Ambasada SUA în România

Asociația Română pentru Asigurarea Securității Informației (ARASEC)

Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI)

Centrul Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO)

ISBN: 978-973-0-33645-0

GHID DE SECURITATE CIBERNETICĂ

TITLUL PROGRAMULUI:

Îmbunătățirea și dezvoltarea capacității cibernetice în România pentru prevenirea și combaterea fenomenului de criminalitate cibernetică

OBIECTIVUL PROGRAMULUI:

Scopul programului este de a consolida capabilitățile cibernetice în România prin creșterea gradului de conștientizare a securității informațiilor și îmbunătățirea abilităților autorităților de aplicare a legii și ale sectorului privat în combaterea criminalității cibernetice.

Ambasada SUA în România

Asociația Română pentru Asigurarea Securității Informației (ARASEC)

Proiect dezvoltat de Asociația Română pentru Asigurarea Securității Informației (ARASEC).
Acest proiect a fost finanțat parțial printr-o subvenție din partea Departamentului de Stat al Statelor Unite ale Americii.
Opiniile, părerile și concluziile enunțate aici sunt cele ale autorilor și nu reflectă neapărat pe cele ale Departamentului de Stat al Statelor Unite.

eBook: Ghid de securitate cibernetică

Autori: Iulian ALECU, Costel CIUCHI, Toma CÎMPEANU, Iulian COMAN, Larisa GĂBUDEANU, Ioan-Cosmin MIHAI, Cosmina MOGHIOR, Nelu MUNTEANU, Gabriel PETRICĂ, Ionuț STOICA, Cătălin ZETU

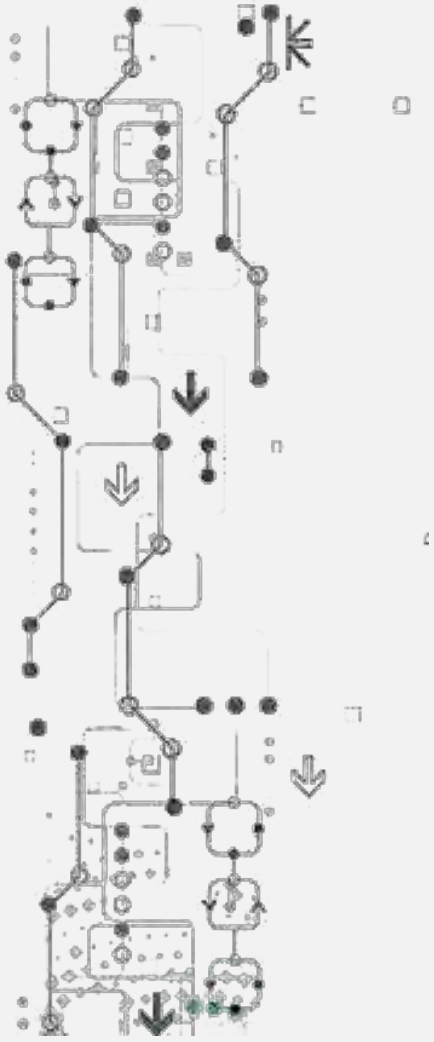
Versiunea: 1.1

Site web: www.cyberlearning.ro/cybersecurity-guide/

ISBN: 978-973-0-33645-0

DOI: 10.19107/CYBERSEC.2021.RO

CUPRINS



DESPRE GHID

DAN CÎMPEAN

Director General al Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO

Suntem martori și actori, uneori involuntari, ai unor transformări digitale accelerate și fără precedent atât la nivel personal, dar și al societății, al economiei. Reflectăm la aceasta și observăm că este nevoie de obținerea unor noi aptitudini, noi cunoștințe, de o schimbare culturală profundă din partea fiecăruia.

Așa cum în copilărie învățam alfabetul cu sprijinul învățătorilor și ne lărgeam orizontul cunoașterii datorită dragostei pentru educație din partea profesorilor, astăzi va trebui să re-începem acumularea un nou bagaj elementar de cunoștințe. De această dată o vom face cu sprijinul unor profesioniști din domeniul securității cibernetice. De această dată, va fi un bagaj de cunoștințe complex, sofisticat, incitant, profund tehnologic dar atât de necesar pentru omul secolului 21. Pentru a reuși aceasta, efortul individual nu este suficient.

Este esențial să existe și promotori activi ai conceptelor, ai programelor de educație și conștientizare privind securitatea cibernetică. Este esențial să putem găsi modalități practice si eficiente de a promova intens chiar la nivel național „igiena cibernetică" dar și alte măsuri preventive ce trebuie transmise spre și aplicate cu regularitate de cetățeni, de organizații și de operatori economici, pentru a reduce la minimum expunerea acestora la riscurile cibernetice.

Iar acum avem o veste bună...

Scrisă sub forma unui ghid concis și pragmatic de securitate cibernetică, această superbă lucrare condensează în doar câteva zeci de pagini peste un secol de experiență concretă în domeniu a celor 11 autori.

Într-o formă clară, simplă, dar nu simplificată, ne sunt transmise și puse la dispoziție atât concepte de bază ca de exemplu confidențialitate, integritate, disponibilitate, protecția datelor personale, dar și elemente specifice provenind din directive și regulamente europene sau din legile României ce abordează subiectul securității cibernetice.

Îndrăznesc să afirm că acest ghid este una din publicațiile atât de necesare azi nouă tuturor. Mai mult, sunt convins că va contribui concret și eficient la educarea publicului larg, în vederea îmbunătățirii stării generale de securitate cibernetică a României, a protecției datelor personale a utilizatorilor tehnologiei informatice și a internetului, prin ajutorul concret pe care îl oferă cititorului privind cunoașterea, prevenirea și contracararea vulnerabilităților, riscurilor și amenințărilor din spațiul cibernetic sau a celor legate de tehnologiile pe care le utilizăm zilnic.
În numele nenumăraților tineri, sau mai puțini tineri, ce vor utiliza practic și pragmatic recomandările ghidului, le transmit autorilor un scurt mesaj de recunoaștere a muncii lor educative și de conștientizare, un mesaj utilizat cu drag în lumea hackerilor etici: ***RESPEKT****!*

SECURIZAREA PC / LAPTOP

Securizarea stațiilor de lucru (PC-uri, laptopuri) și a altor dispozitive conectate la rețele, cu sau fără fir, este o condiție esențială atât pentru asigurarea confidențialității și autenticității datelor sensibile, cât și pentru desfășurarea activităților uzuale la nivelul utilizatorilor tipici.

SOLUȚII

1 *APLICAȚII ȘI SUITE DE SECURITATE*

Se recomandă instalarea unor aplicații anti-malware sau a unor suite de securitate complexe, performante, care să asigure protecția la cele mai recente tipuri de amenințări cibernetice (ransomware, troiani). Actualizarea permanentă a bazei de date cu semnături malware este o condiție necesară pentru detecția celor mai recente forme de amenințări.

2 *CRIPTAREA DATELOR SENSIBILE*

Se recomandă utilizarea unor terțe aplicații sau sisteme de operare ce dețin implementate facilități pentru criptarea datelor sensibile la nivel de fișier individual, folder sau un întreg drive logic.

3 *SECURIZAREA SISTEMULUI DE OPERARE*

Se realizează atât prin repararea breșelor de securitate și a erorilor software la nivelul tuturor componentelor sistemului de operare (prin aplicarea periodică, automată sau manuală, a actualizărilor), cât și prin controlul accesului utilizatorilor la resurse (drepturi de acces la fișiere, servicii și aplicații).

4 *ACTUALIZAREA APLICAȚIILOR*

Este o acțiune absolut necesară deoarece previne unele atacuri cibernetice și scurgeri costisitoare de date, ajutând la păstrarea în siguranță a datelor sensibile. Utilizatorii trebuie să activeze actualizarea automată a tuturor aplicațiilor esențiale (la nivel de sistem de operare, antivirus, firewall sau IDPS).

5 *COPII DE REZERVĂ A DATELOR*

Datele trebuie periodic salvate (*backup*) și stocate pe suporturi magneto-optice de încredere, depozitate în locuri sigure și eventual criptate pentru a evita accesul neautorizat. Aceste copii trebuie păstrate în mai multe locații fizice (sedii) pentru a evita atât dezastrele naturale, cât și amenințările interne din cadrul companiei.

6 *GESTIONAREA PAROLELOR*

În anumite situații se poate recomanda utilizarea unui manager de parole pentru a stoca parole complexe, unice, generate de computer. Parolele folosite trebuie să fie puternice (utilizând caractere alfanumerice și simboluri speciale), să nu fie refolosite la mai multe conturi și trebuie schimbate periodic.

7 *AUTENTIFICAREA CU DOI FACTORI*

Este o metodă foarte eficientă și modernă, care folosește un dispozitiv suplimentar (ex. token de securitate sau un smartphone) pentru a confirma într-un pas suplimentar identitatea persoanei care se autentifică. O autentificare suplimentară poate fi realizată folosind datele biometrice.

8 *UTILIZAREA UNOR CONTURI CU DREPTURI LIMITATE*

Utilizarea unor conturi cu drepturi limitate în locul unui cont de administrator va bloca accesul la zone sensibile ale sistemului de operare și va bloca implicit atacurile ce vizează serviciile sistemului de operare, fișierele sau bibliotecile sale.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

SECURIZAREA ECHIPAMENTELOR MOBILE

În ultimul deceniu, echipamentele mobile (telefoane inteligente, tablete) au cunoscut un grad exponențial de dezvoltare și utilizare. În acest context, asigurarea securității acestui tip de echipament, esențial în comunicații și servicii online, constituie un obiectiv cheie.

SOLUȚII

1 ACTIVAREA FACILITĂȚILOR DE PROTECȚIE ANTIFURT

Printre funcțiile care pot fi activate se numără:

- recunoașterea facială sau a amprentelor;
- deblocarea dispozitivului pe baza unor modele (*patterns*) sau prin PIN;
- localizarea echipamentului;
- blocarea accesului sau ștergerea datelor de la distanță.

2 SINCRONIZAREA DATELOR

Sincronizarea datelor cu alte echipamente sau utilizarea serviciilor în cloud permite ca informații importante (contacte, documente, SMS, imagini) să fie disponibile atunci când echipamentul este pierdut sau furat.

3 ACTUALIZAREA APLICAȚIILOR

Sistemul de operare și aplicațiile trebuie să fie actualizate constant pentru a fixa breșele de securitate și a utiliza cele mai noi funcții.

4 DEZACTIVAREA CONEXIUNILOR NEUTILIZATE

Se recomandă dezactivarea conexiunilor infraroșu, Bluetooth sau Wi-Fi dacă nu sunt utilizate, pentru a bloca accesul neautorizat.

5 UTILIZAREA APLICAȚIILOR SIGURE

Este recomandat să descărcați aplicații numai din surse oficiale și să dezactivați opțiunea privind descărcarea aplicațiilor nesigure.

6 UTILIZAREA UNOR MEDII DE STOCARE VERIFICATE

Înainte de a-l conecta la dispozitivul mobil, mediul de stocare detașabil trebuie scanat cu instrumente antimalware.

7 DISTRIBUIREA INFORMAȚIILOR PERSONALE

Partajarea unor informații personale, cum ar fi locația geografică în timp real (folosind GPS sau rețelele wireless), poate permite unor terți să monitorizeze traseele obișnuite și activitățile zilnice.

8 UTILIZAREA CU PRECAUȚIE A CODURILOR QR (QUICK RESPONSE)

Codurile QR pot conține link-uri către pagini web malițioase, cu diverse efecte dăunătoare în ceea ce privește securitatea datelor: activarea camerei / microfonului, extragerea locației geografice, accesul la fișiere, contacte sau SMS, trimiterea unor mesaje nedorite prin e-mail, SMS sau aplicații de chat, lansarea pachetelor DoS sau furt de identitate.

9 VERIFICAȚI DREPTURILE DE ACCES ALE APLICAȚIILOR

Se recomandă utilizarea Permission Manager pentru a seta accesul unei aplicații la diferite resurse (cameră, microfon, locație, stocare).

10 SECURITATE SUPLIMENTARĂ PENTRU DISPOZITIVELE BUSINESS

Echipamentele furnizate de companii și utilizate în timpul călătoriilor trebuie să fie extra-securizate în ceea ce privește criptarea datelor, conexiunile fără fir (Bluetooth, Wi-Fi) sau mediile amovibile (unități USB, CD/DVD).

11 CONEXIUNI SECURIZATE DE DATE

Se recomandă evitarea hotspot-urilor Wi-Fi publice și utilizarea datele mobile ori de câte ori este posibil.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

SECURIZAREA REȚELEI DE CALCULATOARE

O securizare eficientă a unei rețele locale de calculatoare poate fi realizată prin implementarea următoarelor recomandări cu privire la aspectele tehnice, politicile de securitate, instruirea angajaților unei organizații sau activități de conștientizare a utilizatorilor.

SOLUȚII

1 *SECURITATEA FIZICĂ*

Se referă la controlul accesului în zonele protejate prin supraveghere video, personal de securitate sau blocarea accesului (prin bariere, încuietori, uși), securizarea serverelor și a canalelor de cablu.

2 *FIREWALL, SISTEME IDPS*

Sunt componente strategice ale infrastructurii IT din orice organizație, destinate monitorizării rețelei și urmăririi activităților rău intenționate (detecția intruziunilor, blocarea programelor de tip malware sau filtrarea conținutului periculos).

3 *VIRTUAL PRIVATE NETWORK (VPN)*

Tehnologiile VPN (Rețele private virtuale) sunt soluții pentru acces securizat la distanță și criptarea informațiilor. Se recomandă să fie implementate atunci când datele sensibile sunt transferate prin Internet.

4 *UTILIZAREA PRINCIPIULUI CELUI MAI MIC PRIVILEGIU*

Fiecare cont nou trebuie să aibă alocate cele mai restrictive drepturi de acces, iar drepturi suplimentare vor fi adăugate după necesități. Când nu mai este necesar accesul la date sensibile, trebuie revocate toate privilegiile corespunzătoare.

5 *MONITORIZAREA UTILIZATORILOR*

Pentru a minimiza riscurile unui atac din interior (*insider*) este necesară limitarea numărului de conturi privilegiate și să se acorde permisiuni minime. Orice cont privilegiat trebuie dezactivat dacă nu mai este justificat să fie păstrat.

6 *MĂSURI DE SECURITATE PENTRU REȚELE WIRELESS*

- Utilizarea unor protocoale de rețea securizate (de exemplu WPA2) și a echipamentelor compatibile;
- Dezactivarea serviciilor și a funcțiilor nefolosite;
- Filtrarea echipamentelor permise în rețea pe baza adresei MAC;
- Ascunderea identificatorului rețelei (SSID);
- Atribuirea unor adrese IP statice sau reducerea intervalului de adrese IP alocate dinamic.

7 *SCHIMBAREA PAROLELOR IMPLICITE PENTRU ECHIPAMENTE DE REȚEA ȘI DISPOZITIVE IoT*

Deoarece multe dispozitive au setările implicite publicate pe Internet, pentru a evita deturnarea în scopuri rău intenționate, setările implicite trebuie modificate imediat.

8 *URMĂRIREA ACCESULUI TERȚILOR LA DATE*

Monitorizarea accesului terților (de exemplu, colaboratorii sau partenerii unei companii) la rețeaua internă ar permite detectarea activităților dăunătoare, iar investigațiile pot fi inițiate atunci când este necesar.

9 *CREȘTEREA GRADULUI DE CONȘTIENTIZARE*

Poate fi realizată prin informarea angajaților unei organizații privind motivele și efectele măsurilor de securitate. Pregătirea adecvată a angajaților va duce la un nivel ridicat de securitate cibernetică în organizații.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

PROGRAME MALWARE

Un program malware (software rău intenționat) este o aplicație sau un script conceput cu scopul de a provoca modificarea sau ștergerea datelor informatice, deteriorarea sau restricționarea accesului la calculatoare sau rețele.

Principalele tipuri de programe malware:

- **Viruși**: se replică modificând alte programe de calculator prin introducerea propriului cod.
- **Troieni**: dau impresia că efectuează operațiuni legitime, când încearcă de fapt să exploreze vulnerabilitățile sistemului și să permită infractorilor cibernetici să acceseze sistemul în mod ilegal.
- **Viermi**: aplicații cu efecte distructive care infectează sistemul informatic și se propagă prin Internet.
- **Ransomware**: criptează sau blochează accesul la fișiere și solicită o răscumpărare pentru a elimina restricțiile.
- **Criptomineri**: aplicații care utilizează resursele informatice pentru a mina criptomonede pentru infractorii cibernetici.
- **Adware**: programe care transmit în mod agresiv reclame utilizatorilor.
- **Spyware**: captează diverse informații despre activitatea utilizatorilor pe Internet.
- **Rogueware**: programe care induc în eroare utilizatorii pentru a plăti pentru eliminarea unor infecții false detectate în sistemul de operare.

SOLUȚII

1. ***INSTALAȚI O SOLUȚIE ANTIVIRUS*** pentru a detecta și elimina programele de tip malware în timp real.
2. ***INSTALAȚI O APLICAȚIE DE TIP FIREWALL*** pentru a inspecta traficul de pe paginile web, e-mailuri și aplicații.
3. ***ACTUALIZAȚI APLICAȚIILE ȘI SISTEMELE DE OPERARE*** pentru a remedia eventualele vulnerabilități existente.
4. ***DEZACTIVAȚI EXECUȚIA AUTOMATĂ A SCRIPT-URILOR PE SITE-URI WEB*** pentru a preveni instalarea de programe malware.
5. ***FOLOSIȚI APLICAȚII DE FILTRARE A E-MAILURILOR*** pentru a recunoaște și detecta mesajele și fișierele atașate infectate.
6. ***EVITAȚI SĂ UTILIZAȚI CONTURI DE ADMINISTRATOR*** pentru a preveni ca programele malware să obțină privilegii de administrator.
7. ***FACEȚI COPII DE SIGURANȚĂ A DATELOR*** pentru a le restabili în cazul unei infecții reușite cu malware.
8. ***FOLOSIȚI INSTRUMENTE AVANSATE,*** pentru detectarea programelor malware, cum ar fi sistemele de detectare și prevenire a intruziunilor (IDPS).
9. ***MONITORIZAȚI JURNALELE (LOGS)*** utilizând soluții de gestionare a incidentelor și evenimentelor de securitate (SIEM).
10. ***UTILIZAȚI POLITICI DE SECURITATE*** care specifică pașii care trebuie urmați în cazul unei infectări.
11. ***REDUCEȚI ACCESUL LA FUNCȚIILE POWERSHELL,*** pentru a limita posibilitatea de execuție a codului rău intenționat în consolă.
12. ***RAPORTAȚI INCIDENTE DE SECURITATE*** echipei naționale de răspuns la incidente de securitate cibernetică.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

ATACURI CE VIZEAZĂ CONTURILE DE E-MAIL

Atacurile care folosesc ca vector de atac serviciul de e-mail sunt realizate de obicei dintr-o sursă de încredere, cu intenția de a convinge utilizatorul să deschidă un fișier atașat infectat sau să urmeze un URL către un site web fraudulos. Deși mecanismele atacurilor bazate pe e-mail variază, obiectivul este aproape întotdeauna același: furtul de bani sau date.

Tipuri de atacuri prin e-mail:

- **E-mail bombing:** trimiterea în mod repetat a unui e-mail cu fișiere atașate de dimensiuni mari, la o anumită adresă de e-mail. Acest atac duce la umplerea spațiului disponibil pe server, făcând contul de e-mail inaccesibil.
- **E-mail spoofing:** trimiterea de e-mailuri cu adresa expeditorului modificată. Acest tip de atac este folosit pentru a ascunde identitatea reală a expeditorului și pentru a afla detalii confidențiale sau credențiale necesare pentru a accesa un cont.
- **E-mail spamming:** trimiterea de e-mailuri nesolicitate cu conținut comercial. Scopul acestui atac este de a atrage destinatarii de e-mailuri să acceseze unele site-uri web și să cumpere produse sau servicii mai mult sau mai puțin legitime.
- **E-mail phishing:** trimiterea de mesaje pentru a determina destinatarii e-mailurilor să furnizeze informații despre conturi bancare, carduri de credit, parole sau alte detalii personale.

SOLUȚII

1. ***DEZACTIVAȚI EXECUȚIA AUTOMATĂ A CODULUI***, macrocomenzile, redarea graficelor și preîncărcarea linkurilor în clientul de e-mail.
2. ***FOLOSIȚI SOLUȚII DE SECURITATE PENTRU E-MAIL***, cum ar fi filtre anti spam, scanere antimalware și analizoare URL pentru a identifica site-uri de phishing în timp real.
3. ***PĂSTRAȚI-VĂ CLIENTUL E-MAIL, SISTEMUL DE OPERARE ȘI BROWSERUL WEB ACTUALIZATE ȘI LICENȚIATE.*** Când apar notificările de actualizare, instalați actualizările imediat ce acestea sunt disponibile.
4. ***UTILIZAȚI COMUNICARE SECURIZATĂ PENTRU E-MAIL, CU SEMNĂTURI DIGITALE SAU CRIPTARE*** când transmiteți date și informații sensibile.
5. ***NU DAȚI CLICK PE LINK-URI ȘI NU DESCĂRCAȚI FIȘIERE ATAȘATE*** dacă nu sunteți absolut siguri de sursa e-mailului.
6. ***FOLOSIȚI AUTENTIFICAREA ÎN DOI PAȘI*** pentru a vă proteja conturile. Dacă este implementată este recomandat să o utilizați, pentru a preveni preluarea controlului asupra contului dumneavoastră.
7. ***FOLOSIȚI PAROLE COMPLEXE, PUTERNICE ȘI UNICE*** pentru fiecare serviciu online. Reutilizarea aceleiași parole pentru diverse servicii este o problemă gravă de securitate și ar trebui evitată în orice moment.
8. ***VERIFICAȚI DIN CEL PUȚIN 2 SURSE INFORMAȚIILE PRESTATORULUI BĂNCII PRIN CANALE DIFERITE,*** atunci când transferați bani.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

ATACURI CE VIZEAZĂ SITE-URILE WEB

Aceste tipuri de atacuri sunt metode prin care infractorii cibernetici pot înșela victimele folosind vulnerabilitățile sistemelor și serviciilor web ca vectori de atac. Metodele utilizate acoperă o suprafață vastă de atac, cum ar fi crearea de adrese URL pentru a redirecționa utilizatorii către un alt site web, descărcarea de programe malware și/sau injectarea unui cod rău intenționat într-un site web pentru a exfiltra informații.

Tipuri de atacuri prin web:

- **Drive-By Downloads** - descarcă conținut rău intenționat pe dispozitivul victimei. Utilizatorul final vizitează un site legitim compromis de infractori cibernetici cu scripturi rău intenționate pentru a rula exploit-uri bazate pe browser sau pentru a redirecționa utilizatorul către un alt site web infectat.
- **Watering Hole** - atacuri țintite ca folosesc seturi de exploituri cu caracteristici camuflate. Un actor rău intenționat este interesat să compromită un anumit grup de utilizatori prin utilizarea de exploit-uri sau conținut rău intenționat injectat pe site-ul web.
- **Formjacking** - atacatorii injectează cod rău intenționat în formularele de plată legitime ale unui site web. Acest atac captează în principal informații bancare și alte informații personale de identificare (PII), iar scriptul rău intenționat transmite simultan datele către portal și către infractorii cibernetici.
- **URL rău intenționat** - linkuri create cu intenția de a distribui malware sau de a facilita o înșelătorie. Procesul implică activități de inginerie socială pentru obținerea informațiilor victimelor și pentru a-i convinge să dea clic pe URL-ul rău intenționat, care execută programe malware și compromite calculatorul victimelor.

SOLUȚII

1 *ACTUALIZAȚI SOFTWARE-UL*

Mențineți actualizate sistemele de operare, browserele de internet, plugin-uri, add-on-uri și patch-uri pentru aplicații la zi împotriva vulnerabilităților cunoscute.

2 *ACTIVAȚI FUNCȚII AVANSATE PENTRU PROTECȚIA ENDPOINT*

Utilizați sistemul de prevenire a intruziunii și a prevenirii heuristice a fișierelor pentru o monitorizare completă a comportamentului fișierelor din sistem.

3 *LISTA ALBĂ A APLICAȚIILOR*

Izolați aplicațiile și creați un sandbox pentru a reduce riscul de atacuri de tipul drive-by.

4 *FOLOSIȚI O ABORDARE PROACTIVĂ (SERVERE ȘI SERVICII)*

Controlați periodic versiunea scripturilor de conținut, precum și scanarea fișierelor și a scripturilor găzduite local.

5 *RESTRICȚIONAȚI CONȚINUTUL PE WEB*

Utilizați instrumente precum ad-blockers pentru a limita posibilitatea de a executa coduri rău intenționate în timp ce vizitați anumite site-uri web.

6 *MONITORIZAȚI ȘI FILTRAȚI*

Utilizați instrumente de monitorizare și filtrare a conținutului web și al e-mailurilor pentru detectarea și prevenirea livrării de adrese URL și fișiere dăunătoare.

ATACURI DE TIP DOS ȘI DDOS

Un atac Denial-of-Service (DoS) sau un atac Distributed-Denial-of-Service (DDoS) reprezintă încercări rău intenționate de a perturba traficul normal al unui server, serviciu sau rețea prin suprasolicitarea sistemului țintit sau a infrastructurii cu un volum mare de date.

Tipuri de atacuri DoS sau DDoS:

- **Atacuri bazate pe volum** - obiectivul atacului este de a satura lățimea de bandă a site-ului atacat. (flood UDP, ICMP și alte solicitări cu pachete falsificate).
- **Atacuri de protocol** - acest tip de atac consumă resurse reale ale serverului sau cele ale echipamentelor de comunicații intermediare, cum ar fi firewall-urile și echilibratoarele nivelului de încărcare. (flood SYN, atacuri de pachete fragmentate, Ping of Death, Smurf DDoS etc.).
- **Atacuri la nivel de aplicație** - compuse din cereri aparent legitime, scopul acestor atacuri este de a bloca serverul web. (atacuri reduse și lente, cereri de tip GET / POST, atacuri care vizează vulnerabilitățile Apache, Windows sau OpenBSD etc.).

SOLUȚII

1 *ÎNȚELEGE SERVICIUL*

Înțelegeți punctele în care resursele pot fi epuizate și cine este responsabil pentru aceste resurse.

2 *PLAN DE RĂSPUNS*

Stabiliți un plan de răspuns pentru atacurile *Denial of Service* care să includă degradarea treptată a serviciului.

3 *REDUCEȚI SUPRAFAȚA DE ATAC*

Minimizați suprafața care poate fi atacată, limitând astfel opțiunile pentru atacatori. Nu expuneți porturi, protocoale sau aplicații de unde nu așteaptă nicio formă de comunicare.

4 *PREGĂTIȚI FURNIZORUL DE SERVICII*

Asigurați-vă că furnizorii dvs. de servicii sunt pregătiți să facă față supraîncărcării resurselor și să vă protejeze serviciul.

5 *MONITORIZAȚI ȘI TESTAȚI*

Monitorizați atacurile Denial of Service și testați-vă capacitatea de a răspunde.

6 *ÎNȚELEGEȚI SEMNELE DE ÎNGRIJORARE*

Simptomele unui atac DDoS includ conectivitate neregulată, încetinirea rețelei sau opriri intermitente ale site-ului web. Dacă o lipsă de performanță se prelungește sau este mai severă decât de obicei, rețeaua se confruntă probabil cu un atac DDoS.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

ATACURI CE VIZEAZĂ APLICAȚIILE WEB

Atacurile împotriva aplicațiilor web variază de la manipularea unei baze de date până la perturbarea serviciilor unei rețele pe scară largă. Serviciile și aplicațiile web depind în principal de baze de date pentru a stoca sau furniza informațiile solicitate. Atacurile asupra aplicațiilor web au ca scop exploatarea proprietăților tehnologiilor web și pot fi realizate la diferite niveluri de scară și complexitate și din diverse locații din întreaga lume.

Tipuri de atacuri asupra aplicațiilor web:

- **Cross-Site Scripting (XSS)** - încărcarea unui script malițios pe site-ul web pentru a fura date sau pentru a efectua alte tipuri de daune.
- **SQL Injection (SQLi)** - trimiterea codului distructiv printr-un formular de intrare. Dacă sistemele nu reușesc să curăță aceste informații, acestea pot fi trimise în baza de date, unde pot modifica, șterge sau extrage datele, conform cu cerințele atacatorului.
- **Path Traversal** - protecție necorespunzătoare a datelor care au fost inserate, aceste atacuri de server web implică injectarea de modele în ierarhia serverului web care au permisiunea de a obține drepturi de utilizator, baze de date, fișiere de configurare și alte informații stocate pe servere.
- **Local File Inclusion (Includerea fișierelor locale)** - tehnică de atac care implică forțarea aplicației web de a executa un fișier aflat în partea care nu este publică a sistemului respectiv.

SOLUȚII

1. ***UTILIZAȚI TEHNICI DE VALIDARE ȘI IZOLARE A INTRĂRILOR*** pentru atacuri de tip injecție.
2. ***UTILIZAȚI NIVELURI DE AUTORIZARE ȘI MECANISME STRICTE DE AUTENTIFICARE*** pentru a preveni încălcările de securitate.
3. ***MONITORIZAȚI CAPACITĂȚILE DE GESTIONARE A TRAFICULUI ȘI A LĂȚIMII DE BANDĂ*** și restricționați traficul de intrare numai pentru serviciile necesare.
4. ***DEZVOLTARE SIGURĂ (SECURITY BY DESIGN)*** prin aplicarea procedurilor de securitate în ciclul de viață al dezvoltării și al întreținerii aplicațiilor.
5. ***SCANAȚI APLICAȚIA*** pentru a descoperi orice vulnerabilități și a le remedia cât mai repede posibil.
6. ***IMPLEMETAȚI PROCESE DE GESTIONARE ȘI TESTARE*** a patch-urilor utilizate pentru aplicațiile web.
7. ***REALIZAȚI EVALUĂRI DE RISC ȘI DE EXPUNERE LA VULNERABILITĂȚI*** înainte și în timpul procesului de dezvoltare a aplicațiilor web.
8. ***IMPLEMENTAȚI UN INVENTAR AL API-URILOR (APPLICATION PROGRAMMING INTERFACE) UTILIZATE*** și validați-le împotriva descoperirii scanărilor perimetrale, criptați conexiunea și comunicarea API.
9. ***INSTALAȚI WAF (WEB APP FIREWALL)*** pentru a controla accesul la aplicații web utilizând reguli predefinite pentru a recunoaște și restricționa activitatea suspectă.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

ÎNȘELĂCIUNI PE REȚELELE DE SOCIALIZARE

Înșelăciunile pe rețelele de socializare reprezintă o activitate infracțională concepută pentru a păcăli pe cineva prin utilizarea platformelor de socializare pentru bani sau detalii personale, precum adrese de e-mail, parole și date de naștere.

SOLUȚII

1. ***PROTEJAȚI-VĂ INFORMAȚIILE***
Evitați să distribuiți detalii pe rețelele de socializare care ar putea permite cuiva să vă copieze identitatea și luați în considerare setarea profilului dvs. în modul privat.

2. ***VERIFICAȚI CEREREA***
Verificați solicitările care vin de la prieteni sau cunoștințe înainte de a acționa în acest sens. Contactați direct persoanele respective pentru a vă asigura că nu sunteți înșelat.

3. ***ASIGURAȚI-VĂ CONTURILE***
Creați o parolă puternică și unică pentru toate conturile dumneavoastră online. Nu utilizați niciun fel de detalii personale în parola dumneavoastră.

4. ***AVEȚI GRIJĂ LA CONEXIUNILE DE WI-FI PUBLICE***
Evitați să folosiți aplicații cu informații sensibile în timp ce utilizați conexiuni WI-FI publice.

5. ***TRATAȚI LINK-URILE CU SUSPICIUNE***
Asigurați-vă că analizați cu atenție adresa URL înainte de a vă conecta la orice site web de socializare. Atenție la link-urile scurtate.

6. ***NU COMPLETAȚI CHESTIONARE***
Analizați cu atenție chestionarele atrăgătoare de pe rețelele de socializare. Chiar dacă unele chestionare sunt legitime, acestea pot fi folosite pentru a colecta informații personale.

7. ***EVITAȚI DESCĂRCĂRILE APLICAȚIILOR GRATUITE***
Verificați sursa aplicațiilor care solicită informații personale de pe rețelele dvs. de socializare. Evitați magazinele de aplicații terțe.

8. ***AVEȚI GRIJĂ LA MOMELI***
Fiți conștienți de postările care atrag atenția, indiferent dacă susțin că oferă carduri cadou, câștiguri la o loterie, știri de ultimă oră sau fotografii despre celebrități.

9. ***EVITAȚI DISTRIBUIREA DE INFORMAȚII ÎN EXCES***
Majoritatea oamenilor distribuie informații în exces. Acest lucru poate oferi infractorilor informații utile pentru a crea escrocherii mai bine puse la punct pentru a vă înșela.

10. ***NU DESCĂRCAȚI NICIODATĂ UN FIȘIER ATAȘAT NEAȘTEPTAT***
Nu descărcați un document neașteptat cu aspect legitim atașat unui mesaj, care poate descărca programe malware pe dispozitivul dvs. și poate fura informații personale

11. ***APĂRAȚI-VĂ CONTRA OFERTELOR DE FILME ȘI STREAMING ÎN DIRECT***
Evitați să dați clic pe fluxuri live false sau filme, care merg adesea la site-uri web care distribuie programe malware sau care solicită un card de credit pentru o vizualizare gratuită.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

SIGURANȚA TRANZACȚIILOR ONLINE

Tranzacţiile online prezintă un anumit nivel de risc în ceea ce privește subminarea datelor cu caracter personal, dar există unele metode care pot limita acest risc, folosind mijloace adecvate de prevenire.

Tipuri de atacuri:

- **E-Skimming** sunt atacuri care vizează comercianţii care acceptă plăţi online, prin schimbarea codului sursă a paginilor web aparţinând magazinelor online, pentru a obţine în timp real accesul la datele de acces a clienţilor.
- **Frauda Card-Not-Present (CNP)** este un model de înşelătorie în care atacatorii încearcă să efectueze tranzacţii frauduloase fără a deţine cardul fizic.

SOLUȚII

1. ***VERIFICAȚI MAGAZINELE ȘI VÂNZĂTORII ONLINE*** pentru a vă asigura că sunt legitimi. Un site web de comerţ electronic dezvoltat recent poate fi un semn legat de o posibilă încercare de fraudă.

2. ***VERIFICAȚI SIGURANȚA SITULUI WEB -*** utilizaţi site-uri web care beneficiază atât de un certificat digital, cât şi de o conexiune de tip HTTPS (în stânga adresei URL ar trebui să puteţi vedea semn distinctiv - un lacăt).

3. ***EVITAȚI INTRODUCEREA DATELOR CARDULUI DE CREDIT PE SITE-URI WEB.*** Există numeroase site-uri web în care sunt necesare datele cardului de credit pentru autentificare şi, odată obţinute acele credenţiale, pot fi utilizate ulterior pentru tranzacţii neautorizate.

4. ***INFORMAȚI-VĂ DESPRE DREPTURILE DUMNEAVOASTRĂ*** atunci când alegeţi să achiziţionaţi bunuri şi servicii online şi verificaţi procedura de rambursare.

5. ***ÎNCERCAȚI SĂ EFECTUAȚI PLĂȚI ON-LINE FOLOSIND CARDURI VIRTUALE*** pe care le puteţi reîncărca doar cu sumele minime de bani de care aveţi nevoie pentru tranzacţii şi care pot fi uşor înlocuite în cazul în care au fost compromise sau încercaţi să utilizaţi sisteme alternative de bani electronici, cum ar fi Paypal.

6. ***UNELE MAGAZINE ONLINE OFERĂ CLIENȚILOR POSIBILITATEA DE A PĂSTRA DATELE CARDURILOR*** de credit pentru a facilita tranzacţiile. Examinaţi cu atenţie aceste situaţii şi riscurile asociate acestor site-uri web şi posibilitatea ca acestea să fie compromise de infractori cibernetici (obţinerea accesului la datele dvs.).

7. ***ANUNȚAȚI CÂT MAI RAPID POSIBIL AUTORITĂȚILE COMPETENTE***, dacă consideraţi că aţi fost victima unei fraude.

8. ***FIȚI VIGILENȚI!*** Dacă o ofertă este prea bună pentru a fi adevărată, luaţi în considerare că poate este una falsă!

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

SECURITATEA CARDURILOR DE DEBIT / CREDIT

În urma unor apeluri telefonice sau a unor campanii de phishing prin e-mail, infractorii cibernetici vă pot cere, din diferite motive, datele cardului dvs. de credit. Instituția financiară emitentă sau autoritățile de drept nu vor solicita niciodată aceste date de autentificare, prin urmare, dacă ați furnizat deja aceste date unei alte persoane, trebuie să contactați imediat banca emitentă pentru a bloca cardul.

SOLUȚII

1. ***AVEȚI GRIJĂ DE CARDUL DE CREDIT ÎN ACELAȘI MOD CUM AVEȚI GRIJĂ DE BANI.***

2. ***ATENȚIE LA CODUL PIN ȘI NU ÎL PĂSTRAȚI ÎN PORTOFELUL UNDE ȚINEȚI CARDURILE BANCARE.*** Evitați să fiți văzuți de alții când introduceți codul PIN la bancomat / POS. Nu comunicați codul PIN altor persoane.

3. ***CÂND AVEȚI SUSPICIUNI,*** accesați site-ul web oficial al băncii sau apelați instituția emitentă a cardului.

4. ***EVITAȚI TRIMITEREA DATELOR DE AUTENTIFICARE A CARDURILOR*** prin e-mail sau prin alte mijloace de comunicare.

5. ***NU RĂSPUNDEȚI LA MESAJELE SMS CARE SOLICITĂ PIN-UL,*** datele scrise pe card sau alte elemente de identificare, cum ar fi informațiile utilizate pentru sistemul de tranzacții online.

6. ***PĂSTRAȚI CARDUL ÎN POSESIA DVS.!*** Nu îl dați altor persoane și evitați să-l lăsați în mașină sau în alte locuri publice.

7. ***SETAȚI LIMITE MAXIME PENTRU ACHIZIȚII SAU RETRAGERILE ATM*** pentru a se potrivi nevoilor dvs. și modificați aceste limite doar atunci când este necesar.

8. ***EVITAȚI SĂ UTILIZAȚI ATM-UL DACĂ AVEȚI SUSPICIUNI -*** verificați cu atenție ATM-ul înainte de a efectua retrageri sau tranzacții.

9. ***NU UITAȚI SĂ RIDICAȚI CARDUL DUPĂ CE AȚI COLECTAT BANII DE LA BANCOMAT.***

10. ***NUMĂR TELEFONIC DE URGENȚĂ.*** Este recomandat să aveți numărul de telefon al băncii, să puteți solicita rapid blocarea cardului atunci când există indicii că datele cardului au fost compromise sau când cardul a fost pierdut sau furat.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

FURTUL DE IDENTITATE

Furtul de identitate sau frauda de identificare reprezintă utilizarea ilicită a informațiilor personale de identificare (PII) a victimei de către un infractor, pentru a obține un avantaj financiar și alte beneficii.

Tipuri de tehnici:

- **Identități SIM-Swapping** - această tehnică vizează deținătorii de criptomonede și persoanele sau conturile cu profil înalt, cu intenția de a fura identitatea victimei.
- **Doppelgangers digitali** - tehnica antifraudă „măștile digitale" a fost expusă atunci când identitățile digitale furate au apărut ca un produs de tranzacționare pe piețele darknet.
- **Business Email Compromise (BEC)** - atacatorii fac uz de identitate unei persoane de încredere, de obicei în cadrul companiei, iar victima este păcălită să facă o tranzacție financiară sau să divulge informații sensibile, personale sau corporative.

SOLUȚII

1. ***EVITAȚI UTILIZAREA MANAGERULUI DE PAROLE OFERIT DE BROWSER.*** Dacă este nevoie de unul, utilizați un manager de parole protejat offline.
2. ***AUTENTIFICAREA CU MAI MULȚI FACTORI ESTE O MĂSURĂ DE SIGURANȚĂ*** pentru a preveni furtul sau pierderea parolei și pentru a asigura succesul procesului de autentificare cu mai multe chei.
3. ***AUTENTIFICAȚI ORICE EXPEDITOR AL UNEI CERERI*** pentru a transfera bani personal sau prin telefon.
4. ***PROTEJAȚI ADECVAT TOATE DOCUMENTELE ȘI COPIILE ACTELOR DE IDENTITATE*** (fizic sau digital) împotriva accesului neautorizat.
5. ***NU DIVULGAȚI INFORMAȚII PRIVIND IDENTITATEA*** cererilor nesolicitate prin telefon, e-mail sau care nu ar trebui să primească răspuns.
6. ***UTILIZAȚI DISPOZITIVE PROTEJATE CU PAROLĂ,*** asigurând o bună calitate a credențialelor și metode sigure pentru stocarea acestora.
7. ***ACORDAȚI ATENȚIE SPORITĂ LA UTILIZAREA REȚELELOR PUBLICE WI-FI.*** Dacă se folosește una, evitați accesul la aplicații și date sensibile. Folosiți un serviciu VPN de încredere pentru a vă conecta la rețelele Wi-Fi publice.
8. ***ASIGURAȚI O BUNĂ CALITATE A CREDENȚIALELOR ȘI A METODELOR DE SIGURANȚĂ*** pentru stocarea acestora pe toate mediile utilizate.
9. ***VERIFICAȚI TRANZACȚIILE*** documentate prin extrase bancare sau studiați regulat chitanțele pentru nereguli.
10. ***INSTALAȚI FILTRAREA DE CONȚINUT*** pentru a filtra fișierele atașate nedorite, e-mailurile cu conținut rău intenționat, spamul și traficul de rețea nedorit.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

AMENINȚĂRI DIN INTERIOR

O amenințare din interior este o amenințare care poate duce la un incident de securitate cibernetică, efectuată de o persoană sau de un grup de persoane afiliate care lucrează pentru organizație.

SOLUȚII

STABILIȚI PROGRAMUL

1. Implementați o tehnologie de inspecție profundă a pachetelor (DPI) pentru detectarea anomaliilor. Adoptați o vizualizare orientată către utilizator, pentru identificarea activității de amenințare din interior.

INSTRUIȚI-VĂ ECHIPA

2. O forță de muncă activă, instruită să recunoască și să raporteze activitatea suspectă sau comportamentul inadecvat, poate ajuta la apărarea împotriva amenințărilor din interior.

REDUCEȚI ACCESUL

3. Reduceți numărul de utilizatori cu privilegii și acces la informații sensibile.

ALOCAȚI SCORURI DE RISC

4. Aplicațiile cognitive pentru analiza comportamentală pot atribui scoruri de risc pentru a identifica în mod proactiv riscurile potențiale din interior, înainte de a se produce o încălcare.

INTRODUCEȚI UN PLAN DE CONTRAMĂSURI

5. Includeți un cadru de gestionare a riscurilor, un plan de continuitate a activității, un program de recuperare în caz de dezastru, o politică de management financiar și contabil și un management legal și de reglementare.

IMPLEMENTAȚI CONTROALE TEHNICE ROBUSTE

6. Implementați prevenirea pierderii de date (DLP) pentru a proteja activele și pentru a preveni exfiltrarea datelor.

ÎNTĂRIȚI SECURITATEA CIBERNETICĂ

7. Fiți conștienți de importanța securității rețelei, sistemelor, aplicațiilor, datelor și conturilor.

SOLICITĂRI PRIVIND DATELE PERSONALE

Există cerințe specifice pentru depunerea, răspunsul către și permiterea exercitării în totalitate a drepturilor persoanelor fizice conform GDPR (General Data Protection Regulation).

ASPECTE PRACTICE

1

DEPUNEREA SOLICITĂRILOR

Utilizați canalele stabilite de organizație. Specificați situația/datele/tipul de cerere. Furnizați detalii și documente suficiente.

2

RĂSPUNSUL - PROCEDURĂ

Verificați:
(a) modalitatea de utilizare a pașilor de autentificare;
(b) cerința de a notifica organizațiile către care sunt dezvăluite date;
(c) condițiile de extindere a termenului de răspuns. Furnizați răspunsul într-un mod securizat.

3

RĂSPUNSUL – CONȚINUT

Verificați:
(a) datele structurate și nestructurate;
(b) datele deținute de împuterniciți;
(c) dacă datele confidențiale/secrete comerciale trebuie să nu fie dezvăluite.

4

DREPTUL DE ACCES LA DATE

Solicitați detaliere dacă sunt prea generale solicitările și presupun un volum semnificativ de date. Verificați orice cerințe legale contrare – ex. obligațiile legale de confidențialitate.

5

RECTIFICAREA DATELOR PERSONALE

Efectuați modificările în toate sistemele IT, la împuterniciți și în toate locațiile care conțin date. Verificați acuratețea datelor furnizate.

6

PORTABILITATE

Pregătiți datele într-o manieră structurată, utilizată în general și citibilă de către calculator (ex. .csv). Trimiteți datele către persoanele fizice sau către organizația indicată.

7

DECIZII AUTOMATE

Furnizați suficiente detalii pentru persoanele fizice pentru înțelegerea algoritmului și procesului de decizie. Verificați mecanismul de decizii automate și impactul asupra persoanelor fizice.

8

OBIECȚII, ȘTERGERI ȘI RESTRICȚIONAREA PRELUCRĂRII

Verificați dacă motivele de respingere a solicitării sunt aplicabile. Aplicați măsura către toate copiile datelor personale în organizație și cu împuterniciți.

GHID DE SECURITATE CIBERNETICĂ, ISBN: 978-973-0-33645-0, DOI: 10.19107/CYBERSEC.2021.RO

CONFORMITATEA PROTECȚIEI DATELOR – IMM-URI

Cele patru arii de avut în vedere:
(1) Fluxuri de date personale (în cadrul și către/de la o organizație);
(2) Sisteme IT implicate în fluxul de date;
(3) Dezvăluirea datelor către/de la alte organizații;
(4) Proceduri interne corespunzătoare.

ETAPE PRINCIPALE

1 *FLUXURI DE DATE ȘI SCOP*

Identificați
(a) colectarea, stocarea, procesarea și dezvăluirea de date;
(b) temeiul de prelucrare;
(c) locația datelor;
(d) scopurile de prelucrare inițială și subsecvente.

2 *MINIMIZAREA DATELOR*

Colectați, stocați, procesați și dezvăluiți numai tipurile / volumul de date necesar(e).

3 *TRANSPARENȚA PRELUCRĂRII*

Informați adecvat despre prelucrarea datelor personale în general înainte de colectare/prelucrare.

4 *MĂSURI DE SECURITATE SPECIFICE*

(a) limitați accesul conform principiului de limitare a cunoaștere a clientelei;
(b) protejați datele stocate și în tranzit;
(c) efectuați controale privind confidențialitatea, integritatea și disponibilitatea pe baza datelor deținute și rolul sistemelor IT în fluxul de date.

5 *GESTIONAREA TERȚILOR*

(a) identificați dezvăluirile de date personale;
(b) încheiați contracte corespunzătoare;
(c) monitorizați/asigurați conformități continue corespunzătoare.

6 *PROTECȚIA DATELOR*

Realizați analize specifice pentru a asigura protecția corespunzătoare a drepturilor persoanelor prin referință la interesul / scopul organizației.

7 *PROCEDURI ȘI PROCESE INTERNE*

(a) Planificați (toate de recomandările de mai sus, inclusiv administrarea incidentelor și răspunsul la solicitări pentru persoane);
(b) Implementați (folosiți mecanisme corespunzătoare pentru implementare);
(c) Verificați (realizați o monitorizare continuă a implementării);
(d) Acționați în legătură cu aspecte observate din auditare, monitorizare, investigare sau din incidentele privind datele personale.

REPETAȚI PAȘII.

TRANSPARENȚA PRELUCRĂRII DE DATE

Notele de informare furnizate către persoanele fizice ale căror date sunt prelucrate reflectă specificitatea prelucrării de date, inclusiv înainte de obținerea consimțământului (dacă acesta este temeiul de prelucrare).

ASPECTE PRINCIPALE

1 *FORMA NOTEI DE INFORMARE*

Folosiți text structurat sau metode vizuale (ex. info-grafice). Puteți utiliza întreaga notă de informare sau o abordare etapizată.

2 *ADUCEREA ÎN ATENȚIA PERSOANELOR FIZICE*

În general, aduceți la cunoștință la începutul colectării datelor sau la stabilirea noului scop de prelucrare a acestora.

3 *ETAPE PROCEDURALE*

Păstrați dovada citirii de către persoane (ex. log-uri sau buton pentru luarea la cunoștință). Păstrați toate versiunile notelor de informare folosite.

4 *CONȚINUT AL NOTEI DE INFORMARE*

Folosiți un text concis, clar (fără aspecte interpretabile), inteligibil, ușor de înțeles conform specificității persoanei (ex. copil).

5 *DETALIILE PRINCIPALE DE INCLUS*

- Scopul și temeiul de prelucrare;
- Dezvăluirea către alte organizații;
- Perioada de stocare a datelor;
- Tipuri de date personale prelucrate;
- Transferuri în afara Uniunii Europene;
- Detalii decizii automate.

6 *ADMINISTRAREA CONSIMȚĂMÂNTULUI*

Permiteți retragerea facilă a consimță-mântului, fără pre-bifarea casetei de obținere a consimțământului. Re-obțineți consimțământul după o anumită perioadă.

7 *CONȚINUTUL CONSIMȚĂMÂNTULUI*

Prezentați cu granularitate fiecare scop de prelucrare, detalii specifice pentru scopul de prelucrare. Expuneți nota de informare înainte de obținerea consimțământului.

8 *CONDIȚIILE PENTRU PRELUAREA CONSIMȚĂMÂNTULUI*

Consimțământul trebuie să fie liber acordat (fără condiționare, subordonare sau consecințe negative), printr-o acțiune clară a persoanei fizice.

DIRECTIVA NIS

Directiva NIS este prima lege la nivel european privind securitatea cibernetică. Legea include măsuri concrete pentru creșterea nivelului general de securitate cibernetică în Uniunea Europeană. Directiva este transpusă în România prin Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice.

PRINCIPALELE ELEMENTE

1. ***ASIGURĂ CĂ OPERATORII DE SERVICII ESENȚIALE (OSE)*** iau măsurile de securitate adecvate și notifică incidentele semnificative autorităților naționale.

2. ***SE ADRESEAZĂ OPERATORILOR DE SERVICII ESENȚIALE (OSE),*** care sunt întreprinderi private sau entități publice cu un rol important pentru societate și provin din sectoarele: energie, transport, infrastructura pieței financiare, sectorul bancar, sănătate, furnizarea și distribuirea apei potabile și infrastructura digitală.

3. ***ARMONIZAREA LA NIVELUL UE,*** în special în ceea ce privește identificarea și măsurile de securitate aplicate OSE, este necesară pentru a atinge un nivel similar de reziliență cibernetică pe piața internă, considerând că amenințările cibernetice au impact transfrontalier.

4. ***DIRECTIVA ASIGURĂ BUNA FUNCȚIONARE A PIEȚEI INTERNE*** prin adoptarea măsurilor de securitate care ajută la atingerea unui nivel comun ridicat de securitate a rețelelor și a sistemelor de informatice din întreaga Uniune Europeană.

5. ***CADRUL INSTITUȚIONAL NAȚIONAL*** este actualizat prin desemnarea unei autorități naționale cu responsabilități de reglementare, supraveghere și control în domeniul securității rețelelor și sistemelor informatice, un punct unic de contact la nivel național și echipa națională CSIRT.

6. ***CREEAZĂ UN GRUP DE COOPERARE*** compus din reprezentanți ai statelor membre, ai Comisiei și ENISA. Rolul grupului este de a sprijini și facilita cooperarea strategică și schimbul de informații, stimulând încrederea între statele membre.

7. ***CREEAZĂ O REȚEA CSIRT*** compusă din CSIRT-uri naționale și CERT-EU. Cel mai important rol al său este acela de a face schimb de informații, de a coordona răspunsurile la incidente și de a oferi sprijin în gestionarea incidentelor transfrontaliere.

8. ***ÎNCURAJEAZĂ ADOPTAREA UNEI STRATEGII NAȚIONALE*** privind securitatea rețelelor și a sistemelor informaționale care să definească obiectivele strategice și măsurile politice și de reglementare adecvate.

RAPORTAREA INCIDENTELOR

Apel de urgență: 1911

Cum se raportează?

Sunând la numărul unic de urgență **1911** sau trimițând un e-mail la **alerts[@]cert.ro**.

Cine poate raporta?

Persoanele fizice și juridice pot apela acest număr unic dacă sunt victime ale unui incident cibernetic.

Ce tipuri de incidente?

Sistemele informatice vulnerabile sunt compromise sau infectate cu diferite tipuri de programe malware. Activități rău intenționate, cum ar fi, dar fără a se limita la escrocherii, phishing, fraude și vishing.

Cum putem ajuta?

Se oferă suport, asistență și sortare (ticketing). Asistența tehnică inițială ajută victima potențială să reducă sau să elimine amenințarea. Următorul pas este analizarea informațiilor pentru a pregăti răspunsul la incident și a crea o alertă de securitate cibernetică. Dacă incidentul raportat face obiectul unei infracțiuni, îndreptăm victima potențială către autoritățile de aplicare a legii (de ex. poliția).

Directiva NIS

Cum se raportează?

Raportarea formală inițială se face printr-o platformă dedicată, unde se furnizează o serie de informații specifice. Apoi, pentru gestionarea incidentului, se face schimb de informații și colaborare pe Malware Information Sharing Platform (MISP).

Cine poate raporta?

Operatorii de servicii esențiale sunt obligați să notifice imediat CERT-RO, acționând în calitate de CSIRT național, orice incident care are un impact semnificativ asupra continuității serviciilor esențiale pe care le furnizează.

Ce tipuri de incidente?

Se notifică incidentele care depășesc pragurile semnificative de impact asupra furnizării serviciului esențial. Criteriile pentru stabilirea impactului sunt numărul de utilizatori afectați, durata și distribuția geografică a atacului.

Cum putem ajuta?

După notificare, se evaluează impactul incidentului și se creează o alertă. Echipa națională CSIRT coordonează răspunsul la incident și oferă entității afectate informații pentru a sprijini gestionarea incidentelor.

CVD*

Cum se raportează?

Scriind un e-mail la cvd[@]cert.ro, care să includă toate detaliile tehnice, inclusiv o descriere a vulnerabilității, pașii și tehnicile de reproducere a acesteia, dar și mijloacele de descoperire.

Cine poate raporta?

Profesioniști și neprofesioniști în domeniul rețelelor și sistemelor informatice care au identificat o vulnerabilitate a unui serviciu sau sistem informatic oferit publicului și doresc să-l raporteze pentru remediere.

Ce tipuri de incidente?

Orice tip de vulnerabilitate a unui serviciu sau a unui sistem informatic oferit publicului.

Care este rolul CERT-RO?

Asigură cadrul de desfășurare a activității CVD, emite linii directoare și informații utile și oferă recunoaștere publică atunci când părțile interesate o doresc.

Coordinated Vulnerability Disclosure

REFERINȚE

1. Cybersecurity and Infrastructure Security Agency (CISA), Publications on cybersecurity. Disponibil: https://us-cert.cisa.gov/security-publications.
2. European Union Agency for Cybersecurity (ENISA), Publications from the Threat Landscape 2020 Series. Disponibil: https://www.enisa.europa.eu/publications.
3. European Union Agency for Law Enforcement Cooperation (EUROPOL), Publications and documents on cybercrime. Disponibil: https://www.europol.europa.eu/publications-documents.
4. European Union Agency for Law Enforcement Training (CEPOL), E-Journals on cybercrime. Disponibil: https://www.cepol.europa.eu/science-research/journals/e-journals.
5. European Institute of Romania, Current challenges in the field of cybersecurity – the impact and Romania's contribution to the field. Disponibil: http://ier.gov.ro/wp-content/uploads/2018/10/SPOS_2017_Study_4_FINAL.pdf.
6. International Journal of Information Security and Cybercrime (IJISC). Disponibil: https://www.ijisc.com/.
7. Romanian Association for Information Security Assurance (RAISA), Considerations on challenges and future directions in cybersecurity. Disponibil: https://www.raisa.org/documents/CybersecurityRO2019.pdf.
8. Romanian National Computer Security Incident Response Team (CERT-RO), Cybersecurity guides. Disponibil: https://cert.ro/doc/ghid.
9. National Association for Information Systems Security (ANSSI), Guide for securing computers and networks. Disponibil: https://cert.ro/vezi/document/ghid-bune-practici-pentru-securizarea-calculatoarelor-personale.
10. National Cyberint Center within the Romanian Intelligence Service, Best practices guide for cybersecurity. Disponibil: https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf.

ACRONIME

API - Application Programming Interfaces
APT - Advanced Persistent Threat
ATM - Automated Teller Machine
CD / DVD - Compact Disc / Digital Versatile Disc
CERT- Computer Emergency Response Team
CMS - Content Management System
CSIRT - Computer Security Incident Response Team
CVD - Coordinated Vulnerability Disclosure
DDoS - Distributed Denial of Service
DLP - Data Loss Prevention
DoS - Denial of Service
DPI - Deep Packet Inspection
GPS - Global Positioning System
ICMP - Internet Control Message Protocol
IDPS - Intrusion Detection and Prevention Systems
IoT - Internet of Things
IP - Internet Protocol
LAN - Local Area Network
MAC (address) - Media Access Control
OES - Operators of Essential Services
OS - Operating System
PDF - Portable Document Format
PII - Personal Identifiable Information
PIN - Personal Identification Number
POS - Point of Sale
QR (code) - Quick Response
SIEM - Security Incident and Event Management
SME - Small and Medium-sized Enterprises
SOHO - Small Office / Home Office
SQL - Structured Query Language
SQLI - SQL Injection
SSID - Service Set Identification
UDP - User Datagram Protocol
URL - Uniform Resource Locator
USB - Universal Serial Bus
VPN - Virtual Private Network
WPA2 (protocol) - Wi-Fi Protected Access
XSS - Cross-Site Scripting

AUTORI

Iulian ALECU este directorul general adjunct al Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), cu o experiență de peste opt ani în securitate cibernetică și cooperare internațională. În contextul deținerii de către România a Președinției Consiliului Uniunii Europene, a condus Grupul de cooperare NIS între statele membre.

Costel CIUCHI este expert în cadrul Direcției Tehnologia Informației și Digitalizare, Secretariatul General al Guvernului, cu responsabilități în dezvoltarea aplicațiilor și infrastructurii guvernamentale, securitatea IT (INFOSEC) și coordonarea registrului de domenii GOV.RO. Profesor asociat la Universitatea Politehnica din București, desfășoară activități de cercetare în domeniul proceselor decizionale și securității cibernetice.

Toma CÎMPEANU este directorul executiv al Asociației Naționale pentru Securitatea Sistemelor Informatice (ANSSI). În ultimii 20 de ani a ocupat poziții de conducere atât în sectorul public, cât și în companii private și a contribuit la dezvoltarea multor sisteme integrate naționale precum e-licitatie.ro, ghiseul.ro, Punctul de Contact Unic (PCUe), Ro-Net și altele.

Iulian COMAN este expert național detașat la Agenția Uniunii Europene pentru Formare în Materie de Aplicarea Legii (CEPOL), ofițer de poliție în cadrul Ministerului Afacerilor Interne, România, cu expertiză în analize, instruire în domeniul aplicării legii și relații internaționale. Este doctorand în domeniul ordinii publice și al securității naționale la Academia de Poliție "Alexandru Ioan Cuza" București.

Larisa GĂBUDEANU este un expert în protecția datelor și doctorand la Universitatea Babeș-Bolyai. Cu o experiență vastă ca avocat într-o firmă internațională, oferind consultanță clienților internaționali și coordonând proiecte cu privire la drept informatic și protecția datelor, ea are cunoștințe în domeniul securității informatice din experiența practică într-un grup regional bancar și din zona academică.

Ioan-Cosmin MIHAI este cercetător, profesor, formator și speaker, având o experiență de peste 15 ani în domeniile securității și criminalității cibernetice. Este conferențiar universitar la Academia de Poliție „Al. I. Cuza", profesor invitat la Universitatea Națională de Apărare „Carol I" și Universitatea Politehnica din București, precum și vicepreședinte al Asociației Române pentru Asigurarea Securității Informației (ARASEC).

Cosmina MOGHIOR este expert în politici publice la CERT-RO, unde reprezintă instituția în cadrul Grupului de cooperare NIS și oferă expertiză în cadrul Grupului european de certificare a securității cibernetice. De asemenea, este doctorand la Școala Națională de Studii Politice și Administrative, cu teza „Suveranitatea digitală europeană: independența tehnologică în contextul confruntării strategice".

Nelu MUNTEANU este directorul tehnic al Centrului Național de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), cu o experiență de peste 18 ani în domeniile IT&C și securitate cibernetică. Coordonează departamentul tehnic la CERT-RO din 2016 și participă la numeroase activități dedicate creșterii nivelului de conștientizare și educație privind securitatea cibernetică.

Gabriel PETRICĂ are o vastă experiență dobândită în peste 25 de ani de activitate în domeniul TIC. Cu un doctorat în inginerie electronică și telecomunicații, domeniul său de interes include fiabilitatea sistemelor, programarea Web și securitatea informațiilor. În prezent desfășoară activități didactice și de cercetare în cadrul Facultății de Electronică, Telecomunicații și Tehnologia Informației, Universitatea Politehnica din București.

Ionuț STOICA este ofițer principal de proiect în cadrul Oficiului Consiliului Europei în domeniul Criminalității Informatice (C-PROC), cu o experiență de peste 14 ani în investigații și formare în domeniul criminalității cibernetice. În prezent, este implicat în programe de consolidare a capacităților în securitate cibernetică și este instructor în domeniul criminalității informatice pentru Institutul Bancar Român.

Cătălin ZETU conduce Biroul de investigare a atacurilor cibernetice, din cadrul Poliției Române, cu responsabilități privind investigarea, culegerea de informații și dezvoltarea parteneriatelor public-private, pentru îmbunătățirea capacităților operaționale. Ofițer investigator cu experiență în domeniul criminalității cibernetice, a lucrat sau a supravegheat cazuri importante cu multiple ramificații internaționale.

Asociația Română pentru Asigurarea Securității Informației

Asociația Română pentru Asigurarea Securității Informației (ARASEC) este o asociație științifică non-guvernamentală, non-profit, nepartizană politic, cu beneficiu public. Fondată în anul 2012, ARASEC a apărut ca o inițiativă dedicată promovării securității informației.

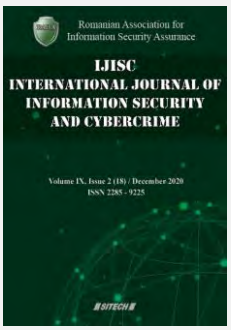
Scopul Asociației Române pentru Asigurarea Securității Informației este promovarea și susținerea activităților de securizare a informației în concordanță cu normele legale în vigoare, precum și crearea unei comunități în domeniu care să permită schimbul de cunoștințe între specialiștii din mediul instituțional, privat și academic din România.

Viziunea Asociației este de a promova cercetarea și educația în domeniul securității informației, precum și de a contribui la crearea și difuzarea cunoștințelor și tehnologiei în domeniu. ARASEC are o reprezentare importantă la nivel național, reunind cadre didactice și cercetători din universitățile și instituțiile românești, doctoranzi, masteranzi sau studenți, precum și societăți comerciale din segmentul IT.

Site web**:** www.arasec.ro (RO) / www.raisa.org (EN)

ARASEC susține activitatea științifică în domeniul securității și criminalității informatice prin publicarea și promovarea unor cărți și studii de specialitate și a revistei științifice *International Journal of Information Security and Cybercrime (IJISC)*. Această revistă este o publicație bianuală ce are ca scop analizarea securității informației, a sistemelor informatice și a comunicațiilor, precum și identificarea noilor valențe ale fenomenului de criminalitate informatică.

Site web: www.ijisc.com



Portaluri și canale media ARASEC:

SECURITATEA INFORMAȚIILOR
www.securitatea-informatiilor.ro

SECURITATEA CIBERNETICĂ
www.securitatea-cibernetica.ro

SECURITATEA REȚELELOR
www.securitatea-retelelor.ro

CRIMINALITATEA INFORMATICĂ
www.criminalitatea-informatica.ro

GHID DE SECURITATE CIBERNETICĂ