GHID

Cum să te ferești de viruși, viermi și troieni

Ghid realizat de către:

Bitdefender

în cadrul campaniei de conștientizare a riscurilor de securitate cibernetică derulată în Romania sub egida ECSM de către CERT-RO.

Pagină albă

CUPRINS

Scopul prezentului document este de a familiariza cititorii cu noțiunile de bază privind tipurile de amenințări informatice, precum și de a propune o serie de practici menite să protejeze sistemul și datele personale, în timpul navigării pe internet.

1. Cele mai întâlnite tipuri de amenințări informatice

- **Viruși:** virușii informatici sunt programe care se autocopiază pe sistemul compromis, fără știrea utilizatorului. Virusul va infecta astfel componente ale sistemului de operare sau alte programe informatice.
- **Viermi:** programe care se pot auto-replica. Acestea folosesc rețeaua de calculatoare pentru a-și trimite propriile copii în alte noduri (calculatoare din rețea), reușind să facă acest lucru fără intervenția vreunui utilizator. Spre deosebire de un virus informatic, un vierme informatic nu are nevoie să fie atașat la un program existent. Viermii provoacă daune rețelei, chiar și prin simplul fapt că ocupă bandă, în timp ce virușii corup sau modifică aproape întotdeauna fișiere de pe computerul țintă.
- **Troieni:** aceste programe se prezintă sub forma unor programe legitime, care, în realitate, sunt create cu scopul de a fura date confidențiale, sau de a permite unor utilizatori sau programe neautorizate accesul la sistemul infectat.
- **Spyware:** o categorie de software malițios, ataşate de obicei la programe gratuite (jocuri, programe de schimbat fișiere, programe de video chat etc.), care captează pe ascuns date de marketing (prin analiza site-urilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ș.a.m.d.) și le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.
- **Adware:** orice program care afișează reclame la rularea acestuia, reclame care pot fi afișate ca bannere în fereastra programului, sau de tip pop-up (care deschide ferestre noi cu reclame, deasupra tuturor ferestrelor). Unele programe adware pot fi considerate o formă de spyware care nu colectează date de marketing, ci doar transmit reclame.

- **Rootkit:** un rootkit este o colecţie de utilitare proiectate să menţină controlul sau accesul la calculator. Dupa instalare, rootkit-ul utilizează funcţii ale sistemului de operare pentru a se “ascunde” astfel încât să rămână nedetectat. Rootkit-urile au fost utilizate mai întâi în Unix, dar sunt folosite în prezent şi în Linux, Windows şi alte sisteme de operare. Acestea pot fi folosite în scopuri legale, dar sunt cunoscute în general pentru utilizarea lor în scopuri maliţioase.
- **Spam:** mesaje electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse și servicii dubioase, folosite de industria e-marketingului și de proprietarii de site-uri cu un conținut indecent. Mesajele spam sunt trimise cu ajutorul unor calculatoare infectate cu troieni, care fac parte dintr-un botnet (o rețea de calculatoare compromise utilizate pentru trimiterea de spam sau atacuri asupra unor site-uri de internet, fără știrea posesorilor calculatoarelor respective). Mesajele spam, deși nu sunt un program maliții în sine, pot include atașamente care conțin astfel de programe, sau trimit utilizatorii către pagini de internet periculoase pentru siguranța sistemului.
- **Hacker:** o persoană care pătrunde în calculatoare (fără acordul proprietarului), de obicei prin accesarea controalelor administrative.

Auxiliar amenințărilor reprezentate de programe create cu scopul compromiterii siguranței sistemului, dorim să atragem atenția asupra tehnicilor de manipulare socială, cele mai des utilizate fiind practicile de **phishing** și **scam**, ce urmăresc manipularea utilizatorilor astfel încât aceștia să furnizeze de bunăvoie informații importante, precum sunt datele bancare.

2. Reguli generale de securitate

Pentru a asigura integritatea calculatorului și a datelor personale, vă recomandăm respectarea următoarelor reguli:

- Instalați o soluție de securitate ce oferă cel puțin protecție la nivel antimalware, antispam și antiphishing
- Aveți în vedere ca soluția de securitate instalată să fie permanent actualizată
- Nu deschideți atașamente și nu accesați link-urile ce vin din partea unor expeditori necunoscuți. Dacă este absolut necesară deschiderea unui atașament, se recomandă ca acesta să fie descărcat și scanat cu soluția antivirus instalată pe calculator
- Nu deschideți atașamentele și nu dați click pe link-urile din mesajele spam
- Nu folosiți niciodată calculatoare publice pentru a efectua tranzacții bancare, sau pentru alte tipuri de achiziții online. Aceste calculatoare ar putea conține programe care înregistrează datele personale, precum troienii bancari
- Evitați să faceți shopping online atunci când sunteți conectați la un hotspot Wi-Fi public, precum cele din aeroporturi, cafenele sau mall-uri. De obicei, informațiile schimbate între dumneavoastră și magazinul online, nu sunt criptate, și pot fi interceptate ușor de către un atacator
- În cazul în care vă conectați la hotspot-uri publice nesecurizate, utilizați o aplicație firewall care să filtreze accesul din exterior
- Dezactivați funcția ”Network Share” înainte de a vă conecta la un hotspot public
- Atunci când doriți să achiziționați software online, introduceți adresa de internet manual în bara de adresă a browserului. Este de preferat să utilizați calculatorul

personal, sau unul care nu este utilizat in mod public de către alți utilizatori, iar conexiunea la internet ar trebui sa fie sigură (rețeaua de acasă sau un modem 3G)

- Verificați în mod repetat pagina de internet a furnizorului dumneavoastră de internet și instalați toate patch-urile puse de către aceștia la dispoziție
- Evitați să accesați link-uri care sunt marcate drept periculoase de către soluția de securitate instalată pe sistem, sau de către browser-ul de internet. Dacă primiți orice mesaj de atenționare în timpul navigării pe o pagină, ieșiți imediat de pe respectiva pagină de internet

- Nu instalați software din locații despre care nu sunteți sigur, mai ales software care pare să fie codec. În schimb, accesați pagina producătorului pentru a descărca acest tip de program.

- Nu vă lăsați amăgiți de probleme privind cardul de credit, sau invitații diverse care provin din partea unor surse necunoscute. Atunci când găsiți astfel de mesaje în inbox, luați legătura cu banca (sau mergeți personal la bancă) pentru a vă asigura ca totul este în regulă referitor la contul dumneavoastră.

- Nu trimiteți niciodată parolele dumneavoastră de cont prin e-mail sau prin atașamente. Nici un furnizor de servicii nu ar trebui să solicite astfel de informații, având în vedere că ar trebui să le aibă deja.
- Este greu de imaginat că o agenție guvernamentală v-ar contacta prin internet pentru a colecta o amendă, așadar, tratați astfel de mesaje cu suspiciune și sub nici o forma nu accesați link-urile sau atașamentele conținute de mesajul respectiv.
- În această situație, chiar și existența unei soluții de securitate eficiente, factorul uman joacă un rol decisiv. Ingineria socială poate ajuta un hacker sau un program să stabilească o conexiune cu utilizatorul, și convingerea acestuia în a oferi date critice sau bani. Așadar, atunci când doriți să cumpărați online bilete de orice fel, asigurați-vă că este un site pe care îl cunoașteți dinainte, și, alternativ, verificați cât mai multe comentarii ale utilizatorilor despre serviciile respectivului website. De asemenea încercați să contactați un reprezentant al companiei, care să vă ofere cât mai multe informații posibil.

3. Reguli de securitate în cadrul rețelelor sociale

- Alegeți o parolă pentru contul dumneavoastră care să nu fie ușor de ghicit de către un alt utilizator sau program. În acest sens, evitați parolele generice, precum ”123456789” sau ”parola” sau o parolă identică cu numele de utilizator;
- Asigurați-vă că știți pe cine urmăriți și pe cine adăugați drept prieten
- Evitați să accesați link-urile împărtășite de către alți utilizatori;
- Evitați să faceți publice informații personale, precum ziua de naștere, adresa de e-mail sau adresa fizică;
- Atunci când împărtășiți poze, asigurați-vă că o faceți doar cu persoanele cunoscute
- Nu dezvăluiți niciodată informații referitoare la perioadele în care părăsiți locuința (mesaje precum: ”plec la mare tot weekend-ul; ”sunt singur acasă” trebuie evitate)
- Utilizați o soluție de securitate specializată, care să scaneze mesajele și comentariile, și care să verifice nivelul de securitate al informațiilor confidențiale;

4. Reguli de securitate privind configurarea rețelei wireless personale

- Majoritatea routerelor vin predefinite cu un nume de utilizator și o parolă generică, care sunt disponibile public, pe pagina producătorului. După achiziția unui astfel de echipament, alegeți un alt nume de utilizator și o altă parolă, astfel încât să evitați posibilitatea ca un intrus să vă modifice setările, sau să se folosească de rețeaua dumneavoastră pentru a-și ascunde identitatea în cadrul unor activități pe internet;
- Dezactivați funcția de acces la distanță (remote access) a routerului, având în vedere că această funcție este utilă doar administratorilor rețelelor unor companii
- În cazul în care echipamentul nu permite accesul strict pentru unele adrese IP predefinite, este recomandat să dezactivați interfața de administrare la distanță;
- Setați o cheie de securitate sub protocolul WPA / WPA2 (Wi-Fi Protected Access), sau, daca nu este posibil, WEP (Wired Equivalent Privacy);
- Setați politici de acces MAC (Media Access Control), care să filtreze dispozitivele care au acces la rețea, în baza identificatorului MAC;
- Opriți difuzarea SSID: routerele își difuzează numele pentru a fi ușor detectabile de către utilizatori. Astfel, ele sunt ușor detectabile și de către un posibil atacator. Dezactivarea acestei funcții va face ca routerul (împreună cu toate dispozitivele conectate la el) să devină invizibile;
- Micșorați puterea de transmisie a routerului, astfel încât raza de transmisie să acopere strict suprafața locuinței, evitând astfel posibilitatea ca un utilizator nepermis să încerce forțarea accesului în rețea, în timp ce este situat în apropierea locuinței. Întrucât micșorarea puterii de emisie va afecta și viteza de transfer, utilizatorul trebuie să descopere raportul optim dintre puterea de transmisie și viteză. De asemenea, în cazul routerelor ce nu dispun de astfel de opțiuni, micșorarea puterii poate fi realizată prin simpla scoatere a antenei (sau a uneia dintre antene, în cazul în care dispozitivul este dotat cu mai multe);
- Plasați echipamentul în centrul locuinței, pentru a acoperi uniform spațiul acesteia, și în nici un caz nu plasați routerul lângă o fereastră, de unde ar putea fi accesat de către persoane străine;

5. Reguli de securitate privind folosirea calculatorului familiei

Dacă aveți un calculator pe care îl partajați cu familia, asigurați-vă că respectați câteva reguli de bază pentru a vă proteja pe dumneavoastră, afacerea dumneavoastră și pe cei dragi.

- În cazul în care aveți copii care au voie să folosească calculatorul familiei, nu le oferiți privilegii de administrator asupra respectivului computer, ci creați-le un cont limitat. Acest lucru îi va împiedica să instaleze aplicații potențial periculoase (cum ar fi keylogger-e sau viruși) și de asemenea, îi va împiedica să modifice setările de control parental pe care le impuneți dumneavoastră;
- Chiar dacă respectați aceste prevederi, nu folosiți niciodată calculatorul familiei pentru chestiuni legate de serviciu sau pentru operațiunii critice, precum e-banking-ul sau plata facturilor. Mediile multi-utilizator sunt periculoase deoarece pot ascunde amenințări plantate voluntar sau involuntar de ceilalți utilizatori;
- Instalați o soluție antivirus cu control parental, filtru de conținut și filtru pentru rețelele sociale. Dată fiind ponderea conținutului pornografic și a violenței on-line, e de datoria dumneavoastră să vă păstrați copilul în siguranță;
- Așezați calculatorul întrun loc vizibil din casă, în care să puteți supraveghea vizual felul în care copilul interacționează cu alți user-i pe Internet;
- Educați ceilalți membri ai familiei asupra riscurilor folosirii de aplicații piratate. Acest lucru nu este doar ilegal, ci poate duce la probleme serioase privind integritatea și securitatea calculatorului. Copiii sunt în mod special atrași de conținutul piratat deoarece nu au un buget pentru aplicații plătite și nu sesizează faptul că descărcarea și instalarea unei aplicații poate fi considerată o infracțiune.

6. Reguli de folosire a telefoanelor inteligente (smartphones)

Smartphone-urile joacă un rol esențial în felul în care comunicăm și ținem legătura cu cei dragi. Securitatea acestor dispozitive este, de multe ori, trecută în afara priorităților, deoarece utilizatorii percep aceste dispozitive ca pe niște simple telefoane, și nu ca pe mini-calculatoare ce sunt.

- Când folosiți rețelele sociale, asigurați-vă că fotografiile făcute cu smartphone-ul și pe care doriți să le încărcați pentru a le partaja cu prietenii, nu conțin informații legate de poziția dumneavoastră actuală. Partajarea locației e ideala pentru întâlnirile cu amicii în locuri publice, dar în același timp, permit persoanelor rău-intenționate să vă monitorizeze obiceiurile și rutina zilnice facilitând tentativele de hărțuire;
- Sincronizați-vă telefonul cu un calculator personal. În cazul în care pierdeți smartphone-ul sau acesta este furat, veți avea o copie de siguranță a contactelor, mesajelor, imaginilor și documentelor de pe acesta;
- Folosiți o soluție de securitate pentru telefoane mobile care să aibă un modul antifurt, în mod special dacă folosiți un telefon care rulează Android. Din cauza cotei de piață ridicate, telefoanele bazate pe Android au devenit ținta predilectă a infractorilor informatici. O soluție antivirus vă permite să filtrați aplicațiile potențial periculoase și să le blocheze înainte ca acestea să cauzeze modificări asupra sistemului. În cazul în care pierdeți telefonul sau vă este furat, modulul de antifurt vă poate ajuta să identificați și să recuperați telefonul, chiar dacă acesta nu are acces la Internet. În cazul în care recuperarea este imposibilă, puteți bloca definitiv accesul la telefon și la datele acestuia și, întrun final, să ștergeți toate informațiile dumneavoastră de pe acesta printr-un simplu SMS;
- Nu uitați că telefonul dumneavoastră este de fapt un mini-calculator personal, care poate fi infectat prin simpla vizitare a unui website sau prin accesarea unui link dintr-un mesaj. Înainte de a accesa un link, asigurați-vă că site-ul pe care doriți să-l vizitați e de încredere. Dacă nu aveți informații despre site sau dacă nu recunoașteți link-ul, cel mai bine este să evitați accesarea acestuia;
- Aveți mare grijă la ce fotografiați. Puteți fi tentat să fotografiați și să procesați coduri QR (coduri de bare care stochează informații despre diverse produse sau linkuri către website-uri). Dacă fotografierea și procesarea codurilor QR de pe ambalajele produselor nu sunt, de obicei, periculoase, puteți găsi coduri QR lipite în locuri publice sau chiar desenate pe elemente de mobilier stradal, ziduri etc. Aceste coduri pot conține URL-uri către website-uri care să exploateze vulnerabilități din telefonul dumneavoastră care să se finalizeze cu o infecție.

7. Reguli de folosire a propriilor dispozitive la muncă

Majoritatea companiilor permit angajaților introducerea propriilor dispozitive mobile in sediu si folosirea acestora în scopuri de business. Pentru securitatea dumneavoastră și a rețelei companiei în care lucrați, vă sfătuim să urmați aceste reguli:

- Informați departamentul IT de faptul că aveți un dispozitiv personal pe care doriți să-l folosiți la serviciu. Echipa IT vă va introduce dispozitivul în rețeaua companiei și vă va informa asupra regulilor de utilizare și întreținere a echipamentului în interiorul companiei;
- Anunțați de urgență pierderea unui dispozitiv mobil pe care aveți date care aparțin companiei. Acest lucru este esențial pentru limitarea accesului unei persoane neautorizate la aceste informații. În cazul pierderii, echipa IT vă va arăta cum să vă ștergeți de la distanță conținutul telefonului;
- Nu uitați că un telefon mobil e și un dispozitiv de stocare portabil. Scanați conținutul memoriei interne și externe a telefonului la fiecare introducere în calculatorul de la serviciu și în cel de acasă. In acest fel, nu veti transfera viruși de la serviciu acasă și viceversa;
- Din același motiv, nu introduceți nici un dispozitiv de stocare găsit (de exemplu, pen-drive, CD/DVD-ROM, card SD) în calculatoarele companiei. Majoritatea atacurilor asupra rețelei companiilor încep cu un astfel de dispozitiv “uitat” de atacator în lift, în parcare sau în locuri din companie în care e permis accesul personalului de întreținere sau a publicului (recepții, spații de aprovizionare etc).

8. Mic ghid de securitate a datelor pentru companii mici si mijlocii

În ultimele luni am asistat la o avalanșă de atacuri împotriva unor companii cu mare vizibilitate în peisajul de afaceri International, precum Google, Facebook, Twitter și Ubisoft, dar și asupra unor instituții de stat printre care NASA sau FBI cu rezultate îngrijorătoare la nivel de securitate a datelor și reputație.

Cu toate că atacurile cu malware s-au dovedit cele mai costisitoare pentru companii, aproximativ 70% din totalul breșelor de securitate sunt rezultatul erorilor umane și a diverselor probleme de sistem și implementare la nivel IT.

Iar miza este mare dacă ne gândim că pe lângă datele companiei, informațiile private ale clienților, colaboratorilor sau partenerilor de afaceri pot fi expuse pe net și ulterior folosite în alte atacuri complexe împotriva țintelor vizate.

Companiile, fie ele mari, mici sau mijlocii trebuie să știe că aceste pericole pot fi evitate sau controlate daca țin seama de câteva reguli simple, dar esențiale, de securitate.

- **Evaluarea datelor pe care le deții**. Este important să știți exact și din timp ce anume puteți pierde în cazul unei breșe de securitate. Ce fel de informații dețineți, daca sunt sau nu confidențiale, cât sunt de importante pentru companie, clienți sau angajați și care sunt riscurile de a pierde controlul acestor date. Odata ce știți ce protejați, veți ști și cum să protejați
- **Nu vă limitați la o singură măsură sau produs de protejare a datelor.** Este capital să folosiți diferite metode de securitate. În caz că unul nu dă rezultate sau se dovedește a fi vulnerabil, rămân celelalte
- **Limitarea accesului fizic în spațiul** de muncă în cazul tuturor persoanelor neautorizate. Cineva poate sustrage din clădire un server, un laptop sau un hard-disk cu date importante. Informațiile secrete pot fi stocate în diferite locații și protejate printr-un sistem de access care să limiteze la minim numărul persoanelor autorizate în spațiile dedicate
- **Configurarea arhitecturii rețelei** trebuie făcută în așa fel încât să se poată interveni rapid pentru a se izola o infecție, să spunem, la nivelul unei singure subrețele, prevenind astfel răspândirea infecției în toată rețeaua departamentului sau a companiei. Acest lucru minimizează impactul pe care l-ar putea avea un atac care a

reușit să penetreze prima linie defensivă. Un firewall bine configurat poate face minuni. Asigurați-vă că cine vă configurează firewall-ul știe ce face

- **Punctele de access (Hot spots) neautorizate trebuie interzise** cu desăvârșire în cadrul rețelei companiei, iar un dispozitiv care se conectează la WI-FI-ul autorizat de companie trebuie să permită doar autentificarea bazată pe datele de conectare din domeniu sau cu certificate digitale
- **Accessul trebuie restricționat** în cazul persoanelor care intră în contact cu resursele companiei cu un username și o parolă proprii care să fie schimbate cu regularitate și să aibă un grad ridicat de dificultate. În clipa în care un angajat sau un colaborator și-a încheiat activitatea în companie, datele de autentificare ale acestuia trebuie imediat anulate
- **Un antivirus competitiv** bazat pe tehnologii anti-spam, anti-phishing și anti-malware care să ruleze la gateway este vital împotriva atacurilor de tip phishing sau exploit
- **Cursuri de securitate** ținute cu regularitate angajaților. Fiecare trebuie să știe să recunoască un mesaj de tip phishing, să știe cum să trateze atașamentele care vin în e-mail-uri, să le scaneze și, foarte important, să raporteze departamentului de IT orice incident sau situație care li s-a părut suspectă.

  Folosirea de parole diferite pentru conturi diferite. Evitarea conectării la conturi personale folosind resursele companiei. Evitarea publicării pe conturile personale din diferite rețele de socializare a informațiilor ce privesc compania angajatoare. Uneori din greșeală, un angajat poate furniza date care ajută un atacator să pătrundă în rețeaua unei companii
- **O atitudine rezervată față de BYOD (bring your own device).** Angajații care aduc în firmă și folosesc la muncă propriile dispozitive, trebuie să fie conștienți că smart phone-ul, tableta, laptop-ul pot reprezenta o provocare mare pentru departamentul de IT al unei companii. Este important ca fiecare device care rulează un sistem de operare diferit să aibă update-urile de securitate la zi și să fie incluse in rețeaua securizată a firmei când rulează din firmă.

Asta nu elimină total riscul unui incident neplăcut de securitate, atâta timp cât se conectează cu telefonul la internet prin rețele WI-FI în cafenele sau aeroporturi

unde pot să se infecteze cu un virus, să-l aducă apoi în firmă și să compromită întreaga rețea a companiei. La fel de grav este și dacă un angajat pierde telefonul sau tableta pe care păstrează informații legate de serviciu care ajunse în mâine nepotrivite pot să aibă impact devastator asupra business-ului

- **Segmentarea este esențială**. Atât la nivelul resurselor, unde, de exemplu, serverul de mail și serverul folosit pentru conectarea la net trebuie să fie diferite, cât și la nivelul informațiilor pe care le dețin angajații cu privire la companie. Toate informațiile suplimentare pot ajunge în posesia unei persoane rău-intenționate și folosite împotriva companiei
- **Whitelisting-ul** are rezultate mai bune decât blacklisting-ul. Companiile pot configura rețeaua în așa fel încât angajații să poată accesa doar site-uri care au fost in prealabil verificate de personalul calificat și aprobate ca fiind sigure și fără risc de atac. Site-uile considerate periculoase pot fi blocate din firewall și astfel din companie nimeni nu se poate conecta la aceste locații web chiar daca, de exemplu, cineva a dat click pe un link periculos sau a deschis un atașament periculos. De foarte multe ori angajații se pot infecta prin intermediul rețelelor sociale precum Facebook. Puteți fie restricționa accesul la aceste resurse sau puteți să oferiți training de securitate pentru folosirea rețelelor sociale.

Toate aceste măsuri de securitate trebuie să facă față unor obiceiuri mai puțin sigure ale utilizatorilor. Pierderea sau distrugerea în totalitate sau parțială a datelor poate avea efecte dezastruoase asupra securității și integrității unei companii.

Astfel, daca nu doriți să ajutați un străin să vă facă rău dumneavoastră sau companiei pentru care lucrați, folosiți discreția atunci când vă actualizați contul de pe rețeaua de socializare preferată cu date care țin de viața privată sau profesională.