Protecția informației. Prevenirea și curmarea fraudelor informatice

Autor: Tatiana Busuncian
Dr., conferențiar universitar

Chișinău 2025

Conținuturi, Obiective de referință

Obiective de referință:

- să definească caracteristicile securității informaționale;
- să determine instrumentele şi metodele de luptă cu amenințările cibernetice;
- să evalueze motivele criminalității cibernetice şi să descrie eforturile întreprinse pentru asigurarea securităţii informaționale şi de securitate națională, în general;
- să estimeze importanța prevenirii amenințărilor complexe și persistente la adresa securităţii informaționale.

Termeni-cheie: *securitate informațională, știri false, mediului informaţional, pericol, politică.*

Asigurarea securităţii informaţionale

→ Misiunile primordiale în prevenirea şi combaterea agresiunilor din mediul virtual, intern sau extern sunt îndreptate spre sistemele informatice şi de comunicaţii electronice de importanţă statală. Aceste misiuni sunt realizate, în conformitate cu legislaţia în vigoare, prin intermediul unor procese operaţionale cum ar fi:

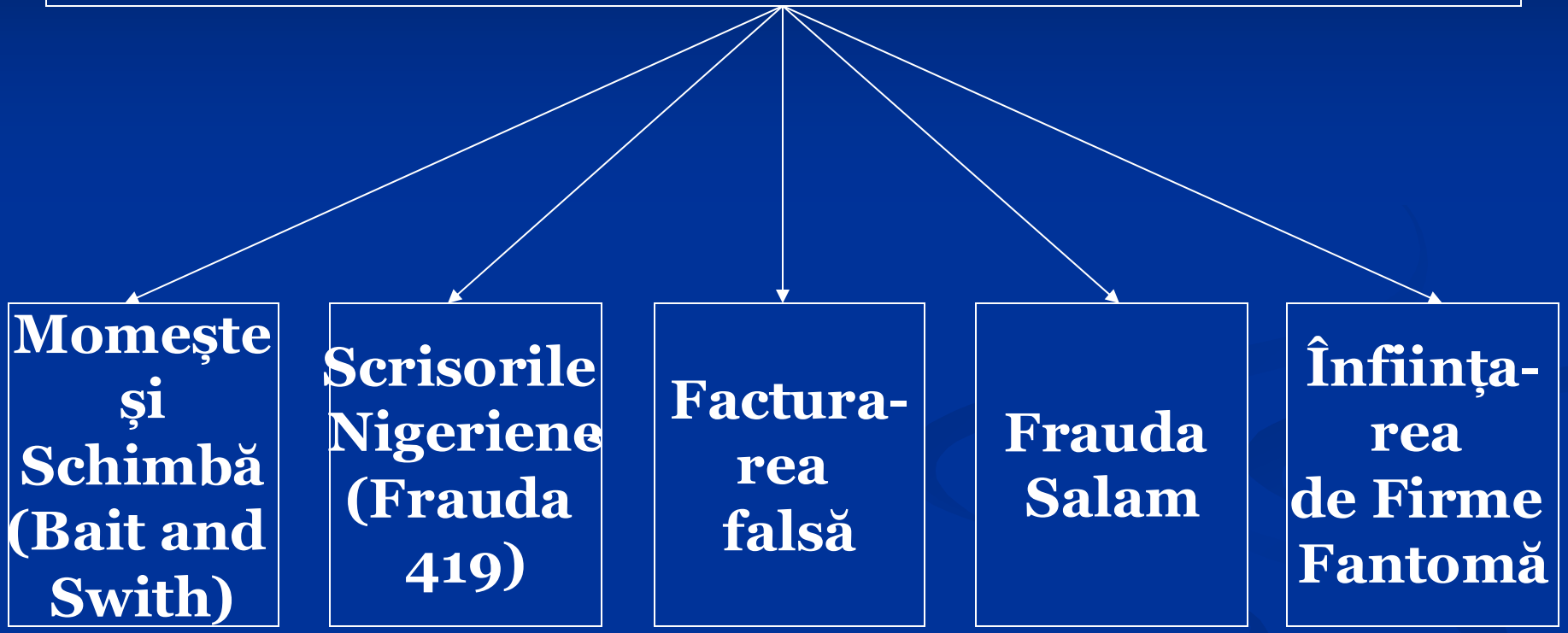
- elaborarea propunerilor privind asigurarea securităţii informatice, elaborarea şi promovarea politicii de stat şi exercitarea controlului în domeniul asigurării protecţiei informaţiei atribuite la secretul de stat în spaţiul cibernetic;
- crearea, asigurarea funcţionării şi securităţii sistemelor guvernamentale de comunicaţii electronice, elaborarea strategiei şi realizarea politicii naţionale în domeniul creării, administrării şi asigurării funcţionării şi securităţii sistemelor speciale de comunicaţii electronice;
- asigurarea conducerii ţării, a ministerelor, departamentelor şi a altor autorităţi publice, inclusiv şi în străinătate, conform Nomenclatorului întocmit de Guvern, cu legătură guvernamentală, cifrată, secretă şi cu alte tipuri de telecomunicaţii, organizarea şi asigurarea siguranţei exploatării lor;
- depistarea emiterilor radio ale mijloacelor radioelectronice emiţătoare a căror activitate periclitează securitatea de stat.

Fraudele informatice: considerații generale

→ **Fraudele informatice** reprezintă „orice infracţiune în care un calculator sau o reţea de calculatoare este obiectul unei infracţiuni, sau în care un calculator sau o reţea de calculatoarea este instrumentul sau mediul de înfăptuire a unei infracţiuni”.

→ **În sens restrîns:** „orice infracţiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor”.

Formele fraudelor informatice vechi



Momește și schimbă

- **Este o formă de fraudă informatică în care făptuitorul ademenește potențiali clienți făcând publicitate unor produse, care fie nu există în realitate, fie sunt ulterior schimbate cu produse aparent similare, dar cu calități net inferioare.**

Scrisorile nigeriene

- **Sunt adesea cunoscute sub denumirea de „transferuri nigeriene” sau „Fraude cu avans” ori, pur si simplu, „înșelătorii 419” (după Codul Penal al Nigeriei se încriminează astfel de fapte).**

Depozite false

- **O altă metodă de fraudare în sisteme informatice prin care, autorul după ce câștiga o licitație de produse pe un site Internet specializat (gen eBay), solicită victimei utilizarea unui site de escrow „sigur”, „neutru” care să „depoziteze” bunurile (produsele – în general echipamente electronice) pâna la perfectarea aranjamentelor financiare.**

Mailbombing

Este considerată cea mai veche metodă de atac, deși esența sa este simplă și primitivă: un număr mare de mesaje de e-mail fac imposibilă lucrul cu cutiile poștale și, uneori, cu servere de mail întregi.

Multe programe au fost dezvoltate în acest scop și chiar și un utilizator neexperimentat ar putea efectua un atac specificând doar e-mailul victimei, textul mesajului și numărul de mesaje necesare.

Selectarea parolei

- Următorul tip de atac este, de asemenea, simplu. Crackerul ridică parole pentru sistemele de control al accesului. La urma urmei, este destul de evident că utilizatorii de sisteme de calcul nu sunt de obicei capabili să țină cont de combinații de litere, cifre și semne lungi de până la o sută de caractere.

Viruși, troieni, viermi de corespondență, sniffer, rootkit-uri și alte programe speciale

Următorul tip de atac este o metodă mai sofisticată de a obține acces la informații clasificate - aceasta este utilizarea de programe speciale pentru a lucra pe computerul victimei.

Astfel de programe sunt concepute pentru a căuta și a transfera informații secrete către proprietarul lor sau pur și simplu pentru a dăuna sistemului de securitate și performanței computerului victimei. Principiile de funcționare ale acestor programe sunt diferite, așa că nu le vom lua în considerare în această prezentare.

Inteligența rețelei

- În timpul unui astfel de atac, hackerul nu efectuează de fapt nicio acțiune distructivă, dar, ca urmare, poate obține informații confidențiale despre construcția și principiile de funcționare a sistemului informatic al victimei. Informațiile obținute pot fi folosite pentru a construi în mod competent atacul viitor și se face de obicei în etapele pregătitoare.

Sniffing pachetelor

Este, de asemenea, un tip de atac destul de comun bazat pe funcționarea unei plăci de rețea în modul promiscuu. În acest mod, toate pachetele primite de placa de rețea sunt trimise pentru procesare către o aplicație specială pentru procesare.

Drept urmare, un atacator poate obține o cantitate mare de informații de serviciu: cine a trimis pachete de unde până unde, prin ce adrese au trecut aceste pachete.

IP-spufing

De asemenea, un tip obișnuit de atac în rețelele insuficient de sigure, atunci când un atacator își uzurpă identitatea unui utilizator autorizat, în timp ce se află în cadrul organizației în sine, sau în afara acesteia.

Pentru a face acest lucru, hackerul trebuie să folosească o adresă IP care este permisă în sistemul de securitate al rețelei.

Un astfel de atac este posibil dacă sistemul de securitate permite identificarea utilizatorului doar prin adresa IP și nu necesită confirmări suplimentare.

Man-in-the-Middle

Din engleza. "Bărbatul din mijloc" Un tip de atac când un atacator interceptează canalul de comunicație între două sisteme și obține acces la toate informațiile transmise. Obținând acces la acest nivel, un hacker poate modifica informațiile în modul în care dorește să-și atingă obiectivele.

Scopul unui astfel de atac este de a fura sau de a falsifica informațiile transmise sau de a obține acces la resursele rețelei.

Injecție

- Un atac de injecție implică introducerea unor comenzi sau date terță parte într-un sistem care rulează pentru a schimba cursul sistemului și, ca urmare, a obține acces la funcții și informații închise sau pentru a destabiliza sistemul în ansamblu. Un astfel de atac este cel mai popular pe Internet, dar poate fi efectuat și prin linia de comandă a sistemului.

SQL-injectia

- Injecția SQL este un atac în care parametrii interogărilor SQL către baza de date sunt modificați. Ca urmare, cererea capătă un sens complet diferit și este capabilă nu numai să afișeze informații confidențiale, ci și să modifice / șterge date. Foarte des, acest tip de atac poate fi văzut pe exemplul site-urilor care utilizează parametrii de linie de comandă (în acest caz, variabile URL) pentru a construi interogări SQL împotriva bazelor de date fără o validare adecvată.

Injecția PHP

Injecția PHP este o modalitate de a pirata site-urile care rulează pe PHP. Constă în executarea codului necesar pe partea de server a site-ului.

Cross Site Scripting sau XSS (abreviar din engleză Cross Site Scripting) este un atac similar cu injecția SQL, dar pentru a efectua acest atac, un hacker nu modifică interogarea SQL, ci variabilele interne ale sistemului de operare (de exemplu, PHP, Perl etc. .d.), folosind deficiențe în procesarea parametrilor de intrare a scripturilor sau erori în configurarea aplicațiilor de procesare a scripturilor.

Inginerie sociala

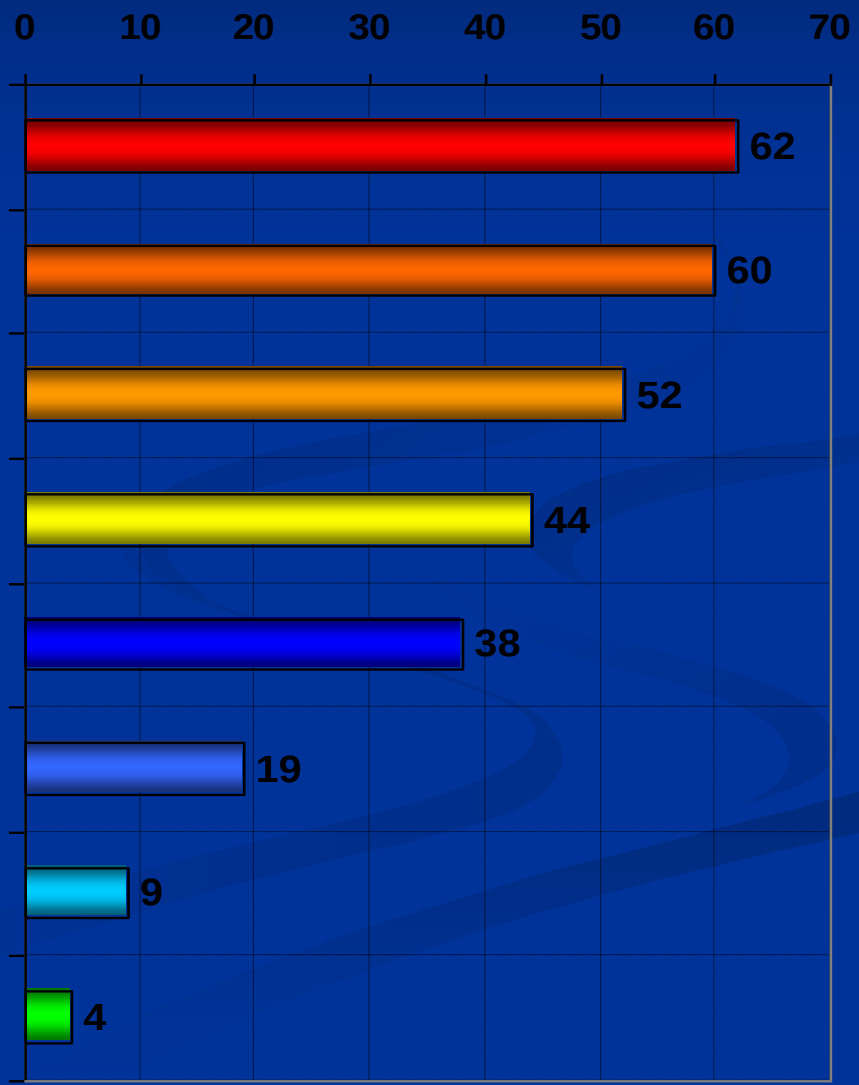
Ingineria socială (din engleză Social Engineering) este utilizarea incompetenței sau neglijenței personalului pentru a obține acces la informații. Această metodă este de obicei folosită fără computer, folosind un telefon obișnuit, poștă sau un pahar de bere.

În acest fel, se obține de obicei o mare varietate de informații. În cursul unui astfel de atac, hackerul stabilește contactul cu victima și, inducând în eroare sau câștigând încredere, încearcă să obțină informațiile necesare care sunt greu de obținut în alt mod, sau alte moduri care sunt mai riscante.

După cum spune vechea vorbă: „Cea mai slabă verigă dintr-un sistem de securitate este Omul”.

Cele mai periculoase amenințări IT

- Acțiuni din interior
- Programe malware
- Atacurile hackerilor
- Neglijența angajaților
- Spam
- Eșecuri hardware și software
- Furtul de echipamente
- Fraudă financiară



Principalele 8 amenințări de securitate cibernetică în 2022

Conform raportului Categorii de amenințări 2022 al Agenției UE pentru securitate cibernetică (Enisa), există opt tipuri de amenințări principale:

Ransomware: atacatorii criptează datele unei organizații și cer o răscumpărare pentru a reda accesul

Malware – un software care afectează un sistem

Inginerie socială: exploatarea erorilor umane pentru a obține acces la informații sau servicii

Amenințări la adresa datelor: vizarea surselor de date pentru acces neautorizat și scurgeri de date

Amenințări la adresa disponibilității: atacuri care blochează accesul la date și servicii (DoS)

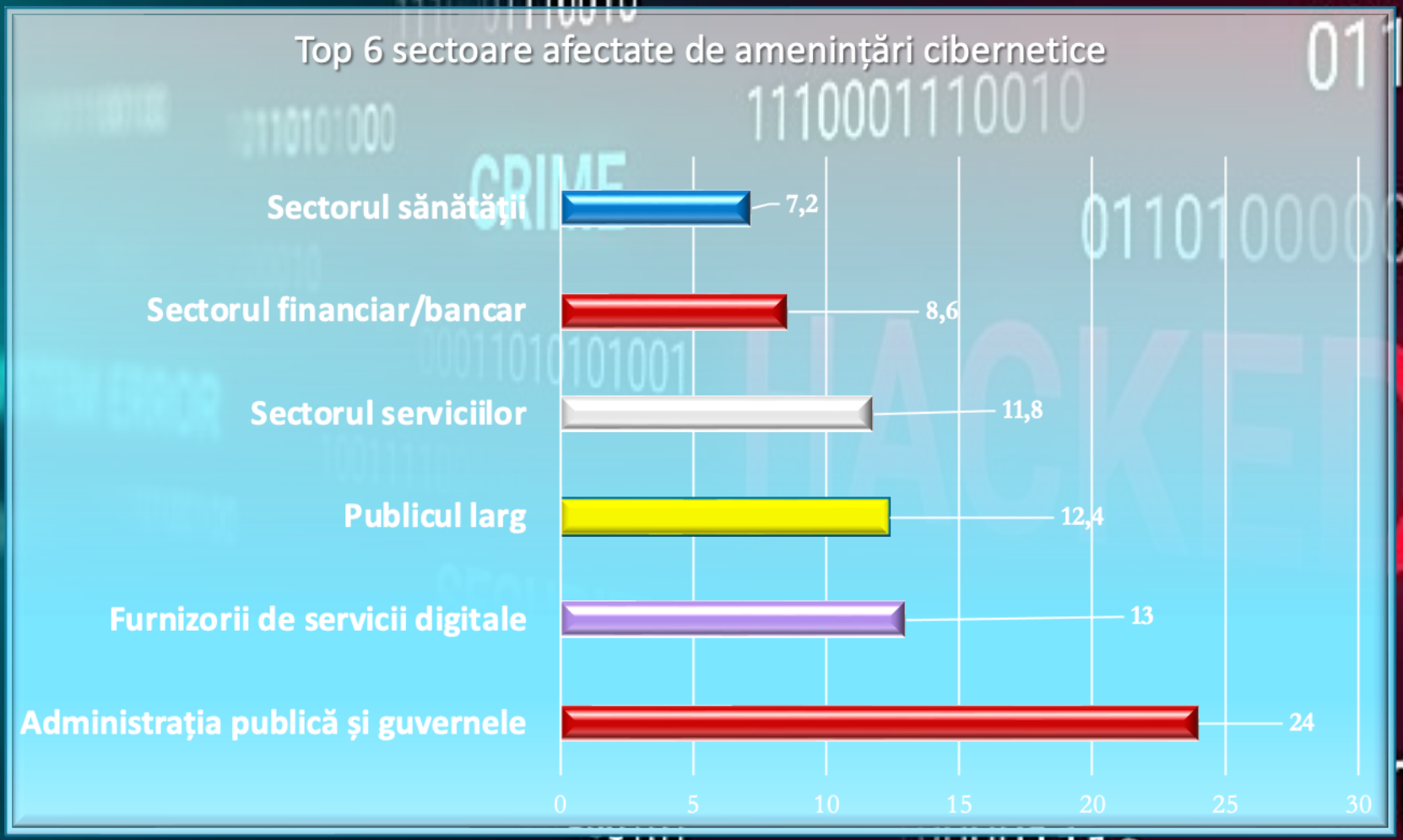
Dezinformare – distribuirea de informații înșelătoare

Amenințări pe lanțul de aprovizionare: vizează relația dintre organizații și furnizorii de servicii

Amenințări la adresa disponibilității - amenințări care împiedică accesul la internet

Top 6 sectoare afectate de amenințări cibernetice

Amenințările la adresa securității cibernetice în Uniunea Europeană afectează sectoare vitale pentru societate. Primele șase sectoare cele mai afectate între iunie 2021 și iunie 2022, conform Agenției europene pentru securitate cibernetică (Enisa)



Infograficul publicat de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) evidențiază principalele amenințări la adresa securității cibernetice care ar putea apărea până în 2030.

Concluzii

- Orice atac nu este altceva decât o încercare de a folosi imperfecțiunea sistemului de securitate al victimei fie pentru a obține informații, fie pentru a dăuna sistemului, de aceea motivul oricărui atac de succes este profesionalismul hackerului și valoarea informațiilor, precum și competența insuficientă a administratorului sistemului de securitate, în special software-ul imperfecțiunii și atenția insuficientă la problemele de securitate din companie în principiu.

Sarcini de autoevaluare

- Prezentarea unei infortmații analitice privind prevenirea și curmarea fraudelor informatice;
- Determinați instrumentele şi metodele de luptă cu amenințările cibernetice;
- Evaluați motivele criminalității cibernetice;
- Descrieți eforturile întreprinse pentru asigurarea securităţii informațiilor şi de securitate națională, în general.

Teme pentru lucru individual

- Riscurile securității informaționale în organizații. Metode de contracarare.
- Infracțiuni pe Internet: hârțuirea electronică
- Considerațiuni privind protecția drepturilor de proprietate intelectuala pe Internet
- Politica și strategia de stat în domeniul informațional în contextul Integrării Europene a Republicii Moldova
- Ingineria socială: metode de manipulare și tehnici de protecție.
- Inteligența artificială și fraudele informatice: risc sau oportunitate.