I.P. "Serviciul Tehnologia Informației și Securitate Cibernetică"

Riscuri de securitate

Cele mai frecvente amenințări cibernetice ale anului 2019

INTRODUCERE

Amenințările cibernetice din mediul online sunt în continuă creștere. Spațiul cibernetic va fi mereu animat de cursa continuă dintre atacatori și cei care sunt afectați de aceste atacuri. Din nefericire, așa cum precizează ENISA, în acest moment infractorii cibernetici sunt cu un pas înainte.

Pentru a ține pasul cu aceștia, este esențial ca utilizatorul să fie informat corespunzător cu privire la metodele de atac cele mai des folosite. Conștientizarea în domeniul securității este o parte esențială în formarea angajaților și este cel mai eficient mod de a securiza companiile față de intruși și hackeri. Astfel, deducem că confidențialitatea informației este vitală pentru fiecare organizație.

Prezentul document conține informații cu privire la principalele amenințări din spațiul cibernetic și are drept scop dezvoltarea culturii cibernetice a angajaților.

ESENȚIAL

O instituție modernă are nevoie de angajați informați care înțeleg riscurile de bază a securității.

E-MAIL

Înțelegerea phishingului, atașamentelor răufăctoare și utilizarea email-ului.

INTERNET

Navigarea în siguranță și intelegerea http sau https,
site-uri de phishing și amenințări ordinare.

LA BIROU

Cum să gestionezi în siguranță conținutul confidențial, tipărit sau digital, și căile corecte de a le depozita și de a le elimina.

ÎN AFARA OFICIULUI

Conștientizarea riscului atunci când se lucrează de acasă folosind un laptop sau un telefon.

CONSTIENTIZARE SOCIALĂ

Conștientizarea riscurile și modul în care ingineria socială funcționează sunt esențiale pentru a securiza accesul la locul de muncă și date.

CONFIDENȚIALITATE

Odată cu intensificarea regulilor de securitate a datelor personale, orice greșeală poate duce la consecințe grave.

TELEFON MOBIL

Telefoanele mobile de astăzi sunt mici computere care pot conține informație importantă.

#1 Ransomware

Ransomware este un program malware sau un virus care criptează datele de pe computer sau în unele cazuri întreaga rețea. Nu puteți accesa fișierele sau imaginile până când nu veți plăti răscumpărare. Paraziţii ransomware normali sunt foarte periculoşi. Astfel de ameninţări pot cauza foarte multe probleme în calculatorul dumneavoastră, deoarece ele pot face ca informaţiile vitale să devină inaccesibile, pot încerca să vă fure datele valoroase şi îmtr-un final să distrugă întregul sistem.

Viruşii ransomware sunt capabili să cripteze datele sensitive ale utilizatorilor, precum documente de afaceri, video-uri, imagini şi alte fişiere. Imediat după ce fac acest lucru, încep să ceară o recompensă pentru decriptarea datelor criptate.

Este recomandat să Nu plătiţi recompensa cerută de către această ameninţare deoarece nu va ajuta la eliminarea parazitului şi la recuperarea datelor afectate.

#2 Phishing

Phishing-ul este practica frauduloasă de a trimite e-mailuri care pretind că provin de la companii cu renume cu scopul de a determina persoanele să dezvăluie informații personale, cum ar fi parole și coduri de la cărțile de credit.
De multe ori, subiectul mesajului va fi unul conceput în așa fel încât să atragă atenția (ex: “Mesaj important – Actualizarea datelor personale”).

Tendințele de atac de phishing pentru anul 2019 sunt următoarele:

- **Criptare HTTPS** - unele site-uri de phishing au început utilizând criptarea HTTPS. De fapt, de la sfârșitul anului 2016, a avut loc o creștere de aproape 900% a acestui tip de atac.
- **Phishing prin telefon mobil** - Examinați o creștere a phishingului mobil. Mai exact, prin mesaje text (SMS) trimise clienților, unde conținutul este vizibil numai pe un dispozitiv mobil.
- **Noi furnizori de gazduire** - Hackerii folosesc noi furnizori de gazduire pentru a determina care gazduieste paginile lor pentru mai mult timp.
- **Foldere abundente** - Pentru a crește timpul în care pagina este activă, infractorii vor folosi de asemenea numeroase dosare care conțin pagini de phishing.

3 Vishing

Vishing este echivalentul telefonic al phishingului. Este descris ca fiind un act de utilizare a telefonului în încercarea de a înșela utilizatorul să renunțe la informația privată care va fi ulterior folosită pentru furtul de identitate. Mai mult, interlocutorul va juca rolul unei entități/instituții de încredere, precum bănci, companii de telecomunicații, etc. Atacatorii atribuie conversației o aură de urgență, la fel ca în cazurile de phishing: conturi blocate, plăți suspicioase, sisteme nesigure, livrare de colete, probleme legate de conturile bancare, accidente, etc.

Totodată, atacatorii pot profita de credulitatea victimelor, pentru a îi convinge să instaleze software malițios sau aplicații de control la distanță (remote desktop), pe dispozitivele utilizate.

Metode de vishing;

- Frauda cu apeluri pierdute
- Frauda „cont bancar blocat”
- Apelurile false de suport

Rețele locale de comunicație

Rețea necunoscută

Este foarte ușor pentru un hacker să instaleze un punct de acces Wi-Fi, dacă vă conectați la o rețea necunoscută. În acest caz o mare parte din comunicarea dvs. poate fi monitorizată sau chiar manipulată.

WiFi gratuit

Oamenii folosesc de obicei WiFi gratuit fără să se gândească. Unul dintre cele mai frecvente atacuri WiFi deschise este numit atacul Man-in-Middle (MitM), unde un hacker poate monitoriza tot traficul și obține informații sensibile.

Rețelele WiFi de domiciliu

Rețelele de domiciliu sunt adesea configurate într-o grabă pentru a obține conectivitate cât mai curând posibil.

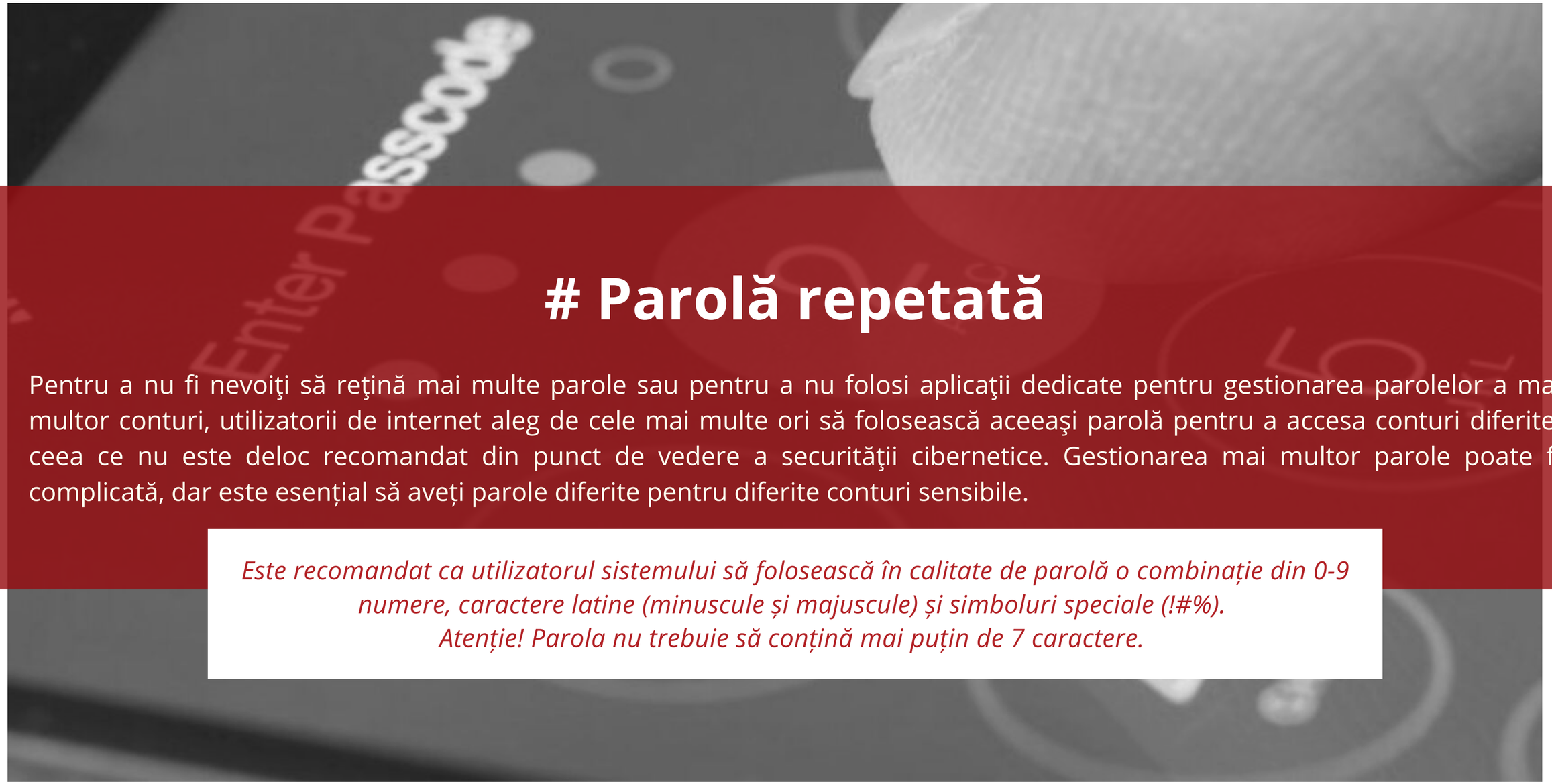
Atașamente rău-intenționate

Atașamentele de e-mail

CAZURI TIPICE DE E-MAILURI NESOLICITATE CU ATAȘAMENTE PERICULOASE:

- Ați câștigat o recompensă sau o loterie și trebuie să completați formularul atașat;
- Comanda dvs. a fost anulată sau ați primit o comandă nouă;
- Email care discută despre anumite facturi;
- Lucrați de acasă și câștigați bani;
- Scrisoare de la o bancă, PayPal etc. vă cere să introduceți datele în funcție de atașament, altfel contul va fi blocat etc.

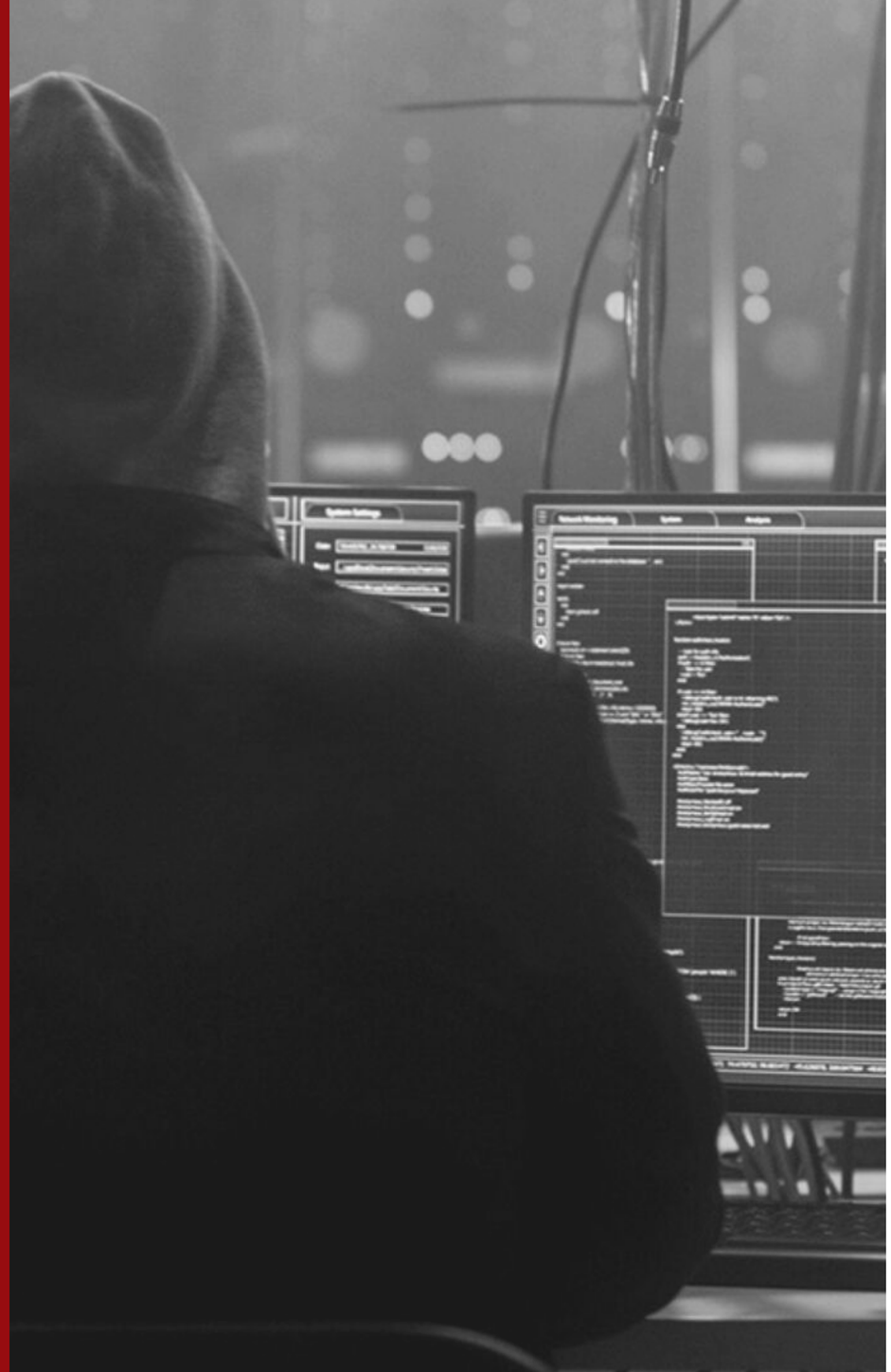
NOTĂ: *Dacă utilizați un software antivirus, efectiv, fișierul rău intenționat poate fi pus automat în carantină atunci când este descărcat pe computer.*



Parolă repetată

Pentru a nu fi nevoiţi să reţină mai multe parole sau pentru a nu folosi aplicaţii dedicate pentru gestionarea parolelor a mai multor conturi, utilizatorii de internet aleg de cele mai multe ori să folosească aceeaşi parolă pentru a accesa conturi diferite, ceea ce nu este deloc recomandat din punct de vedere a securităţii cibernetice. Gestionarea mai multor parole poate fi complicată, dar este esențial să aveți parole diferite pentru diferite conturi sensibile.

Este recomandat ca utilizatorul sistemului să folosească în calitate de parolă o combinație din 0-9 numere, caractere latine (minuscule și majuscule) și simboluri speciale (!#%).
Atenție! Parola nu trebuie să conțină mai puțin de 7 caractere.



Programe malițioase

SPYWARE

Spyware și malware sunt tipuri de programe care permit unui hacker să obțină informații ascunse despre activitățile computerului altei persoane, prin transmiterea datelor de pe computer sau prin accesarea directă a acestuia. Acestea sunt folosite pentru a urmări oamenii şi pentru a înregistra cele mai vizitate website-uri precum şi acţiunile luate atunci când au fost vizitate.

ESCROCHERIA CEO

Escrocheria CEO-ului este atunci când un hacker își asumă identitatea executivului pentru a induce în eroare angajații să trimită informații sensibile. Aceasta include folosirea ingineriei sociale pentru a manipula oamenii și acțiunile lor.

Riscuri de Securitate

Telefon Deblocat

Documentele, notițele, e-mailurile și contactele pot fi furate dacă lăsați telefonul deblocat. Este important să protejați informația. Păstrați întotdeauna telefonul blocat atunci când nu îl utilizați.

Calculator Nesupravegheat

Lăsând computerul deblocat și nesupravegheat poate provoca probleme grave dacă o altă persoană are acces la el.

USB neidentificat

O amenințare cu USB este atunci când un hacker lasă un stick USB într-un spațiu deschis, sperând că cineva îl va conecta la computer. Astfel, hackerul va putea accesa computerul și toate fișierele din rețea.

STUDIILE ARATĂ CĂ

91%

din încălcări se bazează pe erori umane. Securitatea cibernetică are legătură cu oamenii.

Ce putem face?

INSTRUIRI

Instituțiile trebuie să creeze și să dezvolte o cultură de securitate cu instruiri regulate a tuturor angajaților.

MONITORIZĂRI

Monitorizarea permanentă a activităților derulate prin sistemele informatice este esențială, pentru că permite reducerea timpului de reacție în fața potențialelor amenințări de securitate.

ACTUALIZĂRI

Actualizarea tuturor soluțiilor software instalate și utilizate pe sistemele informatice, folosind cele mai recente pachete, puse la dispoziția utilizatorilor de furnizori autorizați.

COPII DE REZERVĂ

Crearea unor copii de rezervă pentru informațiile necesare permite ca recuperarea să se poată face eficient și complet, într-un timp rezonabil, limitând eventualele daune.

Raportează un incident

CERT-GOV-MD este punctul central de raportare şi coordonare privind incidentele de securitate în sistemele de comunicaţii şi informatice, aflate în administrarea Serviciului Tehnologia Informației și Securitate Cibernetică.

incidents@cert.gov.md

+373 22 820 921