10 pași pentru îmbunătățirea securității unui calculator nou

- (v 1.0) -

13 August 2012

TRAFFIC LIGHT PROTOCOL: GREEN

1. Despre document

Acest document este o traducere din limba engleză a articolului intitulat „Ten Ways to Improve the Security of a New Computer", creat în cadrul US-CERT. Articolul original este disponibil la http://www.us-cert.gov/reading_room/TenWaystoImproveNewComputerSecurity.pdf . Articolul inițial nu a fost alterat în nici un fel, RoCSIRT încercând să păstreze pe cât posibil sensul conținutului original.

Documentul este public, conținutul acestuia putând fi folosit de orice persoană sau instituție, atâta timp cât conținutul său rămâne nealterat și atâta timp cât este menționată atât sursa originală cât și sursa traducerii.

2. Audiență

Documentul se adresează în primul rând instituțiilor conectate la RoEduNet.

3. Generalități

3.1. De ce contează securitatea calculatoarelor ?

Calculatoarele personale ne ajută să fim conectați în lumea modernă. Le folosim pentru acces la contul bancar şi pentru plata facturilor, la comerțul online, pentru a ne conecta cu prietenii și familia prin intermediul emailului și a rețelelor de socializare, pentru a naviga pe Internet și pentru multe altele. Depindem atât de mult de calculatoarele noastre încât uneori trecem cu vederea securitatea acestora. Deoarece calculatoarele au un rol atât de important în viețile noastre și le încredințăm atât de multe informații personale, este important să îmbunătățim permanent nivelul lor de protecție, pentru a continua să ne bazăm pe ele și pentru a păstra în siguranță informațiile personale.

Persoane rău intenționate ne pot infecta calculatorul cu aplicații malițioase, sau *malware*, prin mai multe metode. Acestea pot exploata obiceiurile utilizatorilor sau problemele programelor (ce includ vulnerabilități sau servicii incomplet securizate), sau se pot folosi de tehnici de inginerie socială (în care o persoană rău intenționată convinge o altă persoană să realizeze o acțiune precum deschiderea unui atașament la un mail sau accesarea unui site capcană). În momentul în care calculatorul este infectat, persoanele rău intenționate pot folosi aplicații de tip malware pentru a avea acces la calculatorul dumneavoastră fără voia sau știința utilizatorului și ceea ce este și mai rău, poate determina calculatorul să efectueze anumite acțiuni nedorite. Acești atacatori pot fura informațiile personale, pot schimba elemente de configurare ale calculatoarelor, pot face calculatorul să funcționeze sub parametrii optimi sau pot chiar instala mai multe aplicații de tip *malware* cu scopul de a infecta alte calculatoare sau de a produce pagube altor utilizatori.

Unul din cele mai cunoscute atacuri este cel al *malware*-ului Conficker, descoperit în 2008. Acest *malware* s-a extins rapid și a devenit una din cele mai răspândite infecții, afectând milioane de calculatoare și provocând pagube de miliarde de dolari în întreaga lume. Conficker avea abilitatea de a fura și a transmite atacatorilor informațiile personale, dezactivând măsuri de securitate existente, cum ar fi Update-urile Automate Windows sau aplicațiile antivirus, și blocând accesul la cele mai populare site-uri de securitate. Atacatorii puteau folosi calculatoarele personale infectate ca parte a unei armate de zombie (botnet), pentru a porni atacuri îndreptate împotriva altor calculatoare. Malware-ul Conficker a exploatat trei probleme de securitate distincte ale sistemului de operare Microsoft Windows: Serviciul de Transfer de Fișiere, facilitatea AutoRun activată implicit și o vulnerabilitate a serviciului de rețea a Windows Server. Utilizatorii care ar fi urmat cele zece sfaturi de mai jos, ar fi redus semnificativ riscul de infectare cu Conficker.

3.2. Cum îmbunătățesc securitatea calculatorului meu ?

Cele zece sfaturi de mai jos sunt cele mai importante acțiuni pe care un utilizator trebuie să le aplice pentru a crește siguranța calculatorului personal. Deși nici unul din cele zece sfaturi nu poate elimina cu totul aceste riscuri, împreună, sfaturile de mai jos vor îmbunătăți considerabil nivelul de siguranță al calculatorului personal și vor reduce riscul unei infectări (compromiteri ?).

4. Cei 10 paşi

4.1. Pasul 1 - Conectarea la o reţea sigură

Atunci când calculatorul personal este conectat la Internet, el este de asemenea conectat şi la milioane de alte calculatoare, fapt ce poate permite persoanelor rău intenţionate să se conecteze la calculatorul dvs. În majoritatea cazurilor, informaţia este transportată dinspre Internet către reţeaua de acasă, trecând mai întâi prin modem (dacă sunteţi conectat prin cablu TV) apoi printr-un router şi în cele din urmă informaţia ajunge la calculatorul dvs. Pentru că modemul nu are nici o setare de securitate, este foarte important să vă securizaţi routerul, primul dispozitiv care primeşte informaţiile de pe Internet. Pentru a îmbunătăţi nivelul de securitate al calculatorului personal, această acţiune trebuie făcută înainte de a vă conecta la Internet. Dacă nu aveţi un router acasă, contactaţi furnizorul de servicii internet pentru a afla cea mai bună metodă de a securiza accesul în reţea.

Setările din fabrică ale majorităţii routerelor oferă un nivel scăzut de securitate. Deşi timpul petrecut pentru modificarea setărilor de securitate ale routerului nu este în topul activităţilor preferate ale utilizatorilor, cu siguranţă putem spune că efortul merită(este necesar) întrucât routerul este prima linie de apărare. Pentru a vă securiza routerul, consultaţi manualul de utilizare al acestuia şi căutaţi adresa web prin care vă puteţi conecta la interfaţa de administrare, care ar trebui să permită următoarele:

- schimbarea metodei de criptare a datelor transmise prin intermediul reţelei wireless în WPA2-AES, cel mai ridicat standard de criptare a datelor şi a transmisiei de date pe wireless;
- schimbarea numelui de utilizator (doar dacă este cazul şi doar dacă interfaţa de administrare permite acest lucru) şi parola implicită pentru că acestea sunt informaţii publice ce apar în manualele de utilizare;
- permiterea accesului în reţea doar pentru acele echipamente a căror adresă MAC o cunoaşteţi;
- schimbarea identificatorului reţelei wireless (SSID) implicit. Mai multe informaţii despre acest aspect pot fi găsite în documentul "Small Office/Home Office Router Security"[i]

4.2. Pasul 2 - Activarea şi configurarea unui firewall

Un *firewall*, în contextul calculatoarelor personale, este un program ce controlează fluxul de informaţie care circulă între calculatorul personal şi orice alt dispozitiv din reţeaua locală sau din/inspre Internet. Majoritatea sistemelor de operare moderne includ o aplicaţie de tip *firewall*: în Microsoft Windows este disponibilă aplicaţia Windows Firewall, în Linux iptables, etc. Vă invităm să verificaţi ghidul utilizatorului sistemului de operare instalat pe calculator, pentru a afla mai multe detalii. Este bine ca după ce aţi configurat *firewall*-ul, să-l protejaţi de orice modificare printr-o parolă adecvată.

4.3. Pasul 3 - Instalaţi şi utilizaţi un program Antivirus şi Antispyware

Instalarea unui program antivirus/antispyware şi actualizarea periodică a acestuia, reprezintă un pas critic în protejarea calculatorului personal. Multe tipuri de aplicaţii antivirus/antispyware pot detecta prezenţa malware-ului verificând periodic memoria şi fişierele de pe disc, căutând secvenţe cunoscute de cod. De asemenea, acest tip de aplicaţie foloseşte semnături ale celor mai cunoscuţi viruşi şi aplicaţii de tip malware.

Noi tipuri de malware sunt descoperite zilnic, semnăturile acestora fiind actualizate zilnic de către producătorii de programe antivirus/antispyware. Eficacitatea acestor aplicaţii este în mare măsură influenţată de numărul de semnături din baza de date şi de rapiditatea cu care acestea sunt actualizate. Majoritatea aplicaţiilor de acest tip, oferă şi posibilitatea de a face automat actualizările bazei de date cu semnături, fără a fi necesară intervenţia explicită a utilizatorului. Activarea acestei opţiuni este deosebit de importantă, atunci când este prezentă. În cazul în care totuşi facilitatea de actualizare automată nu este oferită, încercaţi pe cât posibil să descărcaţi aplicaţia dintr-o sursă sigură, verificabilă, precum site-ul de web al producătorului sau un CD pus la dispoziţie de către producător.

4.4. Pasul 4 - Înlăturarea aplicaţiilor nefolosite

Persoanele rău intenţionate pot ataca calculatoarele exploatând vulnerabilităţi ale aplicaţiilor(sau a sistemului de operare), prin urmare cu cât aveţi mai puţine aplicaţii instalate, cu atât scad şansele ca un atac îndreptat împotriva calculatorului personal să reuşească. Verificaţi periodic aplicaţiile instalate pe calculator. Dacă nu cunoaşteţi un anumit program şi nu îl folosiţi, încercaţi să determinaţi dacă este cu adevărat necesar. Înlăturaţi orice aplicaţie nefolosită după ce vă asiguraţi că dezinstalarea aplicaţiei de pe calculator nu vă aduce nici un fel de prejudicii.

Întotdeaună efectuaţi copii de siguranţă ale fişierelor şi ale datelor personale înainte de a înlătura aplicaţiile nefolosite, pentru cazul în care ştergeţi din greşeală o aplicaţie ce poate fi necesară sistemului de operare. Dacă este

posibil, păstrați mediul fizic (CD, DVD, USB stick, etc) de pe care ați instalat aplicațiile pe calculator, pentru cazul în care este nevoie de reinstalarea acestora.

4.5. Pasul 5 - Dezactivarea serviciilor neesențiale

La fel ca în cazul aplicațiilor nefolosite, serviciile care nu sunt esențiale pentru rularea în bune condiții a sistemului de operare și a aplicațiilor instalate cresc posibilitatea ca un atac asupra calculatorului dvs să reușească. Două din cele mai comune servicii de care este posibil să nu aveți nevoie sunt cele de partajare a fișierelor, ce permite utilizatorilor să pună la dispoziția altor utilizatori din rețea fișiere, precum muzică și fotografii, și cel de partajare a imprimantei, care oferă posibilitatea de a tipări la imprimante conectate la alte calculatoare din rețea.

Conficker folosește serviciul de partajare a fișierelor pentru a accesa și a infecta alte calculatoare din rețea. Dezactivarea serviciului de partajare a fișierelor, în cazul în care acesta nu este folosit, scade la 0 riscul de a fi infectat cu Conficker alte calculatoare din rețea.

Dacă unul dintre cele două servicii este activat în sistemul dvs. de operare și aveți un singur calculator personal, sau pur și simplu nu folosiți facilitățile oferite de cele două servicii, cel mai bine este să le dezactivați.

Deoarece serviciile diferă și sunt specifice fiecărui sistem de operare și deoarece multe dintre ele sunt absolut necesare pentru buna funcționare a acestuia, verificați atent fiecare serviciu pe care intenționați să-l dezactivați. În cazul în care nu sunteți sigur de utilitatea unui serviciu întrebați producătorul sistemului de operare înainte de a lua o decizie.

4.6. Pasul 6 - Modificaţi facilităţile implicite nefolosite

La fel ca în dezactivarea aplicațiilor și serviciilor nefolosite, modificarea facilităților implicite nefolosite ale sistemului de operare elimină posibile căi de atac. Evaluați cu atenție facilitățile ce sunt activate implicit de către sistemul de operare și dezactivați-le sau personalizați-le. La fel ca în cazul serviciilor neesențiale, informați-vă cu atenție înainte de a le modifica sau dezactiva.

Facilitatea AutoRun disponibilă în cadrul sistemului de operare Microsoft Windows era o facilitate activată implicit atunci când a apărut Conficker și a fost identificată ca una din cele trei modalități prin care un calculator putea fi infectat cu Conficker. Atunci când facilitatea AutoRun este activată implicit pe sistemele de operare Microsoft Windows, ea permite rularea automată a anumitor aplicații când în calculator este inserat un CD sau un dispozitiv de stocare USB.

4.7. Pasul 7 - Operarea după principiul celor mai puține privilegii

În majoritatea cazurilor de infecție, malware-ul rulează cu privilegiile utilizatorului conectat la calculator în momentul infectării. Pentru a micșora impactul malware-ului în cazul unei infectări este bine să luați în calcul folosirea în mod curent a unui cont de utilizator ce are cât mai puține privilegii și drepturi și folosirea unui utilizator privilegiat (administrator) doar atunci când aveți nevoie să instalați noi aplicații sau atunci când trebuie să modificați setări la nivelul sistemului de operare.

4.8. Pasul 8 - Securizaţi navigatorul web

De obicei, navigatorul web instalat pe calculatoarele personale nu are setări cu siguranță sporită. Securizarea navigatorului web este un pas critic pentru îmbunătățirea gradului de siguranță al calculatorului deoarece un număr din ce în ce mai mare de atacuri se concentrează pe exploatarea vulnerabilitatilor navigatoarelor web. Înainte de a naviga pe Internet, securizați-vă browserul de web, efectuând cel puțin următorii pași:

- dezactivați pe cât posibil executarea codului dinamic (Java, Flash, ActiveX și JavaScript) pentru site-urile noi sau cele în care nu aveți încredere. Chiar dacă în mod normal dezactivarea completă a posibilității de a executa cod dinamic ar mări semnificativ gradul de siguranță al calculatorului dvs, unele din site-urile preferate ar putea să nu mai funcționeze normal.
- dezactivarea opțiunii de a seta tot timpul *cookie*-uri. Un *cookie* este un fișier de pe calculatorul dvs în care site-urile vizitate pot stoca date. Un atacator poate accesa un site pe care dvs. l-ați vizitat (de exemplu pentru banking online), folosind informația de autentificare din *cookie*-urile stocate local, pe calculatorul dvs. Pentru a preveni asta, modificați setările navigatorului web astfel încât, înainte de a seta un *cookie*, acesta să ceară permisiunea dvs. explicită; acceptați doar acele *cookie*-uri ce sunt specifice sesiunilor și dezactivați orice altă facilitate care poate reține sesiunile deschise sau care stochează informații introduse de dvs. (text introdus în pagini web, în formulare sau în bara de căutare).
- dacă folosiți Internet Explorer, setați nivelul de securitate pentru site-urile cunoscute (site-urile pe care le vizitați cel mai des și în care aveți încredere) la al doilea nivel de securitate. La cel mai ridicat nivel de

securitate există posibilitatea ca acestea să nu mai funcţioneze normal. Mai multe detalii despre cum se ajustează aceste setări precum şi alte informaţii importante despre cele mai utilizate navigatoare web (Internet Explorer, Mozilla Firefox şi Safari din MacOSX), pot fi găsite în documentul "Securing Your Web Browser"[ii]

4.9. Pasul 9 - Aplicaţi/realizati actualizările de securitate şi activaţi actualizările automate

Majoritatea producătorilor pun la dispoziţie periodic actualizări ce repară(inlatura) vulnerabilităţi sau disfuncţionalităţi ale aplicaţiilor software. Deoarece persoanele rău intenţionate pot exploata aceste probleme pentru a ataca un calculator, actualizarea periodică a aplicaţiilor software este un pas important în prevenirea infectării.

A treia metodă prin care Conficker a atacat calculatoare a fost exploatare unei vulnerabilităţi în sistemul de operare Microsoft Windows. Microsoft a pus la dispoziţie o actualizare pentru această vulnerabilitate. Dacă toată lumea ar fi operat (realizat) actualizarea de securitate în timp util, atunci s-ar fi eliminat aproape complet una din modalităţile de atac ale Conficker şi ar fi redus substanţial numărul de calculataore infectate la nivel global.

Atunci când configurăm un calculator nou (şi după ce au fost aplicate bunele practici definite mai sus), mergeţi pe site-ul web al producătorului pentru actualizarea aplicaţiilor ce au fost livrate împreună cu calculatorul. Activaţi aplicarea/realizarea automată a actualizărilor de securitate, în cazul în care producătorul oferă această variantă; astfel vă asiguraţi că tot timpul aplicaţiile dvs. sunt cele mai recente şi nu trebuie să vă amintiţi să faceţi asta manual din când în când.

Multe sisteme de operare şi aplicaţii au posibilitatea de a face automat actualizările de securitate. Încercaţi pe cât posibil ca operaţiile de rutină efectuate la setarea unui calculator nou să includă şi activarea acestor opţiuni, acolo unde este posibil. Aveţi grijă însă, pentru că persoanele rău voitoare pot crea site-uri web care arată aproape identic cu cele originale. Descărcaţi actualizările de securitate direct de pe site-ul web al producătorului, dintr-o sursă sigură sau prin intermediul actualizărilor automate.

4.10. Pasul 10 - Utilizaţi reguli de bună practică pentru securizare

Puteţi face lucruri simple pentru a îmbunătăţi securitatea calculatorului dvs. Câteva dintre cele mai importante sunt:

- **procedaţi cu atenţie sporită în cazul ataşamentelor la email-uri sau în cazul link-urilor în care nu aveţi încredere.** Malware-ul este răspândit de obicei prin intermediul persoanelor care deschid ataşamentele email-urilor sau link-urile care produc lansarea de malware. Anumite programe de tip malware folosesc calculatoarele pe care le-au infectat pentru a trimite mai departe mesaje infectate. Chiar dacă un email poate apare ca fiind de la o persoană pe care o cunoaşteţi, este posibil ca acesta să fie de fapt trimis de către un calculator infectat. O atenţie sporită trebuie acordată ataşamentelor cu nume senzaţionale sau ieşite din comun, email-urilor care conţin greşeli evidente de gramatică sau acelor email-uri în care sunteţi invitaţi să accesaţi un link sau un ataşament (de exemplu, un email cu un subiect precum: "Hei, nu o să-ţi vină să crezi ce poză am găsit pe Internet !").
- **aveţi grijă atunci când divulgati informaţii personale sau informaţii sensibile.** Anumite email-uri sau pagini web care par a fi trimise de către surse sau persoane cunoscute pot fi de fapt trimise de către o persoană rău intenţionată. De exemplu, un email care pare a fi trimis de către administratorul de sistem şi în care sunteţi invitat să divulgaţi parola sau alte informaţii sensibile, sau un email în care sunteţi direcţionat către un site de web în care vă sunt cerute astfel de informaţii. Chiar dacă unii furnizori de servicii internet sau instituţia la care lucraţi vă pot cere să vă schimbaţi parola, niciodată nu vor solicita parola sau alte informaţii personale.
- **folosiţi parole sigure.** Parolele care au opt sau mai multe caractere, folosesc variaţii de litere mari şi litere mici şi care conţin cel puţin un simbol şi un număr, sunt cele mai sigure. Nu folosiţi parole pe care alte persoane le pot ghici cu uşurinţă, cum ar fi data de naştere sau numele copilului. Există aplicaţii de spart parole care vor încerca atacuri folosind cuvinte din dicţionar până când parola dvs este compromisă. Cu cât parola este mai lungă şi mai complicată, cu atât aceste aplicaţii vor necesita mai mult timp pentru a compromite parola. De asemenea, atunci când alegeţi întrebări de securitate, alegeţi întrebări la care răspunsul să nu poată fi găsit printr-o căutare pe Internet.

5. Cum pot afla mai multe informaţii ?

Aplicarea pașilor din acest articol îmbunătățesc semnificativ gradul de siguranță al calculatorului dvs. Cu cât implementați mai multe cu atât calculatorul va fi mai sigur. Cu toate acestea, chiar după ce ați implementat toți cei 10 pași, este posibil sa nu fiți protejat de toate riscurile ce pot apare la utilizarea unui calculator. Este foarte important să continuați să îmbunătățiți constant și periodic noi modalități de securizare pentru că zilnic apar noi riscuri iar cele vechi evoluează. Câteva resurse disponibile în cadrul US-CERT din care puteți afla mai multe informații:

- "Small Office/Home Office Router Security" (http://www.us-cert.gov/reading_room/HomeRouterSecurity2011.pdf)
- "Socializing Securely: Using Social Networking Services" (http://www.us-cert.gov/reading_room/safe_social_networking.pdf)
- "Securing Your Web Browser" (http://www.us- cert.gov/reading_room/securing_browser/)

[i] http://www.us-cert.gov/reading_room/HomeRouterSecurity2011.pdf
[ii] http://www.us-cert.gov/reading_room/securing_browser/