Asociaţia Naţională pentru Securitatea Sistemelor Informatice

Ghid de bune practici pentru securizarea calculatoarelor și rețelelor personale

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

Ameninţările cibernetice nu se mai limitează în a viza doar reţelele mari ale corporaţiilor. Atacatorii au înţeles că ţintele sunt mai vulnerabile atunci când utilizatorii lucrează acasă, unde, de obicei, măsurile de securitate sunt mai slabe. Utilizatorii trebuie să menţină de asemenea un nivel corespunzător de securitate şi 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 operaţională şi comportament pe Internet, respectiv recomandări avansate de securitate.

I. Recomandări pentru securitatea computerelor personale

1. Migraţi către sisteme de operare şi platforme hardware moderne

Multe dintre caracteristicile de securitate ale acestor sisteme sunt acum activate implicit şi pot preveni o multitudine de atacuri des întâlnite. Mai mult, versiunile acestor sisteme de operare pe 64 de biţi 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 folosiţi, este de a activa mecanismele automate de actualizare (update) ale sistemului de operare.

2. Instalaţi o soluţie completă de software de securitate

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

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

3. Evitaţi 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 activităţile 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. Utilizaţi browsere web cu capabilităţi de tip Sandbox

În momentul de faţă, 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 vulnerabilităţi a sistemului de operare. Majoritatea acestui gen de browsere au şi capabilitatea de auto-actualizare sau de notificare a utilizatorului atunci când apar versiuni noi.

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

5. Folosiţi numai programe cu capabilităţi de Sandboxing pentru a citi fişierele de tip PDF

Capabilitatea de Sandboxing izolează de sistemul de operare orice cod malware conţinut de fişierele PDF. Aceste fişiere au devenit un vector de atac foarte des folosit, ele putând conţine, pe langă informaţia legitimă, cod executabil. În prezent, există câteva versiuni, atât comerciale, cât şi open-source, ale unor astfel de softuri ce au capabilităţi de Sandboxing, cât şi de blocare a linkurilor către website-uri incluse în documentele în format PDF.

6. Folosiţi versiuni ale aplicaţiilor 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 foloseşte 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 fişier infectat.

7. Actualizaţi-vă software-ul

Majoritatea utilizatorilor nu au timpul sau răbdarea de a verifica dacă aplicaţiile instalate pe computer sunt actualizate. De vreme ce există multe aplicaţii ce nu au capabilităţi de auto-actualizare, atacatorii vizează astfel de aplicaţii ca mijloace de a prelua controlul asupra sistemului. Pe piaţă există câteva produse ce monitorizează software-ul instalat pe sistem şi descoperă care aplicaţii au ajuns la sfârşitul duratei ciclului de viaţă sau au nevoie de actualizări, indicând şi locul de unde pot fi obţinute actualizări sau versiuni mai noi pentru respectivele aplicaţii.

8. Criptaţi discurile laptop-urilor

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

9. Actualizaţi-vă sistemele de operare pentru dispozitivele mobile

Este recomandat să faceţi 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 puţin 10 caractere şi să fie complexe, în sensul de a include caractere speciale, cifre, litere mici şi litere mari.

II. Recomandări pentru securitatea reţelelor 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 reţelei

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

2. Implementaţi WPA2 în reţeaua wireless

Reţeaua 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 şi astfel, permiţând unui atacator să intercepteze tot traficul. De menţionat că, este posibil ca sistemele mai vechi să nu suporte WPA2, fiind nevoie de un upgrade de software sau hardware. Dacă urmează să achiziţionaţi dispozitive wireless, asiguraţi-vă că sunt certificate cel puţin WPA2-Personal.

3. Limitaţi accesul la interfeţele de administrare ale dispozitivelor de reţea

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

4. Implementați un furnizor alternativ de servicii DNS

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

5. Setaţi parole puternice pe toate dispozitivele de reţea

Pe langă setarea unei parole puternice şi complexe pentru reţeaua wireless, toate dispozitivele de reţea care oferă posibilitatea de web-management ar trebui să aibă parole puternice. De exemplu, majoritatea imprimantelor de reţea 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 operaţională şi comportament pe Internet

1. Recomandări de călătorie

În diverse locuri (cafenele, hoteluri, aeroporturi, etc.) se găsesc hotspot-uri wireless sau chioşcuri care oferă servicii Internet clienţilor. Având în vedere că infrastructura ce deserveşte aceste reţele este una necunoscută şi 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 reţelele celulare (mobile Wi-Fi, 3G sau 4G), această modalitate fiind de preferat în locul hotspot-urilor.
- Dacă se foloseşte un hotspot Wi-Fi pentru accesul la Internet, indiferent de reţeaua folosită, utilizatorii pot seta un tunel VPN către un furnizor de încredere pentru acest gen de servicii, protejând astfel tot traficul de date efectuat şi prevenind activităţi răuvoitoare cum ar fi interceptarea traficului.
- Dacă utilizarea unui hotspot Wi-Fi este singura modalitate de a accesa Internetul, este recomandat să vă rezumaţi doar la navigarea pe web şi să evitaţi să accesaţi servicii unde trebuie să vă autentificaţi, deci să furnizaţi date de genul user/parolă.

Este recomandat să aveţi tot timpul controlul asupra dispozitivelor mobile și laptop-urilor deoarece acestea pot fi ţinta unui atac dacă un atacator ar avea acces la ele. Astfel, dacă sunteţi nevoit să lăsaţi, de exemplu, un laptop în camera de hotel, se recomandă ca acesta să fie oprit şi să aibă discurile criptate, aşa cum precizam mai sus.

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

În general, reţelele companiilor sunt configurate de o manieră mai sigură şi au servicii (filtrare de e-mailuri, filtrare conținut web, IDS, etc.) care pot detecta conţinutul maliţios. De vreme ce acasă, utilizatorii nu au aceleaşi reguli de securitate ca la locul de muncă, computerele personale sunt ţinte mult mai uşor 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 şi trebuie evitat de câte ori este posibil.

3. Stocarea datelor personale pe Internet trebuie făcută cu precauție

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

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

Site-urile de socilizare sunt foarte comod de folosit şi foarte eficiente atunci când vine vorba de a partaja informaţii personale cu familia şi prietenii. Aceste facilităţi induc totuşi nişte riscuri. De aceea, utilizatorii trebuie să conştientizeze ce date personale sunt accesibile altora şi 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 alţii. Acolo unde este posibil, se recomandă restricţionarea accesului la datele personale, permiţându-l doar prietenilor. Atunci când primiţi mesaje sau aplicaţii de la prieteni, prin intermediul unor site-uri de socializare, gândiţi-vă că multe din atacuri se bazează tocmai pe faptul că astfel de mesaje sau aplicaţii sunt cu prea mare uşurinţă acceptate dacă vin din partea unui prieten. Aparent, aceste aplicaţii oferă noi capabilităţi, în realitate ele conţinând cod maliţios bine ascuns utilizatorului.

Multe din site-urile de socializare oferă acum opţiunea de a renunţa la publicarea datelor cu caracter personal. Se recomandă ca, periodic, să verificaţi politicile de securitate şi setările disponibile pe respectivul site de socializare pentru a descoperi eventuale noi mecanisme de securitate implementate în vederea protecţiei informaţiilor personale.

5. Utilizarea criptării SSL

Criptarea la nivel de aplicaţie (numită SSL - secure soket layer) asigură confidenţialitatea informaţiilor atunci când sunt în tranzit prin alte reţele. Acest gen de criptare previne furtul de identitate de către eventuali atacatori care interceptează traficul din reţele wireless de exemplu şi care ar putea să vadă credenţialele atunci când vă autentificaţi la aplicaţii web.

Atunci când este posibil, este recomandat să folosiţi versiunile criptate ale protocoalelor utilizate de aplicaţiile web. Instituţiile financiare se bazează masiv pe criptarea datelor folosind SSL atunci cand datele tranzacţiilor sunt în tranzit prin alte reţele. Multe dintre aplicaţiile foarte populare precum Facebook sau Gmail sunt implicit configurate să folosească această criptare. Marea majoritate a browserelor web indică faptul că o aplicaţie foloseşte 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 şi cele locale, sunt ţinte 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 şi cel personal, este recomandat să folosiţi 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 preţioasă de informaţii pentru spammeri şi confirmând faptul că este o adresă de e-mail validă

- Folosiţi întotdeauna protocoale securizate atunci când accesaţi e-mailul (indiferent de protocol IMAPS, POP3S, HTTPS), mai ales atunci când folosiţi o reţea wireless. Majoritatea clienţilor de email suportă aceste protocoale, prevenind astfel o interceptare a e-mailului atunci când este în tranzit între computerul dumneavoastră şi serverul de e-mail

- Mailurile nesolicitate care conţin ataşamente sau link-uri trebuie tratate ca suspecte. Dacă identitatea celui care a trimis respectivul email nu poate fi verificată, sfatul este de a şterge acel e-mail fără a-l deschide pentru a-i vedea conţinutul. Nu răspundeţi la emailuri care vă solicită date cu caracter personal. Orice entitate cu care relaţionaţi prin intermediul unor aplicaţii web ar trebui deja să aibă aceste informaţii. În cazul e-mailurilor care conţin link-uri, nu navigaţi direct către acel link. Puteţi copia acel link şi să îl căutaţi de exemplu pe Google.

7. Managementul parolelor

Asiguraţi-vă că parolele şi întrebările setate pentru mecanismele de recuperare a parolelor sunt corespunzător securizate. Parolele trebuie să fie complexe şi unice pentru fiecare cont în parte. O parolă complexă trebuie să aibă cel puţin 10 caractere şi să includă caractere speciale, cifre, litere mici şi litere mari. Parolele trebuie să fie unice pentru fiecare cont pentru a preveni compromiterea tuturor conturilor dacă o parolă este compromisă. Dezactivaţi acele opţiuni 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 intim ştiute de către utilizator şi să nu poată fi găsite pe Internet prin căutări bine direcţionate.

8. Integrarea fotografii/GPS

În prezent, multe din telefoane şi noile camere foto, includ în fotografii şi coordonatele GPS ale locaţiei unde a fost făcută fotografia. Limitaţi accesul la aceste fotografii, permiţându-l doar unei audienţe de încredere, sau, folosind unelte software, eliminaţi coordonatele GPS. Aceste coordonate pot fi folosite pentru a defini profilul unei persoane, a determina obiceiurile şi locurile des frecventate, sau, pot indica aproape în timp real poziţia 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 viaţa privată a utilizatorilor săi.

9. Ingineria sociala

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 frauda 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 niciodata 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 sa își desfășoare activitatea intr-un mod transparent față de utilizatori, neinteracționând decât în cazuri excepționale cu utilizatorii. Nu divulgați niciodata 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 cunoştinţe referitoare la reţele. Aceste recomandări, odată implementate, pot duce la un grad sporit de securitate, dar pot avea un impact asupra modului în care navigaţi pe web, adesea solicitând revizuirea lor în mod repetat.

1. Configurarea routerelor wireless

Se pot face o serie de setări suplimentare pentru reţelele wireless în ideea unei restricţionări a accesului mai riguroasă. Mecanismele de securitate descrise mai jos sunt, totuşi, eficiente doar împotriva unor atacatori mai puţin experimentaţi.

- Filtrarea adreselor MAC – permite accesul la reţea 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 reţeaua este accesibilă, prevenind astfel ca reţeaua să fie accesibilă de exemplu din faţa casei sau din parcare
- Ascunderea SSID-ului routerului – previne detectarea reţelei de către un eventual atacator, dar totodată împiedică computerele client din respectiva reţea 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 reţelei este un alt mecanism de securitate care împiedică computerele neautorizate să se conecteze în reţea

2. Dezactivarea executării de scripturi în browsere

Dacă folosiţi anumite browsere, puteţi folosi opțiunea NoScript / NotScript sau plugin-uri pentru a nu permite execuţia de scripturi ce provin de pe site-uri necunoscute. Dezactivarea execuţiei 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 execuţia 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.