

Reziliența cibernetică și strategia de securitate cibernetică

Măsuri tehnice și organizatorice esențiale pentru sectoarele critice în contextul geopolitic actual

Romeo Andreica,

CISO

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII

UNIVERSITATEA TEHNICĂ

Contextul geopolitic și presiunile cibernetice - introdcere

Războiul hibrid și proliferarea atacurilor asupra infrastructurilor esențiale.

Actori statali și non-statali vizează energia, transporturile, comunicațiile și sănătatea.

Amenințări multidimensionale: tehnice si AI, context remote-work, informaționale și psihologice.

Notă: În 2024, peste 60% dintre atacurile APT din Europa au vizat infrastructuri critice (ENISA Threat Landscape).

Reziliența cibernetică și strategia de securitate cibernetică

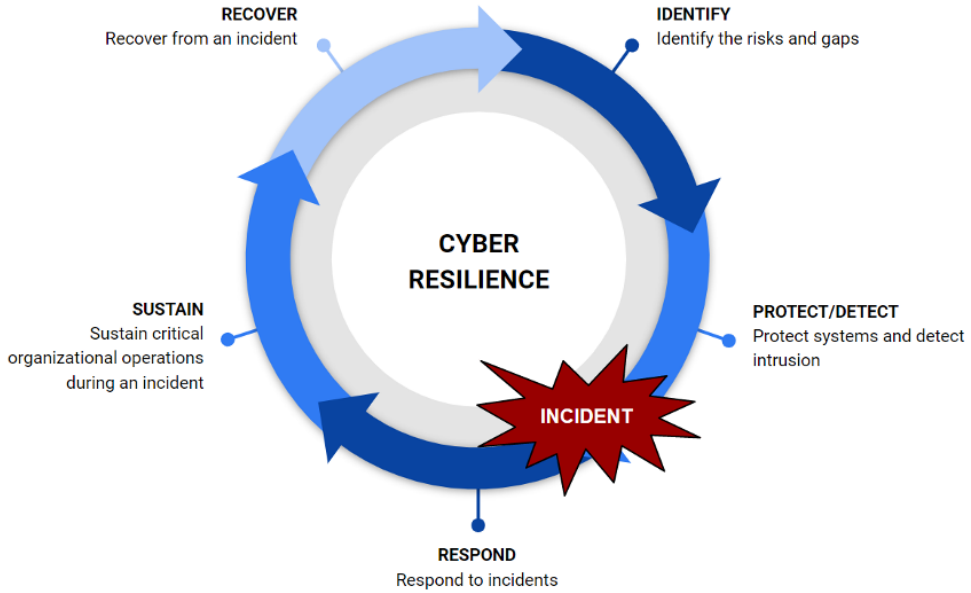
- Perspective strategice de securitate
- Reziliența cibernetica - entități critice importante și esențiale
- Implementarea măsurilor tehnice și organizatorice esențiale
- Utilizarea framework-ului CyFun (Cyber Fundamentals), corelat cu Directiva NIS2 adoptat la nivel UE

Cadrul european: NIS2 și CyFun



- NIS2 și OUG 155/2024 stabilesc cerințe de securitate pentru operatorii de servicii importante și esențiale.
- CyFun Belgia oferă un model operațional pentru implementarea practică a acestor cerințe.
- Nivelurile de asigurare: **Basic** → **Important** → **Essential**.
- **GV.OC-01.1** – Misiunea organizației trebuie să fundamenteze managementul riscului cibernetic.
- **GV.RM-01.1** – Stabilirea obiectivelor de securitate aprobate la nivel managerial.
- *Notă: Modelul CyFun completează NIS2*

Conceptul de reziliență cibernetică



- Capacitatea unei organizații de a anticipa, rezista, răspunde și recupera în urma incidentelor cibernetice.
- Include componenta tehnică (protecție și detecție), organizațională (guvernanță), și culturală (awareness).
- **ID.IM-04.1** – Stabilirea, comunicarea și testarea planurilor de continuitate și contingență.
- **RC.CO-03.1** – Comunicarea activităților de recuperare către părțile interesate interne și externe
- *Notă: Reziliența nu este o reacție la atac, ci o cultură organizațională integrată.*

Managementul riscului și îmbunătățirea continuă



- Reziliența se bazează pe evaluarea periodică a riscurilor și adaptarea controalelor.
- **GV.RM-03.2** – Riscurile cibernetice trebuie integrate în procesele de management al riscurilor organizației.
- **ID.RA-05.3** – Rezultatele evaluărilor de risc trebuie comunicate părților relevante.
- **ID.IM-03.3** – Lecțiile învățate și evaluările trebuie traduse în îmbunătățiri concrete.
- *Notă: Ciclul PDCA (Plan–Do–Check–Act) este fundamentul oricărei reziliențe sustenabile.*

Guvernanță și leadership cybernetic



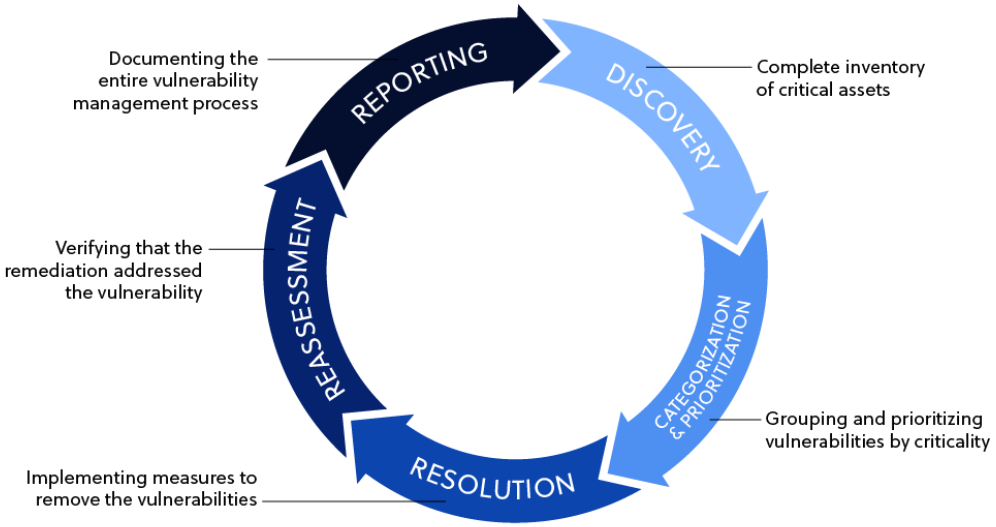
- Reziliența depinde de implicarea managementului de vârf.
- **GV.RR-01.1** – Conducerea organizației este responsabilă și răspunzătoare pentru riscurile cibernetice.
- **GV.RR-02.2** – Se va desemna un CISO cu nivel executiv.
- **GV.OV-03.1** – Performanța în managementul riscului cibernetic se va evalua și ajusta periodic.
- *Notă: CISO-ul trebuie să facă parte din structura strategică, nu doar din cea tehnică.*

Managementul identității și accesului



- Controlul accesului este esențial pentru limitarea mișcărilor laterale și compromiterii interne.
- **PR.AA-03.2** – Se va implementa autentificare multifactor (MFA) pentru acces remote.
- **PR.AA-05.3** – Drepturile de acces vor fi limitate conform principiului „celui mai mic privilegiu”.
- **PR.AA-05.4** – Nimeni nu va deține privilegii administrative pentru activități zilnice.
- *Notă: Majoritatea breșelor din infrastructurile critice provin din acces excesiv sau necontrolat.*

Managementul vulnerabilităților și actualizărilor



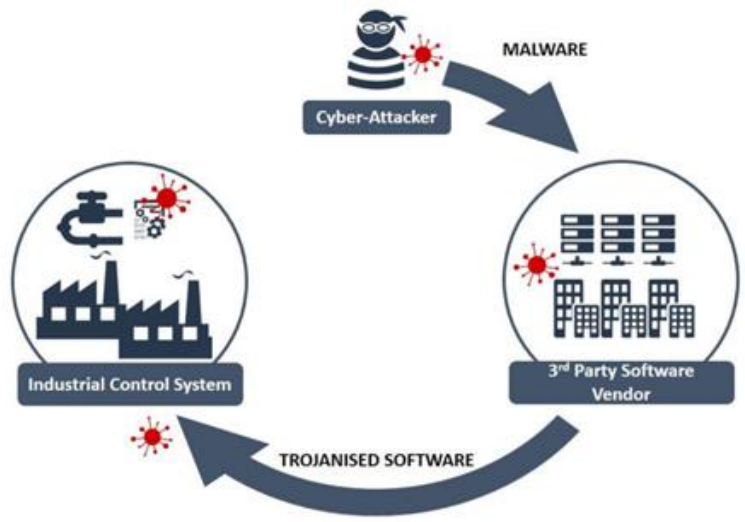
- Identificarea și remedierea proactivă a vulnerabilităților tehnice.
- **ID.RA-08.1** – Implementarea unui plan de management al vulnerabilităților și CVD (Coordinated Vulnerability Disclosure).
- **ID.IM-03.9** – Realizarea de evaluări specializate: scanning, testare de vulnerabilități, evaluarea amenințărilor interne.
- *Notă: Un proces CVD bine implementat reduce timpul de reacție și îmbunătățește cooperarea cu cercetătorii.*

Segmentarea rețelelor și protecția mediilor IT/OT



- Separarea logică a rețelelor critice previne propagarea amenințărilor.
- **PR.IR-01.2** – Implementarea segmentării și segregării rețelei pe baza zonelor de încredere.
- **PR.IR-01.4** – Implementarea măsurilor de protecție la frontierele IT/OT și monitorizarea comunicațiilor.
- *Notă: Segmentarea este pilonul de bază al rezilienței industriale.*

Securitatea lanțului de aprovizionare



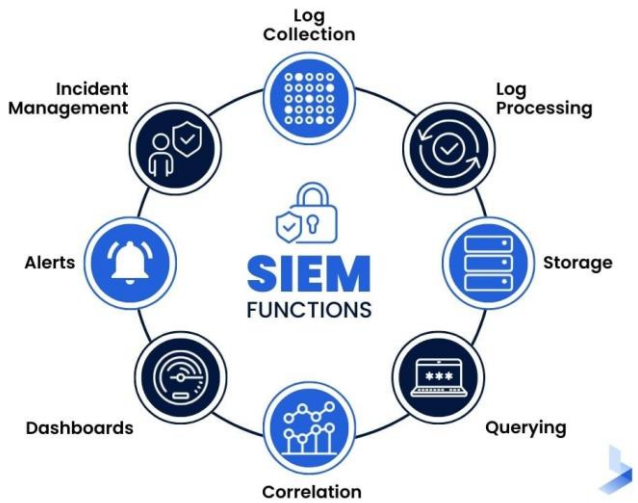
- Compromiterea furnizorilor este una dintre principalele surse de atac.
- **GV.SC-05.2** – Introducerea cerințelor de securitate cibernetică în contractele cu furnizorii.
- **GV.SC-05.3** – Stabilirea dreptului organizației de a audita programele de securitate ale terților.
- **GV.SC-03.1** – Integrarea riscului lanțului de aprovizionare în procesul global de management al riscului.
- *Notă: Reziliența se construiește prin controlul lanțului extins, nu doar al perimetrului propriu.*

Monitorizare, detecție și răspuns



- Implementarea capacităților SOC/SIEM/IDS pentru detecție timpurie.
- **DE.CM-01.3** – Monitorizarea utilizării neautorizate a sistemelor critice (conexiuni locale, rețea, remote).
- **DE.AE-04.1** – Evaluarea impactului evenimentelor detectate asupra operațiunilor și activelor.
- **RS.MI-01.2** – Detectarea accesului neautorizat sau a scurgerilor de date și acțiuni de atenuare imediată.
- *Notă: O infrastructură fără detecție activă este o infrastructură deja compromisă.*

Monitorizare avansată și analiză a evenimentelor



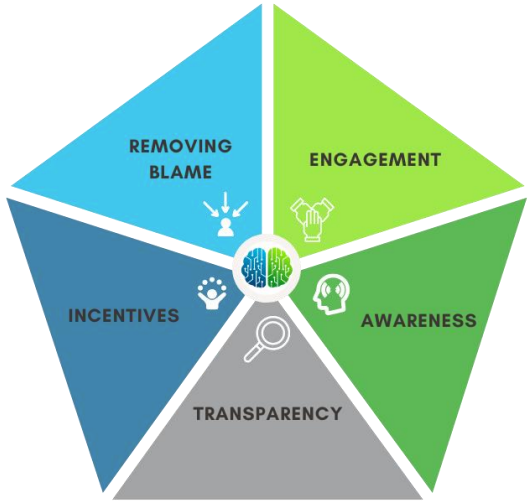
- Detectarea devine eficientă doar prin corelarea inteligentă a surselor multiple.
- **DE.AE-03.1** – Funcționalitățile de logare ale sistemelor de protecție/detecție trebuie activate, arhivate și analizate.
- **DE.AE-04.1** – Impactul evenimentelor detectate trebuie evaluat și corelat cu riscurile identificate.
- **ID.IM-03.9** – Se vor efectua teste avansate (scanning, simulări atacuri, evaluare insider threat).
- *Notă: Integrarea SIEM, IDS/IPS și threat intelligence este cheia reacției rapide și informate.*

Continuitate operațională și planificare în caz de incident



- Continuitatea serviciilor critice trebuie planificată, testată și comunicată periodic.
- **ID.IM-04.1** – Planurile de continuitate și contingență trebuie stabilite, comunicate, testate și îmbunătățite.
- **ID.IM-04.2** – Coordonarea dezvoltării și testării planurilor de răspuns la incidente împreună cu părțile interesate.
- **RC.CO-03.1** – Activitățile de recuperare și restaurare a operațiunilor vor fi comunicate stakeholderilor.
- *Notă: Un plan netestat este doar un document. Reziliența reală se dovedește în criză.*

Cultura de securitate și formarea personalului



- Factorul uman este principala poartă de intrare a atacurilor.
- Educația și conștientizarea trebuie să fie continue, nu ocazionale.
- **GV.RR-01.1** – Top managementul trebuie să promoveze o cultură etică, conștientă de riscuri și orientată spre îmbunătățire.
- **GV.OC-02.1** – Organizația trebuie să înțeleagă și să integreze nevoile stakeholderilor interni și externi privind riscurile cibernetice.
- *Notă: Reziliența se construiește prin oameni informați și responsabili, nu doar prin tehnologii.*

Protecția datelor și a mediilor portabile



- Dispozitivele externe pot fi vectori majori de compromitere.
- **PR.DS-02.1** – Mediile de stocare portabile cu date de sistem trebuie controlate și protejate în tranzit și stocare.
- **ID.AM-08.9** – Uneltele de mentenanță și dispozitivele portabile trebuie scanate anti-malware înainte de utilizare.
- **ID.AM-08.10** – După mentenanță sau patching, controalele de securitate trebuie verificate.
- *Notă: Incidentul „Colonial Pipeline” (SUA) a arătat că o singură stație de mentenanță compromisă poate opri un sector întreg.*

Cooperarea interinstituțională și partajarea informațiilor



- Colaborarea între entitățile critice, CERT-uri și autorități este fundamentală.
- **RS.CO-02.2** – Incidentele cibernetice trebuie raportate părților externe relevante, inclusiv autorităților, în termenii prevăzuți de lege.
- **GV.SC-07.1** – Riscurile asociate furnizorilor și terților trebuie evaluate anual și la fiecare schimbare semnificativă.
- *Notă: Partajarea timpurie a informațiilor poate preveni efectul de domino în lanțurile critice.*

Performanță și indicatori de reziliență



KPIs

Track internal performance of the organization



KRIs

Track internal and external risks affecting the organization

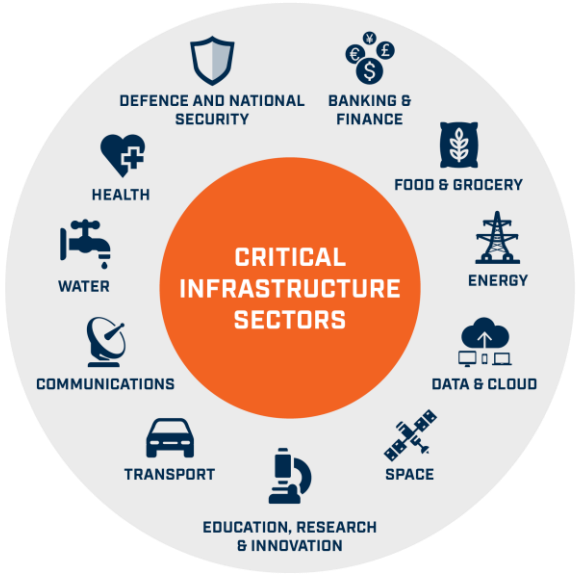
- Măsurarea performanței asigură control și progres.
- **GV.OV-02.1** – Strategia de management al riscului cibernetic trebuie revizuită și ajustată periodic.
- **GV.OV-03.1** – Performanța trebuie evaluată prin indicatori de eficiență și eficacitate.
- **MTTD** – Mean Time to Detect
- **MTTR** – Mean Time to Recover
- Rata incidentelor rezolvate în termen legal NIS2
- *Notă: Reziliența trebuie măsurată și raportată - altfel nu poate fi gestionată.*

Date statistice și tendințe 2025



- +38% creștere a atacurilor cibernetice în infrastructuri critice.
- +33% din atacuri implică lanțul de aprovizionare.
- 1 din 3 organizații critice nu are plan testat de continuitate.
- Costul mediu per incident: 4,35 milioane EUR.
- **GV.RR-03.1** – Asigurarea resurselor proporționale cu strategia de risc.
- **GV.RR-01.1** – Implicarea directă a conducerii în cultura de securitate.
- *Notă: Organizațiile reziliente investesc mai mult în prevenție și coordonare strategică.*

Recomandări pentru sectoarele critice



- Integrarea securității în cultura organizațională.
- Teste periodice (Red Team, Purple Team, Table-top).
- Partajarea amenințărilor între sectoare și state.
- **GV.RR-02.2** – CISO cu autoritate strategică în management.
- **ID.IM-03.3** – Îmbunătățire continuă prin lecțiile învățate.
- **GV.SC-03.1** – Management integrat al riscului lanțului de aprovizionare.
- *Notă: Fiecare incident trebuie privit ca o lecție colectivă, nu ca un eșec izolat.*

Concluzii



- Reziliența cibernetică este un proces, nu un produs.
- Necesită leadership, cultură și colaborare.
- Se construiește prin tehnologie, oameni și guvernanță.
- Este baza securității globale moderne.
- Nevoia de strategie de securitate.
- Investiții cu rol de pevenție – tehnic și organizatoric.
- Conștientizare și cultura organizațională.
- *Notă: Nu putem opri toate atacurile, dar putem controla cât de repede ne ridicăm după ele.” (sursa: ENISA)*





Mulțumesc !

Q/A

Romeo Andreica,

CISO

MINISTERUL EDUCAȚIEI ȘI CERCETĂRII

UNIVERSITATEA TEHNICĂ