rețele peer-to-peer;
    - Alte servicii neutilizate sau vechi.

PR.PS-01.4

Organizația trebuie să implementeze măsuri de protecție tehnice pentru punerea în aplicare a unei politici de refuz total și permitere prin excepție, astfel încât să fie executate doar programele software autorizate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că numai software-ul autorizat în mod explicit este permis să ruleze, reducând riscul ca programe neautorizate sau cu scop nelegitim să afecteze sistemele critice. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Implementarea listei albe de aplicații pentru permiterea executării doar a programelor software aprobate.
- Utilizarea politicilor de grup pentru punerea în aplicare a regulilor de control al aplicațiilor în toate sistemele.
- Aplicarea Politicilor de restricție software (SRP) sau mecanisme similare pentru blocarea software-ului neautorizat pe baza căii de acces la fișier, a hash-ului sau a semnăturii digitale.
- Punerea în aplicare a RBAC pentru a asigura că numai utilizatorii autorizați pot rula anumite aplicații.
- Configurarea Java Security Manager pentru restricționarea claselor și metodelor care pot fi executate în medii bazate pe Java.
- Utilizarea instrumentelor de management al configurației pentru menținerea punerii în aplicare consecvente a software-ului autorizat în toate sistemele.

PR.PS-01.5

Modificările neautorizate ale configurației sistemelor organizației trebuie monitorizate și abordate cu măsuri de atenuare adecvate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a detecta și răspunde la modificările neautorizate ale configurației care ar putea compromite integritatea sau disponibilitatea sistemului.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Monitorizarea modificărilor de configurare în conformitate cu politicile și procedurile definite.
- Detecția și jurnalizarea modificărilor neautorizate ale setărilor sistemului.
- Alertarea personalului desemnat atunci când apar modificări neautorizate.
- Restabilirea promptă a configurațiilor aprobate pentru menținerea stabilității operaționale.
- În cazuri critice, oprirea proceselor sistemului afectat pentru prevenirea impactului suplimentar.
- Consultarea recomandărilor din Ghidul tehnic de implementare a NIS 2 elaborat de către ENISA, care recomandă monitorizarea continuă și atenuarea promptă a modificărilor neautorizate pentru păstrarea rezilienței și conformității sistemului.

PR.PS-02

Software-ul este menținut, înlocuit și eliminat în funcție de risc.

PR.PS-02.1

Organizația trebuie să pună în aplicare restricții privind utilizarea și instalarea software-ului și să se asigure că software-ul este menținut, înlocuit sau eliminat în funcție de riscul său asociat.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscurile operaționale și de securitate prin controlul software-ului utilizat, asigurarea menținerii corespunzătoare a acestuia și eliminarea sa atunci când nu mai este necesar sau nu mai este suportat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Permiterea doar a software-ului aprobat și restricționarea accesului în funcție de rolurile și responsabilitățile utilizatorilor.
- Înlocuirea software-ului nesuportat sau ajuns la EOL pentru evitarea vulnerabilităților fără patch-uri.
- Dezinstalarea software-ului neutilizat sau inutil, inclusiv utilitarele de sistem de operare învechite, pentru reducerea suprafeței de atac.
- Aplicarea patch-urilor în funcție de risc:
    - Vulnerabilităților critice ar trebui să le fie aplicate patch-uri în câteva ore.
    - Actualizările de rutină ar trebui să respecte un program stabilit (de exemplu, săptămânal sau lunar).
- În mediile containerizate, ar trebui utilizate doar imagini de încredere și actualizate; containerele învechite ar trebui înlocuite.
- Eliminarea sau dezactivarea software-ului și serviciilor care prezintă un risc inacceptabil, precum FTP sau instrumentele peer-to-peer, cu excepția cazului în care sunt explicit necesare și securizate.
- În mediile ICS/OT, asigurarea aprobării prealabile și a planificării programării PLC; evitarea modificărilor ad-hoc pentru protejarea siguranței operaționale.
- Menținerea unui inventar al software-ului cu versiunea și starea suportului.
- Definirea procedurilor pentru aprobarea, aplicarea de patch-uri, înlocuirea și eliminarea software-ului.

PR.PS-03

Hardware-ul este menținut, înlocuit și eliminat în funcție de risc.

PR.PS-03.1

Hardware-ul utilizat în mediile critice pentru activitate trebuie menținut, înlocuit sau eliminat în funcție de riscurile sale de securitate și operaționale asociate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că hardware-ul utilizat în medii critice pentru activitate rămâne securizat, fiabil și adecvat scopului, gestionându-l în funcție de riscurile operaționale și de securitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Evaluarea periodică a hardware-ului pentru a stabili dacă suportă funcționalitățile de securitate necesare (de exemplu, criptare, pornire securizată, actualizări de firmware); înlocuirea hardware-ului care nu poate satisface aceste cerințe.
- Retragerea treptată a hardware-ului EOL sau care nu mai este suportat, într-un mod controlat.
- Definirea și menținerea unui plan privind ciclul de viață al hardware-ului, care să includă:
  - Urmărirea inventarului;
  - Termene EOL;
  - Programele de înlocuire;
  - Proceduri de casare securizată.
- Efectuarea mentenanței preventive și a înlocuirilor la timp pentru evitarea defecțiunilor neașteptate care ar putea afecta operațiunile sau securitatea.
- Asigurarea faptului că hardware-ul poate susține rularea unui software securizat și actualizat, precum și abordarea oricăror limitări care împiedică acest lucru.

PR.PS-04

Înregistrările din jurnal sunt generate și puse la dispoziție pentru monitorizarea continuă.

PR.PS-04.1

Jurnalele trebuie menținute, documentate și monitorizate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că jurnalele sunt menținute, documentate și monitorizate în mod consecvent pentru sprijinirea vizibilității, răspunderii și detecției timpurii a anomaliilor sau amenințărilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Activarea jurnalizării în toate sistemele
    - Toate sistemele de operare, aplicațiile, serviciile (inclusiv cele bazate pe cloud) și instrumentele de securitate (de exemplu, firewall-uri, antivirus) ar trebui configurate pentru generarea înregistrărilor din jurnal.
- Includerea unei varietăți de tipuri de jurnale
    - Jurnalele ar trebui să includă, după caz: jurnale de audit, jurnale de evenimente, jurnale de aplicații, jurnale de securitate, jurnale de sistem și jurnale de mentenanță.
- Protejarea datelor din jurnale
    - Jurnalele ar trebui protejate împotriva accesului neautorizat prin criptare și controale de acces.
- Realizarea backup-urilor jurnalelor și păstrarea acestora
    - Realizarea periodică a backup-urilor jurnalelor și păstrarea pentru o perioadă predefinită, stabilită în funcție de necesitățile operaționale ale organizației sau de cerințele de reglementare aplicabile.
- Revizuirea jurnalelor pentru anomalii
    - Jurnalele ar trebui revizuite pentru detecția tiparelor sau comportamentelor neobișnuite, precum detecții repetate de malware sau acces excesiv la site-uri care nu sunt legate de activitatea profesională.
- Definirea perioadelor de păstrare
    - Perioadele de păstrare a jurnalelor ar trebui definite în mod clar. Luarea în considerare a cerințelor specifice sectorului.

- Sprijinirea monitorizării și a răspunderii
    - Monitorizarea ar trebui să fie implementată pentru a oferi vizibilitate asupra activității sistemului și pentru sprijinirea auditării eficace și a răspunsului la incidente.
- Includerea sistemelor OT
    - Practicile de jurnalizare ar trebui să fie extinse la mediile OT, inclusiv la ICS, unde jurnalele pot ajuta la detecția anomaliilor operaționale sau a încercărilor de acces neautorizat.

PR.PS-04.2

Organizația trebuie să se asigure că înregistrările din jurnale conțin o sursă de timp de referință sau o marcă temporală internă a ceasului, care este comparată și sincronizată cu o sursă de timp de referință.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că înregistrările din jurnale ale tuturor sistemelor utilizează o referință temporală consistentă și fiabilă, astfel încât evenimentele să poată fi urmărite și corelate cu precizie.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Utilizarea unei referințe de timp fiabile, precum un ceas GPS, un server de timp intern sau altă sursă de încredere pentru sincronizarea ceasurilor sistemului.
- Configurarea sistemelor pentru actualizarea ceasurilor periodic, pentru evitarea deviațiilor de timp.
- Configurarea mai multor surse de timp pentru asigurarea redundanței și preciziei.
- Monitorizarea stării sincronizării și declanșarea alertelor dacă sistemele nu mai sunt sincronizate.
- Documentarea procedurilor de sincronizare a timpului, inclusiv setările serverului, intervalele de actualizare și procesele de monitorizare.

PR.PS-04.3

Datele de audit din sistemele critice ale organizației trebuie transferate într-un sistem alternativ.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a proteja integritatea înregistrărilor de audit prin transferarea acestora din sistemele critice într-o locație separată și securizată, unde nu pot fi modificate sau falsificate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Transferul datelor de audit într-un sistem separat, unde înregistrările nu pot fi modificate de utilizatori sau servicii din sistemul original.
- Asigurarea faptului că sistemul de destinație păstrează înregistrările de audit nemodificate odată stocate.
- Monitorizarea impactului transferurilor de jurnale pentru evitarea problemelor de performanță pe sistemele sursă.
- Implementarea unor măsuri care protejează datele fără încetinirea sau perturbarea funcționării sistemului.

PR.PS-04.4

Organizația trebuie să se asigure că eșecurile de procesare a auditului din sistemele organizației generează alerte și declanșează răspunsuri definite.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că orice defecțiune în jurnalizarea auditului, precum erori în colectarea, procesarea sau stocarea jurnalelor, declanșează alerte și răspunsuri predefinite pentru menținerea integrității și trasabilității sistemului.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Eșecurile de audit ar trebui să includă probleme de software sau hardware, mecanisme de jurnalizare defecte sau stocare completă.
- Alertele ar trebui să fie generate automat atunci când apar astfel de eșecuri, iar acțiunile predefinite ar trebui declanșate pentru remediere.
- Fiecare depozit de jurnale de audit, fie că se află pe un server, un firewall sau o aplicație, ar trebui monitorizat individual și colectiv.
- Serverele protocolului de jurnalizare a sistemului (Syslog) sau soluții similare de jurnalizare centralizată ar trebui utilizate pentru sprijinirea colectării fiabile a jurnalelor și alertarea.
- Sistemele care generează jurnale ar trebui configurate astfel încât să înregistreze date detaliate privind activitatea, accesul și comportamentul, pentru susținerea principiilor zero-trust.
- Jurnalele de audit ar trebui monitorizate continuu pentru asigurarea disponibilității, integrității și capacității suficiente de stocare.

PR.PS-04.5

Organizația trebuie să se asigure că personalul autorizat poate extinde sau îmbunătăți capabilitățile de jurnalizare de audit și de monitorizare atunci când este necesar, pentru a sprijini investigațiile sau răspunsul la incidente.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că jurnalizarea auditului poate fi adaptată rapid pentru a oferi o vizibilitate mai profundă în timpul incidentelor de securitate sau al investigațiilor, fără a perturba operațiunile normale.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Sistemele de jurnalizare a auditului ar trebui să permită ajustări la cerere, precum creșterea detaliilor jurnalului, extinderea perioadei de păstrare sau extinderea acoperirii.
- Personalul autorizat și condițiile pentru activarea jurnalizării extinse ar trebui să fie clar definite.
- Procedurile de activare ar trebui să includă aprobări, documentație și urmărirea modificărilor.
- Înregistrările din jurnale ar trebui revizuite periodic pentru asigurarea acurateței și exhaustivității acestora în toate sistemele TIC și OT.
- Politicile ar trebui să asigure că jurnalizarea extinsă este utilizată doar atunci când este justificată și înregistrată corespunzător.
- Capacitatea tehnică, căile de escaladare și disponibilitatea personalului ar trebui planificate în prealabil pentru sprijinirea activării în timp util.

PR.PS-05

Instalarea și executarea software-ului neautorizat sunt prevenite.

PR.PS-05.1

Filtre web și e-mail trebuie instalate și utilizate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul de infectare cu malware, atacuri de phishing și breșe de date prin implementarea și menținerea unor soluții eficace de filtrare web și e-mail.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Implementarea filtrării web
    - Filtrele web ar trebui utilizate pentru a controla accesul la site-uri web pe baza:
        - Listelor predefinite de permisiuni/blocări (de exemplu, după URL sau domeniu).
        - Analizei conținutului în timp real pentru detecția conținutului cu scop nelegitim sau inadecvat.
        - Tehnicilor precum filtrarea URL, filtrarea conținutului, filtrarea DNS și filtrarea pe partea clientului sau a serverului.
- Configurarea filtrării e-mail
    - Filtrele de e-mail ar trebui configurate pentru:
        - Blocarea spamului, încercările de phishing și atașamentele sau linkurile cu scop nelegitim.
        - Clasificarea e-mailurilor primite (de exemplu, buletine informative, alerte de pe rețelele de socializare) pentru reducerea aglomerării și îmbunătățirea gradului de conștientizare.
        - Scanarea amenințărilor cunoscute și tiparelor suspecte pentru îmbunătățirea securității e-mailurilor.
- Menținerea filtrelor actualizate
    - Regulile de filtrare și bazele de date cu amenințări ar trebui actualizate periodic pentru a răspunde amenințărilor aflate în continuă evoluție.
- Integrarea cu politicile de securitate
    - Filtrarea web și e-mail ar trebui să fie aliniată cu politicile de securitate și eforturile de conștientizare ale organizației.

- Includerea considerațiilor specifice OT
    - În mediile OT, accesul la internet și e-mail ar trebui restricționat numai la ceea ce este necesar din punct de vedere operațional. Filtrarea ar trebui aplicată oricăror sisteme cu conectivitate externă pentru prevenirea expunerii la amenințări.

PR.PS-05.2

Instalarea și executarea de software neautorizat trebuie prevenite.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul de compromitere prin asigurarea faptului că pe sisteme sunt instalate și executate exclusiv aplicații software de încredere și aprobate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Instalarea și executarea software-ului ar trebui limitată la aplicații și medii preaprobate.
- Platformele ar trebui configurate pentru blocarea software-ului neautorizat și restricționarea executării acestuia în cazul în care riscul justifică aceasta.
- Sursa și integritatea tuturor programelor software noi ar trebui verificate înainte de instalare.
- Accesul la site-uri web dăunătoare ar trebui blocat folosind servicii de filtrare a internetului de încredere și aprobate, proiectate pentru detecția și oprirea amenințărilor online cunoscute.
- Acolo unde este fezabil, sistemele ar trebui configurate astfel încât să permită instalarea doar a software-ului aprobat de organizație.

PR.PS-06

Practicile securizate de dezvoltare a software-ului sunt integrate, iar performanța acestora este monitorizată pe tot parcursul ciclului de viață al dezvoltării software (SDLC).

PR.PS-06.1

Securitatea trebuie luată în considerare pe tot parcursul ciclului de viață al sistemelor și aplicațiilor, indiferent dacă acestea sunt dezvoltate intern sau achiziționate extern.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că securitatea este integrată în sisteme și aplicații de la început și este menținută pe toată durata ciclului de viață al acestora - de la proiectare până la retragere - indiferent dacă sunt dezvoltate intern sau achiziționate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Faza de inițiere
    - Cerințele de securitate ar trebui definite din timp, riscurile identificate, iar părțile interesate relevante, inclusiv experții în securitate, implicați de la început.
- Faza de achiziție sau dezvoltare
    - Pentru soluțiile achiziționate
        - Vânzătorii ar trebui să respecte practicile de dezvoltare securizată, să furnizeze dovezi ale testării și să îndeplinească cerințele contractuale de securitate.
    - Pentru dezvoltarea internă
        - Trebuie aplicate practici de codificare securizată, gestionate modificările și efectuate teste de securitate.
- Faza de implementare
    - Sistemele ar trebui configurate în mod securizat înainte de punerea în funcțiune, cu aplicarea controalelor de acces și a criptării pentru a proteja datele sensibile.
- Faza de operare și mentenanță
    - Sistemele ar trebui monitorizate pentru incidente, actualizate periodic, iar controalele de securitate revizuite și îmbunătățite în funcție de necesitate.

- Faza de casare
    - Sistemele ar trebui scoase din uz și dezafectate în mod securizat, datele sensibile eliminate, iar lecțiile învățate documentate pentru consolidarea proceselor viitoare.

PR.PS-06.2

Modificările și excepțiile trebuie testate și validate înainte de a fi implementate în sistemele operaționale.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul de întreruperi sau vulnerabilități, asigurând că toate modificările și excepțiile sunt testate și validate corespunzător înainte de a fi aplicate în sistemele operaționale.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Toate modificările și excepțiile propuse ar trebui să urmeze un proces formal care include documentarea, revizuirea, testarea și aprobarea.
- Riscurile potențiale ale aplicării sau neaplicării unei modificări ar trebui evaluate și înregistrate.
- Excepțiile, definite ca abateri aprobate de la politicile sau procedurile standard, ar trebui evaluate cu o înțelegere clară a riscurilor și un plan definit pentru reducerea sau gestionarea acestora.
- Riscurile acceptate ar trebui revizuite periodic pentru a confirma că decizia inițială de acceptare a acestora rămâne valabilă, în special dacă condițiile se modifică sau dacă acceptarea s-a bazat pe măsuri sau etape viitoare.
- Aceste practici ar trebui adaptate la mediul operațional pentru evitarea perioadelor de nefuncționare neplanificate sau a problemelor de siguranță, în special în sistemele OT.

PR.PS-06.3

Practicile de dezvoltare securizată a software-ului trebuie integrate în toate fazele ciclului de viață al dezvoltării software-ului, iar eficacitatea acestora ar trebui monitorizată și îmbunătățită periodic.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscurile de securitate în software prin integrarea măsurilor de protecție pe parcursul dezvoltării și îmbunătățirea continuă a acestora pe baza performanței și a amenințărilor în continuă evoluție.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Integrarea securității în ciclul de viață al dezvoltării
  - Ar trebui aplicate standarde de codificare securizată și cadre de dezvoltare de încredere.
  - Modelarea amenințărilor ar trebui efectuată din timp pentru a identifica și reduce riscurile.
  - Toate componentele software ar trebui protejate împotriva manipulării și accesului neautorizat.
  - Ar trebui puse în aplicare controale de acces pentru bazele de date și datele sensibile.
  - Dependențele software și bibliotecile ar trebui să fie actualizate.
  - Software-ul învechit sau neutilizat ar trebui eliminat în mod securizat.
- Monitorizarea eficacității practicilor de securitate
  - Ar trebui definiți și urmăriți indicatori, precum:
    - Vulnerabilitățile descoperite în timpul dezvoltării vs. în producție.
    - Timpul necesar pentru remedierea problemelor identificate.
    - Procentul de cod revizuit sau testat din punct de vedere al securității.
    - Participarea dezvoltatorilor la cursuri de instruire în domeniul codării securizate.
  - Acești indicatori ar trebui utilizați pentru identificarea lacunelor și îmbunătățirea practicilor.
- Consolidarea conștientizării privind securitatea
  - Dezvoltatorii și echipele tehnice ar trebui să primească instruire periodică privind principiile de codificare și proiectare securizate.

- Menținerea și îmbunătățirea
    - Practicile de dezvoltare securizată ar trebui revizuite și actualizate pe baza:
        - Noilor amenințări sau vulnerabilități.
        - Lecțiilor învățate din incidente sau audituri.
        - Standardelor din domeniu și a bunelor practici.

PR.PS-06.4

Pentru modificările planificate ale sistemelor critice ale organizației, trebuie efectuată o analiză a impactului asupra securității într-un mediu de testare separat, înainte de implementarea într-un mediu operațional.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a preveni riscurile de securitate neintenționate prin testarea modificărilor planificate ale sistemelor critice într-un mediu controlat înainte de punerea în funcțiune. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Planificarea scenariului de testare
    - Ar trebui identificate amenințările la adresa securității sistemelor, activelor, proceselor și persoanelor.
    - Modificările planificate ale configurației sau modificările sistemului ar trebui analizate în ceea ce privește impactul lor potențial asupra securității.
- Pregătirea mediului de testare
    - Datele de testare ar trebui să reflecte scenarii operaționale realiste.
    - Cerințele hardware, software și de rețea ar trebui definite clar.
    - Mediul de testare ar trebui să reflecte cât mai fidel mediul de producție în ceea ce privește instalarea și configurarea.
    - Ar trebui alocat spațiu suficient pe disc pentru activitățile de testare.
    - Versiunile software din mediul de testare ar trebui să corespundă cu cele din producție.
- Asigurarea securității și a mentenabilității
    - Software-ul din mediul de testare ar trebui actualizat periodic pentru remedierea vulnerabilităților cunoscute.
    - Tehnologiile de virtualizare sau containerizare ar trebui utilizate pentru crearea unor medii consecvente și replicabile.
    - VM-urile izolate ar trebui utilizate pentru a preveni interferența cu sistemele operaționale.
    - În mediul de testare ar trebui implementate controale de securitate, precum firewall-uri și restricții de acces.

[PR.IR] REZILIENȚA INFRASTRUCTURII TEHNOLOGICE

Arhitecturile de securitate sunt gestionate în conformitate cu strategia de management al riscului al organizației, pentru protejarea confidențialității, integrității și disponibilității activelor, precum și reziliența organizațională.

PR.IR-01

Rețelele și mediile sunt protejate împotriva accesului și utilizării logice neautorizate.

PR.IR-01.1

Firewall-urile trebuie instalate, configurate și menținute în mod activ pe toate rețelele utilizate de organizație pentru a proteja împotriva accesului neautorizat și a amenințărilor cibernetice.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura protejarea tuturor rețelelor utilizate de organizație împotriva accesului neautorizat și a amenințărilor cibernetice prin instalarea, configurarea și mentenanța activă a firewall-urilor.

Acest Control se concentrează pe instalarea, configurarea și mentenanța firewall-urilor la nivel de rețea pentru prevenirea accesului neautorizat prin monitorizarea și controlul traficului care intră sau iese din rețea (accent: control și prevenție). În schimb, Controlul DE.CM-01.1 se referă la firewall-urile la nivel de host, care contribuie la detecția amenințărilor care ocolesc perimetrul rețelei prin monitorizarea traficului către și de la dispozitive individuale (accent: vizibilitate și detecție).

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Protejarea perimetrului rețelei
    - Un firewall ar trebui instalat între rețeaua internă și internet. Acesta poate fi integrat într-un punct de acces wireless, un router sau un echipament furnizat de ISP.
    - Firewall-urile ar trebui configurate pe baza unei politici de securitate de bază, aplicând principiul refuză totul în mod implicit, permite numai excepțiile.
- Securizarea dispozitivelor endpoint
    - Un firewall software ar trebui instalat și actualizat periodic pe toate dispozitivele endpoint, inclusiv laptopuri, smartphone-uri și alte sisteme conectate la rețea.
    - Firewall-urile locale ar trebui să rămână active chiar și atunci când se utilizează VPN-uri sau servicii cloud.
- Securizarea mediilor de lucru de acasă și la distanță
    - Rețelele domestice utilizate pentru telemuncă ar trebui să utilizeze routere cu firewall integrat, care ar trebui activate, configurate în mod securizat și menținute actualizate.

- Firewall-urile software ar trebui să fie active și actualizate pe toate dispozitivele utilizate pentru munca la distanță.
- Datele de acces implicite ale administratorului ale routerelor domestice ar trebui modificate și actualizate periodic.

- Protejarea mediilor OT
  - Accesul la distanță la sistemele OT ar trebui tratat ca acces al unei părți terțe, nu ca telemuncă standard.
  - Ar trebui pusă în aplicare o separare clară între rețelele IT și OT.
  - Atunci când este necesar accesul IT-către-OT, acesta ar trebui să treacă printr-un host jump securizat situat într-o zonă demilitarizată (DMZ) dedicată.
- Îmbunătățirea detecției printr-un sistem de detecție și prevenire a intruziunilor (IDPS)
  - Un IDPS ar trebui avut în vedere pentru monitorizarea și analizarea traficului de rețea în vederea identificării activităților suspecte și pentru consolidarea protecției generale.

PR.IR-01.2

Pentru protejarea sistemelor critice, organizațiile trebuie să implementeze segmentarea și segregarea rețelelor în conformitate cu limitele de încredere și criticitatea activelor, limitând astfel propagarea amenințărilor și impunând un control strict al accesului.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a limita răspândirea amenințărilor cibernetice și a pune în aplicare un control strict al accesului prin implementarea segmentării și segregării rețelei pe baza limitelor de încredere și a criticității sistemelor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea zonelor de securitate
    - Rețelele ar trebui împărțite în zone distincte (de exemplu, birou, producție, vizitatori, mobil). Traficul dintre zone ar trebui monitorizat și controlat, de exemplu folosind firewall-uri.
- Alinierea segmentării cu încrederea și criticitatea
    - Segmentarea ar trebui să reflecte ce utilizatori și sisteme sunt de încredere și cât de critic este fiecare activ. Ar trebui permisă doar comunicarea esențială între zone, respectând principiul privilegiului minim.
- Evitarea rețelelor nesegmentate
    - Rețelele nesegmentate ar trebui evitate, deoarece compromiterea unui singur sistem poate expune întregul mediu. Segmentarea ar trebui să contribuie la izolarea amenințărilor într-o singură zonă.
- Separarea mediilor IT și OT
    - În mediile cu sisteme industriale (OT), rețelele de birou și de producție ar trebui separate. Rețelele pentru vizitatori și cele mobile nu ar trebui să aibă acces direct la sistemele interne de birou sau de producție. Segmentarea ar trebui să respecte standardul IEC 62443, în special cerințele SR 5.1 până la SR 5.3.
- Utilizarea VLAN-urilor cu prudență
    - VLAN-urile ar trebui utilizate doar ca parte a unei strategii de apărare în profunzime mai ample. Nu ar trebui să se bazeze numai pe acestea pentru îndeplinirea cerințelor de Securitate de Nivel 2 prevăzute în IEC 62443-3-3. VLAN-urile ar trebui combinate cu firewall-uri, controale de acces și monitorizare.

- Punerea în aplicare a segmentării prin firewall-uri
    - Firewall-urile ar trebui configurate să blocheze tot traficul în mod implicit și să permită doar conexiunile specifice, aprobate. Segmentarea și segregarea ar trebui puse în aplicare prin reguli de firewall bine menținute, în conformitate cu Controlul PR.IR-01.1.
- Clarificarea diferențelor dintre segmentare și segregare.
    - Segmentarea ar trebui utilizată pentru împărțirea în mod logic rețelelor și controlul traficului dintre zone.
    - Segregarea ar trebui aplicată acolo unde sistemele trebuie izolate, fără comunicare directă, cu excepția cazurilor permise explicit.

PR.IR-01.3

Pentru asigurarea stabilității și securității operaționale, organizația trebuie să identifice, documenteze și controleze conexiunile dintre componentele sistemelor sale critice, fără excepție.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a menține stabilitatea și securitatea operaționale prin asigurarea că toate conexiunile dintre componentele sistemelor critice sunt cunoscute, documentate și gestionate în mod activ.

În mediile OT, conexiunile nedocumentate sau necontrolate - fie ele fizice, wireless sau logice - pot introduce vulnerabilități, perturba procesele sau ocoli mecanismele de siguranță.

Pentru gestionarea și securizarea în mod eficace a conexiunilor de rețea între componentele sistemului, ar trebui luate în considerare următoarele practici:

- Managementul configurației
    - Organizațiile ar trebui să implementeze procese de management al configurației pentru a asigura că toate modificările aduse conexiunilor de rețea sunt documentate, revizuite și aprobate. Fișierele de configurare și jurnalele ar trebui să fie actualizate și menținute în mod securizat.
- Controale de acces
    - Ar trebui puse în aplicare controale stricte de acces pentru a asigura că numai personalul autorizat poate modifica configurațiile rețelei. RBAC ar trebui utilizat pentru restricționarea accesului în funcție de responsabilitățile postului și de necesitățile operaționale.
- Audituri periodice
    - Ar trebui efectuate audituri periodice pentru a verifica dacă toate conexiunile documentate rămân corecte și dacă nu au avut loc modificări neautorizate. Rezultatele auditului ar trebui utilizate pentru actualizarea documentației și consolidarea controalelor.
- Legătură cu Managementul activelor (ID.AM)
    - Conexiunile dintre componentele sistemului ar trebui documentate în ID.AM (Managementul activelor) și controlate în conformitate cu această cerință (PR.IR-01.3) pentru asigurarea coerenței, trasabilității și aplicabilității în arhitectura de securitate cibernetică din cadrul organizației.

PR.IR-01.4

Organizația trebuie să implementeze măsuri adecvate de protecție a granițelor pentru monitorizarea și controlul comunicațiilor la granițele externe și interne cheie ale sistemelor sale critice, atât în mediile IT, cât și în cele OT, pentru a asigura operațiuni securizate și fiabile.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura operațiuni securizate și fiabile prin monitorizarea și controlul activ al comunicațiilor la granițele cheie ale rețelei, în special acolo unde sistemele critice interacționează cu rețele externe sau zone interne mai puțin fiabile.

În mediile OT, unde sistemele vechi nu dispun adesea de securitate integrată, protecția granițelor este esențială pentru prevenirea accesului neautorizat, limitarea potențialelor amenințări și menținerea integrității proceselor în domeniile IT și OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Dispozitive de protecție a granițelor
    - Firewall-urile, gateway-urile de securitate și routerele ar trebui implementate la granițele externe și interne pentru punerea în aplicare a politicilor de filtrare și rutare a traficului. Aceste dispozitive ar trebui să funcționeze după modelul refuz implicit, acceptare prin excepție.
- Zonarea și izolarea în mediile OT
    - În mediile OT, protecția granițelor ar trebui să includă separarea strictă între sistemele de control și rețelele externe. Zonele ar trebui definite în funcție de criticitate și încredere, iar comunicațiile între zone ar trebui controlate și monitorizate cu strictețe.
- Gateway-uri unidirecționale (diode de date)
    - În cazul în care datele trebuie să circule de la sisteme OT securizate către destinații externe (de exemplu, servicii cloud sau autorități de reglementare), ar trebui utilizate gateway-uri unidirecționale pentru prevenirea amenințărilor interne, permițând în același timp transferul de date externe.
- Comunicații criptate
    - Comunicațiile care traversează granițele ar trebui criptate utilizând protocoale securizate (de exemplu, VPN, TLS) pentru protejarea datelor în tranzit și asigurarea confidențialității și integrității.

- Detecția și prevenirea intruziunilor
    - IDPS-urile ar trebui implementate la granițele cheie pentru monitorizarea traficului în vederea detecției anomaliilor, a încercărilor de acces neautorizat și blocarea activităților cu scop nelegitim.
- Punerea în aplicare a controlului accesului
    - Accesul la dispozitivele de graniță și canalele de comunicare ar trebui restricționat la personalul autorizat. Ar trebui luate în considerare soluții de control al accesului la rețea (NAC) pentru a pune în aplicare autentificarea dispozitivelor și a utilizatorilor la punctele de intrare.
- Monitorizarea continuă și aplicarea de patch-uri
    - Dispozitivele de graniță și canalele de comunicare ar trebui monitorizate continuu pentru detecția activităților suspecte. Toate sistemele expuse la comunicații externe sau interzonale ar trebui actualizate și remediate periodic pentru remedierea vulnerabilităților cunoscute.

PR.IR-01.5

Organizația trebuie să implementeze, acolo unde este fezabil, servere proxy autentificate sau firewall-uri cu filtrare URL și capabilități de informații privind amenințările pentru traficul de comunicații definit între sistemele sale critice și rețelele externe.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a reduce riscul de amenințări cibernetice care pătrund în sistemele critice, prin filtrarea și inspectarea comunicațiilor de ieșire și de intrare prin proxy-uri autentificate sau firewall-uri.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Controale de acces
    - Serverele proxy și firewall-urile ar trebui să pună în aplicare controale stricte de acces, permițând accesul numai utilizatorilor și sistemelor autorizate. Pentru susținerea principiilor zero-trust, ar trebui utilizate metode de autentificare puternice, precum MFA.
- Criptarea
    - Comunicațiile dintre clienți și serverele proxy ar trebui criptate utilizând cele mai recente și securizate versiuni ale SSL/TLS pentru protecție împotriva interceptării și atacurilor de tip man-in-the-middle.
- Informații privind amenințările și filtrarea URL-urilor
    - Pentru monitorizarea și controlul efectiv al comunicațiilor din mediile IT și OT, serverele proxy și firewall-urile ar trebui:
        - Să integreze fluxurile de informații privind amenințările pentru detecția și blocarea domeniilor, adreselor IP și URL-urilor cunoscute ca fiind cu scop nelegitim.
        - Să aplice filtrarea URL-urilor pentru împiedicarea accesului la conținut web dăunător sau neautorizat.
    - În mediile OT, unde sistemele nu dispun adesea de funcții de securitate integrate, ar trebui utilizată filtrarea inteligentă la granițele rețelei pentru:
        - Detecția și blocarea traficului cu scop nelegitim înainte ca acesta să ajungă la sistemele critice.
        - Prevenirea exfiltrării datelor și comunicarea externă neautorizată.
        - Punerea în aplicare a politicilor de comunicare fără perturbarea proceselor operaționale.

- Aceste măsuri ar trebui să facă parte dintr-o strategie de apărare pe mai multe niveluri, care să sprijine operațiuni securizate și fiabile atât în domeniul IT, cât și în cel OT.

- Jurnalizarea și monitorizarea
  - Jurnalizarea detaliată și monitorizarea continuă ar trebui activate pentru urmărirea accesului, detecția anomaliilor și sprijinirea răspunsului la incidente. Jurnalele ar trebui revizuite periodic pentru detecția semnelor de compromitere.
- Configurarea firewall-ului
  - Firewall-urile ar trebui configurate astfel încât să permită numai traficul autorizat în mod explicit către și dinspre serverele proxy. Ar trebui pusă în aplicare o politică de refuz implicit.
- Actualizări și aplicare de patch-uri periodice
  - Serverele proxy, firewall-urile și sistemele lor de bază ar trebui actualizate și să le fie aplicate patch-uri periodic pentru remedierea vulnerabilităților cunoscute și pentru menținerea eficacității securității.
- Performanță și fiabilitate
  - Echilibrarea sarcinii ar trebui utilizată pentru distribuirea traficului între mai multe servere proxy sau firewall-uri, asigurând o disponibilitate ridicată și o performanță optimă. Utilizarea resurselor ar trebui monitorizată pentru prevenirea supraîncărcării și degradării.

PR.IR-01.6

Organizația trebuie să se asigure că sistemele sale critice sunt proiectate astfel încât să cedeze în mod securizat și să rămână protejate în cazul unei defecțiuni operaționale a unui dispozitiv de protecție a granițelor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că sistemele critice rămân protejate și nu devin expuse sau vulnerabile în cazul în care un firewall, un proxy sau alt dispozitiv de protecție a granițelor se defectează.

În mediile OT, unde disponibilitatea și siguranța sunt esențiale, sistemele ar trebui proiectate astfel încât să cedeze în mod securizat, de exemplu, trecând în mod implicit la o stare de refuz total, izolând segmentele afectate sau declanșând alerte, astfel încât o defecțiune a unei componente să nu compromită întregul sistem și să nu permită accesul neautorizat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Configurație sigură în caz de defecțiune
    - Dispozitivele ar trebui configurate astfel încât să treacă automat într-o stare sigură (de exemplu, să blocheze tot traficul) în cazul unei defecțiuni, pentru prevenirea accesului neautorizat sau scurgerea de date.
- Redundanță și disponibilitate ridicată
    - Ar trebui să existe sisteme redundante sau mecanisme de failover pentru asigurarea protecției continue. Evitarea punctelor unice de eșec, în special în mediile OT în care timpul de funcționare este critic.
- Testare și mentenanță periodică
    - Mecanismele de failover și configurațiile sigure în caz de defecțiune ar trebui testate periodic. Mentenanța ar trebui să asigure menținerea dispozitivelor într-o stare sigură și funcțională.
- Integritatea controlului accesului
    - Listele de control al accesului (ACL) și politicile de securitate ar trebui să rămână protejate și nemodificate în timpul defecțiunilor, pentru menținerea posturii de securitate a sistemului.
- Monitorizarea și alertele
    - Monitorizarea și alertarea în timp real ar trebui implementate pentru detecția rapidă a defecțiunilor și inițierea acțiunilor corective.

- Segmentarea și izolarea
    - Proiectarea rețelei ar trebui să includă segmentarea și izolarea pentru limitarea impactului unei defecțiuni și pentru prevenirea efectelor în cascadă asupra sistemelor.

Aceste practici sunt aliniate cu standardele recunoscute, inclusiv NIST SP 800-53 Rev. 5, NIST SP 800-53A și IEC 62443-3-3 SR 5.2 RE 3 - Fail Close, care pun accentul pe siguranța în caz de defecțiune și reziliența sistemelor de infrastructură critică.

PR.IR-01.7

Organizația trebuie să asigure că mediile de dezvoltare și testare sunt strict separate de mediul de producție, în special în sistemele ICS/OT, unde orice încrucișare ar putea compromite siguranța, pune în pericol sănătatea sau perturba operațiunile esențiale.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a preveni întreruperile neintenționate, riscurile de siguranță sau încălcările de securitate, asigurând că activitățile de dezvoltare și testare nu interferează cu sistemele operaționale active.

În mediile OT, precum ICS, chiar și cele mai mici interferențe între testare și producție pot conduce la condiții nesigure, întreruperi ale proceselor sau expunerea configurațiilor sensibile. Separarea strictă contribuie la menținerea integrității sistemului, sprijină controlul modificărilor și reduce riscul de acțiuni accidentale sau rău intenționate care afectează operațiunile critice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Separarea strictă a mediilor
    - Activitățile de dezvoltare și testare ar trebui desfășurate în medii separate fizic sau logic de mediul de producție. Aceasta este deosebit de critică în mediile ICS/OT, unde siguranța și fiabilitatea operațională nu trebuie compromise.
- Testarea înainte de punerea în funcțiune
    - Orice modificare destinată mediului TIC sau OT ar trebui testată mai întâi într-un mediu care nu este de producție. Aceasta permite evaluarea impactului potențial și a ajustărilor necesare înainte de punerea în funcțiune.
- Medii de testare realiste
    - Mediile de testare ar trebui să reproducă cât mai fidel mediul de producție în ceea ce privește configurația, arhitectura și fluxul de date, pentru a asigura rezultate precise ale testării.
- Practici de dezvoltare sigure
    - Funcționalitățile de securitate cibernetică ar trebui integrate și testate cât mai devreme posibil în ciclul de viață al dezvoltării, respectând principiile SDLC.

PR.IR-01.8

Organizația trebuie să definească, monitorizeze și controleze fluxul de informații și date în cadrul și între sistemele sale critice pentru a asigura că au loc numai schimburi autorizate și sigure, indiferent de granițele rețelei sau de arhitectura sistemului.

GHID DE IMPLEMENTARE

Această cerință se bazează pe PR.IR-01.3 (controlul conexiunilor sistemului) și PR.IR-01.4 (protecția granițelor), dar merge mai departe, concentrându-se pe ce date pot fi transferate, unde și în ce condiții - nu doar pe modul în care sistemele sunt conectate sau segmentate.

De asemenea, aceasta completează Controlul ID.AM-03.2, care prevede identificarea, documentarea, autorizarea și actualizarea comunicațiilor de rețea și a fluxurilor interne de date. Controlul PR.IR-01.8 asigură că aceste fluxuri documentate sunt, de asemenea, puse în aplicare și monitorizate în mod activ.

Controlul fluxurilor de informații și date este deosebit de critic în mediile ICS/OT, unde orice schimb neautorizat sau neintenționat de date poate compromite sănătatea, siguranța și protecția mediului și, prin urmare, trebuie strict reglementat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea și punerea în aplicare a politicilor de control al fluxurilor
    - Ar trebui utilizate instrumente și politici pentru a controla modul în care datele circulă între sisteme și în diferite părți ale rețelei, asigurând că au loc numai fluxuri autorizate.
- Criptarea datelor în tranzit și în repaus
    - Utilizarea protocoalelor de criptare sigure, precum TLS/SSL pentru datele în tranzit și AES-256 pentru datele stocate, pentru protejarea confidențialității și integrității.
- Utilizarea MFA
    - MFA ar trebui implementat pentru verificarea identității utilizatorilor care accesează sisteme care gestionează sau transmit date sensibile.
- API-uri sigure
    - API-urile utilizate pentru comunicarea între sisteme ar trebui să respecte practicile de dezvoltare securizate și să fie revizuite periodic pentru identificarea vulnerabilităților.
- Implementarea monitorizării continue
    - Instrumentele de monitorizare în timp real ar trebui să detecteze fluxurile de date neautorizate sau anomaliile, însoțite de mecanisme de alertare care să permită intervenția imediată și gestionarea promptă a incidentelor.

- Efectuarea de audituri periodice
    - Auditurile periodice ar trebui să verifice conformitatea cu politicile privind fluxul de date și să identifice potențialele puncte slabe sau modificările neautorizate.
- Aplicarea segmentării rețelei
    - Segmentarea rețelei pentru restricționarea fluxurilor de date inutile şi limitarea impactului potențialelor încălcări.
- Securizarea accesului la distanță
    - VPN-urile ar trebui utilizate pentru conectarea în mod securizat a sistemelor și utilizatorilor la distanță la rețeaua organizației.
- Implementarea DLP
    - Soluțiile DLP ar trebui să monitorizeze și să controleze transferul de informații sensibile, în special atunci când părăsesc organizația.
- Instruirea personalului și conștientizarea
    - Angajații ar trebui instruiți cu privire la politicile de gestionare a datelor și la importanța controlului fluxurilor de informații.
- Simularea atacurilor de phishing
    - Ar trebui efectuate simulări regulate de phishing pentru reducerea riscului de atacuri de inginerie socială.

PR.IR-01.9

Organizația trebuie să gestioneze interfețele cu serviciile externe de telecomunicații ca parte a politicii sale mai ample de securitate a rețelei, definind modul în care este controlat traficul, asigurând confidențialitatea și integritatea informațiilor transmise și revizuind și documentând orice excepții de la regulile stabilite.

GHID DE IMPLEMENTARE

Acest Control se bazează pe PR.IR-01.8, concentrându-se în mod specific pe modul în care comunicațiile externe sunt reglementate în cadrul politicii de securitate a rețelei organizației. În timp ce configurațiile firewall-ului și setările de securitate de bază asigură punerea în aplicare tehnică, această cerință pune accentul pe politica și nivelul de supraveghere.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Integrarea gestionării fluxului de trafic în politica de securitate a rețelei
    - Politica de securitate a rețelei ar trebui să includă reguli clare privind modul în care traficul de date și voce poate circula între sistemele interne și serviciile de telecomunicații externe.
- Definirea obiectivelor și a domeniului de aplicare al securității
    - Politica ar trebui să prezinte obiectivele de protejare a comunicațiilor externe și să specifice sistemele și serviciile acoperite.
- Controlul și monitorizarea traficului
    - Traficul de rețea ar trebui monitorizat continuu pentru a asigura că respectă regulile definite. Fluxurile suspecte sau neautorizate ar trebui să declanșeze alerte și să fie investigate.
- Protejarea datelor în tranzit
    - Confidențialitatea și integritatea datelor transmise ar trebui protejate utilizând protocoale de criptare, precum TLS/SSL.
- Documentarea și revizuirea excepțiilor
    - Orice excepții de la regulile privind fluxul de trafic (de exemplu, accesul temporar al unei părți terțe) ar trebui documentate în mod formal, justificate și revizuite periodic.
- Răspunsul la incidente
    - Organizația ar trebui să fie pregătită să izoleze și să răspundă rapid la tiparele de trafic anormale sau cu scop nelegitim.

- Menținerea alinierii politicilor
    - Componenta fluxului de trafic ar trebui să fie aliniată cu alte elemente ale politicii de securitate a rețelei, inclusiv controlul accesului, utilizarea VPN, managementul patch-urilor și răspunsul la incidente.

PR.IR-02

Activele tehnologice ale organizației sunt protejate împotriva amenințărilor de mediu.

PR.IR-02.1

Organizația trebuie să definească, implementeze și mențină politici și proceduri legate de sistemele de urgență și siguranță, sistemele de protecție împotriva incendiilor și controalele de mediu pentru sistemele sale critice.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a proteja sistemele critice împotriva riscurilor de mediu și a situațiilor de urgență care ar putea perturba operațiunile, deteriora echipamentele sau pune în pericol siguranța - în special în mediile OT, unde condițiile fizice au un impact direct asupra disponibilității sistemului și siguranței umane.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Efectuarea evaluărilor riscurilor pentru toate locațiile care găzduiesc sisteme critice, pentru identificarea riscurilor de mediu și de urgență.
- Definirea politicilor și procedurilor pentru protecția împotriva incendiilor, răspunsul la situații de urgență și controalele de mediu.
- Instalarea unor sisteme de monitorizare, precum senzori de temperatură, umiditate, fum și scurgeri de apă, cu alerte pentru condiții anormale.
- Implementarea măsurilor de protecție împotriva incendiilor, inclusiv sisteme adecvate de stingere (de exemplu, pe bază de gaz pentru centrele de date), alarme, detectoare și stingătoare.
- Inspectarea și menținerea regulată a sistemelor de siguranță împotriva incendiilor și de protecție a mediului, inclusiv sistemele de încălzire, ventilație și climatizare (HVAC) și iluminatul de urgență.
- Includerea cerințelor de protecție a mediului în contractele cu părți terțe și solicitarea unor dovezi de conformitate și mentenanță.
- Instruirea personalului cu privire la procedurile de urgență și organizarea de exerciții de evacuare și intervenție în caz de incendiu cel puțin anual.

PR.IR-02.2

Organizația trebuie să implementeze dispozitive de detecție a incendiilor care se activează și notifică automat personalul cheie în cazul unui incendiu.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura detecția timpurie a incidentelor de incendiu și alertarea automată a personalului cheie, pentru a permite o reacție rapidă și coordonată, în special în medii în care sistemele critice susțin siguranța sau operațiunile esențiale.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Implementarea unor sisteme automate de detecție a incendiilor care utilizează detectoare de fum și căldură și se activează fără intervenție manuală.
- Integrarea detecției incendiilor cu sisteme automate de stingere, acolo unde este cazul (de exemplu, sprinklere sau sisteme pe bază de gaz).
- Configurarea sistemelor astfel încât să notifice automat personalul desemnat sau echipele de intervenție în caz de urgență la activare.
- Definirea și menținerea unei liste de notificări cu roluri atribuite clar, asigurând că persoanele fizice au accesul și autorizația necesare, în special în medii sensibile sau clasificate.

PR.IR-03

Mecanismele pentru îndeplinirea cerințelor de reziliență în situații normale și adverse sunt implementate.

PR.IR-03.1

Organizația trebuie să implementeze mecanisme pentru a asigura că sistemele și serviciile critice rămân operaționale sau pot fi repuse rapid în funcțiune atât în condiții normale de funcționare, cât și în condiții adverse.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că sistemele și serviciile critice rămân operaționale sau pot fi repuse rapid în funcțiune, atât în condiții normale de funcționare, cât și în condiții adverse, precum atacuri cibernetice, defecțiuni hardware sau dezastre naturale.

Acest Control susține obiectivul mai larg al rezilienței operaționale. În timp ce redundanța (astfel cum este abordată în GV.OC-04.3) contribuie la prevenirea întreruperilor prin duplicarea componentelor, reziliența asigură că operațiunile pot continua sau pot fi restabilite rapid chiar și atunci când apar defecțiuni. Ambele sunt esențiale pentru menținerea disponibilității în medii IT și OT complexe.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea obiectivelor de reziliență
  - Identificarea sistemelor critice și definirea valorilor acceptabile ale RTO și RPO.
  - Alinierea obiectivelor de reziliență cu BCP și DRP.
- Proiectarea pentru reziliență
  - Implementarea arhitecturilor tolerante la erori (de exemplu, clustering, echilibrarea sarcinii, redundanța geografică).
  - Utilizarea diverselor tehnologii și furnizori pentru reducerea dependenței de puncte unice de eșec.
- Asigurarea pregătirii operaționale
  - Testarea regulată a sistemelor de failover prin simulări și comutări.
  - Menținerea procedurilor operaționale și instrucțiunilor de recuperare actualizate și exacte.
- Consolidarea rezilienței cibernetice
  - Integrarea strategiilor de reziliență în IRP-uri (de exemplu, limitarea ransomware-ului, restaurarea datelor).

- Utilizarea backup-urilor imuabile și segmentarea rețelei pentru limitarea impactului incidentelor cibernetice.

- Evaluarea rezilienței părților terțe
  - Evaluarea rezilienței furnizorilor de servicii critice și documentarea concluziilor.
  - Includerea cerințelor de reziliență și recuperare în SLA-uri.
- Promovarea îmbunătățirii continue
  - Revizuirea și actualizarea mecanismelor de reziliență după incidente sau modificări majore.
  - Încorporarea lecțiilor învățate în planificarea și testarea viitoare.

PR.IR-04

Capacitatea adecvată a resurselor pentru asigurarea disponibilității este menținută.

PR.IR-04.1

Planificarea adecvată a capacității resurselor trebuie să asigure menținerea disponibilității sistemelor critice ale organizației pentru procesarea informațiilor, rețelele, telecomunicațiile și stocarea datelor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că sistemele critice dispun în permanență de suficiente resurse de calcul, stocare și rețea, prin planificarea în avans a necesităților actuale și viitoare de capacitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Previzionare și planificare
    - Nevoile de resurse ar trebui previzionate periodic, pe baza creșterii organizației, a tiparelor sezoniere și a tendințelor de utilizare. Cererea viitoare de capacitate de calcul, stocare și rețea trebuie anticipată pentru prevenirea problemelor de performanță sau întreruperilor.
- Luarea în considerare a termenelor de aprovizionare
    - Planificarea capacității ar trebui să considere potențialele întârzieri în livrarea hardware-ului sau a serviciilor din cauza perturbărilor lanțului de aprovizionare sau a celor geopolitice. Ar trebui menținută o capacitate tampon pentru a absorbi cererea neașteptată sau întârzierile de expansiune.
- Monitorizarea și stabilirea pragurilor
    - Sistemele ar trebui monitorizate continuu pentru urmărirea utilizării. Pragurile și alertele ar trebui configurate pentru declanșarea acțiunilor de scalare în timp util, înainte ca performanța să fie afectată.
- Utilizarea componentelor cu disponibilitate ridicată
    - Componentele redundante (de exemplu, matrice RAID, interfețe de rețea duale, surse de alimentare de rezervă) ar trebui implementate pentru reducerea timpului de nefuncționare cauzat de defecțiuni hardware. Acestea ar trebui să completeze, nu să înlocuiască, planificarea capacității.

- Revizuirea şi ajustarea periodică
    - Planurile de capacitate ar trebui revizuite periodic și actualizate în funcție de modificările în strategia organizației, tehnologie sau factori externi de risc.

DETECȚIE

[DE.CM] MONITORIZARE CONTINUĂ

Activele sunt monitorizate pentru identificarea anomaliilor, indicatorilor de compromitere (IoC) și alte evenimente potențial adverse.

DE.CM-01

Rețelele și serviciile de rețea sunt monitorizate pentru identificarea evenimentelor potențial adverse.

DE.CM-01.1

Firewall-urile trebuie instalate și operate la granițele rețelei, inclusiv firewall-urile la nivel de endpoint.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a îmbunătăți vizibilitatea și detecția amenințărilor la nivel de dispozitiv, în special a celor care pot ocoli sistemele tradiționale de apărare a perimetrului rețelei.

Acest Control se concentrează pe utilizarea firewall-urilor la nivel de host pentru detecția amenințărilor care pot ocoli perimetrul rețelei, prin monitorizarea și controlul traficului către și de la dispozitive individuale (accent: vizibilitate și detecție). În schimb, Controlul PR.IR-01.1 se referă la firewall-urile la nivel de rețea, care sunt proiectate pentru prevenirea accesului neautorizat prin gestionarea traficului care intră sau iese din rețea (accent: control și prevenție).

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea endpoint-urilor în sens larg
    - Ar trebui incluse desktop-uri, laptop-uri, servere, smartphone-uri și, acolo unde este fezabil, componente OT precum PLC-uri și HMI-uri, precum și dispozitive IoT.
- Implementarea firewall-urilor la nivel de host
    - Asigurarea instalării, activării și configurării corespunzătoare a mecanismelor de tip firewall la nivelul tuturor dispozitivelor endpoint. Aceste firewall-uri contribuie la detecția și blocarea activităților suspecte direct la nivelul dispozitivului, chiar și atunci când acesta este conectat la rețele securizate sau VPN-uri.
- Segmentarea activelor de rețea
    - Gruparea sistemelor în funcție de criticitatea sau funcția lor (de exemplu, plasarea serviciilor publice, precum serverele de e-mail, web și VPN, într-o zonă DMZ).
- Utilizarea regulilor predefinite pentru firewall
    - Stabilirea unor reguli pentru filtrarea traficului de intrare și de ieșire, contribuind astfel la detecția anomaliilor sau a comportamentelor rău intenționate.

- Limitarea punctelor de acces de internet
    - Reducerea numărului de puncte de interconectare la internet pentru minimizarea expunerii și simplificarea monitorizării.

DE.CM-01.2

Programele antivirus, antispyware și alte programe antimalware trebuie instalate și actualizate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate dispozitivele organizației (active IT și OT) sunt protejate împotriva software-ului cu scop nelegitim, prin implementarea și actualizarea periodică a instrumentelor antimalware.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Domeniul de aplicare al protecției
  - Dispozitive IT
    - Instalarea software-ului antimalware pe toate dispozitivele utilizatorilor și ale sistemului, inclusiv desktop-uri, laptop-uri, servere, smartphone-uri și tablete.
  - Dispozitive OT
    - Extinderea protecției la active OT, precum PLC-uri, HMI-uri, servere SCADA și stații de lucru ale inginerilor, acolo unde este fezabil din punct de vedere tehnic.
- Practici de actualizare și scanare
  - IT
    - Configurarea instrumentelor antimalware pentru actualizare în timp real sau cel puțin zilnic, urmată de scanări automate sau programate.
  - OT
    - Planificarea cu atenție a actualizărilor și scanărilor pentru evitarea întreruperii operaționale. Utilizarea ferestrelor de mentenanță și testarea actualizărilor înainte de punerea în funcțiune.
- Soluții personalizate pentru OT
  - Utilizarea instrumentelor antimalware ușoare sau specifice OT, compatibile cu sistemele în timp real.
  - Pentru dispozitivele OT vechi sau cu resurse limitate, ar trebui luate în considerare:
    - Lista albă a aplicațiilor.
    - Detecția malware-ului la nivel de rețea.

        - Utilizarea instrumentelor specializate care monitorizează în mod silențios sistemele industriale pentru detecția activităților neobișnuite sau suspecte, fără a interfera cu modul de funcționare al sistemelor (monitorizare pasivă).

- Munca la distanță și utilizarea dispozitivelor electronice personale (BYOD)
    - Aplicarea acelorași standarde de protecție pentru:
        - Calculatoarele personale utilizate pentru telemuncă.
        - Dispozitive personale (BYOD) utilizate pentru sarcini profesionale.
    - Utilizarea platformelor de protecție a endpoint-urilor pentru punerea în aplicare a politicilor pe toate dispozitivele.
- Gestionare și monitorizare centralizate
    - Utilizarea unor instrumente centralizate pentru a gestiona configurațiile, actualizările și alertele antimalware atât în mediile IT, cât și în cele OT.
    - Integrarea alertelor malware în procesele mai ample de monitorizare a securității și de răspuns la incidente ale organizației.
- Îmbunătățirea continuă
    - Revizuirea și testarea periodică a eficacității soluțiilor antimalware.
    - Actualizarea politicilor și instrumentelor pe baza amenințărilor emergente și a lecțiilor învățate din incidente.

DE.CM-01.3

Organizația trebuie să monitorizeze și identifice utilizarea neautorizată a sistemelor sale critice pentru activitate prin detecția conexiunilor locale neautorizate, a conexiunilor de rețea și a conexiunilor la distanță.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația poate detecta și răspunde la accesul neautorizat sau utilizarea abuzivă a sistemelor sale critice pentru activitate. Aceasta include identificarea conexiunilor locale, de rețea sau la distanță suspecte care ar putea indica o breșă de securitate sau utilizarea abuzivă a sistemelor sensibile.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Monitorizarea comunicațiilor de rețea ar trebui să fie realizată la granița externă a sistemelor organizației critice pentru activitate și la granițele cheie interne din cadrul acestor sisteme.
- Incintele ar trebui monitorizate pentru detecția rețelelor wireless neautorizate sau frauduloase care ar putea permite atacatorilor să ocolească controalele normale.
- Serviciile critice de rețea, precum DNS - care traduce numele site-urilor web în adrese IP, protocol de rutare inter-domenii (BGP) - care ajută la rutarea traficului de internet, și alte servicii de rețea, ar trebui monitorizate pentru detecția semnelor de manipulare sau utilizare abuzivă.
- Atunci când sunt găzduite aplicații accesibile de pe internet, ar trebui luată în considerare utilizarea unui firewall pentru aplicații web (WAF) pentru protecție împotriva atacurilor. Dacă aplicația nu este bazată pe web, aceasta ar trebui protejată utilizând alte metode adecvate, precum un IdP pentru controlul accesului.

DE.CM-01.4

Organizația trebuie să monitorizeze continuu rețeaua sa pentru detecția semnelor de amenințări cibernetice sau activități neobișnuite, utilizând reguli clar definite pentru ceea este considerat un potențial incident de securitate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația monitorizează în mod continuu rețeaua și sistemele sale pentru detecția semnelor de amenințări cibernetice sau activități neobișnuite. Aceasta se realizează utilizând reguli clar definite care contribuie la identificarea a ceea este calificat drept un potențial incident de securitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Acest Control se bazează pe DE.AE-08.1, care impune raportarea incidentelor pe baza unor criterii predefinite.
- Organizația ar trebui să decidă ce tipuri de evenimente de securitate cibernetică și semne de avertizare trebuie monitorizate și să definească ce informații trebuie înregistrate în jurnalele de audit.
- Ar trebui utilizate instrumente automatizate pentru detecția activităților suspecte, precum traficul neașteptat în rețea, încercările eșuate de autentificare sau setările incorecte ale sistemului.
- Monitorizarea ar trebui să fie flexibilă și să fie intensificată în perioadele cu risc ridicat, precum atunci când sunt primite alerte de amenințare, în timpul tensiunilor geopolitice sau după apariția unor probleme interne.
- Monitorizarea ar trebui să includă nu numai sistemele digitale, ci și spațiile fizice, comportamentul personalului și interacțiunile cu furnizorii de servicii, acolo unde este relevant.
- Activitatea rețelei ar trebui analizată în mod continuu pentru detecția modificărilor care ar putea indica o slăbire a securității, urmând principiile zero-trust.
- Alertele ar trebui să fie declanșate automat atunci când sunt atinse anumite praguri, iar alarmele false cunoscute ar trebui filtrate pentru evitarea suprasolicitării personalului.

DE.CM-02

Mediul fizic este monitorizat pentru identificarea evenimentelor potențial adverse.

DE.CM-02.1

Mediul fizic trebuie monitorizat pentru identificarea evenimentelor potențial adverse.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că spațiile fizice în care se află sistemele și datele critice sunt monitorizate pentru detecția semnelor de activități suspecte sau dăunătoare. Acest Control contribuie la detecția potențialelor amenințări, precum accesul neautorizat, manipularea sau alte evenimente neobișnuite în mediul fizic.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Jurnalele sistemelor de acces fizic (precum cititoarele de cartele) ar trebui revizuite pentru detecția tiparelor neobișnuite, precum încercările de acces la ore neobișnuite sau încercările de acces repetate eșuate într-o zonă restricționată.
- Înregistrările accesului vizitatorilor (precum foile de înregistrare sau înregistrările digitale) ar trebui revizuite periodic pentru a asigura că numai persoanele fizice care sunt autorizate au intrat în zonele securizate.
- Echipamentele de securitate fizică (precum încuietori, zăvoare, ştifturi pentru balamale și alarme) ar trebui verificate pentru detecția semnelor de manipulare sau deteriorare care ar putea indica o tentativă de încălcare a securității.

DE.CM-02.2

Accesul fizic la sistemele și dispozitivele critice ale organizației, pe lângă monitorizarea accesului fizic la incintă, trebuie completat cu alarme de intruziune fizică, echipamente de supraveghere și echipe de monitorizare independente.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida protecția sistemelor și dispozitivelor critice prin completarea monitorizării fizice de bază a accesului cu detecția activă a intruziunilor, tehnologii de supraveghere și capabilități independente de monitorizare. Aceasta contribuie la asigurarea detecției și răspunsului în timp util la amenințările la adresa securității fizice.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Sistemele de detecție a intruziunilor ar trebui să fie instalate pentru a identifica încercările de intrare fizică neautorizată. Aceste sisteme pot include senzori de mișcare, senzori de contact pentru uși/ferestre și detectoare de spargere a geamurilor, care declanșează alerte atunci când sunt detectate activități neobișnuite.
- Tehnologiile de supraveghere, precum camerele CCTV, sistemele de înregistrare video și sistemele de control al accesului, ar trebui utilizate pentru monitorizarea și înregistrarea în mod continuu a activității din zonele sensibile. Aceste sisteme contribuie la verificarea incidentelor și sprijină investigațiile.
- Monitorizarea vizitatorilor ar trebui intensificată prin jurnalizarea tuturor intrărilor, inclusiv a contractorilor și a personalului temporar, utilizând sisteme digitale sau jurnale manuale.
- Echipe independente de monitorizare, de obicei formate din profesioniști externi în domeniul securității, ar trebui angajate pentru supravegherea sistemelor de supraveghere și pentru răspunsul la incidente. Aceste echipe aduc expertiză specializată și operează separat de personalul intern, fiind important să fie aplicate cerințele de securitate cibernetică ale părților terțe la operațiunile lor.
- Supravegherea și detecția intruziunilor ar trebui integrate în operațiuni de securitate mai ample, permițând corelarea alertelor cu alți IoC fizici și digitali.

DE.CM-03

Activitatea personalului și utilizarea tehnologiei sunt monitorizate pentru identificarea evenimentelor potențial adverse.

DE.CM-03.1

Trebuie implementate instrumente de protecție a endpoint-urilor și a rețelei pentru monitorizarea comportamentului utilizatorilor finali în ceea ce privește activitățile periculoase.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația poate detecta și răspunde la comportamentul riscant sau suspect al utilizatorilor atât pe dispozitive, cât și în rețele. Acest Control contribuie la identificarea amenințărilor, precum infectare cu malware, utilizarea abuzivă a sistemelor sau încercările de ocolire a controalelor de securitate, indiferent dacă sunt cauzate de atacatori externi sau interni.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Organizațiile ar trebui să ia în considerare utilizarea unei îmbinări de instrumente moderne de securitate care funcționează împreună pentru oferirea unei imagini complete a activității utilizatorilor și a sistemului:
  - IDPS
    - Aceste instrumente monitorizează traficul de rețea și pot bloca sau alerta în cazul activităților suspecte, precum încercările de piratare sau exploatarea vulnerabilităților.
  - WAF-uri și gateway-uri API
    - Acestea contribuie la protejarea aplicațiilor și serviciilor online prin filtrarea traficului dăunător și prevenirea accesului neautorizat.
- În plus, o abordare stratificată care utilizează instrumente avansate de detecție și răspuns poate oferi vizibilitate în timp real și un răspuns mai rapid:
  - Detecție și răspuns la nivel de endpoint (EDR)
    - Monitorizează activitatea pe dispozitive individuale (precum laptopuri sau servere) pentru detecția unor amenințări precum malware sau acces neautorizat.
  - Detecție și răspuns la nivel de rețea (NDR)
    - Analizează traficul de rețea pentru identificarea tiparelor neobișnuite, precum mișcări laterale sau atacuri ascunse.

- Detecție și răspuns la amenințări de identitate (ITDR)
  - Se concentrează pe detecția utilizării abuzive a conturilor de utilizator, precum date de acces furate sau amenințări din interior.
- UEBA
  - Utilizează învățarea automată pentru înțelegerea comportamentului normal și detecția anomaliilor care pot indica o amenințare.

- Aceste instrumente fac parte dintr-o strategie modernă de securitate pe mai multe niveluri și sunt adesea menționate în cele mai bune practici și cadre din industrie, precum Triada de vizibilitate a centrului de operațiuni de securitate (SOC) introdusă de Gartner.

DE.CM-03.2

Instrumentele de protecție a endpoint-urilor și a rețelei care monitorizează comportamentul utilizatorilor finali în vederea detecției activităților periculoase trebuie gestionate.

GHID DE IMPLEMENTARE

Acest Control se bazează pe DE.CM-03.1, mutând accentul de la implementare la gestionarea continuă a instrumentelor de monitorizare. Obiectivul acestui Control este de a asigura că instrumentele utilizate pentru monitorizarea comportamentului utilizatorilor și detecția activităților dăunătoare pe dispozitive și rețele sunt menținute corespunzător și gestionate în mod activ. Aceasta susține eficacitatea continuă a instrumentelor pe măsură ce amenințările evoluează și asigură că alertele pe care le generează sunt precise, relevante și utile pentru identificarea riscurilor reale de securitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Instrumentele care monitorizează dispozitive precum laptopuri, telefoane mobile și servere ar trebui verificate periodic pentru a confirma că funcționează corect, că sunt actualizate cu cele mai recente informații privind amenințările și că sunt capabile să detecteze noi tipuri de atacuri.
- Ar trebui utilizat un sistem central pentru colectarea și analizarea jurnalelor din diferite surse. Aceste jurnale trebuie să fie complete, actualizate și utile pentru identificarea activităților suspecte.
- Jurnalele legate de accesul la sistem, precum încercările de autentificare sau accesul în afara programului normal, ar trebui revizuite periodic. Ar trebui configurate alerte pentru notificarea echipelor de securitate cu privire la tiparele neobișnuite.
- Instrumentele care analizează comportamentul utilizatorilor ar trebui ajustate în timp. Echipele de securitate ar trebui să revizuiască alertele, să ajusteze regulile de detecție pentru reducerea alarmelor false și îmbunătățirea preciziei.
- Instrumentele de înșelăciune, precum sistemele sau fișierele false proiectate pentru atragerea atacatorilor, ar trebui monitorizate îndeaproape. Alertele generate de aceste instrumente sunt adesea semne timpurii ale unui atac real și trebuie tratate cu prioritate maximă.

- Echipele de securitate ar trebui să evalueze periodic performanța tuturor instrumentelor de monitorizare, să actualizeze regulile de detecție și să asigure că instrumentele sunt integrate în procesele de răspuns la incidente.
- Rolurile și responsabilitățile privind monitorizarea și răspunsul la alerte ar trebui definite în mod clar. Personalul ar trebui instruit să utilizeze instrumentele în mod eficace și să răspundă adecvat la incidente.

DE.CM-06

Activitățile și serviciile furnizorilor externi de servicii sunt monitorizate pentru identificarea evenimentelor potențial adverse.

DE.CM-06.1

Activitățile și serviciile furnizorilor externi de servicii trebuie securizate și monitorizate pentru identificarea evenimentelor potențial adverse.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că activitățile desfășurate de furnizorii externi de servicii, fie la distanță, fie la fața locului, sunt gestionate în mod securizat și monitorizate în mod continuu. Aceasta contribuie la detecția oricăror acțiuni neobișnuite sau dăunătoare care ar putea afecta sistemele, datele sau serviciile organizației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Furnizorii externi ar putea include contractori, vânzători de servicii cloud, echipe de asistență IT, dezvoltatori de software și alte părți terțe implicate în mentenanța, dezvoltarea sau securitatea sistemului.
- Monitorizarea ar trebui să fie concentrată pe:
  - Activitatea de acces și autentificare, inclusiv modul și momentul în care utilizatorii externi se conectează la sisteme.
  - Transferurile de date și traficul de rețea, pentru detecția mișcărilor neobișnuite sau neautorizate de informații.
  - Modificările sistemului, precum actualizările de software sau ajustările de configurare efectuate de părți externe.
- Toate activitățile la distanță și la fața locului desfășurate de furnizorii externi ar trebui jurnalizate și revizuite pentru a identifica acțiunile neautorizate sau comportamentele riscante.
- Serviciile cloud și furnizorii de internet ar trebui monitorizați pentru detecția comportamentelor neașteptate sau a problemelor de performanță care ar putea indica o problemă de securitate.
- Ar trebui utilizat un sistem centralizat de jurnalizare pentru colectarea și analizarea datelor de la toate serviciile externe.
- Orice incidente de securitate care implică furnizori externi - precum infectare cu malware, tentative de phishing sau acces neautorizat - ar trebui detectate din timp, raportate rapid și soluționate în mod eficace.

DE.CM-06.2

Conformitatea furnizorilor externi de servicii cu politicile și procedurile de securitate a personalului și cu cerințele de securitate din contract trebuie monitorizată în raport cu riscurile lor de securitate cibernetică.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că furnizorii externi de servicii respectă politicile de securitate a personalului și cerințele contractuale ale organizației, în special atunci când au acces la sisteme sau date sensibile. Aceasta contribuie la reducerea riscului de incidente de securitate cauzate de personalul terț și garantează că furnizorii sunt supuși acelorași standarde ca și personalul intern.
În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Furnizorii externi ar trebui să aibă responsabilități de securitate clar definite, care sunt documentate în contracte sau SLA-uri.
- Contractele ar trebui să includă cerințe precum:
  - Verificări de fond ale personalului furnizorului.
  - Semnarea acordurilor de confidențialitate.
  - Respectarea politicilor de utilizare acceptabilă.
- Respectarea acestor cerințe ar trebui monitorizată periodic, inclusiv verificarea finalizării cursurilor de instruire în domeniul securității și a semnării acordurilor.
- Furnizorii ar trebui să fie obligați să notifice imediat organizația atunci când personalul cu acces la sistem este transferat sau își părăsește funcția, astfel încât drepturile de acces să poată fi revocate fără întârziere.
- Ar trebui efectuate audituri periodice pentru confirmarea respectării politicilor de securitate de către furnizori. Acestea pot include:
  - Revizuirea jurnalelor de acces și a permisiunilor.
  - Verificarea procedurilor aferente proceselor de integrare și de ieșire organizațională.
  - Asigurarea faptului că numai persoanele fizice care sunt autorizate au acces la sistemele critice.
- Orice probleme sau neconformități ar trebui documentate, raportate și soluționate prin acțiuni corective și revizuiri ulterioare.

DE.CM-09

Hardware-ul și software-ul de calcul, mediile de rulare și datele acestora sunt monitorizate pentru identificarea evenimentelor potențial adverse.

DE.CM-09.1

Organizația trebuie să monitorizeze hardware-ul, software-ul, mediile de rulare și datele acestora pentru detecția evenimentelor potențial adverse.

GHID DE IMPLEMENTARE

Acest Control are obiectivul de a asigura că organizațiile monitorizează în mod continuu sistemele și datele informatice pentru detecția timpurie a evenimentelor potențial dăunătoare. Aceasta contribuie la menținerea vizibilității, la sprijinirea răspunsurilor în timp util și reducerea riscului de incidente de securitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Activarea jurnalizării sistemului pe computere și servere pentru înregistrarea evenimentelor importante.
- Utilizarea antivirusului integrat sau protecția pentru endpoint-uri pentru detecția amenințărilor și generarea alertelor.
- Revizuirea periodică a jurnalelor și alertelor pentru identificarea activităților neobișnuite sau a erorilor.
- Stocarea jurnalelor într-un folder partajat sau într-un vizualizator de jurnale simplu, pentru a le accesa și revizui mai ușor.
- Stabilirea unei rutine (de exemplu, săptămânală sau lunară) pentru verificarea jurnalelor și actualizarea instrumentelor de monitorizare.
- Desemnarea unei persoane responsabile cu monitorizarea, chiar dacă este o funcție cu jumătate de normă.

DE.CM-09.2

Organizația trebuie să implementeze verificări ale integrității hardware-ului pentru detecția modificărilor neautorizate ale hardware-ului critic al sistemului. Controalele trebuie să fie proporționale cu profilul de risc și capacitatea operațională a organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura protecția componentelor hardware critice împotriva manipulării neautorizate. Prin implementarea unor verificări de integritate care corespund nivelului de risc și capacității operaționale ale organizației, devine posibilă detecția modificărilor fizice sau la nivel de firmware care ar putea compromite securitatea.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Definirea a ceea ce trebuie protejat
    - Identificarea celor mai critice sisteme, precum serverele care gestionează date sensibile, ICS/SCADA sau dispozitivele criptografice, și prioritizarea lor în funcție de impactul asupra activității, cerințele legale și expunerea la amenințări.
- Alegerea nivelului adecvat de protecție
    - Selectarea controalelor în funcție de cât de critic este sistemul și de ceea ce poate suporta organizația:
        - Măsuri de control de bază
            - → Camere de servere încuiate, sigilii inviolabile, pornire securizată și audituri periodice ale hardware-ului.
        - Măsuri de control intermediare
            - → Alerte la deschiderea hardware-ului, utilizarea modulelor de platformă de încredere (TPM) și instrumente de validare a firmware-ului.
        - Controale avansate
            - → Validarea de la distanță a stării hardware-ului, hardware criptografic rezistent la manipulare (module hardware de securitate - HSM) și monitorizarea anomaliilor la nivel de hardware folosind instrumente de securitate.
- Conectarea la operațiunile de securitate
    - Transmiterea alertelor de la instrumentele de integritate hardware către sistemele centrale de monitorizare (precum SIEM sau SOC) pentru vizibilitate în timp real. Definirea modului de reacție în cazul în care este suspectată o manipulare frauduloasă.

- Atribuirea unor responsabilități clare
    - Desemnarea rolurilor pentru proiectarea, implementarea și răspunsul la problemele de integritate hardware. Utilizarea profilurilor de roluri (de exemplu, din ECSF elaborat de către ENISA) pentru ghidarea responsabilităților:
        - Arhitecții de securitate proiectează controalele.
        - Administratorii de sistem le implementează și le monitorizează.
        - Personalul de răspuns la incidente investighează alertele.
- Documentarea și revizuirea
    - Includerea verificărilor de integritate ale hardware-ului în politicile de securitate, evaluările riscurilor și jurnalele de audit. Revizuirea eficacității acestora cel puțin anual sau după modificări sau incidente majore.
- Instruirea personalului și conștientizarea
    - Instruirea personalului relevant pentru recunoașterea semnelor de manipulare, pentru utilizarea corectă a instrumentelor de integritate și pentru urmarea procedurilor de raportare.

DE.CM-09.3

IRP-ul organizației trebuie să includă măsuri pentru detecția manipulării neautorizate a hardware-ului sistemelor critice.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că IRP-ul organizației include măsuri pentru detecția și răspunsul la manipularea neautorizată a hardware-ului critic. Aceasta ajută organizația să reacționeze rapid și eficace în cazul în care cineva încearcă să compromită fizic sau digital sisteme importante. Acest Control poate fi implementat într-un mod practic și scalabil.

Luând în considerare măsurile de mai jos, inclusiv organizațiile mici pot include în mod eficace detecția manipulării hardware în capabilitățile lor de răspuns la incidente, fără a necesita resurse extinse:

- IRP
    - IRP-ul ar trebui să includă instrucțiuni clare privind măsurile care trebuie luate în cazul în care este suspectată manipularea hardware-ului.
- Inspecții periodice
    - Personalul IT și OT sau personalul desemnat va inspecta periodic hardware-ul critic pentru detecția semnelor de manipulare, precum sigilii rupte, cabluri slăbite sau modificări neașteptate.
- Instrumente de monitorizare
    - Pot fi utilizate instrumente simple pentru trimiterea alertelor, atunci când se întâmplă ceva neobișnuit cu un dispozitiv, precum deschiderea carcasei, conectarea unui nou dispozitiv USB sau repornirea neașteptată a sistemului. Multe dintre aceste instrumente sunt proiectate pentru a fi accesibile și ușor de utilizat, în special pentru organizațiile mici.
- Instruirea și conștientizarea
    - Instruirea angajaților să recunoască semnele de manipulare a hardware-ului și să raporteze orice activitate suspectă. Conștientizarea este esențială pentru detecția timpurie.
- Asistență din partea vânzătorului
    - Utilizarea instrumentelor sau serviciilor oferite de vânzătorii de hardware pentru detecția manipulărilor frauduloase, adesea incluse în contractele de asistență.

DE.CM-09.4

Organizația trebuie să stabilească un sistem pentru a distinge cu precizie între alertele legitime și falsele pozitive, asigurând detecția și eliminarea eficace a codurilor cu scop nelegitim.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația poate identifica cu precizie amenințările reale, evitând în același timp alertele inutile cauzate de falsele pozitive. Aceasta contribuie la îmbunătățirea eficacității detecției și eliminării codurilor cu scop nelegitim, reducând în același timp timpul și resursele irosite pentru a răspunde la activități inofensive.

Pentru a contribui la detecția și eliminarea eficace a codurilor cu scop nelegitim, evitând în același timp alarmele false, ar trebui luate în considerare următoarele:

- Actualizări automate
    - Instrumentele de protecție împotriva codurilor cu scop nelegitim ar trebui configurate să se actualizeze automat, acolo unde este posibil, sau manual, conform unui program definit, în conformitate cu politicile organizației și constrângerile operaționale.
- Practici de dezvoltare securizate
    - Software-ul utilizat în sistemele IT și OT ar trebui să respecte practicile de dezvoltare sigură, inclusiv revizuirea codului și verificarea vulnerabilităților, în vederea reducerii riscului de introducere de cod cu scop nelegitim.
- Protecție stratificată
    - Atât protecția bazată pe semnături (care detectează amenințările cunoscute), cât și protecția bazată pe comportament (care caută activități neobișnuite sau suspecte) ar trebui utilizate în locurile în care rețelele se conectează la internet, în care personalul accesează sistemele de control și în care fișierele sau datele sunt partajate între sisteme.
- Scanarea amenințărilor
    - Instrumentele de protecție ar trebui setate să efectueze scanări regulate și, acolo unde este fezabil, verificări în timp real ale fișierelor și transferurilor de date, în special ale celor provenite din surse externe sau de pe medii amovibile.

- Blocarea și carantina
    - Codul cu scop nelegitim detectat ar trebui blocat și izolat pentru împiedicarea afectării altor sisteme. În mediile OT, aceasta ar trebui realizată într-un mod care să nu perturbe operațiunile critice.
- Alerte și notificări
    - Atunci când sunt detectate coduri cu scop nelegitim, ar trebui trimise alerte personalului desemnat, cu proceduri clare de răspuns atât în contextul IT, cât și în cel OT.

[DE.AE] ANALIZA EVENIMENTELOR ADVERSE

Anomaliile, IoC-urile și alte evenimente potențial adverse sunt analizate pentru caracterizarea evenimentelor și detecția incidentelor de securitate cibernetică.

DE.AE-02

Evenimentele potențial adverse sunt analizate pentru a înțelege mai bine activitățile asociate.

DE.AE-02.1

Evenimentele legate de securitatea cibernetică sau a informației trebuie revizuite și analizate pentru identificarea potențialelor ținte și metode de atac, în conformitate cu legile, reglementările, standardele și politicile aplicabile.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că evenimentele legate de securitatea cibernetică sau a informației sunt revizuite și analizate pentru detecția țintelor și metodelor de atac. Aceasta permite organizațiilor să răspundă în mod eficace la amenințări, menținând în același timp conformitatea cu cerințele legale, de reglementare și de politică.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Organizațiile ar trebui să respecte legislația în vigoare, standardele și politicile interne, atunci când se analizează evenimentele de securitate.
- Instrumentele de analiză a jurnalelor ar trebui utilizate pentru generarea de rapoarte și identificarea activității suspecte.
- Jurnalele de sistem și de aplicații ar trebui revizuite periodic pentru detecția semnelor de amenințări la adresa securității, precum încercări repetate de autentificare eșuate sau transferuri de date neobișnuite.
- Jurnalele ar trebui analizate pentru identificarea tiparelor care indică tentative de atac sau atacuri în curs.
- Informațiile privind amenințările ar trebui utilizate pentru a fi la curent cu amenințările emergente și tehnicile de atac, iar măsurile de securitate ar trebui ajustate în consecință.
- Ar trebui efectuate audituri și evaluări periodice pentru evaluarea posturii de securitate a organizației.
- Rezultatele acestor audituri ar trebui utilizate pentru îmbunătățirea proceselor de monitorizare și analiză.

DE.AE-02.2

Organizația trebuie să implementeze mecanisme automatizate, acolo unde este fezabil, pentru revizuirea și analizarea evenimentelor detectate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația utilizează automatizarea, acolo unde este practic, pentru sprijinirea revizuirii și analizării eficiente și consecvente a evenimentelor de securitate cibernetică detectate. Aceasta contribuie la reducerea riscului de eroare umană, accelerează detecția amenințărilor și răspunsul la acestea și permite resurselor de securitate limitate (în special în organizațiile mai mici) să se concentreze pe sarcini cu valoare mai mare, precum investigarea incidentelor complexe sau îmbunătățirea apărării.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Utilizarea capabilităților integrate
    - Activarea și configurarea funcțiilor de jurnalizare și alertare în platformele existente (de exemplu, Microsoft 365, Google Workspace, firewall-uri) pentru detecția automată a activităților suspecte.
- Implementarea de instrumente de detecție ușoară
    - Utilizarea soluțiilor accesibile EDR care oferă alerte automate și analize de bază, precum detecția malware-ului sau a comportamentului neobișnuit de autentificare.
- Luarea în considerare a serviciilor de detecție gestionate
    - Pentru organizațiile cu resurse interne limitate, serviciile gestionate de detecție și răspuns (MDR) pot furniza monitorizare externalizată, detecția amenințărilor și răspuns la incidente.
- Automatizarea zonelor cu impact ridicat
    - Concentrarea automatizării pe indicatori comuni de amenințare, precum:
        - Multiple tentative eșuate de autentificare.
        - Acces neobișnuit la fișiere sensibile.
        - Trafic de ieșire neașteptat.
- Integrarea informațiilor privind amenințările
    - Utilizarea fluxurilor de informații privind amenințările gratuite sau la preț redus pentru îmbunătățirea instrumentelor de detecție cu IoC-uri cunoscute și comportamente ale atacatorilor.

- Menținerea practicilor de revizuire manuală
    - Programarea revizuirilor manuale regulate ale jurnalelor și alertelor pentru identificarea amenințărilor pe care instrumentele automate le pot omite, în special cele care implică tehnici de atac noi sau subtile.

DE.AE-03

Informațiile sunt corelate din surse multiple.

DE.AE-03.1

Funcționalitatea de jurnalizare a instrumentelor de protecție și detecție trebuie activată. Jurnalele trebuie salvate și păstrate pentru o perioadă predefinită și revizuite periodic pentru identificarea activităților neobișnuite sau potențial dăunătoare.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că instrumentele de securitate au funcția de jurnalizare activată, că jurnalele sunt păstrate pentru o perioadă determinată și verificate periodic pentru identificarea activității neobișnuite sau dăunătoare. Aceasta contribuie la detecția timpurie a amenințărilor și luarea de măsuri. Exemple de astfel de instrumente includ firewall-uri, software antivirus, sisteme de detecție a endpoint-urilor și sisteme de detecție a intruziunilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Jurnalele ar trebui stocate în mod securizat și păstrate conform unui program de păstrare definit, pe baza cerințelor legale, de reglementare sau operaționale aplicabile.
- Instrumentele și soluțiile de detecție a evenimentelor ar trebui configurate astfel încât să genereze alerte automate pentru activități suspecte sau dăunătoare.
- Ar trebui să existe o procedură documentată pentru revizuirea periodică a jurnalelor și a tablourilor de bord, pentru sprijinirea detecției și răspunsul în timp util.
- Revizuirile jurnalelor ar trebui să includă verificări ale tiparelor, precum infectare cu malware repetată, trafic de rețea anormal sau acces excesiv la site-uri web care nu au legătură cu activitatea organizației.
- Dacă sunt identificate astfel de tipare, ar trebui definite acțiuni de urmărire, precum consolidarea controalelor de securitate specifice, actualizarea regulilor de detecție sau organizarea de instruire țintită pentru conștientizare.

DE.AE-03.2

Organizația trebuie să se asigure că datele privind evenimentele din sistemele critice sunt colectate și corelate utilizând informații din mai multe surse relevante.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a permite organizației să detecteze amenințări complexe sau distribuite prin corelarea și analizarea datelor privind evenimentele provenite din diferite sisteme și surse. Corelarea acestor date contribuie la identificarea unor tipare care ar putea să nu fie vizibile atunci când sistemele sunt monitorizate separat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Sursele relevante de date despre evenimente pot include jurnale de sistem, jurnale de audit, instrumente de monitorizare a rețelei, înregistrări ale accesului fizic și rapoarte de la utilizatori sau administratori.
- Datele din jurnale ar trebui trimise în mod continuu, ideal în timp real sau aproape în timp real, către un sistem centralizat pentru stocare și analiză. Aceasta îmbunătățește capacitatea de a detecta tipare și de a răspunde rapid la potențiale probleme.
- Centralizarea jurnalelor pe un număr mic de servere sau platforme dedicate, precum SIEM, instrumente ușoare de gestionare a jurnalelor, servicii de jurnalizare bazate pe cloud sau servicii de detecție gestionate (deseori parte a MDR), poate sprijini analiza și corelarea eficientă a evenimentelor între sisteme.
- Informațiile privind amenințările cibernetice pot fi utilizate pentru îmbunătățirea corelării evenimentelor, oferind contextul privind amenințările cunoscute, metodele de atac și IoC-uri.
- Informațiile privind amenințările ar trebui integrate în mod securizat în instrumentele și procesele de detecție pentru sprijinirea identificării mai precisă și mai rapidă a amenințărilor.

DE.AE-03.3

Organizația trebuie să combine analiza evenimentelor cu informații provenite din scanări de vulnerabilitate, date privind performanța sistemului, monitorizarea sistemelor critice și monitorizarea incintelor, acolo unde este fezabil.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a consolida capacitatea organizației de detecție a amenințărilor complexe sau ascunse prin combinarea analizei evenimentelor cu alte surse de date relevante.

Această viziune mai amplă permite identificarea mai precisă și mai rapidă a activităților suspecte, iar în vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Ar trebui utilizate instrumente care colectează și conectează date din diferite sisteme (precum SIEM, XDR sau SOAR) pentru a sprijini această integrare.
- Problemele de securitate raportate de furnizori sau surse de încredere ar trebui colectate rapid și revizuite pentru identificarea eventualelor riscuri.
- Datele din diferite sisteme de monitorizare ar trebui reunite pentru facilitarea detecției tiparelor sau problemelor.
- Configurația ar trebui să permită detecția și răspunsul rapid atunci când este constatat ceva neobișnuit.

DE.AE-04

Impactul și amploarea estimate ale evenimentelor adverse sunt înțelese.

DE.AE-04.1

Organizația trebuie să evalueze impacturile negative ale evenimentelor detectate asupra operațiunilor, activelor și persoanelor sale fizice și să coreleze aceste impacturi cu rezultatele evaluărilor sale de riscuri.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația înțelege modul în care evenimentele detectate ar putea cauza prejudicii și utilizează această înțelegere pentru a ghida deciziile și răspunsurile bazate pe risc.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Pentru a sprijini această evaluare, ar trebui utilizate instrumente care ajută la estimarea amplorii și impactului evenimentelor.
- Evaluarea ar trebui să ia în considerare modul în care problemele dintr-o parte a sistemului ar putea afecta alte părți conectate.
- Impactul negativ poate include pierderi financiare, întreruperea serviciilor, deteriorarea echipamentelor sau vătămarea persoanelor.
- Evenimentele detectate pot include incidente cibernetice, defecțiuni ale sistemului sau dezastre naturale.
- Gravitatea și probabilitatea acestor impacturi ar trebui evaluate și comparate cu evaluările riscurilor existente.
- Această comparație ar trebui să contribuie la stabilirea priorităților în ceea ce privește acțiunile, alocarea resurselor și îmbunătățirea planificării răspunsului.

DE.AE-06

Informațiile privind evenimentele adverse sunt furnizate personalului autorizat și instrumentelor.

DE.AE-06.1

Informațiile privind evenimentele adverse trebuie transmise prompt personalului și sistemelor autorizate, pentru a permite detecția, investigarea și răspunsul în timp util.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că informațiile despre evenimentele adverse sunt transmise prompt persoanelor și sistemelor potrivite, astfel încât să poată fi luate măsuri adecvate fără întârziere. Aceasta permite detecția, investigarea și răspunsul mai rapid la potențiale amenințări sau perturbări.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Tipuri de evenimente adverse
    - Includerea indicatorilor precum activități neobișnuite ale contului, acces neautorizat, modificări ale configurației sistemului, încălcări ale securității fizice sau alerte de malware.
- Detecția și alertarea
    - Utilizarea instrumentelor de securitate cibernetică pentru a detecta astfel de evenimente și pentru alertarea automată a personalului autorizat (de exemplu, analiști SOC, personal de răspuns la incidente).
- Integrarea cu sistemele de ticketing
    - Alertele ar trebui să fie integrate cu sistemul de ticketing al organizației. Biletele ar trebui să fie:
        - generate automat pentru tipurile de alerte predefinite.
        - create manual atunci când personalul tehnic identifică activități suspecte.
- Acces la jurnale și analize
    - Personalul autorizat trebuie să aibă acces continuu la datele din jurnale și la rezultatele analizelor pentru sprijinirea investigațiilor.
- Evaluarea maturității și eficacității
    - Evaluarea implementării controlului verificând:
        - Documentația procedurilor de generare, revizuire și escaladare a alertelor. Această documentație ar trebui revizuită și actualizată periodic.

- Utilizarea automatizării pentru alertele standard, cu procese manuale ca rezervă.
- Controalele de acces pentru alerte şi jurnale, cu revizuiri periodice ale permisiunilor (accesul la alerte și jurnale trebuie să fie limitat la personalul autorizat).
- Monitorizarea şi raportarea ar trebui, de exemplu, să urmărească numărul de alerte, timpii de răspuns și dacă procedurile sunt respectate.
- Personalul responsabil cu gestionarea alertelor ar trebui să beneficieze de instruire periodică, pentru a asigura că înțelege cum să interpreteze alertele și să acționeze în consecință.

DE.AE-08

Incidentele sunt declarate atunci când evenimentele adverse îndeplinesc criteriile definite pentru incidente.

DE.AE-08.1

Incidentele trebuie raportate atunci când evenimentele adverse îndeplinesc criteriile definite și documentate pentru incidente.

GHID DE IMPLEMENTARE

Acest Control asigură identificarea și raportarea evenimentelor adverse atunci când acestea îndeplinesc criterii de incident clar definite și documentate. Aceasta subliniază importanța existenței unor praguri și linii directoare consecvente pentru a determina momentul în care un eveniment se califică drept incident, sprijinind conștientizarea în timp util și escaladarea sau răspunsul adecvat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Criteriile privind incidentele (regulile care definesc ce se califică drept incident) ar trebui să fie clar definite, documentate și revizuite periodic.
- Aceste criterii ar trebui să contribuie la determinarea momentului în care un eveniment advers devine un incident care trebuie raportat.
- Criteriile ar trebui să fie fundamentate pe tiparele cunoscute de activitate normală și anormală, inclusiv pe lecțiile învățate din incidentele anterioare.
- La stabilirea criteriilor, trebuie luate în considerare falsele pozitive cunoscute, pentru evitarea raportărilor inutile.
- Atunci când un eveniment îndeplinește criteriile definite, acesta ar trebui tratat ca un incident și raportat în conformitate cu procedurile organizației.
- Atunci când este cazul și acolo unde este fezabil, sistemele ar trebui configurate pentru sprijinirea acestui proces prin generarea de alerte atunci când sunt îndeplinite criteriile de incident. Aceasta poate contribui la detecția mai rapidă a incidentelor, în special în medii mai mari sau mai complexe.

RĂSPUNS

[RS.MA] MANAGEMENTUL INCIDENTELOR

Răspunsurile la incidentele de securitate cibernetică detectate sunt gestionate.

RS.MA-01

IRP-ul este executat în coordonare cu părțile terțe relevante odată ce un incident este declarat.

RS.MA-01.1

Un IRP, care include rolurile, responsabilitățile și atribuțiile de autoritate definite, trebuie executat în timpul sau după un eveniment de securitate cibernetică care afectează sistemele critice ale organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura executarea unui IRP bine definit în timpul sau după un eveniment de securitate cibernetică care afectează sistemele critice ale organizației, permițând detecția, limitarea, comunicarea și recuperarea în timp util.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Elaborarea unui plan de răspuns documentat
    - Planul ar trebui să includă instrucțiuni și proceduri predefinite pentru detecția incidentelor de securitate cibernetică, pentru a răspunde în mod eficace și pentru a sprijini recuperarea sistemelor critice.
- Includerea unor capabilități de detecție
    - Ar trebui să existe tehnologii de detecție care să raporteze automat incidentele confirmate și să declanșeze acțiuni de răspuns.
- Definirea rolurilor, responsabilităților și atribuțiilor de autoritate
    - Planul ar trebui să identifice în mod clar:
        - Cine este implicat în răspuns.
        - Datele de contact ale personalului cheie.
        - Cine are autoritatea de a iniția recuperarea.
        - Cine este responsabil pentru comunicarea externă (de exemplu, autoritățile de reglementare, partenerii, mass-media).
- Revizuirea și actualizarea periodică a planului
    - Planul ar trebui revizuit și actualizat pentru reflectarea modificărilor survenite în peisajul amenințărilor, structura organizațională sau lecțiile învățate din incidentele anterioare.

- Testarea planului prin exerciții
  - Ar trebui efectuate simulări și exerciții teoretice pentru validarea eficacității planului și identificarea domeniilor care necesită îmbunătățiri.
- Includerea mediilor OT
  - Planul ar trebui să abordeze răspunsul la incidente în sistemele OT, inclusiv coordonarea cu protocoalele de siguranță, izolarea activelor industriale afectate și restabilirea proceselor operaționale.

RS.MA-01.2

Organizația trebuie să coordoneze acțiunile de răspuns la incidentele de securitate cibernetică sau a informației cu toate părțile interesate predefinite.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate părțile interesate interne și externe relevante colaborează în mod eficace în timpul unui incident de securitate cibernetică sau a informației.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Acțiunile de răspuns la incidente ar trebui coordonate cu părțile interesate predefinite, inclusiv conducerea organizației, responsabilii de sisteme IT și OT, echipele de securitate cibernetică, vânzătorii, departamentul de resurse umane, departamentul juridic, departamentul de securitate fizică, departamentul de operațiuni și departamentul de achiziții.
- Coordonarea ar trebui să respecte IRP-urile documentate ale organizației.
- Pentru fiecare incident ar trebui desemnată o persoană responsabilă care să gestioneze răspunsul și să asigure o comunicare clară.
- Dacă este necesar, ar trebui activate planuri suplimentare, precum continuitatea activității sau recuperarea în caz de dezastru, pentru sprijinirea răspunsului.
- Informațiile ar trebui comunicate persoanelor potrivite la momentul potrivit, urmând procedurile de comunicare stabilite.
- Diferitele tipuri de incidente ar trebui recunoscute și gestionate în mod corespunzător:
    - Incidente legate de informații (de exemplu, expunerea accidentală a datelor).
    - Incidente de securitate cibernetică (de exemplu, programe malware, piraterie informatică).
    - Incidente OT (de exemplu, întreruperi ale ICS).
- Incidentele OT ar trebui să implice personal OT specializat și pot necesita proceduri de răspuns diferite pentru protejarea siguranței și operațiunilor.

RS.MA-02

Rapoartele privind incidentele sunt triate și validate.

RS.MA-02.1

Rapoartele privind incidentele de securitate cibernetică sau a informației trebuie triate și validate în conformitate cu procedurile de răspuns la incidente ale organizației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate incidentele raportate sunt revizuite și evaluate în mod sistematic înainte de a se lua orice altă măsură. Acest Control este un pas fundamental în procesul de răspuns la incidente și ar trebui luate în considerare următoarele:

- Filtrarea rapoartelor irelevante sau false
    - Nu toate rapoartele primite reprezintă incidente reale. Acest Control asigură că sunt luate măsuri numai în cazul incidentelor legitime, relevante pentru securitatea cibernetică.
- Asigurarea unui răspuns prompt și adecvat
    - Prin trierea și validarea timpurie a rapoartelor, organizațiile pot prioritiza amenințările reale și pot evita risipa de resurse pentru probleme neimportante.
- Sprijinirea unui proces decizional consecvent
    - Aplicarea unor criterii structurate de triere și validare contribuie la asigurarea unui răspuns consecvent, repetabil și aliniat la politicile organizației în cazul incidentelor.
- Permiterea escaladării și clasificării eficiente
    - Validarea este o condiție prealabilă pentru clasificarea și escaladarea incidentelor (conform cerințelor din RS.MA-03.1). Fără aceasta, procesul de răspuns ar putea fi direcționat greșit sau întârziat.
- Îmbunătățirea conștientizării situaționale
    - Validarea timpurie contribuie la construirea unei imagini mai clare a peisajului amenințărilor și sprijină o mai bună coordonare între echipe.

RS.MA-02.2

Trebuie utilizate instrumente automatizate pentru sprijinirea investigării și evaluării impactului incidentelor de securitate cibernetică validate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizațiile dispun de capabilitățile tehnice necesare pentru gestionarea în mod eficient și precis a incidentelor de securitate cibernetică odată ce acestea au fost validate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Instrumentele automatizate ar trebui să contribuie la colectarea, analizarea și corelarea datelor privind incidentele, pentru sprijinirea investigării prompte și precise a acestora.
- Aceste instrumente ar trebui să contribuie la identificarea amplorii, gravității și impactului potențial al incidentelor care au fost validate prin triere. Un incident validat este unul care a fost confirmat ca fiind legat de securitatea cibernetică (nu este o alarmă falsă sau o problemă tehnică fără legătură), îndeplinește criteriile de gravitate predefinite (precum IoC-uri, informații privind amenințările sau tipare de atac cunoscute) și necesită acțiuni de răspuns (adică îndeplinește pragul pentru investigații suplimentare, clasificare și escaladare).
- Pentru susținerea acestor activități pot fi luate în considerare următoarele tipuri de instrumente:
  - Sisteme SIEM pentru colectarea și analiza centralizată a jurnalelor.
  - XDR pentru detecția integrată a amenințărilor la nivelul endpoint-urilor, rețelelor și serverelor.
  - SOAR pentru automatizarea fluxurilor de lucru și coordonarea acțiunilor de răspuns.
  - Platforme de informații privind amenințările pentru îmbogățirea datelor privind incidentele cu contextul amenințărilor externe.
  - Sistem de detecție a intruziunilor în rețea (NIDS) pentru monitorizarea și alertarea cu privire la activități suspecte în rețea.
  - Centre de răspuns la incidente informatice (CIRC) pentru coordonare centralizată și analiză de specialitate.
- Mecanismele automatizate ar trebui integrate în procesul de răspuns la incidente pentru a asigura că incidentele validate sunt investigate în mod eficient și prioritizate în mod corespunzător, în conformitate cu IRP-ul organizației.

RS.MA-03

Incidentele sunt clasificate și prioritizate.

RS.MA-03.1

Incidentele de securitate cibernetică sau a informației trebuie clasificate, prioritizate și escaladate conform IRP-ului.

GHID DE IMPLEMENTARE

Acest Control este o evoluție a RS.MA-02.1 și are scopul de a asigura că, odată ce un incident este validat, acesta este clasificat și gestionat în mod sistematic în funcție de natura, urgența și impactul potențial al acestuia, astfel încât organizația să poată răspunde în mod eficace, consecvent și adecvat. În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Incidentele ar trebui revizuite și clasificate în funcție de tipul lor (de exemplu, încălcarea securității datelor, ransomware, DDoS, compromiterea contului) și de amploarea validată a impactului lor.
- Estimarea și validarea amplorii unui incident - dezvoltată în continuare în RS.AN-08.1 (Esențial) - ar trebui să informeze modul în care incidentele sunt clasificate și prioritizate.
- Indicatori precum domeniul de aplicare, gravitatea și sensibilitatea la factorul timp ar trebui să ghideze deciziile privind stabilirea priorităților.
- SBOM-urile pot sprijini evaluarea impactului prin identificarea componentelor și dependențelor afectate.
- Criteriile de clasificare, prioritizare și escaladare ar trebui documentate în IRP și aplicate în mod consecvent.
- Strategiile de răspuns la incidente ar trebui să echilibreze necesitatea unei recuperări rapide cu potențialele beneficii ale observării comportamentului atacatorului sau ale efectuării unei investigații mai aprofundate.
- Procedurile de escaladare ar trebui coordonate cu părțile interesate interne și externe desemnate pentru asigurarea unui răspuns oportun și adecvat.

RS.MA-05

Se aplică criterii pentru inițierea activităților de recuperare în urma unui incident de securitate cibernetică.

RS.MA-05.1

Trebuie definite și aplicate criterii clare pentru determinarea momentului în care trebuie inițiate procesele de recuperare în urma incidentelor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizațiile dispun de un proces decizional clar, consecvent și bazat pe risc pentru determinarea momentului în care trebuie să înceapă acțiunile de recuperare în urma unui incident de securitate cibernetică.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Criteriile pentru inițierea recuperării în urma unui incident ar trebui să fie bazate pe caracteristicile cunoscute sau presupuse ale incidentului, precum gravitatea, amploarea și impactul său potențial asupra operațiunilor, datelor sau sistemelor.
- Decizia de a începe recuperarea ar trebui să țină cont și de potențialele perturbări pe care activitățile de recuperare le pot cauza operațiunilor în curs.
- RPO și RTO ar trebui incluse în criterii pentru a asigura că acțiunile de recuperare sunt în concordanță cu cerințele de continuitate a activității și cu pragurile acceptabile de întrerupere a activității sau de pierdere a datelor.

[RS.AN] ANALIZA INCIDENTELOR

Sunt efectuate investigații pentru asigurarea unui răspuns eficace și pentru sprijinirea activităților de analiză criminalistică și recuperare.

RS.AN-03

Se efectuează analize pentru a stabili ce s-a întâmplat în timpul unui incident și cauza principală a incidentului.

RS.AN-03.1

Fiecare incident trebuie analizat pentru a determina ce s-a întâmplat și pentru a identifica cauza principală a acestuia.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a înțelege amploarea unui incident de securitate cibernetică și de a identifica cauza sa principală, permițând un răspuns eficace și prevenirea unor evenimente similare în viitor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Secvența evenimentelor din timpul incidentului ar trebui reconstituită, identificând sistemele, activele și resursele implicate.
- Ar trebui identificate vulnerabilitățile, amenințările și actorii de amenințare legați de incident, indiferent dacă sunt implicați direct sau indirect.
- Analiza criminalistică ar trebui utilizată atunci când este necesar pentru examinarea datelor colectate și determinarea cauzei principale.
- Analiza ar trebui să se concentreze pe identificarea cauzelor sistemice subiacente, nu doar pe factorii declanșatori imediați.
- Tehnologiile de decepție cibernetică ar trebui revizuite pentru a obține informații suplimentare despre comportamentul atacatorilor.

RS.AN-06

Acțiunile întreprinse în timpul unei investigații sunt înregistrate, iar integritatea și proveniența înregistrărilor sunt păstrate.

RS.AN-06.1

Acțiunile întreprinse în timpul unei investigații trebuie înregistrate, iar integritatea și proveniența înregistrărilor trebuie păstrate.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate acțiunile întreprinse în timpul unei investigații a incidentului sunt înregistrate corespunzător și că integritatea și proveniența acestor înregistrări sunt protejate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Solicitarea tuturor membrilor personalului implicați în răspunsul la incidente (de exemplu, personal de răspuns la incidente, administratorii de sistem, inginerii) să își jurnalizeze acțiunile într-un mod care să împiedice modificarea sau ștergerea acestora.
- Atribuirea responsabilității coordonatorului de răspuns la incidente pentru documentarea întregii investigații, inclusiv cronologia, deciziile și sursele de informații.
- Asigurarea faptului că toate înregistrările sunt stocate în mod securizat și rămân trasabile până la sursa lor originală.

RS.AN-07

Datele și metadatele incidentului sunt colectate, iar integritatea și proveniența acestora sunt păstrate.

RS.AN-07.1

Datele și metadatele incidentului trebuie colectate și protejate pentru asigurarea acurateței, autenticității și trasabilității acestora.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate informațiile relevante despre un incident de securitate cibernetică sunt înregistrate cu acuratețe, stocate în mod securizat și trasabile în mod fiabil, astfel încât să poată fi utilizate în mod eficace în scopuri de răspuns, investigare și legale sau de conformitate.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Datele și metadatele referitoare la incidente (precum sursa datelor și momentul colectării acestora) ar trebui colectate și stocate într-un mod care să le protejeze împotriva falsificării sau pierderii.
- Integritatea și originea acestor informații ar trebui păstrate utilizând metode precum:
  - Documentația lanțului de custodie pentru urmărirea modului în care sunt gestionate datele, de la colectare până la analiză.
  - Semnături digitale și criptare pentru prevenirea accesului neautorizat și confirmarea autenticității.
  - Jurnale de audit pentru a înregistra cine a accesat sau modificat datele și când.
- Colectarea și protejarea acestor informații ar trebui să sprijine:
  - Răspunsul prompt, contribuind la înțelegerea momentului și a modului în care s-a produs incidentul.
  - Investigarea și analiza, prin furnizarea de detalii fiabile despre cauza, amploarea și impactul incidentului.
  - Cerințele legale și de conformitate, asigurând că datele pot fi utilizate ca probe, dacă este necesar.

RS.AN-08

Amploarea unui incident este estimată și validată.

RS.AN-08.1

Amploarea unui incident trebuie estimată și validată.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizațiile au o înțelegere clară a întregii amplori și a impactului unui incident de securitate cibernetică, astfel încât acțiunile de răspuns să poată fi dimensionate, prioritizate și coordonate în mod adecvat.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Amploarea și impactul unui incident ar trebui evaluate prin examinarea nu numai a sistemului afectat inițial, ci și a altor sisteme sau dispozitive care ar putea fi compromise.
- IoC-urile precum activitatea neobișnuită a rețelei, încercările de acces neautorizat sau modificările neașteptate ale software-ului, ar trebui identificate pentru a înțelege cât de mult s-a răspândit incidentul.
- Semnele de persistență, inclusiv backdoor-urile sau malware-ul care permit accesul continuu, ar trebui investigate pentru a determina dacă atacatorul rămâne activ în mediul respectiv.
- Ar trebui utilizate instrumente automatizate pentru scanarea IoC-urilor și mecanismelor de persistență în toate activele potențial afectate, pentru sprijinirea unei analize prompte și aprofundate.
- Amploarea validată a incidentului ar trebui să determine modul în care incidentul este clasificat, prioritizat și escaladat, astfel cum este descris în RS.MA-03.1 (Important), asigurându-se că acțiunile de răspuns sunt aliniate cu riscul real și impactul asupra activității.

[RS.CO] RAPORTAREA ȘI COMUNICAREA RĂSPUNSULUI LA INCIDENTE

Activitățile de răspuns sunt coordonate cu părțile interesate interne și externe, conform cerințelor legilor, reglementărilor sau politicilor.

RS.CO-02

Părțile interesate interne și externe sunt informate cu privire la incidente.

RS.CO-02.1

Informațiile privind incidentele de securitate cibernetică trebuie comunicate angajaților într-un mod clar și ușor de înțeles.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toți angajații sunt informați în timp util și într-un mod ușor de înțeles cu privire la incidentele de securitate cibernetică, astfel încât aceștia să poată reacționa în mod adecvat și să contribuie la reducerea riscurilor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Ar trebui să existe un IRP. Acest plan descrie modul în care organizația va răspunde la incidentele de securitate cibernetică, inclusiv cine este responsabil pentru ce și cum se vor escalada diferitele tipuri de amenințări.
- IRP-ul ar trebui să includă un protocol de comunicare care să explice modul în care se pot partaja rapid și eficient informații exacte și relevante cu angajații în timpul unui incident.
- Planul ar trebui să definească canalele de comunicare care vor fi utilizate, precum e-mailul, platformele interne de mesagerie, apelurile telefonice sau un portal dedicat incidentelor.
- Șabloanele pentru mesajele privind incidentele ar trebui pregătite în avans. Aceste șabloane ar trebui să includă detalii cheie, precum tipul incidentului, gravitatea acestuia, sistemele afectate și acțiunile pe care angajații ar trebui să le ia.
- Mesajele ar trebui redactate într-un limbaj clar și simplu, evitând termenii tehnici, astfel încât toți angajații să înțeleagă ce se întâmplă și ce se așteaptă de la ei.
- Conducerea superioară ar trebui să primească rezumate la nivel înalt care să explice impactul incidentului, riscurile implicate și măsurile luate pentru rezolvarea acestuia.

RS.CO-02.2

Incidentele de securitate cibernetică trebuie comunicate părților interesate externe relevante în termenele definite în IRP, inclusiv raportarea incidentelor semnificative către autorități, conform prevederilor legale.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că toate părțile externe relevante sunt informate cu privire la incidentele de securitate cibernetică în timp util, în mod securizat și adecvat, contribuind la menținerea încrederii și la îndeplinirea obligațiilor legale și contractuale.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Informațiile ar trebui partajate în mod securizat și în conformitate cu IRP-ul organizației și cu orice acorduri de schimb de informații.
- Părțile interesate relevante pot include roluri interne desemnate, clienți afectați, furnizori, furnizori terți de servicii și parteneri ai organizației.
- Clienții și partenerii ar trebui notificați dacă sunt afectați de un incident, cu instrucțiuni clare privind acțiunile pe care ar trebui să le întreprindă.
- Comunicarea cu părțile externe ar trebui să respecte toate cerințele contractuale sau acordurile în vigoare.
- Comunicarea de criză ar trebui coordonată cu furnizorii critici pentru a asigura coerența mesajelor.
- Atunci când sunt partajate informații despre tacticile sau tehnicile atacatorilor, orice date sensibile sau de identificare ar trebui eliminate.
- Departamentul de resurse umane ar trebui informat dacă incidentul implică activități rău intenționate din partea unei persoane din interior.
- Conducerea superioară ar trebui să primească actualizări periodice cu privire la starea incidentelor majore.
- Autoritățile naționale, precum echipele de răspuns la incidente de securitate cibernetică (CSIRT), autoritățile de aplicare a legii sau autoritățile de reglementare, ar trebui să fie notificate pe baza criteriilor definite în IRP și cu aprobarea conducerii superioare a organizației.
- Toate raportările ar trebui să respecte legislația națională și europeană relevantă, precum Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice

și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere.

- Actualizările publice privind incidentele sunt tratate în cadrul unui control separat (RC.CO-04.1).

[RS.MI] ATENUAREA INCIDENTELOR

Sunt desfășurate activități pentru prevenirea extinderii unui eveniment și pentru a-i atenua efectele.

RS.MI-01

Incidentele sunt limitate.

RS.MI-01.1

Incidentele de securitate cibernetică trebuie limitate și eliminate. Orice decizie de acceptare și menținere a anumitor riscuri de securitate cibernetică trebuie documentată în mod formal.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a opri răspândirea incidentelor de securitate cibernetică, de a elimina cauza acestora și de a se asigura că orice riscuri acceptate sunt înregistrate și aprobate în mod clar.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Ar trebui să existe un proces formal de acceptare a riscurilor pentru riscurile de securitate cibernetică considerate a avea un impact redus și care nu amenință sistemele critice pentru organizație. Aceste riscuri ar trebui să fie revizuite și aprobate de persoana sau echipa responsabilă, pe baza toleranței la risc a organizației.
- Instrumentele de securitate cibernetică, precum software-ul antivirus sau funcțiile de securitate integrate în sistemele de operare și dispozitivele de rețea, ar trebui să poată lua automat acțiuni pentru limitarea sau eliminarea amenințărilor, atunci când este cazul.
- Echipele de răspuns la incidente ar trebui să poată alege și executa manual acțiuni pentru oprirea și eliminarea incidentelor atunci când este necesar.
- Părțile terțe de încredere, precum ISP sau furnizori de servicii de securitate gestionate, ar trebui să aibă permisiunea de a contribui la acțiunile de limitare și eliminare, dacă aceasta face parte din planul de răspuns al organizației.

RS.MI-01.2

Organizația trebuie să detecteze accesul neautorizat sau scurgerile de date și să ia acțiunile corespunzătoare de atenuare, inclusiv monitorizarea sistemelor critice la granițele externe și la punctele interne cheie.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a detecta în timp util accesul neautorizat și scurgerile de date și de a lua acțiunile corespunzătoare de atenuare. Aceasta ar trebui să contribuie la protejarea confidențialității, integrității, disponibilității și siguranței datelor, indiferent dacă acestea sunt stocate, transmise sau utilizate în mod activ, atât în mediile IT, cât și în cele OT.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Monitorizarea sistemelor critice
    - Monitorizarea ar trebui implementată la granițele rețelei externe și în punctele interne cheie pentru detecția anomaliilor sau încercărilor de acces neautorizat.
- Protejarea datelor în toate stările
    - Datele ar trebui protejate utilizând criptarea, semnături digitale și hash-uri criptografice pentru asigurarea confidențialității și integrității în timpul stocării, transmiterii și utilizării.
- Controlul comunicațiilor de ieșire
    - Comunicațiile externe care conțin date sensibile ar trebui blocate sau criptate automat în funcție de clasificarea datelor.
- Restricționarea utilizării serviciilor personale
    - Accesul la platformele de comunicare personale (de exemplu, e-mail personal, servicii de partajare a fișierelor) din sistemele organizației ar trebui restricționat pentru reducerea riscului scurgerii de date.
- Prevenirea reutilizării datelor în medii care nu sunt de producție
    - Datele sensibile de producție nu ar trebui reutilizate în medii de dezvoltare sau testare, cu excepția cazului în care sunt anonimizate sau mascate în mod corespunzător.
- Ștergerea datelor temporare
    - Datele sensibile ar trebui șterse din memorie sau din spațiul de stocare temporar odată ce nu mai sunt necesare.

- Auditarea IAM
    - Sistemele precum AD ar trebui auditate periodic, cu accent pe conturile privilegiate și consecvența controlului accesului.
- Asigurarea fezabilității specifice OT
    - În mediile OT, măsurile de detecție și atenuare ar trebui adaptate pentru evitarea perturbării siguranței sau continuității operaționale. Monitorizarea pasivă și jurnalizarea la nivel de interfață pot fi utilizate în cazul în care integrarea directă nu este fezabilă.
- Alinierea la recomandările ENISA
    - Aceste practici sunt aliniate cu Ghidul privind scurgerile de informații și Rapoartele privind peisajul amenințărilor elaborate de către ENISA, care furnizează recomandări pentru detecția și atenuarea încălcărilor securității datelor și a accesului neautorizat.

[RC.RP] EXECUTAREA PLANULUI DE RECUPERARE ÎN CAZ DE INCIDENT

Activitățile de restaurare sunt efectuate pentru asigurarea disponibilității operaționale a sistemelor și serviciilor afectate de incidente de securitate cibernetică.

RC.RP-01

Partea de recuperare a IRP-ului este executată odată ce a fost inițiată din procesul de răspuns la incidente.

RC.RP-01.1

Trebuie elaborat și executat un proces de recuperare în caz de dezastre și incidente de securitate cibernetică sau a informației.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația poate răspunde rapid și eficace la dezastre, incidente de securitate a informației și evenimente de securitate cibernetică, prin elaborarea și executarea unui proces structurat de recuperare care protejează persoanele, sistemele și datele.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Elaborarea unui proces de recuperare
    - Un proces documentat ar trebui să ghideze acțiunile imediate în cazul unui incendiu, unei urgențe medicale, unui furt, unui dezastru natural sau unui incident de securitate cibernetică sau a informației.
- Definirea rolurilor și responsabilităților
    - Procesul de recuperare ar trebui să specifice cine este autorizat să inițieze procedurile de recuperare și cine va comunica cu părțile interesate externe.
- Protejarea informațiilor și a sistemelor
    - Procesul ar trebui să includă măsuri pentru securizarea informațiilor și a sistemelor, precum oprirea sau blocarea dispozitivelor, trecerea la site-uri de rezervă sau securizarea documentelor fizice.
- Stabilirea procedurilor de contact
    - Ar trebui menținută o listă de contacte interne și externe, care să fie inclusă în planul de recuperare pentru a putea fi accesată rapid în cazul unui incident.
- Asigurarea conștientizării și pregătirii
    - Persoanele fizice responsabile cu recuperarea ar trebui să fie familiarizate cu planul de recuperare și să înțeleagă autorizațiile necesare pentru efectuarea fiecărei etape.

- Integrarea cu IRP
    - Procesul de recuperare ar trebui să facă parte din IRP-ul mai larg sau să fie aliniat cu acesta, pentru a asigura consecvența și coordonarea.
- Includerea mediilor OT
    - Planificarea recuperării ar trebui să abordeze sistemele OT, inclusiv procedurile de restabilire a operațiunilor industriale, securizarea sistemelor de control și coordonarea cu protocoalele de siguranță.
- Planificarea îmbunătățirilor viitoare
    - Acest Control servește drept bază pentru planificarea mai avansată a recuperării, astfel cum este dezvoltat în continuare în Controlul RC.RP-06.1.

RC.RP-02

Acțiunile de recuperare sunt selectate, delimitate, prioritizate și efectuate.

RC.RP-02.1

Funcțiile și serviciile esențiale ale organizației trebuie continuate cu pierderi minime sau fără pierderi în ceea ce privește continuitatea operațională, iar continuitatea trebuie menținută până la recuperarea completă a sistemului.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a minimiza întreruperea operațiunilor critice în timpul incidentelor și de a se asigura că acestea rămân funcționale până la restabilirea completă a sistemelor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Planificarea continuității
  - Ar trebui menținut un BCP pentru identificarea funcțiilor esențiale și definirea procedurilor pentru funcționarea neîntreruptă în timpul incidentelor.
  - Ar trebui inclus un IRP, care să detalieze pașii pentru limitarea incidentului, evaluarea daunelor și recuperarea etapizată.
- Menținerea operațiunilor până la recuperare
  - Măsurile de continuitate ar trebui să susțină funcțiile esențiale până la restabilirea completă.
  - Pentru menținerea operațiunilor, ar trebui utilizate soluții temporare, sisteme redundante sau proceduri manuale, acolo unde este necesar.
- Prioritizarea recuperării
  - Analiza impactului asupra activității și clasificarea sistemelor ar trebui utilizate pentru definirea priorităților de recuperare.
  - Sistemele ar trebui clasificate în funcție de impactul pierderii disponibilității, integrității sau confidențialității, acordând o atenție specială mediilor OT critice pentru siguranță.
- Asigurarea rezilienței datelor
  - Ar trebui implementate soluții robuste de backup pentru permiterea restaurării rapide și fiabile a datelor.
  - Backup-urile ar trebui securizate și testate periodic.
- Monitorizarea și reacția
  - Sistemele ar trebui monitorizate continuu pentru detecția din timp a eventualelor întreruperi.

- Ar trebui luate acțiuni de răspuns rapid pentru minimizarea impactului operațional.

- Testarea și îmbunătățirea
  - Procedurile de recuperare ar trebui testate periodic pentru a asigura eficacitatea acestora.
  - Acțiunile de recuperare ar trebui documentate și revizuite pentru îmbunătățirea gradului de pregătire în timp.

RC.RP-05

Se verifică integritatea activelor restaurate, sunt restaurate sistemele și serviciile și se confirmă starea normală de funcționare.

RC.RP-05.1

Integritatea sistemelor și a activelor restaurate trebuie verificată înainte de repunerea în funcțiune. Sistemele și serviciile trebuie restaurate complet, iar funcționarea normală trebuie confirmată.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că sistemele și serviciile nu sunt doar restaurate după un incident, ci și verificate pentru a asigura că sunt sigure, necompromise și complet funcționale înainte de a reveni la funcționarea normală.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Sistemele restaurate ar trebui verificate pentru semne de compromitere, precum malware sau acces neautorizat, înainte de a fi readuse în funcțiune.
- Cauza principală a incidentului ar trebui identificată și remediată pentru prevenirea repetării acestuia.
- Toate acțiunile de recuperare ar trebui revizuite pentru a asigura că au fost realizate corect și că nu mai există lacune de securitate.
- O verificare finală ar trebui să confirme că sistemul este sigur, complet și pregătit pentru utilizarea normală.

RC.RP-06

Finalizarea recuperării incidentului este declarată pe baza unor criterii, iar documentația referitoare la incident este completată.

RC.RP-06.1

Finalizarea recuperării incidentului trebuie declarată formal, pe baza unor criterii predefinite, iar toată documentația referitoare la incident trebuie completată și revizuită.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că procesul de recuperare după incident este încheiat în mod oficial și responsabil și că este completată o documentație cuprinzătoare pentru a sprijini răspunderea, învățarea și pregătirea pentru viitor.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Ar trebui întocmit un raport post-acțiune care să includă:
  - Un rezumat al incidentului și al impactului acestuia.
  - Pașii urmați pentru răspuns și recuperare.
  - Lecțiile învățate și recomandările pentru îmbunătățire.
- Înainte de a declara faza de recuperare finalizată, ar trebui îndeplinite următoarele criterii:
  - Toate sistemele și serviciile afectate sunt deplin operaționale.
  - Nu mai există amenințări sau vulnerabilități cunoscute în mediu.
  - Datele au fost restaurate și verificate din punct de vedere al integrității.
  - Au fost aplicate patch-urile sau actualizările de securitate necesare.
  - Este efectuată monitorizarea pentru detecția oricărei probleme recurente sau conexe.
  - Raportul post-acțiune este finalizat și revizuit de părțile interesate relevante.
  - Toate părțile interesate sunt informate că incidentul a fost rezolvat.

[RC.CO] COMUNICAREA PRIVIND RECUPERAREA INCIDENTULUI

Activitățile de restaurare sunt coordonate cu părțile interne și externe.

RC.CO-03

Activitățile de recuperare și progresul înregistrat în restabilirea capabilităților operaționale sunt comunicate părților interesate interne și externe desemnate.

RC.CO-03.1

Activitățile de recuperare și progresul înregistrat în restabilirea capabilităților operaționale trebuie comunicate părților interesate interne și externe desemnate, în conformitate cu procedurile de comunicare stabilite.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că eforturile de recuperare și progresul restabilirii capabilităților operaționale sunt comunicate în mod clar și consecvent tuturor părților interesate interne și externe relevante. Aceasta sprijină transparența, coordonarea și luarea de decizii informate în timpul fazei de recuperare a unui incident.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Actualizările privind recuperarea, inclusiv progresul înregistrat în ceea ce privește restabilirea sistemelor și serviciilor, ar trebui comunicate în mod securizat și consecvent părților interesate interne și externe, în conformitate cu planurile de răspuns ale organizației și acordurile de schimb de informații.
- Conducerea superioară ar trebui să primească actualizări periodice cu privire la stadiul eforturilor de recuperare, în special în cazul incidentelor majore.
- Protocoalele de comunicare definite în contractele cu furnizorii și partenerii ar trebui respectate pentru asigurarea unui schimb de informații prompt și precis.
- Comunicarea de criză cu furnizorii critici ar trebui coordonată pentru sprijinirea acțiunilor de recuperare aliniate.
- Dacă nu s-au produs incidente reale, ar trebui să fie organizate exerciții teoretice pentru testarea și validarea procedurilor de comunicare în caz de recuperare și coordonarea părților interesate.

RC.CO-04

Actualizările publice privind recuperarea în urma incidentelor sunt comunicate utilizând metode și mesaje aprobate.

RC.CO-04.1

Actualizările publice privind recuperarea în urma incidentelor trebuie comunicate utilizând metode de comunicare și mesaje aprobate, în conformitate cu procedurile stabilite.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că comunicarea publică în timpul fazei de recuperare a unui incident este exactă, oportună și transmisă prin canale aprobate, pentru menținerea încrederii, gestionarea riscului reputațional și respectarea obligațiilor legale sau de reglementare.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Metodele aprobate pentru comunicarea publică, precum comunicatele de presă, site-urile web oficiale sau purtătorii de cuvânt desemnați, ar trebui definite în prealabil și utilizate în mod consecvent.
- Ar trebui stabilite și menținute informațiile de contact ale părților relevante (de exemplu, personalul intern, vânzătorii terți, autoritățile de aplicare a legii, furnizorii de asigurări cibernetice, agențiile guvernamentale).
- Listele de contacte ar trebui revizuite și verificate periodic (de exemplu, anual) pentru a asigura acuratețea acestora.
- Ar trebui identificate mecanismele de comunicare primare și secundare (de exemplu, apeluri telefonice, e-mailuri, scrisori), având în vedere că unele metode pot fi indisponibile în timpul unui incident.
- Protocoalele și mecanismele de comunicare ar trebui revizuite periodic sau atunci când au loc modificări organizaționale semnificative.
- Dacă nu au avut loc incidente reale, ar trebui să fie organizate exerciții teoretice sau simulări pentru testarea procedurilor de comunicare publică și asigurarea pregătirii.

RC.CO-04.2

Organizația trebuie să desemneze un specialist în relații publice (PRO) pentru gestionarea comunicării publice în timpul recuperării în urma incidentelor de securitate cibernetică sau a informației, asigurând că actualizările publice sunt comunicate, menținând în același timp confidențialitatea, integritatea și acuratețea informațiilor.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că, pe parcursul recuperării după un incident de securitate cibernetică sau a informației, comunicarea publică este gestionată în mod profesionist, este corectă și aliniată cu standardele de confidențialitate și integritate ale organizației. Prin desemnarea unui PRO, organizația se asigură că mesajele publice sunt gestionate de o persoană fizică instruită, care poate menține încrederea, proteja reputația organizației și respecta cerințele legale și de reglementare.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Desemnarea unui PRO:
    - Desemnarea unei persoane fizice calificate care să gestioneze comunicarea publică în timpul recuperării în urma incidentului. Fișa postului PRO poate include următoarele:
        - Elaborarea strategiilor de comunicare.
        - Redactarea și distribuirea comunicatelor de presă.
        - Construirea și menținerea relațiilor cu jurnaliștii și mass-media pentru asigurarea unei acoperiri pozitive (relații cu mass-media).
        - Gestionarea comunicării în timpul crizelor pentru menținerea reputației organizației (managementul crizelor).
        - Urmărirea acoperirii mediatice și efectuarea de analize media pentru evaluarea percepției publicului (monitorizarea acoperirii mediatice).
- Elaborarea protocoalelor de comunicare
    - Stabilirea unor protocoale clare pe care PRO să le respecte atunci când comunică actualizări publice, asigurând că toate informațiile mențin confidențialitatea, integritatea și acuratețea.
- Instruirea și pregătirea
    - Furnizarea de instruire pentru PRO cu privire la strategiile de comunicare în caz de incidente și asigurarea faptului că aceștia sunt pregătiți să acționeze rapid în timpul unui incident.

- Revizuiri periodice
    - Revizuirea și actualizarea periodică a protocoalelor de comunicare pentru a se adapta la noile provocări și asigurarea eficacității acestora.

RC.CO-04.3

Organizația trebuie să implementeze o strategie de comunicare de criză pentru a atenua impactul negativ pe parcursul unei crize și pentru a contribui la restabilirea reputației sale după aceasta.

GHID DE IMPLEMENTARE

Obiectivul acestui Control este de a asigura că organizația este pregătită să gestioneze comunicarea în mod eficace în timpul și după o criză, pentru minimizarea prejudiciilor aduse reputației, menținerea încrederii părților interesate și sprijinirea eforturilor de redresare.

În vederea realizării acestui obiectiv, ar trebui luate în considerare următoarele:

- Elaborarea strategiei
    - Crearea unui plan cuprinzător de comunicare de criză, care să prezinte procedurile de gestionare a comunicării în timpul și după o criză cu angajații, clienții, partenerii, autoritățile de reglementare și mass-media. Asigurarea conformității tuturor comunicărilor cu cerințele legale și cu reglementările aplicabile în domeniu.
- Atribuirea rolurilor și responsabilităților
    - Desemnarea unei echipe de comunicare de criză, inclusiv un purtător de cuvânt, care să gestioneze comunicarea publică și internă. Ar trebui considerată participarea profesioniștilor din domeniul relațiilor publice, a consilierilor juridici și a conducerii superioare a organizației.
- Stabilirea canalelor de comunicare
    - Identificarea și configurarea canalelor fiabile pentru diseminarea informațiilor, precum rețelele sociale, comunicatele de presă și platformele de comunicare internă. Acoperirea mediatică și rețelele sociale ar trebui monitorizate în mod continuu pentru identificarea informațiilor eronate sau reacțiilor publice negative. Inadvertențele ar trebui corectate imediat.
- Instruire și exerciții
    - Organizarea unor sesiuni de instruire periodice și simulări de crize pentru a asigura că echipa este pregătită să răspundă în mod eficace.
- Monitorizarea și adaptarea
    - Monitorizarea continuă a situației și adaptarea strategiei de comunicare în funcție de necesitate pentru a gestiona circumstanțele în schimbare.
- Revizuirea post-criză
    - După criză, revizuirea eforturilor de comunicare pentru identificarea lecțiilor învățate și pentru îmbunătățirea răspunsurilor viitoare.

Aplicabilitatea Controalelor pe niveluri de asigurare

Controalele marcate ca Măsuri cheie și Controalele aferente Aspectelor de management sunt prevăzute în tabelul următor. Semnul „X” din coloanele „Nivelul de Bază”, „Nivelul Important” și „Nivelul Esențial” indică faptul că respectivul Control se aplică la nivelul de asigurare corespunzător. Coloana „Măsură cheie” marchează, prin semnul „X”, Controalele care trebuie tratate cu prioritate, iar coloana „Aspect de management” marchează, prin semnul „X”, Controalele aferente Aspectelor de management.

Nr. crt.	Codul Controlului	Nivelul de Bază	Nivelul Important	Nivelul Esențial	Măsură cheie	Aspect de management
GUVERNARE (GV)						
1	GV.OC-01.1		**X**	**X**		
2	GV.OC-02.1			**X**		
3	GV.OC-03.1	**X**	**X**	**X**		
4	GV.OC-03.2		**X**	**X**		
5	GV.OC-04.1		**X**	**X**		
6	GV.OC-04.2		**X**	**X**		
7	GV.OC-04.3			**X**		
8	GV.OC-04.4			**X**		
9	GV.OC-05.1		**X**	**X**		
10	GV.OV-02.1			**X**		
11	GV.OV-03.1			**X**		
12	GV.PO-01.1	**X**	**X**	**X**		
13	GV.PO-01.2		**X**	**X**		
14	GV.RM-01.1		**X**	**X**		**X**
15	GV.RM-02.1		**X**	**X**		**X**
16	GV.RM-03.1	**X**	**X**	**X**		
17	GV.RM-03.2		**X**	**X**		**X**
18	GV.RM-04.1		**X**	**X**		
19	GV.RM-05.1		**X**	**X**		
20	GV.RR-01.1			**X**		
21	GV.RR-02.1		**X**	**X**	**X**	**X**
22	GV.RR-02.2			**X**		**X**
23	GV.RR-03.1		**X**	**X**		
24	GV.RR-03.2		**X**	**X**		

25	GV.RR-04.1	**X**	**X**	**X**		
26	GV.RR-04.2		**X**	**X**		
27	GV.SC-01.1			**X**		**X**
28	GV.SC-02.1		**X**	**X**		
29	GV.SC-03.1			**X**		
30	GV.SC-05.1		**X**	**X**		
31	GV.SC-05.2			**X**	**X**	
32	GV.SC-05.3			**X**	**X**	
33	GV.SC-06.1			**X**		
34	GV.SC-07.1		**X**	**X**		
35	GV.SC-07.2			**X**		
36	GV.SC-07.3			**X**		
37	GV.SC-07.4			**X**		
38	GV.SC-08.1		**X**	**X**		
39	GV.SC-09.1			**X**		
40	GV.SC-10.1			**X**		
IDENTIFICARE (ID)						
41	ID.AM-01.1	**X**	**X**	**X**		
42	ID.AM-01.2		**X**	**X**		
43	ID.AM-01.3		**X**	**X**		
44	ID.AM-01.4			**X**		
45	ID.AM-02.1	**X**	**X**	**X**		
46	ID.AM-02.2		**X**	**X**		
47	ID.AM-02.3		**X**	**X**		
48	ID.AM-02.4		**X**	**X**		
49	ID.AM-02.5			**X**		
50	ID.AM-03.2		**X**	**X**		
51	ID.AM-03.3			**X**	**X**	
52	ID.AM-04.1		**X**	**X**		
53	ID.AM-04.2			**X**		
54	ID.AM-05.1	**X**	**X**	**X**		
55	ID.AM-07.1	**X**	**X**	**X**		
56	ID.AM-07.2		**X**	**X**		
57	ID.AM-08.2	**X**	**X**	**X**	**X**	

58	ID.AM-08.3		**X**	**X**		
59	ID.AM-08.4		**X**	**X**		
60	ID.AM-08.5			**X**		
61	ID.AM-08.6		**X**	**X**		
62	ID.AM-08.7			**X**	**X**	
63	ID.AM-08.8		**X**	**X**		
64	ID.AM-08.9			**X**	**X**	
65	ID.AM-08.10			**X**	**X**	
66	ID.AM-08.11		**X**	**X**		
67	ID.AM-08.12		**X**	**X**		
68	ID.AM-08.13			**X**		
69	ID.IM-02.1		**X**	**X**		
70	ID.IM-03.1	**X**	**X**	**X**		
71	ID.IM-03.2		**X**	**X**		
72	ID.IM-03.3		**X**	**X**		
73	ID.IM-03.4		**X**	**X**		
74	ID.IM-03.5		**X**	**X**		
75	ID.IM-03.6		**X**	**X**		
76	ID.IM-03.7			**X**		
77	ID.IM-03.8			**X**		
78	ID.IM-03.9			**X**		**X**
79	ID.IM-04.1		**X**	**X**		**X**
80	ID.IM-04.2			**X**		**X**
81	ID.RA-01.1	**X**	**X**	**X**		
82	ID.RA-01.2		**X**	**X**		
83	ID.RA-01.3		**X**	**X**		
84	ID.RA-01.4			**X**		
85	ID.RA-01.5		**X**	**X**		
86	ID.RA-01.6		**X**	**X**		
87	ID.RA-02.1		**X**	**X**		
88	ID.RA-02.2			**X**		
89	ID.RA-03.1		**X**	**X**		
90	ID.RA-05.1	**X**	**X**	**X**		
91	ID.RA-05.2		**X**	**X**		**X**

92	ID.RA-05.3			**X**		**X**
93	ID.RA-06.1		**X**	**X**		**X**
94	ID.RA-08.1		**X**	**X**	**X**	
95	ID.RA-08.2			**X**		
PROTECȚIE (PR)						
96	PR.AA-01.1	**X**	**X**	**X**	**X**	
97	PR.AA-01.2		**X**	**X**		
98	PR.AA-01.3			**X**		
99	PR.AA-01.4			**X**		
100	PR.AA-01.5			**X**		
101	PR.AA-02.1		**X**	**X**		
102	PR.AA-02.2			**X**		
103	PR.AA-03.1	**X**	**X**	**X**		
104	PR.AA-03.2	**X**	**X**	**X**	**X**	
105	PR.AA-03.3		**X**	**X**	**X**	
106	PR.AA-03.4			**X**		
107	PR.AA-03.5			**X**		
108	PR.AA-04.1			**X**		
109	PR.AA-05.1	**X**	**X**	**X**	**X**	
110	PR.AA-05.2	**X**	**X**	**X**	**X**	
111	PR.AA-05.3	**X**	**X**	**X**	**X**	
112	PR.AA-05.4	**X**	**X**	**X**	**X**	
113	PR.AA-05.5		**X**	**X**		
114	PR.AA-05.6		**X**	**X**		
115	PR.AA-05.7		**X**	**X**		
116	PR.AA-05.8			**X**		
117	PR.AA-05.9			**X**		
118	PR.AA-06.1	**X**	**X**	**X**		
119	PR.AA-06.2		**X**	**X**		
120	PR.AA-06.3			**X**		
121	PR.AA-06.4			**X**		
122	PR.AT-01.1	**X**	**X**	**X**		
123	PR.AT-01.2		**X**	**X**		
124	PR.AT-01.3		**X**	**X**		

125	PR.AT-01.4			**X**		
126	PR.AT-02.1		**X**	**X**		
127	PR.AT-02.2		**X**	**X**		
128	PR.AT-02.3		**X**	**X**		
129	PR.DS-01.1		**X**	**X**		
130	PR.DS-01.2			**X**		
131	PR.DS-01.3			**X**		
132	PR.DS-01.4		**X**	**X**		
133	PR.DS-01.5		**X**	**X**		
134	PR.DS-01.6			**X**		
135	PR.DS-01.9	**X**	**X**	**X**		
136	PR.DS-02.1			**X**	**X**	
137	PR.DS-02.2			**X**		
138	PR.DS-10.1			**X**		
139	PR.DS-11.1	**X**	**X**	**X**	**X**	
140	PR.DS-11.2		**X**	**X**		
141	PR.DS-11.3		**X**	**X**		
142	PR.DS-11.4			**X**		
143	PR.DS-11.5			**X**		
144	PR.IR-01.1	**X**	**X**	**X**	**X**	
145	PR.IR-01.2	**X**	**X**	**X**	**X**	
146	PR.IR-01.3		**X**	**X**	**X**	
147	PR.IR-01.4		**X**	**X**	**X**	
148	PR.IR-01.5			**X**		
149	PR.IR-01.6			**X**		
150	PR.IR-01.7			**X**		
151	PR.IR-01.8			**X**		
152	PR.IR-01.9			**X**		
153	PR.IR-02.1		**X**	**X**		
154	PR.IR-02.2			**X**		
155	PR.IR-03.1			**X**		
156	PR.IR-04.1		**X**	**X**		**X**
157	PR.PS-01.1		**X**	**X**	**X**	
158	PR.PS-01.2			**X**		

159	PR.PS-01.3			**X**		
160	PR.PS-01.4			**X**		
161	PR.PS-01.5			**X**		
162	PR.PS-02.1		**X**	**X**		
163	PR.PS-03.1		**X**	**X**		
164	PR.PS-04.1	**X**	**X**	**X**	**X**	
165	PR.PS-04.2		**X**	**X**		
166	PR.PS-04.3		**X**	**X**		
167	PR.PS-04.4			**X**		
168	PR.PS-04.5			**X**		
169	PR.PS-05.1	**X**	**X**	**X**		
170	PR.PS-05.2		**X**	**X**		
171	PR.PS-06.1		**X**	**X**		
172	PR.PS-06.2		**X**	**X**		
173	PR.PS-06.3			**X**		
174	PR.PS-06.4			**X**		
DETECȚIE (DE)						
175	DE.AE-02.1		**X**	**X**		
176	DE.AE-02.2			**X**		
177	DE.AE-03.1	**X**	**X**	**X**	**X**	
178	DE.AE-03.2		**X**	**X**		
179	DE.AE-03.3			**X**		
180	DE.AE-04.1			**X**		**X**
181	DE.AE-06.1		**X**	**X**		
182	DE.AE-08.1		**X**	**X**		
183	DE.CM-01.1	**X**	**X**	**X**		
184	DE.CM-01.2	**X**	**X**	**X**	**X**	
185	DE.CM-01.3		**X**	**X**	**X**	
186	DE.CM-01.4			**X**		
187	DE.CM-02.1		**X**	**X**		
188	DE.CM-02.2			**X**		
189	DE.CM-03.1	**X**	**X**	**X**		
190	DE.CM-03.2		**X**	**X**		
191	DE.CM-06.1		**X**	**X**		

192	DE.CM-06.2		**X**	**X**		
193	DE.CM-09.1		**X**	**X**		
194	DE.CM-09.2			**X**		
195	DE.CM-09.3			**X**		
196	DE.CM-09.4			**X**		
RĂSPUNS (RS)						
197	RS.AN-03.1			**X**		
198	RS.AN-06.1			**X**		
199	RS.AN-07.1			**X**		
200	RS.AN-08.1			**X**		
201	RS.CO-02.1	**X**	**X**	**X**		
202	RS.CO-02.2		**X**	**X**	**X**	
203	RS.MA-01.1	**X**	**X**	**X**		
204	RS.MA-01.2		**X**	**X**		
205	RS.MA-02.1		**X**	**X**		
206	RS.MA-02.2			**X**		
207	RS.MA-03.1		**X**	**X**		
208	RS.MA-05.1		**X**	**X**		
209	RS.MI-01.1		**X**	**X**		
210	RS.MI-01.2		**X**	**X**	**X**	
RECUPERARE (RC)						
211	RC.CO-03.1		**X**	**X**		**X**
212	RC.CO-04.1		**X**	**X**		
213	RC.CO-04.2			**X**		
214	RC.CO-04.3			**X**		
215	RC.RP-01.1	**X**	**X**	**X**		
216	RC.RP-02.1			**X**		
217	RC.RP-05.1		**X**	**X**		
218	RC.RP-06.1		**X**	**X**		

Anexa nr. 2

METODOLOGIA

de autoevaluare a maturității măsurilor de gestionare a riscurilor de securitate cibernetică

Articolul 1

(1) Directoratul Național de Securitate Cibernetică dezvoltă și pune la dispoziția tuturor entităților esențiale și importante două mecanisme destinate stabilirii nivelului de maturitate a măsurilor de gestionare a riscurilor de securitate cibernetică ale entității, în conformitate cu art. 12 alin. (4) și art. 37 alin. (8) lit. b) din Ordonanța de urgență a Guvernului nr. 155/2024, respectiv:

a) Platforma NIS2@RO;
b) instrumentele de evaluare a maturității măsurilor de gestionare a riscurilor de securitate cibernetică, corespunzătoare fiecărui nivel de asigurare: EVAL_MMS_B pentru nivelul de Bază, EVAL_MMS_I pentru nivelul Important și EVAL_MMS_E pentru nivelul Esențial.

(2) În cazul în care Platforma NIS2@RO este indisponibilă, se utilizează instrumentele de evaluare a maturității, care se descarcă de pe website-ul oficial al Directoratului Național de Securitate Cibernetică (https://www.dnsc.ro/) și se utilizează la nivel local, conform instrucțiunilor publicate.

Articolul 2

(1) Pentru calcularea scorului de maturitate, reprezentând gradul de conformitate al entității cu Controalele aplicabile nivelului său de asigurare, se atribuie o valoare număr întreg de la 1 la 5 fiecăruia dintre următorii doi parametri atașați fiecărui Control:

a) Maturitatea documentației, care măsoară gradul în care regulile și procedurile scrise satisfac cerințele Controlului;
b) Maturitatea implementării, care măsoară gradul în care practicile operaționale efective corespund Controlului și documentației aferente.

(2) Este obligatorie completarea variabilelor „Scor documentație” și „Scor implementare” pentru fiecare Control.

(3) Atribuirea valorilor prevăzute la alin. (1) se determină prin evaluarea satisfacerii criteriilor și valorilor de prag conform stadiilor de maturitate predefinite, astfel:

a) Stadiul 1 - Inițial: valoarea maturității 1; așteptări privind nivelul de maturitate a documentației - „nu există documentație a procesului sau aceasta nu este aprobată oficial de către conducere”; așteptări privind nivelul de maturitate a implementării - „nu există un proces standard”;
b) Stadiul 2 - Repetabil: valoarea maturității 2; așteptări privind nivelul de maturitate a documentației - „există documentație a procesului aprobată oficial, dar care nu a fost revizuită

în ultimii 2 ani”; așteptări privind nivelul de maturitate a implementării - „există un proces ad-hoc, desfășurat în mod informal”;

c) Stadiul 3 - Definit: valoarea maturității 3; așteptări privind nivelul de maturitate a documentației - „există documentație a procesului aprobată oficial, iar excepțiile sunt documentate și aprobate; excepțiile documentate și aprobate reprezintă mai puțin de 5% din cazuri”; așteptări privind nivelul de maturitate a implementării - „există un proces formal, care este implementat; sunt disponibile dovezi pentru majoritatea activităților; excepțiile de proces sunt mai puțin de 10%”;

d) Stadiul 4 - Gestionat: valoarea maturității 4; așteptări privind nivelul de maturitate a documentației - „există documentație a procesului aprobată oficial, iar excepțiile sunt documentate și aprobate; excepțiile documentate și aprobate reprezintă mai puțin de 3% din cazuri”; așteptări privind nivelul de maturitate a implementării - „există un proces formal, care este implementat; sunt disponibile dovezi pentru toate activitățile; sunt colectate și raportate metrici detaliate ale procesului; a fost stabilită o țintă minimă pentru metrici; excepțiile de proces sunt mai puțin de 5%”;

e) Stadiul 5 - Optimizare: valoarea maturității 5; așteptări privind nivelul de maturitate a documentației - „există documentație a procesului aprobată oficial, iar excepțiile sunt documentate și aprobate; excepțiile documentate și aprobate reprezintă mai puțin de 0,5% din cazuri”; așteptări privind nivelul de maturitate a implementării - „există un proces formal, care este implementat; sunt disponibile dovezi pentru toate activitățile; sunt colectate și raportate metrici detaliate ale procesului; a fost stabilită o țintă minimă pentru metrici, care se îmbunătățește continuu; excepțiile de proces sunt mai puțin de 1%”.

(4) Variabilelor „Scor documentație” și „Scor implementare” le este atribuită valoarea numerică corespunzătoare de la 1 la 5, aferentă stadiului de maturitate stabilit potrivit alin. (3).

(5) Pentru fiecare Control se atribuie valori pentru „Scor documentație” și „Scor implementare”, potrivit alin. (4). Fiecare valoare este justificată în scris, prin informații și argumente.

(6) Pentru fiecare Subcategorie se calculează „Scor maturitate documentație” și „Scor maturitate implementare” ca medie aritmetică a valorilor corespunzătoare ale Controalelor din acea Subcategorie.

(7) Pentru fiecare Categorie se calculează „Scor maturitate documentație” și „Scor maturitate implementare” ca medie aritmetică a valorilor corespunzătoare ale Subcategoriilor din acea Categorie.

(8) Pentru fiecare Categorie se calculează scorul de maturitate ca medie aritmetică a scorurilor prevăzute la alin. (7).

(9) Scorul total de maturitate al entității se obține ca medie aritmetică a scorurilor de maturitate ale Categoriilor.

(10) Scorurile pe Controale și pe Categorii, precum și scorul total de maturitate al entității, indică totodată ecartul față de scorurile-țintă necesare pentru atingerea conformității.

(11) Pentru atingerea conformității, valorile obținute de entitate în urma autoevaluării sunt cel puțin egale cu următoarele scoruri-țintă, stabilite pentru fiecare nivel de asigurare:

a) pentru nivelul de Bază: scorul-țintă al fiecărui Control marcat ca Măsură cheie este de cel puțin 2,5, iar scorul-țintă total al entității este de cel puțin 2,5;
b) pentru nivelul Important: scorul-țintă al fiecărui Control marcat ca Măsură cheie este de cel puțin 3, iar scorul-țintă total al entității este de cel puțin 3;
c) pentru nivelul Esențial: scorul-țintă al fiecărui Control marcat ca Măsură cheie este de cel puțin 3, scorul-țintă total al fiecărei Categorii este de cel puțin 3, iar scorul general al entității este de cel puțin 3,5.

Articolul 3

Atunci când, în urma autoevaluării, nu sunt atinse scorurile-țintă aferente nivelului de asigurare evaluat, prevăzute la art. 2, entitatea are obligația de a întocmi un plan de măsuri pentru remedierea tuturor deficiențelor care au condus la neconformitate, plan ce cuprinde acțiunile ce urmează a fi întreprinse și termenele asumate pentru implementare.

EDITOR: PARLAMENTUL ROMÂNIEI — CAMERA DEPUTAȚILOR

MONITORUL OFICIAL

„Monitorul Oficial” R.A., Str. Parcului nr. 65, sectorul 1, București; 012329
C.I.F. RO427282, IBAN: RO55RNCB0082006711100001 BCR
și IBAN: RO12TREZ7005069XXX000531 DTCPMB (alocat numai persoanelor juridice bugetare)
Tel. 021.318.51.29/150, fax 021.318.51.15, e-mail: marketing@ramo.ro, www.monitoruloficial.ro

Relații cu publicul: șos. Panduri nr. 1, bloc P33, sectorul 5, București; 050651.
Tel. 021.401.00.73, 021.401.00.78/79/83.
Pentru publicări, încărcați actele pe site, la: https://www.monitoruloficial.ro, secțiunea Publicări.

5 948493 651130

Monitorul Oficial al României, Partea I, nr. 712 bis/28.VIII.2026 conține 324 de pagini. Prețul: 486 lei **ISSN** 1453—4495

Acest număr al Monitorului Oficial al României a fost tipărit în afara abonamentului.