

GHID SECURITATE CIBERNETICĂ

PENTRU PROFESORI ȘI ELEVII

AUTORI

Alice Georgescu

Daniela Ionescu

ACUM TOȚI SUNTEM
CONECTAȚI PRIN INTERNET

Editura Casa Corpului Didactic Prahova

Ploiești, 2024

autori

Georgescu Alice

Ionescu Daniela

GHID DE SECURITATE CIBERNETICĂ PENTRU PROFESORI ȘI ELEVI

Toate drepturile asupra prezentei ediții aparțin

Editurii Casa Corpului Didactic Prahova

Ediție publicată de Editura Casa Corpului Didactic Prahova

Adresa: Ploiești, Str. Democrației, Nr. 35

Tel./Fax: 0244577338

Email: edituraccdprahova@ccdph.ro

ISBN 978-606-047-258-2

Ploiești, 2024

CUPRINS:

Prefață	5
Partea I Cum ne apărăm ca simpli utilizatori ai internetului	6
Cronologia securității cibernetice	7
Capitolul 1 Elemente de bază ale securității cibernetice	18
1.1 Importanța securității cibernetice în era digitală	18
1.2 Amenințări cibernetice comune: viruși, programe malware și phishing.....	23
1.3 Impactul amenințărilor cibernetice asupra utilizatorilor obișnuiți: studii de caz și statistici	25
1.4 Concepte de bază ale siguranței online: HTTPS, firewall-uri și VPN-uri.....	26
Capitolul 2 Practici sigure pentru utilizatorii de internet.....	29
2.1 Crearea de parole puternice și utilizarea managerilor de parole.....	29
2.2 Identificarea și evitarea înșelătoriilor de tip phishing: semnale roșii și bune practici	30
2.3 Tehnici de navigare sigură: site-uri web sigure, navigare privată și extensii de browser.....	32
2.4 Protejarea informațiilor personale online: setări de confidențialitate și criptare a datelor	34
Capitolul 3 Instrumente și resurse pentru securitate cibernetică	37
3.1 Utilizarea software-ului antivirus și anti-malware: selecție și întreținere.....	37
3.2 Activarea autentificării în doi factori (2FA) pentru conturi și dispozitive.....	39
3.3 Actualizări regulate de software și corecții: importanță și bune practici.....	40
3.4 Rămâneți informat cu privire la evoluțiile securității cibernetice: știri, bloguri și resurse educaționale deschise.....	42
Partea a II-a Ghid Practic	46
Capitolul 4 Lumea securității cibernetice	47
4.1 Elementele de bază ale securității cibernetice	47
4.2 Tendințe cheie în securitatea cibernetică.....	51
4.3 Provocări în securitatea cibernetică.....	52
4.4 Viitorul securității cibernetice	54
Capitolul 5 Victime și Atacatori	55
5.1 Identitatea online	55

5.2 Încălări ale securității datelor în mediul organizațional	56
5.3 Exemple de încălări ale securității datelor.....	56
5.4 Atacatorii cibernetici	58
5.5 Nivelurile de abordare a atacului cibernetic	63
Capitolul 6 Protejarea informațiilor și confidențialitatea datelor personale	67
6.1 Date cu caracter personal.....	67
6.2 Cadrele juridice care guvernează proprietatea datelor	69
6.3 Provoări în defnirea proprietății datelor și controlul acestora.....	71
6.4 Să verificăm - Conectarea	74
6.5 Să verificăm – Prezența în mediul online	75
Capitolul 7 Protejarea informațiilor și confidențialitatea datelor în cazul organizațiilor	79
7.1 Strategii.....	79
7.2 Sfaturi pentru școli (administratori și departamente IT)	83
7.3 Sfaturi pentru profesori	83
7.3 Sfaturi pentru elevi/copii.....	84
7.4 Sfaturi pentru părinți	85
Bibliografie	86

Prefață

Într-o eră în care tehnologia digitală a devenit o parte integrantă a vieții noastre, securitatea cibernetică nu mai este un lux, ci o necesitate fundamentală. Cartea de față, „Ghid de securitate cibernetică pentru profesori și elevi”, reprezintă un demers esențial în educația și protejarea utilizatorilor de internet, în special a celor care activează în mediul educațional.

Acest ghid oferă o explorare profundă a lumii securității cibernetică, având ca scop echiparea profesorilor și elevilor cu cunoștințele necesare pentru a naviga în siguranță pe internet. Lucrarea este structurată în două părți: una teoretică, care explică fundamentele securității online, și una practică, ce include recomandări concrete și studii de caz din lumea reală.

Pe măsură ce școlile și universitățile adoptă tehnologiile digitale pentru a sprijini procesul educațional, riscurile asociate devin tot mai complexe și variate. Elevii și cadrele didactice sunt vulnerabili la atacuri de tip phishing, malware și alte amenințări cibernetică, care pot compromite date personale și chiar integritatea procesului educațional. De aceea, această carte este mai mult decât un simplu ghid; este un apel la conștientizare și responsabilitate în fața unui peisaj digital tot mai imprevizibil.

Prin exemple clare, soluții practice și recomandări ușor de înțeles, această lucrare contribuie la dezvoltarea unei culturi a securității cibernetică în rândul tinerilor și al educatorilor, punând accent pe importanța educației continue și a adoptării măsurilor preventive. Sperăm ca acest ghid să inspire cititorii să își asume un rol proactiv în protejarea informațiilor digitale, transformându-se în adevărați „gardieni” ai securității cibernetică în comunitățile lor.

Cu speranța că fiecare cititor va învăța să se protejeze mai bine în mediul online, vă invităm să explorați acest ghid cu deschidere și curiozitate, știind că fiecare pas spre o mai bună securitate cibernetică este un pas spre un viitor mai sigur.

Autorii

PARTEA I

CUM NE APĂRĂM

CA SIMPLI UTILIZATORI

AI INTERNETULUI

IONESCU DANIELA

Evoluția securității cibernetice a devenit din ce în ce mai vitală într-o lume interconectată, cu amenințările emergente care determină atât indivizii, cât și organizațiile să adopte poziții sigure în peisajul digital. Acest ghid analizează atât contextul istoric al securității cibernetice, examinând în special călătoria de la software-ul antivirus de bază și firewall-urile tradiționale la tehnologii avansate, cum ar fi firewall-urile de generație următoare (NGFW) și sistemele de detectare bazate pe învățarea automată, dar și sfaturi practice pentru profesori și elevi. Întrebarea principală de cercetare — „Ce putem face pentru a adopta o poziție sigură?” — ghidează explorarea diferitelor măsuri de securitate cibernetică, inclusiv implementarea unor politici solide de protecție a datelor, importanța unor programe riguroase de formare și conștientizare și necesitatea colaborării dintre noi. Discuția evidențiază incidente critice, cum ar fi atacurile Stuxnet și WannaCry, pentru a sublinia nevoia presantă de strategii de securitate adaptive. Concluziile extrase din analiză subliniază faptul că o abordare proactivă, combinată cu monitorizarea continuă, inovația în tehnologie și educația și formarea utilizatorilor, este esențială pentru menținerea unei poziții cibernetice sigure în fața amenințărilor în continuă evoluție. Astfel, promovarea unei înțelegeri cuprinzătoare a securității cibernetice și a aplicațiilor sale este esențială atât pentru organizații, cât și pentru persoanele care navighează în acest mediu complex.

Cuvinte cheie: securitate cibernetică, evoluție, poziție sigură, protecția datelor, informații despre amenințări, monitorizare continuă, program de formare.

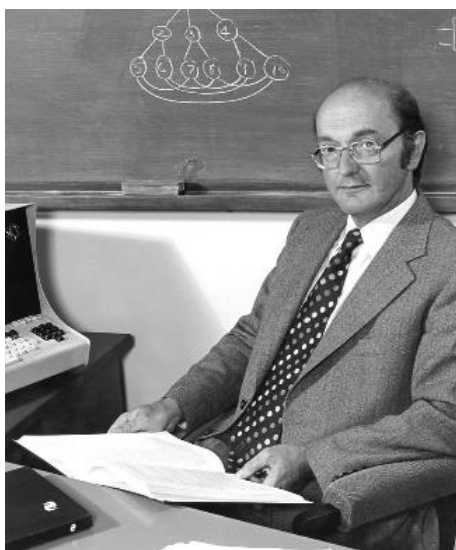
Cronologia securității cibernetice

Iată o privire asupra cronologiei securității cibernetice, subliniind etapele esențiale, descoperirile și evenimentele semnificative care au modelat peisajul securității digitale:

1960 și 1970: Anii de început

Conceptul de securitate a calculatoarelor a apărut între anii 1960 și 1970, când cercetătorii au pus bazele ideilor care ar sta la baza transmiterii securizate a datelor. De la primii viruși de calculator la soluțiile lor corespunzătoare, cursa ”înarmării” în securitatea cibernetică începuse.

1965: Comutarea de pachete, propusă de Donald Davies, presupune împărțirea datelor în unități mai mici numite pachete pentru a fi transmise prin rețele. Aceste pachete pot urma rute diferite și sunt mai puțin susceptibile la interceptare.



Donald Davies, Computerul britanic este o fotografie de Science Photo Library, 6 martie, 2014.

Donald Davies

Un om de știință galez în domeniul calculatoarelor care a propus conceptul de comutare de pachete în 1965, concept care a devenit fundamentul pentru rețelele de calculatoare moderne și securitatea pe internet. Ideile sale au pus bazele transmiterii securizate a datelor.

1969: Departamentul de Apărare al SUA stabilește ARPANET, un precursor al Internetului. Deși inițial destinat cercetării, ARPANET reprezintă prima încercare reușită de a permite calculatoarelor să comunice și să partajeze informații.

Bob Thomas



Bob Thomas, un informatician renumit, este recunoscut pe scară largă drept „Părintele securității cibernetice” pentru contribuțiile sale la securitatea computerelor. Născut în 1943, Thomas și-a început cariera la Massachusetts Institute of Technology (MIT) la sfârșitul anilor 1960. Thomas a descoperit că programele de calculator pot ”călători” prin rețele. El a dezvoltat unele dintre primele protocoale și practici de securitate care sunt folosite și astăzi. Faima lui Thomas a venit în 1971, când a creat primul virus de computer cunoscut, programul „Creep”.

Deși virusul Creeper nu trebuia să fie rău intenționat, crearea sa a servit ca un eveniment special în istoria securității cibernetice. În loc să caute să provoace rău, intenția lui Thomas a fost să studieze comportamentul și propagarea codului auto-replicator. Pe lângă munca sa asupra virușilor, Thomas a contribuit semnificativ la criptografie și la protocoalele de securitate a rețelei. De asemenea, studiile sale privind găsirea punctelor slabe și detectarea modelelor de acces neautorizat au fost esențiale pentru a face sistemele digitale mai sigure.

Contribuțiile lui Thomas la securitatea computerelor au fost revoluționare, ideile sale au ajutat la protejarea a nenumărate sisteme informatice, rețele și informații sensibile de amenințările cibernetice. Impactul său în domeniu se face simțit și astăzi, iar moștenirea sa continuă să inspire noile generații de profesioniști în securitate cibernetică.

În anii 1970, Bob Thomas a fost coautor a două lucrări influente despre securitatea computerelor. Prima lucrare, „Protection in Operating Systems”, a abordat nevoia de măsuri de securitate în sistemele de operare. A doua lucrare, „A Hardware Architecture for Implementing Protection Rings”, a propus o abordare bazată pe hardware pentru implementarea inelelor de securitate. Aceste documente au pus bazele securității computerelor moderne.

1971: Primul virus de calculator este creat. CREEPER este un program ce se multiplică singur conceput să infecteze computerele PDP-10 de la DEC și să afișeze mesajul „I'M THE CREEPER: CATCH ME IF YOU CAN.” REAPER, primul antivirus, a fost creat pentru a elimina CREEPER din computerele infectate.

Ray Tomlinson



Tomlinson a creat programul REAPER, considerat primul software antivirus, conceput pentru a elimina virusul CREEPER din sistemele infectate, deschizând astfel era măsurilor de contracarare a securității informatice.

1976: Protocolul de schimb de chei Diffie-Hellman revoluționează criptografia și comunicarea securizată. Acest protocol permite părților să stabilească o cheie secretă comună printr-un canal nesecurizat, deschizând calea pentru tehnicile moderne de criptare.

Anii 1980: Epoca antivirusului și amenințările emergente.

Anii 1980 au marcat apariția erei antivirusului, pe măsură ce virușii de calculator s-au proliferat. Odată cu introducerea primelor programe antivirus, cum ar fi VirusScan de John McAfee, au început eforturile de a combate noile amenințări, punând bazele luptei continue între apărătorii cibernetici și atacatori.

1983: Atacul informatic asupra sistemelor ARPANET de către grupul de hackeri 414 evidențiază vulnerabilitatea primelor rețele de calculatoare. Acesta a dus la intensificarea preocupărilor de securitate, determinând organizațiile să-și reevalueze strategiile de apărare digitală.

1987: Virusul Vienna, un virus simplu care distruge fișiere la întâmplare, devine primul virus cunoscut care este eliminat de un program antivirus.



John McAfee

Un programator britanico-american care a fondat prima companie de software antivirus comercială, **McAfee Associates**, în 1987, revoluționând lupta împotriva malware-ului¹ și virușilor.

1987: Primul software antivirus comercial, dezvoltat de McAfee Associates, ajunge pe piață. Odată cu lansarea sa, utilizatorii obțin un instrument esențial pentru combaterea noilor amenințări digitale, marcând un progres semnificativ în crearea unor sisteme informatice mai sigure.

¹ Malware este termen rezultat din contragerea cuvintelor „malicious” și „software”. Malware-ul, prin definiție, este orice software conceput în mod intenționat pentru a deteriora sau exploata sistemele informatice, rețelele și diverse dispozitive. Fiind adesea dezvoltat de infractorii cibernetici, scopul acestuia este să perturbe funcționarea normală a mediilor digitale. <https://www.bitdefender.com/ro-ro/business/infozone/what-is-malware>

1988: Viermele **Morris**, creat de **Robert Tappan Morris**, a fost un experiment inofensiv care a luat o întorsătură greșită, scoțând la iveală vulnerabilități în primele versiuni ale internetului. Daunele exacte sunt greu de cuantificat, dar cifrele inițiale porneau de la 100.000 de dolari și au crescut rapid până la milioane.



Robert Tappan Morris

Un om de știință american în domeniul calculatoarelor, faimos pentru crearea primului *vierme* informatic în 1988, a evidențiat neintenționat vulnerabilitățile de securitate ale rețelelor, asigurându-i lui Morris un loc în istoria calculatoarelor. Ulterior, el a co-fondat mai multe companii de tehnologie de succes și a devenit o figură respectată în domeniul științei calculatoarelor.

Anii 1990: Criminalitate cibernetică și standarde de securitate

Pe măsură ce internetul a fost adoptat pe scară largă în anii 1990, istoria securității cibernetice a intrat într-o nouă eră. Interconectivitatea rețelelor globale a adus oportunități fără precedent, dar a introdus și noi amenințări cibernetice. În această perioadă, infractorii cibernetici au devenit din ce în ce mai sofisticăți, exploataând vulnerabilitățile software-ului și ale sistemelor pentru a obține acces neautorizat, a fura date și a perturba operațiunile.

1991: Apare virusul **Polymorphic**, capabil să se modifice pentru a evita detectarea, reprezentând o provocare semnificativă pentru soluțiile antivirus tradiționale.

1995: Prima versiune a **Standardului de Criptare a Datelor (DES)** este adoptată pentru a asigura comunicațiile electronice, marcând un reper în criptografie și punând bazele standardelor moderne de criptare pentru protejarea datelor sensibile în era digitală.



Kevin Mitnick

Un fost hacker cunoscut pentru infracțiunile sale cibernetice de mare notorietate din anii 1990, inclusiv fraude prin telefon și hacking de calculatoare. Exploatările sale au crescut gradul de conștientizare în privința securității cibernetice, ducând la înăsprirea legilor și îmbunătățirea măsurilor de securitate.

1999: Virusul Melissa, creat de David Lee Smith, se răspândește rapid pe internet și câștigă notorietate ca fiind *infectarea* cu cea mai rapidă răspândire din acea perioadă. A provocat daune estimate la 80 de milioane de dolari, obligând organizațiile să investească masiv în eforturile de curățare și reparare pentru a-i atenua impactul extins asupra sistemelor de calculatoare afectate.

Anii 2000: Atacuri cibernetice și *conformitate*

În anii 2000, securitatea cibernetică s-a confruntat cu o creștere a atacurilor cibernetice, determinând organizațiile să prioritizeze conformitatea cu reglementările și standardele. Această perioadă a cunoscut o creștere a breșelor de securitate de mare amploare, subliniind importanța unor măsuri de securitate solide pentru a proteja datele sensibile.

2000: Virusul “Love Bug” se răspândește global, provocând daune de ordinul miliardelor și stimulând măsuri îmbunătățite de securitate.

2001: Viermele **Code Red** exploatează o vulnerabilitate în serverele web IIS de la Microsoft, ducând la întreruperi pe scară largă ale serviciilor de internet. Acest incident a determinat un efort concentrat pentru îmbunătățirea securității software-ului și dezvoltarea unor practici mai robuste de gestionare a patch-urilor pentru a preveni exploatările similare în viitor.

2003: Viermele SQL Slammer exploatează o vulnerabilitate în software-ul de baze de date SQL Server de la Microsoft, provocând întreruperi semnificative ale serviciilor de internet. Ca răspuns, organizațiile prioritizează măsurile de securitate a bazelor de date pentru a reduce riscul de exploatare de către infractorii cibernetici.

2006: Sunt stabilite reglementările de conformitate HIPAA și PCI-DSS. Aceste reglementări, destinate protejării datelor sensibile din sectorul medical și financiar, respectiv, stimulează adoptarea pe scară largă a măsurilor de securitate cibernetică în sectoarele de sănătate și finanțe.

Anii 2010: Securitatea în cloud și amenințările susținute de state

Anii 2010 au marcat o trecere către *computarea* în cloud, determinând o atenție sporită asupra măsurilor de securitate în cloud. Simultan, a apărut o creștere a amenințărilor cibernetice susținute de state, subliniind necesitatea unor eforturi colaborative pentru a apăra împotriva provocărilor digitale în evoluție.

2010: Apariția viermelui Stuxnet, care țintește sistemele de control industrial, evidențiază riscurile asociate războiului cibernetic.

2013: Breșa de date de la Target expune 40 de milioane de carduri de credit, subliniind necesitatea unei securități mai bune în comerțul cu amănuntul. Acest incident a accentuat necesitatea urgentă ca cei care lucrează în acest domeniu să investească în măsuri solide de securitate cibernetică pentru a proteja informațiile sensibile ale clienților.



Edward Snowden

Un specialist american în domeniul calculatoarelor și fost angajat al CIA, care, în 2013, a dezvăluit informații clasificate de la Agenția Națională de Securitate (NSA). El a expus programe de supraveghere globală, declanșând dezbateri în jurul confidențialității, abuzului de

putere al guvernului și echilibrului dintre securitatea națională și libertățile civile în domeniul securității cibernetice.

2017: Atacurile de tip ransomware WannaCry și NotPetya provoacă haos la nivel global, vizând mii de organizații din diverse sectoare și cauzând pagube de miliarde de dolari.

Anii 2020 și mai departe: Inteligența artificială, calculul cuantic și altele

În anii 2020 și mai departe, securitatea cibernetică a evoluat rapid pentru a combate amenințările cibernetice în creștere. Inovații precum detectarea amenințărilor bazată pe AI și criptografia rezistentă la calculul cuantic au apărut pentru a întări strategiile de apărare. Colaborarea dintre specialiști, autorități și mediul academic este esențială pentru protejarea activelor digitale în fața amenințărilor în continuă evoluție.



Parisa Tabriz

O expertă americană în securitatea calculatoarelor, care în prezent ocupă funcția de șef al securității informaționale la Google. Tabriz a contribuit semnificativ la securitatea browserelor, cercetarea vulnerabilităților și promovarea diversității în domeniul securității cibernetice.

2022: ChatGPT demonstrează potențialul inteligenței artificiale în securitatea cibernetică pentru detectarea și răspunsul la amenințări. Acest moment a arătat capacitatea AI de a augmenta abilitățile umane, permițând practici de securitate cibernetică mai eficiente și mai eficiente.

2023: Algoritmi de criptare **rezistenți la calculul cuantic** sunt dezvoltati pentru a pregăti terenul pentru apariția calculului cuantic. Proiectați pentru a rezista vulnerabilităților criptografice pe care computerele cuantice le-ar putea exploata, acești algoritmi asigură securitatea continuă a datelor sensibile în fața unei tehnologii în continuă dezvoltare.



Katie Moussouris

Fondatoarea și CEO-ul companiei **Luta Security**, specializată în coordonarea vulnerabilităților și ”programe de recompensare a descoperirii de bug-uri²” (bug bounty). Moussouris este o pionieră în domeniul divulgării vulnerabilităților și a jucat un rol esențial în construirea unei punți între hackerii etici și organizații.

În continuare: Integrarea AI, a învățării automate și a tehnologiilor emergente continuă să modeleze viitorul securității cibernetice. Sistemele de detectare a amenințărilor bazate pe AI, combinate cu progrese în domenii precum analiza comportamentală și detectarea anomaliilor, sporesc capacitatea organizațiilor de a detecta și de a atenua amenințările cibernetice în timp real. Această evoluție continuă subliniază importanța utilizării tehnologiilor de vârf pentru a rămâne cu un pas înaintea adversarilor cibernetici din ce în ce mai sofisticăți și pentru a proteja în mod eficient activele digitale.

Construirea unui viitor digital sigur cu pregătire și formare în securitatea cibernetică

Istoria securității cibernetice ne reamintește nevoia constantă de vigilență, inovație și colaborare în fața amenințărilor cibernetice în continuă evoluție. Înțelegând lecțiile trecutului

² virus

și adoptând cele mai recente avansuri în securitatea cibernetică, ne putem pregăti mai bine pentru provocările viitoare.

Începutul și evoluția tehnologiilor de securitate cibernetică, cum ar fi firewall-urile și software-ul antivirus, au fost monumentale în modelarea peisajului de apărare digitală de astăzi. Inițial, obiectivul principal a fost de a crea o barieră care ar putea împiedica accesul neautorizat la sisteme și rețele. Călătoria a început cu dezvoltarea firewall-urilor tradiționale, care au fost concepute pentru a gestiona și controla traficul de rețea de intrare și de ieșire pe baza unor reguli de securitate predefinite (Terentyev et al., 2021). De-a lungul anilor, firewall-urile au suferit transformări semnificative pentru a aborda amenințările cibernetică în evoluție, culminând cu apariția firewall-ului „next generation” (NGFW).

Firewall-urile timpurii funcționau în principal ca filtre de pachete, gateway-uri la nivel de program sau gateway-uri la nivel de circuit. Firewall-ul de filtrare a pachetelor, una dintre cele mai vechi variante, a inspectat antetele pachetelor care traversau rețeaua pentru a le accepta sau a le respinge pe baza unor criterii predeterminate. Această metodă, deși eficientă pentru controlul de bază al traficului, a fost insuficientă împotriva amenințărilor mai sofisticate care au apărut odată cu complexitatea tot mai mare a mediilor în rețea (Terentyev et al., 2021). Gateway-urile la nivel de program, cunoscute și ca servere proxy, au acționat ca intermediari între utilizatori și serviciile pe care le accesau, oferind capacități suplimentare de control și monitorizare. În ciuda acestor îmbunătățiri, firewall-urile timpurii erau încă limitate de incapacitatea lor de a inspecta în profunzime încărcăturile utile, lăsând rețelele vulnerabile la o varietate de vectori de atac.

Pentru a aborda aceste limitări, a fost introdus conceptul de NGFW. NGFW-urile au combinat mecanismele tradiționale de filtrare cu funcționalități mai avansate, cum ar fi controlul aplicațiilor, sistemele de prevenire a intruziunilor (IPS) și capacitățile de inspecție aprofundată (Terentyev et al., 2021). Această integrare a permis NGFW-urilor să detecteze și să blocheze amenințările complexe, inclusiv malware și exploit-uri³ pe care firewall-urile tipice

³ Un exploit este o bucată de software, un bloc de date sau o secvență de comenzi care profită de o eroare sau o vulnerabilitate a unei aplicații sau a unui sistem pentru a determina un comportament neintenționat sau neprevăzut. Denumirea provine de la verbul în limba engleză *to exploit* (a exploata), care înseamnă „a folosi ceva în avantajul propriu”. Practic, aceasta înseamnă că ținta unui atac prezintă un defect de proiectare, care permite oamenilor să creeze mijloacele de accesare a acestuia pentru a-l folosi în interesul său propriu. <https://www.bitdefender.ro/consumer/support/answer/21612/>

le-ar putea rata. În plus, NGFW-urile ar putea analiza traficul de ieșire la fel de eficient ca și de intrare, prevenind astfel filtrarea datelor și diminuând riscurile ca dispozitivele să devină parte a rețelelor bot.

Paralel cu evoluția firewall-urilor, și tehnologiile antivirus au avansat semnificativ. Primele programe antivirus au fost dezvoltate pentru a identifica și elimina viruși cunoscuți prin compararea fișierelor cu o bază de date de semnături. Cu toate acestea, pe măsură ce atacurile cibernetice au devenit mai sofisticate, la fel și metodologiile pentru livrarea și execuția malware-ului. Acest lucru a determinat dezvoltarea unor mecanisme de detectare bazate pe euristică capabile să identifice viruși *nefamiliari* sau *polimorfi* (Deshpande și colab., 2023). Programele antivirus moderne încorporează algoritmi de învățare automată pentru a detecta amenințările necunoscute anterior prin analizarea tiparelor comportamentale, sporind și mai mult eficacitatea acestora.

În domeniul securității cibernetice de ultimă oră, apariția calculului cuantic a introdus atât potențiale noi, cât și riscuri fără precedent. Cu computerele cuantice care devin din ce în ce mai accesibile prin intermediul serviciilor cloud, a apărut posibilitatea apariției virușilor specifici cuantici. Acești viruși ar putea manipula sarcini de calcul cuantic sau arhitecturi de inginerie inversă, reprezentând o amenințare gravă atât pentru utilizatori, cât și pentru furnizori (Deshpande et al., 2023). Pentru a contracara acest lucru, cercetătorii au propus dezvoltarea de antivirusuri cuantice pentru computere, care pot detecta și neutraliza în mod preventiv circuitele cuantice potențial rău intenționate înainte de execuție.

Un aspect important al eficienței firewall-ului este capacitatea lor de a încorpora funcții de securitate suplimentare, cum ar fi rețelele private virtuale (VPN), managementul separat al autentificării, controlul aplicațiilor și filtrarea web (Terentyev et al., 2021). Aceste caracteristici îmbunătățesc securitatea generală prin furnizarea de mecanisme de apărare cu mai multe straturi care lucrează împreună pentru a contracara amenințările cibernetice. De exemplu, VPN-urile pot securiza transmiterea datelor prin rețele de încredere, în timp ce filtrarea web poate împiedica accesul la site-uri web rău intenționate.

În concluzie, evoluția tehnologiilor de securitate cibernetică precum firewall-urile și software-ul antivirus subliniază natura dinamică a apărării cibernetice. Pe măsură ce amenințările continuă să evolueze, la fel trebuie să evolueze și tehnologiile concepute pentru a le contracara.

De la firewall-uri tradiționale de filtrare a pachetelor la NGFW-uri sofisticate și soluții antivirus bazate pe euristică până la antivirus pentru computere cuantice, călătoria reflectă o străduință continuă pentru măsuri de securitate mai robuste. Aceste progrese sunt esențiale pentru menținerea unei poziții cibernetice sigure într-o lume din ce în ce mai digitală, în care mizele continuă să crească pe zi ce trece.

Capitolul 1

Elemente de bază ale securității cibernetice

1.1 Importanța securității cibernetice în era digitală

În lumea noastră interconectată digital, importanța securității cibernetice nu poate fi exagerată. Progresul rapid al tehnologiei a revoluționat modul în care interacționăm, ne desfășurăm diverse activități și ne gestionăm viața de zi cu zi, promovând confortul și eficiența fără precedent. Cu toate acestea, această transformare digitală aduce și riscuri semnificative care necesită măsuri solide de securitate cibernetică pentru a proteja datele sensibile, activele financiare și infrastructura digitală. Potrivit Tolossa (2023), dependența din ce în ce mai mare de tehnologie expune organizațiile la un număr tot mai mare de amenințări cibernetice și breșe de securitate, pe care *infractorii* cibernetici le exploatează pentru a compromite sistemele și rețelele. Această realitate evidențiază necesitatea unei conștientizări și acțiuni cuprinzătoare în materie de securitate cibernetică.

Conceptul de securitate cibernetică presupune protecția sistemelor conectate la internet împotriva diferitelor forme de atacuri cibernetice, inclusiv atacuri de *hacking*⁴, *phishing*⁵ și *malware*. Având în vedere utilizarea pe scară largă a platformelor digitale, este esențial pentru indivizi și organizații să își protejeze în mod eficient activele digitale. Amin (2024) subliniază că securitatea cibernetică este vitală pentru protejarea unei multitudini de active digitale, cum

⁴ Hacking-ul este procesul de accesare neautorizată a unui sistem informatic, a unei rețele sau a unui dispozitiv electronic, de obicei cu scopul de a manipula, modifica sau fura date.

⁵ Phishing-ul este un tip de fraudă online care se bazează pe atacuri de inginerie socială pentru a păcăli utilizatorii să își divulge informațiile cu caracter sensibile, inclusiv numărul cardului de credit și datele de autentificare însușindu-și identitatea unei entități de încredere. <https://www.bitdefender.ro/consumer/support/answer/77356/>

ar fi rețelele, datele financiare, proprietatea intelectuală și informațiile personale. Securizarea acestor active nu numai că previne pierderile financiare, dar asigură și integritatea și confidențialitatea informațiilor sensibile, care este esențială pentru menținerea încrederii clienților și a reputației organizaționale.

În plus, practicile eficiente de securitate cibernetică sunt esențiale în atenuarea impactului potențial al amenințărilor cibernetice. Încălcările de securitate pot duce la pierderi financiare substanțiale, întreruperi operaționale și daune reputației. Pentru companii, aceste încălcări pot duce la pierderea încrederii clienților, repercusiuni juridice și dezavantaj competitiv. Tolossa (2023) susține acest lucru subliniind modul în care formarea de conștientizare a securității cibernetice pentru angajați poate reduce incidentele de securitate și poate promova o cultură a conștientizării securității cibernetice în cadrul organizațiilor. Prin programe de formare specifice, companiile își pot sprijini angajații să servească drept primă linie de apărare împotriva atacurilor cibernetice, îmbunătățind astfel poziția lor generală de securitate.

Pe lângă măsurile interne, legile și reglementările privind securitatea cibernetică joacă un rol crucial în stabilirea cadrelor pentru protejarea activelor digitale. Regulamentul general privind protecția datelor (GDPR), de exemplu, impune cerințe stricte de conformitate pentru manipularea și stocarea datelor cu caracter personal, impunând astfel un standard mai ridicat de protecție a datelor în cadrul organizațiilor. Respectarea acestor reglementări nu numai că îmbunătățește securitatea datelor, dar asigură și responsabilitatea juridică și încurajează cooperarea globală în eforturile de securitate cibernetică (Amin, 2024). Acest mediu de reglementare obligă organizațiile să adopte măsuri de securitate cuprinzătoare, care, la rândul lor, le întăresc apărarea împotriva amenințărilor cibernetice în continuă evoluție.

În plus, integrarea măsurilor tehnice cu o strategie holistică de securitate este esențială pentru o securitate cibernetică eficientă. Aceasta include implementarea tehnologiilor avansate de securitate, actualizări regulate ale sistemului și evaluări amănunțite ale vulnerabilităților. Potrivit Tolossa (2023), o abordare cu mai multe fațete care combină soluții tehnologice cu politici de securitate bine definite este esențială pentru protejarea activelor digitale. Adaptarea acestor strategii pentru a aborda provocările unice generate de munca de la distanță întărește și mai mult *reziliența* organizațională împotriva amenințărilor cibernetice.

Semnificația securității cibernetice se extinde dincolo de granițele organizaționale, cuprinzând securitatea națională și stabilitatea economică globală. Atacurile cibernetice asupra infrastructurii critice, cum ar fi rețelele energetice, instituțiile financiare și rețelele de

comunicații, pot avea consecințe de amploare. Prin urmare, cooperarea internațională și schimbul de informații sunt vitale pentru combaterea criminalității cibernetice la scară globală. După cum notează Amin (2024), prioritizarea securității cibernetice asigură siguranța și eficiența activelor digitale și facilitează navigarea securizată în domeniul digital, salvând astfel interesele naționale și promovând conștiința globală a securității cibernetice.

Articolul *The Cybersecurity of Fairy Tales* scris de Luca Viganò și apărut în *Journal of Cybersecurity*, (2024), explorează o abordare creativă și neconvențională a conceptelor de securitate cibernetică folosind analogii din basme clasice. Viganò argumentează că poveștile atemporale precum „Cenușăreasa”, „Scufița Roșie” sau „Ali Baba și cei 40 de hoți” conțin elemente arhetipale care se regăsesc în problemele contemporane de securitate cibernetică.

Articolul propune că basmele pot fi folosite pentru a explica noțiuni complexe de securitate cibernetică într-un mod accesibil și captivant, mai ales pentru publicul nespecializat. Scopul este de a facilita înțelegerea unor concepte precum autentificarea, confidențialitatea, integritatea și atacurile cibernetice prin analogii ușor de înțeles.

Viganò explorează cum povești precum „Cenușăreasa” pot ilustra autentificarea multifactorială (MFA), în timp ce „Ali Baba și cei 40 de hoți” pot fi folosite pentru a explica concepte precum atacurile de tip „replay” sau amenințările avansate persistente (APT). De exemplu:

Autentificarea: Cenușăreasa este recunoscută de Prinț prin potrivirea pantofului, un exemplu simplificat de MFA.

Masquerading (falsificarea identității): Lupul din „Scufița Roșie” se dă drept bunica pentru a accesa resurse (adică casa bunicii).

Confidențialitatea și integritatea: În „Fata fără mâini”, mesaje critice sunt interceptate și modificate, exemplificând breșe de confidențialitate și integritate.

Utilitatea educațională

Autorul subliniază că utilizarea basmelor în explicarea securității cibernetice poate ajuta la reducerea anxietății și a barierelor de înțelegere pe care mulți utilizatori le au față de subiecte tehnice. Basmele oferă un cadru familiar care poate fi folosit pentru a construi o bază de cunoștințe în securitate cibernetică pentru persoane care nu au un background tehnic.

Articolul sugerează că există un potențial neexplorat în folosirea basmelor și a altor forme de povestiri pentru a educa publicul larg despre securitatea cibernetică. Autorul intenționează să extindă cercetarea prin studii sistematice care să valideze eficacitatea acestei abordări și să exploreze utilizarea adaptărilor cinematografice ale basmelor.

Acest articol demonstrează cum poveștile clasice pot deveni un instrument valoros în educația cibernetică, transformând concepte tehnice complexe în lecții captivante și accesibile.

De aici și ideea acestei cărți.

În articolul *Toward effective learning of cybersecurity: new curriculum agenda and learning methods*, autorii Blaži & Blaži (2024) explorează necesitatea îmbunătățirii educației în domeniul cybersecurității în școlile europene, cu un accent deosebit pe pregătirea profesorilor și elevilor din liceu. Principalele concluzii și propuneri din articol sunt:

Lipsa educației formale în domeniul cybersecurității la nivel de liceu în Europa a fost confirmată printr-un studiu amplu realizat în 2021-2023. Deși informatica este introdusă în unele programe școlare, subiectele legate de cybersecuritate sunt rareori acoperite.

Tinerii din Europa folosesc internetul în mod activ, dar sunt expuși la diverse riscuri online, cum ar fi phishing-ul, furtul de identitate și alte atacuri cibernetice. Cu toate acestea, educația lor în ceea ce privește auto-protecția în mediul digital este limitată.

Autorii își propun

- dezvoltarea unui curriculum specific pentru educarea elevilor și formarea profesorilor în domeniul cybersecurității și cyber-siguranței.

- crearea de fișes educative care să includă resurse precum jocuri educaționale, platforme video, chestionare și exerciții practice.

- aplicarea acestui curriculum în nouă școli europene pentru a evalua eficiența metodei propuse în anul școlar 2022-2023.

Ei propun ca metodologie și implementare: activități educative interactive, formarea profesorilor și evaluare continuă

În loc de metode tradiționale, articolul propune utilizarea jocurilor educaționale (ex: „Capture the Flag”), chestionare și prezentări interactive pentru a îmbunătăți implicarea elevilor.

Profesorii au fost instruiți online pentru a utiliza resursele propuse și a-și actualiza cunoștințele în domeniul cybersecurității.

Programul a inclus teste preliminare și activități practice pentru a adapta nivelul de dificultate la cunoștințele elevilor, precum și discuții pentru a stimula interesul și înțelegerea subiectelor.

Participanții la program au indicat că metodele interactive (jocuri, quizuri) au contribuit la o mai bună înțelegere a subiectelor complexe.

Sesiunile de „Capture the Flag” au fost deosebit de apreciate, elevii manifestând un interes sporit pentru cariere în domeniul cybersecurității.

Satisfacția elevilor: Aproximativ 74% dintre elevi au declarat că le-au plăcut lecțiile, iar 62% au raportat o mai mare încredere în utilizarea serviciilor online după finalizarea cursurilor.

Integrarea educației în domeniul cybersecurității în programele școlare ar putea contribui la formarea unei noi generații de specialiști în acest domeniu, reducând astfel deficitul de competențe pe piața muncii.

Introducerea unei metodologii flexibile și interactive în predare a demonstrat că poate face lecțiile mai atractive și eficiente, contribuind la o învățare activă.

Este nevoie de investiții continue pentru a extinde și rafina aceste inițiative educaționale la nivelul tuturor țărilor europene.

Acest articol este foarte util pentru educație, deoarece: provoacă o schimbare de paradigmă în predarea subiectelor legate de informatică și securitate online, promovează metode interactive de învățare, care cresc angajamentul și interesul elevilor și oferă un model replicabil pentru alte școli interesate de implementarea educației în domeniul cybersecurității.

Această cercetare poate servi ca bază pentru elaborarea unor politici educaționale care să integreze mai eficient *cybersecuritatea* în curriculumul școlar, pregătind elevii pentru un mediu digital mai sigur.

În concluzie, importanța securității cibernetice în era digitală nu poate fi banalizată. Pe măsură ce tehnologia continuă să evolueze, la fel evoluează și amenințările care compromit lumea noastră digitală. Implementarea unor practici riguroase de securitate cibernetică, aderarea la standardele de reglementare precum GDPR și promovarea unei culturi de conștientizare a securității cibernetice sunt imperative în protejarea activelor noastre digitale. Înțelegând și

abordând complexitățile securității cibernetice, ne putem proteja mai bine de multitudinea de amenințări cibernetice care pun în pericol existența noastră digitală.

1.2 Amenințări cibernetice comune: viruși, programe malware și phishing

În lumea interconectată de astăzi, evoluția amenințărilor cibernetice a ținut pasul cu progresele tehnologice. Creșterea exponențială a utilizării internetului, accelerată de pandemia de coronavirus, a introdus atât oportunități, cât și riscuri. Pe măsură ce indivizii și companiile efectuează din ce în ce mai mult tranzacții și stochează informații sensibile online, peisajul amenințărilor s-a extins pentru a include forme noi și mai sofisticate de atacuri cibernetice (Aslan, Aktuğ, Ozkan-Okay, Yilmaz și Akin, 2023). Înțelegerea acestor amenințări este esențială pentru utilizatorii de zi cu zi pentru a-și proteja viața digitală.

Virusii și programele malware reprezintă unele dintre cele mai vechi și mai răspândite forme de amenințări cibernetice. Programele malware, o categorie largă care include viruși, viermi, troieni și ransomware, sunt concepute pentru a deteriora, perturba sau obține acces neautorizat la sistemele informatice. Virusii se atașează la software sau fișiere legitime și se răspândesc ori de câte ori programul infectat este executat. Software-ul rău intenționat poate corupe sau șterge date, poate fura informații personale sau poate crea ”uși în spate” pentru alte exploit-uri. Consecințele unor astfel de infecții pot fi devastatoare, ducând la pierderi financiare semnificative și la pierderea integrității datelor (Aslan et al., 2023).

Un exemplu notabil de malware este atacul ransomware WannaCry din 2017, care a exploatat o vulnerabilitate în protocolul Microsoft SMB și s-a răspândit rapid pe tot globul. Atacul a criptat datele de pe computere infectate și a cerut plăți de răscumpărare în Bitcoin pentru a decifra fișierele. Întreruperea pe scară largă a afectat spitalele, întreprinderile și agențiile guvernamentale, ilustrând impactul larg pe care îl poate avea un atac de malware bine coordonat (Aslan et al., 2023).

Phishingul, o altă amenințare cibernetică răspândită, implică păcălirea persoanelor pentru a divulga informații sensibile, cum ar fi nume de utilizator, parole și detalii financiare, prefăcându-se ca o entitate de încredere. Aceste atacuri apar adesea prin e-mail, dar pot implica și site-uri web frauduloase, mesaje text sau apeluri telefonice.

E-mailurile de tip phishing folosesc de obicei tactici de panică, urgență sau inginerie socială pentru a convinge destinatarul să facă clic pe linkuri rău intenționate sau să deschidă atașamente infectate (Gindra, Goyal, Sethi și Kaushal, 2023).

Tehnicile de phishing au devenit din ce în ce mai sofisticate, atacatorii utilizând metode precum manipularea linkurilor, falsificarea site-urilor web și evaziunea filtrelor pentru a evita detectarea. De exemplu, o tactică obișnuită este de a crea o pagină de autentificare falsă care seamănă foarte mult cu un site legitim, atrăgând utilizatorii să-și introducă contul și parola, care sunt apoi culese de atacator. Studiile de caz recente au arătat cum au crescut atacurile de phishing în timpul pandemiei de COVID-19, profitând de incertitudinea larg răspândită și de creșterea activității online (Bajanthri & Sayeesh, 2022). Exemple notabile includ înșelătoriile de tip phishing PayPal și phishingul Rapidshare, în care atacatorii trimit e-mailuri pretinzând a fi de la aceste companii pentru a fura datele de conectare (Bajanthri & Sayeesh, 2022).

Impactul acestor amenințări cibernetice asupra utilizatorilor de zi cu zi poate fi sever, ducând la pierderi financiare, furt de identitate și suferință emoțională. Datele din diverse studii indică o creștere semnificativă a numărului de atacuri de tip phishing și sofisticarea programelor malware (Gindra et al., 2023). Pentru a atenua aceste amenințări, utilizatorii trebuie să rămână vigilenți și să adopte practici de bază de securitate cibernetică, cum ar fi utilizarea software-ului antivirus actualizat, autentificarea cu doi factori și a fi atenți la e-mailurile sau mesajele nesolicitate care îndeamnă la acțiune imediată.

Securitatea cibernetică este un domeniu în continuă evoluție, iar atacatorii dezvoltă continuu noi tehnici pentru a ocoli apărările tradiționale. Inovații precum învățarea automată, învățarea profundă și blockchain-ul sunt promițătoare pentru îmbunătățirea detectării și prevenirii amenințărilor (Aslan et al., 2023). Cu toate acestea, aceste tehnologii nu sunt imune la tehnicile de evaziune, evidențiind necesitatea cercetării continue și a măsurilor de securitate adaptative.

În concluzie, virușii, programele malware și phishingul rămân amenințări semnificative în era digitală, atacatorii utilizând tehnici avansate pentru a-și atinge obiectivele rău intenționate. Înțelegerea acestor amenințări și adoptarea măsurilor proactive de securitate cibernetică sunt pași foarte importanți pentru ca utilizatorii obișnuiți să își protejeze experiențele online. Rămânând informați și vigilenți, utilizatorii își pot reduce semnificativ riscul de a deveni victime ale acestor amenințări cibernetice comune, dar periculoase.

1.3 Impactul amenințărilor cibernetice asupra utilizatorilor obișnuiți: studii de caz și statistici

Creșterea erei digitale a adus beneficii imense, dar și provocări semnificative, în special în ceea ce privește amenințările la adresa securității cibernetice. Utilizatorii obișnuiți de internet sunt din ce în ce mai vulnerabili la aceste amenințări, care pot varia de la simple inconveniente la încălcări grave care au consecințe de amploare. Înțelegerea impactului amenințărilor cibernetice asupra utilizatorilor obișnuiți este crucială pentru o mai bună pregătire și o apărare eficientă împotriva potențialelor atacuri.

Un domeniu semnificativ în care se manifestă amenințările cibernetice este sectorul financiar. După cum au subliniat Kafi și Akter (2023), securizarea informațiilor financiare, în special a datelor contabile, a devenit esențială. Măsurile de securitate cibernetică trebuie să evolueze continuu pentru a contracara aceste amenințări. Cercetătorii au prezentat mai multe cazuri în care organizațiile s-au confruntat cu riscuri substanțiale din cauza protecției inadecvate a datelor contabile. De exemplu, atacurile ransomware care criptează datele financiare ale unei organizații până când se plătește o răscumpărare au dus la pierderi financiare semnificative și la întreruperi operaționale. Studiul subliniază și mai mult necesitatea adoptării de cadre cuprinzătoare de securitate cibernetică și apărări tehnice pentru a proteja datele financiare valoroase. Prin implementarea unor măsuri solide de securitate cibernetică, organizațiile pot atenua impactul amenințărilor cibernetice și pot proteja informațiile sensibile (Kafi & Akter, 2023).

Un alt cadru în care amenințările cibernetice au un impact semnificativ este învățământul superior, după cum indică Oliveira și colab. (2023). Studiul a evaluat gradul de conștientizare a securității cibernetice în rândul a 110 studenți din primul an la informatică din Portugalia și Polonia. A constatat variații considerabile în conștientizarea și cunoștințele cu privire la *igiena securității cibernetice* și amenințările cibernetice majore. Studenții polonezi au obținut scoruri mai mari atât la percepția de sine, cât și la cunoștințele reale, cu un scor de aproximativ 70%, comparativ cu 58% al studenților portughezi. Aceste constatări subliniază importanța educației și conștientizării securității cibernetice, chiar și în rândul *nativilor digitali*, care probabil vor fi *apărătorii* de mâine împotriva amenințărilor cibernetice. Dacă studenții nu sunt pregătiți sau nu sunt conștienți de principiile și amenințările de bază ale securității cibernetice, consecințele se pot extinde dincolo de mediile academice pentru a afecta sisteme mai largi, interconectate (Oliveira et al., 2023).

Impactul mai larg al amenințărilor cibernetice poate fi analizat și prin prisma tehnologiilor predictive. Datta, Namin și Jones (2022) au folosit *Procesarea Limbajului Natural* (NLP) și învățarea profundă pentru a prezice consecințele atacurilor cibernetice prin analiza descrierilor atacurilor. Prevăzând impactul potențial asupra disponibilității, controlului accesului, confidențialității și integrității, această tehnologie ajută experții în securitate și toți cei interesați să se pregătească pentru și să atenueze efectele atacurilor cibernetice. De exemplu, o încălcare anticipată a confidențialității ar putea duce la măsuri preventive pentru protejarea datelor sensibile. Această cercetare subliniază valoarea instrumentelor analitice avansate în înțelegerea și contracararea impactului cu mai multe fațete ale amenințărilor cibernetice asupra utilizatorilor obișnuiți (Datta, Namin și Jones, 2022).

Un caz important care ilustrează în continuare consecințele amenințărilor cibernetice este cazul de extrădare al lui Julian Assange, Statele Unite ale Americii versus Assange. Acest caz exemplifică atât ramificațiile personale, cât și geopolitice ale eșecurilor securității cibernetice. Expunerea de către Assange a documentelor clasificate, facilitată prin accesul neautorizat la sistemele guvernamentale, a arătat modul în care acțiunile individuale pot duce la riscuri semnificative de securitate națională și lupte juridice internaționale. Utilizatorii obișnuiți pot scoate o lecție crucială din cazul lui Assange: importanța considerentelor etice și a ramificațiilor legale în domeniul digital. În plus, evidențiază modul în care chiar și acțiunile menite să promoveze transparența pot avea consecințe negative neintenționate și de anvergură.

Cumularea acestor studii și a exemplurilor din lumea reală prezintă o imagine cuprinzătoare a impactului în creștere al amenințărilor cibernetice asupra utilizatorilor de internet de zi cu zi. Fie prin pierderi financiare directe, deficiențe educaționale, analize predictive sau cazuri juridice, efectele sunt profunde și de anvergură uneori catastrofale. Înțelegând aceste impacturi și adoptând în mod proactiv măsurile adecvate de securitate cibernetică - de la educație și conștientizare până la instrumente avansate de predicție - indivizii și organizațiile deopotrivă se pot proteja mai bine de peisajul amenințărilor cibernetice în continuă evoluție. Era digitală oferă oportunități incredibile, dar cu acestea vin responsabilitățile și nevoia de vigilență pentru a te proteja în lumea interconectată în care navigăm zilnic.

1.4 Concepte de bază ale siguranței online: HTTPS, firewall-uri și VPN-uri

Pe măsură ce internetul devine din ce în ce mai integrat în viața noastră de zi cu zi, înțelegerea conceptelor fundamentale de siguranță online este crucială pentru fiecare utilizator. Măsurile

de bază precum HTTPS, firewall-urile și VPN-urile formează piatra de temelie a unei experiențe online sigure, protejând utilizatorii împotriva amenințărilor cibernetice comune și asigurând confidențialitatea datelor.

HTTPS (Hypertext Transfer Protocol Secure) este o extensie a HTTP și este folosită pentru a transmite în siguranță date între browserul unui utilizator și serverul web. HTTPS folosește Transport Layer Security (TLS) pentru a cripta datele, ceea ce face semnificativ mai greu pentru părțile neautorizate să intercepteze sau să modifice informațiile schimbate. Cercetarea lui Kim et al. (2021) subliniază importanța HTTPS în prevenirea atacurilor de tip phishing. Studiul dezvăluie că un volum mare de atacuri de phishing adoptă acum HTTPS pentru a părea mai legitim și mai credibil pentru utilizatori. În timp ce HTTPS oferă criptare și asigură integritatea datelor, este esențial să recunoaștem că nu toate certificatele HTTPS sunt egale. Eficacitatea HTTPS depinde în mare măsură de practicile de securitate ale autorităților de certificare (CA). Din păcate, studiul identifică lacune semnificative în practicile de securitate ale CA, care sunt actori critici în ecosistemul HTTPS. Aceste lacune pot duce la emiterea de certificate legate de phishing, subminând astfel securitatea pe care ar trebui să o ofere protocolul. În consecință, înțelegerea rolului CA și a limitărilor HTTPS este crucială pentru utilizatorii care doresc să navigheze pe internet în siguranță.

Firewall-urile reprezintă o altă componentă fundamentală a siguranței online. Aceștia acționează ca *gatekeepers*, monitorizează traficul de rețea de intrare și de ieșire și blochează pachetele de date nesigure. Potrivit Fakiha (2022), firewall-urile joacă un rol esențial în protejarea utilizatorilor împotriva atacurilor din rețea, cum ar fi malware, phishing și furtul de identitate. Studiul subliniază că atât firewall-urile hardware, cât și software-urile au punctele lor forte și limitările. Firewall-urile hardware oferă protecție robustă prin filtrarea traficului la nivel de rețea, dar este posibil să nu se apere împotriva tuturor tipurilor de atacuri bazate pe web. În schimb, firewall-urile software, care sunt încorporate în sistemele de operare, oferă un control mai amănunțit asupra traficului, dar ocazional pot eșua în detectarea amenințărilor sofisticate. Cercetarea sugerează că o combinație de firewall-uri hardware și software poate oferi un mecanism de apărare cuprinzător. Astfel, pentru utilizatorii obișnuiți, înțelegerea modului de configurare și utilizare eficientă a firewall-urilor este esențială pentru menținerea unui mediu online sigur.

VPN-urile (Virtual Private Networks) îmbunătățesc siguranța online prin crearea de tuneluri securizate pentru transmiterea datelor prin internet. Aceste tuneluri criptează datele, făcându-

le indescifrabile pentru cei care interceptează. VPN-urile sunt deosebit de utile atunci când se utilizează rețele Wi-Fi publice, care sunt notoriu nesigure. Bodipudi (2023) subliniază tranziția de la IKEv1 la IKEv2 în protocoalele VPN, observând că acesta din urmă oferă caracteristici de securitate îmbunătățite, acceptă algoritmi criptografici moderni și oferă o mai bună rezistență împotriva diferitelor amenințări cibernetice. Această tranziție este determinată de necesitatea unei protecții mai puternice într-o eră în care amenințările cibernetice evoluează continuu. Pentru utilizatorii obișnuiți, selectarea unui VPN care utilizează protocolul IKEv2 le poate îmbunătăți în mod semnificativ securitatea online, asigurându-se că datele lor rămân private și protejate de potențiale amenințări.

În cele din urmă, principiile originale de proiectare ale World Wide Web, așa cum au subliniat de către inventatorul său Tim Berners-Lee (1999), subliniază importanța unui web deschis, securizat și interoperabil. Viziunea lui Berners-Lee subliniază necesitatea ca utilizatorii să fie educați cu privire la practicile de siguranță online. În timp ce instrumentele tehnologice precum HTTPS, firewall-urile și VPN-urile asigură mecanismul de securitate, responsabilitatea utilizării acestor instrumente revine în mod eficient utilizatorilor. Înțelegerea modului de folosire a acestor tehnologii nu numai că protejează utilizatorii individuali, ci contribuie și la securitatea și integritatea generală a web-ului.

În concluzie, conceptele de bază ale siguranței online, cum ar fi HTTPS, firewall-urile și VPN-urile sunt indispensabile oricărui utilizator de internet. Fiecare dintre aceste tehnologii abordează diferite aspecte ale securității, de la criptarea datelor și monitorizarea traficului până la transmisia securizată a datelor. Prin înțelegerea și implementarea acestor măsuri fundamentale de siguranță, utilizatorii se pot proteja împotriva amenințărilor cibernetice comune și pot asigura o experiență online mai sigură. Pe măsură ce peisajul digital continuă să evolueze, rămânerea la curent cu aceste practici de securitate de bază va rămâne crucială pentru toți utilizatorii de internet.

Capitolul 2

Practici sigure pentru utilizatorii de internet

2.1 Crearea de parole puternice și utilizarea managerilor de parole

În era digitală, crearea și păstrarea parolelor puternice este o practică esențială pentru securitatea cibernetică. Parolele servesc ca primă linie de apărare împotriva accesului neautorizat la informațiile personale și la conturile online. Cu toate acestea, eficiența parolelor este adesea compromisă de practicile slabe, cum ar fi folosirea de cuvinte ușor de ghicit sau reutilizarea parolelor pe mai multe site-uri. Această secțiune analizează importanța creării de parole puternice și modul în care *managerii de parole* pot ajuta în acest proces.

Crearea de parole puternice prezintă o provocare cognitivă pentru mulți utilizatori, ceea ce duce adesea la o stare de nervozitate și la reducerea productivității. Cercetările efectuate de Abdrabou, Abdelrahman, Khamis și Alt (2021) au examinat încărcarea cognitivă asociată cu crearea de parole puternice. Studiul a arătat că procesul de generare a parolelor puternice crește semnificativ concentrarea utilizatorilor, măsurată prin modificările diametrului pupilei. Participanții s-au luptat mai mult cu crearea de parole puternice, comparativ cu altele mai slabe, ceea ce indică o concentrare cognitivă mai mare. Acest lucru evidențiază o provocare inerentă: în timp ce parolele puternice sunt esențiale pentru securitate, complexitatea lor poate descuraja utilizatorii să le creeze și să le amintească ușor.

În ciuda necesității unor parole robuste, mulți utilizatori fie nu reușesc să creeze parole puternice, fie reutilizează parolele pe mai multe site-uri, lăsându-și conturile vulnerabile. O soluție viabilă din punct de vedere tehnologic la această problemă larg răspândită este adoptarea managerilor de parole. Aceste aplicații stochează și generează parole complexe, unice pentru fiecare cont, reducând semnificativ sarcina asupra utilizatorilor. Cu toate acestea, utilizarea managerilor de parole rămâne o variantă secundară. Aurigemma, Mattson și Leonard (2017) au explorat motivele pentru care utilizatorii finali casnici rezistă adesea la utilizarea acestor aplicații. Studiul lor a constatat că lipsa de încredere în tehnologie, costurile percepute ridicate și apatia amenințărilor au fost bariere majore. În plus, chiar și utilizatorii cu intenții comportamentale ridicate de a folosi managerii de parole nu au reușit adesea să le adopte din motive precum lipsa de încredere și constrângerile de timp.

Utilizabilitatea managerilor de parole este un alt factor critic care influențează procentul de adaptare la acest stil. Kablo, Kader și Arias-Cabarcos (2024) au studiat interfețele de audit al acreditărilor în cadrul managerilor de parole, care ajută utilizatorii să identifice parolele slabe sau compromise. Descoperirile lor au indicat că, în timp ce securitatea a fost un motiv principal pentru adoptarea managerilor de parole, utilizatorii s-au confruntat cu provocări în a face față unor rezultate copleșitoare ale auditului. Acest lucru sugerează că, deși utilizatorii se angajează să-și securizeze conturile, complexitatea instrumentelor ar putea descuraja utilizarea continuă. Îmbunătățiri precum tehnicile de prioritizare și o mai bună transparență cu privire la deficiențele parolilor ar putea îmbunătăți experiența utilizatorului și ar putea promova o utilizare mai frecventă.

În ciuda progreselor în tehnologia de gestionare a parolilor, rămâne un decalaj semnificativ în adoptarea utilizatorilor din cauza lipsei de conștientizare și înțelegere a acestor instrumente. Perspective istorice precum cele din Tarbell (1904) evidențiază că soluțiile tehnologice singure nu sunt întotdeauna suficiente; educația și motivația utilizatorilor joacă un rol crucial în adoptarea pe scară largă. Utilizatorii trebuie să fie conștienți de riscurile asociate cu parolele slabe și de beneficiile utilizării managerilor de parole nu doar pentru comoditate, ci și pentru securitate sporită.

În concluzie, deși crearea de parole puternice și utilizarea managerilor de parole sunt practici esențiale pentru securitatea cibernetică, provocările rămân în adoptarea utilizatorilor. Sarcinile cognitive asociate cu dezvoltarea parolilor puternice și preocupările privind utilizarea cu managerii de parole trebuie abordate pentru a încuraja utilizarea pe scară largă și eficientă. Eforturile educaționale de a crește gradul de conștientizare cu privire la importanța practicilor puternice de parole și a beneficiilor managerilor de parole ar putea contribui semnificativ la îmbunătățirea securității online pentru utilizatorii obișnuiți. Abordând atât factorii tehnologici, cât și factorii umani, putem *echipa* mai bine indivizii pentru a-și proteja identitățile digitale în mod eficient.

2.2 Identificarea și evitarea înșelătoriilor de tip phishing: semnale roșii și bune practici

Înșelătoriile de tip phishing sunt încercări înșelătoare de a obține informații sensibile, cum ar fi numele de utilizator, parolele și detaliile cărților de credit, prefăcându-se ca entități de încredere în comunicațiile electronice. Identificarea înșelătoriilor de tip phishing și a cunoaște

cum să le evite este crucială pentru utilizatorii de internet de zi cu zi. Înțelegerea psihologiei din spatele acestor escrocherii și adoptarea celor mai bune practici pot reduce semnificativ riscul de a deveni victima unor astfel de activități frauduloase.

E-mailurile de tip phishing par adesea convingătoare și legitime, ceea ce face ca utilizatorii să facă o distincție între comunicațiile autentice și cele rău intenționate. Potrivit Wash (2020), experții IT folosesc un proces cognitiv în trei etape pentru a identifica e-mailurile de phishing. Inițial, ei examinează e-mailul pentru eventuale inconsecvențe sau anomalii. Aceste discrepanțe, cum ar fi adresele neobișnuite ale expeditorului sau cuvintele scrise greșit, acționează ca semne de avertizare timpurie. Pe măsură ce se acumulează mai multe discrepanțe, apare un sentiment de suspiciune, care determină o investigație mai profundă a detaliilor tehnice ale e-mailului, cum ar fi link-uri sau atașamente suspecte. În concluzie, odată ce e-mailul este identificat ca fiind phishing, este fie șters, fie raportat. Acest proces amănunțit și metodic poate servi drept ghid pentru utilizatorii generali pentru a-și îmbunătăți abilitățile de detectare a phishingului.

În studii la scară largă și simulări de antrenament anti-phishing, cum ar fi cel realizat de Sutter și colab. (2022), peste 31.000 de participanți au fost supuși la 144 de simulări diferite de phishing. În mod remarcabil, 66% dintre utilizatori nu au căzut victime ale acestor atacuri după o perioadă de antrenament de douăsprezece săptămâni. Acest lucru sugerează că programele de instruire bine structurate pot crește în mod eficient gradul de conștientizare și pot îmbunătăți capacitatea utilizatorilor de a recunoaște încercările de phishing. Studiul a introdus, de asemenea, un model de învățare automată care a prezis „puterea convingătoare” a e-mailurilor de phishing, ajutând la proiectarea unor module de instruire mai eficiente. Aceste constatări subliniază importanța educației continue și a formării personalizate pentru a întări vigilența utilizatorilor împotriva înșelătoriilor de tip phishing.

Inteligența artificială (AI) și tehnologiile de învățare automată sunt din ce în ce mai utilizate pentru a detecta și a preveni atacurile de tip phishing. Ansari și colab. (2022) subliniază că, în aceeași măsură, conștientizarea și educația bazate pe măsuri de securitate cibernetică bazate pe inteligență artificială pot reduce în mod eficient incidența atacurilor de tip phishing. AI poate analiza cantități mari de date pentru a identifica modele și anomalii care pot indica activități de phishing, oferind alerte în timp real utilizatorilor. În plus, programele de instruire bazate pe inteligență artificială pot simula diverse scenarii de phishing, permițând utilizatorilor să-și

exerseze abilitățile de detectare într-un mediu controlat, crescând astfel pregătirea lor pentru a aborda amenințările din lumea reală.

Câteva bune practici pot echipa utilizatorii în continuare să atenueze riscurile asociate cu escrocherii de tip phishing. O măsură fundamentală este să fii precaut cu e-mailurile nesolicitate, în special cu cele care solicită acțiuni urgente sau oferă stimulente. Examinarea adresei de e-mail a expeditorului pentru nereguli și verificarea încrucișată cu sursele oficiale poate preveni multe încercări de phishing. În plus, utilizatorii ar trebui să evite să facă clic pe linkuri sau să descarce atașamente din e-mailuri necunoscute sau suspecte. În schimb, ar trebui să navigheze la site-urile web oficiale direct prin browserul lor pentru a verifica informațiile.

O altă strategie eficientă este utilizarea autentificării cu mai mulți factori (MFA) ori de câte ori este posibil. Chiar dacă datele de conectare sunt compromise, MFA adaugă un nivel suplimentar de securitate care împiedică în mod semnificativ accesul neautorizat. În plus, folosirea de software antivirus și anti-malware de renume poate oferi o rețea de siguranță suplimentară prin scanarea și blocarea potențialelor amenințări.

Actualizarea regulată a parolilor și utilizarea combinațiilor complexe și unice pentru diferite conturi poate limita, de asemenea, daunele cauzate de atacurile de tip phishing. Managerii de parole pot ajuta la gestionarea acestor acreditări complexe în mod sigur și convenabil. În plus, activarea funcțiilor precum filtrele de e-mail și de browser poate semnaliza și redirecționa automat e-mailurile de phishing, reducând șansele ca utilizatorii să interacționeze cu acestea.

În concluzie, recunoașterea și evitarea înșelătoriilor de tip phishing necesită o combinație de vigilență, educație și utilizarea unor instrumente tehnologice avansate. Înțelegând semnele roșii ale tentativelor de phishing și adoptând cele mai bune practici, cum ar fi programele de instruire bazate pe MFA și AI, utilizatorii își pot îmbunătăți în mod semnificativ siguranța online. Învățarea continuă și adaptabilitatea sunt esențiale în peisajul în continuă evoluție al amenințărilor cibernetice, asigurându-se că utilizatorii rămân cu un pas înaintea actorilor rău intenționați.

2.3 Tehnici de navigare sigură: site-uri web sigure, navigare privată și extensii de browser

În era digitală de astăzi, navigarea securizată a devenit o practică esențială pentru protejarea informațiilor personale și pentru asigurarea siguranței tranzacțiilor online. Tehnicile de

navigare sigură includ identificarea site-urilor web sigure, utilizarea modurilor de navigare privată și utilizarea extensiilor de browser concepute pentru a spori securitatea. Fiecare dintre aceste practici joacă un rol esențial în fortificarea utilizatorilor împotriva diferitelor amenințări cibernetice și escrocherii.

Identificarea site-urilor web sigure este primul pas în asigurarea unei experiențe online sigure. O metodă eficientă este de a verifica dacă un site web utilizează HTTPS, indicând faptul că comunicarea dintre browserul utilizatorului și site-ul web este criptată. Această criptare ajută la prevenirea interceptării datelor de către actori rău intenționați. Pe lângă HTTPS, utilizatorii pot căuta certificate de securitate și sigilii de la autorități de încredere, asigurând în continuare legitimitatea site-ului. În plus, o abordare vigilentă față de adresele URL ale site-urilor web poate atenua riscul atacurilor de tip phishing. Potrivit lui Sathvik et al. (2023), Web Extension, un instrument de securitate bazat pe browser, poate analiza adresele URL, poate verifica certificatele SSL și poate utiliza algoritmi de învățare automată pentru a detecta site-uri web suspecte. Prin încrucișarea bazelor de date de phishing cunoscute, Extensia Web alertează utilizatorii cu privire la potențiale amenințări, ajutându-i să evite site-urile rău intenționate. Această abordare proactivă este critică, deoarece phishingul rămâne una dintre cele mai răspândite amenințări care vizează utilizatorii online.

Modurile de navigare privată, cum ar fi Incognito din Chrome sau Navigarea privată din Firefox, oferă un alt nivel de securitate pentru utilizatori. Aceste moduri împiedică browserul să stocheze istoricul, cookie-urile și fișierele temporare, ceea ce poate fi benefic atunci când accesează informații sensibile sau efectuează tranzacții confidențiale. Cu toate acestea, este esențial să recunoaștem că navigarea privată nu face utilizatorii complet anonimi online; limitează doar stocarea datelor pe dispozitivul local. Pentru o securitate completă, combinarea navigării private cu alte tehnici, cum ar fi utilizarea VPN-urilor, protejează utilizatorii de urmărirea și monitorizarea de către terți.

Extensiile de browser pot îmbunătăți în mod semnificativ securitatea, dar pot prezenta și riscuri dacă nu sunt utilizate cu atenție. În timp ce multe extensii, cum ar fi blocarea reclamelor și managerii de parole, adaugă funcții de securitate valoroase, extensiile rău intenționate pot compromite datele utilizatorilor. Marimuthu și colab. (2023) evidențiază pericolele extensiilor rău intenționate care pot fura informații sensibile, cum ar fi parolele și detaliile cărților de credit. Pentru a contracara aceste amenințări, au fost propuse mecanisme de apărare robuste, cum ar fi API-ul Secure Vault. Folosind tehnici de criptare, hashing și izolare, Secure Vault

protejează conținutul web confidențial de extensiile rău intenționate. Extensia Sentinel, parte a Secure Vault, verifică integritatea conținutului unei pagini web, asigurându-se că acesta rămâne nemodificat. Astfel de măsuri creează un mediu sigur, reducând riscul încălcării datelor. Utilizatorii ar trebui să fie precauți atunci când instalează extensii, asigurându-se că provin din surse de încredere și au recenzii favorabile.

Creșterea muncii la distanță a schimbat peisajul amenințărilor, făcând navigarea sigură și mai critică. Lee (2023) subliniază că dependența crescută de browserele web pentru comunicare și productivitate a atras actori rău intenționați. Această tendință necesită o conștientizare sporită a practicilor de navigare sigură în rândul utilizatorilor. Actualizarea regulată a browserelor și eliminarea extensiilor neutilizate sau suspecte pot atenua potențialele vulnerabilități. În plus, utilizarea funcțiilor de securitate ale browserului, cum ar fi phishingul încorporat și protecția împotriva programelor malware, poate spori siguranța. A fi informat cu privire la cele mai recente amenințări și tendințe de securitate este vital pentru adaptarea și consolidarea apărării cuiva.

Un caz interesant care subliniază importanța navigării securizate este Statele Unite împotriva Microsoft Corp. În acest caz, dominația Microsoft pe piața browserelor a dus la practici monopoliste, care afectează alegerea și securitatea consumatorilor. Bătălia juridică a evidențiat necesitatea unor soluții de navigare competitive și sigure. Utilizatorii trebuie să utilizeze opțiuni diverse și sigure de browser pentru a-și proteja activitățile online și pentru a se proteja de potențialele vulnerabilități monopoliste.

În concluzie, tehnicile de navigare sigură sunt primordiale în mediul digital modern. Prin identificarea site-urilor web sigure, prin utilizarea modurilor de navigare private și prin utilizarea cu prudență a extensiilor de browser, utilizatorii își pot reduce substanțial expunerea la amenințările cibernetice. Pe măsură ce amenințările cibernetice continuă să evolueze, rămânerea informată și adoptarea de soluții avansate de securitate va contribui la asigurarea unei experiențe online sigure și securizate.

2.4 Protejarea informațiilor personale online: setări de confidențialitate și criptare a datelor

În societatea digitală de astăzi, protejarea informațiilor personale online este esențială. Creșterea utilizării internetului a adus confort, dar și riscuri sporite de încălcare a datelor, furt

de identitate și acces neautorizat. Înțelegerea setărilor de confidențialitate și utilizarea criptării datelor sunt strategii cruciale pentru protejarea informațiilor personale online. Acest subcapitol analizează importanța configurării corecte a setărilor de confidențialitate și rolul criptării în asigurarea securității datelor, susținut de informații din studii recente.

Setările de confidențialitate de pe platformele și aplicațiile online reprezintă prima linie de apărare împotriva accesului nedorit la informațiile personale. Cu toate acestea, mulți utilizatori consideră că este dificil să navigheze în aceste setări. Cercetarea lui Ye et al. (2022) evidențiază dificultatea cu care se confruntă utilizatorii în configurarea setărilor de confidențialitate pe rețelele sociale online (OSN). Studiul lor a introdus PrivacyRec, un sistem de recomandare bazat pe învățare profundă care sugerează setări optime de confidențialitate bazate pe conținutul generat de utilizatori și comportamentul contului. Această abordare îmbunătățește semnificativ capacitatea utilizatorului de a-și gestiona confidențialitatea în mod eficient prin simplificarea procesului de configurare prin algoritmi avansați și analiza datelor utilizatorului. Prin automatizarea recomandărilor privind setările de confidențialitate, instrumente precum PrivacyRec pot reduce decalajul dintre intenția utilizatorului și controlul real al confidențialității, asigurându-se că chiar și cei mai puțin cunoscători de tehnologie pot menține o protecție robustă a confidențialității.

În contextul dependenței crescute de instrumentele de comunicare digitală în timpul pandemiei de COVID-19, conștientizarea setărilor de securitate și confidențialitate a devenit și mai critică. Alammary, Alshaikh și Pratama (2022) au studiat gradul de conștientizare de către membrii facultății cu privire la aceste setări în aplicațiile de videoconferință, care au devenit indispensabile pentru învățarea online. Descoperirile lor au demonstrat un nivel „slab” de conștientizare în rândul utilizatorilor, în special în rândul celor care au trebuit să se adapteze rapid la aceste tehnologii. Factori precum securitatea percepută, alfabetizarea digitală și familiaritatea cu aplicațiile au fost legați în mod semnificativ de o mai bună conștientizare și utilizare a setărilor de confidențialitate. Acest lucru subliniază nevoia de inițiative educaționale și design de interfață ușor de utilizat, care să facă setările de confidențialitate mai accesibile și mai ușor de înțeles pentru toți utilizatorii, reducând astfel potențialele vulnerabilități în mediile virtuale.

Criptarea este o altă componentă fundamentală a protecției informațiilor personale online. Se asigură că datele rămân confidențiale și securizate împotriva accesului neautorizat, fie în timpul transmiterii, fie în timpul stocării. Criptarea funcțională, de exemplu, permite utilizatorilor să

cripteze datele cu o cheie publică, permițând în același timp calcule specifice asupra datelor criptate folosind chei restricționate, așa cum a explicat Gay (2023). Această formă de criptare permite un control mai fin asupra accesului și utilizării datelor, făcând posibilă partajarea în siguranță a informațiilor sensibile chiar și în medii nesigure, cum ar fi serviciile cloud. Capacitatea de a efectua calcule restricționate fără a dezvălui întregul set de date este deosebit de valoroasă pentru păstrarea confidențialității și integrității datelor în diverse aplicații, de la asistență medicală la finanțe.

Semnificația confidențialității și a protecției datelor este evidențiată în continuare de cadrele legale, cum ar fi al patrulea amendament al Constituției SUA, care consacră dreptul la confidențialitate împotriva perchezițiilor și confiscărilor nerezonabile. Această bază legală întărește importanța protejării datelor cu caracter personal împotriva accesului neautorizat și subliniază necesitatea unor măsuri solide de securitate cibernetică. Prin respectarea drepturilor de confidențialitate ale persoanelor, platformele digitale și utilizatorii deopotrivă pot promova un ecosistem online mai sigur și mai de încredere.

Pe scurt, protejarea informațiilor personale online implică o abordare cu mai multe fațete. Utilizatorii trebuie să fie proactivi în configurarea setărilor de confidențialitate și să rămână informați cu privire la funcționalitățile acestor setări. Soluțiile avansate precum PrivacyRec pot ajuta la optimizarea configurațiilor de confidențialitate, în timp ce eforturile educaționale pot crește gradul de conștientizare cu privire la setările de securitate, în special în tehnologiile nou adoptate, cum ar fi aplicațiile de videoconferință. Tehnologiile de criptare, inclusiv criptarea funcțională, oferă o protecție robustă a datelor, asigurându-se că numai calculele autorizate pot fi efectuate pe datele criptate. În cele din urmă, cadre juridice puternice susțin aceste eforturi subliniind dreptul fundamental la viață privată. Împreună, aceste strategii formează o apărare cuprinzătoare împotriva nenumăratelor amenințări la adresa informațiilor personale în era digitală.

Capitolul 3

Instrumente și resurse pentru securitate cibernetică

3.1 Utilizarea software-ului antivirus și anti-malware: selecție și întreținere

În lumea foarte conectată de astăzi, nevoia de software robust antivirus și anti-malware a devenit indispensabilă. Cu amenințările ciberneticе în continuă evoluție, este esențial să înțelegem cum să selectați și să mențineți soluții antivirus eficiente. Deși au existat unele dezbateri cu privire la necesitatea software-ului antivirus de la terți, în special pe sistemele cu măsuri de securitate inerente precum Windows 11, consensul general este că o soluție antivirus robustă rămâne o linie crucială de apărare împotriva unei multitudini de amenințări ciberneticе (Garba et al., 2022). Acest subcapitol analizează importanța software-ului antivirus, criteriile de selectare a soluțiilor de încredere și cele mai bune practici pentru întreținerea acestor instrumente.

În primul rând, este esențial să înțelegem de ce sunt necesare instrumente antivirus și anti-malware. Amenințările ciberneticе sunt din ce în ce mai sofisticate, utilizând tehnici avansate pentru a se infiltra în sisteme. Rolul software-ului antivirus este de a detecta, preveni și elimina programele rău intenționate care ar putea compromite datele și integritatea sistemului. Potrivit Pérez-Sánchez și Palacios (2022), software-ul antivirus standard se confruntă cu provocări în detectarea amenințărilor care utilizează tehnici avansate de evaziune, cum ar fi extragerea din memorie. Studiul lor a demonstrat că soluțiile antivirus comerciale nu reușesc uneori să detecteze încărcăturile rău intenționate, subliniind necesitatea unor măsuri de securitate avansate și complementare.

Când vine vorba de selectarea software-ului antivirus, înțelegerea nevoilor specifice ale utilizatorului este esențială. Piața este inundată de diverse soluții antivirus și anti-malware, fiecare promițând o protecție de neegalat. O diferențiere semnificativă constă în metoda de detectare și clasificare a amenințărilor folosită de fiecare software. Programele antivirus tradiționale se bazează în general pe detectarea bazată pe semnături, care identifică amenințările cunoscute printr-o bază de date de semnături malware. Cu toate acestea, după cum au remarcat Pérez-Sánchez și Palacios (2022), actorii amenințărilor în evoluție folosesc tactici precum obscurcarea pentru a ocoli metodele tradiționale de detectare. Prin urmare, este recomandabil să optați pentru software antivirus care combină detectarea bazată pe semnătură

cu metodologiile euristice și bazate pe comportament. Această combinație este mai abil în identificarea și atenuarea amenințărilor noi, necunoscute anterior.

În plus, capacitatea unei soluții antivirus nu este definită doar de protocoalele sale de detectare, ci și de capacitatea sa de a se integra cu alte mecanisme de apărare. De exemplu, Garba et al. (2022) a ridicat o întrebare importantă despre dacă utilizatorii Windows 11 au nevoie de software antivirus de la terți. Cercetările lor au indicat că măsurile de securitate încorporate ale Windows 11, evaluate în raport cu mai multe instrumente de evaziune antivirus gratuite și open-source, ar putea rezista în mod independent anumitor amenințări. Cu toate acestea, ei au subliniat, de asemenea, că o soluție antivirus terță parte ar putea suplimenta și îmbunătăți securitatea încorporată, oferind o rețea de siguranță suplimentară împotriva atacurilor sofisticate care apar continuu.

Întreținerea este un alt aspect critic care are un impact semnificativ asupra eficacității instrumentelor antivirus. Sunt necesare actualizări și corecții regulate pentru a se asigura că software-ul rămâne eficient împotriva amenințărilor nou dezvoltate. Dezvoltatorii de antivirus lansează frecvent actualizări ale bazelor de date de amenințări și ale funcționalităților software. Prin urmare, utilizatorii trebuie să activeze actualizările automate sau să verifice în mod regulat noi versiuni pentru a-și menține protecția actuală. Scanările regulate ale sistemului ar trebui, de asemenea, programate pentru a identifica și atenua cu promptitudine potențialele amenințări. Pérez-Sánchez și Palacios (2022) subliniază că sistemele învechite sunt mai vulnerabile la atacuri, deoarece soluțiile antivirus mai vechi ar putea să nu recunoască forme mai noi de malware, subliniind importanța menținerii software-ului la zi.

În cele din urmă, conștientizarea, formarea și educarea utilizatorilor joacă un rol indispensabil în menținerea soluțiilor antivirus eficiente. Utilizatorii ar trebui să fie educați cu privire la riscurile potențiale de descărcare de software neverificat, de clic pe linkuri de e-mail necunoscute sau de partajarea informațiilor sensibile fără o criptare adecvată. Avocatul software-ului liber Richard Stallman (2002) a subliniat importanța alfabetizării utilizatorilor în libertatea și securitatea digitală. Educarea utilizatorilor cu privire la bunele practici de securitate cibernetică nu numai că completează garanțiile tehnice oferite de software-ul antivirus, ci și reduce în mod inerent șansele de a deveni victima atacurilor de phishing, a programelor malware și a altor amenințări cibernetice.

În concluzie, în timp ce dezbateră privind necesitatea software-ului antivirus de la terți poate persista, în special pentru sisteme precum Windows 11 cu apărări solide încorporate, consensul

este clar: soluțiile antivirus și anti-malware sunt indispensabile în peisajul modern de amenințări cibernetice. Selectarea cu atenție a soluțiilor antivirus avansate, menținerea lor regulată prin actualizări și scanări și educarea utilizatorilor cu privire la cele mai bune practici de securitate cibernetică întăresc în mod colectiv apărarea unui sistem împotriva potențialelor amenințări cibernetice.

3.2 Activarea autentificării în doi factori (2FA) pentru conturi și dispozitive

Autentificarea cu doi factori (2FA) servește ca un nivel esențial de securitate dincolo de utilizarea tradițională a numelor de utilizator și a parolelor. Această măsură de securitate cibernetică îmbunătățește protecția contului, solicitând două forme de identificare înainte de a acorda acces: de obicei ceva pe care îl cunoașteți (o parolă) și ceva pe care îl aveți (un telefon sau un token hardware). În ciuda beneficiilor sale în consolidarea securității, implementarea și adoptarea 2FA se confruntă cu provocări semnificative de utilizare. Chiar dacă multora dintre utilizatori nu le place asta, este o soluție sigură.

Utilizarea facilă rămâne un factor critic în adoptarea pe scară largă a 2FA. Potrivit Pandey și Taffese (2021), problemele de utilizare în timpul fazei de configurare împiedică în mod semnificativ adoptarea la scară largă de către utilizatori. Abordarea acestor probleme de utilizare nu este doar o chestiune de comoditate, ci are un impact direct asupra faptului că utilizatorii se vor implica cu 2FA.

Într-adevăr, Acemyan și colab. (2018) subliniază că, deși 2FA adaugă un nivel de securitate crucial, poate fi împovărător pentru utilizatori. Studiul lor evaluează diferite metode 2FA oferite de Google, găsind diferențe minime de utilizare între diferite metode 2FA. Metrici precum eficiența, eficacitatea și satisfacția utilizatorilor indică faptul că toate metodele au loc de îmbunătățire. În special, faza de configurare inițială este adesea cea în care utilizatorii întâmpină cele mai multe frecări, descurajându-i să finalizeze procesul de autentificare. În consecință, cercetarea sugerează o nevoie urgentă pentru dezvoltatori de a simplifica și accelera procesul de integrare pentru 2FA pentru a crește gradul de adoptare de către utilizatori.

Lyastani, Backes și Bugiel (2022) analizează călătoriile utilizatorilor 2FA pe site-uri web de top. Studiul lor evidențiază o lipsă semnificativă de coerență în aspectele de design, cum ar fi denumirea și locația setărilor 2FA. Această inconsecvență introduce un oarecare disconfort, ceea ce duce adesea la frustrarea utilizatorului și la eventuala respingere a 2FA. Unele aspecte,

chiar și atunci când au fost realizate în mod constant pe site-uri, au fost identificate ca problematice și dăunătoare experienței utilizatorului. De exemplu, procesele de configurare inconsistente și descrierile neclare pot deruta utilizatorii, diminuând valoarea percepută a 2FA. Studiul pledează pentru liniile directoare standardizate UX pentru a simplifica *călătoria* utilizatorului 2FA pe diferite platforme.

În plus față de utilizare, liniile directoare furnizate de NIST (2017) subliniază importanța integrării 2FA în cadre mai largi de gestionare a identității digitale. Conform acestor linii directoare, 2FA ar trebui să fie proiectat pentru a fi atât sigur, cât și ușor de utilizat. Acest echilibru este critic deoarece măsurile de securitate prea complexe pot îndepărta utilizatorii, în timp ce măsurile simplificate ar putea compromite securitatea. NIST subliniază nevoia de actualizări periodice și corecții pentru sistemele 2FA pentru a aborda amenințările emergente la adresa securității cibernetice și pentru a menține robustețea.

În concluzie, în timp ce 2FA este o componentă esențială în protejarea identităților digitale, implementarea sa este plină de provocări, în special în ceea ce privește gradul de utilizare. Studiile indică faptul că elementele de design mai consistente și intuitive pot îmbunătăți substanțial ratele de adoptare ale utilizatorilor. Dezvoltatorii sunt încurajați să se concentreze pe simplificarea proceselor de configurare și utilizare, menținând în același timp măsuri de securitate robuste. Folosirea instrumentelor de analiză predictivă a performanței și aderarea la liniile directoare standardizate UX poate crea o experiență de utilizator 2FA mai fluidă, mai rapidă și mai fiabilă. Această abordare holistică a 2FA nu numai că întărește securitatea, dar asigură și că utilizatorii au șanse mai mari să se implice și să beneficieze de acest instrument esențial de securitate cibernetică.

3.3 Actualizări regulate de software și corecții: importanță și bune practici

Una dintre practicile fundamentale în asigurarea securității cibernetice este actualizarea și corecția regulată a software-ului. Această practică este vitală nu numai pentru utilizatorii individuali, ci și pentru companii și organizații de toate dimensiunile. Actualizările regulate ajută la abordarea vulnerabilităților care ar putea fi exploatare de actori rău intenționați, îmbunătățind astfel poziția generală de securitate a sistemelor.

Importanța actualizărilor regulate de software poate fi înțeleasă analizând peisajul care evoluează rapid al amenințărilor cibernetice. Infracții cibernetice găsesc continuu noi

modalități de a exploata vulnerabilitățile din software. De exemplu, dispozitivele Internet of Things (IoT), care devin din ce în ce mai omniprezente, sunt deosebit de vulnerabile la diferite atacuri datorită capacităților lor de calcul limitate. Gupta și Oorschot (2019) evidențiază importanța unui mecanism de actualizare securizat și automatizat pentru dispozitivele IoT, având în vedere puterea și memoria lor limitate de procesare. Ei propun o arhitectură care utilizează criptografia cu curbă eliptică (Curve25519) și stabilirea cheilor autentificate pentru a se asigura că actualizările software sunt atât sigure, cât și eficiente. Această arhitectură implică un mecanism de blocare a tastelor bazat pe continuitate, în care o cheie publică încorporată în imaginea software curentă verifică semnătura oricăror actualizări. Această abordare nu numai că protejează dispozitivele IoT de potențiale exploatari, dar asigură și faptul că dispozitivele rămân funcționale chiar dacă producătorul încetează să ofere actualizări.

O altă industrie care beneficiază enorm de pe urma actualizărilor regulate de software este sectorul auto. Tranziția de la sistemele tradiționale centrate pe hardware la arhitecturi avansate, definite de software, a permis o autonomie, conectivitate și caracteristici de siguranță îmbunătățite în vehicule. Bazzi și colab. (2024) discută o metodologie de actualizare a software-ului bogată în variabilitate folosind o abordare Merkle arbore, care este deosebit de eficientă în tratarea cu mai multe unități de control electronic distribuite (ECU). Această metodă asigură coerența pe toate platformele, ceea ce este crucial având în vedere complexitatea arhitecturilor moderne de vehicule. Actualizările regulate ale software-ului în acest context nu numai că îmbunătățesc caracteristicile vehiculului, ci și mențin standarde înalte de siguranță și securitate, care sunt esențiale pentru industria auto modernă.

Pe lângă aceste aplicații specializate, actualizările și corecțiile regulate sunt cruciale pentru software-ul obișnuit utilizat în computerele personale și dispozitivele mobile. Legea Sarbanes-Oxley (2002), deși se concentrează în primul rând pe governanța corporativă și practicile financiare, influențează indirect securitatea cibernetică prin obligarea stabilirii de controale interne care pot include actualizări regulate de software și gestionarea corecțiilor. Companiile care aderă la aceste reglementări sunt în general mai bine echipate pentru a preveni încălcările de securitate care ar putea apărea din cauza software-ului învechit.

Cele mai bune practici pentru actualizări regulate de software includ nu doar instalarea automată a actualizărilor, ci și o strategie cuprinzătoare care implică educarea utilizatorilor cu privire la importanța acestor actualizări. Programele de conștientizare pot ajuta utilizatorii să înțeleagă că actualizările includ adesea corecții critice de securitate care le protejează datele și

confidențialitatea. O altă bună practică este utilizarea sistemelor centralizate de gestionare a corecțiilor în setările organizaționale. Aceste sisteme asigură că toate dispozitivele sunt actualizate într-o manieră coordonată, reducând șansele de a avea vulnerabilități în rețea.

Mai mult, practica de a testa actualizările înainte de a le implementa într-un mediu live este crucială. Acest lucru asigură că actualizările nu introduc din neatenție probleme noi sau conflicte cu sistemele existente. Organizațiile ar trebui, de asemenea, să mențină un inventar al tuturor software-urilor și dispozitivelor, asigurându-se că toate sunt actualizate. Acest lucru poate fi facilitat de instrumente automate care scanează actualizările lipsă și alertează administratorii.

Pe scurt, peisajul amenințărilor cibernetice necesită o abordare proactivă a actualizărilor software și a corecțiilor. Folosirea mecanismelor de actualizare sigure, așa cum sunt propuse de Gupta și Oorschot (2019) pentru dispozitivele IoT și de Bazzi și colab. (2024) pentru sistemele auto poate spori semnificativ securitatea. În plus, aderarea la cadrele de reglementare precum Legea Sarbanes-Oxley asigură că organizațiile mențin controale interne solide, care includ actualizări regulate de software. Urmând aceste bune practici, indivizii și organizațiile deopotrivă își pot reduce în mod semnificativ vulnerabilitatea la atacurile cibernetice.

3.4 Rămâneți informat cu privire la evoluțiile securității cibernetice: știri, bloguri și resurse educaționale deschise

Într-o epocă în care amenințările cibernetice devin din ce în ce mai sofisticate, a rămâne informat cu privire la evoluțiile securității cibernetice este esențial pentru persoanele care doresc să-și protejeze prezența digitală. Educația și conștientizarea continuă pot contribui la atenuarea riscurilor, oferind utilizatorilor cunoștințele necesare pentru a recunoaște și a răspunde eficient amenințărilor emergente. Această secțiune explorează diverse resurse, cum ar fi posturi de știri, bloguri și platforme educaționale pe care persoanele fizice le pot utiliza pentru a fi la curent cu evoluțiile securității cibernetice.

Una dintre căile cheie pentru a rămâne informat este prin intermediul știrilor specializate în domeniul securității cibernetice și al motoarelor de informații despre amenințări. Un exemplu este SecBuzzer, o platformă multicanal concepută pentru a colecta informații despre amenințări din diverse surse, inclusiv sisteme publice de diseminare a amenințărilor, cum ar fi NVD (National Vulnerability Database) și CERT (Computer Emergency Response Team) (Huang,

Huang și Mao, 2019). SecBuzzer folosește inteligența crowdsourced și contribuie la un model de alertă de amenințări cibernetice bazat pe rețea, oferind astfel perspective complete asupra amenințărilor emergente. Pentru utilizatorul obișnuit, abonarea la astfel de platforme poate oferi alerte critice și actualizări cu privire la cele mai recente activități rău intenționate și potențiale vulnerabilități, ceea ce reprezintă un atu de neprețuit în menținerea unei igiene solide a securității cibernetice.

Resursele educaționale au câștigat, de asemenea, importanță, în special în timpul pandemiei de COVID-19, care a necesitat o trecere la medii de învățare la distanță. Instituții precum Murray State University (MSU) s-au adaptat prin integrarea platformelor precum Discord pentru a construi comunități educaționale virtuale (Joyce, Sahawneh și Dixon, 2022). Prin astfel de platforme, atât studenții, cât și profesorii se pot angaja în comunicare în timp real, pot partaja resurse și pot participa la sesiuni de învățare interactivă axate pe securitatea cibernetică. Aceste comunități nu numai că îmbunătățesc înțelegerea conceptelor de securitate cibernetică, dar și țin participanții la curent cu cele mai recente tendințe și amenințări. Prin alăturarea sau formarea unor grupuri similare de învățare colaborativă, indivizii pot beneficia de cunoștințe colective și de împărtășirea experienței.

În plus, integrarea exercițiilor practice și a experiențelor practice în educația în domeniul securității cibernetice este crucială pentru dezvoltarea unei înțelegeri mai profunde. După cum Weiss și colab. (2021) sugerează că competițiile și exercițiile axate pe securitate au devenit mai răspândite și ar trebui încorporate în programele educaționale. Aceste activități oferă expunere practică la scenarii din lumea reală, ajutând participanții să-și dezvolte abilitățile necesare pentru a detecta și a răspunde amenințărilor cibernetice. Prin implicarea în astfel de exerciții, indivizii pot rămâne la curent cu tehnicile și instrumentele utilizate în securitatea cibernetică, îmbunătățindu-și astfel capacitățile defensive.

Sfatul etern al lui Benjamin Franklin, „O investiție în cunoaștere plătește întotdeauna cel mai bun interes”, servește drept principiu călăuzitor în domeniul educației în domeniul securității cibernetice. A se menține educat și informat cu privire la cele mai recente evoluții nu este doar o opțiune, ci o necesitate. Platformele și resursele moderne oferă oportunități ample de învățare continuă. De exemplu, blogurile de securitate cibernetică oferă adesea informații actualizate despre noile vulnerabilități, corecții și bune practici. Abonarea la bloguri și site-uri de știri bine respectate, cum ar fi Krebs on Security sau The Hacker News, poate îmbunătăți în mod semnificativ înțelegerea și vigilența cuiva la noile amenințări și tehnici defensive.

Pe lângă acestea, participarea la seminarii web și ateliere online găzduite de experți în securitate cibernetică poate fi incredibil de benefică. Aceste sesiuni de obicei aprofundează mai profund în aspectele specifice ale apărării cibernetice, oferind perspective care nu sunt ușor disponibile prin alte medii. De asemenea, oferă oportunități de creare de rețele, permițând participanților să se conecteze cu profesioniști din industrie și colegi, promovând o comunitate de practică care contribuie la învățarea comună și la îmbunătățirea continuă.

Legea nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României

Scopul Legii: Legea nr. 58/2023 stabilește cadrul juridic pentru securitatea și apărarea cibernetică a României, având ca scop protejarea infrastructurii critice și prevenirea atacurilor cibernetice la nivel național. Aceasta include măsuri pentru a consolida securitatea cibernetică și pentru a îmbunătăți capacitatea de apărare împotriva amenințărilor cibernetice.

Domenii vizate:

1. **Infrastructura critică:** Legea se aplică instituțiilor publice, operatorilor economici și organizațiilor care dețin sau gestionează infrastructură critică.
2. **Protecția datelor:** Se instituie măsuri stricte pentru protejarea datelor confidențiale, inclusiv ale persoanelor fizice și juridice.
3. **Colaborarea interinstituțională:** Este promovată cooperarea între instituțiile publice și private pentru a asigura un răspuns prompt și eficient la incidentele cibernetice.

Principalele prevederi:

- **Responsabilități instituționale:** Autoritățile statului, precum Serviciul Român de Informații (SRI) și alte agenții, au atribuții sporite în detectarea și prevenirea atacurilor cibernetice.
- **Obligații pentru entitățile vizate:** Toți operatorii de infrastructură critică trebuie să implementeze măsuri minime de securitate cibernetică și să raporteze incidentele către autoritățile competente.
- **Formarea personalului:** Se pune un accent puternic pe instruirea și certificarea experților în securitate cibernetică pentru a gestiona riscurile emergente.

Măsuri de securitate și apărare cibernetică:

- **Planuri de apărare:** Instituțiile sunt obligate să dezvolte și să actualizeze planuri de apărare cibernetică pentru a răspunde la atacuri și breșe de securitate.
- **Monitorizare și control:** Autoritățile pot desfășura activități de monitorizare a rețelelor și sistemelor informatice pentru a preveni și a detecta atacuri.
- **Sanctiuni:** Legea prevede sancțiuni pentru entitățile care nu respectă obligațiile privind securitatea cibernetică, inclusiv amenzi considerabile.

Impactul legii: Această lege este esențială în contextul creșterii amenințărilor cibernetice la nivel global și în România. Prin întărirea cadrului juridic și a colaborării între entitățile publice și private, se urmărește reducerea vulnerabilităților și asigurarea securității naționale în spațiul cibernetic.

Publicare oficială: Legea a fost publicată în *Monitorul Oficial al României, Partea I, nr. 214 din 15 martie 2023* și a intrat în vigoare la data publicării.

În concluzie, a rămâne informat cu privire la evoluțiile securității cibernetice necesită o abordare cu mai multe fațete, valorificând știri și platforme de informații despre amenințări, comunități educaționale, exerciții practice și oportunități de învățare continuă. Utilizarea acestor resurse nu numai că îmbunătățește conștientizarea și cunoștințele cuiva, ci îi permite și utilizatorilor obișnuiți să se apere mai bine împotriva peisajului în continuă evoluție al amenințărilor cibernetice.

PARTEA A II-A

GHID PRACTIC

“Acum toți suntem conectați prin internet, ca neuronii dintr-un creier uriaș.”

Stephen Hawking

ALICE GEORGESCU

Lumea securității cibernetice este un peisaj vast și în continuă evoluție, esențial în era hiperconectată de astăzi. Acest text explorează elementele fundamentale ale securității cibernetice, cum ar fi protecția rețelelor, securitatea informațiilor, securitatea aplicațiilor, protecția punctelor finale, și securitatea în cloud. În capitolele următoare sunt abordate concepte precum managementul identității și accesului (IAM), răspunsul la incidente, și Threat Intelligence. De asemenea, sunt prezentate provocările actuale, inclusiv complexitatea amenințărilor, factorul uman, și conformitatea reglementărilor.

Se subliniază importanța protejării datelor personale și confidențialității, oferind practici pentru utilizatori individuali și organizații. De asemenea, sunt prezentate strategii specifice pentru protejarea datelor în mediul educațional și pentru educația digitală a elevilor și profesorilor. Conformitatea cu reglementări precum GDPR, CCPA și HIPAA este crucială pentru menținerea confidențialității și securității în mediul online.

Cuvinte chei: Securitate cibernetică, Threat Intelligence, Răspuns la incidente, IAM, GDPR, Zero Trust, AI, Ransomware, Phishing, Protecția datelor, Confidențialitate, Atacatori cibernetici, Educație digitală, Malware, Cloud Security, Endpoint Protection.

Capitolul 4

Lumea securității cibernetice

Lumea securității cibernetice este vastă, dinamică și în continuă evoluție, deoarece cuprinde instrumentele, practicile și strategiile utilizate pentru a proteja de amenințările cibernetice atât sistemele digitale și rețelele cât și datele.

Securitatea cibernetică este crucială în lumea hiperconectată de astăzi, deoarece apără totul - de la dispozitive individuale până la infrastructura națională critică – de criminali cibernetici, hacktiviști și chiar actori reprezentând state naționale.

O succintă prezentare a acestei lumi ne obligă să abordăm o prezentare generală a elementelor de bază dar și o evaluare a tendințelor emergente, a provocărilor din lumea securității cibernetice și a viitorului acestei lumi.

4.1 Elementele de bază ale securității cibernetice

Pentru a înțelege lumea cibernetică trebuie să stăpânim înțelegerea câtorva termeni de bază cu care limbajul acesteia operează.

Securitatea rețelei

Asigurarea securității unei rețele, și putem să ne referim la rețeaua locală a unei organizații sau la rețelele guvernamentale, implică protejarea integrității, confidențialității și accesibilității rețelei și a datelor transmise prin aceasta.

Ea include sisteme de tip firewall, sisteme de detectare a intruziunilor (IDS Intrusion Detection System) și controale de acces la rețea pentru a preveni accesul neautorizat și a atenua amenințările.

Securitatea informațiilor (InfoSec)

Asigurarea securității informațiilor se concentrează pe protejarea confidențialității, integrității și disponibilității datelor, indiferent dacă sunt în repaus sau în tranzit. Confidențialitatea, Integritatea și Disponibilitatea, denumite adesea triada CIA (Confidentiality, Integrity and

Availability - nu are nimic de-a face cu Agenția Centrală de Informații!), sunt principiile de bază, dar fundamentale pentru menținerea securității solide într-un mediu dat.

Ea include criptarea, mascarea datelor și practicile de stocare securizată.

Securitatea aplicației

Asigurarea securității aplicațiilor implică securizarea aplicațiilor software de vulnerabilități pe tot parcursul ciclului lor de viață, de la dezvoltare până la implementare. Acestea includ practici de codare sigure, corecții regulate și evaluări periodice ale vulnerabilităților.

Securitate punct final

Punctele finale (End Point) sunt dispozitive fizice care se conectează la o rețea de calculatoare și fac schimb de informații cu aceasta. Ca exemple de puncte finale putem enumera dispozitivele mobile, computerele desktop, mașinile virtuale, serverele, dispozitivele Internet-of-Things (camere de supraveghere, dispozitive de control al iluminării sau temperaturii).

Securitate punctelor finale implică protejarea acestora prin folosirea unui software antivirus, a sistemelor EDR (Endpoint Detection and Response) și a unor mecanisme puternice de autentificare.

Securitate în cloud

Pe măsură ce tot mai multe organizații trec la infrastructura bazată pe cloud, securitatea în cloud se concentrează pe securizarea datelor și a aplicațiilor găzduite în acesta. Securitatea în cloud include implementarea managementului identității, criptării datelor și controalelor de acces.

Gestionarea identității și a accesului (IAM - Identity Access Management)

Managementul identității, cunoscut și sub numele de management al identității și al accesului, este un cadru de politici și tehnologii care asigură că numai utilizatorii autorizați pot accesa anumite resurse. Acesta include autentificare (verificarea identității unui utilizator) și autorizare (acordarea de permisiuni).

Autentificarea cu mai mulți factori (MFA - Multi-Factor Authentication) și autentificarea unică (SSO - Single Sign-On) sunt exemple de strategii IAM.

Răspuns la incident și managementul incidentului

Răspunsul la incident și managementul incidentului se referă la procesul de identificare, gestionare și recuperare în urma incidentelor de securitate cibernetică. Acestea includ crearea de planuri de răspuns la incident (IRP - Incident Response Plan), efectuarea de investigații criminalistice și implementarea strategiilor de izolare și recuperare. Toate organizațiile ar trebui să aibă un plan de răspuns la incident. Acesta este un document scris, aprobat oficial de echipa de conducere, care va ajuta organizația înainte, în timpul și după un incident de securitate confirmat sau suspectat. El clarifică rolurile și responsabilitățile și oferă îndrumări cu privire la activitățile cheie. De asemenea, ar trebui să includă o listă de securitate cibernetică a persoanelor cheie care ar putea fi necesare în timpul unei crize.

Threat Intelligence

Informațiile privind amenințările cibernetică cuprind date extinse, concepute pentru a anticipa și a contracara amenințările specifice unei organizații, indiferent de dimensiunea acestia, industria din care face parte sau nivelul de maturitate a securității cibernetică al organizației.

Threat Intelligence se referă la colectarea și analiza informațiilor privind amenințările emergente, vulnerabilitățile și metodele de atac pentru a anticipa și a răspunde la potențiale incidente de securitate.

Conformitate și reglementări

Securitatea cibernetică este puternic reglementată în multe industrii, cu legi și standarde precum GDPR (General Data Protection Regulation), HIPAA (Health Insurance Portability and Accountability Act) și PCI DSS (Payment Card Industry Data Security Standard) care ghidează organizațiile cu privire la modul de protejare a informațiilor sensibile.

Amenințare sau atac cibernetic

Un atac cibernetic este o încercare rău intenționată și deliberată a unei persoane sau a unei organizații de a încălca sistemul de informații al altei persoane sau organizații. De obicei, atacatorul caută un anumit tip de beneficiu de la întreruperea rețelei victimei.

Putem distinge mai multe tipuri de amenințări cibernetice însă vom descrie pe scurt doar 10 dintre acestea ⁶ :

1. Malware: software rău intenționat conceput pentru a perturba, deteriora sau obține acces neautorizat la un sistem. Exemplele includ viruși, viermi, ransomware și spyware.
2. Phishing: un atac în care infractorii cibernetici păcălesc victimele să dezvăluie informații personale, cum ar fi parole sau numere de card de credit, dându-se drept entități legitime în e-mailuri, mesaje text sau apeluri telefonice.
3. Ransomware: un tip de malware care criptează datele unei victime, atacatorii cerând o răscumpărare pentru decriptare. Ransomware-ul a devenit o amenințare cibernetică de vârf la nivel mondial, afectând atât organizațiile, cât și persoanele fizice.
4. Inginerie socială: Tactici care manipulează indivizi pentru a efectua acțiuni sau a divulga informații confidențiale, cum ar fi prin uzurparea identității, înșelăciunea sau manipularea emoțională.
5. DDoS (Distributed Denial of Service): un atac care inundă un sistem cu trafic, copleșindu-l și făcându-l inaccesibil pentru utilizatorii legitimi.
6. Amenințări interne: amenințări care provin de la indivizi din cadrul unei organizații, cum ar fi angajații, care pot cauza prejudicii intenționat sau neintenționat securității digitale a organizației.
7. Amenințări persistente avansate (APT): Campanii de spionaj cibernetic pe termen lung, țintite, desfășurate de actori sofisticăți, adesea state naționale, care își mențin prezența în rețeaua victimei pentru perioade îndelungate.
8. Zero-Day Exploits: Atacurile care exploatează vulnerabilități în software care sunt necunoscute furnizorului de software și pentru care încă nu au fost realizate patch-uri de securitate.
9. Atacuri Man-in-the-Middle (MitM): Atacatorii interceptează și manipulează comunicarea dintre două părți fără știrea lor, adesea pentru a fura date sau acreditări.

⁶ o lista mai completă poate fi găsită pe site-ul companiei Fortinet la adresa <https://www.fortinet.com/resources/cyberglossary/types-of-cyber-attacks>

10. SQL Injection: Atacatorii exploatează vulnerabilitățile din baza de date a unei aplicații web prin injectarea de cod SQL rău intenționat, care le poate permite să acceseze, să modifice sau să șteargă date.

4.2 Tendințe cheie în securitatea cibernetică

Conform raportului Fortinet 2023 “în a doua jumătate a anului 2023, peisajul securității cibernetică a înregistrat dezvoltări semnificative care au impactat considerabil suprafața de atac digital. Printre acestea, s-a remarcat creșterea atacurilor cibernetică sofisticate care vizează entități de mari dimensiuni și infrastructura esențială”.⁷

Inteligență artificială (AI) și învățare automată (ML – Machine Learning) sunt din ce în ce mai utilizate în securitatea cibernetică atât defensivă, cât și ofensivă. Pe partea defensivă, acestea sunt aplicate în detectarea anomaliilor, răspunsul automat la amenințări și monitorizarea securității. Cu toate acestea, atacatorii folosesc AI pentru atacuri mai sofisticate, cum ar fi e-mailurile de phishing generate de AI sau ocolirea sistemelor de securitate.

Au apărut grupurile de ransomware, care au adoptat un model de afaceri în care oferă instrumente de ransomware pentru o taxă sau o parte din profit - Rise of Ransomware-as-a-Service (RaaS). Acest lucru a redus bariera de intrare pentru atacatorii mai puțin calificați, dar a contribuit la creșterea numărului de incidente ransomware.

A crescut și numărul atacurilor care vizează elemente mai puțin sigure din cadrul lanțului de aprovizionare al unei organizații, atacuri prin care un cod rău intenționat a fost injectat în actualizările software. Aceste atacuri au evidențiat riscurile prezentate de furnizorii terți.

Pe măsură ce mai multe organizații migrează către cloud, se confruntă cu noi provocări de securitate, cum ar fi configurații greșite, breșe ale securității datelor și probleme de conformitate. Astfel că securizarea mediilor și serviciilor cloud precum SaaS (Software as a Service) și IaaS (Infrastructure as a Service) a devenit o prioritate.

⁷ Raport Fortinet 2023 <https://www.fortinet.com/resources/analyst-reports/threat-report-2h-2023>

Arhitectura Zero Trust (ZTA)⁸ a devenit rapid o piatră de temelie a securității cibernetice moderne și implicațiile ei pentru afaceri devin din ce în ce mai profunde. Conceptul principal din spatele modelului de securitate Zero Trust este „nu ai încredere niciodată, verifică întotdeauna”, ceea ce înseamnă că niciun utilizator sau dispozitiv, în interiorul sau în afara rețelei, nu este automat de încredere. Ca urmare accesul este acordat pe baza unei verificări stricte a identității și a politicilor, și contribuie la reducerea căilor de atac.

Odată cu proliferarea dispozitivelor IoT în case, întreprinderi și infrastructura critică, securizarea acestor dispozitive adesea subprotejate este o provocare în creștere. Dispozitivele IoT pot fi exploatate ca puncte de intrare în rețele mai mari.

Deși încă în stadiile sale incipiente, calculul cuantic reprezintă atât o amenințare viitoare, cât și o oportunitate. Calculatoarele cuantice ar putea schimba metodele tradiționale de criptare, ceea ce înseamnă că dezvoltarea criptării rezistente la cuanți este deja în curs.

Există o lipsă globală de profesioniști calificați în securitate cibernetică, ceea ce pune presiune asupra organizațiilor pentru a menține poziții de securitate robuste. Se preconizează că această lipsă va crește, crescând cererea de formare și educație în domeniul securității cibernetice.

4.3 Provocări în securitatea cibernetică

În lumea în care trăim sunt o mulțime de variabile care apar și influențează totul, ca într-un efect de domino: un hacker din Rusia, un tsunami din Asia, un grup terorist din Orient sau ...

Lumea cibernetică, deși este o lume “mai nouă” este supusă unor provocări constante pe multiple paliere.

Complexitatea amenințărilor

Amenințările cibernetice devin din ce în ce mai sofisticate. În același timp, consecință directă a proceselor de transformare digitală stimulate de progresul unei lumi din ce în ce mai

⁸ O descriere detaliată a acestui tip de arhitectură se găsește la adresa https://en.wikipedia.org/wiki/Zero_trust_security_model

tehnologizate, zona expusa a unei companii este din ce în ce mai extinsă, A ține pasul cu aceste amenințări în evoluție este o provocare constantă.

Extinderea rețelelor de tip dark web, mai ales după perioada pandemiei de COVID-19, reprezintă o provocare majoră și întărește importanța efectuării activităților de informare despre amenințările posibile din aceste colțuri întunecate ale internetului. Conform unui raport al Cybersecurity Ventures⁹, se preconizează că costurile globale ale criminalității ar putea ajunge la 10,5 trilioane de dolari pe an.

Echilibrare între securitate și utilizare, conformitate vs. securitate

Devine tot mai dificilă găsirea echilibrului corect între măsurile stricte de securitate și confortul utilizatorului. Folosirea unor protocoale de securitate puternice pot împiedica uneori productivitatea, și asta poate conduce la respingerea de către utilizatori a diverselor produse.

Organizațiile se concentrează adesea pe îndeplinirea conformității cu reglementările, mai degrabă decât pe asigurarea securității reale. A fi conform nu înseamnă întotdeauna a fi în siguranță, ceea ce poate lăsa organizațiile vulnerabile la atacuri.

Factorul uman

În ciuda progreselor tehnologice, oamenii rămân veriga cea mai slabă a securității cibernetice.

Ingenieria socială, phishingul și eroarea umană contribuie la un procent mare de încălcări ale protocoalelor de securitate. Prin urmare, educația și conștientizarea utilizatorilor sunt vitale.

Lipsa de personal certificat și calificat pentru a satisface cererea tot mai mare de profesioniști din domeniul securității cibernetice continuă să crească. Forumul Economic Mondial, în colaborare cu mai multe companii, a lansat o platformă de educație online destinată atât persoanelor fizice cât și organizațiilor numită Cybersecurity Learning Hub¹⁰. Scopul acestui proiect este de a forma și de a îmbunătăți abilitățile profesioniștilor în securitate

Securizarea lucrului de la distanță:

⁹ <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>

¹⁰ <https://www.weforum.org/projects/cybersecurity-learning-hub/>

Trecerea la munca de la distanță din cauza pandemiei de COVID-19 a creat noi provocări de securitate. Securizarea rețelelor de acasă, a dispozitivelor și a accesului de la distanță la sistemele corporative este crucială pentru menținerea unui mediu de lucru sigur.

4.4 Viitorul securității cibernetice

Viitorul securității cibernetice va fi probabil modelat de atât de progresele tehnologice și interconectivitatea tot mai mare a sistemelor cât și de amenințările persistente din partea infractorilor cibernetici.

Ca urmare direcțiile de interes în ceea ce privește dezvoltarea domeniului securității cibernetice includ: ¹¹

- Automatizare și IA: Pe măsură ce amenințările cibernetice devin mai complexe, automatizarea detectării și a răspunsului amenințărilor va fi esențială pentru gestionarea atacurilor la scară largă.
- Criptografie post-cuantică: pregătirea metodelor de criptare pentru apariția calculului cuantic.
- Confidențialitate și protecția datelor: Cu cât mai multe date sunt colectate și stocate online, asigurarea unei protecții solide a confidențialității va rămâne o preocupare principală.
- Reziliența cibernetică: în loc să se concentreze exclusiv pe prevenire, strategiile viitoare vor acorda prioritate rezilienței, capacității de a se recupera rapid după incidente.

¹¹ Informațiile au fost preluate din următoarele documente:

1. https://www.researchgate.net/publication/381779828_A_Report_on_The_Future_Landscape_of_Cybersecurity
2. https://www.researchgate.net/publication/372778266_The_Future_of_Cybersecurity_and_Its_Potential_Threats

Capitolul 5

Victime și Atacatori

“Învață din greșelile altora. Nu vei trăi atât de mult încât să le faci tu pe toate”

Eleanor Roosevelt

Lumea securității cibernetice este un peisaj în continuă schimbare, în care victimele, apărătorii și atacatorii sunt blocați într-o luptă continuă. Ce putem face pentru ca în această luptă să nu devenim victime? Cum putem să îi identificăm pe atacatori? Pentru a putea răspunde, în parte, la aceste întrebări trebuie să înțelegem vulnerabilitățile noastre și ale organizațiilor noastre.

5.1 Identitatea online

Identitatea online se referă la persoana digitală pe care o creează un individ atunci când folosește internetul și poate fi folosită pentru a autentifica și autoriza accesul la diverse servicii digitale.

Componentele cheie ale identității online:

1. Informații personale: nume, adrese, numere de telefon, date de naștere etc.
2. Acreditări digitale: nume de utilizator, parole, întrebări de securitate, date biometrice (cum ar fi amprente digitale sau recunoașterea facială).
3. Prezența în rețelele sociale: profiluri, postări, aprecieri și conținut partajat pe platforme precum Facebook, Twitter, Instagram etc.
4. Informații financiare: detalii card de credit, date de conectare bancare, istoricul plăților.

Principalele riscuri la care poate fi supusă o persoană sunt:

1. Furtul de identitate: atunci când infractorii cibernetici fură informații personale pentru a uzurpa identitatea online a unei persoane ei pot deschide noi conturi de credit, pot scurge conturi bancare sau pot comite diverse fraude.
2. Atacuri de preluare a conturilor (ATO): Hackerii folosesc acreditările de conectare furate (obținute adesea din breșe de securitate ale datelor) pentru a accesa diferite conturi online. Atacatorii adună, de obicei, o listă de nume de utilizator valide sau adrese de e-mail asociate conturilor de utilizator. Apoi, încearcă o selecție de parole utilizate frecvent sau slabe (de exemplu, „parola123” sau „qwerty”) pentru toate conturile colectate.
3. Phishing: infractorii cibernetici păcălesc indivizii să dezvăluie informații personale prin comunicări frauduloase, uzurpând adesea identitatea unor entități legitime.

5.2 Încălcări ale securității datelor în mediul organizațional

Încălcări ale securității datelor apar atunci când persoane neautorizate obțin acces la date confidențiale sau sensibile, care pot include identități personale, informații financiare, secrete de afaceri sau proprietăți intelectuale. Breșele de date pot rezulta din piratare, vulnerabilități ale sistemului organizațional, amenințări interne sau chiar expunerea accidentală a datelor.

Principalele modalități de încălcare a securității datelor sunt:

1. Hacking: infractorii cibernetici exploatează vulnerabilitățile sistemelor pentru a fura date (de exemplu, prin programe malware, ransomware sau prin exploatarea directă a sistemului).
2. Atacurile de tip phishing: Atacatorii înșală utilizatorii pentru a-și furniza datele de conectare sau date sensibile, care pot fi apoi folosite pentru acces neautorizat.
3. Amenințări interne: angajații sau contractanții care au acces la date sensibile scurg sau vând informații în mod intenționat sau neintenționat.
4. Inginerie socială: Atacatorii manipulează oamenii pentru a divulga informații confidențiale, cum ar fi acreditările de conectare, fără a utiliza tehnici tehnice de hacking.
5. Furt fizic: dispozitivele precum laptopurile, hard disk-urile sau smartphone-urile care conțin date sensibile pot fi furate și exploatate.

Consecințele încălcării securității datelor pot fi grave sau mai puțin grave, dar întotdeauna se plătește un cost!

Costurile pot fi de natură financiară atunci când persoanele fizice, companiile se confruntă cu pierderi monetare directe din cauza fraudei, amenzilor de reglementare pentru că nu protejează în mod adecvat datele sensibile, plăților de răscumpărare sau a scăderii valorilor generate de pierderea încrederii în companie. Dar putem să vorbim și de costuri morale, daune reputaționale pentru că majoritatea companiilor care suferă breșe ale datelor se confruntă adesea cu o pierdere a încrederii care erodează relațiile cu clienții.

5.3 Exemple de încălcări ale securității datelor

Equifax (https://en.wikipedia.org/wiki/2017_Equifax_data_breach)

Ce s-a întâmplat: prin breșa de securitate Equifax a compromis informațiile personale ale aproximativ 147 de milioane de persoane, inclusiv numerele de securitate socială, datele de naștere și detaliile cardului de credit.

Impact: furt de identitate pe scară largă, procese colective și sancțiuni de reglementare în urma cărora Equifax a plătit peste 700 de milioane de dolari în acorduri și amenzi.

Facebook (<https://teampassword.com/blog/facebook-hacks-a-history-of-security-breaches-at-facebook>)

Ce s-a întâmplat: În 2019 o vulnerabilitate a platformei Facebook a expus datele personale a peste 530 de milioane de utilizatori, inclusiv numere de telefon, adrese de e-mail și alte informații sensibile. Scurgeri de date au apărut și în 2021.

Impact: această încălcare a evidențiat preocupările permanente legate de confidențialitate asociate cu platformele de social media și capacitatea acestora de a proteja datele utilizatorilor. De asemenea, a condus la o analiză suplimentară a practicilor de date ale Facebook.

Yahoo (2013 și 2014 - https://en.wikipedia.org/wiki/Yahoo!_data_breaches)

Ce s-a întâmplat: Yahoo a suferit două breșe majore care au expus în mod colectiv datele a peste 3 miliarde de conturi, inclusiv nume de utilizator, parole și întrebări de securitate.

Impact: aceasta rămâne una dintre cele mai mari breșe ale securității datelor din istorie. Încălcarea a erodat încrederea în practicile de securitate ale Yahoo și a contribuit la o devalorizare semnificativă a companiei.

Target (2013 <https://www.cardconnect.com/launchpointe/payment-trends/target-data-breach/>)

Ce s-a întâmplat: Hackerii au obținut acces la sistemele Target prin intermediul unui furnizor terț, compromițând informațiile despre cardul de credit și debit a aproximativ 40 de milioane de clienți în timpul sezonului de cumpărături de sărbători.

Impact: Target s-a confruntat cu acțiuni legale, amenzi de reglementare și a trebuit să cheltuiască milioane pentru îmbunătățiri de securitate și compensarea clienților.

Marriott International (2018, 2020 , 2022 <https://www.threater.com/blog/lessons-learned-from-the-marriott-hack-of-2022/>)

Ce s-a întâmplat: Breșa de securitate a afectat sistemul de rezervare al diviziei Starwood a Marriott, expunând datele personale a până la 500 de milioane de clienți, inclusiv numerele de pașapoarte și informații despre cardul de credit.

Impact: Marriott a fost amendat cu 123 de milioane de dolari de către Biroul Comisarului pentru Informații (ICO) din Regatul Unit în conformitate cu GDPR, iar încălcarea a ridicat îngrijorări semnificative cu privire la securitatea datelor clienților în industria ospitalității.

Capital One (2019 <https://www.capitalone.com/digital/facts2019/>)

Ce s-a întâmplat: Un hacker a obținut acces la datele personale a peste 100 de milioane de clienți Capital One, inclusiv scoruri de credit, numere de securitate socială și numere de cont bancar, din cauza unui firewall greșit configurat în infrastructura cloud.

Impact: provocări legale și amenzi de reglementare, ridicând îngrijorări cu privire la securitatea sistemelor bazate pe cloud utilizate de instituțiile financiare.

LinkedIn (2021 <https://www.linkedin.com/pulse/linkedin-data-breach-700m-2021-david-sehyeon-baek--ex85c/>)

Ce s-a întâmplat: Datele de la 700 de milioane de utilizatori LinkedIn (aproximativ 93% din baza de utilizatori a platformei) au fost răzuite și vândute pe dark web. Datele includ informații personale, cum ar fi nume complete, numere de telefon și detalii profesionale.

Impact: Deși nu s-au scurs informații financiare sau parole sensibile, încălcarea a provocat îngrijorare larg răspândită cu privire la confidențialitate și potențiala utilizare greșită a identităților profesionale.

Exemplele demonstrează că, din perspectiva consecințelor, aceste incidente pot avea consecințe devastatoare personale, financiare și reputaționale. Pe măsură ce dependența noastră de serviciile digitale crește, la fel crește și nevoia de practici solide de securitate cibernetică, atât la nivel individual, cât și la nivel organizațional.

5.4 Atacatorii cibernetici

Atacatorii cibernetici sunt persoane sau grupuri care folosesc tehnologia pentru a desfășura activități rău intenționate, cum ar fi furtul de date sensibile, întreruperea serviciilor digitale sau cauzarea de prejudicii organizațiilor, guvernelor sau persoanelor. Acești atacatori variază foarte mult în ceea ce privește motivațiile, metodele și nivelurile de abordare a atacului cibernetic.

Motivațiile atacatorilor cibernetici pot fi variate dar cele mai multe se încadrează în următoarele direcții:

- Câștig financiar: Mulți criminali cibernetici sunt motivați de profit.
- Ideologie: Hacktiviștii și teroriștii cibernetici sunt adesea conduși de dorința de a promova o anumită cauză politică, socială sau religioasă. Scopul lor este să perturbe, să defăimeze sau să crească gradul de conștientizare cu privire la problemele alese.
- Spionaj și colectare de informații: atacatorii sponsorizați de stat caută adesea să fure informații clasificate, tehnologie proprietară sau informații economice de la alte națiuni, afaceri sau organizații.
- Răzbunare sau răfuieli personale: hackerii pot fi motivați de dorința de răzbunare împotriva unei organizații sau a unui individ, adesea din cauza unor greșeli percepute, cum ar fi încetarea locului de muncă sau dispute personale.
- Notorietate și statut: Mulți atacatori, în special copii, sunt motivați de dorința de faimă, recunoaștere sau validare din partea colegilor lor din comunitatea hackerilor.
- Sabotaj: atacatorii pot încerca să perturbe operațiunile, să distrugă date sau să deterioreze reputația unei organizații, fie din motive politice, economice sau competitive.

Tipuri de atacatori cibernetici

Hacktiviști

Descriere: Hacktiviștii sunt hackeri motivați politic sau social care își folosesc abilitățile pentru a promova sau promova o cauză. Obiectivele lor pot include proteste împotriva guvernelor, corporațiilor sau organizațiilor pe care le consideră nedrepte.

Tactici obișnuite: modificarea site-urilor web, atacuri de tip DDoS (Distributed Denial of Service) prin care se trimite un aflus mare de trafic către o rețea sau server pentru a copleși sistemul și pentru a-i perturba capacitatea de a opera, scurgeri de date și hack-uri pe rețelele sociale.

Exemplu: Anonymous¹², un cunoscut colectiv de hacktiviști, a desfășurat diverse atacuri cibernetice împotriva site-urilor web guvernamentale, corporațiilor și chiar grupurilor extremiste pentru a susține libertatea de exprimare și a protesta împotriva injustițiilor percepute.

Infractorii cibernetici

¹² [https://en.wikipedia.org/wiki/Anonymous_\(hacker_group\)](https://en.wikipedia.org/wiki/Anonymous_(hacker_group))

Descriere: Infractorii cibernetici sunt atacatori motivați financiar care caută să profite de pe urma activităților ilegale. Aceștia se angajează adesea în activități precum fraudă, furtul de identitate, atacurile ransomware și vânzarea de date furate pe dark web.

Tactici comune: phishing, malware, ransomware, fraudă online și furt de carduri de credit.

Exemplu: grupul de ransomware REvil¹³ cu baza în Rusia a vizat mai multe organizații, criptându-le datele și solicitând plăți mari de răscumpărare în schimbul cheilor de decriptare.

Atacatori sponsorizați de stat

Descriere: Acești atacatori lucrează în numele guvernelor și se angajează în spionaj cibernetic, sabotaj și alte forme de război cibernetic. Obiectivele lor sunt adesea politice, militare sau economice și tind să vizeze infrastructura critică, agențiile guvernamentale sau industriile de importanță națională.

Tactici comune: Amenințări persistente avansate (APT), spionaj, campanii de dezinformare și atacuri asupra infrastructurii critice.

Exemplu: grupul rus APT29¹⁴ (cunoscut și ca „Cozy Bear”) a fost legat de mai multe campanii de spionaj cibernetic, inclusiv încercări de a influența alegerile și de a fura date sensibile ale guvernului.

Atacatori din interiorul organizației

Descriere: amenințările interne provin de la persoane din cadrul unei organizații, cum ar fi angajații, contractanții sau partenerii de afaceri, care dăunează în mod intenționat sau neintenționat securității cibernetice a organizației. Amenințările interne pot fi deosebit de dificil de detectat, deoarece acești indivizi au adesea acces legitim la informații sensibile.

Tactici comune: furt de date, sabotaj și spionaj.

¹³ <https://en.wikipedia.org/wiki/REvil>

¹⁴ https://en.wikipedia.org/wiki/Cozy_Bear

Exemplu: Edward Snowden¹⁵, un fost contractant NSA, a scurs informații clasificate despre programele globale de supraveghere, ceea ce a stârnit dezbateri internaționale despre confidențialitate și excesul guvernului.

Script Kiddies

Descriere: Script kiddies sunt hackeri amatori sau fără experiență care folosesc scripturi, instrumente sau programe prefabricate dezvoltate de atacatori mai pricepuți pentru a efectua atacuri de bază. Ei sunt adesea motivați de dorința de notorietate sau de divertisment, mai degrabă decât de câștiguri financiare sau politice semnificative.

Tactici obișnuite: modificarea site-urilor, atacuri DDoS și tehnici de bază de hacking.

Exemplu: Atacul cibernetic TalkTalk¹⁶ din 2015 este doar un exemplu de script kiddies care efectuează atacuri la scară largă. Acest atac a provenit de la un băiat de 17 ani care folosea software de hacking pentru a scana site-urile pentru vulnerabilități de securitate. Motivația lui a fost capacitatea de a-și demonstra cunoștințele IT prietenilor săi, iar când a fost depistată o vulnerabilitate pe site-ul TalkTalk, el a postat detaliile online. Alții au început apoi să profite de acest defect de securitate, accesând informații confidențiale ale clienților TalkTalk. Peste 15.000 de persoane le-au fost furate detaliile, inclusiv adrese de e-mail, numere de telefon și detalii bancare complete.

Teroriști ciberneticici

Descriere: teroriștii ciberneticici folosesc atacurile ciberneticice pentru a provoca frică, a perturba serviciile esențiale sau pentru a-și promova obiectivele ideologice, adesea aliniate cu terorismul. Ele urmăresc să creeze panică, să destabilizeze guvernele sau să provoace daune semnificative societăților.

Tactici comune: atacuri asupra infrastructurii critice (cum ar fi rețelele electrice sau instituțiile financiare), spionaj cibernetic și inginerie socială.

¹⁵ https://en.wikipedia.org/wiki/Edward_Snowden

¹⁶ <https://ciber.uk/areas-of-ciber-security/ciber-security-threat-groups-2/script-kiddies-case-study/> https://en.wikipedia.org/wiki/2015_TalkTalk_data_breach

Exemplu: Sandworm: O unitate militară rusă legată de atacuri cibernetice asupra infrastructurii critice, inclusiv rețeaua electrică a Ucrainei (2015) și atacul malware NotPetya (2017).

Centrul pentru studii strategice internaționale înregistrează incidente cibernetice semnificative din începând cu anul 2006. Această cronologie vizează atacurilor cibernetice asupra agențiilor guvernamentale, a companiilor de apărare și de înaltă tehnologie sau a crimelor economice cu pierderi de peste un milion de dolari. Ea poate fi accesată la următorul link <https://www.csis.org/programs/strategic-technologies-program/significant-ciber-incidents> .

Black hat și white hat hacker

Descriere: hackeri black hat sunt persoane care se angajează în activități ilegale pentru câștig personal sau pentru a exploata pe alții. De obicei, aceștia nu sunt afiliați cu organizații criminale mai mari sau cu grupuri sponsorizate de stat, dar se pot angaja în activități similare, cum ar fi furtul de informații despre cardul de credit sau piratarea sistemelor pentru câștiguri financiare.

Hackerii white hat, numiți uneori și “hackeri etici” sau “hackeri buni” exploatează sistemele sau rețelele informatice pentru a-și identifica defectele de securitate, astfel încât să poată face recomandări de îmbunătățire

Tactici comune: exploatarea vulnerabilităților, furtul de date, ransomware și escrocherii online.

Exemple: Unul dintre cei mai faimoși hackeri de pălărie neagră este Kevin Mitnick, care, la un moment dat, a fost cel mai căutat criminal cibernetic din lume. În calitate de hacker de pălărie neagră, a spart peste 40 de corporații importante, inclusiv IBM și Motorola, și chiar sistemul de avertizare al Apărării Naționale din SUA.

Mai multe exemple și descrieri ale acestor tipuri de hackeri se găsesc la acest link: <https://www.kaspersky.com/resource-center/definitions/hacker-hat-types>

Mercenarii cibernetici

Descriere: Aceștia sunt hackeri angajați sau grupuri de hackeri care își oferă serviciile celui mai mare ofertant. Ar putea lucra pentru corporații, state naționale sau organizații criminale. Activitățile lor pot include spionaj corporativ, furt de date sau sabotaj cibernetic.

Tactici obișnuite: dezvoltare personalizată de malware, atacuri direcționate și recrutare din interior.

Exemplu: Grupul “NSO Group”¹⁷, o companie israeliană, a fost acuzat că și-a vândut puternicul program spion Pegasus guvernelor care l-au folosit pentru a viza activiști, jurnaliști și oponenți politici.

5.5 Nivelurile de abordare a atacului cibernetic

Complexitatea atacurilor cibernetice din ultima perioadă demonstrează faptul că victima poate fi un individ, o organizație sau un grup de organizații și chiar o națiune. Confruntările militare recente au arătat că războiul cibernetic nu mai este de domeniul science fiction.

Războiul cibernetic este o formă modernă de război care extinde conflictele tradiționale în spațiul cibernetic, unde bătăliile sunt purtate mai degrabă cu coduri rău intenționate decât cu arme fizice. Spre deosebire de războiul tradițional, războiul cibernetic nu implică violență fizică, dar poate provoca perturbări semnificative, pierderi financiare și chiar pierderi de vieți omenești (de exemplu, atacuri asupra spitalelor sau a infrastructurii critice care duc la consecințe în lumea reală). Interconectarea infrastructurii digitale globale înseamnă că atacurile de război cibernetic pot avea consecințe de amploare, afectând mai multe țări și organizații dincolo de țintele vizate.

Războiul cibernetic poate îmbraca mai multe forme și putem enumera:

Spionajul cibernetic

Obiectiv: colectarea informațiilor de la adversari, cum ar fi furtul de informații militare sau politice, proprietate intelectuală sau date economice.

Tactici: utilizarea de programe malware, atacuri de phishing și exploit-uri pentru a se infiltra în sisteme și a extrage informații sensibile.

¹⁷ https://en.wikipedia.org/wiki/NSO_Group

Exemplu: grupul chinez de spionaj cibernetic APT10¹⁸, cunoscut pentru piratarea în rețelele mai multor corporații occidentale pentru a fura proprietatea intelectuală și secretele comerciale

Sabotaj

Obiectiv: întreruperea sau distrugerea sistemelor sau infrastructurii cheie pentru a slăbi capacitățile unui adversar.

Tactici: implementarea de programe malware, atacuri DDoS sau manipularea sistemelor de control din medii industriale.

Exemplu: atacul Stuxnet (2010)¹⁹, atribuit pe scară largă SUA și Israelului, a vizat centralele nucleare ale Iranului, provocând daune fizice semnificative programului nuclear al țării.

Atacurile cibernetice asupra infrastructurii critice

Obiectiv: paralizarea sau întreruperea serviciile esențiale, cum ar fi rețelele electrice, sistemele de transport sau unitățile de asistență medicală, adesea în perioadele de conflict politic sau militar.

Tactici: exploatarea vulnerabilităților în sistemele de control industrial (ICS) sau sistemele SCADA (Supervisory Control and Data Acquisition), care gestionează infrastructura.

Exemplu: atacul asupra rețelei electrice a Ucrainei²⁰ (2015, 2016), atribuit actorilor cibernetici ruși, care a provocat pene de curent pe scară largă în anumite părți ale țării. Malware-ul folosit, cunoscut sub numele de „BlackEnergy”, a dezactivat alimentarea mai multor stații. Un al doilea atac din 2016 a folosit malware-ul mai sofisticat „Industroyer”.

Un ultim exemplu este atacul recent asupra spitalelor din Romania prezentat pe pagina Direcției Naționale de Securitate Cibernetică <https://dnsc.ro/citeste/atac-cibernetice-ransomware-spitale-Romania>.

¹⁸ <https://www.ncsc.gov.uk/news/apt10-continuing-target-uk-organisations>

¹⁹ Detalii despre Stuxnet se pot găsi la următoarele adrese

1. <https://www.scientia.ro/tehnologie/8675-virusul-stuxnet-atacul-asupra-programului-nuclear-iranian.html>
2. <https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet>

²⁰ https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack

Campanii de dezinformare

Obiectiv: influențarea opiniei publice, răspândirea haosul și destabilizarea guvernelor sau alegerilor prin diseminarea de informații false.

Tactici: folosirea platformelor de social media și a altor instrumente online pentru a răspândi propagandă, narațiuni false și conținut divizionar.

Exemplu: ingerința Rusiei în alegerile prezidențiale din SUA²¹ din 2016, în care actorii sponsorizați de stat ar fi folosit rețelele sociale pentru a influența opinia publică și a semăna discordie. Ingerința a ridicat îngrijorări globale cu privire la integritatea alegerilor în era digitală și a dus la sancțiuni și tensiuni diplomatice între SUA și Rusia.

Atacurile ciber-fizice

Obiectiv: atacuri cibernetice care au ca rezultat direct consecințe fizice, cum ar fi deteriorarea hardware-ului, întreruperea operațiunilor din fabrici sau cauzarea de accidente în infrastructura critică.

Tactici: exploatarea vulnerabilităților în sistemele care controlează procesele fizice, cum ar fi cele găsite în fabricile de producție sau instalațiile energetice.

Exemplu: atacul malware Triton²² (2017), care a vizat sistemele de siguranță ale unei fabrici petrochimice din Arabia Saudită, amenințând, potențial, vieți prin dezactivarea măsurilor critice de siguranță.

Operațiuni cibernetice militare

Obiectiv: întreruperea operațiunilor militare inamice, dezactivarea sistemelor de comandă și control sau interferarea comunicațiilor în timpul conflictului.

Tactici: blocarea comunicațiilor, dezactivarea sistemelor radar sau atacarea rețelelor logistice.

²¹ https://en.wikipedia.org/wiki/Russian_interference_in_the_2016_United_States_elections

²² <https://www.technologyreview.com/2019/03/05/103328/cibersecurity-critical-infrastructure-triton-malware/>

Exemplu: în timpul conflictului dintre Rusia și Georgia din 2008²³, atacurile cibernetice rusești au vizat site-urile web ale guvernului georgian, instituțiile media și rețelele de comunicare, afectând capacitatea Georgiei de a răspunde.

Una dintre cele mai mari provocări în războiul cibernetic este atribuirea cu acuratețe a atacurilor unor actori specifici. Operațiunile cibernetice sunt adesea desfășurate pe ascuns, iar atacatorii pot folosi tehnici pentru a-și ascunde identitatea sau a încadra alți actori. În plus, costul relativ scăzut al instrumentelor cibernetice în comparație cu hardware-ul militar tradițional îl face accesibil pentru o gamă mai largă de actori.

O altă provocare este legată de aspecte juridice și etice pentru că legile internaționale care guvernează războiul (cum ar fi Convențiile de la Geneva) nu se aplică în mod clar operațiunilor cibernetice. Acest lucru creează ambiguitate juridică cu privire la ceea ce constituie un atac cibernetic sau un răspuns legal.

²³ https://en.wikipedia.org/wiki/Ciberattacks_during_the_Russo-Georgian_War

Capitolul 6

Protejarea informațiilor și confidențialitatea datelor personale

“O minte educată va avea mereu mai multe întrebări decât răspunsuri.”

Helen Keller

Există 5,35 miliarde de oameni care folosesc internetul în 2024, ceea ce reprezintă 66,2% din populația totală a lumii. Utilizatorii de internet au crescut cu 1,8% în ultimul an, 97 de milioane de utilizatori noi fiind online pentru prima dată în 2023²⁴!

Internetul este accesibil de oriunde și oricând. Suntem într-o lume superconectată! Rețelele sociale și stocarea online au devenit o parte integrantă a vieții multor oameni. Fișierele, fotografiile și videoclipurile sunt partajate între prieteni și familie. Colaborarea și întâlnirile online se desfășoară la locul de muncă cu oameni care sunt la mulți kilometri unul de celălalt. Stocarea datelor nu se mai limitează doar la dispozitivele pe care le accesăm local. Așa că sunt câteva întrebări la care ar fi bine să răspundem înainte de a înțelege cum să ne protejăm:

1. *Ce drept de proprietate și control aveți asupra datele dumneavoastră personale în mediul online*
2. *Cine ar putea dori datele dumneavoastră personale?*
3. *Care este domeniul de aplicare al unui astfel de interes?*

6.1 Date cu caracter personal

Date personale

Definiție: Datele personale includ informații care pot identifica direct sau indirect o persoană, cum ar fi nume, adrese, numere de telefon, numere de securitate socială și adrese de e-mail.

²⁴ <https://presagalati.ro/cati-oameni-utilizeaza-internetul-in-2024/#:~:text=La%20C3%AEnceputul%20lui%202024%2C%20C3%AEn,este%20accesarea%20re%20C8%9Belelor%20de%20socializare>

Proprietate: din punct de vedere legal, sunteți considerat „subiectul datelor” al datelor dumneavoastră personale. Deși este posibil să aveți drepturi asupra modului în care sunt utilizate aceste date, entitățile care le colectează (cum ar fi companiile, aplicațiile sau site-urile web) își afirmă adesea un anumit control sau proprietate asupra datelor.

Date generate de utilizator

Definiție: aceasta include conținutul pe care îl creați și partajați online, cum ar fi postări pe rețelele sociale, fotografiile, videoclipuri, bloguri și comentarii.

Proprietate: deși din punct de vedere tehnic „dețineți” conținutul pe care îl creați, platforme precum Facebook, Instagram sau YouTube solicită adesea să le acordați licențe de utilizare, distribuire sau modificare a conținutului dumneavoastră odată ce acesta este încărcat.

Date comportamentale

Definiție: datele comportamentale urmăresc modul în care interacționați cu site-urile web, aplicațiile și dispozitivele, inclusiv istoricul de navigare, modelele de achiziție și preferințele.

Proprietate: companiile care colectează date comportamentale le consideră adesea proprietatea lor. Ei folosesc aceste date pentru publicitate direcționată, recomandări de produse sau analize, adesea cu o contribuție sau un control minim din partea utilizatorului.

Metadate

Definiție: metadatele se referă la date despre alte date, cum ar fi ora și locația unei fotografii sau tipul și dimensiunea fișierului unui document. Metadatele sunt adesea generate automat.

Proprietate: în timp ce metadatele sunt generate din activitățile dumneavoastră, acestea sunt de obicei controlate de platformele sau dispozitivele care le colectează.

Date de sănătate

Definiție: datele de sănătate includ informații precum fișe medicale, date de urmărire a fitnessului, informații genetice și date biometrice.

Proprietate: datele de sănătate sunt de obicei considerate sensibile și sunt adesea protejate de legi precum HIPAA ²⁵(în S.U.A.). Cu toate acestea, odată ce partajați aceste date cu aplicații

²⁵ <https://www.hhs.gov/regulations/index.html>

de sănătate, companii de asigurări sau servicii online, controlul poate fi transferat acestor entități.

6.2 Cadrele juridice care guvernează proprietatea datelor

Legile privind confidențialitatea datelor

Regulamentul general privind protecția datelor GDPR²⁶ (UE): oferă persoanelor fizice drepturi extinse asupra datelor lor personale, inclusiv dreptul de a accesa, corecta și șterge datele lor. Acesta prevede ca companiile să obțină consimțământul explicit pentru a colecta și utiliza datele cu caracter personal.

California Consumer Privacy Act CCPA (S.U.A.): oferă rezidenților din California drepturi similare cu GDPR, cum ar fi posibilitatea de a renunța la colectarea datelor și dreptul de a solicita ștergerea datelor cu caracter personal.

Legea proprietății intelectuale

Drepturi de autor: pentru conținutul pe care îl creați, cum ar fi artă, scris sau videoclipuri, legile privind drepturile de autor vă oferă dreptul de proprietate asupra materialului respectiv. Cu toate acestea, platformele pe care încărcați acest conținut vă cer adesea să le acordați licențe, ceea ce vă poate afecta controlul asupra modului în care conținutul este utilizat sau partajat.

Acorduri privind termenii și condițiile

Acorduri de platformă: atunci când utilizați platforme sau servicii online, sunteți de obicei de acord cu termenii și condițiile acestora, care includ adesea clauze despre proprietatea datelor. Aceste acorduri pot transfera un anumit control sau proprietate asupra datelor dumneavoastră către platformă în schimbul utilizării serviciului lor.

Proprietate versus Control

Deși puteți „deține” datele dumneavoastră, în practică, companiile care colectează, stochează și prelucrează datele dumneavoastră exercită adesea un control semnificativ asupra acestora.

²⁶ <https://eur-lex.europa.eu/RO/legal-content/summary/general-data-protection-regulation-gdpr.html>

Capacitatea dumneavoastră de a accesa, șterge sau restricționa modul în care sunt utilizate datele dumneavoastră este de obicei guvernată de legile de confidențialitate și de termenii și condițiile pe care le-ați acceptat.

Să analizăm câteva scenarii privind proprietatea datelor.

1. Rețele sociale

Proprietate: puteți deține fotografiile, videoclipurile și postările pe care le creați. Cu toate acestea, platformele precum Facebook sau Instagram solicită adesea să le acordați o licență neexclusivă, fără drepturi de autor pentru a vă folosi, partaja și distribui conținutul.

Control: păstrați un anumit control asupra cine vă poate vedea sau distribui postările, dar platforma vă folosește în continuare datele pentru publicitate direcționată, recomandări de conținut și optimizare a algoritmului.

2. Aplicații de sănătate și fitness

Proprietate: dețineți datele dumneavoastră de sănătate, dar atunci când le partajați cu aplicații sau platforme online, sunteți de obicei de acord să le permiteți să vă folosească datele pentru cercetare, publicitate sau dezvoltarea de produse.

Control: Unele aplicații vă permit să vă ștergeți datele sau să limitați modul în care sunt utilizate, dar altele pot păstra datele chiar și după ștergere sau le pot partaja cu terțe părți.

3. Stocare în cloud

Proprietate: păstrați dreptul de proprietate asupra fișierelor, fotografiilor și documentelor pe care le stocați în cloud. Cu toate acestea, furnizorii de cloud au de obicei termeni care le permit să gestioneze și să vă întrețină datele.

Control: aveți posibilitatea de a vă șterge sau modifica datele, dar furnizorii de stocare în cloud pot avea în continuare acces la anumite metadate sau copii de siguranță ale datelor dumneavoastră

4. Platforme de comerț electronic

Proprietatea: deși dețineți istoricul achizițiilor și detaliile personale, platforma de comerț electronic consideră adesea că datele comportamentale (cum ar fi obiceiurile de navigare) pe care le colectează în timpul vizitelor dumneavoastră sunt proprietatea lor.

Control: de obicei, controlul este limitat la setările contului, cum ar fi renunțarea la anunțurile personalizate sau solicitarea ștergerii contului.

6.3 Provocări în definirea proprietății datelor și controlul acestora

Atunci când mai multe entități sunt implicate în colectarea, stocarea și procesarea datelor (cum ar fi furnizorii terți, agenții de publicitate și brokerii de date), proprietatea devine fragmentată. Fiecare entitate poate revendica proprietatea asupra diferitelor aspecte ale datelor.

Chiar dacă din punct de vedere tehnic „dețineți” datele dumneavoastră, o vulnerabilitate a sistemului vă poate expune informațiile personale fără consimțământul dumneavoastră, compromițându-vă confidențialitatea și securitatea.

„Dreptul de a fi uitat” - legi precum GDPR și CCPA permit persoanelor să solicite ștergerea datelor lor. Cu toate acestea, aplicarea poate fi dificilă, mai ales atunci când datele au fost partajate pe mai multe platforme sau stocate în copii de rezervă.

Proprietatea datelor dumneavoastră este o problemă cu mai multe fațete, influențată de considerente juridice, tehnice și contractuale. Deși este posibil să dețineți datele dumneavoastră personale și generate de utilizatori, controlul revine adesea companiilor și platformelor care le colectează și le prelucrează. Înțelegerea drepturilor, a fi selectiv cu privire la datele pe care le partajați și a folosi instrumentele de confidențialitate sunt esențiale pentru a recâștiga controlul asupra datelor dumneavoastră în era digitală.

Datele personale online²⁷ sunt valoroase și diverse entități pot fi interesate de ele din diferite motive. Iată o prezentare generală a celor care ar putea dori datele dumneavoastră și domeniul de interes al acestora:

1. Agenții de publicitate și companii de marketing

Interes: agenții de publicitate și firmele de marketing vă folosesc datele pentru a vă viza cu anunțuri personalizate bazate pe preferințele dumneavoastră, istoricul de navigare și detaliile demografice.

²⁷ https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data

Domeniul de aplicare: aceasta poate include urmărirea activităților dumneavoastră online (cum ar fi clicurile, căutățile și achizițiile) pentru a crea un profil al intereselor dumneavoastră

2. Platforme de social media

Interes: companiile de rețele sociale colectează date pentru a vă personaliza feedul, pentru a recomanda conținut și pentru a îmbunătăți implicarea utilizatorilor. De asemenea, aceștia pot vinde date anonime către terți.

Domeniul de aplicare: postările, aprecierile, distribuirile și chiar mesajele private ar putea fi analizate pentru a îmbunătăți algoritmi și publicitatea direcționată.

3. Brokeri de date

Interes: brokerii de date colectează și vând informații personale companiilor pentru marketing, verificarea antecedentelor și alte scopuri.

Domeniul de aplicare: Ei colectează totul, de la activitatea dumneavoastră pe rețelele sociale până la comportamentul dumneavoastră de cumpărare și îl vând terților.

4. Hackeri și criminali cibernetici

Interes: infractorii cibernetici caută date personale pentru furt de identitate, fraudă și alte activități ilegale.

Domeniul de aplicare: informațiile sensibile, cum ar fi datele de conectare, numerele de card de credit și numerele de securitate socială sunt ținte principale.

5. Agenții guvernamentale

Interes: guvernele pot colecta date în scopuri de securitate națională, de aplicare a legii sau de reglementare.

Domeniul de aplicare: aceasta ar putea include monitorizarea activităților online, a comunicațiilor și a tranzacțiilor pentru a detecta potențialele amenințări sau încălcări, crearea unui dosar de sănătate

6. Angajatorii

Interes: Unii angajatori monitorizează comportamentul online al angajaților, în special pe dispozitivele companiei, pentru a asigura productivitatea și a proteja informațiile companiei.

Domeniul de aplicare: aceasta poate include istoricul dumneavoastră de navigare, comunicările prin e-mail și activitatea pe rețelele sociale.

7. Instituții financiare

Interes: băncile și instituțiile financiare colectează date pentru a detecta fraudă, pentru a evalua bonitatea și pentru a oferi produse financiare personalizate.

Domeniul de aplicare: analizează tranzacțiile dumneavoastră financiare, istoricul de credit și modelele de cheltuieli.

8. Companii de tehnologie

Interes: marile firme de tehnologie (cum ar fi Google, Amazon, Apple etc.) adună date pentru a îmbunătăți serviciile, a oferi personalizare și a dezvolta produse noi.

Domeniul de aplicare: aceasta include totul, de la istoricul căutărilor la utilizarea dispozitivului, stocarea în cloud, date despre locație și multe altele.

Ca un scurt exercițiu vă propun să răspundeți la următoarele întrebări:

1. Aveți un cont la un furnizor de servicii online? Dacă da, ați citit acordul privind Termenii și condițiile?
2. Care este politica de utilizare a datelor?
3. Care sunt setările de confidențialitate?
4. Care este politica de securitate?
5. Care sunt drepturile dumneavoastră cu privire la datele dumneavoastră? Puteți solicita o copie a datelor dumneavoastră?
6. Ce poate face furnizorul cu datele pe care le încărcați?
7. Ce se întâmplă cu datele dumneavoastră când vă închideți contul?
8. După ce ați creat un cont și ați fost de acord cu Termenii și condițiile, știți cu adevărat la ce v-ați înscris?

Pe scurt, multe entități sunt interesate de datele dumneavoastră din diverse motive, de la marketing și îmbunătățirea serviciilor până la fraudă și supraveghere. Protejarea datelor dumneavoastră personale online necesită înțelegerea riscurilor și practicarea unor obiceiuri.

Să privim împreună la 2 liste de verificare a practicilor noastre!

6.4 Să verificăm - Conectarea

1. V-ați asigurat că aveți o conexiune la Internet securizată?
2. Ați stabilit o politică de utilizare acceptabilă (numită uneori o politică de utilizare responsabilă) pentru oricine care utilizează/accesează Internetul prin intermediul rețelei și dispozitivelor dumneavoastră?
3. Aveți toate dispozitivele securizate?
4. Înțelegeți suficient de mult conceptele de localizare geografică și Bluetooth pentru a vă folosi dispozitivele confortabil și în siguranță?
5. Folosiți parole puternice și activarea autentificării cu doi factori?

Sfaturi:

- Securizați-vă rețeaua - criptați datele sensibile și asigurați-vă că comunicațiile de rețea sunt criptate (de exemplu, site-uri web HTTPS, VPN-uri pentru lucru la distanță). Setati parole puternice pentru rețeaua dumneavoastră Wi-Fi și utilizați criptarea WPA3. Evitați utilizarea rețelei Wi-Fi publice pentru activități sensibile, cu excepția cazului în care utilizați o rețea privată virtuală VPN.

Asigurați-vă că știți cum să accesați pagina de configurare a routerului dumneavoastră Cel mai adesea, dacă introduceți una dintre următoarele adrese IP în browser, o puteți accesa: 192.168.1.0 sau 192.168.1.1. De ce este acest lucru important? Majoritatea paginilor de configurare Wi-Fi au conturi de administrator „implicit” cu nume de utilizator și parole foarte simple (de exemplu, numele de utilizator „admin” și parola „admin”). Este foarte important să securizați accesul la pagina de configurare a routerului, deoarece poate fi utilizat cu ușurință pentru a vă schimba setările sau pentru a obține acces la rețeaua computerului dumneavoastră de acasă.

- Opriți întotdeauna dispozitivele (calculatoarele) sau dezactivați conexiunea Wi-Fi de pe telefonul inteligent/tableta dumneavoastră când mergeți la culcare. Lăsarea dispozitivelor conectate poate crește riscul de securitate pentru datele dumneavoastră și poate prezenta, de asemenea, riscuri pentru sănătate.

- Evitați accesarea conturilor sensibile (de exemplu, servicii bancare, e-mail) prin Wi-Fi public și dezactivați conexiunile Wi-Fi automate pentru a preveni conectarea accidentală la rețele nesigure.

- Elaborați o politică de utilizare acceptabilă sau o politică de utilizare responsabilă dacă alții vor folosi computerul sau rețeaua pentru care sunteți responsabil.

- Folosiți parole puternice, unice, utilizând un amestec de litere (atât majuscule, cât și mici), numere și simboluri. Puteți utiliza manageri de parole pentru a genera și stoca parole unice pentru diferite conturi și veți evita reutilizarea parolelor în mai multe conturi.

- Activați autentificarea cu mai mulți factori (MFA) solicitând o a doua formă de verificare (cum ar fi un cod de telefon) în plus față de parola dumneavoastră. Aplicați MFA oriunde este posibil, în special pentru e-mail, conturi bancare și conturi legate de muncă.

- Asigurați-vă că sistemele dumneavoastră de operare, software-ul și aplicațiile sunt actualizate cu cele mai recente corecții de Securitate - instalați software antivirus și anti-malware de renume pe toate dispozitivele, utilizați firewall-uri pentru a monitoriza și controla traficul de rețea de intrare și de ieșire, luați în considerare utilizarea extensiilor de browser care blochează anunțurile, instrumentele de urmărire și eventualele programe malware.

- Limitați permisiunile pentru aplicații doar la ceea ce este necesar și evitați descărcarea de aplicații din surse necunoscute

- Dezactivați serviciile de urmărirea locației pe dispozitivele și aplicațiile dumneavoastră atunci când nu este necesar și examinați în mod regulat permisiunile aplicațiilor și dezactivați accesul la locație, contacte, cameră și microfon, dacă nu este absolut necesar.

- Securizați-vă dispozitivele asigurându-vă că dispozitivele dumneavoastră (telefoane, laptopuri etc.) sunt criptate, astfel încât datele dumneavoastră să rămână în siguranță dacă sunt pierdute sau furate și configurați parole puternice, coduri PIN sau blocări biometrice pe toate dispozitivele dumneavoastră

6.5 Să verificăm – Prezența în mediul online

1. Ați inclus detalii de contact pe site-ul, blogul sau platformele sociale pe care le utilizați?
Ați luat măsuri pentru a vă proteja confidențialitatea online?
2. Vă protejați blogul sau vlog-ul de hackeri prin stabilirea măsurilor de securitate adecvate și salvându-vă conținutul în mod regulat.

3. Ați verificat dacă conținutul pe care îl utilizați în mediul online este în conformitate cu legea drepturilor de autor? Înțelegeți obiectivul și publicul blogului dumneavoastră atunci când postați conținut?
4. Cereți în mod sistematic permisiunea persoanelor care apar în fotografiile și videoclipurile pe care le postați online?
5. Sunteți precaut cu emailurile sau link-urile necunoscute?
6. Recomandările utilizatorilor pe site-urile de călătorii și servicii sau produse pot fi utile, dar sunteți sigur că sunt reale?
7. Puteți identifica un site nesigur?
8. Citiți acordul privind Termenii și condițiile pentru utilizarea unui site/serviciu/produs?

Sfaturi:

- Păstrați evidența și urmăriți regulat toate conturile dumneavoastră organizând informațiile pentru a vă face mai ușoară gestionarea acestora.

- Utilizați întotdeauna adresa dumneavoastră de e-mail, nu contul de rețea socială, atunci când vă înregistrați la servicii online importante. Oricât de convenabil ar părea să vă înregistrați la servicii folosind Facebook, Google+ sau alte conturi de rețele sociale, nu uitați că sunteți de acord ca aceste servicii să acceseze o mare parte din informațiile dumneavoastră. De asemenea, în timp ce unele rețele sociale par să continue pentru totdeauna, în cazul în care serviciile lor vor înceta într-o zi, este posibil să nu vă puteți conecta la contul dumneavoastră

- Utilizați aliasuri: atunci când vă înscrieți pentru servicii sau site-uri web, luați în considerare utilizarea unui alias, adresă de e-mail alternativă sau informații false pentru conturile neesențiale sau utilizați adrese de e-mail temporare sau de unică folosință atunci când vă înscrieți pentru servicii sau promoții unice

- Partajarea de conținut online prin intermediul unui site web, blog sau vlog este o oportunitate excelentă de a vă împărtăși opiniile, dar poate doriți să vă protejați confidențialitatea utilizând un pseudonim și reținând anumite detalii personale.

- Fiți atent la ceea ce distribuiți: evitați distribuirea excesivă a detaliilor personale (cum ar fi datele de naștere, adresele etc.) pe rețelele de socializare și profilurile online, revizuiți și ajustați setările de confidențialitate pe platformele de rețele sociale, asigurându-vă că informațiile dumneavoastră sunt partajate numai persoanelor de încredere.

- Aveți grijă de e-mailurile nesolicitate, în special de cele care solicită informații personale sau care conțin atașamente sau link-uri suspecte, confirmați legitimitatea e-mailurilor din surse necunoscute sau neașteptate, contactând direct expeditorul (fără a răspunde la e-mail). Evitați să faceți clic pe linkuri necunoscute: treceți cursorul peste linkuri pentru a vedea destinația reală și evitați să faceți clic pe linkuri din surse nesigure.

- Utilizați aplicații de mesagerie criptate precum Signal sau WhatsApp pentru conversații private.

- Navigați în siguranță și în mod privat utilizând o rețea VPN și utilizați modul de navigare incognito sau privat pentru a împiedica browserul dumneavoastră să stocheze cookie-uri, istoricul căutărilor și alte date temporare sau utilizați browsere axate pe confidențialitate precum Firefox, Brave, DuckDuckGo sau Startpage, Tor browser și instalați extensii de blocare de anunțuri (Ad block)sau extensii anti-urmărire precum uBlock Origin sau Privacy Badger. Gestionați modulele cookie și trackererele fie prin ștergerea cookie-urilor și a istoricul de navigare pentru a reduce urmărirea, fie prin instalarea unor extensii precum Ghostery sau Disconnect pentru a bloca instrumentele de urmărire și cookie-urile terță parte, fie prin limitarea permisiunilor la accesarea unor site-uri.

- Utilizați servicii cloud securizate pentru a vă asigura că datele dumneavoastră sunt protejate împotriva accesului neautorizat și faceți în mod regulat copii de siguranță ale datelor importante în locații sigure.

- Configurați copii de rezervă automate și regulate ale datelor critice și asigurați-vă că backupurile sunt stocate în siguranță (de exemplu, offline sau într-un cloud cu criptare).

- Monitorizați încălcările datelor utilizând servicii precum HaveIBeenPwned pentru a verifica dacă e-mailul dumneavoastră sau alte date au fost compromise într-o încălcare.

- Fiți proactiv: dacă datele dumneavoastră au fost expuse, schimbați-vă parolele și activați imediat MFA pentru conturile afectate.

- Citiți politicile de confidențialitate: înainte de a vă înscrie pentru servicii, examinați politicile de confidențialitate ale acestora pentru a înțelege cum sunt colectate, utilizate și partajate datele dumneavoastră Renunțați la colectarea datelor: ori de câte ori este posibil, renunțați la colectarea de date inutile și examinați opțiunile pentru limitarea publicității direcționate.

Capitolul 7

Protejarea informațiilor și confidențialitatea datelor în cazul organizațiilor

“Secretul pentru a face progrese este să începi.”

Mark Twain

Protejarea datelor și a activelor unei organizații de amenințările cibernetice este o responsabilitate critică pentru orice companie. Ea necesită implementarea unui cadru de securitate robust, care încorporează tehnologie, politici și elemente umane.

7.1 Strategii

Enumerăm strategiile cheie pe care companiile ar trebui să le adopte pentru a se proteja împotriva amenințărilor cibernetice și pentru a asigura securitatea datelor:

1. Stabilirea unei politici de securitate cibernetice

Este necesar ca fiecare organizație să dezvolte și să aplice o politică clară de securitate cibernetice care subliniază responsabilitățile, procedurile și protocoalele pentru protejarea datelor și sistemelor companiei.

Este utilă implementarea un sistem de clasificare a datelor din cadrul companiei, în funcție de sensibilitatea acestora și aplicați măsuri de protecție adecvate pentru fiecare categorie (de exemplu, confidențial, intern, public).

2. Instruirea și conștientizarea angajaților²⁸

Instruirea, în mod regulat, a angajaților, cu privire la cele mai bune practici de securitate cibernetice, cum ar fi recunoașterea încercărilor de phishing, securizarea parolelor și respectarea politicilor companiei este unul din cei mai importanți factori în consolidarea securității cibernetice a companiei. Ea poate fi completată de efectuarea unor atacuri de

²⁸ Acesta este un principiu evidențiat foarte clar în capitolul 3 al documentului DNSC <https://dnsc.ro/vezi/document/principii-strategice-de-securitate-cibernetica-pentru-managementul-organizatiei>

phishing simulate și alte exerciții care să testeze gradul de conștientizare și răspunsul angajaților la amenințări.

3. Controlul accesului și managementul identității

Limitarea accesului la date și sisteme pe baza principiului privilegiului minim, asigură accesul angajaților doar la resursele de care au nevoie pentru a-și îndeplini funcțiile de serviciu. Implementarea controlului accesului bazat pe roluri (RBAC) permite gestionarea permisiunilor și reduce riscul accesului neautorizat la datele sensibile.

Implementarea autentificarilor cu mai mulți factori (MFA) pentru accesarea sistemelor critice, aplicațiilor și datelor sensibile reduce semnificativ riscul penetrărilor în sistem.

4. Actualizarea regulată de software

Gestionarea corecțiilor presupune asigurarea tuturor sistemelor, aplicațiile și dispozitivele cu cele mai recente corecții de securitate.

Efectuarea actualizărilor automate, acolo unde este posibil, reduce riscul de a pierde remedieri critice de securitate.

5. Criptarea datelor

Criptarea datelor sensibile, atât a celor în repaus și cât și a celor în tranzit (e-mailuri, baze de date și copii de rezervă) asigură acestea rămân ilizibile, chiar dacă datele sunt interceptate

6. Securizarea rețelei

Folosirea de Firewall-uri și a sistemelor de detecție și de prevenire a intruziunilor (IDS/IPS) permite monitorizarea și blocarea traficului neautorizat de rețea.

Pentru a izola sistemele sensibile și a reduce amenințărilor se folosește tehnica de segmentare a rețelei

Pentru lucrătorii de la distanță se oferă acces securizat prin utilizarea unor VPN-uri și gateway-uri de acces securizate care asigură comunicarea criptată între dispozitivele de la distanță și rețelele companiei.

7. Protecție endpoint

Se instalează pe toate dispozitivele companiei soluții antivirus și anti-malware.

Se asigură criptarea și securitatea tuturor dispozitivelor companiei (laptopurile, telefoanele mobile și alte dispozitive utilizate de angajați sunt criptate și au instalat software de Securitate).

Folosirea sistemelor de gestionare a dispozitivelor mobile (MDM) pentru a aplica politicile de securitate pe dispozitivele angajaților, pentru a controla instalările aplicațiilor și pentru a șterge de la distanță dispozitivele pierdute sau furate.

8. Backup și recuperare în caz de atac

Efectuarea regulată a copiilor de siguranță ale datelor și sistemelor critice, asigurarea stocării lor în siguranță și testarea acestora în mod regulat pentru integritate permite refacerea rapidă a unui sistem atacat.

Dezvoltarea planului de recuperare în caz de atac va descrie și reglementa modul în care compania va restabili operațiunile și va recupera datele în cazul unui atac cibernetic sau al altor întreruperi.

9. Sisteme de monitorizare și audit

Monitorizarea în timp real a traficului de rețea, a activității sistemului și a comportamentului utilizatorilor pentru a detecta și a răspunde la potențialele amenințări, folosirea jurnalelor de acces ale utilizatorilor permit examinarea modificărilor sistemului și evenimentelor de Securitate (anomalii sau activități suspecte) și generează alerte pentru activități suspecte.

10. Managementul riscului de la terți

Efectuarea evaluări amănunțite ale riscurilor furnizorilor și furnizorilor de servicii terți, pentru a vă asigura că aderă la practici puternice de securitate cibernetică, revizuirea și actualizarea nivelului de acces pe care furnizorii terți îl au la sistemele și datele dumneavoastră, includerea cerințelor de securitate cibernetică și obligațiilor de conformitate în contractele cu furnizorii asigură responsabilitatea pentru protejarea datelor dumneavoastră

11. Răspunsul și raportarea incidentelor

Fiecare organizație trebuie să aibă un Plan de răspuns la incident care acoperă strategiile de izolare, eradicare, recuperare și comunicare subliniind pașii pe care compania îi va lua în cazul unui atac cibernetic.

Definirea protocoalelor pentru raportarea incidentelor de Securitate trebuie să vizeze atât planul intern al organizației, cât și părțile interesate externe, cum ar fi clienții, partenerii și organismele de reglementare.

12. Conformitate și obligații legale

Conformitatea cu reglementările legale asigură că sunt respectate legile și reglementările relevante privind securitatea cibernetică, cum ar fi GDPR, HIPAA, CCPA²⁹ sau standarde specifice industriei, cum ar fi PCI-DSS³⁰ prin implementarea politicilor, legilor privind protecția datelor, inclusiv procedurile adecvate de manipulare, stocare și ștergere a datelor.

Obținerea unei asigurări cibernetice pentru a atenua impactul financiar al încălcării datelor și al atacurilor cibernetice (o poliță care acoperă domenii precum recuperarea datelor, costurile legale și eforturile de relații publice) nu este o obligație legală dar este de drept.

13. Testare de penetrare și evaluări ale vulnerabilităților

Efectuarea unor teste regulate de penetrare pentru a identifica și remedia vulnerabilitățile din sistemele dumneavoastră înainte ca acestea să poată fi exploatate de atacatori, scanarea vulnerabilităților prin utilizarea instrumentelor automate pentru depistarea vulnerabilităților și configurațiilor greșite din sistemele, aplicațiile și infrastructura de rețea este una din cele mai bune căi de prevenire a unui atac cibernetic.

Dacă până în acest punct am enumerate doar politici și tehnologii să vedem cum poate influența factorul uman consolidarea securității cibernetice în cazul unei instituții de învățământ.

Iată câteva sfaturi pentru școli, profesori și copii despre cum să îmbunătățiți confidențialitatea și securitatea datelor.

²⁹ California Consumer Privacy Act <https://oag.ca.gov/privacy/ccpa>

³⁰ Payment Card Industry Data Security Standard

7.2 Sfaturi pentru școli (administratori și departamente IT)

- Dezvoltați o politică de confidențialitate a datelor: stabiliți linii directoare clare cu privire la practicile de colectare, stocare și partajare a datelor. Acest lucru ar trebui să respecte legile locale precum GDPR.
- Utilizați tehnologia sigură: investiți în instrumente de comunicare criptate, rețele securizate (VPN-uri, firewall-uri) și software actualizat în mod regulat pentru a proteja datele sensibile.
- Limitați accesul la date: implementați controlul accesului bazat pe roluri, asigurându-vă că numai personalul autorizat poate accesa informațiile sensibile (cum ar fi datele elevilor).
- Oferiți instruire în materie de securitate cibernetică și confidențialitate a datelor pentru personal și elevi. Aceasta include recunoașterea încercărilor de phishing, utilizarea parolelor puternice și protejarea dispozitivelor personale.
- Criptarea datelor: Asigurați-vă că toate datele sensibile (note, informații personale etc.) sunt criptate atât în stocare, cât și în timpul transmisiei prin internet.
- Backup de date: faceți în mod regulat copii de siguranță ale datelor importante în locații sigure pentru a evita pierderile din cauza atacurilor cibernetice sau a problemelor tehnice.
- Monitorizarea sistemelor: Monitorizați continuu activitatea rețelei pentru comportament neobișnuit și auditați în mod regulat sistemele de date pentru a vă asigura că sunt actualizate și sigure.
- Consimțământul părinților: obțineți consimțământul explicit de la părinți pentru colectarea și utilizarea datelor elevilor, în special atunci când utilizați aplicații sau servicii terță parte.

7.3 Sfaturi pentru profesori

- Fiți conștienți de legile privind confidențialitatea: înțelegeți reglementările privind protecția datelor care se aplică educației și asigurați-vă conformitatea la clasă.
- Utilizați platforme sigure: atunci când desfășurați cursuri online sau utilizați aplicații educaționale, alegeți platforme care acordă prioritate securității și confidențialității datelor. Asigurați-vă că au procese de criptare și de conectare securizate.

- Limitați partajarea datelor cu caracter personal: evitați partajarea inutilă a informațiilor personale ale elevilor. Când este posibil, anonimiizați datele în rapoarte, evaluări sau comunicări publice.
- Gestionarea parolelor: Încurajați elevii să creeze parole puternice și unice pentru conturile școlii și să vă asigurați că nu le partajează. Folosiți instrumente de gestionare a parolelor acolo unde este posibil.
- Dispozitive personale securizate: dacă utilizați dispozitive personale pentru predare sau comunicare cu elevii, asigurați-vă că sunt securizate cu parole, criptare și software actualizat.
- Educați elevii despre confidențialitatea digitală: Învățați elevii despre confidențialitatea online, riscurile de partajare excesivă și cum să se protejeze pe internet. Includeți lecții despre recunoașterea phishing-ului, înșelătoriilor și practicilor de navigare sigură.
- Fiți atenți cu fotografiile și videoclipurile: obțineți consimțământul înainte de a posta sau de a partaja fotografii/videoclipuri ale elevilor online, în special pe platformele publice sau site-urile școlilor.

7.3 Sfaturi pentru elevi/copii

- Înțelegeți ceea ce distribuiți: fiți atenți la informațiile personale pe care le distribuiți online, chiar și pe platformele școlare. Evitați distribuirea adreselor, numerelor de telefon sau fotografiilor personale, dacă nu este necesar.
- Utilizați parole puternice: creați parole puternice și unice pentru conturile de școală și nu le distribuiți niciodată nimănui, inclusiv prietenilor. O parolă bună este un amestec de litere, cifre și simboluri.
- Activați autentificarea în doi factori (2FA): atunci când este disponibil, utilizați 2FA pentru conturile online pentru a adăuga un nivel suplimentar de securitate.
- Fiți atenți online: evitați să faceți clic pe linkuri suspecte sau să descărcați fișiere necunoscute, chiar dacă acestea par să provină de la un prieten sau profesor.
- Nu distribuiți excesiv pe rețelele de socializare: fiți atenți la ceea ce distribuiți pe platformele de rețele sociale, în special în ceea ce privește viața școlară, locația și interesele personale.
- Deconectați-vă de la conturi: deconectați-vă întotdeauna de la dispozitivele partajate după ce utilizați platformele sau conturile școlare.

- Gândește-te înainte de a posta: Odată ce ceva este online, poate fi dificil să îl retragi. Gândește-te bine înainte de a posta ceva, mai ales dacă ți-ar putea afecta confidențialitatea sau a celorlalți.
- Raportați o activitate suspectă: dacă primiți mesaje ciudate sau bănuiți că cineva încearcă să vă acceseze conturile, informați imediat un profesor sau un părinte.

7.4 Sfaturi pentru părinți

- Monitorizați activitatea online: verificați în mod regulat activitatea online a copilului dumneavoastră, în special pentru elevii mai mici, și îndrumați-i cu privire la utilizarea în siguranță a internetului.
- Examinați aplicațiile și platformele școlare: asigurați-vă că aplicațiile și platformele pe care le utilizează școala copilului dumneavoastră sunt sigure și conforme cu reglementările de confidențialitate.
- Discutați confidențialitatea și siguranța: purtați conversații continue cu copiii dumneavoastră despre importanța confidențialității și riscurile potențiale online.

Confidențialitatea și securitatea datelor în școli este o responsabilitate comună între administratori, profesori, elevi și părinți. Stabilirea de politici puternice, utilizarea tehnologiei sigure, educarea tuturor părților și promovarea vigilenței sunt pași cheie în protejarea informațiilor personale și menținerea unui mediu de învățare online sigur.

Bibliografie

- Abdrabou, Y., Abdelrahman, Y., Khamis, M., & Alt, F.. (2021). Think Harder! Investigating the Effect of Password Strength on Cognitive Load during Password Creation. Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems. <https://doi.org/10.1145/3411763.3451636>
- Acemyan, C., Kortum, P., Xiong, J., & Wallach, D.. (2018). 2FA Might Be Secure, But It's Not Usable: A Summative Usability Assessment of Google's Two-factor Authentication (2FA) Methods. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 62, 1141–1145. <https://doi.org/10.1177/1541931218621262>
- Alammary, A., Alshaikh, M., & Pratama, A. R.. (2022). Awareness of security and privacy settings in video conferencing apps among faculty during the COVID-19 pandemic. PeerJ Computer Science, 8. <https://doi.org/10.7717/peerj-cs.1021>
- Amin, M.. (2024). The Importance of Cybersecurity and Protecting of Digital Assets and Understanding the Role of Cybersecurity Laws in Safeguarding Digital Assets. Indian Journal of Public Administration, 70(3), 493–501. <https://doi.org/10.1177/00195561241271520>
- Ansari, M. M., Sharma, P. K., & Dash, B.. (2022). Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. International Journal of Smart Sensor and Adhoc Network.. <https://doi.org/10.47893/ijssan.2022.1221>
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E.. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. <https://doi.org/10.3390/electronics12061333>
- Aurigemma, S., Mattson, T., & Leonard, L. N. K.. (2017). So Much Promise, So Little Use: What is Stopping Home End-Users from Using Password Manager Applications?. Hawaii International Conference on System Sciences, 1–10. <https://doi.org/10.24251/HICSS.2017.490>
- Baek, D. S. *LinkedIn data breach: 700M users compromised*. <https://www.linkedin.com/pulse/linkedin-data-breach-700m-2021-david-sehyeon-baek--ex85c/>
- Bajanthri, B., & Sayeesh, M.. (2022). A Study on Various Phishing Techniques and Recent Phishing Attacks. International Journal of Advanced Research in Science, Communication and Technology, 296–302. <https://doi.org/10.48175/ijarsct-2870>
- Bazzi, A., Shaout, A., & Ma, D.. (2024). Software Update Methodologies for Feature-Based Product Lines: A Combined Design Approach. Software, 3(3), 328–344. <https://doi.org/10.3390/software3030017>
- Blažič, A. J., & Blažič, B. J. (2024). Toward effective learning of cybersecurity: new curriculum agenda and learning methods. *Journal of Cybersecurity*, 10(1), 1-17. <https://doi.org/10.1093/cybsec/tyae018>

- Benjamin Franklin, 1753. "Advice to a Young Tradesman".
- Berners-Lee, T. (1999). *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web by Its Inventor*.
- Bittnet Systems *Tendințe de top privind securitatea cibernetică în prezent*.
<https://www.bittnet.ro/noutati/tendinte-de-top-privind-securitatea-cibernetica-in-prezent/>
- Bodipudi, A.. (2023). Enhancing the VPN Tunnels from IKEv1 to IKEv2 with improved Security Settings. *Journal of Engineering and Applied Sciences Technology*.
[https://doi.org/10.47363/jeast/2023\(5\)262](https://doi.org/10.47363/jeast/2023(5)262)
- Capital One *Digital facts*. <https://www.capitalone.com/digital/facts2019/>
- CardConnect *Target data breach*. <https://www.cardconnect.com/launchpointe/payment-trends/target-data-breach/>
- Center for Strategic & International Studies (CSIS) *Significant cyber incidents*.
<https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>
- Cisco Blogs *Ghid de abordare a atacurilor cibernetice: Mai bine să previi decât să tratezi*.
<https://gblogs.cisco.com/ro/ghid-de-abordare-a-atacurilor-cibernetice-mai-bine-sa-previi-decat-sa-tratezi/>
- Consiliul Uniunii Europene *Cyber threats: EU response*.
<https://www.consilium.europa.eu/ro/infographics/cyber-threats-eu/>
- CyberExperts *Cybersecurity articles*. <https://cyberexperts.com/category/cybersecurity/>
- Cybersecurity Ventures *Cybercrime damages \$6 trillion by 2021*.
<https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>
- Datta, P., Namin, A., & Jones, K. S.. (2022). Can We Predict Consequences of Cyber Attacks?. 2022 21st IEEE International Conference on Machine Learning and Applications (ICMLA), 1047–1054.
<https://doi.org/10.1109/ICMLA55696.2022.00174>
- ENISA *European Cybersecurity Skills Framework*.
<https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework>

- Fakiha, B.. (2022). Effectiveness of Forensic Firewall in Protection of Devices from Cyberattacks. *International Journal of Safety and Security Engineering*. <https://doi.org/10.18280/ijssse.120110>
- Garba, F. A., Dima, R. M., Isa, A. B., Bello, A., Aliyu, A., Yarima, F. U., & Ibrahim, S. A.. (2022). Re-Evaluating the Necessity of Third-Party Antivirus Software on Windows Operating System. *Journal of Cybersecurity and Information Management*. <https://doi.org/10.54216/jcim.090105>
- Gay, R.. (2023). Functional Encryption. *Trends in Data Protection and Encryption Technologies*, 55–58. https://doi.org/10.1007/978-3-031-33386-6_11
- General Data Protection Regulation (GDPR). (2016). Regulation (EU) 2016/679.
- Ghid de bune practici de securitate cibernetica SRI - https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf
- Ghid de securitate cibernetica DNSC <https://dnsc.ro/vezi/document/ghid-securitate-cibernetica-2021>
- Gindra, R. S., Goyal, K., Sethi, J., & Kaushal, C.. (2023). Phishing and Web Hacking: Examining the Vulnerabilities and Defenses in the Digital Age. *2023 6th International Conference on Contemporary Computing and Informatics (IC3I)*, 6, 862–868. <https://doi.org/10.1109/IC3I59117.2023.10397837>
- Gupta, H., & Oorschot, P. V.. (2019). Onboarding and Software Update Architecture for IoT Devices. *2019 17th International Conference on Privacy, Security and Trust (PST)*, 1–11. <https://doi.org/10.1109/PST47121.2019.8949023>
- Huang, S.-Y., Huang, Y., & Mao, C.-H.. (2019). A multi-channel cybersecurity news and threat intelligent engine - SecBuzzer. In *2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 691–695). <https://doi.org/10.1145/3341161.3345309>
- Joyce, R., Sahawneh, F., & Dixon, B.. (2022). Developing a Cybersecurity Educational Community Using Discord During the COVID-19 Pandemic. *The Journal of the Southern Association for Information Systems*. <https://doi.org/10.17705/3jsis.00026>
- Julian Assange's extradition case, United States v. Assange. <https://www.judiciary.uk/wp-content/uploads/2022/07/USA-v-Assange-judgment101221.pdf>
- Kablo, E., Kader, K., & Arias-Cabarcos, P.. (2024). "I'm actually going to go and change these passwords": Analyzing the Usability of Credential Audit Interfaces in Password Managers. *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems*. <https://doi.org/10.1145/3613905.3650889>
- Kafi, M. A., & Akter, N.. (2023). Securing Financial Information in the Digital Realm: Case Studies in Cybersecurity for Accounting Data Protection. *American Journal of Trade and Policy*. <https://doi.org/10.18034/ajtp.v10i1.659>
- Kim, D., Cho, H., Kwon, Y., Doupé, A., Son, S., Ahn, G.-J., & Dumitras, T.. (2021). Security Analysis on Practices of Certificate Authorities in the HTTPS Phishing Ecosystem.

- Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security. <https://doi.org/10.1145/3433210.3453100>
- Lee, J.. (2023). Responding to worsening web browser attacks. *Network Security*, 2023(1). [https://doi.org/10.12968/s1353-4858\(23\)70002-0](https://doi.org/10.12968/s1353-4858(23)70002-0)
- Lyastani, S. G., Backes, M., & Bugiel, S.. (2022). A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites (Extended Version). Arxiv, abs/2210.09373. <https://doi.org/10.48550/arXiv.2210.09373>
- Marimuthu, M., Mohanraj, G., Karthikeyan, D., & Vidyabharathi, D.. (2023). Safeguard confidential web information from malicious browser extension using Encryption and Isolation techniques. *J. Intell. Fuzzy Syst.*, 45, 6145–6160. <https://doi.org/10.3233/jifs-233122>
- Monroe College *Cybersecurity history: Hacking & data breaches*.
<https://www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches>
- Nastase, R. (n.d.). *Introducere în Securitate Cibernetică*. <https://www.microsoft.com/ro-ro/security/business/security-101/what-is-a-cyberattack>
- NCSS *Raportul Fortinet 2023: Tendințe cheie și recomandări în securitatea cibernetică*.
<https://www.ncss.ro/raportul-fortinet-2023-tendinte-cheie-si-recomandari-in-securitatea-cibernetica/>
- NIST (2017). Digital Identity Guidelines. NIST Special Publication 800-63B.
- Oliveira, L., Chmielewski, A., Rutecka, P., Cicha, K., Rizun, M., Torres, N., & Pinto, P.. (2023). Assessing Cybersecurity Hygiene and Cyber Threats Awareness in the Campus - A Case Study of Higher Education Institutions in Portugal and Poland. 2023 IEEE International Conference on Cyber Security and Resilience (CSR), 168–173. <https://doi.org/10.1109/CSR57506.2023.10224910>
- Pandey, S., & Taffese, T.. (2021). Using Performance Predictions to Evaluate Two-factor Authentication Setup Processes. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 65, 999–1003. <https://doi.org/10.1177/1071181321651328>
- Parlamentul României. (2023). *Legea nr. 58 din 14 martie 2023 privind securitatea și apărarea cibernetică a României, precum și pentru modificarea și completarea unor acte normative*. Monitorul Oficial al României, Partea I, nr. 214 din 15 martie 2023.
- Pérez-Sánchez, A., & Palacios, R.. (2022). Evaluation of Local Security Event Management System vs. Standard Antivirus Software. *Applied Sciences*, 12(3), 1076. <https://doi.org/10.3390/app12031076>
- Sarbanes-Oxley Act. (2002). Public Law 107-204.
- Sathvik, D., Dhanalakshmi, D., Prahasith, A., Hariharan, S., Pendam, K., & Kukreja, V.. (2023). Web Extension For Phishing Website Identification: A Browser-Based Security Solution. 2023 International Conference on Research Methodologies in Knowledge

Management, Artificial Intelligence and Telecommunication Engineering (RMKMATE), 1–5. <https://doi.org/10.1109/RMKMATE59243.2023.10369766>

Scientia.ro *Virusul Stuxnet: Atacul asupra programului nuclear iranian.*

<https://www.scientia.ro/tehnologie/8675-virusul-stuxnet-atacul-asupra-programului-nuclear-iranian.html>

SecArmy (2022, October 19) *Introduction to Cybersecurity.* [YouTube].

<https://www.youtube.com/watch?v=x3c1ih2NJEg>

Stallman, R. M. (2002). *Free software, free society: Selected essays of Richard M. Stallman.*

Sutter, T., Bozkir, A. S., Gehring, B., & Berlich, P.. (2022). Avoiding the Hook: Influential Factors of Phishing Awareness Training on Click-Rates and a Data-Driven Approach to Predict Email Difficulty Perception. *IEEE Access*, 10, 100540–100565. <https://doi.org/10.1109/ACCESS.2022.3207272>

Tarbell, I. M. (1904). *The history of the standard oil company.*

TeamPassword *Facebook hacks: A history of security breaches at Facebook.*

<https://teampassword.com/blog/facebook-hacks-a-history-of-security-breaches-at-facebook>

Threater *Lessons learned from the Marriott hack of 2022.*

<https://www.threater.com/blog/lessons-learned-from-the-marriott-hack-of-2022/>

Tolossa, D.. (2023). IMPORTANCE OF CYBERSECURITY AWARENESS TRAINING FOR EMPLOYEES IN BUSINESS. *VIDYA - A JOURNAL OF GUJARAT UNIVERSITY.* <https://doi.org/10.47413/vidya.v2i2.206>

U.S. Constitution, Fourth Amendment.

United States v. Microsoft Corp., 253 F.3d 34 (D.C. Cir. 2001).

Wash, R.. (2020). How Experts Detect Phishing Scam Emails. *Proceedings of the ACM on Human-computer Interaction*, 4(CSCW2), 1–28. <https://doi.org/10.1145/3415231>

Weiss, R. S., Mache, J., Hawthorne, E. K., Siraj, A., Taylor, B., Kaza, S., & Chattopadhyay, A.. (2021). Integrating Hands-on Cybersecurity Exercises into the Curriculum in 2021. In *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education.* <https://doi.org/10.1145/3408877.3439530>

Wikipedia *2017 Equifax data breach.*

https://en.wikipedia.org/wiki/2017_Equifax_data_breach

Wikipedia *Anonymous (hacker group).*

[https://en.wikipedia.org/wiki/Anonymous_\(hacker_group\)](https://en.wikipedia.org/wiki/Anonymous_(hacker_group))

Wikipedia *Cozy Bear*. https://en.wikipedia.org/wiki/Cozy_Bear

Wikipedia *Yahoo! data breaches*. https://en.wikipedia.org/wiki/Yahoo!_data_breaches

World Economic Forum *Cybersecurity Learning Hub*.

<https://www.weforum.org/projects/cybersecurity-learning-hub/>

Ye, Q., Cao, Y., Chen, Y., Li, C., & Li, X.. (2022). Deep Learning-Based User Privacy Settings Recommendation in Online Social Networks. 2022 International Joint Conference on Neural Networks (IJCNN), 1–9. <https://doi.org/10.1109/IJCNN55064.2022.9892734>

Viganò, L. (2024). The cybersecurity of fairy tales. *Journal of Cybersecurity*, 10(1), 1-11. <https://doi.org/10.1093/cybsec/tyae005>