OUCH! | Aprilie 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Generalități**
- **Indicii asupra unui atac reușit**
- **Cum să reacționați**

Am fost victima unui atac cibernetic, acum ce-i de făcut?

Generalități

Știm că sunteți preocupați de protecția calculatorului și a dispozitivelor mobile personale și că luați măsuri pentru securizarea lor. Cu toate astea, oricât de precauți sunteți în folosirea tehnologiei, mai devreme sau mai târziu veți fi victima unui atac sau veți fi „compromiși“. În acest buletin informativ veți învăța cum să verificați dacă propriul calculator sau dispozitiv mobil a fost ținta unui atac și ce-i de făcut dacă aceasta se confirmă. În ultimă instanță, cu cât detectați mai rapid că ceva e în neregulă și cu cât reacționați mai repede, cu-atât e mai probabil ca să reduceți stricăciunile cauzate de un răufăcător.

Editor Invitat

Samantha Davison (**@sam_e_davison**) este Manager al Programului de Sensibilizare și Instruire în Securitatea Informației la compania Uber, cu angajați în peste 350 de orașe în întreaga lume.

Indicii asupra unui atac reușit

Este dificil de identificat dacă ați fost victima unui atac cibernetic, deoarece deseori nu există o singură manieră în care să vă dați seama de aceasta. Răufăcătorii lasă în schimb mai multe urme, denumite frecvent indicii. Cu cât sistemul dumneavoastră reflectă mai clar aceste indicii, cu atât crește probabilitatea de a fi fost atacat.

- Programul antivirus a generat o alertă despre o infecție a sistemului, mai ales că nu a fost capabil să șteargă sau să pună în carantină fișierele afectate.
- Pagina de start în programul de navigare pe Internet s-a schimbat în mod neașteptat sau sunt afișate pagini ale unor site-uri pe care nu ați avut intenția să le vizitați.
- Există conturi noi pe calculator sau pe dispozitivul mobil, pe care nu le-ați creat, sau programe noi pe care nu le-ați instalat sunt în execuție.
- Calculatorul sau aplicațiile se blochează frecvent, apar ideograme pentru aplicații necunoscute sau se deschid tot felul de ferestre ciudate pe ecran.
- Un program cere permisiunea pentru modificarea sistemului, deși nu instalați sau actualizați niciuna dintre aplicații în acel moment.
- Parola nu mai este validă atunci când încercați să vă autentificați pe sistem sau într-un cont online, deși sunteți siguri că este corectă.
- Prietenii vă întreabă de ce le trimiteți mesaje spam, deși știți bine că nu le-ați trimis niciun email.

Am fost victima unui atac cibernetic, acum ce-i de făcut?

- Dispozitivul mobil generează costuri neautorizate pentru folosirea de servicii SMS premium.
- Dispozitivul mobil are brusc un volum inexplicabil de mare de trafic de date sau consum excesiv al bateriei.

Mai devreme sau mai târziu calculatorul sau dispozitivul mobil personal ar putea fi compromis; cu cât depistați un incident mai repede și reacționați prompt, cu-atât mai bine.

Cum să reacționați

Dacă aveți impresia că v-a fost compromis calculatorul sau dispozitivul mobil, cu cât reacționați mai rapid, cu-atât mai bine. Dacă acesta v-a fost pus la dispoziție de către angajator sau este folosit pentru activitatea profesională, nu încercați să rezolvați problema singuri. Nu numai că puteți face mai mult rău decât bine, dar puteți distruge probe ce pot fi folosite ulterior pentru o investigație. Cel mai bine raportați imediat incidentul angajatorului, în mod normal contactând serviciul intern de asistență Helpdesk, echipa de securitate sau superiorul ierarhic. Dacă dintr-un motiv sau altul nu puteți lua legătura cu compania sau sunteți îngrijorați de o întârziere, deconectați echipamentul de la rețea și treceți-l în regim de funcționare suspendat temporar. Chiar și dacă nu aveți certitudinea unei intruziuni pe sistemul propriu, e mult mai bine să raportați acum aceasta, pentru a fi siguri. Dacă este calculatorul sau dispozitivul mobil propriu, iată câțiva pași pe care-i puteți urma:

- **Schimbați-vă parolele**: Aceasta înseamnă nu numai schimbarea parolelor pe calculatorul personal și dispozitivele mobile, dar și pentru toate conturile proprii online. Asigurați-vă că nu folosiți calculatorul compromis pentru a schimba parolele. Folosiți în schimb un alt calculator sau dispozitiv care știți că este securizat pentru schimbarea parolelor.
- **Antivirusul**: Dacă programul antivirus vă semnalează prezența unui fișier infectat, puteți urma pașii recomandați de acesta. Aceasta include în mod obișnuit includerea fișierului în carantină, curățarea sau ștergerea acestuia. Cea mai mare parte a programelor antivirus vor avea referințe online pe care le puteți urma pentru a afla mai multe detalii despre acea infecție în particular. Atunci când aveți suspiciuni, puneți fișierul în carantină. Dacă nu se poate, ștergeți-l.
- **Reinstalarea**: Dacă nu reușiți să remediați infecția sau vreți să fiți absolut siguri că sistemul este curat, o variantă mai sigură este reinstalarea acestuia. Pentru calculatoare, urmați instrucțiunile fabricantului. În majoritatea cazurilor aceasta va implica folosirea utilitarelor furnizate pentru reinstalarea sistemului de operare. Dacă aceste utilitare lipsesc, sunt compromise sau infectate, luați legătura cu furnizorul pentru îndrumare sau vizitați-le site-ul. Nu reinstalați sistemul de operare din copiile de siguranță, acestea putând avea aceleași vulnerabilități care au facilitat răufăcătorului accesul inițial. Copiile de siguranță trebuie folosite doar pentru recuperarea datelor personale. Pentru dispozitivele mobile urmați instrucțiunile fabricantului sau cele ale furnizorului de servicii de telefonie, acestea trebuie să fie disponibile pe site-urile lor. În multe cazuri e vorba doar de o restaurare a dispozitivului la configurația inițială, din fabrică. Dacă nu

Am fost victima unui atac cibernetic, acum ce-i de făcut?

vă simțiți confortabil făcând singuri reinstalarea, apelați la un service profesionist pentru a vă ajuta cu aceasta. Dacă dispozitivul mobil sau calculatorul este vechi s-ar putea să fie mai simplu și mai ieftin să cumpărați unul nou. În final, odată ce ați reinstalat sistemul sau ați cumpărat un dispozitiv nou, asigurați-vă că este complet actualizat și că ați activat funcția de actualizare automată, ori de câte ori e posibil.

- **Copiile de siguranță**: Cel mai important pas pe care-l puteți face pentru a vă proteja este să vă pregătiți din timp făcând copii de siguranță periodic. Cu cât faceți copii de siguranță mai des, cu-atât mai bine. Unele soluții vor salva automat orice fișier nou sau recent modificat la intervale de o oră. Indiferent ce soluție de creare a copiilor de siguranță folosiți, verificați la intervale regulate că puteți restaura fișierele salvate. Destul de des recuperarea datelor din copii de siguranță este singura cale prin care vă puteți restaura sistemul după un atac cibernetic reușit.
- **Acțiunea legală**: Dacă vă simțiți în vreun fel amenințați, semnalați incidentul autorităților legale locale.

Aflați mai multe

Abonați-vă la buletinul informativ lunar OUCH!, accesați arhiva și aflați mai multe despre programele de instruire asupra domeniului securității informației vizitând pagina web SANS http://www.securingthehuman.org

Versiunea în limba română

Grupul Cegeka este un furnizor privat de servicii IT&C fondat în 1992. Având sediul central în Belgia, Cegeka este prezentă în Austria, Republica Cehă, Franța, Germania, Italia, Luxemburg, Olanda, România și Republica Slovacă. Compania furnizează servicii clienților din întreaga Europă: soluții Cloud pentru companii, servicii de securitate, dezvoltare de aplicații folosind tehnicile Agile, mentorat în metodologii Agile și externalizarea infrastructurii IT&C. Cegeka are 3200 de angajați și a realizat o cifră de afaceri combinată de 330 milioane euro în 2013. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Copiile de siguranță:	https://securingthehuman.sans.org/ouch/2015#august2015
Propoziții-parolă:	https://securingthehuman.sans.org/ouch/2015#april2015
Ce sunt programele malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Securizarea tabletei:	https://securingthehuman.sans.org/ouch/2016#january2016

Echipa editorială: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Traducere: Cosmin Hănulescu