Modul 5: Securitatea cibernetică, ca o necesitate de bază a fiecărui proces de învățare

4.0 ANDCOM

URV | Versiune 3| Date 07/10/2020

This project is co-funded by the Erasmus+ programme of the European Union.

Cuprins

CAPITOLUL 1: Introducere și prezentare generală a securității cibernetice

Sursa: https://www.pngegg.com/en/png-wjpvk

INTRODUCERE

În prezent, putem trimite sau primi date sub orice formă, de exemplu e-mail-uri, fișiere video sau audio, printr-o simplă apăsare de buton, dar ne-am gândit vreodată cât de sigur au fost transmise datele celeilalte persoane, fără vreo scurgere de informații? Breșele de securitate pot apărea când scriem pe hârtie, trimitem informații prin fax sau chiar verbal. Dar consecințele încălcării normelor de securitate în cazul informațiilor digitale sunt potențial mult mai grave deoarece aceste informații pot fi distribuite mai ușor către un public mai larg. Iar rezolvarea acestei probleme stă în Securitatea cibernetică. Astăzi internetul este infrastructura cu cea mai rapidă dezvoltare din viața de zi cu zi.

Securitatea cibernetică este denumirea măsurilor de protecție luate pentru a evita sau a reduce orice perturbare cauzată de un atac asupra datelor, computerelor sau dispozitivelor mobile. Securitatea cibernetică acoperă nu numai protejarea confidențialității și a vieții private, ci și disponibilitatea și integritatea datelor, ambele fiind vitale pentru calitatea și siguranța acestora.

Securitatea cibernetică este un domeniu în continuă schimbare, cu o mulțime de termeni de specialitate, iar uneori poate părea destul de greoaie. Cu toate acestea, pot fi luate multe măsuri eficiente și relativ simple pentru a vă proteja informațiile, pe dvs. și organizația dvs. Așadar, luarea unor măsuri simple și eficiente și practicarea unor comportamente sigure vor reduce amenințările online.

Consecințele atacurilor cibernetice sunt costisitoare – în ceea ce privește cheltuieli, timp de recuperare și pierderea reputației. De aceea securitatea cibernetică este prioritară pentru afaceri și tot personalul trebuie să fie conștient de modul de implementare a măsurilor de protecție.

Oamenii ar trebui, de asemenea, să fie conștienți de măsurile de Securitate cibernetică de bază referitoare la uzul personal și profesional.

Până la sfârșitul acestui modul veți învăța despre:

- Înțelegerea spațiului cibernetic,
- Necesitatea și importanța securității cibernetice,
- Concepte și elemente fundamentale ale securității cibernetice,
- Mediile securității cibernetice.

SPAȚIUL CIBERNETIC

Spațiul cibernetic este format din diverse sisteme informatice conectate și sisteme de telecomunicații integrate. A devenit o caracteristică a societății moderne, îmbunătățind și permițând comunicarea rapidă, sistemele de comandă și control distribuite, stocarea și transferul de date în masă și o serie de sisteme foarte distribuite.

Toate acestea sunt acum considerate de către societate a fi de la sine înțelese și au devenit esențiale pentru afaceri, pentru viața noastră de zi cu zi și pentru furnizarea de servicii. Această omniprezență și dependență de spațiul cibernetic poate fi întâlnită chiar și în sferele militare, unde elementele de comunicare, comandă și control, informații și atac de precizie se bazează pe multe "sisteme cibernetice" și pe sisteme de comunicații conexe.

Omniprezența acestor sisteme interconectate a adus o doză de dependență și vulnerabilitate persoanelor, industriilor și guvernelor, care este dificil de prevăzut, gestionat, atenuat sau prevenit. Unele națiuni consideră că astfel de dependențe vulnerabile sunt preocupări de securitate națională sau apărare națională și au însărcinat elemente existente ale forțelor lor de securitate să răspundă, în timp ce alte națiuni au creat organizații complet noi însărcinate cu gestionarea sau coordonarea politicilor naționale de securitate cibernetică.

Securitatea cibernetică a apărut ca o importantă problemă transversală, care necesită răspunsuri din partea persoanelor fizice, firmelor private, a organizațiilor neguvernamentale, a "întregii guvernări" și a unei serii de agenții și organisme internaționale.

IMPORTANȚA CIBERSECURITĂȚII

O parte din viața în era digitală este înțelegerea faptului că informațiile noastre private sunt mai vulnerabile ca niciodată. Știrile despre furtul de identitate și încălcarea securității datelor abundă, efectele fiind resimțite de milioane de consumatori. Și în timp ce companiile și instituțiile lucrează constant pentru a se proteja prin măsuri de securitate crescânde, dvs. puteți, de asemenea, să jucați un rol în această luptă.

Securitatea cibernetică nu implică doar întreprinderile și guvernul. Computerul, tableta și telefonul dvs. conțin probabil informații pe care hackerii și alți infractori ar dori să le aibă, cum ar fi adresele de e-mail ale altor persoane, numele și datele de naștere. Să presupunem, de exemplu, că un hacker a avut acces la informațiile dumneavoastră de contact. El ar putea apoi să trimită un e-mail sau un mesaj text tuturor celor pe care îi cunoașteți, folosindu-vă numele, încurajându-i să facă clic pe un link care conține malware, precum "Hei, am crezut că ți-ar plăcea asta! Clic aici."

Orice lucru care se bazează pe internet pentru comunicare sau este conectat la un computer sau la alt dispozitiv inteligent, poate fi afectat de o încălcare a securității. Aceasta include:

- sisteme de comunicare, cum ar fi email, telefoane și mesaje text
- sisteme de transport, inclusive controlul traficului, motoare auto, sisteme de navigație pentru avioane
- baze de date guvernamentale, inclusiv coduri numerice personale, licențe, fișe fiscale
- sisteme financiare, inclusiv conturi bancare, împrumuturi și salarii
- sisteme medicale, inclusiv echipamente și fișe medicale
- sisteme educaționale, inclusiv note, buletine și informații din cercetare

Riscul de securitate cibernetică este în creștere, determinat de conectivitatea globală și de utilizarea serviciilor cloud, precum Amazon Web Services, pentru a stoca date sensibile și informații cu caracter personal. Foarte răspândita configurare slabă a serviciilor cloud, asociată cu infractori cibernetici din ce în ce mai sofisticați, înseamnă că riscul ca organizația dvs. să sufere un atac cibernetic sau o încălcare a securității datelor este în creștere. Se pare că acum lunar, sau uneori chiar săptămânal, există un segment în știri dedicat discutării consecințelor unei încălcări a securității datelor la o companie importantă sau că hackerii au restricționat accesul la o rețea locală de calculatoare și pentru deblocare cer sume mari de bani (numit și ramsomware.)

ELEMENTE FUNDAMENTALE ALE SECURITĂȚII CIBERNETICE

Sursa: Imagine creată de autor

Securitatea cibernetică în ansamblu este un termen foarte larg dar se bazează pe trei concepte fundamentale cunoscute sub numele de "Triada CIA" - Confidențialitate, Integritate și Disponibilitate. Acest model este conceput pentru a ghida organizația în privința politicilor de Securitate cibernetică, în domeniul Securității informațiilor.

Confidențialitatea: definește regulile care limitează accesul la informații. Pe baza confidențialității se iau măsuri pentru a restricționa accesul la informațiile sensibile a atacatorilor și hackerilor cibernetici. Într-o organizație, angajaților li se permite sau li se refuză accesul la informații în funcție de categoria lor, prin autorizarea persoanelor corespunzătoare dintr-un departament. De asemenea, li se oferă o pregătire adecvată despre schimbul de informații și securizarea conturilor lor cu parole puternice. Aceștia pot schimba modul în care datele sunt gestionate în cadrul unei organizații pentru a le asigura protecție. Sunt diverse modalități de a asigura confidențialitatea, cum ar fi autentificarea prin doi factori, criptarea datelor, clasificarea datelor, verificarea biometrică și cartelele de securitate.

Integritate: se referă la faptul că datele sunt consistente, precise, corecte și de încredere, pe întreaga perioadă. Aceasta înseamnă că datele aflate în tranzit nu ar trebui modificate, șterse sau accesate ilegal. Așadar, trebuie luate măsuri adecvate într-o organizație pentru a garanta siguranța acesteia. Controlul accesului la fișiere și controlul accesului utilizatorilor sunt măsuri care reduc încălcarea securității datelor. De asemenea, ar trebui să existe instrumente și tehnologii implementate pentru a detecta orice modificare sau încălcare a securității datelor. Diferite organizații utilizează o sumă de verificare și chiar o sumă de verificare criptografică pentru a controla integritatea datelor. Pentru a face față pierderii de date, ștergerii accidentale sau chiar atacurilor cibernetice, ar trebui să se facă backup-uri regulate. Backup-urile în cloud sunt acum cea mai bună soluție pentru acest lucru.

Disponibilitate: Disponibilitatea în ceea ce privește toate componentele necesare, cum ar fi hardware, software, rețele, dispozitive și echipamente de securitate, ar trebui menținută și actualizată. Acest lucru va asigura buna funcționare și accesul la date fără nicio întrerupere. De asemenea, trebuie asigurată o comunicare constantă între componente, prin asigurarea unei lățimi suficiente de bandă. Aceasta implică, de asemenea, optarea pentru echipamente de securitate suplimentare în caz de dezastre sau blocaje. Utilitățile precum firewall-urile, planurile de recuperare în caz de dezastru, serverele proxy și o soluție adecvată de backup trebuie asigurate pentru a face față atacurilor DoS. Pentru o abordare de succes, aceasta ar trebui să treacă prin mai multe straturi de securitate pentru a asigura protecția tuturor componentelor securității

cibernetice, implicând în special calculatoare, sisteme hardware, rețele, programe software și datele care sunt partajate între ele.

Într-o organizație, pentru a realiza o abordare eficientă a securității cibernetice, angajații, procesele, computerele, rețelele și tehnologia organizației, fie că este mică sau mare, ar trebui să fie la fel de responsabili. Dacă toate componentele se completează reciproc, este foarte posibil să reziste cu succes amenințărilor și atacurilor cibernetice dure.

MEDIUL SECURITĂȚII CIBERNETICE

Tabloul securității cibernetice este într-o continuă schimbare. Atacatorii caută în mod constant în rețelele companiilor noi puncte slabe și vulnerabilități pentru a le exploata, în timp ce organizațiile sunt nevoite să adopte noi abordări mai deschise la sistemele IT pentru a sprijini tendințe precum Bring-Your-Own-Device și cloud computing

De la phishing la ransomware, peisajul securității cibernetice cuprinde atacuri care au devenit din ce în ce mai sofisticate pe măsură ce timpul a trecut, amintind companiilor că, în timp ce instrumentele de Securitate cibernetică și practicile de protecție au devenit din ce în ce mai complexe, la fel s-a întâmplat și cu metodele de atac.

Sursa: https://unsplash.com/photos/JJPqavJBy_k

Pentru a înțelege necesitatea măsurilor de Securitate cibernetică și a practicilor sale, să aruncăm o privire rapidă asupra câtorva tipuri răspândite de amenințări și atacuri din spațiul cibernetic.

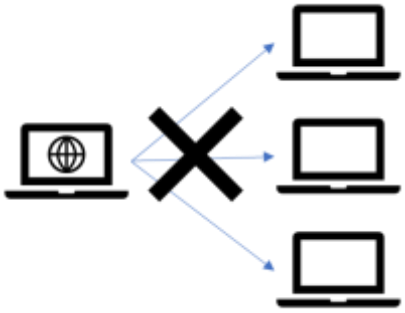
Ransomware: Ransomware este un program software de criptare a fișierelor care utilizează un algoritm puternic de criptare pentru a codifica fișierele de pe sistemul țintă. Autorii amenințării Ransomware generează o cheie de decriptare unică pentru fiecare dintre victimele sale și o salvează într-un server la distanță. Astfel, utilizatorii nu își pot accesa fișierele cu nicio aplicație. Autorii atacului ransomware profită de acest lucru și cer victimelor o sumă considerabilă pentru a le furniza codul de decriptare sau pentru a decripta datele. În urma unor astfel de atacuri, nu există nicio garanție de recuperare a datelor, chiar și după plata răscumpărării.

Atacuri Botnet: Botnet-urile au fost inițial concepute pentru a îndeplini o sarcină specifică în cadrul unui grup. Sunt definite ca o rețea sau un grup de dispozitive conectate la aceeași rețea pentru a executa o sarcină. Dar acest lucru este utilizat acum de către răuvoitori și hackeri care încearcă să acceseze rețeaua și să injecteze coduri dăunătoare sau malware pentru a perturba funcționarea acesteia. Unele atacuri botnet includ:

• Atacuri de tip Denial of Service (DDoS) distribuite

• Trimitere de email-uri spam

• Furt de date confidențiale



Sursa: Imagine creată de autor

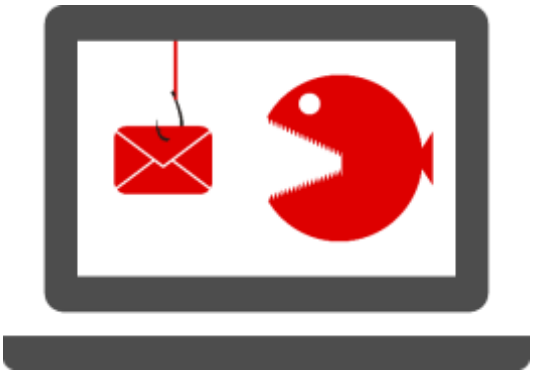
Atacurile de tip botnet se desfășoară în general împotriva companiilor și organizațiilor mari pentru că acestea dețin cantități imense de date. Prin atacul de acest tip, hackerii pot controla un număr mare de dispozitive și le pot compromite pentru a-și atinge scopurile.

Sursa: https://thecollegeinvestor.com/32760/prevent-identity-theft-tips/ (picture modified by author)

Atacuri de inginerie socială: Ingineriile sociale sunt acum tactici obișnuite folosite de infractorii cibernetici pentru a aduna informații sensibile despre utilizatori. Vă pot păcăli afișând reclame atractive, premii, oferte de nerefuzat, și așa ajung să vă ceară să furnizați detalii ale contului personal bancar. Toate informațiile pe care le introduceți sunt clonate și utilizate pentru fraude financiare, furt de identitate etc. Merită amintit virusul ZEUS, care este activ din 2007 și este folosit ca metodă de atac de inginerie socială pentru a fura datele bancare ale victimelor. Împreună cu pierderile financiare, atacurile de inginerie socială pot descărca alte amenințări distructive asupra sistemului în cauză.

Deturnarea criptomonedelor: Deturnarea criptomonedelor este un nou element al acestei lumi cibernetice. Monedele digitale și "mineritul" sunt tot mai populare, inclusiv printre infractorii cibernetici. Aceștia au descoperit că pot profita ilicit de mineritul monedelor digitale, care implică procese de calcul complexe pentru a mineri criptomonede precum Bitcoin, Ethereum, Monero, Litecoin și altele. Brokerii și investitorii în criptomonede sunt ținte ușoare pentru aceste atacuri. Deturnarea criptomonedelor este un program gândit pentru a introduce, discret, coduri de minerit în sistem. Astfel, hacker-ul folosește pe ascuns procesorul, unitatea de procesare grafică și sursa de alimentare ale computerului atacat pentru a mineri criptomonede. Acest lucru cauzează și o uzare prematură a echipamentelor atacate.

Sursa: https://unsplash.com/photos/iGYiBhdNTpE



Sursa: https://imgbin.com/png/wph1R90K/spear-phishing-social-engineering-png

Phishing: Phishing-ul este o acțiune frauduloasă de trimitere de email-uri spam, imitând pe cele ce provin din surse legitime. Astfel de email-uri au subiecte de interes, conțin false atașamente ca de exemplu facturi, oferte de locuri de muncă, oferte tentante de la companii de curierat cu reputație sau orice fel de e-mail important de la reprezentanți de rang înalt din companii etc. Atacurile de tip phishing sunt cele mai frecvente atacuri cibernetice și au ca scop furtul datelor sensibile, cum ar fi date de conectare, numere de carduri bancare, informații despre conturile bancare și așa mai departe. Pentru a evita acest lucru, ar trebui să aflați mai multe despre campaniile de e-mail phishing și măsurile de prevenție ce trebuiesc luate. Se pot folosi și tehnologii de filtrare a email-urilor pentru a preveni acest tip de atac.

Pe lângă acestea, în viitor vom vedea atacuri biometrice, atacuri AI (inteligență artificială) și atacuri IoT (Internetul lucrurilor). Multe companii și organizații sunt supuse unor atacuri cibernetice de mare amploare și nu au modalități de a le stopa. În pofida analizelor și actualizărilor constante în materie de securitate, creșterea amenințării cibernetice este consistentă. Așadar, merită să vă instruiți în domeniul elementelor de bază ale securității cibernetice și al implementării lor.

Pe scurt, pe măsură ce apar amenințări cibernetice din ce în ce mai complexe, cea mai bună abordare este vigilența constantă. Nu presupuneți niciodată că nu veți fi victima unei încălcări a securității datelor sau ținta unui atac cibernetic major – compania dvs. va trebui întotdeauna să gestioneze corect amenințările și să aibă sistemele și serviciile de detectare și răspuns potrivite.

TEST – INTRODUCERE ȘI PREZENTARE GENERALĂ A SECURITĂȚII CIBERNETICE

Acum, că a fost prezentată introducerea în securitatea cibernetică, o auto-evaluare rapidă poate fi efectuată după cum urmează:

1. Securitatea cibernetică este denumirea măsurilor de protecție luate pentru a evita sau a reduce orice perturbare cauzată de un atac asupra datelor, computerelor sau dispozitivelor mobile?
   a. Da
   b. Nu

2. Care dintre următoarele **nu** face parte din principiile fundamentale ale securității cibernetice?
   a. Confidențialitate
   b. Umanitate
   c. Integritate
   d. Disponibilitate

3. Vă rugăm să selectați cea mai bună opțiune referitoare la Spațiul cibernetic
   a. Constă din sisteme informatice conectate și sisteme integrate de telecomunicații
   b. Îmbunătățește și permite comunicarea rapidă
   c. Îmbunătățește sistemele distribuite de comandă și control
   d. Toate cele de mai sus

4. Dacă unul dintre prietenii tăi primește un email de la ID-ul tău, dar nu trimis de tine, iar el conține un text precum "Salut, m-am gândit că ți-ar plăcea să vezi asta! Clic pe link-ul de mai jos.", ce tip de atac cibernetic este acesta?
   a. Ransomware
   b. **Inginerie socială**
   c. Deturnarea criptomonedelor
   d. Atac Botnet

5. Care dintre următorii este cel mai puțin probabil să fie afectat de atacuri cibernetice?
   a. Bănci moderne
   b. Utilizatori individuali
   c. Organizații guvernamentale
   d. Toți cei de mai sus pot fi afectați

CAPITOLUL 2: Tipuri de amenințări și atacuri de securitate

Sursa: Imagine creată/modificată de autor

INTRODUCERE

O firmă de Securitate cibernetică, numită Cybersecurity Ventures, a anticipat că infracțiunile informatice vor costa întreaga lume 6 trilioane de dolari anual până în 2021, în creștere de la 3 trilioane de dolari în 2015. Criminalitatea cibernetică este una din cele mai mari provocări cu care se va confrunta omenirea în următoarele două decenii. Toți trebuie să fie conștienți de acest lucru și să fie pregătiți să facă față prin măsuri adecvate de securitate cibernetică.

Gradul de vulnerabilitate poate fi, în mare, legat de suprafața de atac la care lumea este probabil să fie expusă. Și aceasta este mult mai mare decât se crede în mod normal. Ea se întinde de la tranzacții pe internet la social media, dispozitive, cloud, dispozitive purtabile, ca să numim doar câteva. De multe ori, hackerii știu mai multe despre suprafața dvs. de atac digital decât dvs. Domenii, subdomenii, pagini de destinație, website-uri, aplicații mobile și profiluri de socializare deghizate sunt toate folosite, de multe ori în combinație, pentru a păcăli consumatorii și angajații să dezvăluie informații de acces și alte date personale sau să instaleze programe malware. Telefoanele mobile sunt, de asemenea, o țintă a atacurilor în multe cazuri. Contrar percepției generale că există un număr mic de magazine pentru aplicații mobile: sunt multe aplicații secundare și afiliate care deservesc în principal piața Android și oferă o oportunitate pentru cei rău intenționați.

Cu cât există mai multe date în spațiul cibernetic, cu atât este mai mare riscul pentru companii și oportunitățile mai crescute pentru hackeri. Cu cât crește mai mult cantitatea de date, cu atât mai multe atacuri se produc. În plus, pe măsură ce companiile continuă să integreze sisteme și aplicații, atacurile cibernetice vor deveni mult mai ample și vom vedea mai multe atacuri cibernetice care vor afecta întreaga afacere. Folosind conectivitatea companiei împotriva ei înșăși, hackerii pot bloca un site web, pot împiedica accesul la documente, sisteme și aplicații esențiale sau chiar pot tăia liniile de comunicare.

Pe măsură ce costurile scad, adoptarea IoT va crește în viitor, în special în mediul corporatist. Aceste dispozitive conectate devin mai puțin "bine de avut" și mai mult scontate în companii. Cu cât mai multe dispozitive conectate la internet prin 5G, cu atât mai mulți atacatori cibernetici vor avea posibilitatea să compromită sistemele și rețelele. Și, deși s-a înregistrat o creștere a spațiilor de birouri dotate cu IoT, nu s-a realizat în mod necesar aceeași creștere a securității în jurul lor.

Până la sfârșitul acestui modul veți învăța despre:

- Amenințări comune la adresa securității,
- Evoluția amenințărilor de securitate,
- Creșterea costului/varietății noilor amenințări la adresa securității.

AMENINȚĂRI COMUNE DE SECURITATE

Tabloul securității cibernetice este în continuă schimbare. Atacatorii caută constant noi puncte slabe și vulnerabilități de exploatat în rețelele corporatiste, în timp ce companiile sunt nevoite să adopte noi abordări mai deschise pentru sistemele IT pentru a sprijini tendințe precum Bring-Your-Own-Device și cloud computing. În plus față de cele câteva amenințări de securitate populare care au fost prezentate în capitolul 1, mai jos sunt descrise o serie de amenințări cibernetice de referință. Trebuie remarcat faptul că pe măsură ce securitatea cibernetică evoluează, noi amenințări vor continua să apară iar cele vechi își vor pierde relevanța. Este o zonă dinamică și ar trebui să fie actualizată extrem de des.

AMENINȚĂRI CIBERNETICE	DETALII
Malware	Software care execută o activitate rău intenționată pe un dispozitiv sau în rețea, de ex. coruperea datelor sau preluarea unui sistem.
Spear Phishing	O formă mai complexă de phishing, în care atacatorul învață despre victimă și joacă rolul cuiva cunoscut de victimă și în care ea are încredere.
Atac "Man in the Middle" (MitM)	Cazul în care un atacator se intercalează între expeditorul și destinatarul mesajelor electronice și le interceptează, probabil schimbându-le în tranzit. Expeditorul și destinatarul cred că comunică direct unul cu altul. Un atac MitM poate fi folosit în armată pentru a deruta un inamic.
Troieni	Numit după calul troian al grecilor antici, troianul este un tip de malware care intră într-un sistem țintă, arătând ca, de exemplu, o bucată de software standard, dar, odată ce intră în interiorul sistemului gazdă, lansează codul dăunător.
Atacul forței brute	Presupune încercări repetate de a obține acces la informații protejate (de ex. parole, criptare etc.) până când se găsește cheia corectă și se intră în posesia informațiilor dorite.
Atac distribuit de tip Denial of Service (DDoS)	Cazul în care un atacator preia mai multe dispozitive (poate mii) și le folosește pentru a solicita funcțiile unui sistem țintă, de exemplu un website, provocând blocarea acestuia din cauza unei supraîncărcări a cererii.

Atacuri asupra dispozitivelor IoT	Dispozitivele IoT, cum ar fi senzorii industriali, sunt vulnerabile la mai multe tipuri de amenințări cibernetice. Acestea includ hackeri care preiau dispozitivul pentru a-l face parte dintr-un atac DDoS și accesul neautorizat la datele colectate de dispozitiv. Având în vedere numărul lor, distribuția geografică și sistemele de operare frecvent depășite, dispozitivele IoT sunt o țintă principală pentru atacatori.
Încălcarea securității datelor	O încălcare a securității datelor este un furt de date realizat de un atacator cibernetic. Motivele pentru încălcarea securității datelor includ infracțiuni (de ex. furtul de identitate), dorința de a pune într-o lumină nefavorabilă o instituție (de ex. Edward Snowden sau DNC hack) și spionaj.
Malware pe aplicații mobile	Dispozitivele mobile sunt vulnerabile la atacuri malware, la fel ca alte componente hardware. Atacatorii pot încorpora programe malware în descărcări de aplicații, site-uri web mobile sau email-uri și mesaje de tip phishing. Odată compromis, un dispozitiv mobil poate oferi atacatorului acces la informații personale, date de localizare, conturi financiare etc.
Water Holing	Crearea unui website fals sau compromiterea unui site legitim pentru a exploata utilizatorii care-l vizitează.
Cross-Site Scripting	Este o metodă de atac ce presupune ca hackerul să trimită un link către țintă. Accesând linkul respectiv, victima va ajunge pe un website vulnerabil, cu coduri dăunătoare și astfel computerul îi va fi infectat.

EVOLUȚIA AMENINȚĂRILOR LA ADRESA SECURITĂȚII CIBERNETICE

Pe măsură ce atacatorii cibernetici folosesc metode din ce în ce mai sofisticate, organizațiile și experții în securitate cibernetică devin mai buni în gestionarea amenințărilor. Și în timp ce măsurile de securitatea cibernetică evoluează, crește și ingeniozitatea atacatorilor cibernetici, deci este un ciclu continuu de îmbunătățire a ambelor părți.

Asta nu înseamnă că atacatorii cibernetici câștigă întotdeauna, ci doar că în situația actuală companiile și persoanele fizice trebuie să facă tot ce pot ca să diminueze riscul pentru operațiunile și clienții lor, fie că e vorba de rularea celui mai recent software antivirus pentru a contracara atacuri de tip ransomware, DDoS sau să gestioneze corespunzător atacuri asupra securității datelor, mai ales când vine vorba de consecințele acestor atacuri.

Într-un tablou digital în continuă schimbare, este esențial să se țină pasul cu tendințele din domeniul amenințărilor cibernetice. Atacurile cibernetice se schimbă în principal din cauza:

- **Evoluției țintelor:** furtul informațiilor este consecința infracțiunilor cibernetice cea mai costisitoare și cu cea mai mare rată de creștere. Dar datele nu sunt singura țintă. Sistemele de bază, cum ar fi cele industriale, sunt piratate în mod periculos pentru a perturba și distruge.
- **Evoluției impactului:** Deși datele rămân o țintă, furtul nu reprezintă întotdeauna obiectivul final. Un nou val de atacuri cibernetice relevă că datele nu mai sunt pur și simplu copiate, ci sunt distruse — sau chiar modificate în

încercarea de a genera neîncredere. Atacarea integrității datelor — sau prevenirea alterării lor — este următoarea frontieră.

- **Evoluției tehnicii:** Infractorii cibernetici își adapteze metodele de atac. Aceștia vizează factorul uman, cea mai slabă verigă din apărarea cibernetică, prin creșterea atacurilor de tip ransomware, phishing sau inginerie socială, folosite ca o cale de intrare. O evoluție interesantă este atunci când statele naționale și grupurile lor de atac asociate folosesc aceste tipuri de tehnici pentru a ataca afacerile comerciale. Există încercări de a clasifica atacurile din aceste surse ca fiind 'acte de război' în încercarea de a limita decontările din asigurări de securitate cibernetică.

Conform unor experți în acest domeniu, unele dintre predicțiile despre viitorul apropiat sunt creionate mai jos pentru a conștientiza astfel de posibilități și a spori vigilența.

Tehnologia 5G va crește vulnerabilitățile existente legate de IoT, vor apărea noi vulnerabilități din noua infrastructură necesară pentru a sprijini 5G, iar atacatorii cibernetici vor exploata aceste slăbiciuni prin intermediul dispozitivelor IoT.

Datele biometrice vor fi utilizate frecvent pentru autentificarea utilizatorilor, creând astfel un risc suplimentar (suprafața de atac) pentru ei. Cu parolele din ce în ce mai puțin sigure și cu unii utilizatori finali care nu adoptă autentificarea multi-factor, folosirea datelor biometrice va deveni obișnuită.

Atacarea aplicațiilor mobile bancare pentru a fura date de acces și fonduri este deja în creștere, iar această tendință este de așteptat să continue pe termen scurt și mediu, pe măsură ce tot mai mulți oameni folosesc aceste aplicații bancare mobile.

AI (Inteligența Artificială) a fost folosită pentru a juca rolul persoanelor reale prin imitarea realistă a vocii lor, ceea ce este util atunci când se solicită transfer de fonduri. Hackerii vor continua să utilizeze progresele AI pentru a scana rețelele în vederea depistării vulnerabilităților, vor automatiza atacurile tip phishing și vor efectua atacuri de inginerie socială pe scară largă pentru a propaga răspândirea "știrilor false," printre altele.

Seturile de instrumente de hacking gata de utilizat, capabile să exploateze vulnerabilitățile sau să fure informații și date de logare, nu au fost niciodată mai accesibile ca în prezent, iar numărul mare de hackeri crește și el probabilitatea atacurilor cibernetice.

CREȘTEREA COSTURILOR/ IMPACTULUI NOILOR AMENINȚĂRI LA ADRESA SECURITĂȚII CIBERNETICE

Înțelegând mai bine impactul asociat criminalității informatice, se poate conștientiza gravitatea și dimensiunile unor astfel de infracțiuni. Costul anual total al tuturor tipurilor de atacuri cibernetice este în creștere. Atacurile de tip malware și bazate pe Web continuă să fie cele mai scumpe, conform unui raport realizat de Accenture. Costul atacurilor de tip ransomware (21 %) și din interior (15 %) au crescut cel mai rapid în ultimii ani.

SURSA: NINTH ANNUAL COST OF CYBERCRIME STUDY - BY ACCENTURE

Creșterea rapidă a pierderilor de informații în ultimii trei ani este îngrijorătoare. Noile reglementări, cum ar fi GDPR și CCPA, au ca scop responsabilizarea companiilor și a directorilor acestora pentru protecția activelor informaționale și în ceea ce privește utilizarea cu responsabilitate a datelor clienților. Incidentele viitoare de pierdere a informațiilor (furt) ar putea contribui semnificativ la impactul financiar al acestor atacuri deoarece autoritățile de reglementare încep să impună amenzi. Costul întreruperii activității — inclusiv productivitatea scăzută a angajaților și eșecurile afacerilor care apar după un atac cibernetic — continuă să crească într-un ritm constant. Întreruperea activității continuă să crească permanent și este a doua mare consecință a criminalității informatice. Resursele ar trebui să fie direcționate către atacuri DoS, din interior și malware pentru a reduce acest cost.

De asemenea, trebuie acordată atenție și ratei de creștere a fiecărui tip de atac. Doar în ultimul an, consecințele financiare ale ransomware-ului au crescut cu 21%. Deși unul dintre costurile mai mici ale criminalității informatice în ansamblu, companiile nu ar trebui să ignore această amenințare cu creștere rapidă.

Costurile globale ale daunelor ransomware au depășit 5 miliarde dolari în 2017, fiind de 15 ori mai mari comparativ cu cele din 2015. Iar în 2019 acest tip de costuri a urcat la 11,5 miliarde dolari, iar pentru 2021 se estimează că va ajunge la 20 miliarde dolari.

Iată câteva statistici suplimentare (de la Cybersecurity Ventures[1]). În 2018 au existat aproape 4 miliarde de utilizatori de Internet (aproape jumătate din populația globală de 7,7 miliarde), în creștere față de 2 miliarde în 2015. Cybersecurity Ventures estimează că până în 2022 vor exista 6 miliarde de utilizatori de Internet (75% din populația mondială preconizată a fi de 8 miliarde) — și mai mult de 7,5 miliarde utilizatori de Internet până în 2030 (90% din populația mondială, estimată la 8,5 miliarde, cu vârsta de 6 ani și peste).

1 HTTPS://CYBERSECURITYVENTURES.COM/

TEST – INTRODUCERE ȘI PREZENTARE GENERALĂ A SECURITĂȚII CIBERNETICE

6. Care din următoarele reprezintă exemplu de suprafață de atac de securitate cibernetică?
    a. Rețele sociale
    b. Dispozitive mobile
    c. Portabile
    d. Toate cele de mai sus

7. Care dintre următoarele nu este un tip de impact pe care îl pot provoca atacurile de Securitate cibernetică?
    a. Impact economic
    b. Impact social
    c. Impact politic
    d. Impact biologic

8. Ce fel de amenințare de Securitate cibernetică este "Software care efectuează o sarcină rău intenționată pe un dispozitiv sau rețea țintă"?
    a. Troian
    b. Malware
    c. Phishing
    d. DoS

9. Care dintre următoarele sunt exemple de suprafață de atac în expansiune care ar putea apărea în viitorul apropiat?
    a. Tehnologia 5G care permite un transfer mai rapid și mai mare de date în tot spectrul digital
    b. Utilizarea frecventă a datelor biometrice pentru autentificarea utilizatorilor, care creează riscuri suplimentare
    c. Creșterea numărului de aplicații mobile
    d. Toate cele de mai sus

10. Vă rugăm să examinați declarația și să alegeți cea mai bună opțiune pentru a descrie acest lucru: "Consecințele financiare ale Securității cibernetice au crescut semnificativ în ultimii ani și este probabil să crească în continuare."
    a. Adevărat
    b. Fals

CAPITOLUL 3: Arhitectură și componente de Securitate cibernetică

Sursa: https://www.freepik.com/free-vector/cyber-security-concept_4520117.htm#page=1&query=background%20security&position=18

INTRODUCERE

În urmă cu aproape 30 de ani, securitatea cibernetică avea o sarcină extrem de ușoară, dat fiind numărul redus de dispozitive pe care trebuia să le protejeze (treaba lor era simplă). În prezent, utilizarea tehnologiilor digitale în mediile de lucru este în creștere puternică datorită necesității ca întreprinderile să devină mai adaptabile și mai performante. Aceasta creează un număr tot mai mare de atacatori cibernetici care vor să aibă acces la informații. Securitatea tradițională nu mai este suficientă deoarece amenințările devin tot mai complexe. Pe măsură ce câmpul de luptă cibernetic global a evoluat dramatic, este bine să aveți o idee clară și precisă a arhitecturii securității cibernetice.

Acum, securitatea cibernetică nu mai este doar preocuparea departamentului de IT, ci responsabilitatea tuturor. Ea sporește interacțiunea dintre departamente pentru a identifica ce trebuie protejat, reducând astfel impactul unor viitoare atacuri neașteptate. Securitatea cibernetică își extinde raza de acțiune până la limita în care datele sunt un obiectiv cibernetic în mișcare – date generate de IoT deținute pe dispozitive mobile sau date generate, stocate și accesate în cloud.

Arhitectura de Securitate cibernetică precizează structura organizațională, comportamentul funcțional, standardele și politicile unei rețele informatice, care include atât caracteristici de rețea cât și de securitate.

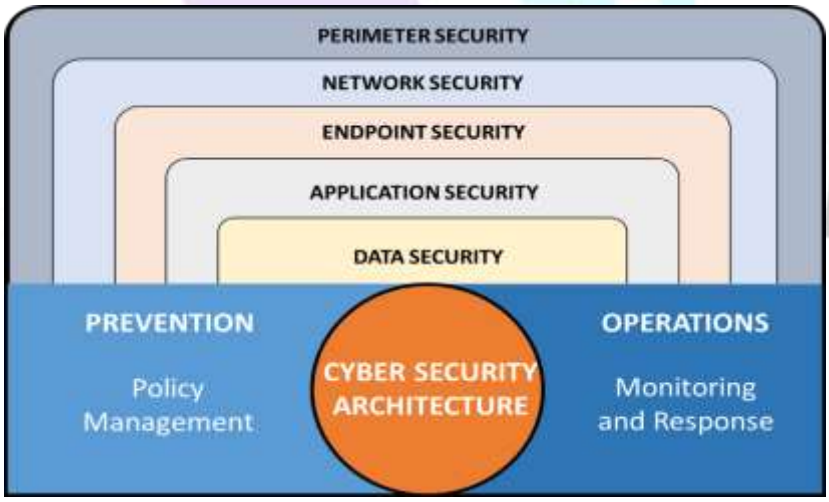
Obiectivele principale ale unei bune arhitecturi de Securitate cibernetică sunt de a se asigura că toate suprafețele de atac cibernetice sunt minimizate, ascunse și dinamice, toate datele sensibile/confidențiale/clasificate sunt puternic criptate și toate atacurile cibernetice sunt detectate, atenuate și contracarate în mod agresiv. Sistemele de apărare cu țintă mobilă și contra-măsuri agresive sunt puternic încurajate.

Deși acest curs nu urmărește să ofere detalii tehnice ale arhitecturii, totuși, până la sfârșitul lui, veți învăța despre:

- Arhitectura securizată (date, aplicație, punct final, rețea și securitate perimetrală).
- Perspectiva produs/soluție (Identitate și Gestionare acces, Securitate rețea, Securitate finală, Securitate mesagerie, Securitate Web, Securitate și Gestionarea vulnerabilităților),
- Tehnologie de Securitate (Firewall-luri, VPN, Wireless, Detectarea și prevenirea intruziunilor, alte instrumente de securitate (Criptografie)).

ARHITECTURA SECURIZATĂ (SECURITATEA CIBERNETICĂ)

Unitățile de securitate cibernetică au nevoie de o arhitectură de securitate adaptativă. Este un cadru important care ajută companiile să clasifice toate investițiile potențiale și existente în securitate pentru a determina unde sunt deficitare și pentru a se asigura că există o abordare echilibrată a securității cibernetice. Asemeni unui comandant militar competent, care trebuie să înțeleagă pe deplin diferitele tipuri de teren și punctele slabe ale forțelor sale pentru a-și apăra efectiv trupele și teritoriul, un arhitect inteligent de securitate cibernetică trebuie să înțeleagă profund diferitele topologii de rețea și vulnerabilități ale suprafeței la atacuri cibernetice, pentru a-și apăra în mod eficient rețeaua, datele sensibile și aplicațiile critice.



Sursa: Imagine creată de autor

Este logic să înțelegem arhitectura de securitate începând de la stratul exterior.

Perimeter Security (Perimetru de securitate): Ansamblul de securitate fizică - tehnică și politici programatice care oferă niveluri de protecție împotriva activităților

periculoase de la distanță; folosit pentru a proteja sistemele back-end împotriva accesului neautorizat. Atunci când este configurat corect, modelul de securitate al apărării perimetrului poate preveni, întârzia, absorbi și/sau detecta atacuri, reducând astfel riscul pentru sistemele back-end critice.

Nerwork Security (Securitatea rețelei): Nivelul care partiționează rețeaua largă de active și conexiuni în enclave; o enclavă este o zonă delimitată distinct, închisă într-o unitate mai mare. Enclavele încorporează controalele lor individuale de acces și mecanismele de protecție. Acest nivel de securitate a rețelei, când este utilizat în mod corespunzător, poate preveni daunele cauzate de trecerea de la o enclavă la altele și stabilește, de asemenea, politici de acces specifice enclavelor.

Endpoint Security (Securitatea punctului final): Mecanisme și controale de protecție a securității care se află direct pe un dispozitiv terminal (dispozitive finale precum computere, laptopuri, telefoane mobile, tablete etc.) care interacționează cu orice rețea sau sistem.

Application Security (Securitatea aplicațiilor): Mecanisme și controale de protecție a securității care sunt încorporate în aplicațiile aflate în rețea, enclave și dispozitive terminale. Exemple de astfel de aplicații ar putea fi – MS Office, aplicația ERP, aplicații mobile etc.

Data Security (Securitatea Datelor): Nivelul de securitate care protejează datele din companie, indiferent de starea datelor, adică indiferent dacă acestea sunt în mișcare, în repaus sau în uz.

Prevention (Prevenire): Acest lucru se realizează prin politici, proceduri, instruire, simularea amenințărilor, evaluarea riscurilor, teste de penetrare și toate celelalte activități de susținere incluzive pentru o poziție sigură.

Operations (Operațiuni): Observarea constantă a companiei cu un ochi atent, împreună cu instrumentele și procesele potrivite, pentru a recunoaște incidentele și evenimentele și a răspunde corespunzător în timp util.

PERSPECTIVA PRODUSULUI/SOLUȚIEI

Securitatea cibernetică este o preocupare pentru toți și, prin urmare, este logic să credem că trebuie să existe o soluție sau un mod de a crea o soluție care să rezolve parțial/total această problemă. Aceasta este foarte probabil să provină de la furnizori de soluții care sunt în principal întreprinderi comerciale. Nu există o soluție "unică pentru toți" în ceea ce privește securitatea cibernetică. Cu toate acestea, în general, soluțiile ar trebui să includă atât tehnologie sofisticată, cât și componente "umane", cum ar fi instruirea angajaților/utilizatorilor și stabilirea priorităților în consiliile de administrație ale companiei. Schița unei astfel de categorii de soluții este discutată în această secțiune.

Managementul identității și al accesului: Managementul identității și al accesului (IAM) se referă la definirea și gestionarea rolurilor și privilegiilor de acces ale utilizatorilor individuali de rețea și circumstanțele în care li se acordă (sau li se refuză) aceste privilegii. Acești utilizatori pot fi clienți (managementul identității clienților) sau

angajați (managementul identității angajaților). Sistemele IAM oferă administratorilor instrumentele și tehnologiile necesare pentru a schimba rolul unui utilizator, pentru a urmări activitățile utilizatorilor, pentru a crea rapoarte cu privire la aceste activități și pentru a pune în aplicare politicile în mod continuu.

Securitatea rețelei: aceasta este practica de prevenire și protecție împotriva intruziunilor neautorizate în rețele. Securitatea rețelei este implementată prin sarcinile și instrumentele folosite pentru a împiedica accesul persoanelor sau programelor neautorizate la rețelele dvs. și la dispozitivele conectate la acestea. Computerul dvs. nu poate fi piratat dacă hackerii nu pot ajunge la el prin rețea. La un nivel ridicat, aceasta constă în protecție, detectare și reacție la amenințări.

Securitatea punctului final: Se referă la o metodologie de protecție a rețelei atunci când este accesată prin intermediul dispozitivelor aflate la distanță, cum ar fi laptop-uri sau alte dispozitive wireless și mobile. Fiecare dispozitiv cu o conexiune de la distanță în rețea creează un potențial punct de intrare pentru amenințările de securitate. Aceasta este concepută pentru a securiza fiecare punct final din rețeaua creată de aceste dispozitive. Securitatea punctelor finale devine o funcție și o preocupare de securitate IT frecventă deoarece tot mai mulți angajați folosesc dispozitive mobile personale iar companiile permit forței de muncă să utilizeze aceste dispozitive în rețea.

Securitatea mesajelor: este axată pe securizarea și protejarea canalelor de comunicații ale unei organizații (software de email, aplicații de mesagerie și platforme de rețea socială). Acest nivel suplimentar de Securitate poate ajuta la securizarea dispozitivelor și poate bloca o gamă largă de viruși sau atacuri malware. Securitatea mesajelor contribuie la asigurarea confidențialității și autenticității metodelor de comunicare ale unei organizații sau companii.

Securitate Web

Website-urile și aplicațiile web sunt la fel de predispuse la breșe de securitate precum locuințele, magazinele, locațiile guvernamentale. Din păcate, criminalitatea cibernetică are loc în fiecare zi și sunt necesare măsuri de Securitate web pentru a proteja website-urile și aplicațiile web împotriva compromiterii. Exact asta face securitatea web – este un sistem de măsuri de protecție și protocoale care poate proteja site-ul web sau aplicația web împotriva piratării sau a accesului persoanelor neautorizate. Această împărțire integrală a Securității Informațiilor este esențială pentru protecția site-urilor, aplicațiilor și a serviciilor web. Orice site de pe internet ar trebui să aibă o formă de Securitate web pentru a fi protejat.

Managementul Securității și Vulnerabilității

Managementul vulnerabilității este o abordare pro-activă a gestionării securității rețelei prin reducerea probabilității ca erorile de programare sau de proiectare să compromită securitatea unui punct final sau a unei rețele. Este "practica ciclică de identificare clasificare, prioritizare, remediere și atenuare" a vulnerabilităților software.

TEHNOLOGII DE SECURITATE

Intrarea în detaliile tehnice ale tehnologiei cheie de securitate depășește domeniul de aplicare al prezentului document. Totuși, prezentăm mai jos o imagine privind tehnologia esențială de Securitate cibernetică, pentru referință.

TEHNOLOGIE	CATEGORIE 1	CATEGORIE 2	DETALII
HARDWARE	MANAGEMENT CONȚINUT	MANAGEMENT CONȚINUT	HARDWARE-UL DE MANAGEMENT AL CONȚINUTULUI INCLUDE DISPOZITIVE LA LOCAȚIE PENTRU SECURITATEA WEB ȘI A MESAJELOR.
	SECURITATE DATE	CLASIFICARE DATE ȘI PREVENIRE PIERDERI DE DATE (DLP)	SOFTUL DLP POATE DETECTA DATE CONFIDENȚIALE ÎN MIȘCARE (TRANZITÂND O REȚEA), ÎN UZ (FIIND VIZUALIZATE SAU ACCESATE PRIN INTERMEDIUL UNUI DISPOZITIV DE UTILIZATOR FINAL) ȘI ÎN REPAUS (DE EX. DATE STOCATE PE ECHIPAMENTE TERMINALE, SERVERE ȘI SUPORTURI MEDIA).
	SECURITATEA REȚELEI	FIREWALL	PRODUSELE FIREWALL SUNT CREATE PENTRU FILTRAREA TRAFICULUI ÎN REȚEA, RUTARE STATICĂ ȘI/SAU PROXY. UNELE FIREWALL-URI POT INCLUDE REȚELE VIRTUALE PRIVATE ȘI ALTE CARACTERISTICI DE SECURITATE.
		DETECTARE ȘI PREVENIRE INTRUZIUNI (IDP)	PRODUSELE IDP COMPARĂ ACTIVITATEA CURENTĂ CU O LISTĂ DE SEMNĂTURI CUNOSCUTE PENTRU A CĂUTA AMENINȚĂRI ȘI UTILIZEAZĂ ANALIZA PROTOCOLULUI, ANOMALIILOR, COMPORTAMENTULUI SAU EURISTICA PENTRU A DESCOPERI ACTIVITĂȚI NEAUTORIZATE ÎN REȚEA.
		MANAGEMENT UNIFICAT AL AMENINȚĂRII	ÎN MOD UZUAL, PRODUSUL POATE EFECTUA PROTEJAREA REȚELEI CU FIREWALL, DETECTAREA ȘI PREVENIREA INTRUZIUNILOR ÎN REȚEA, ȘI ANTIVIRUS LA PUCTUL DE ACCES.

		REȚEA VIRTUALĂ PRIVATĂ (VPN)	PRODUSELE VPN PERMIT UNEI COMPANII SĂ EXTINDĂ CONECTIVITATEA SECURIZATĂ A REȚELEI SALE LA BIROURI ȘI UTILIZATORI DE LA DISTANȚĂ, UTILIZÂND TEHNOLOGII DE CRIPTARE ȘI AUTENTIFICARE.
SOFTWARE	SECURITATE DATE	CLASIFICARE DATE ȘI PREVENIRE PIERDERI DE DATE (DLP)	SOFTUL DLP POATE DETECTA DATE CONFIDENȚIALE ÎN MIȘCARE, ÎN UZ (FIIND VIZUALIZATE SAU ACCESATE PRIN INTERMEDIUL UNUI DISPOZITIV DE UTILIZATOR FINAL) ȘI ÎN REPAUS (DE EX. DATE STOCATE PE TERMINALE, SERVERE ȘI SUPORTURI MEDIA).
	SOFTWARE DE SECURITATE TERMINAL	SOFTWARE DE SECURITATE TERMINAL	ACCES ȘI PROTECȚIE A INFORMAȚIILOR, ANTI-MALWARE, GESTIONARE PROACTIVĂ A RISCURILOR PENTRU UTILIZATORII FINALI, SECURITATE A SERVERELOR.
	IDENTITATE ȘI ÎNCREDERE DIGITALĂ	IDENTITATE ȘI ÎNCREDERE DIGITALĂ	AUTENTIFICARE, AUTENTIFICARE LEGACY, ACCES PRIVILEGIAT, CONFIGURARE , CONECTARE UNICĂ
	SECURITATE MESAGERIE	SECURITATE MESAGERIE	SECURITATEA MESAGERIEI INCLUDE ANTI-SPAM, ANTI-MALWARE, FILTRAREA CONȚINUTULUI ȘI E IMPLEMENTATĂ PE TOATE PLATFORMELE DE SECURITATE.
	SOFTWARE DE SECURITATE A REȚELEI	SOFTWARE DE SECURITATE A REȚELEI	SOFTWARE-UL DE SECURITATE A REȚELEI PROTEJEAZĂ REȚELELE CORPORATIVE ȘI RESURSELE ÎNCORPORARE ÎN REȚEA ÎMPOTRIVA PERTURBĂRILOR CAUZATE DE AMENINȚĂRILE EXTERNE.
	ANALIZE DE SECURITATE, CONTRA-INFORMAȚII, REACȚIE	ANALIZE DE SECURITATE, CONTRA-INFORMAȚII, REACȚIE	EVALUARE VULNERABILITĂȚI DISPOZITIVE/SOFTWARE, CRIMINALISTICĂ ȘI INVESTIGAREA INCIDENTELOR, POLITICĂ ȘI CONFORMITATE, GESTIONAREA SISTEMELOR DE SECURITATE, INFORMAȚII DE

			SECURITATE ȘI GESTIONARE A EVENIMENTELOR
	INSPECTARE CONȚINUT WEB	INSPECTAREA CONȚINUT WEB	SOFTWARE-UL DE SECURITATE WEB PROTEJEAZĂ ÎMPOTRIVA AMENINȚĂRILOR DE INTRARE (MALWARE) ȘI DE IEȘIRE (SCURGERI DE DATE) .

TEST – INTRODUCERE ȘI PREZENTARE GENERALĂ A SECURITĂȚII CIBERNETICE

Acum, că au fost discutate amenințările și atacurile comune privind securitatea cibernetică, o autoevaluare rapidă poate fi efectuată după cum urmează:

11. Scopul principal al arhitecturii de Securitate cibernetică este de a face suprafața atacului:
    a. Minimizată
    b. Ascunsă
    c. Dinamică
    d. Toate cele de mai sus

12. Care sunt nivelurile cheie ale arhitecturii de Securitate cibernetică?
    a. Securitatea perimetrală
    b. Securitatea rețelei
    c. Securitatea echipamentelor terminale
    d. Toate cele de mai sus

13. Care dintre următoarele nu este o practică de gestionare a vulnerabilității la securitatea cibernetică?
    a. Identificare
    b. Proiectare
    c. Clasificare
    d. Prioritizare

14. Care din exemplele de mai jos nu este un dispozitiv terminal?
    a. Calculator Desktop
    b. Dispozitive mobile
    c. Server
    d. Laptop/Notebook

15. Vă rugăm să citiți declarația și să alegeți cea mai bună opțiune pentru a descrie acest lucru: "prevenirea atacurilor cibernetice este realizată prin politici, proceduri, formare, simularea amenințărilor, evaluarea riscurilor, teste de penetrare și toate celelalte activități de susținere incluzive pentru a asigura o poziție sigură":
    a. Adevărat
    b. Fals

CAPITOLUL 4: Prevenirea amenințărilor de securitate cibernetică și cele mai bune practici

Sursa: https://unsplash.com/photos/uh5TTKr5e_w

INTRODUCERE

Peisajul amenințărilor cibernetice este în continuă schimbare. Odată cu modificarea motivațiilor care stau la baza atacurilor, de la o perturbare a unui sistem individual, perturbarea serviciilor, perturbări ale rețelei, atacuri organizate de state, economie subterană la recentele cereri de răscumpărare, toată lumea este acum nevoită să își revizuiască măsurile de securitate ale sistemelor IT sau ale infrastructurii. Au trecut vremurile în care atacatorii trebuiau să depună eforturi considerabile, să facă inginerie inversă pentru a dezvolta un exploit, după ce un patch este lansat pentru o vulnerabilitate cunoscută. Odată cu disponibilitatea instrumentelor și exploit-urilor online, atacatorii trebuie să depună acum eforturi mult mai mici pentru a îmbunătăți sau a construi noi instrumente de atac. Pentru a contracara în mod eficient aceste pericole, trebuie făcută o revizuire aprofundată a nivelului de securitate.

Prevenirea amenințărilor cibernetice și gestionarea incidentelor sunt tratate puțin diferit pentru cele două categorii generale – măsurile luate de companii și măsurile luate de persoane fizice. Deși domeniul de aplicare al acestui document este centrat în principal pe persoanele fizice, o vizualizare rapidă a activităților utilizate de o companie poate ajuta la construirea unei perspective complete.

Companiile ating de obicei obiectivul prin anumite măsuri - gestionarea riscurilor (a sistemului lor IT), crearea capacităților de gestionare a incidentelor și de răspuns la incidente, revizuirea periodică a indicatorilor de Securitate cibernetică, implementarea unor instrumente eficiente de detectare și prevenire, gestionarea continuă a patch-urilor

și, foarte important, instruirea resursei umane, creșterea și menținerea gradului ridicat de conștientizare în rândul angajaților.

Persoanele fizice iau măsuri simple, cum ar fi instalarea de antivirus, instalarea unui firewall, folosire de software/aplicații autentice, precauția în legătură cu orice atașament email, back-up regulat de fișiere etc. Măsurile individuale vor fi discutate mai detaliat în acest document.

Până la sfârșitul acestui modul, veți descoperi:

- O prezentare generală a practicilor de prevenire a pericolelor și de gestionare a incidentelor
- Cele mai bune practici sugerate pentru a proteja o persoană împotriva amenințărilor la adresa securității cibernetice
- O prezentare generală a anumitor tendințe viitoare în amenințările cibernetice.

PREZENTARE GENERALĂ A PRACTICILOR DE PREVENIRE A PERICOLELOR ȘI DE GESTIONARE A INCIDENTELOR

Practici principale comune ale companiilor – Cele mai bune practici ale companiilor pentru apărarea împotriva atacurilor cibernetice includ contramăsuri de bază, dar extrem de importante. Unele din practicile principale sunt:

Managementul riscurilor – Minimizarea impactului negativ și necesitatea unei baze solide în luarea deciziilor sunt principalele motive pentru care organizațiile implementează Managementul Riscurilor pe sistemele IT. Modificările aduse resurselor IT pot introduce vulnerabilități și pot modifica starea generală de risc. Gestionarea eficientă a riscurilor ajută la identificarea resurselor mai critice sau mai sensibile, astfel încât să poată fi aplicate controale de securitate mai stricte sau să se depună mai multe eforturi pentru a le proteja. Integrarea gestionării riscurilor în ciclul de viață al dezvoltării sistemului contribuie la abordarea securității în toate etapele ciclului de viață și produce rezultate eficiente.

Managementul incidentelor – Un program eficient de gestionare a riscurilor include capacități eficiente de gestionare a incidentelor și de răspuns. Un risc, care nu este prevenit de controalele de gestionare a riscurilor, stabilește un incident. Organizațiile trebuie să aibă o echipă puternică de răspuns la incidente, cu roluri și responsabilități clar definite, precum și cu planuri de management al incidentelor, pentru a le gestiona și a împiedica producerea unui dezastru. Managementul incidentelor este mai degrabă o gestionare a crizelor și, prin urmare, politicile și procedurile ar trebui să fie clare și să poată fi urmate cu ușurință. Procedurile ar trebui revizuite și testate periodic pentru o mai mare eficacitate.

Revizuire periodică – Organizațiile ar trebui să monitorizeze în permanență indicatorii de securitate și să le revizuiască periodic eficacitatea. Acest lucru ajută la cunoașterea eficacității controalelor de securitate implementate, la realinierea

controalelor existente sau la implementarea controalelor suplimentare pentru a gestiona securitatea informațiilor.

Instrumente de Detectare/Prevenire – Majoritatea companiilor au un sistem de detecție a intruziunilor sau de prevenire a intruziunilor sau ambele sisteme pentru a detecta atacurile cibernetice și a proteja rețeaua de atacuri. Pe lângă detectarea amenințărilor sau atacurilor, sistemul poate fi utilizat și pentru identificarea problemelor legate de politica de securitate a unei companii, pentru a documenta amenințările existente și a utiliza informațiile pentru actualizarea programelor de conștientizare cu scopul de a împiedica utilizatorii să încalce politicile de securitate a informațiilor ale companiei. Ajustarea regulată a acestor instrumente pentru a maximiza acuratețea recunoașterii amenințărilor reale, reducând în același timp numărul de rezultate fals pozitive, ar ajuta la detectarea și apărarea efectivă în fața atacurilor noi.

Managementul patch-urilor – Organizațiile ar trebui să revizuiască procesul de gestionare a patch-urilor și să extindă acest lucru la sistemele IT complete. Atacurile crescute asupra dispozitivelor IoT pot fi abordate prin includerea actualizărilor de Firmware în procesul de gestionare a patch-urilor din organizație.

Instruire și conștientizare – Oamenii reprezintă cel mai mare risc pentru orice organizație. Acțiunile lor făcute din greșeală, accident, lipsă de cunoștințe și poate ocazional cu rea intenție, duc la incidente. Oferirea de instruire periodică privind cunoștințele operaționale și campaniile de sensibilizare cu privire la conceptele de Securitate a informațiilor îi vor ajuta să contribuie la managementul securității informațiilor. Sunt incluse și cunoștințe despre gestionarea atașamentelor de email, Phishing, Vishing, Click-jack, Inginerie Socială etc. E necesară testarea periodică a eficienței instruirii de conștientizare.

Pentru persoanele fizice, cele mai bune practici sunt simple.

Vestea bună este că, în cele mai multe cazuri, unele organizații de Securitate destul de mari se află între consumator și hacker, de exemplu echipa SecOps de la Verizon sau AT&T. Există încă măsuri preventive pe care ar trebui să le luați pentru a vă garanta siguranța informațiilor și acestea sunt discutate în detaliu în următoarea secțiune a acestui document.

SUGESTII DE BUNE PRACTICI

Măsuri comune de siguranță

Parola: Pentru a împiedica utilizatorii neautorizați să se conecteze wireless la router-ul nostru, să fure conexiunea noastră la Internet și chiar să acceseze alte computere din rețeaua noastră locală, acestea sunt de obicei protejate cu o parolă. Fără aceasta, accesul nu poate fi posibil. Cu toate acestea, unele parole sunt adesea slabe și ușor de piratat. Dacă ne verificăm router-ul, cu siguranță vom găsi unul din aceste 3 elemente: admin/admin; admin/password; admin/. Odată ce a accesat router-ul nostru, hackerul are libertatea totală de a schimba parola Wi-Fi și de a ne împiedica să accesăm orice dispozitiv pe care-l folosim. Pentru a evita acest lucru, trebuie să schimbăm parola de

acces implicită a rețelei Wi-Fi livrată de furnizorul nostru de Internet. Aceste parole sunt configurate cu un algoritm disponibil oricui. Așadar, citind pur și simplu un tutorial pe internet, am putea folosi noi înșine acele informații. Prin urmare, trebuie să atribuim o parolă care să respecte toate măsurile de securitate:

- Conține litere mici, majuscule, cifre și litere.
- Nu utilizați date de naștere, nume de animale de companie, alimente preferate și alte date ușor de ghicit.

Criptare: Trebuie să fiți foarte atenți la ceea ce publicați pe rețelele sociale. Ele stochează cantități mari de informații despre activitățile pe care le desfășurați, locurile pe care le vizitați, oamenii cu care interacționați, hobby-uri, mâncare preferată etc. Toate aceste informații pot fi folosite de un atacator pentru a cunoaște profilul sau planul dvs. și de a lansa atacuri personalizate, cum ar fi phishing-ul, menționat în prima parte a acestui ghid. În plus, informațiile colectate pot fi utilizate pentru răpiri sau extorcări.

Cum se știe care aplicație este sigură? În tehnologia mobilă, majoritatea serviciilor de mesagerie precum WhatsApp, de exemplu, oferă un sistem de criptare în toate conversațiile noastre. Aceasta înseamnă că numai noi și persoana cu care comunicăm putem citi mesajele, împiedicând accesul terților. De fapt, și chiar dacă infractorul cibernetic ar putea obține toate informațiile partajate, el ar putea vedea doar coduri care nu ar putea fi descifrate.

Când navigați pe Internet, este recomandat să o faceți pe acele site-uri web unde HTTPS este plasat în bara de adrese, ceea ce oferă utilizatorului o criptare suplimentară. Când URL-ul unui website începe cu https: //, computerul dvs. este conectat la o pagină care vă vorbește într-un limbaj codificat, inaccesibil atacatorilor și mai sigur. Și trebuie să navigăm în aceste tipuri de site-uri web în special atunci când facem achiziții online, atâta timp cât acestea sunt conectate la puncte de plată electronice recunoscute, precum Visa, Mastercard, Paypal, printre altele.

Firewall-uri: Un instrument suplimentar de protecție împotriva amenințărilor de pe Internet este utilizarea unui firewall. Este pur și simplu un instrument de securitate care controlează ce aplicații au acces la Internet și ce conexiuni au permisiunea de a accesa computerul nostru. Firewall-urile sunt de obicei programate pentru a recunoaște automat amenințările, ceea ce înseamnă că sunt de obicei ușor de utilizat și nu interferează cu modul în care folosim computerul.

VPN Rețea Privată Virtuală: O altă măsură foarte bună este utilizarea VPN (Rețea Privată Virtuală), care este o tehnologie de rețea ce ne permite să creăm o rețea locală (LAN), chiar dacă navigăm de la distanță și trebuie să transmitem informațiile printr-o rețea publică. Un VPN creează un fel de tunel și împiedică ca informațiile transmise să fie accesate și utilizate de alte persoane. Astfel, ne asigurăm că tot ce iese din dispozitivele noastre este criptat până când receptorul mesajului primește acele informații. Acest lucru poate preveni atacurile de tip man-in-the-middle, un tip de amenințare în care infractorul cibernetic dobândește capacitatea de a devia sau controla comunicațiile dintre cele două părți.

Antivirus: Este esențial să ne menținem sistemul de operare actualizat și să folosim cel mai bun antivirus pentru a ne alerta și proteja împotriva posibilelor amenințări. De asemenea, este important să-l rulați periodic pentru a găsi și elimina malware, precum și pentru a efectua actualizări automate. Dacă oscilați între cumpărarea unei licențe antivirus sau obținerea uneia gratuite, trebuie să aveți în vedere că, deși majoritatea software-urilor gratuite sunt de înaltă calitate și oferă un nivel rezonabil de securitate pentru utilizatorii persoane fizice, ele nu oferă întotdeauna același nivel de protecție. Cea mai bună opțiune ar fi să consultați un expert și, dacă este posibil, să alegeți un antivirus care are suport tehnic pentru a vă ajuta cu configurația.

- Cea mai bună opțiune este să nu ne încredem în primul lucru care intră în căsuța noastră de email, în acel link care ne oferă un produs gratuit, în acel utilizator pe care nu-l cunoaștem și dorește să ne adauge la o rețea socială etc.
- Trebuie să vă gândiți de două ori înainte de a face oricare dintre aceste acțiuni – dacă este ceva prea frumos pentru a fi adevărat, atunci este foarte posibil să fie ceva fraudulos sau dăunător.
- Este întotdeauna recomandabil să utilizați filtre spam care ajută la blocarea e-mailurilor care pot conține programe malware.
- Trebuie să fiți atenți dacă cineva, chiar și un prieten cu intenții bune sau un membru al familiei, vă oferă un USB sau un CD, poate conține malware fără ca cel care vi l-a dat să știe acest lucru. Prin urmare, este esențial să scanați cu un antivirus fiecare element pe care-l introduceți în dispozitivele dvs. sau îl descărcați de pe web.
- De asemenea, trebuie să vă obișnuiți să faceți periodic copii de rezervă ale datelor care le aveți pe dispozitivele dvs., pentru a minimiza pierderile acestor date.

Dispozitive precum smartphone-uri, tablete, televizoare inteligente, electrocasnice inteligente, ca de exemplu frigidere sau cuptoare, chiar și termostate, jaluzele, uși, lumini controlate de pe telefon – acesta este Internetul Obiectelor sau IoT. În prezent, toate aceste dispozitive sunt conectate prin conexiuni Wi-Fi, Bluetooth sau infraroșu și comunică un control central care se găsește de obicei în același domiciliu sau cu un server central al producătorului. Se preconizează că vor fi mai multe dispozitive decât oameni în fiecare casă. Și aceste dispozitive joacă un rol din ce în ce mai important în viața casnică.

Totuși IoT reprezintă o provocare pentru securitate. Senzorii tuturor dispozitivelor casnice, chiar și aspiratoarele-robot care au devenit atât de cunoscute în ultimii ani, pot stoca informații valoroase despre locuințele utilizatorilor. Brandul Roomba, cunoscut pe plan internațional, stochează informații despre dimensiunile caselor, și intenționează să le vândă altor mari companii de tehnologie.

Dispozitivele IoT colectează date chiar și despre noi: știu ce programe TV urmărim, ce spunem în interiorul unei camere, la ce oră ajungem acasă etc.

PREZENTARE GENERALĂ A TENDINȚELOR VIITOARE ÎN AMENINȚĂRILE CIBERNETICE

Cât de gravă este problema criminalității informatice? Un studiu realizat de Cybersecurity Ventures prezice că aceste infracțiuni vor ajunge să coste la nivel global 6 trilioane de dolari pe an până în 2021. Infracțiunile cibernetice au devenit știri importante cu date și breșe de securitate la mari companii și amenințări cibernetice din țări precum China sau Rusia, periclitând afacerile și alegerile din SUA.

Deepfakes reprezintă o combinație a cuvintelor "deep learning" – învățare profundă și "fake" – fals. Deepfakes se întâmplă atunci când tehnologia Inteligenței Artificiale creează imagini și sunete false care par reale. Un Deepfake ar putea crea un videoclip în care cuvintele unei persoane sunt manipulate, făcând să pară că acea persoană a spus ceva ce în realitate nu a spus niciodată. Tehnologia vocală Deepfake permite oamenilor să falsifice vocile altor persoane - adesea politicieni, vedete sau directori generali – folosind Inteligența Artificială.

Identitățile Sintetice sunt o formă de fraudă a identității în care escrocii folosesc o combinație de real și artificial pentru a crea iluzia unei persoane adevărate. De exemplu, un infractor ar putea crea o identitate sintetică care să includă o adresă fizică legitimă.

Folosind Inteligența Artificială, hackerii sunt capabili să creeze programe care imită comportamentele umane cunoscute. Ei pot folosi apoi aceste programe pentru a păcăli oamenii să le furnizeze informații personale sau financiare. În aceste atacuri, cunoscute sub numele de poisoning attacks – atacuri otrăvitoare, infractorii cibernetici pot injecta date alterate într-un program AI. Aceste date alterate pot determina sistemul AI să învețe să facă lucruri pe care nu ar trebui să le facă.

Ideea de calcul cuantic este încă nouă dar**,** foarte simplu explicat, acesta este un tip de calcul ce poate utiliza anumite elemente ale mecanicii cuantice. Ceea ce este important pentru securitatea cibernetică este că aceste computere sunt rapide și puternice. Amenințarea constă în faptul că aceste computere cuantice pot descifra coduri criptografice mult, mult mai rapid comparativ cu calculatoarele tradiționale, asta dacă cele tradiționale pot realiza aceste descifrări.

Pe măsură ce mai multe autovehicule sunt conectate la Internet, amenințarea atacurilor cibernetice asupra vehiculelor crește. Îngrijorarea este că infractorii cibernetici vor putea accesa vehicule pentru a fura date cu caracter personal, urmări locația sau istoricul conducerii acestor vehicule, sau chiar dezactiva și prelua funcțiile de siguranță.

Pe măsură ce lumea continua să adopte transformarea digitală, având în vedere rata de schimbare, informația fiabilă și care permite luarea de măsuri despre un pericol devine foarte importantă. Măsurile informative comune privind amenințările sunt:

Informații bazate pe evaluări inter pares privind amenințările: Prima, și cea mai comună, se bazează pe un sondaj al liderilor de Securitate sau al unor persoane similare care întreabă despre tipurile de amenințări pe care le-au experimentat ceilalți. Această

modalitate poate fi valoroasă dacă persoanele intervievate lucrează în aceeași industrie sau locuiesc în aceeași regiune geografică.

Rapoarte privind amenințările realizate de experți: Informațiile privind amenințările nu trebuie să furnizeze numai un istoric și o analiză a tabloului amenințărilor, ci și să anticipeze potențiale puncte evolutive ale programelor malware și ale strategiilor cibernetice. Se poate începe cu rapoartele privind amenințările redactate de echipe profesionale de cercetare a amenințărilor cibernetice.

Fluxuri de amenințări și informații colectate intern: Pe lângă aceste surse de informații, liderii de Securitate trebuie să se aboneze la fluxuri live de amenințări care oferă informații importante și care permit luarea de măsuri, precum și la servicii care oferă actualizări și recomandări în timp real din partea liniilor de luptă din securitate cibernetică.

Îmbunătățirea capacității companiei de a se apăra nu numai în mod corespunzător împotriva tendințelor actuale de amenințare, ci și de a prezice un număr mare de atacuri viitoare necesită informații despre amenințări care să permită companiilor să fie proactive. Această abilitate de a "vedea viitorul" tendințelor de amenințare le permite companiilor nu numai să se apere eficient împotriva atacurilor cibernetice actuale, ci și să prevină următorul val de atacuri înainte ca acesta să apară.

TEST – INTRODUCERE ȘI PREZENTARE GENERALĂ A SIGURANȚEI CIBERNETICE

Acum, că a fost discutată prevenirea comună a amenințărilor la adresa securității cibernetice, se poate efectua o autoevaluare rapidă, după cum urmează:

16. Care **nu** este o motivație din spatele unui atac cibernetic?
    a. Perturbarea unui sistem
    b. Perturbarea serviciilor
    c. Obținerea răscumpărării
    d. Întreținerea sistemului

17. Care este/sunt măsura/măsurile luate de organizații pentru prevenirea/gestionarea amenințărilor cibernetice?
    a. Managementul Riscurilor
    b. Managementul Patch-urilor
    c. Instruirea angajaților
    d. Toate cele de mai sus

18. Care dintre următoarele este/sunt măsură/măsuri de securitate luate de persoane fizice?
    a. Utilizarea furnizorilor de servicii de mesagerie criptate
    b. Folosirea parolelor complicate
    c. Folosirea de antivirus
    d. Toate cele de mai sus

19. Care nu este cea mai bună practică legată de Parolă?
    a. Parola trebuie să conțină litere mici, majuscule, numere și litere
    b. Folosirea datelor de naștere, a numelor animalelor de companie, mâncăruri preferate sau alte date ușor de ghicit
    c. Schimbarea parolelor în mod regulat
    d. Schimbarea parolei rețelei wi-fi dacă este utilizată acasă

20. Vă rugăm să citiți enunțul și să alegeți cea mai bună opțiune pentru a descrie acest lucru: "Amenințările cibernetice evoluează constant și, prin urmare, trebuie să evolueze și modalitățile de prevenire și control al amenințării, iar oamenii trebuie să fie la curent cu evoluția măsurilor de securitate cibernetică aflate la dispoziția lor."
    a. Adevărat
    b. Fals

CAPITOLUL 5: Conformitate, Probleme Etice și Profesionale în domeniul Securității Cibernetice

Sursa: https://www.freepik.es/foto-gratis/cubos-madera-titulo-etica_3648617.htm#page=1&query=etica&position=3

INTRODUCERE

Tehnologiile nu sunt 'neutre' din punct de vedere etic, deoarece reflectă valorile pe care le includem în ele cu alegerile noastre de design, precum și valorile care ne ghidează în distribuția și utilizarea acestora. Tehnologiile dezvăluie și modelează ceea ce prețuiesc oamenii, ceea ce credem că este 'bun' în viață și merită căutat. Practicile de securitate cibernetică au ca scop securizarea — adică păstrarea în siguranță — a datelor, a sistemelor informatice și a rețelelor (software și hardware). În timp ce aceste date, sisteme și rețele ar putea avea o anumită valoare economică sau de altă natură în sine, ceea ce protejează practicile de Securitate cibernetică sunt integritatea, funcționalitatea și fiabilitatea instituțiilor/practicilor umane care se bazează pe astfel de date, sisteme și rețele.

Nu există un cod unic și detaliat de etică în materie de Securitate cibernetică care se potrivește la toate contextele și practicile; prin urmare, companiile și profesioniștii ar trebui să fie încurajați să dezvolte politici interne explicite, proceduri, ghiduri și bune practici pentru etica securității cibernetice, care să fie adaptate în mod specific propriilor activități și provocări.

Un regulament de Securitate cibernetică cuprinde directive care protejează tehnologia informației și sistemele informatice pentru a forța companiile și organizațiile să-și protejeze sistemele și informațiile împotriva atacurilor cibernetice, cum ar fi viruși, viermi informatici, cai troieni, phishing, atacuri de tip DOS, acces neautorizat (pentru furt de proprietate intelectuală sau informații confidențiale) și atacuri asupra sistemului de control. Există numeroase măsuri disponibile pentru prevenirea atacurilor cibernetice.

Au existat încercări de îmbunătățire a securității cibernetice prin reglementare și colaborare între guvern și sectorul privat pentru a încuraja îmbunătățirea voluntară a securității cibernetice. Autoritățile de reglementare din industrie, inclusiv autoritățile de reglementare din sectorul bancar, au luat în considerare riscul legat securitatea cibernetică și fie au început, fie au planificat să înceapă includerea securității cibernetice ca un aspect al verificărilor periodice.

Până la sfârșitul acestui modul veți învăța despre:

- Prezentarea generală a Reglementărilor și Conformităților privind Securitatea cibernetică necesare la nivel global și în UE.
- O privire de ansamblu asupra problemelor etice în Securitatea cibernetică
- Bune practici sugerate

PREZENTARE GENERALĂ A REGLEMENTĂRILOR ȘI CONFORMITĂȚILOR PRIVIND SECURITATEA CIBERNETICĂ NECESARE LA NIVEL GLOBAL ȘI ÎN UE

În general, conformitatea este definită ca respectarea regulilor și îndeplinirea cerințelor. În securitatea cibernetică, conformitatea înseamnă crearea unui program care stabilește controale bazate pe risc pentru a proteja integritatea, confidențialitatea și accesibilitatea informațiilor stocate, procesate sau transferate. Cu toate acestea, respectarea securității cibernetice nu se bazează pe un standard sau pe un regulament independent. În funcție de industrie, se pot suprapune diferite standarde, ceea ce poate crea confuzie și eforturi mari pentru organizații care utilizează o abordare bazată pe liste de verificare. De exemplu, în SUA, domeniul asistenței medicale trebuie să îndeplinească cerințele în conformitate cu Legea Health Insurance Portability and Accountability Act (HIPAA) – Legea privind Portabilitatea și Responsabilitatea Asigurărilor de Sănătate -, dar dacă un furnizor acceptă și plăți printr-un dispozitiv POS, atunci trebuie să îndeplinească și cerințele standardului PCI DSS - Payment Card Industry Data Security Standard. Și nu este neobișnuit ca firmele să trebuiască să respecte mai multe reglementări simultan, ceea ce face mai greoi procesul de a rămâne conforme. Acestea includ, dar nu se limitează la:

• **NIST** (National Institute of Standards and Technology) – *Institutul Național de Standarde și Tehnologie*

• **CIS Controls** (Center for Internet Security Controls) – *Centrul pentru Controale de Securitate pe Internet*

• **ISO** (International Organization for Standardization) – *Organizația Internațională de Standardizare*

• **HIPAA** (Health Insurance Portability and Accountability Act) / HITECH Omnibus Rule – *Legea privind Portabilitatea și Responsabilitatea Asigurărilor de Sănătate / Regula Omnibus HITECH*

• **PCI-DSS** (The Payment Card Industry Data Security Standard) – *Standardul de Securitate a Datelor din Industria Cardurilor de Plată*

• **GDPR** (General Data Protection Regulation) – *Regulamentul General privind Protecția Datelor*

• **CCPA** (California Consumer Privacy Act)

• **AICPA** (American Institute of Certified Public Accountants) – *Institutul American al Contabililor Publici Autorizați*

• **SOX** (Sarbanes-Oxley Act)

• **COBIT** (Control Objectives for Information and Related Technologies) – *Obiective de Control pentru Informații și Tehnologii Conexe*

• **GLBA** (Gramm-Leach-Bliley Act) – *Legea Gramm-Leach-Bliley*

• **FISMA** (Federal Information Security Modernization Act of 2014) – *Legea Federală de Modernizare a Securității Informațiilor din 2014*

• **FedRAMP** (The Federal Risk and Authorization Management Program) – *Programul Federal de Gestionare a Riscurilor și Autorizațiilor*

• **FERPA** (The Family Educational Rights and Privacy Act of 1974) – *Legea privind drepturile educaționale și confidențialitatea familiei din 1974*

• **ITAR** (International Traffic in Arms Regulations) – *Regulamentul Internațional privind Traficul de Arme*

• **COPPA** (Children's Online Privacy Protection Rule) – *Regula de Protecție a Confidențialității online a copiilor*

• **NERC CIP Standards** (NERC Critical Infrastructure Protection Standards) – *Standarde NERC pentru Protecția Infrastructurilor Critice*

Desigur, este extrem de important să fie respectate cerințele de reglementare. Companiile trebuie să respecte legile și reglementările de stat, federale și internaționale relevante pentru operațiunile lor. Nerespectarea poate duce la potențiale procese și răspundere financiară, fără a mai menționa pierderea încrederii clienților, partenerilor etc. Cu toate acestea, este costisitor, complex și necesită expertiza potrivită doar pentru a ajunge la înălțimea standardelor existente, nemaivorbind de cele noi. Rezultatul este că adesea companiile se concentrează pe îndeplinirea cerințelor minime în loc să pună în aplicare politici adecvate de Securitate cibernetică, asta însemnând că în momentul actual atacatorii sunt cu un pas înaintea apărării împotriva atacurilor, ceea ce nu este un lucru bun.

Pentru a respecta cele mai bune practici și pentru a îndeplini cerințele tehnice și de altă natură, organizațiile folosesc adesea cadrele pentru conformitatea cu securitatea cibernetică și conformitatea cu reglementările. Aceste cadre oferă cele mai bune practici și îndrumări ce ajută la îmbunătățirea securității, la optimizarea proceselor de afaceri, la îndeplinirea cerințelor de reglementare și a altor sarcini necesare pentru atingerea obiectivelor specifice de afaceri, ca de exemplu intrarea într-o nișă de piață sau vânzarea către agenții guvernamentale.

Regulile de conformitate cu reglementările stabilesc, de obicei, cerințe foarte specifice și deseori stricte pe care companiile și sectoarele industriale trebuie să le respecte, să respecte standardele stabilite și legislația existentă. Aceste cerințe pot fi numeroase și complexe – așadar cadrele concepute pentru a ajuta la îndeplinirea lor sunt o completare a bazei de resurse și cunoștințe a majorității întreprinderilor. Câteva exemple sunt ilustrate mai jos:

Documentul	Ce reglementează	Companii interesate
NIST	Cadru creat pentru a oferi un ghid personalizabil privind modul de gestionare și reducere a riscurilor legate de securitatea cibernetică prin combinarea standardelor, ghidurilor și a celor mai bune practici existente. Ajută și la încurajarea comunicării între părțile interesate, interne și externe, prin crearea unui limbaj comun al riscurilor între diferite industrii.	Este un cadru voluntar care poate fi implementat de orice organizație care dorește să-și reducă riscul general.
CIS Control	Vă protejați activele și datele organizației dvs. împotriva vectorilor de atac cibernetic cunoscuți.	Companiile care doresc să consolideze securitatea în IoT.
Familia ISO 27000	Familie de standarde care prezintă cerințele de securitate legate de menținerea sistemelor de gestionare a securității informațiilor prin implementarea controalelor de securitate.	Aceste reglementări sunt mai largi și se pot potrivi unei game extinse de companii. Toate companiile pot utiliza această familie de reglementări pentru evaluarea practicilor lor de securitate cibernetică.
Familia ISO 31000	Acest set de reglementări guvernează principiile de implementare și de gestionare a riscurilor.	Aceste reglementări sunt largi și sunt indicate unei game mari de companii. Toate companiile pot utiliza această familie de reglementări pentru evaluarea practicilor lor de securitate cibernetică.
HIPAA/ HITECH	Acest act e o lege în două părți. Titlul I protejează asistența medicală a persoanelor care trec de la un loc de muncă la altul sau sunt concediate. Titlul II e menit să simplifice procesul de asistență medicală prin trecerea la date electronice. Protejează și confidențialitatea pacienților individuali. Acest lucru a fost extins și mai mult prin regula HITECH / Omnibus.	Orice organizație care gestionează date privind asistența medicală. Aceasta include, dar nu se limitează la, cabinete medicale, spitale, companii de asigurări, asociați afaceri și angajatori.
PCI-DSS	Un set de 12 reglementări menite să reducă frauda și să protejeze informațiile despre cardul de credit al clienților.	Companii care manipulează informații despre carduri de credit.

GDPR	Acesta reglementează protecția datelor și confidențialitatea cetățenilor Uniunii Europene.	Orice companie care desfășoară afaceri în Uniunea Europeană sau care manipulează datele unui cetățean al Uniunii Europene.
CCPA	Drepturile de confidențialitate și protecția consumatorilor pentru rezidenții din California.	Orice companie, inclusiv orice entitate cu scop lucrativ, care face afaceri în California și colectează datele personale ale consumatorilor.
AICPA SOC2	Securitatea, disponibilitatea, integritatea procesării și confidențialitatea sistemelor care prelucrează datele utilizatorilor și confidențialitatea acestor sisteme.	Organizații de servicii care procesează datele utilizatorilor.
SOX	Acest document impune companiilor să păstreze evidențe financiare pentru o perioadă de până la 7 ani. A fost implementat pentru a preveni un alt scandal Enron.	Consiliile de administrație ale companiilor publice din SUA, societățile de administrare și societățile publice de contabilitate.
COBIT	Acest cadru a fost dezvoltat pentru a ajuta organizațiile să gestioneze informațiile și tehnologia prin interconectarea obiectivelor de afaceri și IT.	Organizațiile care sunt responsabile cu procesele de afaceri legate de tehnologie și controlul calității informațiilor. Aceasta include, dar nu se limitează la, domenii precum audit și asigurare, conformitate, operațiuni IT, guvernare și gestionarea securității riscurilor.
GLBA	Acest act a permis firmelor de asigurări, băncilor comerciale și băncilor de investiții să se afle în aceeași companie. În ceea ce privește securitatea, acesta impune companiilor să securizeze informațiile private ale clienților.	Prezentul act definește "instituțiile financiare" astfel: "…companiile care oferă produse sau servicii financiare persoanelor fizice, cum ar fi împrumuturi, consultanță financiară sau de investiții, sau asigurări."
FISMA	Acest act recunoaște securitatea informațiilor ca o chestiune de securitate națională. Astfel, se impune ca toate agențiile federale să dezvolte o metodă de protejare a sistemelor lor de informații.	Toate agențiile federale intră sub incidența acestui proiect de lege.
FedRAMP	Servicii Cloud în cadrul guvernului federal.	Departamentele și agențiile executive.
FERPA	Secțiunea 3.1 a actului se referă la protejarea dosarelor educaționale ale elevilor.	Orice instituție post-secundară, care include, dar nu se limitează la, academii, colegii, seminarii, școli tehnice, școli profesionale.
ITAR	Controlează vânzarea articolelor de apărare și a serviciilor de apărare (oferind capacități militare sau de informații critice).	Oricine produce sau vinde echipamente pentru apărare sau servicii de apărare.

COPPA	Colectarea online a informațiilor personale despre copiii cu vârsta sub 13 ani.	Orice persoană sau entitate aflată sub jurisdicția USA.
Standarde NERC CIP	Îmbunătățirea securității sistemului energetic din America de Nord.	Toți proprietarii și operatorii de sisteme energetice.

PREZENTARE GENERALĂ A PROBLEMELOR ETICE ÎN SECURITATEA CIBERNETICĂ

Baza tuturor sistemelor de securitate este formată din principiile morale, din practici ale persoanelor implicate și din standardele profesiei. Adică, în timp ce oamenii fac parte din soluție, ei sunt, de asemenea, cea mai mare problemă. Problemele de securitate cu care o organizație ar avea de-a face includ luarea de decizii responsabile, confidențialitate, prioritizare, piraterie, fraudă și abuz, răspundere, drepturi de autor, secrete comerciale, sabotaj. Această metaforică cursă a înarmării nu dă semne de încetinire având în vedere că tehnologii interconectate sunt integrate și mai mult în viața profesională.

Personalul de securitate IT are adesea acces la date confidențiale și cunoștințe despre rețelele și sistemele persoanelor fizice și ale companiilor, fapt ce le oferă o mare putere. De această putere se poate abuza, în mod deliberat sau involuntar. Nu există standarde obligatorii pentru problemele cibernetice pe care profesioniștii în securitate cibernetică să fie obligați să le respecte. De fapt, mulți profesioniști IT nici măcar nu realizează că locurile lor de muncă implică probleme etice. Cu toate acestea, ei iau zilnic decizii care ridică întrebări de natură etică. Multe din problemele etice implică protecția vieții private. De exemplu:

- Ar trebui să citiți e-mail-ul privat al utilizatorilor de rețea doar pentru că puteți? Este corect să citiți e-mail-ul angajaților ca măsură de securitate pentru a vă asigura că informațiile sensibile ale companiei nu sunt dezvăluite? Este bine să citiți e-mail-ul angajaților pentru a vă asigura că regulile companiei (de exemplu, împotriva utilizării personale a sistemului de e-mail) nu sunt încălcate? Dacă citiți e-mail-ul angajaților, ar trebui să le divulgați acest lucru? Înainte sau după fapt?
- Este bine să monitorizați site-urile web vizitate de utilizatorii dvs. de rețea? Ar trebui să păstrați în mod obișnuit jurnalele site-urilor vizitate? Este neglijent să nu se monitorizeze o astfel de utilizare a internetului pentru a preveni posibilitatea pornografiei la locul de muncă care ar putea crea un mediu de lucru ostil?
- Este normal să plasați programe Key Logger pe dispozitivele din rețea pentru a captura tot ceea ce scrie utilizatorul? Dar despre programele de captură ecran, astfel încât să puteți vedea tot ce este afișat pe display? Ar trebui să fie informați utilizatorii că sunt urmăriți în acest fel?
- Este corect să citiți documentele și să priviți fișierele grafice care sunt stocate pe computerele utilizatorilor sau în directoarele lor de pe serverul de fișiere?

Amintiți-vă că nu este vorba de întrebări legale aici. O companie poate avea foarte bine dreptul legal de a monitoriza tot ceea ce face un angajat cu echipamentele sale informatice. E vorba despre aspectele etice ale capacității de a face acest lucru.

Un concept comun în orice discuție etică este "**panta alunecoasă".** Acest lucru se referă la ușurința cu care o persoană poate trece de la a face ceva care nu pare cu adevărat lipsit de etică, cum ar fi scanarea email-urilor angajaților "doar pentru distracție," la a face lucruri din ce în ce mai lipsite de etică, cum ar fi efectuarea de mici modificări în mesajele de email ale angajaților, sau redirecționarea lor către destinatari greșiți. Conceptul de pantă alunecoasă poate merge dincolo de utilizarea abilităților de IT ale persoanei respective. Dacă este bine să citească email-ul altor angajați, este atunci în regulă să le umble prin sertarele biroului atunci când ei lipsesc? Sau să le deschidă servietele sau poșetele?

Apoi există probleme legate de bani. Proliferarea atacurilor de rețea, pirateriei, a virușilor și a altor amenințări la adresa infrastructurilor IT au determinat multe companii "să se teamă, să se teamă foarte mult". În calitate de consultant de Securitate, poate fi foarte ușor să joci pe această temere și să convingi companiile să cheltuie mult mai mulți bani decât au nevoie. Este greșit să percepeți sute sau chiar mii de dolari pe oră pentru serviciile dvs., sau este vorba despre "orice poate să suporte piața".

O altă problemă etică presupune să promiți mai mult decât poți livra sau să manipulezi date pentru a obține taxe mai mari. Puteți instala tehnologii sau configura setări pentru a face rețeaua unui client mai sigură, dar niciodată nu o puteți face complet sigură.

SUGESTII DE BUNE PRACTICI

Niciun cod unic, detaliat de etică a securității cibernetice nu poate fi adaptat tuturor contextelor și practicienilor; prin urmare, companiile și profesioniștii ar trebui încurajați să dezvolte politici interne explicite, proceduri, ghiduri și bune practici pentru etica securității cibernetice, care sunt adaptate în mod specific propriilor activități și provocări. Unele dintre ele sunt sugerate mai jos:

- **Mențineți etica în materie de securitate cibernetică în centrul atenției:** Etica este un aspect general al practicii de securitate cibernetică. Datorită imensei puteri sociale a tehnologiei informației, problemele etice sunt practic totdeauna în joc atunci când ne străduim să menținem această tehnologie și funcționarea sa în condiții de siguranță.
- **Luați în considerare viețile și interesele umane din spatele sistemelor:** În contexte tehnice, se pot pierde ușor din vedere modalitățile de îmbunătățire a vieții și protejarea intereselor umane.
- **Stabiliți lanțuri de responsabilitate etică:** În cadrul organizației, 'problema mai multor mâini' este o provocare constantă pentru o practică responsabilă și responsabilitate.
- **Practicați Securitatea cibernetică în caz de dezastru și răspuns la criză:** Majoritatea oamenilor nu doresc să anticipeze eșecul sau criza; vor să se concentreze asupra potențialului pozitiv al unui proiect sau sistem.

- **Promovarea transparenței, autonomiei și credibilității:** Este important să se mențină o relație sănătoasă între practicienii din domeniul securității cibernetice și public, este indicat să se înțeleagă importanța transparenței, a autonomiei și a credibilității.
- **Faceți ca reflecțiile și practica etice să fie standard, generalizate, iterative și satisfăcătoare:** reflecțiile și practica etice, așa cum am spus deja, sunt o parte esențială și centrală a excelenței profesionale în securitatea cibernetică.

Unele din cele mai bune practici în materie de etică în domeniul securității cibernetice

Practicați Auto-Reflecția/Examinarea: aceasta implică petrecerea timpului în mod regulat gândindu-vă la persoana care doriți să deveniți, în raport cu persoana care sunteți astăzi.

- **Căutați exemple morale:** Mulți dintre noi petrecem o mare parte din timp, adesea mai mult decât ne dăm seama, judecând deficiențele altora.
- **Recunoașteți propria forță morală:** În cea mai mare parte, trăind bine în sens etic face viața mai ușoară, nu mai grea.
- **Căutați compania altor persoane morale:** Mulți au remarcat importanța prieteniei în dezvoltarea morală; în secolul al IV-lea î.e.n., filozoful grec Aristotel a susținut că un prieten virtuos poate fi un 'al doilea eu,' care reprezintă însăși calitățile caracterului pe care-l prețuim și aspirăm să-l păstrăm în noi înșine.

Sursa: https://unsplash.com/s/photos/meditation

TEST – INTRODUCERE ȘI PREZENTARE GENERALĂ A SECURITĂȚII CIBERNETICE

Acum, după ce s-a discutat despre etică și conformitate legate de securitatea cibernetică, se poate efectua o autoevaluare rapidă, după cum urmează:

21. Ce aspecte ale instituțiilor/practicilor umane protejează securitatea cibernetică (prin protejarea datelor conexe)?
    a. Integritate
    b. Funcționalitate
    c. Fiabilitate
    d. Întreținerea sistemului

22. Vă rugăm să examinați declarația și să alegeți cea mai bună opțiune pentru a descrie acest lucru: "Un regulament de securitate cibernetică cuprinde directive care protejează tehnologia informației și sistemele informatice cu scopul de a obliga companiile și organizațiile să își protejeze sistemele și informațiile împotriva atacurilor cibernetice"?
    a. Adevărat
    b. Fals

23. Care dintre următoarele este/sunt cele mai bune practici de etică a securității cibernetice?
    a. Practicarea Auto-Reflecției/Examinarea
    b. Căutarea exemplelor morale
    c. Compania altor persoane morale
    d. Toate cele de mai sus

24. Care dintre următoarele reglementări se aplică Uniunii Europene?
    a. CCPA (California Consumer Privacy Act)
    b. GDPR (Regulamentul General privind Protecția Datelor)
    c. COPPA (Regula de protecție a confidențialității online a copiilor)
    d. SOX (Sarbanes-Oxley Act)

25. Vă rugăm să citiți declarația și să alegeți cea mai bună opțiune pentru a descrie acest lucru: " Tehnologiile nu sunt 'neutre' din punct de vedere etic, deoarece reflectă valorile pe care le includem în ele cu alegerile noastre de design, precum și valorile care ne ghidează în distribuția și utilizarea acestora".
    a. Adevărat
    b. Fals