

## Ghid de bune practici pentru securizarea calculatoarelor și rețelelor personale

Ghidul de bune practici emis de **Asociația Națională pentru Securitatea Sistemelor Informatice** oferă recomandări necesare în vederea asigurării unui nivel de securitate informatică eficient.

Amenințările cibernetice nu se mai limitează în a viza doar rețelele mari ale corporațiilor. Atacatorii au înțeles că țintele sunt mai vulnerabile atunci când utilizatorii lucrează acasă, unde, de obicei, măsurile de securitate sunt mai slabe. Utilizatorii trebuie să mențină de asemenea un nivel corespunzător de securitate și atunci când lucrează acasă, utilizând Internetul.

Ghidul este structurat în patru capitole: recomandări pentru securitatea computerelor personale, recomandări pentru securitatea rețelelor personale, recomandări de securitate operațională și comportament pe Internet, respectiv recomandări avansate de securitate.

### I. Recomandări pentru securitatea computerelor personale

#### 1. Migrați către sisteme de operare și platforme hardware moderne

Multe dintre caracteristicile de securitate ale acestor sisteme sunt acum activate implicit și pot preveni o multitudine de atacuri des întâlnite. Mai mult, versiunile acestor sisteme de operare pe 64 de biți solicită eforturi mai mari din partea unui atacator care încearcă să capete controlul unui computer.

O setare obligatorie, indiferent de sistemul de operare pe care îl folosiți, este de a activa mecanismele automate de actualizare (update) ale sistemului de operare.

#### 2. Instalați o soluție completă de software de securitate

O astfel de soluție trebuie să cuprindă software anti-virus, anti-phishing și să aibă capabilități de tip firewall și IPS, de prevenire a atacurilor și de navigare securizată. Aceste servicii, lucrând conjugat pot oferi o apărare stratificată împotriva celor mai des întâlnite amenințări. Mai multe astfel de soluții oferă și un serviciu care verifică site-urile pe care le accesați, având un istoric al reputației domeniilor web care au avut vreodată un rol în răspândirea de malware.

Nu uitați să activați orice serviciu automat de actualizare automată a acestor softuri pentru a vă asigura că folosiți ultimele versiuni de semnături ale programelor anti-malware.

#### 3. Evitați pe cât posibil folosirea contului de administrator

Primul cont creat în mod implicit când este instalat sistemul de operare, este cel de administrator local. Este necesară crearea unui cont de utilizator care să nu aibă toate privilegiile specifice contului de administrator. Acest cont va fi folosit pentru activitățile uzuale, cum ar fi web-browsing, creare sau editare de documente, acces la e-mail, etc. Contul de administrator ar trebui folosit numai atunci când se fac actualizări de software sau când este necesară reconfigurarea sistemului. Navigarea pe web sau accesul la e-mail folosind contul de administrator este riscantă, dând ocazia atacatorilor să preia controlul asupra sistemului.

#### 4. Utilizați browsere web cu capabilități de tip Sandbox

În momentul de față, există câteva astfel de browsere, care, atunci când se execută un cod malware, izolează acest cod de sistemul de operare, făcând astfel imposibilă exploatarea unei eventuale vulnerabilități a sistemului de operare. Majoritatea acestui gen de browsere au și capacitatea de auto-actualizare sau de notificare a utilizatorului atunci când apar versiuni noi.

Există pe piață și abordări care mută navigarea pe web în întregime pe mașini virtuale, dar care nu au încă maturitatea tehnologică necesară pentru a fi folosite de publicul larg.

#### 5. Folosiți numai programe cu capacitatea de Sandboxing pentru a citi fișierele de tip PDF

Capabilitatea de Sandboxing izolează de sistemul de operare orice cod malware conținut de fișierele PDF. Aceste fișiere au devenit un vector de atac foarte des folosit, ele putând conține, pe lângă informația legitimă, cod executabil. În prezent, există câteva versiuni, atât comerciale, cât și open-source, ale unor astfel de softuri ce au capacitatea de Sandboxing, cât și de blocare a linkurilor către website-uri incluse în documentele în format PDF.

#### 6. Folosiți versiuni ale aplicațiilor de tip Office cât mai recente

În versiunile mai recente, formatul de stocare al documentelor este XML, un format care nu permite executarea de cod la deschiderea unor documente, astfel protejând utilizatorii de malware-ul ce folosește ca mod de propagare astfel de documente. Unele din versiunile cele mai recente oferă o facilitate de tip "protected view", deschizând documentele în modul "read-only", astfel eliminând o serie de riscuri generate de un fișier infectat.

#### 7. Actualizați-vă software-ul

Majoritatea utilizatorilor nu au timpul sau răbdarea de a verifica dacă aplicațiile instalate pe computer sunt actualizate. De vreme ce există multe aplicații ce nu au capacitatea de auto-actualizare, atacatorii vizează astfel de aplicații ca mijloace de a prelua controlul asupra sistemului. Pe piață există câteva produse ce monitorizează software-ul instalat pe sistem și descoperă care aplicații au ajuns la sfârșitul duratei ciclului de viață sau au nevoie de actualizări, indicând și locul de unde pot fi obținute actualizări sau versiuni mai noi pentru respectivele aplicații.

#### 8. Criptați discurile laptop-urilor

Sistemele de operare recente oferă nativ capacitatea de criptare a discurilor prin mecanisme proprii. Pentru versiuni mai vechi, dar și pentru celelalte există produse care implementează acest serviciu. Astfel, puteți evita accesul neautorizat la informații confidențiale, în caz că laptop-ul este pierdut sau furat.

#### 9. Actualizați-vă sistemele de operare pentru dispozitivele mobile

Este recomandat să faceți acest lucru atunci când apar versiuni noi și să verificați acest lucru periodic. Sunteți mult mai vulnerabili atunci când utilizați dispozitivele mobile (telefon, tableta, etc.) în timpul unor călătorii, deoarece amenințările sunt mai probabile în rețelele publice din aeroporturi, gări, obiective turistice etc.

#### 10. Utilizați parole complexe

Ca o regulă generală, toate parolele asociate cu orice cont de utilizator ar trebui să aibă cel puțin 10 caractere și să fie complexe, în sensul de a include caractere speciale, cifre, litere mici și litere mari.

## II. Recomandări pentru securitatea rețelelor personale

Rețelele personale sunt rețele informatice de mici dimensiuni utilizate cel mai adesea la domiciliu bazate din ce în ce mai mult pe tehnologia wireless.

### 1. Designul rețelei

De obicei, furnizorii de servicii Internet furnizează un dispozitiv de conectare la rețeaua lor (un modem de cablu, un modem ADSL, etc.) cu capabilități de routare și wireless. Pentru a maximiza controlul utilizatorului asupra rutării și a capabilităților wireless, este recomandat ca utilizatorul să instaleze un router wireless separat de cel al furnizorului de servicii, asupra căruia să aibă control complet.

### 2. Implementați WPA2 în rețeaua wireless

Rețeaua wireless ar trebui să fie protejată prin folosirea tehnologiei Wi-Fi Protected Access 2 (WPA2), care este de preferat în locul WEP (Wired Equivalent Privacy). Actualmente, tehnologia WEP este vulnerabilă, criptarea asociată putând fi spartă în timp foarte scurt și astfel, permițând unui atacator să intercepteze tot traficul. De menționat că, este posibil ca sistemele mai vechi să nu suporte WPA2, fiind nevoie de un upgrade de software sau hardware. Dacă urmează să achiziționați dispozitive wireless, asigurați-vă că sunt certificate cel puțin WPA2-Personal.

### 3. Limitați accesul la interfețele de administrare ale dispozitivelor de rețea

Administrarea acestor dispozitive (modem-uri, router-e, switch-uri) trebuie să fie permisă doar din partea internă a rețelei, și acolo unde este posibil, opțiunea de administrare externă a acestor dispozitive să fie dezactivată, prevenind astfel ca un atacator să obțină controlul rețelei.

### 4. Implementați un furnizor alternativ de servicii DNS

De obicei, furnizorii de servicii Internet implementează servicii simple de DNS (domain name service), neoferind facilități care să blocheze accesul către site-uri periculoase sau infectate. Există alternative atât comerciale, cât și open-source care mențin o bază de date de tip blacklist pentru protecția și restricționarea accesului la Internet.

### 5. Setări parole puternice pe toate dispozitivele de rețea

Pe lângă setarea unei parole puternice și complexe pentru rețeaua wireless, toate dispozitivele de rețea care oferă posibilitatea de web-management ar trebui să aibă parole puternice. De exemplu, majoritatea imprimantelor de rețea pot fi configurate via web, gama de setări fiind una vastă, de la servicii până la alerte prin e-mail sau jurnalizări.

### III. Recomandări de securitate operațională și comportament pe Internet

#### 1. Recomandări de călătorie

În diverse locuri (cafenele, hoteluri, aeroporturi, etc.) se găsesc hotspot-uri wireless sau chioșcuri care oferă servicii Internet clienților. Având în vedere că infrastructura ce deservește aceste rețele este una necunoscută și că adeseori, securitatea nu e o preocupare în aceste locuri, există o serie de riscuri. Pentru a le contracara, iată câteva recomandări:

- Dispozitivele mobile (laptop-uri, smart-phones) ar trebui să fie conectate la Internet folosind rețelele celulare (mobile Wi-Fi, 3G sau 4G), această modalitate fiind de preferat în locul hotspot-urilor.
- Dacă se folosește un hotspot Wi-Fi pentru accesul la Internet, indiferent de rețeaua folosită, utilizatorii pot seta un tunel VPN către un furnizor de încredere pentru acest gen de servicii, protejând astfel tot traficul de date efectuat și prevenind activități răuvoitoare cum ar fi interceptarea traficului.
- Dacă utilizarea unui hotspot Wi-Fi este singura modalitate de a accesa Internetul, este recomandat să vă rezumați doar la navigarea pe web și să evitați să accesați servicii unde trebuie să vă autentificați, deci să furnizați date de genul user/parolă.

Este recomandat să aveți tot timpul controlul asupra dispozitivelor mobile și laptop-urilor deoarece acestea pot fi ținta unui atac dacă un atacator ar avea acces la ele. Astfel, dacă sunteți nevoit să lăsați, de exemplu, un laptop în camera de hotel, se recomandă ca acesta să fie oprit și să aibă discurile criptate, așa cum precizăm mai sus.

#### 2. Schimbul de date între computerul de la locul de muncă și cel de acasă

În general, rețelele companiilor sunt configurate de o manieră mai sigură și au servicii (filtrare de e-mailuri, filtrare conținut web, IDS, etc.) care pot detecta conținutul malițios. De vreme ce acasă, utilizatorii nu au aceleași reguli de securitate ca la locul de muncă, computerele personale sunt ținte mult mai ușor de compromis pentru un atacator. Astfel, fluxul de date (folosind e-mailul sau stick-uri de memorie, etc.) dinspre computerul de acasă spre cel de la birou induce o serie de riscuri și trebuie evitat de câte ori este posibil.

#### 3. Stocarea datelor personale pe Internet trebuie făcută cu precauție

Informațiile personale, stocate până acum în mod tradițional pe sisteme locale, tind să fie mutate pe Internet, în cloud. Putem da exemplul de astfel de date cum ar fi: serviciile de webmail, informații de natură financiară sau informații personale postate pe site-uri de socializare. Odată postată, informația din cloud este dificil de înlăturat și este reglementată de regulile de securitate și confidențialitate ale sistemului pe care este postată. Cei care postează astfel de informații folosind aceste servicii web trebuie să se gândească foarte bine înainte de a o face și să își răspundă la următoarele întrebări: "Cine va avea acces la aceste informații?" și "Cum pot controla felul în care această informație e stocată și publicată?". Utilizatorii de Internet ar trebui, de asemenea, dacă au temeri, să verifice periodic dacă informații cu caracter personal ce îi privesc au fost publicate pe Internet, căutând astfel de informații cu ajutorul celor mai populare motoare de căutare.

#### 4. Utilizarea cu precauție a datelor personale pe site-urile de socializare

Site-urile de socializare sunt foarte comod de folosit și foarte eficiente atunci când vine vorba de a partaja informații personale cu familia și prietenii. Aceste facilități induc totuși niște riscuri. De aceea, utilizatorii trebuie să conștientizeze ce date personale sunt accesibile altora și cine le poate accesa. Nu este recomandată postarea numărului de telefon, a locului de muncă sau a altor date ce pot fi folosite în mod răuvoitor de către alții. Acolo unde este posibil, se recomandă restricționarea accesului la datele personale, permițându-l doar prietenilor. Atunci când primiți mesaje sau aplicații de la prieteni, prin intermediul unor site-uri de socializare, gândiți-vă că multe din atacuri se bazează tocmai pe faptul că astfel de mesaje sau aplicații sunt cu prea mare ușurință acceptate dacă vin din partea unui prieten. Aparent, aceste aplicații oferă noi capacități, în realitate ele conținând cod malițios bine ascuns utilizatorului.

Multe din site-urile de socializare oferă acum opțiunea de a renunța la publicarea datelor cu caracter personal. Se recomandă ca, periodic, să verificați politicile de securitate și setările disponibile pe respectivul site de socializare pentru a descoperi eventuale noi mecanisme de securitate implementate în vederea protecției informațiilor personale.

#### 5. Utilizarea criptării SSL

Criptarea la nivel de aplicație (numită SSL - secure socket layer) asigură confidențialitatea informațiilor atunci când sunt în tranzit prin alte rețele. Acest gen de criptare previne furtul de identitate de către eventuali atacatori care interceptează traficul din rețele wireless de exemplu și care ar putea să vadă credențialele atunci când vă autentificați la aplicații web.

Atunci când este posibil, este recomandat să folosiți versiunile criptate ale protocoalelor utilizate de aplicațiile web. Instituțiile financiare se bazează masiv pe criptarea datelor folosind SSL atunci când datele tranzacțiilor sunt în tranzit prin alte rețele. Multe dintre aplicațiile foarte populare precum Facebook sau Gmail sunt implicit configurate să folosească această criptare. Marea majoritate a browserelor web indică faptul că o aplicație folosește SSL, folosind simbolul unui lacăt plasat lângă URL-ul respectivului site.

#### 6. Recomandări pentru folosirea e-mail-ului

Conturile de e-mail, atât cele web-based, cât și cele locale, sunt ținte foarte vizate de atacatori. Următoarele recomandări se pot dovedi utile pentru a reduce riscurile legate de acest serviciu:

- În ideea de a nu vă compromite atât contul de email de la birou, cât și cel personal, este recomandat să folosiți nume diferite pentru aceste conturi. Numele de utilizator unice pentru aceste conturi diminuează riscul de a fi vizate ambele conturi într-un atac
- Setarea unor mesaje de genul "out-of-office" pentru contul personal de e-mail nu este recomandată, fiind o sursă prețioasă de informații pentru spammeri și confirmând faptul că este o adresă de e-mail validă
- Folosiți întotdeauna protocoale securizate atunci când accesați e-mailul (indiferent de protocol IMAPS, POP3S, HTTPS), mai ales atunci când folosiți o rețea wireless. Majoritatea clienților de email suportă aceste protocoale, prevenind astfel o interceptare a e-mailului atunci când este în tranzit între computerul dumneavoastră și serverul de e-mail
- Mailurile nesolicitate care conțin atașamente sau link-uri trebuie tratate ca suspecte. Dacă identitatea celui care a trimis respectivul email nu poate fi verificată, sfatul este de a șterge acel e-mail fără a-l deschide pentru a-i vedea conținutul. Nu răspundeți la emailuri care vă solicită date cu caracter personal. Orice entitate cu care relaționați prin intermediul unor

aplicații web ar trebui deja să aibă aceste informații. În cazul e-mailurilor care conțin link-uri, nu navigați direct către acel link. Puteți copia acel link și să îl căutați de exemplu pe Google.

## 7. Managementul parolelor

Asigurați-vă că parolele și întrebările setate pentru mecanismele de recuperare a parolelor sunt corespunzător securizate. Parolele trebuie să fie complexe și unice pentru fiecare cont în parte. O parolă complexă trebuie să aibă cel puțin 10 caractere și să includă caractere speciale, cifre, litere mici și litere mari. Parolele trebuie să fie unice pentru fiecare cont pentru a preveni compromiterea tuturor conturilor dacă o parolă este compromisă. Dezactivați acele opțiuni care permit programelor să memoreze parole. Multe site-uri implementează mecanisme de recuperare a parolelor de tip “challenge-response”. Răspunsurile la aceste întrebări trebuie să fie lucruri intime știute de către utilizator și să nu poată fi găsite pe Internet prin căutări bine direcționate.

## 8. Integrarea fotografiei/GPS

În prezent, multe din telefoane și noile camere foto, includ în fotografii și coordonatele GPS ale locației unde a fost făcută fotografia. Limitați accesul la aceste fotografii, permițându-l doar unei audiențe de încredere, sau, folosind unelte software, eliminați coordonatele GPS. Aceste coordonate pot fi folosite pentru a defini profilul unei persoane, a determina obiceiurile și locurile des frecventate, sau, pot indica aproape în timp real poziția unei persoane atunci când sunt încărcate pe un site de socializare prin intermediul unui smartphone. Unele site-uri de socializare, cum ar fi Facebook, elimină automat coordonatele GPS din fotografii, în scopul de a proteja viața privată a utilizatorilor săi.

## 9. Ingineria socială

În domeniul securității informatice, sensul ingineriei sociale constă în puterea de a manipula oamenii astfel încât să divulge informații confidențiale în scopul de a strânge informații, a fraudă sau a accesa în mod neautorizat sisteme informatice. În cele mai multe cazuri, victima nu are contact personal cu atacatorul. Astfel, trebuie conștientizat faptul ca administratorii de rețea sau ale altor servicii informatice pe care le folosiți, nu vă vor solicita niciodată date cu caracter personal, cum ar fi numărul cardului dumneavoastră de credit, codul pin sau parole ale contului de e-mail sau al vreunui alt serviciu. Administratorii, nu au nevoie de date ale utilizatorilor, ei fiind capabili să își desfășoare activitatea într-un mod transparent față de utilizatori, neinteracționând decât în cazuri excepționale cu utilizatorii. Nu divulgați niciodată date cu caracter personal sau confidențiale în urma unor solicitări telefonice sau prin e-mail și verificați întotdeauna identitatea interlocutorului dacă are loc un astfel de dialog.

#### IV. Recomandări avansate de securitate

Următoarele recomandări solicită un nivel mai ridicat de cunoștințe referitoare la rețele. Aceste recomandări, odată implementate, pot duce la un grad sporit de securitate, dar pot avea un impact asupra modului în care navigați pe web, adesea solicitând revizuirea lor în mod repetat.

##### 1. Configurarea routerelor wireless

Se pot face o serie de setări suplimentare pentru rețelele wireless în ideea unei restricționări a accesului mai riguroasă. Mecanismele de securitate descrise mai jos sunt, totuși, eficiente doar împotriva unor atacatori mai puțin experimentați.

- Filtrarea adreselor MAC – permite accesul la rețea doar sistemelor autorizate în prealabil, prin configurarea routerului cu adresele MAC ale stațiilor autorizate să acceseze rețeaua
- Limitarea puterii de transmisie a routerului pentru a limita aria în care rețeaua este accesibilă, prevenind astfel ca rețeaua să fie accesibilă de exemplu din fața casei sau din parcare
- Ascunderea SSID-ului routerului – previne detectarea rețelei de către un eventual atacator, dar totodată împiedică computerele client din respectiva rețea să o descopere, ele trebuind să fie configurate manual
- Reducerea plajei de adrese dinamic alocate de către router sau configurarea de adrese IP statice în cadrul rețelei este un alt mecanism de securitate care împiedică computerele neautorizate să se conecteze în rețea

##### 2. Dezactivarea executării de scripturi în browsere

Dacă folosiți anumite browsere, puteți folosi opțiunea NoScript / NotScript sau plugin-uri pentru a nu permite execuția de scripturi ce provin de pe site-uri necunoscute. Dezactivarea execuției de scripturi poate cauza probleme de folosire facilă a browserului, dar este o tehnică foarte eficientă pentru a elimina o serie de riscuri legate de execuția acestor scripturi.

*Acest Ghid a fost elaborat de ANSSI luând în considerare bunele practici în vederea asigurării unui nivel acceptabil de securitate precum și diverse materiale de specialitate.*