Managementul securității sistemelor informatice

- Notițe-sinteză -

varianta martie 2026

CUPRINS

Managementul securității sistemelor informatice 1
- Notițe-sinteză - 1
CUPRINS 1
Cursul nr. 1 5
Prezentarea securității cibernetice 5
Managementul riscurilor de securitate cibernetică 5
Rolul managementului riscurilor în strategia de securitate cibernetică a organizațiilor 7
Cubul securității cibernetice 8
Managerul de securitate cibernetică. Profil, atribuții și responsabilități 8
Cursul nr. 2 9
Termeni și concepte cheie în securitatea cibernetică 9
Cursul nr. 3 11
Riscuri, amenințări și vulnerabilități de securitate cibernetică 11
Metode și tehnici pentru identificarea și atenuarea riscurilor 13
Instrumente de securitate cibernetică 13
Cursul nr. 4 15
Strategia de securitate cibernetică 16
Politica de securitate cibernetică 17
Etapele dezvoltarea și implementarea strategiilor și politicilor de securitate cibernetică 17
Rolul CISO în elaborarea și implementarea strategiilor și politicilor de securitate cibernetică 18
Cursul nr. 5 19
Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României 19
Legea nr.124 din 7 iulie 2025 pentru aprobarea Ordonantei de urgentă a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor si sistemelor informatice din spatiul cibernetic national civil 22
Ordinul DNSC nr. 1/2025 CERINŢE privind procesul de notificare în vederea înregistrării şi metoda de transmitere a informațiilor 24

Ordinul 2/2025 pentru aprobarea Criteriilor şi pragurilor de determinare a gradului de perturbare a unui serviciu şi a Metodologiei privind evaluarea nivelului de risc alentităţilor 25
Cursul nr. 6 26
Managementul răspunsului la incidente de securitate cibernetică 26
Echipa de răspuns la incidente de cecuritate cibernetică (CSIRT/CERT) 27
Recuperarea în caz de dezastre, monitorizare și asigurarea continuității 27
Instrumente de răspuns la incidente de securitate cibernetică 29
Cursul nr. 7 32
Asigurarea confidențialității și protecției datelor 33
Securitatea rețelelor 33
Securitatea aplicațiilor 34
Securitatea dispozitivelor mobile 34
Securitatea cibernetică a personalului 34
Securitatea facilităților 35
Securitatea operațională 35
Reacția la incidente și recuperarea după dezastre 35
Managementul identității și accesului 36
Educația și formarea 36
Cursul nr. 8 37
Etapa întâi. Planificarea 37
Etapa a II-a. Detecția, analiza și raportarea 37
Etapa a III-a. Evaluarea și clasificarea incidentelor 38
Etapa a IV-a. Izolarea și eradicarea 38
Etapa a V-a. Recuperarea și asigurarea continuității 38
Etapa a VI-a. Implementarea lecțiilor învățate 38
Etapa a VII-a. Comunicare, cooperare și colaborare 38
Etapa a VIII-a. Actualizarea planului de răspuns 38
Modele de organizare a răspunsului la incidente 38
Modelul in-house 39
Modelul MSSP/MSP 39
Modelul mixt 40
Alegerea modelului optim pentru gestionarea incidentelor de securitate cibernetică 41
Cursul nr. 9 42
Obiectivele auditului 42
Beneficiile auditului de conformitate 43
Tipuri de audituri de conformitate 43

Principiile auditului de conformitate 44
Livrabile 44
Recomandări în privința auditului 45
Exemplu de flux de lucru 46
Instrumente utilizate 46
Rolul CISO în auditul organizației 46
Cursul nr. 10 47
Security Operations Center (SOC) 47
Organizarea unui SOC 48
Clasificarea SOC 48
Tehnologii SOC 49
Cursul nr. 11 51
Importanța protecției datelor 51
Măsuri generale de protecție a datelor 52
Politicile de Data Loss Prevention (DLP) 52
Datele cu caracter personal (DCP) 53
Regulamentul (UE) 2016/679 (GDPR) 54
Termeni relevanți GDPR 55
Principalele cerințe ale GDPR 55
Responsabilul cu protecția datelor personale (DPO) 56
Evidența prelucrării DCP 57
Evidențe obligatorii conform GDPR 57
Evaluarea impactului asupra protecției datelor (DPIA) 59
Sancțiuni GDPR 60
Știați că… 61
Cursul nr. 12 61
Contextul global 61
Tehnologii emergente 62
Soluții inovatoare de securitate cibernetică 63
Cursul nr. 13 64
Nevoia de standardizare în magementul securității cibernetice 64
Beneficiile standardizării 65
Exemple de standarde comune 66
Acreditare, evaluare și certificare 66
Studiu de caz: CIS Controls (fost Critical Security Controls) 68
1. Inventarul și controlul activelor hardware 68
2. Inventarul și controlul activelor software 69

3. Protecția datelor 70
4. Securizarea hardware și software 70
5. Administrarea conturilor 71
6. Controlul accesului 71
7. Gestionarea continuă a vulnerabilităților 72
8. Gestionarea log-urilor/ jurnalelor de audit 72
9. Protecția pentru email și browserul web 73
10. Protecția împotriva malware-ului 74
11. Recuperarea datelor 74
12. Administrarea rețelei 75
13. Monitorizarea și protecția rețelei 75
14. Educație și formare 76
15. Gestionarea furnizorilor de servicii 77
16. Securitatea aplicațiilor 78
17. Răspunsul la incidente 79
18. Testarea de penetrare 80

Cursul nr. 1

Prezentarea securității cibernetice

- Definiția securității cibernetice
- Importanța securității cibernetice pentru organizații
- Principiile de bază ale securității cibernetice

Securitatea cibernetică reprezintă starea de normalitate a sistemelor informatice/ cibernetice, dată de totalitatea tehnologiilor, proceselor și practicilor ce sunt utilizate pentru a proteja infrastructurile, rețelele, terminalele, aplicațiile, datele și utilizatorii acestora în fața amenințărilor.

Securitatea cibernetică include activitățile necesare pentru protejarea rețelelor și a sistemelor informatice, a utilizatorilor acestor sisteme și a altor persoane afectate de amenințări cibernetice. (Regulamentul UE privind securitatea cibernetică (Comisia Europeană)

Securitatea cibernetică devine esențială pentru protejarea datelor, menținerea încrederii clienților și evitarea pierderilor financiare cauzate de incidentele cibernetice diverselor organizații.

Principiile de bază ale securității cibernetice:

- **Confidențialitate**: informațiile sunt accesibile doar persoanelor autorizate.
- **Integritate**: datele și informațiile trebuie protejate de modificări neautorizate.
- **Disponibilitate**: resursele informatice/ cibernetice sunt accesibile doar de către utilizatorii autorizați.

Managementul riscurilor de securitate cibernetică

Definiția riscurilor de securitate cibernetică

Riscurile de securitate cibernetică se referă la potențialele vulnerabilități sau amenințări care pot compromite securitatea informatică/ cibernetică. Identificarea, evaluarea și diminuare acestor riscuri sunt esențiale pentru protejarea activelor organizațiilor.

Procesul de management al riscurilor cibernetice presupune mai multe etape:

- **Identificarea riscurilor**: recunoașterea amenințărilor și vulnerabilităților existente
- **Evaluarea riscurilor**: Determinarea probabilității și impactului potențial al amenințărilor identificate asupra organizațiilor
- **Diminuarea riscurilor**: Implementarea măsurilor de securitate adecvate pentru reducerea riscurilor la un nivel acceptabil. Eliminarea riscurilor de securitate cibernetică este posibilă doar teoretic.
- **Monitorizarea și evaluarea periodică**: Supravegherea continuă a ecosistemului de securitate cibernetică și ajustarea măsurilor de securizare

conform evoluțiilor înregistrate de amenințările și vulnerabilitățile de securitate cibernetică.

Identificarea Riscurilor

Primul pas în managementul riscurilor de securitate cibernetică este identificarea riscurilor. Acesta implică o înțelegere clară a activelor digitale/informatice/cibernetice ale organizației (date, sisteme, rețele) și a potențialelor amenințări și/sau vulnerabilități care le pot compromite securitatea. Identificarea riscurilor include:

- Inventarierea activelor: cunoașterea resurselor care necesită protecție este fundamentală. Aceasta include hardware, software, date și orice alte resurse critice.
- Clasificarea datelor: Nu toate datele au aceeași valoare sau necesită același nivel de protecție. Prin urmare, este important să se clasifice datele în funcție de sensibilitatea și importanța lor.
- Identificarea amenințărilor și vulnerabilităților: Acest pas implică recunoașterea potențialelor amenințări (ex. atacuri malware, phishing, atacuri DDoS etc.) și vulnerabilități (slăbiciuni ale software-ului, configurări greșite etc.) care ar putea fi exploatate de atacatori.

Evaluarea riscurilor

După identificarea riscurilor, urmează evaluarea lor. Acest proces determină probabilitatea ca o anumită amenințare să se materializeze și impactul potențial asupra organizației. Evaluarea riscurilor ajută la prioritizarea răspunsurilor bazate pe:

- Probabilitate: Cât de probabil este ca o anumită vulnerabilitate să fie exploatată?
- Impact: Care ar fi consecințele exploatării acelei vulnerabilități? Impactul poate fi analizat din perspective financiare, operaționale, legale sau de reputație.

Matricea probabilitate-impact este un instrument esențial în managementul riscurilor, inclusiv în domeniul securității cibernetice. Acesta oferă o metodologie structurată pentru evaluarea și prioritizarea riscurilor, permițând organizațiilor să aloce resursele în mod eficient pentru diminuarea celor mai semnificative riscuri.

Matricea clasifică riscurile pe baza a două dimensiuni principale: probabilitatea ca un risc să se materializeze și impactul pe care l-ar avea acesta asupra organizației dacă se materializează.

Utilizarea matricei în managementul riscurilor cibernetice ajută la:

- Prioritizarea riscurilor: Matricea ajută la identificarea rapidă a riscurilor care necesită atenție imediată (de exemplu, riscuri cu probabilitate înaltă și impact înalt) și a celor care pot fi monitorizate sau acceptate (de exemplu, riscuri cu probabilitate scăzută și impact scăzut).
- Alocarea resurselor: Prin identificarea priorităților, organizațiile pot aloca resursele de securitate mai eficient, concentrându-se pe mitigarea riscurilor cu cel mai mare potențial de a afecta negativ operațiunile.
- Comunicarea riscurilor: Matricea oferă un cadru vizual simplu pentru comunicarea riscurilor și a strategiilor de mitigare către părțile interesate, inclusiv managementul și echipele operative.

Exemplu de aplicare a matricei

Considerăm un scenariu în care o organizație evaluează riscul unui atac ransomware. Dacă probabilitatea este considerată înaltă (datorită unei recente creșteri a atacurilor ransomware în industrie) și impactul este de asemenea înalt (de exemplu, accesul la date critice ar putea fi pierdut, afectând grav operațiunile), atunci acest risc se va plasa în zona de risc 'înalt' sau 'extrem' a matricei. Aceasta indică necesitatea unei atenții și resurse semnificative pentru diminuarea riscului.

Matricea propabilitate-impact este un instrument flexibil și puternic, care poate fi adaptat și personalizat în funcție de specificul și nevoile fiecărei organizații. Utilizarea sa sistematică în cadrul proceselor de management al riscurilor cibernetice contribuie la o mai bună înțelegere, evaluare și gestionare a riscurilor, sprijinind adoptarea unor decizii informate și strategice în domeniul securității informației.

Diminuarea riscurilor
Aceasta implică implementarea de măsuri pentru a reduce probabilitatea și/sau impactul amenințărilor identificate și poate include:

- Implementarea de soluții tehnice: Firewall, antivirus, criptare, și alte tehnologii de securitate.
- Politici și proceduri de securitate: Dezvoltarea de politici de securitate cibernetică, proceduri de răspuns la incidente și programe de formare și conștientizare a angajaților.
- Planuri de recuperare după incidente: Crearea de planuri pentru restaurarea rapidă a operațiunilor în cazul unui incident de securitate cibernetică.

Monitorizarea și revizuirea
Managementul riscurilor de securitate cibernetică este un proces continuu, nu o activitate unică. Pe măsură ce organizația se dezvoltă și peisajul amenințărilor se schimbă, este esențial să se monitorizeze în mod constant riscurile și să se ajusteze strategiile de diminuare. Acest lucru include:

- Audituri de securitate periodice: Evaluarea regulată a infrastructurii IT și a politicilor de securitate pentru a identifica noi vulnerabilități.
- Actualizarea planurilor de răspuns la incidente: Asigurarea că planurile de răspuns sunt actualizate pentru a reflecta schimbările în infrastructura tehnologică și în strategiile de afaceri.
- Formare și conștientizare continuă: Menținerea nivelului de conștientizare a securității în rândul angajaților prin formare regulată și actualizată.

Rolul managementului riscurilor în strategia de securitate cibernetică a organizațiilor

Managementul riscurilor cibernetice este un proces continuu, care trebuie integrat în cultura organizațională. O strategie eficientă de securitate cibernetică trebuie să includă politici de prevenire, detectare, răspuns și recuperare pentru a face față incidentelor de securitate cibernetică.
Este crucial ca toate organizațiile să înțeleagă și să implementeze practici de securitate cibernetică adecvate pentru a se proteja în fața amenințărilor și vulnerabilităților de securitate cibernetică.

Cubul securității cibernetice

Cubul securității cibernetice, cunoscut și sub denumirea de "Cubul McCumber", este un model conceptual care ilustrează diferite aspecte ale securității informației. A fost dezvoltat de John McCumber în anii '90 ca o metodă pentru a ajuta la înțelegerea și aplicarea securității informației într-un mod holistic. Modelul încorporează trei dimensiuni principale ale securității informației: confidențialitate, integritate, și disponibilitate (principiile CIA), și le intersectează cu trei tipuri de măsuri de securitate: tehnice, organizatorice și umane, precum și cu trei stadii ale informației: stocare, procesare și transmisie.

Cubul securității cibernetice oferă o perspectivă completă asupra securității informației, evidențiind faptul că securitatea cibernetică nu este doar o problemă tehnică, ci implică și aspecte organizatorice și de resurse umane.

Prin utilizarea acestui model, organizațiile pot aborda securitatea informației într-un mod structurat, asigurându-se că toate aspectele importante sunt luate în considerare. Acest lucru ajută la identificarea lacunelor în politicile și procedurile de securitate și la stabilirea priorităților pentru acțiuni de diminuare a riscurilor.

Organizațiile pot folosi cubul securității cibernetice pentru a se asigura că îndeplinesc cerințele legale și de reglementare referitoare la securitatea informațiilor, prin verificarea că toate dimensiunile securității sunt acoperite în politicile și procedurile lor.

Managerul de securitate cibernetică. Profil, atribuții și responsabilități

Managerul de securitate cibernetică este un specialist înalt calificat, cu o înțelegere profundă a peisajului de securitate cibernetică și a metodologiilor de protecție a organizației. Acest profil necesită o combinație de competențe tehnice avansate, abilități de comunicare și leadership, precum și o înțelegere solidă a proceselor de business și a legislației în domeniul securității datelor. În general, managerul de securitate cibernetică are studii superioare în domenii precum informatica, inginerie, studii de securitate, securitate cibernetică, completate de certificări profesionale recunoscute în industrie (ex. CISSP, CISM).

În Clasificarea Ocupațiilor din România (COR), codul pentru poziția de Chief Information Security Officer (CISO), cunoscută și sub numele de Manager Securitatea Informațiilor, este 121118.

Printre responsabilitățile cheie ale CISO se numără:

- Dezvoltarea și implementarea strategiilor și politicilor de securitate.
- Evaluarea riscurilor și gestionarea amenințărilor și vulnerabilităților
- Coordonarea răspunsului la incidente
- Educație și conștientizare
- Menținerea conformității
- Conducerea și managementul echipei de securitate

În multe organizații, Chief Information Security Officer (CISO) ocupă o poziție de lider în cadrul echipei de securitate cibernetică și, în mod tradițional, este responsabil pentru managementul securității cibernetice la nivelul întregii organizații. Deși CISO

nu este întotdeauna direct conducătorul Security Operations Center (SOC), el colaborează strâns cu SOC și alte echipe de securitate pentru a asigura alinierea operațiunilor de securitate cibernetică cu strategia generală de securitate a organizației.

Rolul de CISO este unul dintre cele mai dinamice și provocatoare în domeniul securității cibernetice, necesitând o combinație de expertiză tehnică, abilități de leadership și capacitatea de a lua decizii strategice.

Relațiile funcționale ale unui Chief Information Security Officer (CISO) cu ceilalți membri ai conducerii unei organizații sunt esențiale pentru integrarea eficientă a securității cibernetice în strategia generală de business și operațiunile zilnice. Aceste relații ajută la asigurarea că toate departamentele sunt aliniate cu politicile și obiectivele de securitate cibernetică, facilitând o abordare holistică a securității informației.

Relațiile funcționale ale CISO-ului cu alți directori executivi și departamentele cheie ale organizației sunt fundamentale pentru crearea unui mediu organizațional în care securitatea cibernetică este integrată în toate aspectele activității.

Cursul nr. 2

Termeni și concepte cheie în securitatea cibernetică

Conform Checkpoint Software, **securitatea cibernetică** se referă la fiecare aspect al protejării unei organizații, a personalului și a activelor acesteia împotriva amenințărilor cibernetice.

Risc cibernetic: se referă la probabilitatea ca o organizație sau o persoană să fie expusă la pierderi sau daune ca urmare a unei amenințări cibernetice.

Amenințare cibernetică: materializarea riscului cibernetic. O amenințare cibernetică este orice posibil eveniment malițios care ar putea prejudicia sistemele informatice, rețelele, datele sau utilizatorii.

Atac cibernetic: o acțiune ostilă asupra unui sistem informatic, unei rețele, unui dispozitiv sau unui utilizator, cu scopul de a fura, altera, distruge sau compromite activitatea acestora. Atacurile cibernetice nu pot ieși din sfera spațiului cibernetice și nu pot viza decât dispozitive cibernetice. NU este posibil să utilizăm un atac cibernetic împotriva unui dispozitiv analogic (ex. mașină de tocat carne, râșniță de cafea, etc.)

Vulnerabilitate cibernetică: o slăbiciune a unui sistem, a unei rețele sau aplicații, a unui utilizator care poate fi exploatată de un atacator pentru a efectua orice acțiuni ostile sau neautorizate.

Terorism cibernetic: utilizarea în orice fel a spațiului cibernetic, a infrastructurilor, a rețelelor, a terminalelor sau a utilizatorilor acestora pentru a pregăti sau săvârși orice fel de acte de terorism.

Război cibernetic: ansamblul de acțiuni ofensive și defensive care implică utilizarea TIC pentru a ataca, apăra sau spiona sisteme informatice și rețele, în contextul unui conflict militar, politic sau economic mai amplu.

Antivirus: Software conceput pentru a detecta și elimina programe dăunătoare, cum ar fi virușii și troienii.

Firewall: Un sistem care filtrează și controlează traficul de rețea,
permițând sau blocând anumite conexiuni în funcție de reguli de securitate.

Malware: Software rău intenționat creat pentru a dăuna sau exploata orice program sau rețea.

Phishing: Tehnică de înșelăciune în care atacatorul trimite e-mailuri false care par a fi de la o sursă de încredere pentru a obține informații sensibile.

VPN (Virtual Private Network): Tehnologie care permite crearea unei conexiuni securizate peste o rețea nesecurizată, precum internetul.

Criptare: Procesul de convertire a datelor într-un cod pentru a preveni accesul neautorizat.

Autentificare cu doi factori (2FA): Metodă de securitate care necesită două forme separate de verificare a identității.

Spam: E-mailuri nesolicitate, adesea folosite în campanii de marketing sau în tentative de înșelăciune.

Ransomware: Tip de malware care criptează fișierele utilizatorului și cere răscumpărare pentru descifrare.

Botnet: Rețea de calculatoare infectate, controlată de un atacator pentru a efectua sarcini automate, cum ar fi atacurile DDoS.

DDoS (Distributed Denial of Service): Atac în care mai multe sisteme vizează și suprasolicită resursele unei ținte pentru a bloca serviciile sale.

Patch: Actualizare a software-ului destinată remedierii vulnerabilităților sau îmbunătățirii performanței.

Intrusion Detection System (IDS): Sistem care monitorizează și detectează activități suspecte într-o rețea sau pe un sistem.

Intrusion Prevention System (IPS): sistem care monitorizează traficul de rețea și încearcă să identifice și să blocheze activitățile potențial dăunătoare. Spre deosebire de un Intrusion Detection System (IDS), care doar detectează și alertează în legătură cu activitățile suspecte, IPS este capabil să intervină activ, blocând sau prevenind atacul.

Social Engineering: Tehnici de manipulare psihologică pentru a induce oamenii să divulge informații confidențiale.

Cookies: Fișiere mici stocate pe computerul tău de către site-uri web pentru a memora preferințele și datele de sesiune.

White Hat: Termen pentru hackerii etici care efectuează teste de penetrare pentru a îmbunătăți securitatea.

Black Hat: Hackerii care utilizează abilitățile lor pentru scopuri ilegale sau rău intenționate.

(Spear) Phishing: Versiunea țintită a phishing-ului, în care atacatorul se concentrează pe o țintă specifică.

Worm: Tip de malware care se replică și se răspândește singur, fără interacțiunea umană.

Virus: Software rău intenționat atașat unui program legitim, care se propagă infectând alte fișiere sau sisteme.

Zero-Day Vulnerability: O vulnerabilitate necunoscută publicului și neîmbunătățită, exploatabilă de atacatori.

Penetration Testing (PENTEST): Proces de testare a securității unei rețele sau a unui sistem, simulând atacuri cibernetice.

Secure Socket Layer (SSL): Protocol pentru securizarea comunicației dintre browser și server.

Honeypot: Sistem fals menit să atragă atacatorii, pentru a-i analiza și a înțelege metodele lor.

Identity Theft: Furtul informațiilor personale pentru a îmbrățișa identitatea altei persoane, adesea în scopuri financiare.

Cursul nr. 3

Riscuri, amenințări și vulnerabilități de securitate cibernetică

Riscurile, amenințările și vulnerabilitățile în domeniul securității cibernetice sunt adesea interconectate și necesită o abordare de tip 360 pentru corecta identificare, evaluare și atenuare (diminuare) ulterioară. Cunoașterea în detaliu a acestora ne ajută să înțelegem mai bine cum să protejăm organizațiile împotriva potențialelor incidente și/sau atacuri.

Prin înțelegerea adecvată acestor trei concepte, organizațiile pot dezvolta strategii eficiente de securitate care să le protejeze infrastructura IT, datele și resursele

împotriva potențialelor incidente și/sau atacuri cibernetice. Implementarea unor măsuri proactive de securitate, împreună cu o vigilență constantă și adaptarea la noile contexte, printre altele, constituie cheia pentru managementul eficient al securității cibernetice în cadrul organizațiilor.

Riscurile cibernetice se referă la posibilitatea ca o entitate să experimenteze pierderi și/sau daune ca urmare a unui atac cibernetic. Aceste riscuri pot avea diverse origini, inclusiv erori umane, defecțiuni tehnice sau atacuri intenționate. Riscurile sunt există la nivel teoretic și au o anumită probabilitate de materializare în practică. Riscuri „0" nu există decât teoretic.

Exemple de riscuri cibernetice:

- Pierderile financiare: Atacurile cibernetice pot duce la pierderi directe (ex. furtul de fonduri, răscumpărări pentru deblocarea accesului la date) sau indirecte (ex. pierderi operaționale datorate întreruperii activității).
- Pierderi reputaționale: Incidentele de securitate pot afecta grav reputația unei organizații, erodând încrederea clienților și a partenerilor.
- Pierderea/furtul de date: Pierdere, furtul, distrugerea, compromiterea sau ștergerea datelor sensibile poate avea consecințe dintre cele mai grave pentru o organizație.
- Riscuri de conformitate: Nerespectarea cadrului legal și a recomandărilor de bune practici privind securitatea cibernetică poate rezulta în aplicarea unor sancțiuni pentru organizații și personalul acestora.

Amenințările cibernetice sunt acțiuni sau evenimente care pot compromite securitatea datelor, sistemelor, infrastructurilor, aplicațiilor și personalului. Conceptual, amenințarea se referă la situația când un risc este materializat în practică. Exemplele cele mai comune includ malware-ul, atacurile de tip phishing, atacurile DDoS, spionajul cibernetic, ingineria socială sau furtul de identitate.

Exemple de amenințări cibernetice comune:

- Malware: software rău intenționat, precum viruși, troieni, ransomware și spyware, conceput pentru a infecta și a dăuna sistemelor informatice.
- Phishing: Tehnici de inginerie socială care vizează obținerea unor foloase (ex. credențiale de acces) prin înșelăciune.
- Atacuri DDoS: Atacurile care încearcă să supraîncarce resursele unui sistem informatic pentru a-l face inaccesibil utilizatorilor legitimi.

Vulnerabilitățile cibernetice reprezintă slăbiciuni ale sistemelor informatice, aplicațiilor sau chiar ale personalului care pot fi exploatate pentru a cauza daune și/sau pierderi. Acestea pot fi legate de software, hardware, personal sau de practicile de securitate ale organizațiilor.

Exemple de vulnerabilități cibernetice comune:

- Erori de software/hardware: Bug-urile sau defectele în aplicațiile software sau la nivel hardware pot oferi atacatorilor căi de a pătrunde neautorizat în sistemele și rețelele informatice.
- Configurații defectuoase/erori de configurare: setările necorespunzătoare ale sistemelor sau ale aplicațiilor pot genera adesea breșe de securitate.

- Lipsa actualizărilor de securitate: Sistemele neactualizate sunt vulnerabile la atacuri, deoarece nu includ cele mai recente patch-uri/remedii de securitate.
- Comunicații nesecurizate: Protocoalele nesigure de transmitere a datelor pot permite interceptarea sau alterarea informațiilor.

Metode și tehnici pentru identificarea și atenuarea riscurilor

Identificarea riscurilor, amenințărilor și vulnerabilităților de securitate cibernetică se realizează prin:

- **Analiza riscurilor**: evaluarea sistematică a mediului IT&C pentru a identifica potențialele riscuri cibernetice, inclusiv analiza amenințărilor și identificarea vulnerabilităților.
- **Audituri de securitate**: examinarea detaliată a infrastructurii IT&C și a politicilor de securitate pentru a detecta slăbiciunile în materie de securitate cibernetică.
- Testare de penetrare: simularea atacurilor cibernetice asupra sistemelor informatice pentru a identifica vulnerabilitățile exploatabile.
- **Scanarea vulnerabilităților**: utilizarea instrumentelor (cvasi)automate pentru a scana sistemele și aplicațiile în scopul identificării vulnerabilităților cunoscute.

Atenuarea riscurilor
Atenuarea riscurilor, în contextul managementului securității cibernetice, se referă la procesul de implementare a măsurilor, practicilor și strategiilor care au ca scop reducerea probabilității și impactului potențialelor amenințări și vulnerabilități asupra sistemelor informatice și datelor organizațiilor.
Atenuarea riscurilor este o componentă esențială a managementului riscurilor de securitate cibernetică care ajută organizațiile să minimizeze slăbiciunile din sistemele informatice și să se protejeze împotriva incidentelor de securitate cibernetică.

Exemple de metode și tehnici uzuale pentru atenuarea riscurilor:

- **Actualizări și patch-uri de securitate**, prin implementarea regulată a actualizărilor de software și aplicarea patch-urilor de securitate pentru a corecta vulnerabilitățile identificate.
- **Firewall-uri și sisteme de detectare/prevenire a intruziunilor**, prin utilizarea firewall-urilor pentru a bloca traficul nedorit și a sistemelor de detectare și prevenire a intruziunilor pentru a identifica și opri activitățile suspecte.
- **Criptarea datelor** se referă la protejarea confidențialității datelor prin criptare, atât în repaus cât și în tranzit, pentru a preveni accesul neautorizat.
- **Controlul accesului** se referă la gestionarea accesului la resursele informatice prin implementarea unor soluții de autentificare puternice și a politicilor de minimizare a privilegiilor.
- **Educația și conștientizarea**, prin instruirea periodică și temeinică a personalului cu privire la practicile de securitate cibernetică și sensibilizarea lor cu privire la riscurile, amenințările și vulnerabilitățile comune.

Instrumente de securitate cibernetică

Instrumentele de securitate cibernetică sunt esențiale pentru protejarea organizațiilor împotriva riscurilor, amenințărilor și vulnerabilităților cibernetice. Acestea oferă

mijloacele necesare pentru a detecta, preveni și răspunde la incidentele de securitate, asigurând integritatea, confidențialitatea și disponibilitatea datelor și sistemelor informatice. Dintre acestea, cele mai utilizate și relevante sunt:

- **Scannerele de vulnerabilități**: instrumente automate care ajută la identificarea slăbiciunilor în sistemele și aplicațiile software. Acestea scanează rețelele, sistemele și aplicațiile în căutarea vulnerabilităților cunoscute, oferind rapoarte detaliate care includ recomandări pentru remedierea problemelor identificate.
    - Exemple:
        - Nessus: Unul dintre cele mai cunoscute scannere de vulnerabilități ce oferă evaluări cuprinzătoare ale securității pentru a identifica vulnerabilități, probleme de configurare și alte slăbiciuni.
        - OpenVAS: O soluție de tipă open source foarte utilă pentru scanarea vulnerabilităților care oferă un set vast de teste pentru a detecta slăbiciunile din rețele și sisteme.
- **Framework-urile de securitate**: oferă organizațiilor un cadru structurat pentru gestionarea riscurilor de securitate cibernetică, inclusiv standarde, politici și cele mai bune practici. Acestea ajută la organizarea eforturilor de securitate într-un mod coerent și eficient.
    - Exemple:
        - **NIST Cybersecurity Framework**: Dezvoltat de Institutul Național de Standarde și Tehnologie din SUA, acest framework oferă linii directoare pentru gestionarea riscurilor de securitate cibernetică în organizații de toate dimensiunile.
        - **ISO/IEC 27001**: Un standard internațional care specifică cerințele pentru un sistem de management al securității informației (SMSI), ajutând organizațiile să protejeze informațiile în mod confidențial, integru și disponibil.
        - CIS Controls: e un framework conceput pentru a ajuta organizațiile de toate dimensiunile să se apere împotriva celor mai răspândite și semnificative incidente și/sau atacuri cibernetice.
- Aplicații de criptare: instrumentele de criptare sunt esențiale pentru protejarea confidențialității datelor, asigurând că datele și informațiile sensibile sunt inaccesibile pentru persoanele neautorizate. Acestea criptează datele atât în repaus, cât și în tranzit.
    - Exemple:
        - BitLocker: O caracteristică de criptare a discurilor integrată în versiunile Pro și Enterprise ale sistemelor de operare Windows, care protejează datele împotriva furtului sau accesului neautorizat.
        - VeraCrypt: Un instrument open source de criptare a discurilor, succesor al TrueCrypt, care poate cripta întregi partiții sau dispozitive de stocare, oferind securitate robustă pentru date.
- **Soluții de backup și recuperare**: Instrumentele de backup și recuperare sunt vitale pentru asigurarea continuității activității organizațiilor și recuperarea rapidă în urma unui incident de securitate. Aceste soluții automatizează

procesul de backup al datelor și oferă metode eficiente pentru restaurarea datelor și informațiilor pierdute și/sau compromise.
    - Exemple:
        - Veeam: o soluție foarte cunoscută în industrie pentru backup, recuperare și gestionarea datelor în medii virtuale, fizice și cloud, asigurând protecția datelor esențiale.
        - Acronis: Oferă soluții de backup și recuperare post-incident/dezastru pentru mediile cloud, virtuale și fizice, cu capacitatea de a restaura sistemele rapid și eficient.
- **Firewall-urile și sistemele de detectare/prevenire a intruziunilor** sunt esențiale pentru monitorizarea traficului de rețea și blocarea activităților suspecte sau rău intenționate.
    - Firewall-uri sunt dispozitive sau software-uri care filtrează traficul de rețea pentru a împiedica accesul neautorizat la rețele și sisteme informatice.
    - Sistemele de prevenire a intruziunilor (IPS) și sistemele de detectare a intruziunilor (IDS) sunt componente esențiale ale infrastructurii de securitate cibernetică ale unei organizații, având rolul de a monitoriza, detecta și răspunde la activități suspecte sau malițioase din rețelele de calculatoare. În timp ce IDS este concentrat pe detectarea și alertarea privind activitățile potențial dăunătoare, IPS merge un pas mai departe, blocând activitatea identificată ca fiind malițioasă înainte ca aceasta să cauzeze daune. Astfel, IDS și IPS joacă roluri complementare în strategia de securitate cibernetică a unei organizații. În timp ce IDS oferă detectarea și alertarea, IPS adaugă un strat suplimentar de protecție prin prevenirea activă a atacurilor.
        - Exemple de IDS:
            - Snort este un sistem de detectare a intruziunilor open-source, care poate efectua analiza traficului în timp real și packet logging pe rețele IP.
            - Suricata este un alt motor open-source de detectare, prevenire și monitorizare a intruziunilor, care utilizează reguli și semnături pentru a detecta comportamentul suspect în traficul de rețea. Este cunoscut pentru performanța sa înaltă și capacitatea de a analiza traficul criptat.
        - Exemple de IPS:
            - Check Point IPS este conceput pentru a oferi protecție împotriva atacurilor și exploatărilor cunoscute, fără a afecta performanța rețelei.
            - Fortinet FortiGate include funcționalități IPS de top pentru a proteja rețelele împotriva amenințărilor cunoscute și emergente. FortiGate utilizează baza de date FortiGuard Labs pentru a identifica și bloca atacurile în timp real.

Cursul nr. 4

Strategia de securitate cibernetică

Este un document de tip plan care stabilește direcția generală și obiectivele pe termen lung ale unei organizații în materie de securitate cibernetică.
Strategia include evaluarea riscurilor, alocarea resurselor și definirea unui cadru pentru gestionarea și minimizarea potențialelor amenințări cibernetice. De regulă, elementele sale componente includ mai multe secțiuni precum:

- **Viziune și scop**: Definirea clară a obiectivelor de securitate în concordanță cu misiunea și obiectivele organizației.
- **Evaluarea riscurilor**: Identificarea și clasificarea riscurilor în funcție de probabilitatea și impactul lor asupra organizației.
- **Alocarea resurselor**: Stabilirea resurselor necesare pentru implementarea măsurilor de securitate.
- **Controalele și măsurile de securitate**: Enumeră controalele și măsurile de securitate cibernetică care vor fi implementate pentru a proteja organizația împotriva riscurilor identificate.
- **Cadrul de guvernanță**: Definirea structurii organizaționale și a responsabilităților pentru gestionarea securității cibernetice în cadrul organizației.
- **Răspunsul la incidente**: Stabilește procedurile pentru gestionarea și răspunsul la incidentele de securitate cibernetică.
- **Monitorizare și revizuire**: Prevede mijloacele și metodele prin care strategia și eficiența măsurilor de securitate cibernetică vor fi monitorizate și revizuite periodic.

Strategia este un document crucial pentru a ghida acțiunile organizației în domeniul managementului securității cibernetice.
Documentul este de obicei elaborat de experți în securitatea cibernetică sau de un responsabil cu securitatea informației (CISO - Chief Information Security Officer), fie intern, fie printr-un serviciu externalizat, beneficiind de regulă de contribuții de la departamentele IT, juridic, resurse umane și alte departamente relevante ale organizații. Este important ca elaborarea stratefiei să fie un proces colaborativ, pentru ca toate aspectele securității cibernetice a organizației să fie abordate.

Implementarea strategiei este urmărită de CISO sau de o echipă dedicată de securitate cibernetică, care raportează direct conducerii executive. Aceștia sunt responsabili pentru monitorizarea progresului, soluționarea oricăror obstacole și asigurarea că toate departamentele respectă strategia.
Planificarea securității cibernetice pe baza strategiei implică dezvoltarea unui plan de acțiune detaliat care să includă sarcini specifice, termene limită și indicatori de performanță. Planificarea este efectuată de CISO împreună cu echipa de securitate cibernetică și necesită aprobarea conducerii executive.

Ce trebuie să se regăsească obligatoriu în cadrul unei strategii?

- Detalii specifice despre cum vor fi protejate datele, informațiile și alte active ale organizației.
- Proceduri clare pentru răspunsul la incidente.
- Roluri și responsabilități definite pentru securitatea cibernetică în cadrul organizației.

- Calendarul pentru revizuiri periodice și actualizări ale strategiei.

Ce **NU** trebuie să se regăsească obligatoriu în cadrul unei strategii?

- Informații confidențiale sau detalii tehnice specifice care, dacă sunt divulgate, ar putea compromite securitatea organizației.
- Proceduri generice care nu oferă valoare practică sau orientare specifică.
- Promisiuni nerealiste care nu pot fi îndeplinite de organizație având în vedere resursele alocate sau capabilitățile de care dispune.

Politica de securitate cibernetică

Politicile sunt instrumente operative care derivă din strategia de securitate și sunt menite să reglementeze modul în care securitatea informațiilor este gestionată zilnic. Politicile se referă la un set de reguli și proceduri specifice care ghidează comportamentul utilizatorilor, administratorilor și al sistemelor în cadrul organizației. Componentele tipice includ de:

- Standarde și proceduri: Instrucțiuni detaliate pentru implementarea măsurilor de securitate.
- Responsabilități ale angajaților: Detalierea așteptărilor în ceea ce privește comportamentul și responsabilitățile legate de securitate.
- Gestionarea incidentelor: Proceduri de urmat pentru raportarea și răspunsul la incidentele de securitate.
- Controlul accesului: Regulile pentru accesarea anumitor date și resurse.

Etapele dezvoltarea și implementarea strategiilor și politicilor de securitate cibernetică

1. Evaluarea riscurilor la care este expusă organizația

Primul pas în dezvoltarea strategiei este evaluarea riscurilor pentru a identifica potențialele vulnerabilități și amenințări. Aceasta implică analiza activelor critice ale organizației și a potențialelor lor expuneri.

2. Definirea obiectivelor

Odată ce riscurile sunt identificate, obiectivele și politice trebuie stabilite pentru a aborda aceste riscuri. Obiectivele ar trebui să fie SMART (Specifice, Măsurabile, Tangibile, Realiste, și Temporal definite).

3. Crearea cadrelor de guvernanță

Include atât strategia, cât și politicile. Acest cadru ar trebui să descrie structura de guvernanță, rolurile și responsabilitățile, precum și procedurile de monitorizare și revizuire.

4. Formularea politicilor

Pe baza strategiei, se formulează politici de securitate cibernetică care să adreseze aspecte specifice, cum ar fi gestionarea parolelor, utilizarea e-mailurilor, accesul la internet și securitatea fizică.

5. Implementarea
Implementarea strategiei și a politicilor implică distribuirea resurselor, formarea angajaților și punerea în aplicare a măsurilor de securitate specificate în politicile formulate.

6. Monitorizare și revizuire
Strategia și politicile de securitate cibernetică trebuie să fie documente vii, supuse unei monitorizări și revizuiri periodice pentru a asigura că rămân relevante în fața noilor amenințări și tehnologii.

Rolul CISO în elaborarea și implementarea strategiilor și politicilor de securitate cibernetică

Rolul CISO în dezvoltarea și implementarea strategiilor și politicilor de securitate cibernetică este crucial pentru asigurarea securității cibernetice a organizației împotriva amenințărilor cibernetice și pentru protejarea activelor organizației. Prin leadership-ul său, CISO-ul contribuie semnificativ la creșterea rezilienței organizației în fața riscurilor de securitate cibernetică.

Principalele responsabilități ale unui CISO în privința elaborării și implementării strategiilor și politicilor de securitate cibernetică includ:

- **Leadership și viziune strategică:** CISO-ul este cel care stabilește direcția strategică și viziunea pentru securitatea cibernetică în cadrul organizației, asigurându-se că aceasta este aliniată cu obiectivele organizaționale generale.
- **Promovarea culturii de securitate**: Implică promovarea unei culturi organizaționale care prioritizează securitatea, sensibilizând și implicând toate nivelurile organizației în practici de securitate cibernetică.
- **Dezvoltarea strategiei și politicilor**: CISO-ul identifică obiectivele cheie, evaluând riscurile și stabilind prioritățile de securitate. De asemenea, este responsabil pentru crearea și revizuirea politicilor de securitate cibernetică, asigurând că acestea sunt relevante, cuprinzătoare și conform legilor și reglementărilor aplicabile.
- **Gestionarea riscurilor**: CISO conduce procesul de evaluare a riscurilor de securitate cibernetică, identificând vulnerabilitățile și amenințările potențiale, și dezvoltând planuri pentru diminuarea acestora.
- **Supravegherea implementării**: CISO este responsabil pentru monitorizarea implementării strategiei și politicilor de securitate, inclusiv alocarea resurselor și urmărirea realizării obiectivelor de securitate.
- **Asigurarea conformității:** CISO verifică respectarea politicilor și standardelor de securitate în cadrul organizației și de către partenerii externi.
- **Răspuns la incidente:** CISO dezvoltă și menține planuri de răspuns la incidente de securitate cibernetică, asigurând pregătirea organizației pentru a răspunde eficient la incidente de securitate
- **Educație și conștientizare:** CISO inițiază și supraveghează programe de educație și conștientizare în securitatea cibernetică pentru angajați, crescând gradul de conștientizare asupra amenințărilor cibernetice și a celor mai bune practici de prevenire.

- **Comunicare și raportare**: CISO comunică regulat cu conducerea executivă a unei organizații, raportând despre starea securității cibernetice, riscurile identificate și eficiența măsurilor de securitate implementate.

Cursul nr. 5

Cadrul legislativ primar și secundar care reglementează securitatea cibernetică in România este format din mai multe reglementări care se completează reciproc. În contextul acestei discipline, cele mai relevante dintre acestea sunt:

Legea nr. 58/2023 privind securitatea și apărarea cibernetică a României

Legea nr. 58 din 2023 („Legea 58") este un act normativ complex care a consolidat semnificativ cadrul legislativ național în domeniul securității și apărării cibernetice.

Legea 58 definește cadrul juridic și instituțional pentru securitatea și apărarea cibernetică, având ca obiective principale adoptarea și implementarea de politici și măsuri pentru prevenirea și contracararea vulnerabilităților, riscurilor și amenințărilor în spațiul cibernetic.

În esență, legea 58 operează o delimitare conceptuală importantă, în sensul că securitatea cibernetică nu mai este tratată exclusiv ca o dimensiune tehnică sau de conformare administrativă, ci ca o componentă integrată a apărării naționale și a rezilienței statului. Astfel, normativul introduce o distincție fundamentală între „securitate cibernetică", definită ca stare de normalitate rezultată din implementarea unor măsuri de protecție a informațiilor și sistemelor, și „apărare cibernetică", înțeleasă ca ansamblul acțiunilor, inclusiv de natură militară, destinate contracarării amenințărilor cibernetice și diminuării efectelor acestora. Această diferențiere reflectă alinierea la doctrinile NATO și UE și marchează o extindere a rolului statului în spațiul digital.

Legea nr. 58 definește și distinge între spațiul cibernetic național civil și militar. Acest lucru este esențial pentru a delimita clar domeniile de aplicabilitate și responsabilitate în ceea ce privește securitatea și apărarea cibernetică a României.

Legea 58 stabilește cadrul cooperării între instituțiile cu atribuții în domeniile securității și apărării cibernetice, desemnează autoritățile naționale în domeniu, precum și responsabilitățile pe care acestea le au.

Legea 58 instituie o serie de măsuri de securitate și apărare cibernetică la nivel național care vizează crearea și implementarea de politici, proceduri și măsuri de protecție la nivelul rețelelor și sistemelor informatice. Auditurile de securitate cibernetică sunt prevăzute ca mecanisme de evaluare a conformității și eficacității măsurilor de securitate implementate.

Legea 58 recunoaște importanța gestionării eficiente a incidentelor de securitate cibernetică și a crizelor cibernetice, stabilind cadrul pentru identificarea, prevenirea și contracararea acțiunilor ostile în spațiul cibernetic. Echipele de răspuns la incidente

de securitate cibernetică și centrele operaționale de securitate joacă un rol crucial în acest proces.

Sistemul Național de Securitate Cibernetică (SNSC), instituit prin Legea nr. 58/2023, reprezintă cadrul general de cooperare la nivel național pentru asigurarea securității cibernetice. SNSC are rolul de a coordona acțiunile întreprinse de autoritățile naționale și alte entități publice cu responsabilități și capabilități în domeniul securității cibernetice. Scopul SNSC este organizarea și desfășurarea unitară a activităților specifice securității cibernetice pe teritoriul României, precum și asigurarea unei cooperări eficiente între autorități, sectorul privat, mediul academic, asociațiile profesionale și organizațiile neguvernamentale.

SNSC este coordonat de Consiliul Operativ de Securitate Cibernetică (COSC). COSC este un organ consultativ, fără personalitate juridică, în coordonarea Consiliului Suprem de Apărare a Țării (CSAT), format din consilierul prezidențial pentru probleme de securitate națională, consilierul prim-ministrului pe probleme de securitate națională, secretarul CSAT, precum și reprezentanți ai: Ministerului Apărării Naționale, Ministerului Afacerilor Interne, Ministerului Afacerilor Externe, Ministerului Cercetării, Inovării și Digitalizării, SRI, SIE, STS, SPP, ORNISS, ANCOM și ai Directoratului Național de Securitate Cibernetică (DNSC). Conducerea COSC este asigurată de un președinte - consilierul prezidențial pentru probleme de securitate națională și un vicepreședinte - consilierul prim-ministrului pe probleme de securitate națională.

Sistemul Național de Alertă Cibernetică (SNAC) este o componentă crucială introdusă prin Legea nr. 58/2023, destinată prevenirii, descurajării și combaterii acțiunilor sau inacțiunilor ce pot constitui vulnerabilități, riscuri sau amenințări la adresa securității cibernetice a României. SNAC este definit ca un ansamblu de măsuri tehnice și procedurale, având rolul de a furniza un serviciu de notificare publică privind nivelul de alertă cibernetică existent la nivel național, fie că este vorba de o zonă geografică delimitată sau de un anumit domeniu de activitate. Acesta este stabilit în funcție de gradul de risc asociat amenințărilor, incidentelor sau atacurilor cibernetice identificate la un moment dat.

Legea 58 desemnează următoarele autorități competente în materie de securitate și apărare cibernetică:

- Directoratul Național de Securitate Cibernetică (DNSC) este autoritatea națională de securitate pentru spațiul cibernetic național civil (autoritatea națională de securitate cibernetică); DNSC dezvoltă și asigură managementul Platformei naționale pentru raportarea incidentelor de securitate cibernetică, denumită în continuare PNRISC;
- Ministerul Cercetării, Inovării și Digitalizării (MCID), pentru elaborarea și inițierea actelor normative și politicilor publice naționale în domeniul securității cibernetice, al transformării digitale, societății informaționale, comunicațiilor, cercetării, dezvoltării și inovării;
- ANCOM, pentru coordonarea activităților desfășurate în vederea asigurării securității cibernetice a rețelelor și sistemelor informatice proprii și a celor deținute de persoanele fizice și juridice de drept privat și utilizate în vederea furnizării de servicii de comunicații electronice către autoritățile și instituțiile administrației publice centrale și locale;

- MApN este autoritate competentă la nivel național în domeniul apărării cibernetice, având atribuții în domeniul securității cibernetice pentru rețelele și sistemele informatice care susțin capabilitățile militare de apărare;
- MAI, prin Direcția Generală de Protecție Internă (DGPI), este autoritate competentă la nivel național în domeniul securității cibernetice;
- MAE este autoritate competentă, la nivel național, în domeniul diplomației cibernetice, pentru asigurarea componenței diplomatice și de relații internaționale aferente securității cibernetice;
- SRI este autoritate competentă la nivel național în domeniul cyber intelligence, precum și pentru cunoașterea, analizarea, prevenirea și contracararea incidentelor și atacurilor cibernetice care reprezintă amenințări, riscuri și vulnerabilități la adresa securității naționale a României;
- SIE este autoritate competentă pentru cunoașterea, analizarea, prevenirea și contracararea incidentelor și atacurilor cibernetice care reprezintă amenințări, riscuri și vulnerabilități cibernetice la adresa rețelelor și sistemelor informatice din responsabilitate;
- STS este autoritate competentă în domeniul securității cibernetice pentru infrastructurile, rețelele, sistemele, serviciile proprii și spectrul de frecvențe radio proprii, precum și pentru cele reglementate prin legi speciale;
- SPP este autoritate competentă în domeniul securității cibernetice pentru infrastructurile, rețelele, sistemele și serviciile proprii, coordonează măsurile de securitate cibernetică pentru demnitarii cărora le asigură protecție;
- Oficiul Registrului Național pentru Informații Secrete de Stat (ORNISS) coordonează activitățile desfășurate în vederea asigurării securității cibernetice a rețelelor și sistemelor informatice care stochează, procesează sau transmit informații clasificate;
- Poliția Română (Inspectoratul General al Poliției Române – IGPR), prin structurile centrale și teritoriale, Direcția de Investigare a Infracțiunilor de Criminalitate Organizată și Terorism (DIICOT) și Ministerul Public (i.e Parchetele), prin structurile centrale și teritoriale, sunt autorități de aplicare a legii în domeniul criminalității informatice/ cibernetice (prevenție și combatere), fiecare conform competențelor conferite de lege; atenție, aceste instituții nu sunt autorități de securitate cibernetică, ci sunt instituții de aplicare a legii, având un rol deosebit pentru guvernanța spațiului cibernetic național, deoarece gestionează prevenirea și combaterea criminalității în spațiul cibernetic;

Un element central al legii, cu relevanță directă pentru managementul securității IT, este instituirea unui sistem formalizat de gestionare a incidentelor. Directoratul Național de Securitate Cibernetică administrează Platforma Națională pentru Raportarea Incidentelor de Securitate Cibernetică (PNRISC), iar entitățile vizate au obligația de a notifica incidentele în termen de maximum 48 de ore de la constatare, cu completări ulterioare în termen de cinci zile. Această obligație introduce un mecanism de raportare rapidă și standardizată, esențial pentru detectarea timpurie a atacurilor și pentru coordonarea răspunsului la nivel național.

Legea 58 o importanță majoră conceptului de reziliență cibernetică, definit ca capacitatea sistemelor de a rezista și de a reveni la starea de funcționare normală după un incident. În acest sens, sunt prevăzute atât măsuri proactive – precum dezvoltarea de capabilități de detecție, constituirea de echipe de răspuns, instruirea personalului și realizarea de analize de risc –, cât și măsuri reactive, care includ

implementarea planurilor de răspuns, restaurarea funcționalității sistemelor și diseminarea alertelor. Din perspectivă managerială, legea impune o abordare continuă a securității, bazată pe ciclul prevenție–detectare–răspuns–recuperare.

Nu în ultimul rând, legea 58 evidențiază rolul diplomației cibernetice în promovarea intereselor de politică externă și de securitate ale României pe scena internațională, subliniind necesitatea cooperării internaționale și a dialogului bilateral și multilateral în domeniul securității cibernetice

Legea nr.124 din 7 iulie 2025 pentru aprobarea Ordonantei de urgentă a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor si sistemelor informatice din spatiul cibernetic national civil

Reglementarea în vigoare este OUG 155/2024 astfel cum a fost modificată și completată prin Legea 124/2025. Împreună, ele traduc în dreptul intern logica NIS2: nu mai vorbim doar de bune practici tehnice, ci de obligații legale ferme pentru o gamă largă de actori – de la spitale și operatori de energie, până la platforme online și infrastructura digitală.

Legea 124 instituie un cadru juridic modern și extins pentru securitatea cibernetică a spațiului cibernetic național civil, având ca obiectiv principal asigurarea unui nivel comun ridicat de securitate cibernetică, în deplină aliniere cu exigențele Directivei NIS2 și cu evoluțiile recente ale amenințărilor cibernetice.

Din punct de vedere normativ, se operează o delimitare clară între domeniul civil și cel al securității naționale, excluzându-se explicit instituțiile din apărare, ordine publică și securitate națională, precum și sistemele care gestionează informații clasificate, dar menținându-se corelarea cu Legea nr. 58/2023 în situațiile particulare în care aceste entități furnizează servicii de încredere.

Arhitectura normativă este construită pe un set de principii fundamentale – responsabilitate, proporționalitate, cooperare, minimizarea efectelor și prioritatea interesului public – care structurează întregul regim juridic al securității cibernetice.

Prin intervenția legislativă din 2025 se consolidează suplimentar regimul de confidențialitate, stabilindu-se expres că informațiile gestionate de DNSC în procesele de supraveghere și raportare nu constituie informații de interes public, ceea ce întărește protecția intereselor comerciale și de securitate ale entităților vizate.

Un element central al legii îl constituie delimitarea subiecților de drept, prin introducerea clasificării duale: entități esențiale și entități importante.

Entitățile esențiale includ, în mod automat, administrația publică centrală, operatorii critici, furnizorii de infrastructuri digitale fundamentale (precum DNS, TLD sau servicii de încredere), precum și anumite categorii de operatori economici de dimensiune mare sau medie cu rol sistemic.

Entitățile importante includ operatorii relevanți din aceleași sectoare care nu ating pragul de criticitate stabilit pentru categoria esențială. Criteriile de calificare sunt bazate pe impactul potențial asupra siguranței publice, economiei, sănătății sau stabilității sistemice, inclusiv dimensiunea transfrontalieră a riscurilor.

În plan operațional, regimul juridic impune entităților vizate o obligație generală de implementare a unor măsuri tehnice, organizatorice și operaționale adecvate și proporționale cu nivelul de risc, fundamentate pe o abordare integrată a managementului riscurilor. Aceste măsuri trebuie să acopere întreg ciclul de securitate, de la analiză și prevenție, până la detectare, răspuns și recuperare, incluzând politici de securitate, utilizarea criptografiei, securitatea lanțului de aprovizionare, gestionarea vulnerabilităților, controlul accesului, continuitatea activității și instruirea personalului.

Prin legea 124 se introduce, de asemenea, un regim robust de guvernanță internă, în care responsabilitatea este transferată explicit la nivelul organelor de conducere ale entităților. Acestea au obligația de a aproba, supraveghea și asigura implementarea măsurilor de securitate cibernetiucă, fiind direct răspunzătoare pentru nerespectarea acestora. Modificările aduse prin Legea nr. 124/2025 întăresc dimensiunea de responsabilitate managerială, prin clarificarea obligației de formare profesională continuă și a responsabilităților privind desemnarea persoanelor responsabile cu securitatea sistemelor informatice.

Un pilon esențial al cadrului normativ îl reprezintă mecanismul de raportare a incidentelor, care introduce un regim strict, etapizat și cu termene scurte. Entitățile sunt obligate să notifice incidentele semnificative fără întârzieri nejustificate, inclusiv printr-o avertizare timpurie în maximum 24 de ore, urmată de o raportare detaliată în 72 de ore și de un raport final în termen de o lună. În cazul incidentelor cu impact transfrontalier, obligațiile sunt și mai stricte, inclusiv notificarea în termen de 6 ore de la identificarea elementelor relevante.

Pe dimensiunea conformării, legea instituie obligații extinse de audit, autoevaluare și raportare periodică, inclusiv evaluarea anuală a maturității măsurilor de securitate și elaborarea de planuri de remediere asumate la nivel managerial. Totodată, este instituit un registru național al entităților esențiale și importante, gestionat de DNSC, în care operatorii au obligația de a se înregistra și de a furniza informații detaliate privind activitatea, infrastructura și expunerea la risc.

Legea nr. 124/2025 aduce o serie de clarificări și întăriri punctuale ale cadrului inițial, cu impact direct asupra conformării. Printre acestea se remarcă consolidarea obligației producătorilor și furnizorilor de produse și servicii TIC de a notifica vulnerabilitățile către DNSC și de a le remedia într-un termen agreat, ceea ce introduce un mecanism explicit de responsabilizare în lanțul de aprovizionare.

De asemenea, modificările legislative extind cooperarea instituțională, în special în sectorul financiar, prin formalizarea schimbului de informații între DNSC, BNR și ASF, precum și prin consolidarea mecanismelor de cooperare la nivel european, inclusiv cu ENISA și Comisia Europeană.

Regimul sancționator este unul sever și aliniat standardelor europene, introducând sancțiuni diferențiate în funcție de categoria entității și gravitatea încălcării, inclusiv amenzi care pot ajunge până la 10 milioane euro sau 2% din cifra de afaceri globală pentru entitățile esențiale. Modificările din 2025 detaliază noțiunea de încălcare gravă, extind lista contravențiilor și introduc obligații stricte de implementare și raportare a măsurilor corective, cu termene precise și sancțiuni aferente.

În plan sectorial, Legea nr. 124/2025 actualizează anexele privind domeniile critice, extinzând și detaliind în special sectorul sănătății și infrastructura digitală, ceea ce reflectă creșterea relevanței acestor domenii în contextul riscurilor cibernetice contemporane.

În ansamblu, forma consolidată a OUG nr. 155/2024 configurează un regim juridic de tip „compliance-driven", caracterizat printr-o intensificare a obligațiilor operaționale, o responsabilizare directă a managementului și o integrare profundă în mecanismele europene de securitate cibernetică. Pentru managementul securității sistemelor informatice, implicația majoră constă în instituționalizarea unui model de guvernanță a riscurilor cibernetice bazat pe auditabilitate, trasabilitate și reacție rapidă, cu expunere semnificativă la risc juridic în cazul neconformării.

Ordinul DNSC nr. 1/2025 CERINŢE privind procesul de notificare în vederea înregistrării şi metoda de transmitere a informațiilor

La nivelul legislației subsecvente, Ordinul DNSC nr. 1/2025 instituie cadrul operațional necesar implementării obligației de notificare prevăzute de OUG nr. 155/2024. Ordinul are ca obiect de reglementare standardizarea procesului prin care entitățile sunt identificate, evaluate și înregistrate ca entități esențiale sau importante în registrul național gestionat de DNSC.

Un element central al reglementării îl constituie instituirea unor mecanisme digitale dedicate, respectiv instrumentul de evaluare și generare a notificării (Instrument NIS2@RO) și platforma de înrolare și interacțiune (Platforma NIS2@RO). Acestea sunt concepute ca instrumente integrate de conformare, având rolul de a facilita atât autoevaluarea entităților, cât și colectarea și standardizarea datelor la nivel național.

Procesul de notificare este structurat într-o succesiune clară de etape: autoevaluarea entității, generarea formularului de notificare, validarea internă a datelor, transmiterea către DNSC și evaluarea de către autoritate. DNSC are competența de a verifica exhaustiv informațiile furnizate, inclusiv sub aspectul acurateței și relevanței, și poate solicita completări sau documente suplimentare înainte de emiterea deciziei de înregistrare.

Un element esențial al Ordinului 1 îl reprezintă standardizarea conținutului notificării, prin instituirea unui formular structurat în șase secțiuni, care acoperă atât dimensiunea juridico-organizațională a entității, cât și dimensiunea tehnică și operațională. În mod particular, sunt solicitate date privind identificarea entității, dimensiunea economică (inclusiv indicatori financiari și de personal), sectorul și tipul de servicii furnizate, infrastructura IT (inclusiv intervale de IP), prezența în Uniunea Europeană, precum și

desemnarea persoanelor responsabile cu securitatea cibernetică și a punctelor de contact.

Ordinul 1 introduce, de asemenea, o componentă de autoevaluare substanțială, prin care entitatea trebuie să analizeze impactul potențial al perturbării serviciilor sale, caracterul critic al activității și eventualele riscuri sistemice sau transfrontaliere. Această autoevaluare are rolul de a fundamenta calificarea preliminară a entității și de a sprijini DNSC în procesul de încadrare juridică.

În ansamblu, din perspectivă practică, Ordinul 1 reprezintă una dintre cele mai importante piese de legislație ale regimului de conformare NIS2 la nivel național, condiționând aplicarea ulterioară a tuturor obligațiilor de securitate cibernetică de parcurgerea corectă și completă a procesului de notificare și înregistrare.

Ordinul 2/2025 pentru aprobarea Criteriilor şi pragurilor de determinare a gradului de perturbare a unui serviciu şi a Metodologiei privind evaluarea nivelului de risc alentităţilor

Din perspectiva obiectului de reglementare, Ordinul 2 operează o concretizare juridică a mecanismelor de clasificare și diferențiere a obligațiilor de securitate, prin introducerea unor instrumente cuantificabile de evaluare a impactului și riscului de securitate cibernetică. Astfel, se creează legătura funcțională între statutul juridic al entității (esențială sau importantă) și nivelul de complexitate al măsurilor de securitate cibernetică pe care aceasta este obligată să le implementeze.

Un prim element esențial al Ordinului 2 îl constituie instituirea obligației de autoevaluare a gradului de perturbare a serviciilor pentru acele entități care nu sunt automat încadrate ca esențiale sau importante potrivit criteriilor legale primare. În acest context, ordinul definește perturbarea ca incluzând atât întreruperea serviciului, cât și afectarea confidențialității sau funcționării acestuia, ceea ce extinde semnificativ sfera de analiză dincolo de indisponibilitatea tehnică propriu-zisă.

Evaluarea trebuie realizată în raport cu toate serviciile relevante furnizate de entitate, în special cele incluse în sectoarele reglementate de legislația primară, ceea ce impune o abordare exhaustivă și sistemică. În mod corelativ, rezultatele acestei autoevaluări sunt utilizate atât în procesul de notificare (în temeiul Ordinului nr. 1/2025), cât și în determinarea nivelului de măsuri de securitate aplicabile.

Ordinul 2 introduce o regulă clară de calificare juridică suplimentară, în situația în care o entitate este unic furnizor al unui serviciu esențial. În acest caz, calificarea drept entitate esențială sau importantă se realizează automat, în funcție de sectorul în care se încadrează serviciul respectiv, chiar și în absența altor criterii de încadrare, ceea ce reflectă importanța strategică a continuității serviciilor critice.

Componenta centrală a Ordinului 2 este reprezentată de metodologia de evaluare a nivelului de risc, care introduce un model standardizat de evaluare (scoring). Acest model pornește de la valori de bază stabilite la nivel sectorial sau pe tipuri de entități, definite de DNSC, și permite calcularea unui scor general care determină nivelul de risc al entității. În funcție de acest scor, se stabilește nivelul de complexitate al

măsurilor tehnice, operaționale și organizatorice pe care entitatea trebuie să le implementeze.

Metodologia are un caracter flexibil, permițând entităților să ajusteze valorile de impact și probabilitate în funcție de realitățile proprii, însă numai pe baza unei justificări temeinice și cu validarea prealabilă a DNSC. Această prevedere introduce un echilibru între standardizare și adaptabilitate, evitând aplicarea rigidă a unor criterii generale în situații particulare.

În cazul entităților care operează în mai multe sectoare, Ordinul 2 instituie principiul prevalenței riscului maxim, obligând entitatea să aplice nivelul de măsuri corespunzător celui mai ridicat scor obținut. Această regulă reflectă o abordare precaută și orientată spre protejarea infrastructurilor critice, evitând fragmentarea măsurilor de securitate în funcție de activități individuale.

Ordinul 2 introduce și o obligație de reevaluare periodică a riscului, stabilind un termen general de recalculare la fiecare trei ani, precum și obligația de reevaluare ori de câte ori sunt depășite pragurile de impact relevante. Totodată, este permisă recalcularea voluntară în cazul reducerii riscurilor, ceea ce încurajează o abordare dinamică și adaptativă a managementului securității.

În ansamblu, Ordinul 2 configurează un mecanism tehnic esențial pentru implementarea efectivă a regimului NIS2 la nivel național, transformând evaluarea riscurilor dintr-o obligație generală într-un proces standardizat, cuantificabil și auditabil. Din perspectivă juridică și operațională, obiectivul urmărit este de a asigura proporționalitatea măsurilor de securitate cibernetică la nivelul entităților.

Cursul nr. 6

Managementul răspunsului la incidente de securitate cibernetică

Presupune pregătirea și implementarea unui plan structurat care să permită organizației să reacționeze rapid și eficient cu ocazia unor incidente de securitate cibernetică. Sunt două premise de la care trebuie plecat în ceea ce privește managementul incidentelor de securitate cibernetică:

1. Incidentele de securitate cibernetică vor avea loc la un moment dat, ele fiind o chestiune de tip „când?” și nu de tip „dacă?”.
2. Există două tipuri de sisteme informatice: cele care au fost penetrate deja, respectiv cele despre care nu știm că au fost penetrate deja.
3. 20% dintre incidente generează 80% dintre pagubele sau daunele cele mai însemnate asupra unei organizații.
4. Incidentele de securitate cibernetică nu pot fi prevenite 100%.
5. Într-o abordare echilibrată a securității cibernetice, prevenția ar putea fi considerată ca reprezentând între 20% și 40% din eforturile și resursele alocate gestionării incidentelor de securitate, această estimare variind în funcție de specificul fiecărei organizații. Este important de înțeles că investiția în prevenție poate reduce cu până la 80% costurile și impactul asociate cu detectarea, răspunsul și recuperarea după incidente.

Răspunsul la incidente de securitate cibernetică include mai multe faze, precum:

1. **Pregătirea**: Înțelegerea amenințărilor, evaluarea vulnerabilităților și formarea personalului.
2. **Identificarea incidentelor**: Utilizarea unor sisteme de monitorizare și detectare pentru a identifica activitățile suspecte sau malițioase.
3. **Analiza și evaluarea**: Determinarea gravității incidentului și a impactului potențial asupra organizației.
4. **Răspunsul**: Implementarea acțiunilor necesare pentru a limita daunele, izola sistemele afectate și eradicara amenințările.
5. **Recuperarea**: Restaurarea serviciilor și a sistemelor afectate la starea normală de operare.
6. **Management post-incident**: Revizuirea incidentului pentru a îmbunătăți procedurile și planurile de răspuns.

Echipa de răspuns la incidente de cecuritate cibernetică (CSIRT/CERT)

Crearea unei echipe de răspuns la incidente de securitate cibernetică (Computer Security Incident Response Team - CSIRT sau Computer Emergency Response Team - CERT) este vitală pentru gestionarea eficientă a incidentelor. Echipa CSIRT/CERT este responsabilă pentru coordonarea răspunsului la incidente și poate include membri din diferite departamente, cum ar fi IT, securitate cibernetică, juridic și comunicații.

Rolurile și atribuțiile membrilor CSIRT/CERT:

Membrii CSIRT/CERT au roluri și responsabilități specifice, pe mai multe niveluri, însemnând:

- Managerul CSIRT/CERT: Coordonează echipa și acțiunile de răspuns la incidente.
- Analiștii de securitate: Evaluează incidentele, determină impactul și recomandă acțiuni de remediere.
- Specialiștii/inginerii IT: Asigură suport tehnic pentru izolarea și eradicarea amenințărilor, precum și pentru recuperarea sistemelor afectate.
- Threat-hunteri: examinează datele și logurile de sistem pentru a identifica activități neobișnuite sau anomalii care ar putea indica prezența unui atacator în rețea. De asemenea, acești specialiști dezvoltă ipoteze specifice pe care le testează în rețele și sisteme, identificând astfel vulnerabilități neexploatate sau atacuri în curs de desfășurare.
- Specialiști din zona de servicii suport: Asigură gestionarea incidentului din perspectiva juridică, etică, reputațională, colaborativă sau în privința comunicării publice.

Recuperarea în caz de dezastre, monitorizare și asigurarea continuității

Recuperarea în caz de dezastre

Se concentrează pe restabilirea rapidă a sistemelor și a datelor afectate după un incident major de securitate cibernetică sau alte dezastre (naturale sau provocate de om).

Planul de recuperare în caz de dezastre și strategia de continuitate a afacerii sunt esențiale pentru minimizarea întreruperilor operaționale și pentru restaurarea rapidă a serviciilor ca urmare a unui incident asupra unei organizații. De regulă, planul prevede:

- **Opțiuni de backup și recuperare**: ca urmare a implementării soluțiilor de backup regulat, respectiv a procedurilor de recuperare a datelor.
- **Planuri de continuitate a afacerii** care să permită continuarea operațiunilor critice în cazul unui incident major.
- **Utilizarea instrumentelor de monitorizare** pentru a detecta rapid incidentele și pentru a evalua eficacitatea măsurilor de securitate.

De reținut: Organizarea eficientă a răspunsului la incidente de securitate cibernetică necesită o planificare atentă, resurse dedicate și o colaborare strânsă între toate departamentele implicate. Prin înființarea unei echipe CSIRT/CERT bine pregătite și prin implementarea unor planuri solide de recuperare în caz de dezastre și continuitate a afacerii, organizațiile pot asigura o poziție mai puternică în fața amenințărilor cibernetice.

Monitorizarea securității
Monitorizarea continuă a securității este vitală pentru detectarea timpurie a incidentelor de securitate și a activităților suspecte în cadrul organizației. Componentele cheie includ:

- **Sisteme de detectare și prevenire a intruziunilor (IDS/IPS)**
- **Analiza comportamentală** (behavioral analytics) prin aplicarea tehnologiilor care analizează comportamentul utilizatorilor și al sistemelor pentru a identifica activități anormale care ar putea indica o breșă de securitate.
- **Răspuns automatizat** la anumite tipuri de incidente de securitate, limitând astfel impactul acestora.

Asigurarea continuității
Se concentrează pe menținerea funcțiilor critice ale organizației în timpul și după un incident major, asigurându-se că ea poate continua să opereze. Planul de continuitate a afacerii include:

- **Analiza impactului asupra afacerii (BIA)**: Este esențială în planificarea continuității organizației și a recuperării în caz de dezastre, servind drept fundament pentru înțelegerea modului în care diferite scenarii de dezastre ar putea afecta organizația. Informațiile obținute prin BIA sprijină luarea deciziilor în ceea ce privește investițiile în măsuri de prevenire, în tehnologii de backup și recuperare, și în alte resurse necesare pentru asigurarea continuității afacerii.
- **Strategii de continuitate**: Identificarea și implementarea soluțiilor alternative este vitală pentru menținerea operațiunilor critice în caz de incident major (ex. locații alternative de operare, soluții de telecomunicații de rezervă).
- **Modele de exerciții și testări**: Desfășurarea periodică a exercițiilor de simulare este necesară pentru a testa eficacitatea planurilor de continuitate a afacerii și de recuperare în caz de dezastre.

Instrumente de răspuns la incidente de securitate cibernetică

Instrumentele de răspuns la incidente de securitate cibernetică sunt esențiale pentru detectarea, analiza și remedierea rapidă și eficientă a incidentelor de securitate. Aceste instrumente pot varia considerabil în funcție de complexitate, scop și metoda de implementare.

Clasificarea instrumentelor de răspuns la incidente de securitate cibernetică poate fi structurată în mai multe categorii, fiecare având rolul său specific.

1. Sisteme de Detectare și Prevenire a Intruziunilor (IDS/IPS)

- Exemple:
  - **Snort**: un IDS open-source foarte popular, care poate detecta și preveni intruziunile pe baza unui set de reguli definit de utilizator.
  - **Cisco Firepower IDS/IPS**: O soluție comercială care oferă atât funcționalități IDS, cât și IPS, integrându-se cu alte produse CISCO pentru o securitate îmbunătățită.

2. Sisteme de gestionare a informațiilor de securitate (security information and event management SIEM)

SIEM colectează și agregă logurile legate de evenimente din multiple surse din întreaga infrastructură IT&C a organizației, inclusiv servere, dispozitive de rețea, sisteme de securitate, aplicații și alte surse de date, iar prin analiza datelor colectate, SIEM pot identifica modele sau activități suspecte care pot indica o potențială breșă de securitate sau un atac în curs. Aceste sisteme folosesc reguli, algoritmi și inteligență artificială pentru a detecta anomalii.
Odată identificate activitățile suspecte, SIEM-urile generează alerte în timp real, permițând echipei de securitate să investigheze și să răspundă rapid la incidente.

SIEM pot corela evenimente aparent disparate pentru a identifica atacuri complexe sau amenințări care altfel ar putea fi trecute cu vederea. Aceste sisteme facilitează conformitatea cu standardele și reglementările din industrie prin generarea de rapoarte automate și detaliate privind evenimentele de securitate și măsurile luate.

- Exemple:
  - **Splunk Enterprise Security**: Oferă analiză de securitate avansată, monitorizare și alerte bazate pe o varietate largă de surse de date.
  - **IBM QRadar**: O platformă SIEM care utilizează analize sofisticate pentru a detecta amenințările ascunse și pentru a automatiza răspunsurile la incidente.

3. Instrumente de analiză forensic

Software-urile de analiză forensic sunt utilizate pentru investigații detaliate după ce un incident de securitate a avut loc. Acestea permit specialiștilor în securitate cibernetică să examineze în profunzime datele digitale pentru a determina cauza și amploarea incidentului. Prin examinarea detaliată a semnăturilor digitale și a altor indicii lăsate de atacatori, software-urile de analiză forensic pot contribui la identificarea surselor atacurilor.

De reținut: Informațiile obținute din analiza forensic sunt esențiale pentru a înțelege cum a fost posibil un atac și pentru a îmbunătăți măsurile de securitate în scopul prevenirii incidentelor similare în viitor.

- Exemple:
    - EnCase Forensic: Permite examinarea detaliată a hardisk-urilor și a datelor digitale pentru investigații și analize forensic.
    - Autopsy: Un instrument open-source de analiză forensic digitală, care oferă funcționalități pentru analiza sistemelor de fișiere și recuperarea datelor.

4. Platforme de Threat Intelligence

Platformele de Threat Intelligence joacă un rol crucial în cadrul securității cibernetice prin furnizarea de date și informații valoroase despre amenințările existente și emergente. Aceste platforme colectează, agregă și analizează date și informații din diverse surse pentru a oferi o înțelegere detaliată a amenințărilor, permițând organizațiilor să ia decizii informate și proactive în ceea ce privește securitatea cibernetică. De asemenea, Platformele de Threat Intelligence furnizează informații actualizate despre tactici, tehnici și proceduri (TTP-uri) specifice atacatorilor, precum și despre indicatorii de compromitere (IoC-uri), ajutând organizațiile să detecteze și să prevină atacurile într-un stadiu incipient.
Prin oferirea de informații despre gravitatea și impactul potențial al diferitelor tipuri de amenințări, platformele permit echipelor de securitate să prioritizeze răspunsul la incidente, concentrându-se pe cele mai critice probleme.
Cele mai multe platforme de Threat Intelligence permit partajarea de informații despre amenințări între organizații și industrii, îmbunătățind astfel capacitatea colectivă de a răspunde la amenințările cibernetice.

- Exemple:
    - **FireEye Threat Intelligence**: Oferă informații detaliate despre amenințările emergente și avansate, ajutând organizațiile să înțeleagă și să combată tactici sofisticate de atac.
    - **Recorded Future**: Utilizează inteligența artificială pentru a analiza datele de pe internet și pentru a oferi alerte timpurii despre amenințările emergente.
    - **CrowdStrike Falcon X**: O platformă de Threat Intelligence care automatizează colectarea și analiza informațiilor despre amenințări, oferind acces la date despre atacuri, adversari și campanii malițioase.

5. Software-uri de gestionare a actualizărilor
Software-urile de gestionare a actualizărilor, cunoscute și ca sisteme de patch management, automatizează procesul de identificare, descărcare și aplicare a actualizărilor de software (patch-uri) pentru sistemele de operare, aplicații și alte componente software.

Patch-urile de securitate sunt emise pentru a remedia vulnerabilitățile descoperite în software. Fără aplicarea promptă a acestor patch-uri, organizațiile rămân expuse la atacuri cibernetice care pot exploata aceste vulnerabilități. Software-urile de

gestionare a actualizărilor automatizează procesul de aplicare a acestor patch-uri critice, reducând fereastra de oportunitate pentru atacatori.

Multe reglementări și standarde de industrie, cum ar fi GDPR, impun organizațiilor să mențină sistemele actualizate și protejate împotriva vulnerabilităților cunoscute. Software-urile de gestionare a actualizărilor ajută la îndeplinirea acestor cerințe de conformitate prin asigurarea aplicării sistematice a patch-urilor de securitate.

De reținut: Procesul manual de aplicare a patch-urilor este consumator de timp și resurse. Software-urile de gestionare a actualizărilor automatizează acest proces, permițând echipei IT să aloce timpul și resursele economisite către alte inițiative de securitate sau proiecte IT strategice.

- Exemple:
    - **ManageEngine Patch Manager Plus**: O soluție completă de gestionare a patch-urilor pentru Windows, macOS și Linux, care ajută la automatizarea procesului de patching.
    - **SolarWinds Patch Manager**: Simplifică procesul de aplicare a patch-urilor pentru software-ul Microsoft și al treilea, reducând riscul de vulnerabilități neexploatate.
    - **WSUS (Windows Server Update Services)**: Permite administratorilor de rețea să distribuie actualizările emise de Microsoft către computerele dintr-o rețea corporativă.

6. Instrumente de backup și recuperare

Software-urile de backup și recuperare sunt esențiale pentru orice organizație, oferind o linie de apărare crucială împotriva pierderii datelor cauzate de incidente de securitate cibernetică, erori umane, dezastre naturale sau defecțiuni hardware. Aceste instrumente permit organizațiilor să copieze și să stocheze în siguranță datele în locații secundare, astfel încât acestea să poată fi recuperate rapid și eficient în cazul în care datele originale sunt pierdute sau compromise.

Backup-ul regulat al datelor asigură că informațiile critice ale organizației, cum ar fi bazele de date ale clienților, documentele financiare și proprietatea intelectuală, sunt protejate împotriva pierderilor accidentale sau intenționate. Aceasta este o componentă cheie a strategiei de continuitate a afacerii.

De reținut: În cazul unui incident major, cum ar fi un atac ransomware care criptează sau șterge datele critice, software-urile de backup și recuperare permit organizațiilor să restaureze rapid datele afectate, minimizând întreruperea activităților operaționale și asigurând continuitatea serviciilor oferite clienților.

Facilitățile de backup și recuperare oferă funcționalități avansate precum de-duplicarea datelor, compresia și criptarea, care pot îmbunătăți eficiența proceselor de backup, reducând necesarul de spațiu de stocare și asigurând securitatea datelor.

- Exemple:

- **Veeam Backup & Replication**: O soluție robustă pentru backup și recuperare, care oferă protecție pentru datele din centrele de date virtuale, fizice și cloud.
- **Acronis Cyber Backup**: Oferă backup fiabil și opțiuni de recuperare rapidă pentru a minimiza întreruperile operaționale în caz de dezastre.

Cursul nr. 7

Planificarea securității cibernetice implică dezvoltarea unui set structurat de acțiuni și politici menite să protejeze activele digitale și infrastructura IT&C a unei organizații împotriva amenințărilor și vulnerabilităților cibernetice. Aceasta este parte integrantă a strategiei de securitate cibernetică a organizației, servind ca un plan de acțiune pentru implementarea efectivă a strategiei.

Prin planificarea securității cibernetice, organizațiile își propun să identifice riscurile, să stabilească prioritățile de protecție, să aloce resurse și să dezvolte proceduri de răspuns la incidente.

Planificarea securității cibernetice este necesară pentru identificarea și protejarea activelor valoroase prin evaluarea riscurilor și stabilirea priorităților de securitate. Acest lucru conduce la o mai bună protecție a datelor și a infrastructurii IT&C, reducând șansele ca incidentele de securitate să aibă loc, respectiv impactul acestora.

Planificarea eficientă a securității cibernetice oferă o serie de beneficii semnificative pentru organizații, precum:

- **Protecția datelor sensibile**: Previne pierderea sau furtul de date critice, asigurând confidențialitatea, integritatea și disponibilitatea datelor și informațiilor.
- **Reducerea riscurilor de securitate** și, prin urmare, reducerea probabilității și/sau frecvenței incidentelor de securitate.
- **Conformitate sporită:** Ajută la îndeplinirea cerințelor legale și de conformitate, evitând amenzi și alte penalități.
- **Optimizarea costurilor**: Diminuează costurile asociate cu brețele de securitate, prin prevenirea și gestionarea eficientă a incidentelor.
- **Îmbunătățirea reputației și încrederii:** Consolidează reputația organizației și crește încrederea clienților și a partenerilor în practicile de securitate ale organizației.

Planificarea securității cibernetice implică mai mulți pași și este de obicei coordonată de către CISO, împreună cu echipa de securitate IT&C și alte departamente, cum ar fi resurse umane, legal și operațiuni.

Planificarea efectivă constă în elaborarea unor strategii și proceduri detaliate pentru a proteja organizația împotriva amenințărilor cibernetice și pentru a gestiona orice breșe de securitate care pot apărea.

De regulă, domeniile de acțiune ale planificării securității cibernetice vizează cel mai adesea:

- Asigurarea confidențialității şi protecției datelor

- Securitatea rețelelor
- Securitatea aplicațiilor
- Securitatea dispozitivelor mobile
- Securitatea cibernetică a personalului
- Securitatea facilităților
- Securitatea operațională
- Reacția la incidente și recuperarea după dezastre
- Managementul identității și accesului
- Educația și formarea
- Securitatea cloud
- Securitatea dispozitivelor IoT
- Securitatea fizică a infrastructurii

Asigurarea confidențialității și protecției datelor

Obiectiv: Protejarea datelor sensibile împotriva accesului neautorizat, dezvăluirii, modificării sau distrugerii.

Elementele de acţiune ale planului:

- **Clasificarea datelor**: Implementarea unui sistem de clasificare a datelor pentru a identifica și proteja datele sensibile.
- **Controlul accesului**: Implementarea de controale de acces granulare pentru a restricționa accesul la datele sensibile.
- **Criptarea**: Utilizarea soluțiilor de criptare pentru a proteja datele în stare de repaus și în tranzit.
- **Pseudonimizarea**: Utilizarea tehnicilor de pseudonimizare pentru a reduce riscul de identificare a persoanelor vizate.
- **Monitorizarea și auditul**: Monitorizarea și auditarea accesului la datele organizației pentru a detecta și preveni accesul neautorizat.
- **Plan de răspuns**: Implementarea unui plan de răspuns la incidente pentru a gestiona incidentele de confidențialitate a datelor.

Securitatea rețelelor

Obiectiv: Protejarea rețelelor și a infrastructurii IT împotriva atacurilor cibernetice.

Elemente de acțiune ale planului:

- **Segmentarea rețelei:** Segmentarea rețelei pentru a limita impactul atacurilor cibernetice.
- **Arhitectura de securitate zero-trust:** Implementarea unei arhitecturi de securitate zero-trust pentru a verifica în mod constant identitatea și autorizarea utilizatorilor și dispozitivelor.
- **Sisteme de prevenție a intruziunilor (IPS):** Implementarea de soluții IPS pentru a bloca traficul malițios.
- **Sisteme de detectare a intruziunilor (IDS):** Implementarea de soluții IDS pentru a identifica activitățile suspecte din rețea.

- **Analiza traficului de rețea:** Utilizarea soluțiilor de analiză a traficului de rețea pentru a identifica anomalii și a detecta amenințări cibernetice.
- **Testarea de penetrare:** Efectuarea periodică de teste de penetrare pentru a identifica vulnerabilitățile din rețea.

Securitatea aplicațiilor

Obiectiv: Protejarea aplicațiilor împotriva vulnerabilităților și atacurilor cibernetice.

Elemente de acțiune ale planului:

- **Security software development lifecycle (SDLC):** Implementarea de practici de securitate în toate etapele SDLC.
- **Analiza statică a codului:** Utilizarea de instrumente de analiză statică a codului pentru a identifica vulnerabilități în codul sursă.
- **Analiza dinamică a codului:** Utilizarea de instrumente de analiză dinamică a codului pentru a identifica vulnerabilități în codul executabil.
- **Testarea de penetrare a aplicațiilor:** Efectuarea de teste de penetrare a aplicațiilor pentru a identifica vulnerabilități exploatabile.
- **Managementul vulnerabilităților:** Implementarea unui proces de management al vulnerabilităților pentru a remedia rapid vulnerabilitățile identificate.

Securitatea dispozitivelor mobile

Obiectiv: Protejarea dispozitivelor mobile împotriva vulnerabilităților și atacurilor cibernetice.

Elemente de acțiune ale planului:

- **Managementul dispozitivelor mobile (MDM):** Implementarea unei soluții MDM pentru a gestiona și securiza dispozitivele mobile.
- **Containerizare:** Utilizarea soluțiilor de containerizare pentru a separa datele personale de datele de afaceri.
- **Criptarea:** Criptarea datelor stocate pe dispozitivele mobile.
- **Politici de BYOD:** Implementarea de politici BYOD (bring your own device) pentru a reglementa utilizarea dispozitivelor personale în scopuri profesionale.
- **Autentificare multi-factor (MFA):** Utilizarea MFA pentru a spori securitatea autentificării pe dispozitivele mobile.

Securitatea cibernetică a personalului

Obiectiv: Protejarea personalului împotriva vulnerabilităților și atacurilor cibernetice.

Elemente de acțiune ale planului:

- **Programe de educare și formare:** Implementarea de programe de educare și formare pentru a crește gradul de conștientizare a personalului cu privire la riscurile cibernetice.
- **Simulări de phishing:** Realizarea de simulări de phishing pentru a testa capacitatea personalului de a identifica și evita atacurile de phishing.
- **Campanii de conștientizare:** Implementarea de campanii de conștientizare pentru a informa personalul despre practicile de securitate cibernetică.
- **Training de securitate cibernetică:** Oferirea de traininguri specializate de securitate cibernetică pentru personalul cu roluri sensibile.

Securitatea facilităților

Obiectivul principal al securității facilităților este de a proteja infrastructura fizică a unei organizații împotriva accesului neautorizat, daunelor și furtului.

Elemente de acțiune ale planului:

- **Controlul accesului fizic:** Implementarea de controale de acces fizic stricte pentru a restricționa accesul la spațiile sensibile.
- **Supraveghere video:** Utilizarea de sisteme de supraveghere video pentru a monitoriza spațiile sensibile.
- **Securitate perimetrală:** Implementarea de măsuri de securitate perimetrală pentru a proteja infrastructura fizică.
- **Controlul mediului:** Monitorizarea și controlul mediului (temperatură, umiditate) pentru a proteja echipamentele sensibile.
- **Planificare de contingență:** Implementarea unui plan de contingență pentru a gestiona incidentele de securitate fizică.

Securitatea operațională

Obiectivul principal al securității cibernetice la nivel operațional este de a proteja sistemele IT&C și infrastructura critică ale unei organizații împotriva atacurilor cibernetice și a incidentelor de securitate.

Elemente de acțiune ale planului:

- **Managementul patch-urilor:** Implementarea unui proces de management al patch-urilor pentru a remedia rapid vulnerabilitățile cunoscute.
- **Backup și recuperare:** Implementarea de soluții de backup și recuperare pentru a asigura disponibilitatea datelor și a sistemelor.
- **Monitorizare și audit:** Monitorizarea și auditarea sistemelor IT pentru a identifica și preveni incidentele de securitate.
- **Managementul configurațiilor:** Implementarea unui sistem de management al configurației pentru a menține o configurație sigură a sistemelor IT.
- **Planificare de contingență:** Implementarea unui plan de contingență pentru a gestiona incidentele de securitate operațională.

Reacția la incidente și recuperarea după dezastre

Obiectivul principal al răspunsului la incidente și al recuperării post-criză este de a minimiza impactul unei amenințări sau vulnerabilități de securitate cibernetică și de a reface operațiunile organizației cât mai aproape de normal și cât mai rapid posibil.

Elemente de acțiune ale planului:

- **Plan de răspuns la incidente:** Implementarea unui plan de răspuns (IR) care definește rolurile, responsabilitățile și acțiunile specifice pentru a gestiona incidentele de securitate.
- **Plan de recuperare în caz de dezastre (DR):** Implementarea unui plan DR care definește etapele de recuperare a sistemelor IT&C și a datelor în urma unui dezastru.
- **Îmbunătățirea capacității de a detecta incidentele:** Implementarea de soluții de monitorizare și detectare a amenințărilor pentru a identifica rapid incidentele de securitate cibernetică.
- **Investigații digitale:** Efectuarea de investigații digitale pentru a identifica cauza și amploarea incidentelor de securitate, respectiv utilizarea de tehnici de analiză forensic pentru a colecta și analiza dovezi digitale.
- **Reducerea timpului de recuperare:** Implementarea de soluții de backup și recuperare a datelor pentru a reduce timpul necesar pentru a reface operațiunile organizației după un incident.
- **Comunicare în caz de criză:** Implementarea unui plan de comunicare în caz de criză pentru a informa părțile interesate despre incidentele de securitate.

Managementul identității și accesului

Obiectivul principal al managementului identității și accesului (IAM) este de a controla accesul utilizatorilor la resursele IT ale unei organizații.

Elemente de acțiune ale planului:

- **Autentificare puternică:** Implementarea de metode de autentificare puternică,cum ar fi autentificarea multi-factor (MFA) și autentificarea biometrică.
- **Autorizare bazată pe roluri (RBAC):** Implementarea de roluri și permisiuni specifice pentru a controla accesul la resursele IT.
- **Gestionarea privilegiilor:** Implementarea de controale stricte pentru a gestiona accesul privilegiat la sistemele IT.
- **Acces just-in-time (JIT):** Acordarea accesului la resursele IT&C doar atunci când este necesar și pentru o perioadă limitată de timp.
- **Monitorizare și audit:** Monitorizarea și auditarea accesului la resursele IT pentru a identifica și preveni accesul neautorizat.

Educația și formarea

Obiectivul principal al educației și formării în domeniul securității cibernetice este creșterea gradului de conștientizare a personalului cu privire la riscurile cibernetice și promovarea bunelor practici de securitate cibernetică.

Elemente de acțiune ale planului:

- **Programe de educare și conștientizare:** Implementarea de programe de educare și conștientizare pentru a informa personalul despre riscurile cibernetice și practicile de securitate cibernetică.
- **Training specializat:** Oferirea de traininguri specializate de securitate cibernetică pentru personalul cu roluri sensibile.
- **Simulări și exerciții:** Realizarea de simulări și exerciții de securitate cibernetică pentru a testa capacitatea personalului de a răspunde la incidente.
- **Dezvoltarea culturii de securitate:** Promovarea unei culturi a securității în cadrul organizației.

Cursul nr. 8

Organizarea răspunsului la incidente de securitate cibernetică înseamnă proiectarea, implementarea și gestionarea unor procese și mijloace structurate pentru prevenirea, detectarea, evaluarea și combaterea incidentelor de securitate cibernetică într-o manieră sistematică.

Răspunsul la incidente de securitate cibernetică implică prevenirea și combaterea acestora, iar în cazul în care acestea au produs pagube sau daune, inclusiv asigurarea continuității la nivel operațional.
Răspunsul la incidente implică o conlucrare între factorul uman (ex. personal, echipa specializate, etc) și echipamentele de securitate cibernetică care operează de regulă automatizat sau semi-automatizat pentru derularea proceselor de răspuns.

Atenție: răspunsul la incidente de securitate cibernetică NU înseamnă doar activități reactive, de combatere a incidentelor!
Un incident de securitate cibernetică înseamnă orice eveniment care are loc la nivelul unor sisteme, terminale, infrastructuri sau echipamente cibernetice care are potențialul de a compromite confidențialitatea, integritatea, disponibilitatea sau autenticitatea datelor și informațiilor stocate, procesate sau transmise. Un incident de securitate cibernetică poate avea loc accidental (ex. eroare umană, defecțiune tehnică, etc.) sau intenționat (ex. atac cibernetic).

Organizarea răspunsului la incidente presupune mai multe etape și pași de urmat de către o organizație, ce poate fi descris generic după cum urmează:

Etapa întâi. Planificarea

Stabilirea unui plan de răspuns care definește procedurile, rolurile și responsabilitățile în cadrul organizației. Această etapă include de regulă pregătirea echipelor de răspuns la incidente și implementarea unor măsuri tehnice pentru monitorizarea, evaluarea și detectarea incidentelor.

Etapa a II-a. Detecția, analiza și raportarea

Presupune implementarea unor sisteme de detectare a activităților suspecte sau neautorizate pe baza unor semnalări, notificări, comportamente suspecte sau indicatori de compromitere. În această etapă se colectează 24/7/365 și se analizează

date (manual, semi-automatizat sau automatizat) pentru a se identifica potențialele incidente de securitate, respectiv pentru a le raporta conform procedurilor stabilite.

Etapa a III-a. Evaluarea și clasificarea incidentelor

Odată ce un incident a fost detectat, trebuie evaluate gravitatea, impactul și natura atacului, respectiv trebuie clasificat corespunzător incidentul pentru a se determina răspunsul adecvat.

Etapa a IV-a. Izolarea și eradicarea

În această fază, echipa de răspuns la incidente ia măsurile necesare pentru a limita impactul incidentului și pentru a înlătura sursa amenințării. Acest lucru poate include izolarea sistemelor afectate și eliminarea malware-ului sau a altor elemente suspecte și/sau periculoase.

Etapa a V-a. Recuperarea și asigurarea continuității

După ce incidentul a fost izolat și eradicat, procesul de recuperare presupune restabilirea operațiunilor la starea existentă înaintea incidentului și asigurarea că toate sistemele sunt securizate și funcționale.

Etapa a VI-a. Implementarea lecțiilor învățate

După rezolvarea incidentului, se recomandă cu tărie realizarea unei analiză post-incident pentru a se înțelege, respectiv evalua cauzele și consecințele incidentului, precum și eficiența răspunsului. Această etapă include identificarea lecțiilor învățate în urma incidentului și implementarea măsurilor necesare de pe urma acestora pentru a preveni incidente similare în viitor.

Etapa a VII-a. Comunicare, cooperare și colaborare

În funcție de natura și gravitatea incidentului, poate fi necesară notificarea și colaborarea cu terțe părți, precum partenerii organizaționali, autoritățile, clienții sau alte părți interesate.

Etapa a VIII-a. Actualizarea planului de răspuns

Revizuirea și actualizarea regulată a planului de răspuns la incidente este necesară pentru a reflecta schimbările ce au loc la nivelul sistemelor, terminalelor, infrastructurii sau personalului organizației, precum și schimbările sau evoluțiile de natură tehnologică ori din peisajul amenințărilor. Această etapă poate avea loc concomitent cu etapa a VI-a și/sau etapa a VII-a.

De reținut: răspunsul la incidente de securitate cibernetică este un proces continuu, ciclic, neîntrerupt, ce are loc „în buclă”.
În funcție de nevoile și resursele de care dispune o organizație, există mai multe modele organizaționale prin intermediul cărora se poate organiza răspunsul la incidentele de securitate cibernetică: modelul „in-house”, modelul MSSP/MSP, modelul mixt.

Modele de organizare a răspunsului la incidente

În general, alegerea unui model organizațional se face în funcție de dimensiunea organizației, de tipul organizației, de procesele și/sau serviciile gestionate, de amenințările probabile și posibile, respectiv de resursele de care dispune și pe care le poate aloca pentru răspunsul la incidente de securitate cibernetică.

De reținut: Obiectul rezonabil al organizării unui răspuns adecvat NU înseamnă 0 incidente de securitate cibernetică, ci înseamnă, în cazul ideal, 0 incidente care produc pagube, daune sau perturbări ale activității.

Nu există un model ideal, toate modele au avantaje și dezavantaje, iar alegerea modelului optim pentru o organizație pleacă de la o analiză riguroasă de tip cost-beneficiu. Modelul ales trebuie să se plieze în primul rând pe 2 factori determinanți: (1) pe nevoile reale de securitate cibernetică ale unei organizații, respectiv pe (2) expunerea la riscurile de securitate cibernetică pe care organizația o are.

Adesea, alegerea inadecvată a modelului organizațional generează fie costuri nejustificate, fie pierderi operaționale, creșterea expunerii la riscuri sau materializarea unui spectru mai larg de amenințări și vulnerabilități de securitate cibernetică.

Modelul in-house

Modelul „in-house" înseamnă că o organizație gestionează și coordonează intern procesele și procedurile de răspuns la incidente de securitate cibernetică, fără a recurge la serviciile unui furnizor extern specializat.
Acest model este pretabil pentru organizațiile care dispun pe plan intern de toate resursele necesare și le pot aloca în consecință. Fie este vorba de organizații mici care gestionează procese și infrastructuri nu tocmai complexe, fie este vorba de organizații specializate care gestionează procese extrem de sensibile și care dispun „in-house" de toate resursele necesare organizării adecvate a răspunsului la incidente.

Organizațiile care adoptă acest model trebuie să se asigure că au capabilități adecvate și mențin personal dedicat pentru răspunsul la incidente, în acord cu riscurile de securitate cibernetică la care sunt supuse.

AVANTAJE
✓ organizația are un controlul asupra datelor și proceselor de securitate cibernetică; ✓ riscul de expunere a datelor sensibile către terți este mai redus; ✓ o mai mare flexibilitate, deoarece organizațiile au posibilitatea de a adapta din mers răspunsul la incidente în acord cu procedurile, nevoile și cerințele interne specifice; ✓ costurile inițiale sunt mai reduse;
DEZAVANTAJE
➢ costuri ridicate pe termen lung; ➢ capacitate de adaptare la amenințări și agilitate reduse; ➢ capacitatea de răspuns este drastic limitată de accesul limitat la resurse, capabilități și expertiză dinafara organizației;

Modelul MSSP/MSP

Abordarea MSSP (Managed Security Service Provider) sau MSP (Managed Security Provider) este situația în care o organizație își externalizează gestionarea securității cibernetice către un furnizor specializat de servicii de securitate cibernetică.
Pentru majoritatea organizațiilor, externalizarea securității cibernetice se poate dovedi o opțiune atractivă pentru a beneficia de expertiză și tehnologii avansate de securitate cibernetică fără investiții interne semnificative.
În funcție de specificul organizației și nivelul său de risc, acest model presupune o colaborare continuă cu un furnizor de servicii specializat care are rolul de a gestiona

și menține securitatea cibernetică a organizației-client. MSSP/MSP se va asigura că are o vizibilitate de 100% asupra infrastructurii și sistemelor clientului, pe care le va monitoriza constant pentru a preveni, monitoriza, detecta, izola și răspunde timpuriu la incidentele de securitate cibernetică, asigurând astfel o protecție optimă a organizației-client.

De regulă, organizațiile care nu au competențe interne specializate sau care nu își permit dezvoltarea acestora pe plan intern pot apela la un MSSP/ MSP ca o alternativă eficientă și rentabilă pentru gestionarea tuturor aspectelor referitoare la securitatea cibernetică. Externalizarea serviciilor de securitate cibernetică este cel mai adesea o soluție convenabilă prin care o organizație își optimizează costurile operaționale și cele cu resursele umane.

De cele mai multe ori, o astfel de soluție va reduce semnificativ costurile pentru o organizație-client, putându-se astfel redirecționa importante resurse umane și financiare către zonele/ direcțiile unde este cea mai mare nevoie. În acest fel, organizația client va putea să se concentreze asupra obiectivelor sale de bază, în timp ce MSSP/ MSP va gestiona securitatea cibernetică.

AVANTAJE
✓ optimizarea costurilor cu securitatea cibernetică (-20% până la -85% în funcție de specificul organizației); ✓ **acces facil la expertiza specializată pe care un MSSP/ MSP o oferă;** ✓ **monitorizare continuă, 24/7;** ✓ **flexibilitate și scalabilitate, deoarece serviciile pot fi adaptate și dimensionate în funcție de nevoile organizației-client;** ✓ rezultate măsurabile;
DEZAVANTAJE
➢ **organizația este dependentă de un terț pentru aspectele critice ale securității cibernetice;** ➢ **aspectele sensibile ale organizație sunt partajate cu un terț;** ➢ **costuri recurente în cazul unor schimbări organizaționale;** ➢ pot apărea dificultăți în comunicarea și integrarea eficientă a serviciilor oferite;

Modelul mixt

Modelul mixt de gestionare a securității cibernetice reprezintă o abordare combinată în care o organizație își gestionează intern anumite aspecte de bază ale securității cibernetice, în timp chestiunile de o complexitate ridicată vor fi externalizate către un furnizor specializat MSSP/ MSP.

Nu se poate vorbi de un „tipar” sau un „rețetar” standard pentru acest model, el fiind de cele mai multe ori organizat ad-hoc, în funcție de resursele interne ale unei organizații, de nevoile sale de securitate cibernetică sau de expunerea la risc.

Modelul mixt se recomandă organizațiilor care dispun de o anumită expertiză internă în securitatea cibernetică, dar care nu pot face față tuturor provocărilor și evoluțiilor în continuă schimbare. Combinația dintre resursele interne și cele externalizate oferă organizației un grad sporit de flexibilitate, putând optimiza astfel cheltuielile cu securitatea cibernetică care se pot dovedi costisitoare.

Acest model are o complexitate ridicată și de aceea se recomandă ca deciziile privind internalizarea, respectiv externalizarea serviciilor de securitate cibernetică să fie luate alături de un consultant sau un MSSP/ MSP.

Alegerea modelului optim pentru gestionarea incidentelor de securitate cibernetică

Alegerea modelului optim de organizare a răspunsului la incidente de securitate cibernetică pentru o organizație este o decizie strategică ce trebuie să ia în considerare mai mulți factori cheie. Acești factori includ resursele disponibile, competențele interne, specificul activității, nivelul de risc și amenințările specifice industriei, precum și obiectivele de afaceri și cerințele de conformitate. Principalele pentru alegerea modelului adecvat:

Dimensiunea și complexitatea organizației
Organizațiile mari, cu infrastructuri IT&C complexe, ar putea beneficia mai mult de un model in-house sau mixt, datorită nevoii de control și personalizare a răspunsului la incidente.
Organizațiile mai mici sau cu infrastructuri mai puțin complexe ar putea beneficia mai mult de un model MSSP/MSP mai cost-eficient și mai simplu de gestionat.

Resursele disponibile
Capacitatea de a aloca resurse financiare și umane pentru gestionarea securității cibernetice este crucială. Organizațiile cu resurse limitate ar putea beneficia de expertiza și economiile oferite de un MSSP/MSP. Organizațiile cu resurse ample ar putea prefera să își dezvolte propriile echipe de răspuns la incidente pentru a menține un control mai strict asupra datelor și proceselor.

Expertiza internă
Prezența sau absența unei echipe de securitate cibernetică cu expertiză poate influența alegerea modelului. Organizațiile cu expertiză internă solidă pot opta pentru un model in-house sau mixt, în timp ce altele pot externaliza această funcție pentru a accesa competențele necesare.

Natura și sensibilitatea datelor
Organizațiile care gestionează date extrem de sensibile sau confidențiale (de exemplu, în domeniile financiar, sănătate, guvernamental) preferă de cele mai multe ori un model in-house pentru a maximiza controlul asupra securității datelor. Totuși, chiar și aceste organizații pot beneficia de serviciile specializate ale unui MSSP/MSP pentru anumite aspecte ale securității cibernetice.

Conformitatea și reglementările legale
Cerințele specifice de conformitate și reglementare pot dicta necesitatea unor măsuri (controale) de securitate specifice și a unor rapoarte detaliate, influențând alegerea modelului de organizare a răspunsului la incidente.

Toleranța la risc și strategia de securitate cibernetică
Strategia generală de securitate cibernetică și toleranța la risc a organizației ghidează de cele mai multe ori alegerea modelului, asigurându-se că răspunsul la incidente este

aliniat cu obiectivele de afaceri și cu toleranța față de riscurile de securitate ale organizației.

Cursul nr. 9

Auditul în securitatea cibernetică se concentrează pe evaluarea modului în care practicile de securitate ale unei organizații respectă standardele și reglementările în vigoare. Prin standarde și reglementări în vigoare, se înțeleg toate reglementările cu incidență asupra organizației, atât interne, cât și externe.

Obiectivele auditului

Auditurile de securitate sunt esențiale, deoarece oferă garanții că organizațiile auditate își protejează eficient activele digitale și sunt conforme cu obligațiile legale și de reglementare, minimizând astfel riscul de breșe de securitate și potențialele sancțiuni.

- **Identificarea și evaluarea riscurilor de securitate cibernetică**
- **Verificarea implementării controalelor de securitate**
- **Evaluarea eficacității controalelor de securitate**
    - Auditul trebuie să evalueze dacă controalele de securitate implementate de organizație sunt eficiente în prevenirea, detectarea și reacționarea la incidentele de securitate.
    - Se analizează dacă controalele sunt adecvate pentru riscurile identificate și dacă sunt implementate și administrate în mod corespunzător.
- **Verificarea conformității continue a organizației**
- **Identificarea oportunităților de îmbunătățire a securității**
    - Auditul poate identifica oportunități de îmbunătățire a posturii de securitate a organizației.

Exemplu:

1. Verificarea respectării politicilor de securitate ale organizației
Obiective specifice:

- Toți utilizatorii au parole complexe și unice.
- Parolele sunt modificate periodic conform politicii.
- Accesul la resursele IT este controlat pe baza principiului „necesității de a ști”.
- Toate dispozitivele portabile sunt criptate.

2. Testarea eficienței soluțiilor de protecție
Obiective specifice:

- Soluțiile antivirus și anti-malware sunt actualizate la zi.
- Se realizează scanări periodice ale sistemelor pentru a identifica malware-ul.
- Soluțiile de firewall blochează accesul neautorizat la resursele IT.
- Se realizează teste de penetrare pentru a evalua eficacitatea soluțiilor de securitate.

3. Evaluarea procesului de gestionare a incidentelor
Obiective specifice:

- Există un plan documentat de gestionare a incidentelor de securitate.

- Angajații sunt instruiți cu privire la modul de raportare a incidentelor de securitate.
- Incidentele de securitate sunt investigate și remediate în timp util.
- Se realizează lecții învățate din incidentele de securitate pentru a preveni repetarea lor.

4. Identificarea vulnerabilităților

Obiective specifice:

- Se realizează scanări de vulnerabilități a sistemelor și aplicațiilor IT.
- Vulnerabilitățile identificate sunt remediate în timp util.
- Se utilizează soluții de gestionare a vulnerabilităților pentru a monitoriza și remedia vulnerabilitățile.

5. Verificarea respectării reglementărilor

Obiective specifice:

- Se verifica respectarea reglementărilor conform cu GDPR, ISO/IEC 27001, CIS CSS, șamd.
- Se iau măsuri prompte pentru a remedia orice neconformitate identificată.

Acesta este un exemplu minimalist ce conține obiective specifice care pot fi incluse în auditul de conformitate a securității cibernetice.

De reținut: Obiectivele specifice vor varia în funcție de specificul organizației, de riscurile identificate și de reglementările aplicabile.

Beneficiile auditului de conformitate

- **Îmbunătățește postura de securitate**: Auditul poate identifica vulnerabilitățile și riscurile care pot fi exploatate de atacatori.
- **Asigură respectarea standardelor și reglementărilor**: Auditul poate ajuta organizațiile să se conformeze standardelor și reglementărilor relevante, cum ar fi GDPR, ISO/IEC 27001 sau CIS CSS.
- **Crește încrederea în organizație și reputația acesteia**: Auditul poate crește încrederea clienților, partenerilor și altor părți interesate în securitatea organizației.
- **Reduce costurile**: Identificarea și remedierea vulnerabilităților în stadiu incipient ajută la evitarea costurilor semnificative asociate cu incidentele de securitate.

Tipuri de audituri de conformitate

- **Audit intern**: Realizat de personalul intern al organizației.
  - Avantaje:
    - Costuri mai mici (de obicei între 1.000 și 10.000 EUR)
    - Flexibilitate mai mare
    - Posibilitatea de a concentra auditul pe anumite domenii de interes
  - Dezavantaje:
    - Lipsa de independență
    - Posibilitatea de a fi influențat de management
    - Lipsa de expertiză specifică în domeniul securității cibernetice

- **Audit extern**: Realizat de un terț independent specializat și acreditat pentru audit și consultanță (de regulă).
    - Avantaje:
        - Independență și obiectivitate sporite
        - Expertiză specifică în domeniul securității cibernetice
        - Acces la o gamă largă de instrumente și resurse
    - Dezavantaje:
        - Costuri mai mari (de obicei între 5.000 și 20.000 EUR)
        - Durata mai mare a auditului
        - Posibilitatea ca auditorii externi să nu aibă o cunoaștere detaliată a sistemelor și proceselor interne
- **Audit (test) de penetrare**: Simulează posibile atacuri cibernetice asupra organizației pentru a identifica vulnerabilitățile din sistemele acesteia. Costurile variază foarte mult, în funcție de dimensiunea organizațiile și obiectivele specifice. De obicei, în ceea ce privește costurile, poate varia între 100 și 300 EUR om-oră. Un test de penetrare complex, care include mai multe scenarii și tehnici avansate, poate avea un cost om-oră mai mare.
    - Teste de penetrare tip „cutia neagră”: Auditorii nu au nicio informație prealabilă despre sistemele organizației.
    - Teste de penetrare „cutia gri”: Auditorii au o informație limitată despre sistemele organizației.
    - Teste de penetrare „cutia albă”: Auditorii au acces complet la sistemele organizației.

Alegerea tipului de audit potrivit depinde de mai mulți factori, cum ar fi dimensiunea organizației, bugetul disponibil și riscurile de securitate identificate. Este recomandat să se realizeze o combinație de audituri interne și externe pentru a beneficia la maxim de avantajele auditării. Auditul de penetrare este un instrument foarte valoros pentru a identifica vulnerabilitățile din sistemele organizației și pentru a evalua eficacitatea controalelor de securitate.

Principiile auditului de conformitate

- **Independența:** Auditorul trebuie să fie independent de entitatea auditată pentru a menține obiectivitatea.
- **Obiectivitatea:** Auditul trebuie să fie imparțial și bazat pe dovezi concrete.
- **Profesionalismul:** Auditorul trebuie să dețină competențele și calificările necesare pentru a efectua auditul.
- **Confidențialitatea:** Informațiile obținute în timpul auditului trebuie păstrate confidențiale.
- **Documentarea:** Toate etapele auditului trebuie documentate în mod clar și concis.

Livrabile

Exemple de livrabile:

- Raport de audit de securitate cibernetică (document principal)

- Lista de vulnerabilități identificate
- Raport tehnic detaliat al testelor de penetrare
- Recomandări de remediere a vulnerabilităților
- Anexe: Documente suplimentare care conțin informații detaliate, cum ar fi liste de vulnerabilități, recomandări de remediere și rapoarte tehnice.

Structura raportului de audit

- **Introducere:** Prezentarea organizației, scopul auditului și metodologia utilizată.
- **Constatări:** Prezentarea detaliată a vulnerabilităților identificate, cu descrierea lor, riscul asociat și recomandări de remediere.
- **Concluzii:** O sinteză a rezultatelor auditului, cu o evaluare generală a stării de securitate a organizației.
- **Recomandări:** Propuneri concrete pentru remedierea vulnerabilităților identificate.
- **Anexe:** Pot include liste de vulnerabilități, rapoarte tehnice detaliate, dovezi ale testelor efectuate etc.

Dimensiunea raportului de audit

Depinde de complexitatea auditului și de cantitatea de informații identificate. De obicei, un raport de audit are între 10 și 50 de pagini pentru o organizație mică sau medie.

Formatul livrabilelor

Stilul de redactare trebuie să fie clar, concis și ușor de înțeles. Terminologia tehnică utilizată trebuie explicată în termeni simpli, iar tonul adoptat trebuie să fie profesional și imparțial.

De obicei, livrabilele sunt redactate în limba română. Pot fi în format electronic sau tipărit, depinde de preferințele clientului și de scopul livrabilelor. Se recomandă combinarea formatelor electronic și tipărit pentru a beneficia de avantajele ambelor.

De regulă, raportul de audit include diagrame și grafice pentru a ilustra informații complexe, iar aprobarea finală cu privire la structură va fi acordată în prealabil de către organizația auditată.

Recomandări în privința auditului

- Implementarea unui program regulat de audit de conformitate asupra organizației
- Utilizarea de instrumente și tehnologii avansate pentru a facilita procesul de audit.
- Angajarea de personal calificat cu experiență în auditul de securitate cibernetică.
- Educarea și sensibilizarea personalului cu privire la importanța securității cibernetice.

Exemplu de flux de lucru

1. **Planificarea**: Definirea scopului auditului, identificarea resurselor și selectarea instrumentelor.
2. **Colectarea datelor**: Utilizarea instrumentelor de scanare, penetrare și analiză a traficului de rețea pentru a colecta date și informații despre sistemele informatice ale organizației.
3. **Analiza datelor**: Identificarea vulnerabilităților și a altor probleme de securitate.
4. **Raportarea**: Redactarea unui raport de audit care prezintă constatările și recomandările de remediere.
5. **Remediere**: Implementarea recomandărilor de remediere pentru a îmbunătăți starea de securitate a organizației.

Instrumente utilizate

- **Scanere de vulnerabilități**: Identifică automat vulnerabilitățile cunoscute în sistemele informatice.
  Exemple: Nessus, OpenVAS, Nmap.
- **Instrumente pentru teste de penetrare**: Simulează atacuri cibernetice pentru a identifica vulnerabilitățile exploatabile.
  Exemple: Metasploit, Burp Suite, OWASP ZAP.
- **Instrumente de analiză a traficului de rețea**: Monitorizează traficul de rețea pentru a identifica activități suspecte.
  Exemple: Wireshark, tcpdump, Suricata.
- Instrumente de analiză a logurilor (jurnalelor): Analizează jurnalele de sistem pentru a identifica semne de intruziune sau alte probleme de securitate.
  Exemple: Splunk, ELK Stack, Graylog.
- Instrumente de gestionare a identității și accesului (IAM): Ajută la controlul accesului la resursele IT.
  Exemple: Active Directory, Azure Active Directory, Okta.
- Alte instrumente utile:
  - Instrumente de analiză a malware-ului: VirusTotal, Cuckoo Sandbox
  - Instrumente de conștientizare a securității cibernetice: KnowBe4, Cybrary

Alegerea instrumentelor cele mai potrivite depinde de specificul organizației, de riscurile de securitate identificate și de resursele disponibile. Se recomandă o combinație de mai multe tipuri de instrumente pentru a obține o imagine completă a stării de securitate a organizației. Este esențial să fie utilizate instrumente de la furnizori de încredere, actualizate la ultima versiune disponibilă.

Rolul CISO în auditul organizației

1. **Planificarea auditului**:
   - Stabilește obiectivele și scopul auditului.
   - Identifică resursele necesare și selectează echipa de audit.
   - Aprobă metodologia de audit și instrumentele utilizate.
2. **Executarea auditului**:
   - Supraveghează desfășurarea auditului și se asigură că respectă planul stabilit.

- Oferă consultanță echipei de audit cu privire la aspectele tehnice și de securitate.
- Asigură colaborarea cu alte departamente implicate in audit.

3. **Raportarea rezultatelor**:
   - Revizuiește și aprobă raportul de audit.
   - Prezinta concluziile și recomandările auditului conducerii organizației.
   - Răspunde la întrebările conducerii și ale altor părți interesate cu privire la rezultatele auditului.
4. Implementarea recomandărilor:
   - Dezvoltă un plan de remediere a vulnerabilităților identificate in urma auditului.
   - Monitorizează implementarea planului de remediere.
   - Informează conducerea organizației cu privire la progresul realizat in remedierea vulnerabilităților.

Cursul nr. 10

Security Operations Center (SOC)

În multe organizații, activitatea unui CERT/CSIRT are loc în cadrul unui SOC (Security Operations Center), entitate care este asemănătoare ca obiective, însă este mai complexă din perspectiva capabilităților de care dispune.

SOC este entitatea centralizată pentru toate operațiunile de securitate cibernetică. În vreme ce funcția de bază a unui CERT/CSIRT este răspunsul la incidentele de securitate cibernetică, funcțiile unui SOC sunt prevenirea, detectarea, monitorizarea, combaterea și remedierea incidentelor.

Ca principiu, în SOC are loc monitorizarea și detectarea amenințărilor în timp real în rețeaua unei organizații, în timp ce, de regulă, CERT/CSIRT se ocupă de răspunsul la incidente de securitate cibernetică după ce acestea au avut loc.
În timp ce un SOC și CERT/CSIRT funcționează 24/7, în multe cazuri, mai ales în funcție de specificul unei organizații, echipa CERT/CSIRT poate fi activată doar când are loc un incident de securitate.

Personalul care deservește un SOC are drept atribuții principale prevenirea, detectarea, monitorizarea, combaterea și remedierea incidentelor de securitate cibernetică, incluzând aici și răspunsul la incidente de securitate cibernetică.

Totodată, în timp SOC este de obicei localizat fizic în cadrul unei organizații, dar poate funcționa în anume cazuri ca serviciu (SOC-as-a-service), un CERT/CSIRT poate fi o entitate națională sau regională care oferă servicii unui număr mult mai mare de organizații sau chiar unor țări.

De pildă, în ceea ce privește resursele umane, pe lângă personalul CERT/CSIRT, într-un SOC putem regăsi și threat-hunteri, adică investigatori înalt specializați în domeniul securității cibernetice care se ocupă cu identificarea și contracararea amenințărilor cibernetice într-o organizație înainte ca acestea să apăra. De regulă, investigatorul se folosește de cunoștințele sale, de tehnici avansate și instrumente specializate pentru a cerceta, identifica și combate activ amenințările avansate și persistente care ar putea să fie neglijate de către sistemele automatizate de răspuns la incidente. Așadar,

din acest punct de vedere, spre deosebire de un CERT/CSIRT, într-un SOC prevenția și cunoașterea anticipativă sunt procese mult mai ample și mai complexe.

În esență, SOC și CERT/CSIRT au responsabilități similare și deservesc aceleași obiective de securitate cibernetică, însă rolul și modul de organizare sunt diferite. CERT/CSIRT pot opera în cadrul unui SOC, dar nu și viceversa.

Organizarea unui SOC

Organizarea unui Security Operations Center (SOC) implică structurarea și coordonarea unui ecosistem complex de procese, personal și tehnologii dedicate monitorizării continue, detectării, analizei și răspunsului la incidentele de securitate cibernetică. Un SOC eficient va proteja organizația împotriva amenințărilor cibernetice, reducând timpul de detectare și răspuns la incidente, minimizând impactul acestora.

Din ce este format SOC?

- **Personal**: Echipa unui SOC include analiști de securitate, threat hunteri, manageri de securitate, ingineri de sisteme și alți specialiști cu roluri dedicate în prevenirea, detectarea și răspunsul la amenințări cibernetice.
- **Procese și proceduri**: SOC-ul trebuie să aibă proceduri bine stabilite pentru gestionarea incidentelor, de la detectarea inițială până la remedierea completă și raportarea incidentelor.
- **Tehnologie**: Instrumentele și platformele tehnologice sunt esențiale pentru funcționarea SOC-ului, incluzând soluții de Security Information and Event Management (SIEM), instrumente de analiză forensic, soluții de threat intelligence, sisteme de detectare și prevenire a intruziunilor (IDS/IPS), etc.

De reținut: CISO este responsabil pentru selectarea tehnologiilor adecvate care să susțină operațiunile SOC-ului, luând în considerare nevoile specifice ale organizației și peisajul de amenințări. CISO supraveghează operațiunile zilnice ale SOC-ului, coordonând echipa și asigurându-se că procedurile de răspuns la incidente sunt eficient executate. CISO raportează conducerii executive din cadrul unei organizații în legătură cu performanța SOC, incidentele de securitate și despre recomandările necesare pentru îmbunătățirea continuă a securității.

Clasificarea SOC

SOC de nivel 1 (nivel triaj)

La acest nivel, activitatea se concentrează pe monitorizarea sistemelor și rețelelor pentru a detecta activități suspecte sau neobișnuite. Analistii de nivel 1 sunt primii care primesc alertele generate de sistemele automatizate de securitate (de exemplu, IDS, firewalls, SIEM) și sunt responsabili pentru triajul inițial al acestor alerte. Acest SOC are capacitatea de a filtra alertele false de cele legitime și de a escalada incidentele potențial grave către nivelurile superioare pentru investigații suplimentare. Totodată, acest tip de SOC asigură o monitorizare continuă și o reacție rapidă la incidentele de securitate de bază.

SOC de nivel 2 (nivel investigații)

În plus față de SOC nivel 1, SOC de nivel 2 poate prelua incidentele de securitate escalate de la Tier 1 și poate efectua o analiză mai aprofundată pentru a identifica sursa, metoda de atac și impactul potențial al incidentului. SOC de nivel 2 dispune de instrumente avansate pentru analiză forensic și poate determina amploarea unei breșe de securitate, concomitent cu implementare de măsuri de limitare a impactul incidentului.

SOC de nivel 3 (nivel threat-hunting)
SOC avansat care dispune de capabilitățile necesare pentru remedierea vulnerabilităților identificate, eradicarea rapidă a amenințărilor și implementarea măsurilor de securitate pentru a preveni reapariția incidentelor similare. Personalul acestui tip de SOC dispune de expertiză avansată în securitate cibernetică, capabili să dezvolte patch-uri, să configureze sistemele pentru a îmbunătăți securitatea și să lucreze la recuperarea datelor afectate. De asemenea, acest tip de SOC dispune de capabilități complexe de eliminare a surselor de amenințare, de restabilire a funcționalităților post-incident și de protejare avansată împotriva unor incidente viitoare. SOC de nivel 3 are capabilități de tip Threat Hunting și cyberintelligence. Personalul poate realiza activități complexe de threat hunting sau de analiză a tendințelor, respectiv de dezvoltare a unor strategii de prevenție pe termen lung. Poate realiza activități de anticipare și prevenire a amenințărilor emergente, respectiv de consolidare a posturii de securitate a organizației pe termen lung.

Diferența principală între aceste niveluri constă în gradul de specializare și în complexitatea activităților desfășurate. Pe măsură ce avansăm de la Tier 1 la Tier 4, nivelul de expertiză necesar și capacitatea de a gestiona incidente de securitate complexe cresc semnificativ. Alegerea structurii SOC-ului și a nivelului de tier adecvat depinde de specificul organizației, de resursele disponibile și de profilul de risc al acesteia.

Tehnologii SOC

Tehnologiile utilizate în SOC trebuie să asigure detectarea eficientă a amenințărilor, răspunsul rapid la incidente și monitorizarea continuă a securității cibernetice. Aceste tehnologii ajută echipa SOC să protejeze infrastructura organizației împotriva atacurilor cibernetice. Cele mai relevante categorii de tehnologii pentru SOC sunt:

Security Information and Event Management (SIEM)
Prin agregarea, normalizarea, analiza și raportarea datelor de log și evenimente de securitate colectate din diverse surse din infrastructura IT, SIEM-urile permit detectarea, alertarea și răspunsul la incidentele de securitate într-un mod eficient.

Funcții:
- Agregarea, normalizarea și analiza datelor de log și evenimente din multiple surse.
- Generarea de alerte bazate pe anomalii sau semnături de atacuri cunoscute.
- Asistență în investigația incidentelor și în raportarea pentru conformitate.

Exemple:

- **Splunk**: Oferă o platformă extensivă pentru monitorizarea securității, analiza datelor și obținerea de insight-uri operative.
- **IBM QRadar**: Un lider recunoscut în domeniul SIEM, care oferă detectarea sofisticată a amenințărilor și capabilități puternice de analiză.

Endpoint Detection and Response (EDR)
Endpoint Detection and Response (EDR) este o soluție de securitate cibernetică care monitorizează endpoint-urile (cum ar fi laptopuri, desktopuri, servere și dispozitive mobile) într-o rețea, în scopul de a detecta, investiga și răspunde la activități suspecte sau malițioase. EDR-urile sunt concepute pentru a oferi organizațiilor vizibilitate detaliată asupra activităților de pe endpoint-uri, capturând și stocând continuu datele de evenimente de securitate, care pot fi ulterior analizate pentru a identifica semnele de compromitere.

Funcții:
- Monitorizarea activităților suspecte la nivelul endpoint-urilor (ex. laptopuri, servere).
- Răspuns rapid la incidente, izolarea dispozitivelor, colectare date forensic și remediere.

Exemple:
- **CrowdStrike Falcon**: O soluție EDR cunoscută pentru capacitatea sa de a detecta și răspunde rapid la atacuri avansate.
- **SentinelOne**: Oferă prevenție, detectare, răspuns și vânătoare de amenințări, toate într-o singură platformă.

Threat Intelligence Platform (TIP)
TIP este un sistem sofisticat care colectează, agregă, corelează și analizează informații despre amenințări cibernetice dintr-o varietate de surse pentru a furniza organizațiilor cunoștințe actionable și contextuale despre amenințările actuale și emergente. Scopul acestei platforme este de a îmbunătăți capacitatea de detectare a amenințărilor, de a accelera răspunsul la incidente și de a informa strategiile de securitate cibernetică prin oferirea de insight-uri relevante și în timp util.

Funcții:
- Colectarea și analiza informațiilor despre amenințările cibernetice actuale și emergente.
- Integrarea cu alte sisteme de securitate pentru a îmbunătăți detectarea amenințărilor și răspunsul la incidente.

Exemple:
- **Anomali**: Permite organizațiilor să integreze și să coroboreze intelligence-ul de amenințare pentru a îmbunătăți detectarea și răspunsul.
- ThreatConnect: Oferă o platformă care combină analiza amenințărilor, automatizarea operațiunilor de securitate și colaborarea în echipă.

Network Traffic Analysis (NTA)
Prin examinarea detaliată a traficului de rețea în timp real sau înregistrat, soluțiile NTA oferă organizațiilor capacitatea de a detecta rapid amenințările de securitate, cum ar

fi malware, atacuri de tip insider, exfiltrarea de date și alte forme de comportament periculos sau neautorizat care nu sunt întotdeauna identificate prin metode tradiționale de securitate.

Funcții:

- Analiza traficului de rețea pentru a identifica activități suspecte, anomalii de trafic și modele potențial malițioase.
- Oferă vizibilitate asupra comunicațiilor de rețea și poate detecta malware, exfiltrări de date și alte amenințări.

Exemple Comerciale:

- **Darktrace**: Utilizează inteligența artificială pentru a detecta și răspunde automat la amenințările din rețea în timp real.
- **Vectra**: Oferă detectarea amenințărilor bazată pe AI și monitorizarea continuă a rețelei, identificând atacurile în desfășurare.

Security Orchestration, Automation, and Response (SOAR)
(SOAR) se referă la colecția de tehnologii software care permit organizațiilor să colecteze date despre incidentele de securitate din diverse surse, să orchestreze și să automatizeze procesele de răspuns la aceste incidente și să ofere echipelor de securitate instrumentele necesare pentru a răspunde la amenințări într-un mod mai eficient și scalabil.

Funcții:

- Automatizarea răspunsurilor la incidente și a workflow-urilor de securitate.
- Integrarea diferitelor tehnologii de securitate și facilitarea colaborării între echipe.

Exemple:

- **Palo Alto Networks Cortex XSOAR**: O platformă completă care combină orchestration, automatizare, managementul incidentelor și colaborarea.
- **IBM Resilient**: Oferă capabilități avansate de orchestration și automatizare, îmbunătățind eficiența răspunsului la incidente.

Alegerea tehnologiilor pentru un SOC trebuie să se bazeze pe o evaluare aprofundată a nevoilor specifice de securitate ale organizației, a arhitecturii IT existente și a capabilităților echipei de securitate. Rolul CISO în acest proces include definirea strategiei de securitate cibernetică, selecția soluțiilor tehnologice care susțin această strategie și asigurarea unei implementări și gestionări eficiente a SOC-ului în concordanță cu obiectivele organizației.

Cursul nr. 11

Importanța protecției datelor

Protecția datelor înseamnă procesul de securizare a acestora împotriva accesului neautorizat, utilizării, dezvăluirii, perturbării, modificării sau distrugerii acetora. Este important pentru organizații să protejeze datele pentru că astfel:

- Asigură securitatea generală a organizației prin asigurarea confidențialității clienților, angajaților sau a proceselor organizaționale.
- Respectă reglementările legale, cum ar fi GDPR.
- Reduc riscurile reputaționale care pot fi costisitoare și dăunătoare organizației
- Cresc încrederea față de organizație

Măsuri generale de protecție a datelor

Există o serie de măsuri generale pe care organizațiile le pot lua pentru a proteja datele, cum ar fi:

- Implementarea politicilor și procedurilor de securitate a datelor (ex. DLP)
- Educarea personalului propriu, respectiv a terților cu privire la importanța protecției datelor și a modului de protejare a datelor.
- Utilizarea tehnicilor și tehnologiilor specializate, cum ar fi criptarea și firewall-urile.
- Monitorizarea sistemelor de securitate pentru a detecta și preveni încălcările.

Politicile de Data Loss Prevention (DLP)

Politicile DLP sunt un set de reguli și proceduri implementate de o organizație pentru a proteja datele sensibile de accesul neautorizat, utilizarea, dezvăluirea, furtul sau distrugerea lor.

DLP:

- **Protejează datele sensibile:** Politicile DLP ajută la protejarea datelor confidențiale, cum ar fi informațiile financiare, datele despre clienți, proprietatea intelectuală și informațiile de identificare personală (PII).
- **Reduc riscul de încălcări ale securității datelor:** Politicile DLP pot ajuta la prevenirea scurgerilor de date și a altor încălcări ale securității datelor, care pot fi costisitoare și dăunătoare reputației organizației.
- **Asigură respectarea reglementărilor:** Politicile DLP pot ajuta organizațiile să respecte reglementările, cum ar fi GDPR, care le obligă să protejeze datele cu caracter personal.

Elemente cheie ale politicilor DLP:

- **Clasificarea datelor:** Politicile DLP definesc diferite tipuri de date sensibile și clasifică datele organizației în funcție de nivelul lor de sensibilitate.
- **Controale de acces:** Politicile DLP definesc cine are acces la diferite tipuri de date sensibile și ce pot face cu ele.
- **Educarea utilizatorilor:** Politicile DLP includ instruire pentru utilizatori cu privire la importanța protecției datelor și a modului de respectare a politicilor DLP.
- **Monitorizare și auditare:** Politicile DLP includ monitorizarea și auditarea accesului la datele sensibile pentru a identifica și preveni încălcările politicilor.

Tipuri de politici DLP:

- **Politici bazate pe reguli:** Aceste politici definesc reguli specifice care trebuie respectate pentru a accesa sau utiliza datele sensibile.
- **Politici bazate pe riscuri:** Aceste politici evaluează riscul asociat cu accesul la datele sensibile și permit accesul în funcție de nivelul de risc.

Implementarea politicilor DLP:

Implementarea politicilor DLP este un proces continuu care implică:

- Definirea politicilor DLP: Organizația trebuie să definească politicile DLP care se potrivesc nevoilor sale specifice.
- Implementarea controalelor DLP: Organizația trebuie să implementeze controalele DLP necesare pentru a pune în aplicare politicile DLP.
- Educarea utilizatorilor: Organizația trebuie să educe utilizatorii cu privire la importanța protecției datelor și a modului de respectare a politicilor DLP.
- Monitorizare și auditare: Organizația trebuie să monitorizeze și să auditeze accesul la datele sensibile pentru a identifica și preveni încălcările politicilor.

Datele cu caracter personal (DCP)

Datele cu caracter personal (DCP) se referă la orice informație cu privire la o persoană fizică identificată sau identificabilă, denumită conform Regulamentului (UE) 2016/679 (GDPR) drept „persoană vizată”.

DCP necesită o atenție specială din punct de vedere organizațional și legal pentru a le proteja de accesul neautorizat și de utilizarea necorespunzătoare. Implementarea unor măsuri adecvate de protecție a datelor și respectarea reglementărilor specifice privind protecția datelor sunt esențiale pentru a proteja confidențialitatea și drepturile persoanelor vizate.

Exemple de DCP obișnuite:

- Numele și prenumele
- Adresa de domiciliu sau de corespondență
- Numărul de telefon
- Adresa de e-mail
- Codul numeric personal (CNP)
- Informații medicale
- Informații financiare
- Imagini și înregistrări video
- Date de locație
- Adresa IP

Exemple de DCP speciale:

- Origine rasială sau etnică
- Opinii politice

- Convingeri religioase sau filosofice
- Date genetice
- Date biometrice (amprente digitale, recunoaștere facială)
- Date privind sănătatea
- Date privind viața sexuală sau orientarea sexuală

Motive pentru atenție sporită

DCP necesită o atenție specială din punct de vedere organizațional și legal datorită sensibilității lor și a riscului ridicat de încălcare a vieții private. Utilizarea necorespunzătoare a DCP poate duce la:

- **Furtul de identitate:** Persoanele rău intenționate pot folosi DCP furate pentru a se pretinde a fi alte persoane și a comite fraude.
- **Discriminare:** DCP pot fi utilizate pentru a discrimina anumite persoane pe baza rasei, religiei, orientării sexuale sau altor criterii.
- **Spam și marketing nedorit:** DCP pot fi utilizate pentru a trimite spam și marketing nedorit persoanelor.
- **Pierderea reputației:** O încălcare a datelor care implică DCP poate deteriora grav reputația unei organizații.

Prin urmare, organizațiile care colectează și prelucrează DCP trebuie să ia măsuri sporite pentru a le proteja.

Regulamentul (UE) 2016/679 (GDPR)

GDPR este un regulament european adoptat în 2016 care are ca scop protejarea datelor cu caracter personal ale cetățenilor Uniunii Europene. Se aplică tuturor organizațiilor care prelucrează date cu caracter personal, indiferent de locația lor.

Domeniul de aplicare al GDPR:

- **Organizații cu sediul în UE:** Indiferent unde are loc prelucrarea datelor, GDPR se aplică tuturor organizațiilor care au sediul în Uniunea Europeană.
- **Organizații care oferă bunuri sau servicii cetățenilor UE:** Chiar dacă nu are sediul în UE, o organizație trebuie să respecte GDPR dacă oferă bunuri sau servicii cetățenilor UE.
- **Organizații care monitorizează comportamentul cetățenilor UE:** Indiferent de scopul monitorizării, GDPR se aplică organizațiilor care monitorizează comportamentul cetățenilor UE, atâta timp cât are loc în Uniunea Europeană.

De reținut:
- GDPR protejează drepturile tuturor persoanelor aflate pe teritoriul UE, indiferent de poziționarea geografică a operatorului de date;
- GDPR extinde sfera de aplicare şi asupra operatorilor de date stabiliți în afara UE, în măsura în care bunurile şi/sau serviciile acestora sunt adresate (şi) persoanelor aflate pe teritoriul UE;

Termeni relevanți GDPR

- **Prelucrare DCP**: Orice operațiune sau set de operațiuni efectuate asupra datelor cu caracter personal sau asupra seturilor de date cu caracter personal, cu sau fără utilizarea de mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, extragerea, consultarea, utilizarea, divulgarea prin transmitere, diseminarea sau punerea la dispoziție în orice alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea.
- **Consimțământ**: Orice manifestare de voință liberă, specifică, informată și neechivocă a subiectului datelor, prin care acesta acceptă, printr-o declarație sau printr-o acțiune clară afirmativă, prelucrarea datelor cu caracter personal care îl privesc.
- **DPO** sau responsabilul cu protecția DCP este o persoană desemnată de o organizație pentru a se asigura că aceasta respectă GDPR și standarde și/sau reglementări privind protecția datelor personale.
- **Operator DCP**: Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care, singur sau împreună cu altele, stabilește scopurile și mijloacele de prelucrare a datelor cu caracter personal.
- **Persoana împuternicită:** Persoana fizică sau juridică, autoritatea publică, agenția sau alt organism care prelucrează date cu caracter personal în numele controlorului.

Pseudonimizare: Tehnica de prelucrare a datelor cu caracter personal prin care datele nu mai pot fi atribuite unei persoane vizate specifice fără utilizarea de informații suplimentare, care sunt stocate separat și supuse unor măsuri tehnice și organizatorice pentru a se asigura că datele cu caracter personal nu pot fi atribuite unei persoane fizice identificate sau identificabile.

Principalele cerințe ale GDPR

- **Legalitate, corectitudine și transparență:** Prelucrarea datelor cu caracter personal trebuie să fie legală, corectă și transparentă.
- **Scop specific, explicit și legitim:** Datele cu caracter personal trebuie colectate în scopuri specifice, explicite și legitime și nu pot fi prelucrate ulterior într-un mod incompatibil cu aceste scopuri.
- **Minimizare a datelor:** Datele cu caracter personal trebuie să fie adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile pentru care sunt prelucrate.
- **Exactitate:** Datele cu caracter personal trebuie să fie exacte și actualizate.
- **Limitarea stocării:** Datele cu caracter personal trebuie stocate doar pentru o perioadă de timp care este necesară pentru scopurile pentru care sunt prelucrate.
- **Integritate și confidențialitate:** Datele cu caracter personal trebuie să fie păstrate în siguranță și confidențiale.
- **Drepturile persoanelor vizate:** Persoanele vizate au o serie de drepturi, cum ar fi dreptul de acces, de rectificare, de ștergere și de opoziție.

Obligația de a desemna un responsabil cu protecția datelor (DPO) revine următoarelor entități:

1. Autorități și organisme publice:

- Toate autoritățile și organismele publice, cu excepția instanțelor care acționează în cadrul funcției lor jurisdicționale.

2. Operatori care prelucrează date sensibile:

- Operatorii care prelucrează date cu caracter personal sensibile pe scară largă.
- Operatorii care efectuează o monitorizare regulată și sistematică a persoanelor vizate la scară largă.

3. Operatori care prelucrează cantități mari de date:

- Operatorii ale căror activități principale constau în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate, cum ar fi companiile care oferă motoare de căutare online sau rețele sociale.

Exemple de operatori de date:

- O companie care colectează datele clienților săi pentru a le oferi produse și servicii.
- Un spital care colectează datele pacienților săi pentru a le oferi îngrijire medicală.
- O autoritate publică care colectează datele cetățenilor săi pentru a le oferi servicii publice.

GDPR obligă operatorii și persoanele împuternicite să țină o evidență a activităților de prelucrare în mai multe situații, inclusiv:

- **Operatorul are mai mult de 250 de angajați.**
- **Prelucrarea este susceptibilă să genereze un risc ridicat pentru drepturile și libertățile persoanelor vizate.**
- **Prelucrarea include categorii speciale de date (de exemplu, date privind sănătatea, originea rasială sau etnică, convingerile religioase sau filosofice).**
- **Prelucrarea nu este ocazională.**

Deoarece prelucrarea datelor nu este de obicei ocazională în activitatea unei firme, este recomandat ca **toți operatorii** să țină o evidență a activităților de prelucrare.

Responsabilul cu protecția datelor personale (DPO)

Atribuțiile DPO:

- Informează și consiliază operatorul sau persoana împuternicită și angajații acestora cu privire la obligațiile care le revin în temeiul GDPR.

- Oferă consultanță cu privire la evaluarea impactului asupra protecției datelor și la monitorizarea sa.
- Informează persoanele vizate cu privire la prelucrarea datelor lor cu caracter personal.
- Monitorizează respectarea GDPR de către operator sau persoana împuternicită.
- Cooperează cu autoritatea de supraveghere.
- Acționează ca punct de contact pentru autoritatea de supraveghere și pentru persoanele vizate.
- Asigură respectarea politicilor interne ale operatorului sau ale persoanei împuternicite în domeniul protecției datelor.
- Oferă consultanță cu privire la proiectele de acte juridice care implică prelucrarea datelor cu caracter personal.

Cine poate îndeplini funcția de DPO?

Funcția de DPO poate fi îndeplinită de:

- Un membru al personalului operatorului sau al persoanei împuternicite.
- O persoană fizică sau juridică externă.

Calificări necesare:

Persoana care îndeplinește funcția de DPO trebuie să aibă:

- Cunoștințe și experiență aprofundate în domeniul protecției datelor.
- Capacitatea de a-și îndeplini sarcinile în mod independent.
- Abilitatea de a menține confidențialitatea informațiilor.

Recomandări:

- Este important ca DPO să aibă experiență și cunoștințe relevante în domeniul protecției datelor, respectiv are resursele necesare pentru a-și îndeplini sarcinile.

Evidența prelucrării DCP

Evidența prelucrării datelor cu caracter personal este un instrument esențial pentru a demonstra respectarea GDPR. Această evidență trebuie să fie ținută de către operatori și persoane împuternicite și trebuie să conțină anumite informații specifice.

Evidențe obligatorii conform GDPR

Evidența operatorului:

Conform GDPR, evidența operatorului trebuie să cuprindă obligatoriu următoarele informații:

(a) Identificarea

- Numele și datele de contact ale operatorului.
- Datele de contact ale operatorului asociat, ale reprezentantului operatorului și ale responsabilului cu protecția datelor (dacă este cazul).

(b) Scop

- O descriere clară a scopurilor prelucrării datelor cu caracter personal.

(c) Categorii de date

- O descriere a categoriilor de persoane vizate și a categoriilor de date cu caracter personal prelucrate.

(d) Destinatari

- Categoriile de destinatari cărora le-au fost sau le vor fi divulgate datele cu caracter personal.
- Specificarea destinatarilor din țări terțe sau organizații internaționale (dacă este cazul).

(e) Transferuri către țări terțe

- Informații detaliate despre transferurile de date cu caracter personal către o țară terță sau o organizație internațională (dacă este cazul).

(f) Termene de ștergere

- Termenele-limită preconizate pentru ștergerea diferitelor categorii de date (dacă este posibil).

(g) Măsuri de securitate

- O descriere generală a măsurilor tehnice și organizatorice de securitate implementate pentru a proteja datele (conform GDPR, articolul 32 alineatul (1)).

Evidența persoanei împuternicite

Evidența persoanei împuternicite trebuie să cuprindă obligatoriu următoarele informații:

(a) Identificarea:

- Numele și datele de contact ale persoanei sau persoanelor împuternicite de operator.
- Numele și datele de contact ale fiecărui operator în numele căruia acționează persoana împuternicită.
- Datele de contact ale reprezentantului operatorului sau al persoanei împuternicite de operator (dacă este cazul).

(b) Activități de prelucrare:

- O descriere a categoriilor de activități de prelucrare desfășurate în numele fiecărui operator.

(c) Transferuri către țări terțe:

- Informații detaliate despre transferurile de date cu caracter personal către o țară terță sau o organizație internațională (dacă este cazul).

(d) Măsuri de securitate:

- O descriere generală a măsurilor tehnice și organizatorice de securitate implementate pentru a proteja datele (conform GDPR, articolul 32 alineatul (1)).

Formatul evidențelor

Evidența poate fi ținută sub orice format, fie pe hârtie, fie în format electronic. Este important ca formatul ales să fie ușor accesibil și lizibil.

Actualizarea evidențelor

Evidența trebuie actualizată periodic pentru a reflecta orice modificare a operațiunilor de prelucrare a datelor.

Accesul la evidențe

Evidența trebuie să fie pusă la dispoziția autorităților de supraveghere la cerere.

În România, autoritatea de supraveghere este Autoritatea Națională pentru Supravegherea Prelucrării Datelor cu Caracter Personal (ANSPDCP).

Evaluarea impactului asupra protecției datelor (DPIA)

DPIA este un proces sistematic menit să evalueze riscurile și impactul potențial al unei prelucrări de date cu caracter personal asupra drepturilor și libertăților persoanelor vizate. DPIA este un instrument important pentru a demonstra conformitatea cu GDPR și pentru a implementa măsuri adecvate de protecție a datelor.

Când este necesară o DPIA?

O DPIA este obligatorie in urmatoarele situatii:

- Prelucrarea implică **categorii speciale de date cu caracter personal** (de exemplu, date privind sănătatea, originea rasială sau etnică, convingerile religioase sau filosofice).
- Prelucrarea are loc la **scară largă** și implică monitorizarea sistematică a zonelor accesibile publicului.
- Prelucrarea implică **operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate** la scară largă.

De asemenea, o DPIA este recomandată în urmatoarele situații:

- Prelucrarea implică **un risc ridicat** pentru drepturile și libertățile persoanelor vizate.
- Operatorul dorește să demonstreze respectarea GDPR.

Ce conține o DPIA?

O DPIA conține o serie de informații, inclusiv:

- O descriere a operațiunilor de prelucrare.
- O evaluare a riscurilor și impactului potențial al prelucrării.
- Măsurile luate pentru a atenua riscurile și a proteja datele.
- Consultarea cu autoritatea de supraveghere (dacă este necesar).

Beneficiile utilizării DPIA:

- Ajută la identificarea și atenuarea riscurilor asociate prelucrării datelor.
- Demonstrează conformitatea cu GDPR.
- Crește încrederea persoanelor vizate in modul in care operatorul prelucrează datele lor.

Sancțiuni GDPR

Principalele sancțiuni conform GDPR sunt:

Amenzi administrative:

- pentru încălcări minore, amenda poate ajunge până la 10.000.000 EUR sau până la 2% din cifra de afaceri globală anuală totală a exercițiului financiar precedent, alegându-se valoarea cea mai mare.
    - Aceste încălcări includ, de obicei, nerespectarea cerințelor organizaționale și tehnice, cum ar fi neîndeplinirea obligației de a numi un responsabil cu protecția datelor sau nerespectarea cerințelor legate de securitatea datelor.
- Pentru încălcări majore, amenda poate ajunge până la 20.000.000 EUR sau până la 4% din cifra de afaceri globală anuală totală a exercițiului financiar precedent, alegându-se valoarea cea mai mare.
    - Încălcările majore includ încălcări ale drepturilor fundamentale ale subiecților de date, cum ar fi prelucrarea ilegală a datelor cu caracter personal sau încălcarea principiilor de bază pentru prelucrarea datelor, cum ar fi consimțământul.

Alte sancțiuni:

- Avertisment și ordonanță de remediere: Acestea sunt măsuri preventive sau corective care pot fi aplicate înainte de a se ajunge la sancțiuni financiare. Ele sunt folosite pentru a ghida organizațiile spre conformitate fără a aplica direct amenzi.
- Interdicția sau restricția prelucrării și ștergerea datelor: Aceste sancțiuni pot avea un impact semnificativ asupra operațiunilor unei organizații, deoarece pot

restricționa capacitatea acesteia de a opera cu datele cu caracter personal sau pot impune eliminarea completă a unor seturi de date.

Știați că…

- **Dreptul de a fi uitat**: Unul dintre cele mai discutate aspecte ale GDPR este "dreptul de a fi uitat" (Articolul 17), cunoscut și ca dreptul la ștergerea datelor. Acest drept permite unei persoane să solicite ștergerea datelor personale colectate de o organizație atunci când acestea nu mai sunt necesare pentru scopul pentru care au fost colectate sau dacă persoana își retrage consimțământul.
- **GDPR are aplicabilitate globală**: GDPR nu se limitează doar la organizațiile din UE. Orice companie, indiferent de locația acesteia, care procesează datele personale ale rezidenților UE, trebuie să respecte GDPR.
- **Obligații de notificare**: GDPR a introdus obligația pentru organizații de a raporta orice încălcare a securității datelor în termen de 72 de ore de la descoperirea acesteia.

Cursul nr. 12

Contextul global

În contextul global actual, securitatea cibernetică a devenit un pilon deosebit de important al strategiilor de securitate ale statelor și organizațiilor din întreaga lume. Peisajul amenințărilor cibernetice este într-o continuă evoluție, reflectând schimbările tehnologice rapide și capacitatea crescută a atacatorilor de a exploata vulnerabilități complexe.

Atacurile cibernetice au cunoscut o creștere exponențială în ultimii ani, atât în frecvență, cât și în complexitate. Printre cele mai comune forme de atacuri se numără:

- Atacurile de tip ransomware, care criptează fișierele victimelor și solicită plata unui răscumpărare pentru decriptarea datelor.
- Phishing-ul, prin care atacatorii încearcă să fure date și informații confidențiale, cum ar fi datele de autentificare sau informațiile financiare
- Malware, inclusiv viruși și troieni, care se infiltrează în sisteme pentru a le compromite sau distruge.
- Atacuri zero-day, care exploatează vulnerabilități necunoscute publicului și producătorilor de software la momentul atacului.

Pe lângă acestea, infracțiunile cibernetice, precum furtul de identitate și fraudele financiare sau spionajul cibernetic reprezintă amenințări majore pentru individ, organizații și pentru securitatea națională. Atacatorii cibernetici devin din ce în ce mai sofisticați, folosind tehnici avansate de atac pentru a pătrunde în sisteme aparent bine protejate. Aceștia exploatează vulnerabilitățile din infrastructura IT&C, adesea prin combinarea mai multor tehnici și vulnerabilități în atacuri coordonate și foarte bine țintite. În plus, utilizarea inteligenței artificiale și a automatizării de către atacatori îi ajută să deruleze atacuri mai complexe și să identifice rapid vulnerabilitățile exploatabile.

Impactul atacurilor cibernetice asupra organizațiilor și societăților poate fi devastator. Daunele financiare rezultate din atacuri pot atinge sume foarte mari, mai ales ca urmare a pierderilor operaționale sau legale ulterioare. Întreruperea operațiunilor poate afecta serviciile critice și infrastructura esențială, de la sănătate publică până la aprovizionarea cu energie.

Pierderea reputaționale și de încredere pot avea efecte de lungă durată asupra organizațiilor, în timp ce riscurile pentru securitatea națională sunt evidente, atacurile cibernetice putând perturba comunicațiile, sistemele de apărare și chiar integritatea proceselor electorale.

În fața acestui peisaj complex și în continuă schimbare, colaborarea internațională, schimbul de date și informații între sectoarele public și privat, precum și investițiile în tehnologii avansate de protecție și în resurse umane specializate sunt esențiale pentru contracararea amenințărilor tot mai sofisticate.

Noile tehnologii, deși oferă oportunități transformative pentru organizații și societate, prezintă vulnerabilități și riscuri specifice. Ele modelează amenințările cibernetice emergente și ridică întrebări complexe din punct de vedere legal și etic.

Tehnologiile emergente, datorită naturii lor inovatoare și adoptării rapide, pot prezenta riscuri de securitate neașteptate. De exemplu, dispozitivele Internet of Things (IoT) sunt adesea criticate pentru standardele lor de securitate insuficiente, oferind atacatorilor cibernetici numeroase oportunități de intrare în rețele și sisteme.

Inteligența artificială (AI) și Machine Learning (ML) pot fi manipulate sau folosite pentru a dezvolta atacuri cibernetice sofisticate, cum ar fi crearea de phishing personalizat extrem de convingător sau identificarea automată a vulnerabilităților în software.

Utilizarea AI și ML de către atacatori reprezintă o amenințare emergentă majoră, capabilă să automatizeze și să optimizeze atacurile cibernetice. În plus, IoT extinde suprafața de atac, în timp ce sistemele de cloud computing și blockchain, deși concepute pentru mai multă securitate, sunt supuse unor tipuri noi de atacuri specifice, cum ar fi atacurile laterale în cloud sau atacurile în blockchain.

Tehnologii emergente

- **Inteligența Artificială (AI)** și **Machine Learning (ML)**: Aceste tehnologii pot îmbunătăți semnificativ detectarea amenințărilor și răspunsul la incidente prin identificarea modelelor care ar putea indica activități malitioase. Totuși, ele pot fi, de asemenea, folosite pentru a dezvolta atacuri mai sofisticate și personalizate.
- **Internetul Lucrurilor (IoT)**: Extinderea IoT crește complexitatea rețelelor și numărul de dispozitive vulnerabile. Gestionarea securității acestor dispozitive diverse este o provocare majoră.
- **Blockchain**: Deși oferă o securitate îmbunătățită prin transparența și imutabilitatea sa, blockchain-ul poate fi vulnerabil la atacuri specifice, cum ar fi cele de tip 51%.

- **Cloud Computing**: Cloudul oferă flexibilitate și eficiență, dar adaugă complexitate în gestionarea datelor și a accesului, necesitând strategii de securitate robuste.
- **Robotic Process Automation (RPA)**: Automatizarea proceselor poate eficientiza operațiunile, dar trebuie securizată corespunzător pentru a preveni abuzurile.
- **Biometrie**: Îmbunătățește securitatea prin autentificare unică, dar stocarea și gestionarea sigură a datelor biometrice sunt esențiale pentru protecția intimității.

Soluții inovatoare de securitate cibernetică

În contextul actual, organizațiile trebuie să implementeze soluții inovatoare pentru a îmbunătăți managementul securității. Adoptarea unor strategii proactive și adaptabile este crucială pentru a răspunde eficient la aceste provocări. Câteva dintre cele mai promițătoare direcții în domeniul securității cibernetice a organizațiilor:

Arhitecturile de securitate de tip „Zero Trust"
Principiul de bază al arhitecturii Zero Trust este „niciodată să nu ai încredere, întotdeauna să verifici". Acest model presupune verificarea constantă a tuturor utilizatorilor și dispozitivelor care încearcă să acceseze resursele rețelei, indiferent dacă solicitarea provine din interiorul sau din exteriorul perimetrului de securitate tradițional. Arhitectura Zero Trust minimizează suprafața de atac și limitează mișcarea laterală a atacatorilor în interiorul rețelei, asigurând că accesul este acordat strict pe baza necesității și în conformitate cu politicile de securitate.

Securitatea cibernetică adaptivă
Securitatea cibernetică adaptivă oferă un cadru dinamic, care permite organizațiilor să răspundă rapid la amenințări și să se adapteze la schimbările din peisajul de securitate. Această abordare utilizează tehnologii avansate de analiză și machine learning pentru a analiza comportamentul rețelei și a identifica activitățile suspecte, permitând implementarea de măsuri de securitate personalizate. Prin anticiparea amenințărilor și ajustarea continuă a posturii de securitate, organizațiile pot reduce riscul de incidente de securitate.

Automatizarea cecurității cibernetice
Automatizarea proceselor de securitate este esențială pentru gestionarea eficientă a numărului mare de alerte de securitate și a volumului crescut de date de securitate. Soluțiile de automatizare permit echipei de securitate să se concentreze pe amenințările care necesită intervenție umană, în timp ce sarcinile repetitive și analiza inițială sunt preluate de sisteme automate. Automatizarea poate îmbunătăți timpul de răspuns la incidente și eficiența generală a operațiunilor de securitate.

Threat Intelligence
Este esențial pentru înțelegerea peisajului de amenințări și pentru anticiparea atacurilor potențiale. Colectarea și analiza datelor despre tactici, tehnici și proceduri utilizate de adversari permit organizațiilor să își adapteze strategiile de securitate și să implementeze măsuri de protecție specifice. Integrarea threat intelligence-ului în procesele de securitate ajută la identificarea proactivă a riscurilor și la prioritizarea răspunsurilor la incidente.

Managementul identității și accesului (IAM)
Sistemele de management al identității și accesului sunt fundamentale pentru controlul accesului la resursele IT&C. Prin implementarea politicilor stricte de IAM, organizațiile pot asigura că doar utilizatorii autorizați au acces la informațiile și sistemele critice. Soluțiile IAM moderne oferă funcționalități avansate, cum ar fi autentificarea multi-factor, gestionarea privilegiilor de acces și integrarea cu sisteme externe de identitate, contribuind la consolidarea securității și la reducerea riscului de acces neautorizat.

Deception cybersecurity
Aceste tehnologii implică crearea deliberată de sisteme, aplicații sau date false (decoys) pentru a induce în eroare atacatorii și pentru a-i devia de la țintele reale. Această metodologie se bazează pe principiul că, prin oferirea unor ținte false atractive, atacatorii pot fi detectați și izolați în timp ce încearcă să interacționeze cu aceste resurse false. Aceste tehnici de înșelăciune pot include honeypots (capcane), care sunt sisteme sau rețele aparent vulnerabile menite să atragă atacatorii, și honeytokens, care sunt date false inserate într-o bază de date sau un sistem de fișiere. Avantajul acestei abordări este că oferă informații valoroase despre metodele și intențiile atacatorilor, permițând organizațiilor să își îmbunătățească continuu strategiile de securitate.

Implementarea acestor soluții inovatoare în cadrul unei organizații poate duce la o îmbunătățire semnificativă a capacității de a preveni, detecta și răspunde la amenințările cibernetice. Pe măsură ce tehnologia continuă să evolueze, adaptabilitatea și inovația vor rămâne elemente cheie în gestionarea eficientă a securității cibernetice.

Cursul nr. 13

Nevoia de standardizare în magementul securității cibernetice
Creșterea exponențială a amenințărilor cibernetice, care variază de la atacuri de tip phishing și malware până la atacuri sofisticate direcționate, subliniază nevoia imperativă de standardizare în managementul securității sistemelor informatice/ cibernetice.

Standardizarea nu numai că răspunde necesității de a proteja activele digitale ale organizațiilor, dar facilitează și o abordare coerentă și eficientă în managementul riscurilor cibernetice.

Nevoia de standardizare a managementului securității cibernetice în organizații este justificată de:

- **Creșterea complexității riscurilor**: Pe măsură ce tehnologia evoluează, crește complexitatea atacurilor cibernetice. Adversarii profită de vulnerabilitățile tehnologice și umane pentru a pătrunde în sistemele de informații, provocând daune semnificative, de la pierderi financiare până la afectarea reputației. Standardizarea securității cibernetice oferă un cadru prin care organizațiile pot

implementa măsuri de protecție adaptate la nivelul de risc și la tipologia specifică a amenințărilor cu care se confruntă.

- **Lipsa de coerență**: Fără un set comun de standarde, organizațiile pot ajunge să implementeze măsuri de securitate ineficiente sau incoerente, ceea ce le face mai vulnerabile în fața atacurilor cibernetice. Standardizarea introduce un limbaj comun și o înțelegere unificată a celor mai bune practici în domeniul securității cibernetice, facilitând astfel schimbul de informații și colaborarea între entități.
- **Dificultățile de evaluare și comparare**: În absența unui cadru standardizat, este dificil pentru organizații să evalueze și să compare eficacitatea măsurilor de securitate cibernetică. Standardele oferă indicatori de performanță și benchmark-uri care ajută la măsurarea progresului și la identificarea domeniilor care necesită îmbunătățiri.
- **Cerințe legale și de reglementare**: Tot mai multe industrii sunt obligate să respecte anumite standarde de securitate cibernetică. Prin implementarea unor standarde de securitate cibernetică, organizațiile pot asigura conformitatea cu aceste cerințe legale și pot evita sancțiuni potențiale.

Beneficiile standardizării

Standardizarea în managementul securității sistemelor informatice/ cibernetice aduce numeroase beneficii, esențiale pentru sustenabilitatea și succesul organizațiilor. Aceste avantaje nu doar că optimizează procesele de securitate, dar și consolidează relațiile interorganizaționale și întăresc încrederea în rândul partenerilor și clienților. Cele mai semnificative beneficii:

- **Îmbunătățirea securității cibernetice**: Prin adoptarea standardelor recunoscute la nivel internațional, organizațiile pot beneficia de o abordare sistematică și cuprinzătoare a securității cibernetice Standardele oferă un cadru de referință pentru identificarea, evaluarea și gestionarea riscurilor de securitate, asigurând că măsurile de protecție sunt aliniate la cele mai bune practici și la cele mai recente evoluții în domeniul securității cibernetice. Acest lucru nu numai că întărește protecția împotriva atacurilor cibernetice, dar și sporește capacitatea organizațiilor de a răspunde rapid și eficient în cazul unei breșe de securitate.
- **Creșterea eficienței**: Implementarea unui set standardizat de practici de securitate poate duce la optimizarea proceselor, reducerea costurilor operaționale și economisirea timpului. Standardizarea proceselor permite organizațiilor să automatizeze anumite sarcini legate de securitatea cibernetică, reducând astfel efortul manual și posibilitatea erorilor umane. Astfel, organizațiile pot aloca mai eficient bugetul destinat securității cibernetice, concentrându-se pe măsurile care oferă cel mai mare nivel de protecție.
- **Facilitarea cooperării**: Standardele comune în domeniul securității cibernetice facilitează colaborarea și partajarea de date și informații între diferite organizații, private, entități guvernamentale și organizații internaționale. Aceasta este esențială în contextul actual, în care amenințările cibernetice nu cunosc granițe și necesită o reacție coordonată. Prin utilizarea unui limbaj comun și a unor practici standardizate, organizațiile pot colabora mai eficient în identificarea și contracararea amenințărilor cibernetice, contribuind la consolidarea securității cibernetice la nivel global.

- **Creșterea încrederii**: Adoptarea standardelor de securitate cibernetică transmite un mesaj puternic despre angajamentul organizației față de protecția datelor și a informațiilor. Aceasta poate crește încrederea terților, care devin din ce în ce mai conștienți de importanța securității cibernetice. În plus, respectarea standardelor recunoscute poate facilita accesul la noi piețe și poate îmbunătăți competitivitatea organizației, oferindu-i un avantaj distinct în fața concurenților care nu pun un accent similar pe securitatea cibernetică.

Exemple de standarde comune

- **ISO/IEC 27001**: Standardul international pentru sisteme de management al securității informației (SMSI).
- **CIS Critical Security Controls (CIS CSS)**: Set de controale de securitate cibernetică recomandate de Center for Internet Security (CIS).
- **NIST Cybersecurity Framework**: Cadru cuprinzător pentru gestionarea riscurilor cibernetice elaborat de Institutul Național de Standarde și Tehnologie (NIST) din SUA.

Acreditare, evaluare și certificare

Conform OUG 104/2021, DNSC este de a crea și dezvolta cadrul național de certificare în domeniul securității cibernetice, în cooperare cu instituțiile care au competențe și atribuții în domeniu. DNSC îndeplinește „Funcția de autoritate națională de certificare privind securitatea cibernetică” având calitatea de organism național care asigură mecanismele naționale privind evaluarea, certificarea și acreditarea produselor, serviciilor și proceselor în domeniul securității cibernetice, cu următoarele roluri și competențe.

De asemenea, DNSC:

- stabileşte norme, cerinţe tehnice, standarde şi proceduri pentru implementarea Regulamentului (UE) 2019/881
- înfiinţează şi gestionează Registrul Naţional al Activelor, Produselor şi Serviciilor de Securitate Cibernetică (RNAPSSC);
- autorizează laboratoarele civile de testare, evaluare şi certificare a securităţii cibernetice a produselor şi serviciilor care sunt utilizate în cadrul reţelelor şi sistemelor informatice;
- cooperează cu instituţiile naţionale şi internaţionale în domeniul standardizării şi acreditarii produselor, serviciilor şi proceselor în domeniul securităţii cibernetice;
- evaluează, testează şi certifică produse şi servicii de securitate cibernetică, pentru nevoi proprii sau la solicitarea instituţiilor din SNAOPSN şi/sau a Guvernului;
- stabileşte reguli, prescripţii sau caracteristici pentru activităţi sau pentru rezultatele acestora din domeniul securităţii cibernetice, pentru asigurarea unei abordări unitare la nivel naţional în scopul realizării unui nivel ridicat al securităţii cibernetice;
- în colaborare cu organismele specializate, participă la elaborarea, aprobarea şi adoptarea de standarde în domeniul de competenţă, pe care le pune la dispoziţia publicului;

- participă la lucrările comitetelor tehnice naţionale şi internaţionale pentru punerea în aplicare a standardelor şi specificaţiilor tehnice acceptate la nivel internaţional, aplicabile securităţii reţelelor şi a sistemelor informatice, fără a impune sau discrimina în favoarea utilizării unui anumit tip de tehnologie;

Totodată conform art. 18 din OUG 104/2021 privind înființarea DNSC funcționarea laboratoarelor civile autorizate ce efectuează activități de testare, evaluare și certificare a securității cibernetice a produselor și serviciilor care sunt utilizate în cadrul rețelelor și sistemelor informatice este condiționată de obținerea prealabilă a unei autorizații din partea DNSC, cu o perioadă de valabilitate de maxim 3 ani.

DNSC autorizează și gestionează organismele de evaluare a conformității, se ocupă de adoptarea, supravegherea și controlul schemelor europene de certificare implementate, de certificarea produselor, serviciilor și tehnologiilor pentru nivelul de asigurare înalt, precum și de gestionarea certificatelor de securitate cibernetică eliberare pentru nivelul de asigurare comun și substanțial.

Procesul de certificare a securității cibernetice în România implică participarea a două autorități competente la nivel național.

- **RENAR (Asociația de Acreditare din România)**: este unic organism național de acreditare, are rolul de a dezvolta/perfecționa programele de acreditare și de a executa acreditarea organismelor de evaluare a conformității (OEC)
- **DNSC**: are responsabilitatea de a autoriza OEC-urile, notificare și supraveghere a acestora, precum și de gestionare a plângerilor.

Așadar, OEC-urile (entități publice sau private) sunt singurele entități care pot elibera certificate de conformitate pentru produsele și serviciile, inclusiv cele de securitate cibernetică, care sunt utilizate în cadrul rețelelor şi sistemelor informatice.

Regulamentul (UE) 2019/881 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor prevede 3 niveluri de certificare a securității cibernetice (comun, substanțial și înalt) care reflectă gradul de rezistență împotriva incidentelor de securitate cibernetică:

- **Comun (de bază)**: Acest nivel este destinat produselor și serviciilor care necesită un nivel de asigurare minim pentru securitatea cibernetică. Certificarea de nivel "comun" se adresează riscurilor de securitate cibernetică de nivel scăzut și presupune că produsele sau serviciile sunt capabile să reziste la acte de perturbare de nivel scăzut.
- **Substantial**: Nivelul „substantial" oferă un grad mediu de asigurare și este destinat produselor și serviciilor care trebuie să facă față unor riscuri de securitate cibernetică mai serioase. Produsele și serviciile certificate la acest nivel sunt evaluate ca fiind capabile să reziste la atacuri cibernetice sofisticate.
- **Înalt (Ridicat)**: Cel mai înalt nivel de asigurare, este destinat produselor și serviciilor care sunt critice din punct de vedere al securității și care trebuie să reziste la cele mai avansate și persistente atacuri cibernetice. Certificarea de nivel "înalt" presupune că produsele și serviciile pot asigura protecția datelor și serviciilor chiar și în fața unor actori de amenințare foarte capabili.

Sistemele de certificare stabilite sub egida Regulamentului (UE) 2019/881 sunt recunoscute în toate statele membre ale UE, facilitând astfel comerțul transfrontalier al produselor și serviciilor IT&C certificate.

Categoriile de produse, procese și servicii IT&C ce pot intra sub incidența evaluării conformității securității cibernetice, sunt cele de detecție și prevenție, servicii de depunere electronică, servicii de stocare, backup, restaurare centralizată, evaluări de risc și capabilitatea de răspuns a organizațiilor, sisteme de protecție a datelor personale sau critice, servicii tip cloud, echipamente de securitate, servicii de management al echipamentelor IT&C și de securitate.

Exemple de organisme de evaluare a conformității din domeniul IT&C din România:

- SGS România
- TÜV Rheinland România
- Bureau Veritas România

Studiu de caz: CIS Controls (fost Critical Security Controls)

CIS Controls este un standard „de facto", structurat în 18 controale esențiale, reflectând o abordare strategică, operațională și tehnică pentru securitatea cibernetică. Este dezvoltat de Center for Internet Security (CIS), o organizație non-profit cu o reputație globală în domeniul securității cibernetice și este utilizat de organizații din diverse industrii și de toate dimensiunile, inclusiv guverne, companii Fortune 500 și instituții financiare. Totodată, este recomandat de numeroase agenții guvernamentale și organizații de reglementare, inclusiv National Institute of Standards and Technology (NIST) din SUA.

Beneficii ale CIS Controls:

- Este disponibil gratuit, în mai multe limbi, inclusiv română.
- Tratează o gamă largă de aspecte ale securității cibernetice și a demonstrat că reduce semnificativ riscul de atacuri cibernetice și îmbunătățește postura de securitate a organizațiilor.
- Se bazează pe cele mai bune practici din domeniul securității cibernetice și este actualizat periodic pentru a reflecta cele mai recente amenințări și vulnerabilități.
- Oferă o abordare pragmatică și flexibilă care poate fi adaptată la nevoile specifice ale multor organizații.

Cele 18 controale ale CIS Controls sunt:

1. Inventarul și controlul activelor hardware

Ghidează identificarea, urmărirea și gestionarea tuturor dispozitivelor hardware din cadrul organizației, inclusiv dispozitive mobile și IoT.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Dezvoltarea și menținerea unui inventar al activelor** hardware: Organizațiile trebuie să creeze și să actualizeze continuu un inventar al tuturor dispozitivelor hardware care accesează rețeaua. Acest inventar ar trebui să includă detalii precum tipul dispozitivului, proprietarul, funcția și informațiile de rețea.

- **Controlul accesului**: se referă la implementarea de controale de acces pentru a restricționa conectarea la rețeaua organizației doar pentru dispozitivele autorizate prin:
    - Utilizarea autentificării puternice pentru dispozitivele care accesează resurse sensibile.
    - Segmentarea rețelei pentru a izola dispozitivele cu risc ridicat.
    - Monitorizarea rețelei pentru a detecta dispozitivele neautorizate.
- **Managementul vulnerabilităților hardware prin:**
    - Identificarea și remedierea promptă a vulnerabilităților cunoscute din firmware-ul și software-ul dispozitivelor hardware.
    - Implementarea unui proces de patch management pentru a aplica actualizări de securitate la toate dispozitivele.
    - Utilizarea de instrumente automate pentru a scana dispozitivele în căutarea vulnerabilităților.
    -
- Dezafectarea hardware-ului prin:
    - Stabilirea unui proces de dezafectare pentru dispozitivele hardware care nu mai sunt utilizate sau care sunt la sfârșitul duratei de viață.
    - Ștergerea sigură a datelor de pe dispozitivele hardware înainte de a fi eliminate.
    - Asigurarea eliminării responsabile a dispozitivelor hardware

2. Inventarul și controlul activelor software

Justifică necesitatea creării și menținerii unui inventar complet al tuturor aplicațiilor software utilizate în organizație pentru a preveni utilizarea software-ului neautorizat și vulnerabil.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Inventarierea software-ului:** Efectuarea unui inventar complet al tuturor aplicațiilor software utilizate în organizație, respectiv menținerea actualizată a inventarului cu informații detaliate despre fiecare aplicație.
- **Controlul accesului la software** prin:
    - Implementarea de controale de acces pentru a restricționa instalarea și utilizarea software-ului la aplicațiile autorizate.
    - Utilizarea de liste de aprobare pentru a defini software-ul permis în organizație.
    - Implementarea de controale de privilegii pentru a restricționa cine poate instala și modifica software-ul.
- Managementul vulnerabilităților software
    - Identificarea și remedierea promptă a vulnerabilităților cunoscute din software-ul utilizat în organizație.
    - Implementarea unui proces de patch management pentru a aplica actualizări de securitate la toate aplicațiile.
    - Utilizarea de instrumente automate pentru a scana aplicațiile în căutarea vulnerabilităților.
- **Dezafectarea software-ului** prin:
    - Stabilirea unui proces de decommissioning pentru aplicațiile software care nu mai sunt utilizate sau care sunt la sfârșitul duratei de viață.
    - Eliminarea completă a software-ului de pe dispozitivele hardware și din sistemele organizației.

3. Protecția datelor

Se concentrează pe implementarea măsurilor necesare pentru a proteja datele sensibile ale organizației împotriva pierderii, furtului sau accesului neautorizat.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Identificarea și clasificarea datelor** prin:
  - Identificarea tuturor tipurilor de date sensibile din organizație
  - Clasificarea datelor sensibile în funcție de nivelul de risc și de impactul potențial al unei breșe de securitate.
- **Controlul accesului la date** prin:
  - Implementarea de controale de acces bazate pe roluri pentru a restricționa accesul la datele sensibile doar la utilizatorii care au nevoie de ele.
  - Utilizarea autentificării puternice pentru a verifica identitatea utilizatorilor care accesează datele sensibile.
  - Monitorizarea accesului la datele sensibile pentru a detecta activități suspecte.
- **Criptarea datelor** prin:
  - Utilizarea de algoritmi de criptare puternici și a cheilor de criptare gestionate în siguranță.
- **Prevenirea pierderii datelor** prin:
  - Implementarea de controale pentru a preveni pierderea accidentală sau intenționată a datelor sensibile.
  - Utilizarea de soluții de prevenție a pierderii datelor (DLP) pentru a monitoriza și bloca transferul neautorizat de date sensibile.

4. Securizarea hardware și software

Acest control prezintă măsuri pentru configurarea sigură a tuturor sistemelor și aplicațiilor pentru a minimiza vulnerabilitățile lor și pentru a le proteja împotriva atacurilor cibernetice.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Configurare sigură a dispozitivelor**, hardware și software, prin:
  - Implementarea standardelor de configurare sigură pentru toate dispozitivele hardware și pentru toate software din organizație
- **Utilizarea de liste de verificare pentru configurația dispozitivelor**.
- **Managementul vulnerabilităților** prin:
  - Implementarea unui proces de management al vulnerabilităților pentru a identifica și remedia prompt vulnerabilitățile
- **Controlul aplicațiilor** prin:
  - Implementarea de controale pentru a gestiona instalarea și utilizarea aplicațiilor software în organizație.
  - Utilizarea unei liste de aprobare pentru a defini aplicațiile care pot fi instalate pe dispozitivele organizației.
  - Monitorizarea utilizării aplicațiilor pentru a identifica activități suspecte.
- **Controlul dispozitivelor** mobile prin:

    - Implementarea de controale pentru a gestiona dispozitivele mobile utilizate în organizație.
    - Utilizarea de soluții de management organizațional al dispozitivelor mobile (MDM) pentru a configura și securiza dispozitivele mobile.
- **Criptarea datelor stocate pe dispozitivele mobile**
- **Controlul firmware-ului** prin:
    - Menținerea actualizată a firmware-ului dispozitivelor hardware din organizație cu cele mai recente patch-uri de securitate.
    - Utilizarea de soluții de gestionare a firmware-ului pentru a automatiza actualizarea firmware-ului.
- **Securitatea configurărilor** prin:
    - Implementarea de controale pentru a gestiona configurările dispozitivelor hardware și a aplicațiilor software din organizație.
    - Utilizarea de soluții de gestionare a configurației pentru a automatiza configurarea dispozitivelor și a aplicațiilor.
    - Implementarea de controale pentru a menține configurația sigură a dispozitivelor și a aplicațiilor.

5. Administrarea conturilor

Acest control prezintă măsurile necesare pentru a gestiona autorizarea acreditărilor pentru conturile de utilizator, inclusiv conturile de administrator, precum și pentru conturile de serviciu din cadrulș organizației.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Stabilirea și menținerea unui inventar al conturilor**
- **Dezactivarea conturile inactive**
- **Restricționarea privilegiilor de administrator la conturi dedicate**
- **Stabilirea și menținerea unui inventar al conturilor de serviciu**
- **Centralizarea managementului conturilor prin:**
    - Folosirea unui serviciu specializat pentru gestionarea conturilor

6. Controlul accesului

Acest control prezintă implementarea politicilor și procedurilor pentru controlul accesului la resursele organizației, având la bază pe principiul celor mai restrictive drepturi.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Standardizarea acordării a accesului prin:**
    - Implementarea unui proces automatizat (dacă este posibil) pentru a acorda acces utilizatorilor la active. Acest proces ar trebui să definească cine poate acorda acces, ce nivel de acces este necesar pentru fiecare rol și pentru modul în care se acordă accesul.
- **Standardizarea revocării accesului** prin:
    - Implementarea unui proces automatizat (dacă este posibil) pentru a revoca accesul utilizatorilor la active atunci când sunt concediați, li se revocă drepturile sau li se schimbă rolul. Acest proces ar trebui să includă dezactivarea conturilor de utilizator în loc de ștergerea lor pentru a păstra logurile pentru auditarea ulterioară.

- **Implementarea MFA**
- **Stabilirea și menținerea unui inventar al sistemelor de autentificare și autorizare**
    - Crearea și actualizarea periodică (cel puțin anual) a listei cu toate sistemele de autentificare și autorizare utilizate de organizație, inclusiv cele găzduite intern sau la un furnizor extern.
- **Centralizarea controlului accesului prin:**
    - Utilizarea unui serviciu de director sau un furnizor specializat pentru a gestiona centralizat accesul utilizatorilor la toate activele organizației.
- **Implementarea accesului bazat pe roluri (RBAC)** prin:
    - Definirea și documentarea permisiunilor de acces necesare fiecărui rol din organizație pentru a-și îndeplini sarcinile.
    - Efectuarea periodică (cel puțin anual) de verificări ale controlului accesului pentru toate privilegiile autorizate.

7. Gestionarea continuă a vulnerabilităților

Acest control prezintă măsurile pentru gestionarea vulnerabilităților din sistemele și aplicațiile organizației în mod regulat, pentru a reduce riscul de exploatare neautorizată.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Stabilirea și menținerea unui proces de management al vulnerabilităților** prin:
    - Dezvoltarea și implementarea unui proces pentru identificarea, evaluarea și remedierea vulnerabilităților din activele organizației.
    - Actualizarea periodică a acestuia (anual sau când apar schimbări semnificative).
- **Stabilirea și implementarea unui proces de remediere a vulnerabilităților** prin:
    - Implementarea unei strategii de remediere a vulnerabilităților bazată pe evaluări de risc care se va revizui lunar sau mai des.
- **Implementarea și gestionarea automată a patch-urilor pentru sistemele de operare și pentru aplicații**
- **Efectuarea de scanări automate** de vulnerabilitate pentru activele interne și pentru cele expuse extern
- **Remedierea vulnerabilităților detectate** lunar sau mai des, pe baza procesului de remediere.

8. Gestionarea log-urilor/ jurnalelor de audit

Acest control prezintă măsurile necesare pentru colectarea, analizarea și stocarea în siguranță a logurilor de sistem pentru detectarea activităților suspecte și investigarea incidentelor de securitate.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Stabilirea și menținerea unui proces standardizat de management al logurilor**
- **Jurnalizarea activităților** prin:

    - Activarea înregistrării activităților pe toate activele organizației, conform procesului de management al jurnalelor de audit. Spațiul de stocare pentru jurnalele de audit trebuie să fie suficient pentru a respecta procesul de management al jurnalelor de audit.
- **Colectarea jurnalelor de audit detaliate**
    - Jurnalele detaliate trebuie să includă sursa evenimentului, data, utilizatorul, ora, adresele sursă și destinație și alte elemente utile pentru investigații ulterioare.
- **Centralizarea jurnalelor de audit** prin:
    - Centralizarea colectării și stocării jurnalelor de audit pentru toate activele organizației, în măsura posibilului.
- **Păstrarea și analizarea periodică a jurnalelor de activități** (loguri)

9. Protecția pentru email și browserul web

Standardizează măsurile de securitate necesare pentru a proteja organizația împotriva amenințărilor propagate prin email și web.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Utilizarea doar a browserelor și clienților de e-mail complet compatibili**
    - Se recomandă utilizarea numai a versiunilor recente ale browserelor web și alșe clienților de e-mail.
- **Utilizarea de servicii de filtrare DNS**
    - Implementarea de servicii de filtrare DNS pentru toate activele organizației pentru a bloca accesul la domenii cunoscute ca fiind periculoase.
- **Menținerea și aplicarea de filtre URL**
- **Restricționarea extensiilor de browser inutile sau neautorizate**
- **Implementați DMARC**
    - DMARC este un acronim pentru Domain-based Message Authentication, Reporting and Conformance (Autentificare, Raportare și Conformitate a Mesajelor pe Bază de Domeniu).
    - Pentru a reduce șansa de primi email-uri neautentice sau modificate provenind de la domenii legitime, se recomandă implementarea politicii de verificare DMARC, începând cu implementarea standardelor Sender Policy Framework (SPF) și DomainKeys Identified Mail (DKIM).
- **Utilizarea de servicii de filtrare DNS**
    - Implementarea de servicii de filtrare DNS pentru toate activele organizației pentru a bloca accesul la domenii cunoscute ca fiind periculoase.
    - Blocați tuturor fișierelor suspecte/ periculoase care încearcă să intre în gateway-ul de e-mail al organizației.
- **Restricționarea fișierelor inutile**
- **Securizare antimalware a serverelor de email**

10. Protecția împotriva malware-ului

Acest control se concentrează pe implementarea de măsuri pentru a proteja organizația de atacuri malware prin detectarea, prevenirea și eliminarea programelor malware periculoase.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Implementați soluțiilor anti-malware** prin:
  - Instalarea și actualizarea periodică antimalware pentru toate dispozitivele din organizație.
- **Configurarea actualizărilor automate anti-malware**
- **Dezactivarea rulării automate pentru mediile amovibile** (stick-uri USB, carduri SD etc.)
- **Configurarea scanării automate anti-malware pentru mediile amovibile**
- **Activarea funcțiilor anti-exploit**
  - Acolo unde este posibil, se recomandă activarea funcțiilor anti-exploit, cum ar fi Microsoft Data Execution Prevention (DEP), Windows Defender Exploit Guard (WDEG) sau Apple System Integrity Protection (SIP) Aceste funcții ajută la prevenirea executării codului malițios.
- **Gestionarea centralizată a software-ului anti-malware**
  - Se recomandă utilizarea unei modalități centralizate pentru a gestiona software-ul anti-malware la nivel de organizație, simplificând administrarea și actualizarea acestuia.
- **Utilizarea de software anti-malware bazat pe comportament**
  - Pe lângă software-ul anti-malware tradițional bazat pe semnături, se recomandă utilizarea soluțiilor care analizează comportamentul programelor pentru a detecta malware necunoscut.

11. Recuperarea datelor

Acest control se concentrează pe implementarea unui plan de recuperare a datelor pentru a se asigura că organizația își poate restabili datele în cazul unor evenimente neprevăzute, cum ar fi dezastrele naturale, atacurile cibernetice sau erorile umane.

Principalele măsuri recomandate includ, dar nu se limitează la:

- Stabilirea și menținerea unuiu proces de recuperare a datelor prin:
  - Implementarea unui proces care definește cum se recuperează datele în cazul unui incident. Acesta ar trebui să includă:
    - Ce tipuri de date vor fi recuperate
    - Prioritatea recuperării datelor
    - Cum se păstrează în siguranță backup-urile
- Efectuarea de backup-uri automate prin:
  - Configurarea de backup-uri automate pentru toate datele importante din organizație. Frecvența backup-urilor depinde de importanța datelor. Datele critice ar trebui salvate mai des (de exemplu, zilnic), în timp ce datele mai puțin sensibile pot fi salvate săptămânal.
- Implementarea unor măsuri de protejare a datelor din backup\
  - Se recomandă aplicarea unor măsuri de securitate pentru backup-uri cel puțin la fel de stricte ca cele aplicate datelor originale.
- Implementarea unor locații separate față de datele originale pentru datele in backup

    - Se recomandă păstrarea copiilor de rezervă într-o locație separată de datele originale pentru a minimiza riscul ca ambele seturi de date să fie pierdute în același timp.
- Testarea periodică a recuperării datelor
    - Se recomandă testarea periodică a procesului de recuperare a datelor pentru a vă asigura că acesta funcționează corect.
    - Se recomandă testarea recuperării datelor dintr-un eșantion de seturi de date critice trimestrial sau mai des.

12. Administrarea rețelei

Acest control vizează implementarea de controale pentru securizarea rețelei organizației pe principiul segmentării rețelei pentru a limita răspândirea atacurilor.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Menținerea infrastructurii de rețea actualizate** prin:
    - Aplicarea celor mai recente actualizări de software și firmware pentru dispozitivele din rețea.
- **Stabilirea și menținerea unei arhitecturi sigure de rețea** prin:
    - Segmentarea rețelei pentru a limita impactul unui atac, implementarea principiului privilegiului minim
- **Gestionarea în siguranță a infrastructurii de** rețea prin:
    - Folosirea de protocoale sigure de management al rețelei (SSH, HTTPS)
- **Actualizarea diagramelor de arhitectură**
    - Se recomandă documentarea topologiei rețelei și actualizarea periodică a acesteia sau când apar modificări majore.
- **Centralizarea AAA (Autentificare, Autorizare și Audit)**
    - Se recomandă utilizarea unui sistem centralizat pentru gestionarea utilizatorilor, permisiunilor și monitorizarea activității din rețea.
- **Folosirea de protocoale sigure de comunicații**
    - Se recomandă implementarea 802.1X pentru rețelele cu fir și WPA2 Enterprise sau o versiune superioară pentru Wi-Fi.
- **Utilizarea VPN**
    - Se recomandă ca utilizatorii de pe dispozitive remote să se autentifice printr-un VPN înainte de a accesa resursele organizației.
- **Segregarea dispozitivelor de rețea**
    - Se recomand dispozitive separate fizic sau logic pentru sarcinile de lucru care necesită privilegii sporite. Aceste dispozitive nu trebuie să aibă acces direct la internet.

13. Monitorizarea și protecția rețelei

Acest control standardizează monitorizarea continuă a traficului de rețea pentru a detecta și răspunde rapid la activitățile suspecte sau rău intenționate.

Amenințările cibernetice devin din ce in ce mai sofisticate, iar simpla implementare a unor tehnologii de securitate nu este suficientă. Este esențial să aveți o echipă calificată care să analizeze datele colectate și să răspundă la incidente.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Centralizarea alertelor de securitate** prin:
  - Utilizarea unui SIEM (Security Information and Event Management) pentru a colecta și analiza datele din evenimentele de securitate.
- **Implementarea unui sistem de detecție a intruziunilor** pe dispozitive (Host-Based Intrusion Detection Solution).
  - Acest sistem monitorizează activitatea pe dispozitive individuale pentru a detecta comportamente suspecte.
- **Implementarea unui sistem de detecție a intruziunilor în rețea** (Network Intrusion Detection Solution).
  - Acest sistem monitorizează traficul din rețea pentru a detecta activități malițioase.
- **Filtrarea traficului între segmentele rețelei**
  - Segmentarea rețelei limitează pagubele pe care le poate produce un atac.
- **Gestionarea controlul accesului pentru dispozitivele remote**
  - Se recomandă acordarea accesului la resursele rețelei doar dispozitivelor care îndeplinesc criteriile de securitate stabilite.
- **Colectarea logurilor de trafic de rețea**
  - Se recomandă monitorizarea traficului din rețea pentru a identifica activități suspecte.
- **Implementarea unui sistem de prevenție a intruziunilor pe dispozitive și în rețea** (Host-Based Intrusion Prevention Solution, Network Intrusion Prevention Solution).
  - Aceste sisteme blochează tentativele de intruziune în rețea și pe dispozitive
- **Implementarea controlului accesului la nivel de port**
  - Se recomandă restricționarea accesului la rețea doar la porturile necesare.
- **Filtrați traficului la nivel de aplicație** prin:
  - Blocarea aplicațiilor sau traficului nedorite.
- **Reglarea periodică a pragurilor de alertă pentru evenimente de securitate**

14. Educație și formare

Acest control subliniază importanța implementării unui program de instruire privind conștientizarea securității pentru angajați. Un program eficient îi ajută pe angajați să identifice amenințările cibernetice și să ia măsuri pentru a le proteja pe cele mai importante resurse ale organizației.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Stabilirea și menținerea unui program de conștientizare a securității** prin:
  - Organizarea de sesiuni de instruire cel puțin o dată pe an, la angajare și ori de câte ori apar modificări majore în organizație.
- **Instruirea angajaților să recunoască atacurile de tip inginerie socială**
- **Instruirea angajaților cu privire la cele mai bune practici de autentificare**
- **Instruirea angajaților cu privire la cele mai bune practici de gestionare a datelor**

    - Privind metodele de identificare, stocare sigură, transfer, arhivare și distrugere a datelor confidențiale.
- **Instruirea angajaților cu privire la cauzele expunerii accidentale a datelor**
    - Privind transmiterea datelor confidențiale, pierderea dispozitivelor sau publicarea datelor către destinatari neintenționați.
- **Instruirea angajaților să recunoască și să raporteze incidentele de securitate**
    - Privind principalele metode de identificare a potențialelor incidente și modalități de raportare a acestora.
- **Instruirea angajaților să identifice și să raporteze actualizările de securitate lipsă**
    - Privind principalele metode de verificare a actualizărilor de software și raportare a problemelor către departamentul IT.
- **Instruirea angajaților cu privire la pericolele conectării la rețele nesigure**
    - Privind riscurile utilizării rețelelor publice pentru activități profesionale.
- **Organizarea de sesiuni de instruire specifice rolurilor din organizație**

15. Gestionarea furnizorilor de servicii

Acest control se concentrează pe dezvoltarea unui proces de evaluare a furnizorilor de servicii care dețin date confidențiale sau sunt responsabili pentru platformele sau procesele IT critice ale organizației, pentru a vă asigura că aceștia își protejează corespunzător platformele și datele respective.

Obiective:

- Evaluarea furnizorilor terți care dețin date sensibile sau furnizează servicii critice.
- Reducerea riscului de incidente de securitate cibernetică care rezultă din breșe la terți.
- Asigurarea respectării reglementărilor privind securitatea datelor și confidențialitatea.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Stabilirea și menținerea unui inventar al furnizorilor de servicii** prin
    - Elaborarea unei liste a a tuturor furnizorilor cunoscuți, clasificarea acestora și desemnarea unei persoane de contact din cadrul organizației pentru fiecare furnizor de servicii.
    - Revizuirea și actualizarea anuală sau când apar modificări semnificative în organizație a acestei liste
- **Stabilirea și menținerea unei politici de management al furnizorilor de servicii**
    - Asigurați-vă că politica abordează clasificarea, inventarul, evaluarea, monitorizarea și scoaterea din uz a furnizorilor de servicii.
    - Revizuiți și actualizați politica anual sau când apar modificări semnificative în organizație care ar putea afecta această măsură de protecție.
- **Clasificarea furnizorilor de servicii**

    - Clasificați furnizorii de servicii în funcție de sensibilitatea datelor, volumul de date, cerințele de disponibilitate, reglementările aplicabile, riscurile de securitate.
      Actualizați și revizuiți clasificările anual sau când apar modificări semnificative în organizație care ar putea afecta această măsură de protecție.
- **Evaluarea periodică a furnizorilor de servicii**
    - Evaluați furnizorii de servicii conform politicii de management al furnizorilor de servicii a organizației. Scopul evaluării poate varia în funcție de clasificare și poate include revizuirea rapoartelor de evaluare standardizate, chestionare personalizate sau alte procese suficient de riguroase.
    - Reevaluați furnizorii de servicii anual, cel puțin, sau odată cu contractele noi și reînnoite.
- **Monitorizarea furnizorilor de servicii**
    - Monitorizați furnizorii de servicii conform politicii de management al furnizorilor de servicii a organizației. Monitorizarea poate include reevaluarea periodică a respectării de către furnizorul de servicii, monitor

16. Securitatea aplicațiilor

Acest control se concentrează pe gestionarea ciclului de viață al securității aplicațiilor dezvoltate intern, găzduite sau achiziționate pentru a preveni, detecta și remedia vulnerabilitățile de securitate înainte ca acestea să afecteze organizația.

Obiective:

- Gestionarea ciclului de viață al securității aplicațiilor pentru a identifica și remedia vulnerabilitățile.
- Dezvoltarea aplicațiilor securizate care minimizează riscul de compromise a datelor.
- Asigurarea respectării reglementărilor privind protecția datelor.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Stabilirea și menținerea unui proces sigur de dezvoltare a aplicațiilor** prin:
    - Standardele de proiectare sigură a aplicațiilor, practici de codare sigură, instruirea dezvoltatorilor, gestionarea vulnerabilităților, securitatea codului terță parte și proceduri de testare a securității aplicațiilor.
- **Stabilirea și menținerea unui proces de acceptare și abordare a vulnerabilităților software**
    - Procesul trebuie să includă elemente precum o politică de gestionare a vulnerabilităților care identifică procesul de raportare, persoana responsabilă cu gestionarea raportărilor vulnerabilităților și un proces de primire, atribuire, remediere și testare a remedierii.
- **Realizarea analizei cauzelor fundamentale ale vulnerabilităților de securitate**
    - Pentru vulnerabilitățile de securitate, analiza cauzelor fundamentale reprezintă evaluarea problemelor care creează vulnerabilități în cod și

permite echipelor de dezvoltare să meargă mai departe de simpla remediere a vulnerabilităților individuale pe măsură ce apar.

- **Stabilirea și gestionarea unui inventar al componentelor software terțe**
  - Acest inventar trebuie să includă orice riscuri pe care le-ar putea prezenta fiecare componentă terță parte. Evaluați lista cel puțin lunar pentru a identifica orice modificări sau actualizări ale acestor componente și pentru a valida faptul că acestea sunt încă acceptate.
- **Utilizarea de software terțe actualizate și de încredere**

17. Răspunsul la incidente

Acest control tratează dezvoltarea și menținerea unei capacități de răspuns la incidente pentru a pregăti, detecta și răspunde rapid unui atac cibernetic.

O capabilitate adecvată de răspuns la incidente de securitate cibernetică include mijloace de protecție, detecție, răspuns și recuperare în cazul unui incident de securitate cibernetică. Scopul principal al răspunsului la incidente este de a identifica amenințările la adresa organizației, de a răspunde la acestea înainte ca ele să se poată propaga și de a le remedia înainte ca acestea să poată provoca daune.

Timpul de reacție de la momentul producerii unui atac până la identificarea lui poate fi de zile, săptămâni sau luni. Cu cât atacatorul este prezent mai mult în infrastructura organizației, cu atât devine mai integrat și va dezvolta mai multe metode de a menține accesul persistent pentru momentul în care va fi în cele din urmă descoperit.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Desemnarea personalului pentru gestionarea incidentelor** –
  - Este esențial să se desemneze o persoană cheie, precum și cel puțin un înlocuitor, responsabili cu gestionarea procesului de gestionare a incidentelor în cadrul organizației. Acest personal poate fi alcătuit din angajați interni, furnizori terți, sau o ambele. În cazul utilizării unui furnizor terț, este indicat să se desemneze cel puțin o persoană din cadrul organizației pentru a supraveghea munca terților.
- **Stabilirea și menținerea informațiilor de contact pentru raportarea incidentelor de securitate**
  - Trebuie stabilite și revizuite periodic informațiile de contact pentru părțile care trebuie informate despre incidentele de securitate.
- **Stabilirea și menținerea unui flux de lucru clar la nivelul organizației pentru raportarea incidentelor**
  - Este crucial să se stabilească și să se mențină acest flux pentru raportarea incidentelor de securitate. Fluxul include termenele de raportare, personalul căruia trebuie să i se raporteze, mecanismul de raportare și informațiile minime care trebuie raportate. Procesul trebuie să fie accesibil public pentru toți cei din organizație și revizuit anual sau când au loc schimbări semnificative în cadrul organizației.
- **Stabilirea și menținerea unui proces de răspuns la incidente** - Este important să se stabilească și să se mențină un proces de răspuns la incidente care să abordeze rolurile și responsabilitățile, cerințele de conformitate și un plan de comunicare. Acest proces trebuie revizuit anual sau la schimbări semnificative în cadrul întreprinderii.

- **Atribuirea rolurilor și responsabilităților cheie**
  - Trebuie atribuite roluri și responsabilități cheie pentru răspunsul la incidente, incluzând personalul din departamente precum juridic, IT, securitatea informațiilor, management logistic și de securitate, relații publice, resurse umane, conformitate, după caz.
  - Revizuirea acestor atribuiri se face anual sau la schimbări semnificative.
- **Definirea mecanismelor de comunicare în timpul răspunsului la incidente**
  - Se recomandă stabilirea unor mecanismele primare și secundare care vor fi folosite pentru comunicare și raportare în timpul unui incident de securitate, având în vedere că anumite mecanisme, cum ar fi e-mailurile, pot fi afectate în timpul unui incident de securitate.
- **Desfășurarea exercițiilor regulate de răspuns la incidente**
  - Se recomandă planificarea și desfășurarea exercițiilor regulate de răspuns la incidente și „jucarea" de scenarii pentru personalul cheie implicat în procesul de răspuns la incidente.
- **Stabilirea și menținerea pragurilor de alertă pentru incidentele de securitate**
  - Este vital să se stabilească și să se mențină praguri de alertă pentru incidentele de securitate, incluzând, la minimum, diferențierea între un (1) eveniment, (2) incident și (3) atac cibernetic. Revizuirea acestor praguri se va face anual sau la schimbări semnificative în cadrul organizației.

18. Testarea de penetrare

Acest control se concentrează pe efectuarea de teste atacuri cibernetice simulate asupra sistemelor și rețelelor organizației, pentru a identifica și remedia vulnerabilitățile înainte ca acestea să fie exploatate de atacatori. Testarea penetrării este o tehnică de evaluare a securității cibernetice prin care se imită atacurile cibernetice asupra unor rețele, aplicații web, interfețe și/sau sisteme din cadrul unei organizații.

Principalele măsuri recomandate includ, dar nu se limitează la:

- **Stabilirea și menținerea unui program de testare a penetrării**
  - Acesta trebuie să fie Adaptat dimensiunii, complexității și maturității organizației.
- **Efectuarea periodică teste externe de penetrare** pentru a identifica vulnerabilitățile din rețeaua externă a organizației.
- **Remedierea vulnerabilităților identificate** în urma testelor de penetrare conform politicii de securitate a organizației
- **Validarea măsurilor de securitate după fiecare test de penetrare**
- **Efectuarea periodică teste interne de penetrare** pentru a evalua securitatea rețelei interne.

Atenție:

- Testarea penetrării poate fi o activitate ilegală dacă nu este autorizată de proprietarul sistemelor și aplicațiilor testate.
- Este important să fie respectate legile și reglementările aplicabile când sunt efectuate teste de penetrare.

Exemple de tool-uri comune pentru testele de penetrare:

- **Scanare de vulnerabilități**:
  - Nmap: Un scanner de porturi și rețea foarte popular și versatil.
  - Nessus: Un scanner de vulnerabilități cu o interfață grafică ușor de utilizat.
  - OpenVAS: Un scanner de vulnerabilități open-source cu o gamă largă de pluginuri.
- **Scanere de vulnerabilități**:
  - Metasploit: Un framework open-source cu o gamă largă de module pentru exploatarea vulnerabilităților.
- **Analiza traficului**:
  - Wireshark: Un sniffer de rețea popular pentru capturarea și analiza traficului de rețea.

De reținut: Cele 18 controale ale CIS Controls oferă o abordare holistică a securității cibernetice, acoperind aspectele cele mai vitale pentru o organizație. Fiecare dintre cele 18 controale din CIS Controls conține măsuri specifice ce au rolul de a oferi o orientare cu privire la implementarea a controalelor.