Co-funded by the Erasmus+ Programme of the European Union

Module de instruire InCyT

Securitatea informațiilor pentru manageri **Unitatea 2 Săptămâna 4** **Denumirea unității: Managementul securității informațiilor-2**	
Activități de învățare	❑ **Webinar** ❑ **Exerciții** ❑ **Workshop** ❑ **Prezentare** ❑ **Alte** Streaming webinar, text, exerciții de autoevaluare, exerciții cu răspunsuri pe forumuri de discuții și să fie discutate cu trainerul/mentorul
Responsabil de învățare	• Fatma Gökdemir • Ali Gökdemir
Obiectivele activității de învățare	1. Evaluarea amenințărilor și vulnerabilității 2. Managementul amenințărilor și vulnerabilităților 3. Tipuri de evaluare a vulnerabilității 4. Continuitatea cibernetică a operațiunilor 5. Cyber Asset 6. Evaluarea eficacității politicilor de securitate cibernetică
Abilități de dobândit	• IS 1 • IS 3 • MS 5
Durata activității de învățare	2 săptămâni
Cerințe de învățare	***Ce e necesar?*** • Cunoștințe medii de utilizare a calculatorului

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Informații scurte despre modul

Descriere
Managementul activelor ocupă un loc important în domeniul de aplicare al Sistemului de Management al Securității Informaționale ISO 27001. De fapt, identificarea și clasificarea activelor informaționale este unul dintre primii pași ai securității informațiilor. Identificarea și atribuirea valorii activelor dintr-o organizație este un pas fundamental în procesul de analiză a riscurilor. Un inventar al activelor este pregătit pentru a atribui valoare activelor. Un studiu exploratoriu care să acopere toți angajații trebuie efectuat înainte de inventarierea activelor. Cu acest studiu, inventarul de active al departamentului este explorat și listat cu posibilele riscuri și gradul de confidențialitate. Inventarul activelor ar trebui făcut unul câte unul pe baza proceselor acoperite. În timpul pregătirii inventarului bunurilor; grupul de active, mediul în care se află activul specificat, se determină codul de clasificare și se calculează valoarea activului (confidențialitate, integritate, accesibilitate). În funcție de rezultatul calculului, se determină statutul de prioritate și se iau decizii de acțiune. După finalizarea lucrărilor de inventariere a activelor, este pregătită o listă de inventar detaliată pentru inventarele software-hardware detectate. Condițiile/controalele privind managementul activelor în standardul ISO27001 sunt adunate în Anexa A.8. În acest modul vom examina termenii pentru răspunderea activelor definiți în A.8.1.

Conținutul materialului de învățare

1. Evaluarea managementului securității informațiilor

În prima etapă a gestionării activelor, ar fi util să dezvăluim mai întâi și să enumeram ce active avem. Ceea ce are sau nu are o instituție trebuie cunoscut mai întâi. Apoi trebuie definită proprietatea lor. Nicio afacere sau tranzacție nu trebuie lăsată nesupravegheată. Apoi, ar trebui stabilite regulile de utilizare a acestor active.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Pentru detaliile subiectului, trebuie examinat standardul ISO27002. Așteptările privind managementul activelor în ISO27002 sunt incluse în articolul 8 al standardului:

Gestionarea activelor și răspunderea pentru active

Scop: Să identifice activele organizației și să definească responsabilitățile de protecție adecvate.

1. Inventarul activelor

Control: Activele legate de informațiile și instalațiile de procesare a informațiilor ar trebui identificate și ar trebui făcut și menținut un inventar al acestor active.

Ghid de aplicare: O organizație ar trebui să identifice activele relevante în ciclul de viață al informațiilor și să documenteze importanța acestora. Ciclul de viață al informațiilor ar trebui să includă crearea, procesarea, stocarea, transmiterea, ștergerea și distrugerea. Documentația trebuie păstrată în conformitate cu inventarele existente sau în mod specific.

Inventarul activelor; trebuie să fie actuale, consecvente, exacte și compatibile cu alte inventare.

Proprietatea activelor ar trebui să fie alocată pentru fiecare activ identificat (a se vedea articolul 2) și clasa acestuia ar trebui determinată.

Alte informații: Inventarul de active ajută la asigurarea unei protecții eficiente și poate fi necesar și în alte scopuri, cum ar fi sănătatea și siguranța, asigurarea sau motivele financiare (gestionarea activelor).

Standardul ISO/IEC 27005[11] oferă exemple de active care ar putea trebui luate în considerare de către organizație la identificarea activelor. Procesul de compilare a unui inventar al activelor este o condiție prealabilă importantă pentru managementul riscului (a se vedea ISO/IEC 27000 și ISO/IEC 27005[11]).

2. Proprietatea asupra activelor

Control: Atribuțiile proprietarilor trebuie făcute pentru toate bunurile deținute în inventar.

Ghid de aplicare: Persoanele fizice și alte entități cu responsabilitate de management aprobată pentru ciclul de viață al activelor sunt eligibile pentru a fi desemnate drept proprietari de active.

Un proces este adesea folosit pentru a se asigura că proprietatea asupra activelor este determinată în timp util. Proprietatea trebuie să fie determinată atunci când activele sunt create sau transferate către organizație. Proprietarul activului ar trebui să fie responsabil pentru gestionarea corectă a activului pe tot parcursul ciclului de viață al acestuia.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Proprietarul bunului:

a) Asigurați-vă că inventarul de active este înregistrat,

b) să se asigure că activele sunt clasificate și protejate în mod corespunzător;

c) să definească și să revizuiască periodic restricțiile privind accesul la activele semnificative și clasificarea acestora, ținând cont de politica de control al accesului aplicabilă;

d) Asigurați-vă că sunt luate măsuri adecvate în ștergerea sau distrugerea activelor.

Alte informații: Poate fi o persoană fizică sau o entitate cu aprobare pentru responsabilitatea conducerii de a controla un activ pe parcursul ciclului său de viață. Proprietarul identificat nu are niciun drept de proprietate asupra activului.

Sarcinile de rutină pot fi delegate; (de exemplu, un custode care are grijă de un bun zilnic), dar responsabilitatea revine proprietarului bunului.

Identificarea grupurilor de active în cadrul sistemelor informaționale complexe poate fi utilă în furnizarea de funcții împreună. În acest caz, acest proprietar al serviciului este responsabil pentru furnizarea serviciului, inclusiv pentru exploatarea activelor.

3. Utilizarea acceptabilă a activelor

Control: Reguli cu privire la utilizarea acceptabilă a informațiilor și a activelor legate de informațiile și instalațiile de procesare a informațiilor ar trebui determinate, documentate și implementate.

Ghid de aplicare: Angajații și utilizatorii externi care utilizează sau au acces la activele organizației trebuie să fie informați cu privire la cerințele de securitate a informațiilor ale activelor organizației asociate cu informațiile și facilitățile și resursele de procesare a informațiilor. Acești utilizatori ar trebui să fie responsabili pentru utilizarea tuturor resurselor de procesare a informațiilor și pentru orice utilizare care are loc pe propria răspundere.

4. Returnarea bunurilor

Control: Toți angajații și utilizatorii părților externe trebuie să returneze toate activele corporative aflate în posesia lor la încetarea angajării, contractului sau acordului..

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Ghid de aplicare: Procesul de reziliere ar trebui să fie formulat astfel încât să includă returnarea dreptului de proprietate asupra tuturor activelor fizice și electronice acordate anterior sau escrows ale organizației.

Atunci când un angajat sau un utilizator extern cumpără sau folosește echipamentul organizației, procedurile sunt urmate pentru a se asigura că toate informațiile relevante sunt transferate organizației și șterse în siguranță din echipament.

În cazul în care un angajat sau un utilizator extern deține informații importante pentru operațiunile în desfășurare, aceste informații trebuie să fie documentate și transferate organizației.

În perioada de preaviz de încetare, organizația; controlează copierea neautorizată a informațiilor conexe, cum ar fi proprietatea intelectuală, de către angajații și contractorii reziliați.

2. Evaluarea și managementul amenințărilor și vulnerabilităților

Aproape fiecare organizație are active sensibile și valoroase care trebuie protejate. Cu toate acestea, nu fiecare organizație are o strategie cuprinzătoare și complet gândită pentru protejarea acestor active. În securitatea cibernetică, strategiile de gestionare a vulnerabilităților reprezintă fundamentul unei apărări puternice. De obicei, strategiile de gestionare a vulnerabilităților sunt concepute pentru a ajuta sistemele, rețelele, aplicațiile etc. ale unei organizații. Adoptă o abordare holistică și continuă pentru gestionarea vulnerabilităților de securitate în Aceste vulnerabilități sunt apoi identificate, evaluate și remediate cât mai curând posibil.

Amenințările și tendințele de securitate evoluează constant, necesitând eforturi eficiente și preventive pentru a gestiona amenințările și vulnerabilitățile care v-ar putea compromite datele. Pentru a identifica toate țintele potențiale pentru o încălcare sau un atac, riscul acestuia trebuie mai întâi atenuat prin efectuarea unui inventar de active. Țintele trebuie apoi clasificate și monitorizate continuu pentru noi vulnerabilități potențiale. Ar trebui apoi dezvoltat și testat un model de amenințare care identifică cele mai valoroase active ale organizației cu risc ridicat. Scopul principal al procesului de testare a amenințărilor și vulnerabilităților (evaluarea) este de a înțelege cel mai bine criticitatea activelor, vulnerabilitățile la aceste active și de a reduce măsurile necesare pentru a proteja eficient aceste active.

2.1. Ce este evaluarea vulnerabilității?

Evaluarea vulnerabilităților este procesul de identificare, identificare, clasificare și prioritizare a vulnerabilităților din sistemele informatice, aplicațiile și infrastructurile de rețea.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Evaluările vulnerabilității oferă, de asemenea, unei organizații cunoștințele, conștientizarea și fundalul riscurilor necesare pentru a înțelege și a răspunde amenințărilor la adresa mediului său. Un proces de evaluare a vulnerabilității are ca scop identificarea amenințărilor și a riscurilor pe care le prezintă. Adesea, acestea implică utilizarea unor instrumente automate de testare, cum ar fi scanere de securitate în rețea, ale căror rezultate sunt enumerate într-un raport de evaluare a vulnerabilităților.

Organizațiile de orice dimensiune, chiar și persoanele cu risc crescut de atacuri cibernetice, pot beneficia de o anumită formă de evaluare a vulnerabilității, dar organizațiile mari și alte tipuri de organizații expuse la atacuri în curs vor beneficia cel mai mult de pe urma analizei vulnerabilității.

Deoarece vulnerabilitățile pot permite hackerilor să obțină acces la sisteme și aplicații IT, este esențial pentru organizații să identifice și să remedieze vulnerabilitățile înainte ca acestea să fie exploatate. O evaluare cuprinzătoare a vulnerabilității combinată cu un program de management poate ajuta companiile să își îmbunătățească securitatea sistemelor.

2.2. Importanța evaluării vulnerabilității

Pentru a clarifica mai bine importanța evaluării vulnerabilității, să o luăm în considerare prin ochii unui proprietar fizic de proprietate. Dacă dețineți o clădire valoroasă, probabil că luați o serie de măsuri pentru ao proteja: o întrețineți, o asigurați și vă asigurați că ușile, ferestrele sunt încuiate și alarmele sunt activate. Toți acești pași pot fi numiți gestionarea riscului asupra proprietății și conținutului acesteia.

Acum ce se întâmplă dacă ai putea angaja pe cineva să testeze și să raporteze alarmele și apărările tale externe? Vulnerabilitățile de securitate cibernetică sunt abordate într-un mod similar. Managementul vulnerabilităților este o strategie generală și continuă, în timp ce evaluările vulnerabilităților sunt un instrument specific utilizat în această strategie de management mai largă.

O evaluare a vulnerabilității oferă unei organizații informații detaliate despre orice deficiențe de securitate din mediul său. De asemenea, oferă instrucțiuni privind modul de evaluare a riscurilor asociate cu aceste deficiențe. Acest proces oferă organizației o mai bună înțelegere a activelor sale, a defectelor de securitate și a riscului general, reducând probabilitatea ca un infractor cibernetic să-și încalce sistemele și să-și surprindă afacerea cu priză..

2.3. Tipuri de evaluare a vulnerabilității

Evaluările vulnerabilităților descoperă diferite vulnerabilități ale sistemului sau ale rețelei. Aceasta înseamnă că procesul de evaluare include utilizarea unei varietăți de instrumente,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

scanere și metodologii pentru a identifica vulnerabilități, amenințări și riscuri.

Unele dintre diferitele tipuri de scanări de evaluare a vulnerabilităților includ (Figura 1):

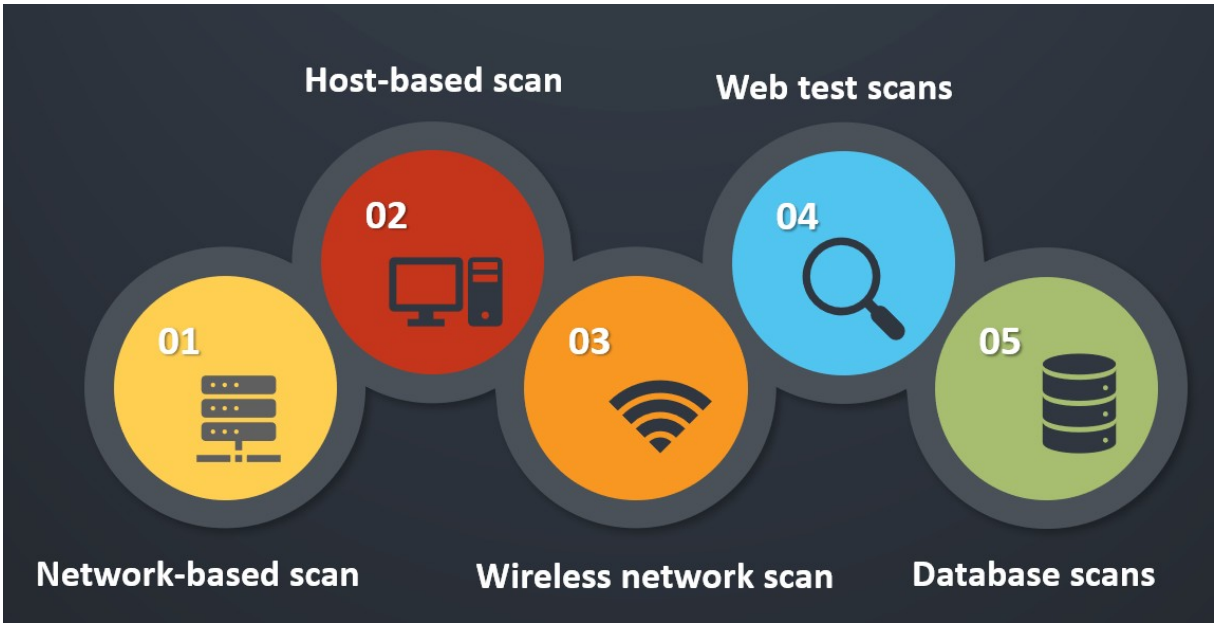

Figura 1. Tipuri de evaluare a vulnerabilității

- **Scanările bazate pe rețea** sunt utilizate pentru a identifica potențialele atacuri la securitatea rețelei. Acest tip de scanare poate detecta și sisteme vulnerabile din rețelele cu fir sau fără fir.
- **Scanările bazate pe gazdă** sunt utilizate pentru a găsi și identifica vulnerabilități în servere, stații de lucru sau alte gazde din rețea. Acest tip de scanare examinează de obicei porturile și serviciile, care pot fi văzute și în scanările bazate pe rețea. Cu toate acestea, oferă o vizibilitate mai mare asupra setărilor de configurare și a istoricului de corecție a sistemelor scanate, inclusiv a sistemelor vechi.
- **Scanările rețelelor wireless** ale rețelelor Wi-Fi ale unei organizații se concentrează adesea pe punctele de atac din infrastructura rețelei fără fir. Pe lângă identificarea punctelor de acces necinstite, scanarea rețelei fără fir poate verifica și dacă rețeaua unei companii este configurată în siguranță.
- **Site-uri de testare** de scanare web pentru a detecta vulnerabilități software cunoscute și configurații greșite în aplicații, rețea sau aplicații web.
- **Scanările** bazelor de date pot identifica punctele slabe dintr-o bază de date pentru a preveni atacurile rău intenționate.Atacuri cu injecție SQL.

2.4. Evaluări de vulnerabilitate și teste de penetrare

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

O evaluare a vulnerabilității include adesea o componentă de testare a pătrunderii pentru a identifica vulnerabilități în personalul, procedurile sau procesele unei organizații. Evaluările vulnerabilităților au multe dintre aceleași caracteristici ca și testele de penetrare, deoarece ambele permit organizațiilor să-și examineze riguros apărările. Este posibil ca aceste vulnerabilități să nu fie detectate în mod normal de scanările rețelei sau ale sistemului. Procesul este uneori denumit evaluarea vulnerabilității/testarea de penetrare sau **VAPT**.

Cu toate acestea, testarea de penetrare nu este suficientă ca evaluare completă a vulnerabilității și este de fapt un proces separat. O evaluare a vulnerabilităților urmărește să descopere vulnerabilitățile dintr-o rețea și să sugereze atenuarea sau remedierea adecvată pentru a atenua sau elimina riscurile.

O evaluare a vulnerabilității folosește instrumente automate de scanare a securității rețelei. Rezultatele sunt enumerate în raportul de evaluare a vulnerabilităților, care se concentrează pe furnizarea organizațiilor cu o listă de vulnerabilități care necesită remediere. Cu toate acestea, face acest lucru fără a evalua ținte sau scenarii specifice de atac.

Organizațiile ar trebui să efectueze în mod regulat teste de vulnerabilitate pentru a asigura securitatea rețelelor lor, în special atunci când se fac modificări. De exemplu, testarea ar trebui făcută atunci când sunt adăugate servicii, sunt instalate echipamente noi sau sunt deschise porturi.

În schimb, testarea de penetrare implică identificarea vulnerabilităților într-o rețea și încercările de a le utiliza pentru a ataca sistemul. Deși uneori efectuată împreună cu evaluările vulnerabilităților, scopul principal al testării de penetrare este de a verifica dacă există într-adevăr o vulnerabilitate. În plus, testarea de penetrare încearcă să demonstreze că exploatarea unei vulnerabilități poate dăuna aplicației sau rețelei.

În timp ce o evaluare a vulnerabilităților este de obicei automatizată pentru a acoperi o mare varietate de vulnerabilități nepatchate, testarea de penetrare combină adesea tehnici automate și manuale, ajutând testerii să investigheze în continuare vulnerabilitățile și să le folosească pentru a obține acces la rețea într-un mediu controlat.

2.5. Managementul vulnerabilităților și managementul riscurilor

În timp ce managementul vulnerabilităților este un proces continuu de gestionare a vulnerabilităților, managementul riscurilor are o viziune mai largă asupra a tot ceea ce poate reprezenta o amenințare pentru o organizație. O strategie solidă de management al riscurilor permite identificarea, analizarea și atenuarea eficientă a riscurilor. Această abordare ajută organizațiile să înțeleagă nu numai vulnerabilitățile care există, ci și amploarea daunelor care

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

pot apărea dacă sunt abuzate. O evaluare a riscurilor și a vulnerabilității efectuată sub umbrela managementului riscului poate oferi o perspectivă deosebit de largă asupra puterii unei poziții de securitate organizațională.

3. Continuitatea operațiunilor cibernetice

Creșterea rezistenței împotriva amenințărilor de malware distructiv necesită o perspectivă asupra poziției actuale de securitate, planificarea și coordonarea acțiunilor defensive cheie și alinierea corectă a resurselor defensive cheie.

Incidentele cibernetice au provocat, de asemenea, eforturile de bază de planificare a continuității. În timp ce multe jurisdicții au echipamente și strategii pentru a identifica, detecta și proteja împotriva atacurilor cibernetice, mult mai puține au lucrat la realitățile dure ale continuității operațiunilor lor printr-un atac real. Când atacurile cibernetice lovesc, multe jurisdicții afectate constată că planurile lor de bază COOP nu rezistă. Deși planurile sunt adecvate pentru tranziția la un loc de muncă alternativ, ele au mult mai puțin de oferit atunci când vine vorba de lucrul fără acces la sistemele și datele necesare personalului pentru a-și îndeplini misiunea esențială. Planurilor existente le lipsește, de asemenea, specificitatea necesară pentru a ghida răspunsul, iar părțile interesate majore, cum ar fi membrii personalului IT, adesea nu sunt integrați în structurile de răspuns. Și planurile nu sunt testate împotriva unui exercițiu sau a unui incident din lumea reală.

Planurile COOP tradiționale sunt insuficiente pentru continuitate în timpul incidentelor cibernetice în mai multe moduri (Figura 2):

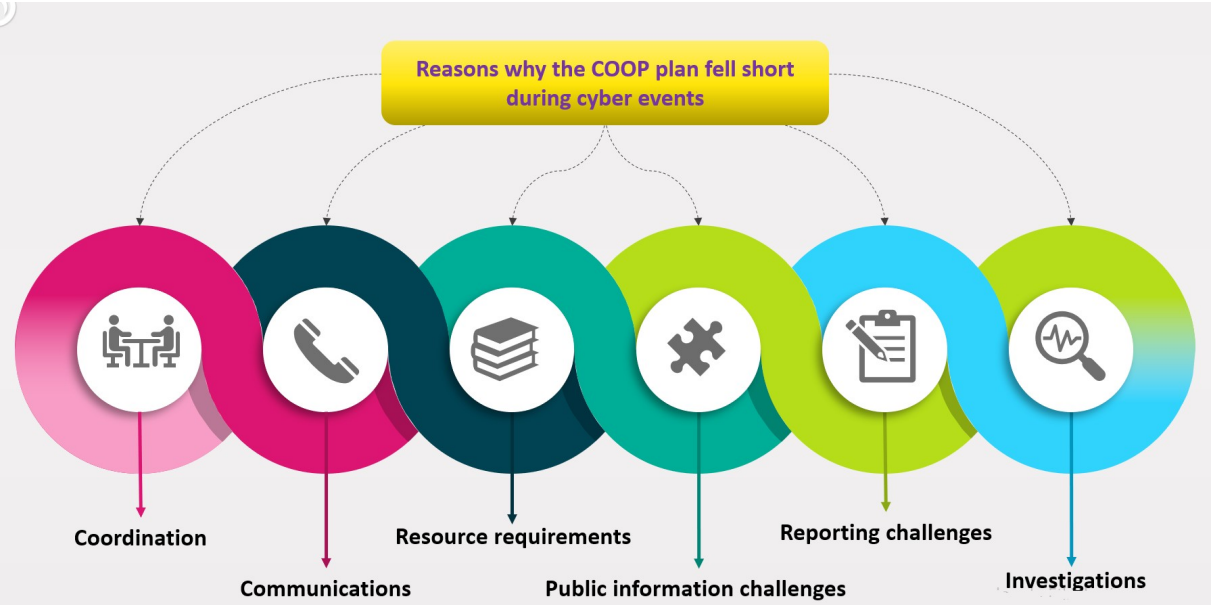

Figura 2. Motive pentru care planurile COOP sunt insuficiente pentru continuitate în timpul

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

evenimentelor cibernetice

Coordonare: inclusiv cine este implicat în luarea deciziilor când vine vorba de ransomware, deciziile de a scoate sistemele offline și deciziile de activare a Centrului de operațiuni de urgență jurisdicțional. În plus, majoritatea guvernelor locale nu au niveluri clare de escaladare pentru un atac și nici elementele de acțiune asociate pentru fiecare nivel. Conducerea de răspuns și personalul pot fi, de asemenea, neclare; tipurile de expertiză în materie necesare pentru a ghida o comunitate printr-un incident cibernetic sunt diferite de cele necesare pentru vreme extremă.

Comunicatii: inclusiv modul în care managerii locali vor furniza rapid informații personalului atunci când un atac cibernetic a compromis sever comunicațiile. Aceasta include atât comunicări imediate care explică ce trebuie făcut când începe atacul, cât și comunicări continue, cum ar fi modul în care salariile vor fi furnizate în ziua de plată. Ambele sunt esențiale pentru răspuns și, totuși, ambele ar trebui să fie transmise fără beneficiul sistemelor tipice de comunicații de urgență.

Cerințe de resurse: Care pot fi foarte diferite de cele pentru un răspuns mai tradițional. De exemplu, personalul ar putea avea nevoie de computere curate, servere curate, imprimante locale și chiar faxuri și hârtie. Este important că cerințele de personal pot crește și mai mult în timpul recuperării decât ca răspuns, deoarece departamentele și agențiile se luptă să reproducă datele lipsă sau suspecte..

Provocări de informare publică: Inclusiv ofițeri de informare publică cu puțină sau deloc pregătire sau experiență în securitate cibernetică, lipsă de mesaje pre-scriptate și dezacord cu privire la momentul în care informațiile despre atac ar trebui făcute publice. Furnizarea de informații către public este esențială, deoarece cetățenii își fac griji pentru datele lor și de încrederea sistemelor democratice cheie, cum ar fi votul și justiția.

Raportarea provocărilor: Acest lucru poate întârzia răspunsul, deoarece întreruperile nu sunt raportate într-un mod consecvent, lăsând departamentele IT fără imaginea operațională comună necesară pentru a identifica rapid un atac. În plus, liniile de raportare sunt adesea neclare și puțini oameni din afara IT înțeleg ce sisteme sunt conectate atât în interiorul, cât și în exteriorul jurisdicției.

Investigatii: Care este o cutie neagră pentru multe localități. Implicarea uneia sau mai multor organizații federale și limitele pe care investigațiile le impun eforturilor de remediere nu sunt bine înțelese sau planificate. Acest lucru face ca planificarea continuității să fie extrem de dificilă, deoarece există incertitudine cu privire la cum și când poate începe chiar remedierea.

3.1. Priorități pentru acțiune imediată cu apărare coordonată

• Dezvoltați un „Go Bag” cibernetic cu proceduri și informații esențiale.
  o Asamblați seturi de instrumente de securitate cibernetică mobilă care includ proceduri

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

pentru stabilirea, implementarea, menținerea și permiterea continuării TTP-urilor rezistente cibernetice într-o unitate desemnată de COOP

• Dezvoltați, testați și validați manuale, roluri, responsabilități și instrumente.

o Desemnați roluri cibernetice specifice, responsabilități asociate și instrumentele cibernetice care pot fi implementate pentru a asigura implementarea COOP cibernetic.

o Definiți jocuri COOP cibernetice standard pentru execuția individuală sau în echipă cibernetică folosind instrumente cibernetice „Go Bag" și TTP-uri elastice.

o Efectuați diferite tipuri de exerciții cibernetice (de exemplu, exerciții de tip mini-masă) folosind „Go Bag" cibernetic și manualul de joc.

• Definiți procesele de colaborare și achiziționați instrumente pentru apărătorii cibernetici și cei care răspund la incident.

o Asigurați-vă că atât procesele COOP cibernetice mobile, cât și cele staționare încorporează comunicarea și coordonarea pentru a promova gestionarea adecvată a apărării cibernetice, sinergia între toate activitățile de răspuns și reducerea decalajelor de acoperire a securității în timpul activităților de recuperare..

În timp ce planurile de bază COOP au sporit pregătirea locală pentru multe dintre amenințările cu care se confruntă jurisdicțiile, acestea nu sunt insuficiente în situațiile care creează un mediu foarte diferit de cel normal. Pe măsură ce departamentele IT din toată țara continuă să asigure sistemele și datele cât mai sigure posibil, este la latitudinea managerilor de urgență să-și dezvolte imaginația și să planifice atacurile cibernetice care afectează serios sistemele și datele critice..

3.2. Priorități pentru acțiune imediată cu realiniere

• Identificați dependențele misiunii și ale funcției de afaceri de resursele cibernetice.

o Determinați scopurile misiunii ale resurselor, astfel încât utilizările care cresc riscul fără niciun beneficiu corespunzător misiunii să poată fi identificate și eliminate.

✓ Identificați și eliminați sau înlocuiți fluxurile de date și conexiunile pentru care riscurile depășesc beneficiile.

o Luați în considerare interdependența dintre și între funcțiile și organizațiile de afaceri din misiune și non-misiune care împărtășesc roluri critice în furnizarea capabilităților NEF.

✓ Realocați resurse sau reatribuiți responsabilitatea administrativă și de management pe baza riscului misiunii și funcției de afaceri.

• Identificați dependențele non-misiunii și ale funcțiilor de afaceri de sau utilizări ale resurselor cibernetice.

o Folosiți analiza fluxului misiunii, analiza dependenței misiunii, exercițiile de pe masă și Red Teaming pentru a descoperi dependențe nedocumentate ale misiunii.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

o Revizuirea și corelarea misiunii și a funcțiilor de afaceri cu cartografierea modelului de dependență și activitățile și rezultatele de analiză a impactului.

o Identificați sistemele, aplicațiile și procesele funcțiilor care nu sunt esențiale pentru misiune și resursele care le susțin.

- ✓ Evaluați aceste funcții în raport cu o strategie fluidă de implementare Cyber COOP pentru a adapta operațiunile prioritare și o mai bună utilizare sau eliminare a dependenței.

4. Gestionarea activelor cibernetice, schimbărilor și configurației

- ✓ **Atu:** Să începem cu definiția unui activ. Definiția din dicționar a unui activ este un lucru sau persoană utilă sau valoroasă. În mod similar, activele unui furnizor de servicii IT sunt instrumentele sale, aplicațiile, elementele de configurare și orice alte elemente valoroase care ajută la furnizarea de servicii clienților sau afacerii. Activele sunt o parte din gestionarea activelor de serviciu și a configurației.
- ✓ **Element de configurare:** Elementul de configurare este abreviat ca CI și un element de configurare este orice componentă care trebuie gestionată pentru a furniza un serviciu IT. Exemple de elemente de configurare sunt serviciile IT, hardware-ul, software-ul, clădirile, oamenii și documentația formală. Deci, pe scurt, orice componentă sau element care ajută la furnizarea unui serviciu IT către client este clasificat ca Element de configurare. Informațiile despre fiecare element de configurare sunt înregistrate într-o înregistrare de configurare în cadrul sistemului de management al configurației și aceste informații sunt menținute pe parcursul ciclului său de viață de către Managementul configurației..
- ✓ **Baza de date de management al configurației:** Baza de date Configuration Management este abreviată ca CMDB. CMDB este o bază de date folosită pentru a stoca înregistrările de configurare pe tot parcursul ciclului de viață. CMDB stochează informații despre CI-urile dvs., fiecare distingându-se printr-un identificator unic, inclusiv informații de identificare precum numărul de serie, adresa MAC sau adresa IP; versiunea sa actuală; amplasarea acestuia; și informațiile despre furnizor și furnizor.
- ✓ **Sistem de management al configurației:** Sistemul de management al configurației este abreviat ca CMS și este un set de instrumente și baze de

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

date care sunt utilizate pentru a gestiona datele de configurare ale unui furnizor de servicii IT. Datele despre elementele de configurare sunt stocate în înregistrările de configurare, iar înregistrările de configurare sunt incluse în bazele de date ale sistemului de management al configurației. CMDB-urile unui furnizor de servicii IT pentru a gestiona datele de configurare sunt incluse în procesul de gestionare a configurației și a activelor serviciului. Sistemul de management al configurației include, de asemenea, informații despre incidente, probleme, erori cunoscute, modificări și versiuni, angajați, furnizori, locații, unități de afaceri, clienți și utilizatori. Pe scurt, toate informațiile necesare despre elementele de configurare și activele IT sunt incluse în Sistemul de management al configurației. Când este necesar, aceste informații sunt achiziționate de la CMS și, respectiv, utilizate.

Managementul configurației, care este definit practic ca procesul de identificare, control, monitorizare și auditare a modificărilor efectuate, este o parte critică a unui program de securitate puternic. Gestionarea schimbărilor și a configurației în cadrul unei organizații are legături puternice cu cerințele de audit în aproape toate cadrele și reglementările de securitate.

Managementul configurației se bazează pe controlul și lansarea diferitelor versiuni de produs. Configurațiile implicite pentru sistemele de operare și aplicații sunt, în general, orientate spre ușurința implementării și utilizării, nu spre cele mai bune practici de securitate cibernetică. Astăzi, managementul configurației este o disciplină solicitată, cu implicații semnificative în domeniul securității cibernetice, mai ales pe măsură ce organizațiile trec de la configurații implicite de tip out-of-box la configurații de aplicații și hardware mai sigure.

Astăzi, managementul configurației înseamnă lucruri diferite pentru diferiți oameni. În unele implementări, se referă la modul în care sunt configurate dispozitivele de rețea. În altele, este vorba despre versiunea unei aplicații pe care o rulează o echipă. Uneori, oamenii din industrie confundă managementul activelor IT cu managementul schimbărilor și al configurației. Deși sunt similare și la fel de importante pentru afacere, nu sunt la fel. Soluțiile de management IT monitorizează, optimizează și gestionează activele pe întregul stil de viață al activelor. Între timp, CM colectează, stochează, gestionează, actualizează și analizează toate elementele de configurare.

Deși multe organizații au programe CM imature, acestea sunt esențiale pentru peisajul modern de securitate cibernetică și vor crește doar în importanță pe măsură ce peisajul amenințărilor continuă să evolueze.

4.1. Managementul configurației și recuperarea în caz de dezastru

Când vine vorba de recuperarea modernă în caz de dezastru, gestionarea configurației este esențială. În cazul unui dezastru de securitate cibernetică, (la urma urmei, 76% dintre organizații au experimentat un incident de securitate cibernetică IoT) poate fi imposibil să reveniți la cea mai recentă configurație dacă nu există documentație privind configurația menționată.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Același lucru este valabil și pentru securitatea cibernetică: este imposibil pentru echipe să știe dacă ceva nu este în regulă dacă nu există o modalitate standardizată de configurare, modificare și documentare a mediului digital.

4.2. Managementul schimbării

Managementul schimbărilor rulează în paralel cu gestionarea configurației, deși cele două lucruri nu sunt la fel. Oamenii le confundă tot timpul.
În timp ce managementul configurației este procesul de identificare și documentare a componentelor hardware și a software-ului și a setărilor asociate, gestionarea modificărilor este o funcție de bază a procesului mai amplu de management al configurației. Managementul schimbărilor se referă la procesele asociate și urmărește să creeze stabilitate în cadrul unui sistem și să prevină schimbările necontrolate sau aleatorii sau să documenteze procesele de schimbare atunci când ai cifra de afaceri în cadrul organizației. Cu alte cuvinte, permite companiilor să planifice schimbarea, mai degrabă decât să reacționeze la ea.

4.2.1. Procesul de management al schimbării

Astăzi, un proces de management al schimbărilor bine structurat va include următoarele:

- Modificarea cererilor trimise
- Evaluări de risc și impact
- Aprobați/respingeți funcțiile de modificare
- Testare
- Funcții de programare/notificare utilizator/instruire
- Implementarea
- Validare
- Documentație

Unul dintre locurile în care gestionarea schimbărilor prosperă este în cazul deciziilor de urgență, când trebuie făcute schimbări. Odată ce modificarea a fost implementată, aceasta ar trebui să fie reintrodusă în procesul de management al schimbării, unde va beneficia apoi de protocoalele de validare și documentare care au fost deja stabilite..

4.3. Managementul activelor de securitate cibernetică

Managementul activelor de securitate cibernetică este procesul de colectare a datelor despre active (dispozitive, instanțe cloud și utilizatori) pentru a consolida funcțiile de bază de securitate, inclusiv:

- **Detectare și răspuns:** asigurarea capacităților de detectare și răspuns oferă acoperire în

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

întreaga întreprindere

- **Managementul vulnerabilităților:** înțelegerea activelor care pot fi vulnerabile la exploatare și asigurarea faptului că toate activele sunt evaluate pentru vulnerabilități
- **Securitate în cloud:** asigurarea faptului că instanțele cloud sunt securizate și configurate pentru a preveni drepturile de acces prea permisive, chiar și atunci când sunt puse în funcțiune și dezafectate rapid
- **Răspunsul la incident:** Utilizarea datelor îmbogățite, corelate asupra activelor pentru a accelera investigațiile de răspuns la incident și remedierea
- **Monitorizarea continuă a controlului**: identificarea momentelor în care controalele de securitate lipsesc și trebuie aplicate

5. Evaluarea eficacității politicilor de securitate cibernetică

Dezvoltarea unui sistem informatic progresează prin mai multe faze distincte, de la analiza problemei până la implementarea sistemului. De-a lungul acestui proces, fiecare pas este documentat printr-o serie de livrabile care variază de la un studiu de fezabilitate până la manuale de instruire și documentație de sistem. În dezvoltarea unei politici de securitate, acest proces de auto-documentare nu are loc în general.

Multe politici dezvoltate în prezent încearcă să încadreze totul în politica de securitate: justificarea importanței și instrucțiuni și descrieri specifice sistemului. Cu siguranță, politica de securitate în sine este deja suficient de lungă, fără a avea detalii despre modul în care a fost creat documentul, cine a fost consultat în elaborarea lui sau cum a fost realizată formularea politicii. Nici nu va exista nicio documentare a problemelor politice care ar fi putut apărea în timpul implementării politicii sau a modului de instruire a oamenilor despre politică. Cu toate acestea, odată cu utilizarea tehnicilor de documentare în timpul dezvoltării politicii, o politică de securitate ar putea deveni din nou un document de principii. Alte probleme care nu se referă la principiile politicii de securitate ar fi documentate în altă parte, împreună cu justificarea politicii.

Cea mai importantă informație care adesea lipsește sau pur și simplu inadecvată atunci când încercăm să evaluăm o politică de securitate într-o organizație este documentația cerințelor. Fără o înțelegere clară a cerințelor, evaluarea calității unei politici de securitate este aproape imposibilă. O analiză a riscurilor/amenințărilor cu care se confruntă organizația este doar o parte din cerințele necesare pentru dezvoltarea unei politici de securitate. Obiectivele organizației și alte probleme politice care influențează dezvoltarea, implementarea și acceptarea politicii de securitate sunt la fel de importante. Disponibilitatea unei documentații extinse, inclusiv rezultatele unei analize extinse a cerințelor, va permite ca evaluarea politicii de securitate să atingă o mai mare profunzime, în loc să evalueze doar superficial produsul final. De exemplu, în loc să se concentreze doar pe dacă politica a fost implementată într-un anumit

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

domeniu, evaluarea poate acum să ia în considerare și modul în care a fost dezvoltat acel domeniu în cadrul politicii. Dovezile documentare ar putea fi evaluate pentru a determina dacă politica acoperă în mod adecvat toate problemele identificate în cadrul dezvoltării, fără a reduce niciuna dintre ele. Cu toate acestea, politicile de securitate variază foarte mult în funcție de contextul organizației și ne-am aștepta ca și dezvoltarea lor să varieze. Ar exista unele puncte comune între politici, chiar dacă zonele țintă se îndepărtează. Spre deosebire de evaluarea produselor însă, multe criterii în evaluarea politicii de securitate vor fi de natură subiectivă. Acest lucru se datorează naturii subiective a dezvoltării unei politici și a mediului în care politica este implementată.

5.1. Menținerea eficacității politicilor de securitate IT

Tehnologia informației, sau IT, este, fără îndoială, tehnologia secolului. Cu siguranță a transformat lumea. Cu toate beneficiile IT, totuși, o mulțime de riscuri de securitate au pătruns și în viața noastră. Organizațiile trebuie să elaboreze politici eficiente de securitate a informațiilor pentru a se asigura că operațiunile lor de afaceri rămân ferite de intrușii rău intenționați și de date de furt. În mod ironic, o modalitate excelentă de a menține eficiența politicilor de securitate împotriva peisajului în schimbare a riscurilor IT este utilizarea mai multor IT.

Iată câteva dintre modalitățile prin care IT-ul poate menține eficiența politicilor de securitate:

- **Evaluare mai bună a riscurilor:** Evaluarea riscului de securitate este un prim pas esențial în proiectarea oricărei politici de securitate a informațiilor. Pentru a aborda amenințările care decurg din sectorul IT care evoluează rapid, IT este singurul antidot. Deoarece riscurile se schimbă în mod constant, IT este o necesitate pentru a ține sub control noile amenințări. Vă permite să descoperiți cu ușurință noi riscuri pe baza înregistrărilor dumneavoastră anterioare de conformitate, să clasificați și să clasificați factorii de risc și să evaluați daunele pe care le poate provoca. Prin urmare, este important să învățați din noile evoluții – bune sau rele – din IT. Acest lucru vă va îmbunătăți evaluarea riscurilor, precum și pregătirea dumneavoastră în cazul în care o amenințare este iminentă.
- **Conformitate mai bună**: IT vă ajută să monitorizați cât de bine angajații și șefii organizației dumneavoastră rămân în conformitate cu autoritățile de reglementare, precum și cu politicile de securitate specifice organizației dumneavoastră. Printr-un singur software, puteți urmări autorizațiile de acces, partajarea nesigură a datelor, navigarea nesigură pe web, criptarea insuficientă a datelor și nenumărați alți factori care vă pot afecta grav securitatea.
- **Actualizarea constantă este o necesitate:** Deoarece lumea IT se schimbă cu fiecare respirație pe care o luăm, trebuie să fiți în permanență în căutarea noilor schimbări care vă pot distruge sistemul. Monitorizați evoluțiile din lumea riscurilor cibernetice, a criminalității cibernetice și a securității cibernetice. Actualizați-vă politicile de securitate

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

a informațiilor și software-ul de securitate în mod frecvent și regulat, deoarece acestea pot deveni depășite foarte repede. În acest fel, puteți menține eficiența politicilor dvs. de securitate.

- **Atenuare rapidă:** dacă organizația dvs. se confruntă cu o amenințare iminentă de securitate care poate duce la potențiale pierderi sau furt de date, trebuie să aveți la îndemână un plan de atenuare sau de remediere. IT vă ajută să planificați atenuarea într-un mod simplu și eficient. Cu IT, puteți atribui și lega pașii de reducere a riscurilor la diferite riscuri potențiale atunci când vă proiectați politicile de securitate. Acest lucru va face atenuarea oportună și mai eficientă, menținând astfel eficacitatea politicilor dvs. de securitate.
- **Responsabilitate îmbunătățită:** Nicio politică de informare nu poate rămâne eficientă dacă oamenii nu sunt considerați responsabili și responsabili pentru riscuri, conformitate și atenuare. IT facilitează asigurarea responsabilității acțiunilor de remediere. Poate îmbunătăți considerabil evaluarea vizibilității riscurilor și a maturității, conformitatea și măsurile de remediere pe care le întreprinde organizația dvs. Aceasta înseamnă că angajații dvs. vor fi mai prompți și mai responsabili față de pașii enumerați în politicile dvs. de securitate a informațiilor.

5.2. Evaluarea riscurilor de securitate

Evaluarea riscurilor, după determinarea activelor informaționale care vor fi protejate, se selectează metoda de evaluare a riscurilor și se definesc riscurile. Conform metodei alese de evaluare a riscului, activele informaționale sunt poziționate pe harta riscurilor prezentată în figură. După efectuarea evaluării, harta de evaluare a riscurilor acoperă procesele de îmbunătățire și control al riscurilor pentru amenințări cu impact și probabilitate ridicate. Deoarece locația activelor informaționale în harta riscurilor se poate modifica, harta de evaluare a riscurilor ar trebui actualizată în mod regulat și trebuie luate măsurile de precauție necesare.

Riscul este definit ca combinația dintre probabilitățile unui eveniment și rezultatul acestuia. Evaluarea riscurilor, care este o etapă a managementului riscului, este un proces în care riscurile sunt definite și sunt determinate efectele și prioritățile acestor riscuri identificate. Managementul riscului este de a determina un nivel acceptabil de risc, de a evalua riscul curent, de a lua măsurile necesare pentru a reduce acest risc la un nivel acceptabil și de a menține acest nivel de risc. Informațiile și alte active, amenințările la adresa acestor active, vulnerabilitățile din sistemul existent și controalele sistemului de securitate sunt componentele care determină riscul curent. Identificarea informațiilor sau a bunurilor care trebuie protejate; determinarea cât de valoroase sunt aceste bunuri pentru unități; dezvăluirea care dintre amenințările cunoscute și posibile la adresa acestor active vor fi încercate să fie prevenite; investigarea modului în care ar putea apărea posibilele pierderi; identificarea amplorii posibilelor amenințări la adresa

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

fiecărui activ; Examinarea a ceea ce se poate face în primul rând pentru a reduce amploarea și probabilitatea pierderilor care pot apărea în aceste active și planificarea pașilor care trebuie întreprinși pentru a menține amenințările prospective la un nivel minim sunt anumite faze ale evaluării riscului. Costul sistemului de securitate care urmează să fie stabilit și implementat ca urmare a managementului riscului este o altă problemă importantă care trebuie luată în considerare. Costul sistemului de securitate ar trebui să fie limitat de valoarea informațiilor protejate și de riscul determinat prin examinarea posibilelor amenințări. Alături de principiul că nu va exista securitate 100%, configurația ideală a securității informațiilor se realizează prin trei procese. Aceste procese sunt prevenirea, detectarea și răspunsul (răspuns sau reacție).

Prevenirea; Este procesul pe care sistemele de securitate se concentrează și funcționează cel mai mult. Sunt în curs de dezvoltare diverse măsuri pentru a izola sistemul împotriva amenințărilor și atacurilor împotriva sistemelor informatice, cum ar fi măsurile de securitate folosite în viața de zi cu zi, cum ar fi împrejmuirea grădinii unei case și utilizarea unei uși de oțel. În ceea ce privește securitatea computerului personal, având instalate programe de scanare viruși, efectuarea acestor programe și pachete de service ale sistemului de operare și corecția erorilor și actualizările la intervale regulate, utilizarea unui screen saver protejat prin parolă pe computer, părăsirea sistemului după ce a fost departe de computer pentru o perioadă de timp. mult timp, estimarea parolelor utilizate este dificilă. determinarea, păstrarea confidențialității acestor parole și schimbarea acestora la intervale regulate, acordarea de atenție la partajarea discurilor, acordarea atenției la fișierele descărcate de pe Internet sau trimise prin e-mail, protejarea documentelor importante cu o parolă sau păstrarea lor criptată, confidențialitatea e-mail-urilor sau informatii importante, site-uri fara certificate de securitate. Unele dintre măsurile care pot părea simple, dar salvează vieți, cum ar fi să nu fii trimis prin mijloace nesigure, să dezactivezi accesul la internet atunci când nu este folosit, să faci copii de rezervă regulate ale informațiilor și documentelor importante. Pașii de prevenire care trebuie implementați în securitatea computerelor în mediile corporative sunt mai largi și mai complexi. Unele dintre lucrurile care se fac despre prevenire în astfel de sisteme în care lucrează experți în securitate:

- Revizuirea periodică a pachetelor de service și a actualizărilor sistemului de operare și software-ului;
- Menținerea drepturilor utilizatorului la minimum, fără a rula protocoale, servicii, componente și procese neutilizate;
- Tehnici de criptare în transmiterea datelor, scanere de vulnerabilitate,
- Utilizarea rețelei private virtuale,
- Utilizarea infrastructurii cu cheie publică și a semnăturii electronice poate fi enumerată ca fiind utilizarea sistemelor bazate pe biometrice.

De fapt, dacă progresul determinat în procesul de prevenire ar putea fi perfect, nu ar mai fi deloc necesare procese ulterioare. Toate atacurile ar fi fost prevenite în cel mai rău caz. Dar

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

niciun produs de securitate nu este perfect sau complet. În plus, aproape în fiecare zi, sunt detectate diverse vulnerabilități în sistemele de transmisie, serviciile de internet, tehnologiile web și aplicațiile de securitate. Din acest punct de vedere, utilizarea proceselor de detectare și potrivire crește.

Determinare; Securitatea nu este doar o chestiune de prevenire. De exemplu, faptul că un muzeu este bine protejat, că muzeul este înconjurat de garduri, că ușile sunt închise și încuiate, nu necesită folosirea paznicilor pe timp de noapte în muzeul respectiv. În același mod, este sporită și utilizarea metodelor de detectare a tentativelor de atac asupra sistemelor informatice. Prevenirea înseamnă construirea unei bariere care fie face atacurile mai puternice (dar nu imposibile), fie descurajează (dar nu distruge) atacatorii. Prevenirea fără detectare și răspuns poate avea doar beneficii limitate. Dacă ar fi suficientă doar prevenirea, majoritatea atacurilor nici nu ar fi fost cunoscute. Odată cu detectarea, atacurile cunoscute anterior sau nou apărute pot fi raportate și pot fi oferite răspunsuri adecvate. Primul și cel mai de bază pas în detectare este monitorizarea întregii stări și mișcare a sistemului și păstrarea înregistrărilor acestor informații. În acest fel, sunt colectate și date și dovezi pentru analiza post-atac. Firewall-uri, sisteme de detectare a intruziunilor, monitoare de trafic în rețea, scanere de porturi, utilizarea honeypot, instrumente de protecție în timp real împotriva virusurilor și a programelor spion, programele de control al sumelor de verificare a fișierelor și senzorii de rețea Sniffer sunt unele dintre cele mai frecvente metode utilizate în procesul de detectare..

Răspunde înapoi; Așa cum un loc dotat cu paznici, câini, camere de supraveghere, senzori poate atrage atenția hoților, sistemele informatice cu sisteme de detectare în timp real sunt atractive și pentru hackeri și atacatori. Răspunsul rapid apare ca un element esențial care completează sistemul de securitate pentru a respinge aceste atacuri. Răspunsul poate fi definit ca execuția unor acțiuni care vor răspunde imediat sau cât mai curând posibil la încercările de atac care nu pot fi tratate de procesul de prevenire și determinate de procesele de detectare. Sistemele de detectare a intruziunilor pot avea sens dacă există cineva sau un sistem care să răspundă la această detectare. În rest, această situație nu depășește beneficiul unei alarme auto de care nimeni nu o aude și de care nu-i pasă. În acest sens, reciprocitatea este o verigă importantă care completează procesul de securitate. Chiar dacă atacul nu este complet prevenit; Permite sistemului să revină la starea sa normală, să identifice cauzele atacului, să prindă atacatorul, atunci când este necesar, să identifice vulnerabilitățile sistemului de securitate și să reorganizeze procesele de prevenire, detectare și răspuns. Planificarea acțiunilor care trebuie întreprinse atunci când este detectat un atac, în avans, va asigura că acest proces funcționează eficient și nu va pierde timp și bani. Recuperarea în caz de dezastru se află în fruntea planurilor majore de cel mai rău caz întreprinse pentru această fază.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Întrebări:

1. Care dintre următoarele nu este una dintre etapele managementului activelor.

A) Efectuarea unui inventar al bunurilor

B) Determinarea dreptului de proprietate asupra bunurilor

C) Stabilirea contului de cost

D) Determinarea regulilor de utilizare a activelor

2. Care este scopul principal al procesului de testare a amenințărilor și vulnerabilităților?

A) Să înțeleagă cel mai bine vulnerabilitățile de securitate ale activelor și să ia măsurile necesare pentru a proteja efectiv aceste active.

B) Gestionarea vulnerabilităților de securitate

C) Obținerea de informații preliminare despre inventarul activelor

D) Închiderea vulnerabilităților de securitate

3. Care dintre următoarele nu este un tip de evaluare a vulnerabilității?

A) Scanări în rețea

B) Scanări bazate pe gazdă

C) Scanări de baze de date

D) Scanări bazate pe server

4. Care dintre următoarele nu face parte din procesul de gestionare a activelor de securitate cibernetică?

A) Managementul vulnerabilităților

B) Managementul costurilor

C) Monitorizarea controlului continuu

D) Detectare și intervenție

5. Care dintre următoarele nu este o modalitate pentru IT de a menține eficiența politicilor sale de securitate?

A) Evaluarea riscului

B) Modernizare constantă

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

C) Atenuare rapidă

D) Politici de securitate

6. Care dintre următoarele nu este unul dintre cele trei procese care constituie configurația ideală a securității informațiilor?

A) Pregătirea

B) Prevenirea

C) Determinare

D) Răspuns

Întrebări de autoevaluare. După ce răspunde, cursantul poate vedea rezultatele și le poate compara cu cele salvate pe platformă

- **Ce este vulnerabilitatea sistemelor IT**
- **Explicați și oferiți eșantion pentru managementul vulnerabilităților și managementul riscurilor**

Atasamente *(Prezentare PowerPoint, fișe, printuri, link-uri, video ...):*

Referințe:

1. Evaluating IS Security Policy Development S.B. Maynard1 & A.B. Ruighaver2 Department of Information Systems University of Melbourne Australia
2. https://www.bizzsecure.com/how-it-can-maintain-the-effectiveness-of-security-policies/
3. https://blog.masterofproject.com/service-asset-and-configuration-management/
4. https://www.apptega.com/blog/change-configuration-management-cybersecurity
5. https://cam.scmagazine.com/it-service-management-vs-cybersecurity-asset-management/
6. http://www2.mitre.org/public/industry-perspective/documents/06-ar-cyber-coop-planning.pdf
7. https://icma.org/articles/pm-magazine/cyber-continuity-planning-go-big-or-go-home
8. https://www.kroll.com/en/services/security-risk-management/security-consulting/threat-vulnerability-assessments
9. https://www.xmcyber.com/blog/what-is-the-difference-between-vulnerability-assessment-and-vulnerability-management/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

10. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.