OUCH! | Octombrie 2014

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- Generalități
- Cinci elemente de bază

Cinci elemente de bază pentru păstrarea securității

Generalități

Pe măsură ce tehnologia capătă un rol mai proeminent în viețile noastre, crește, de asemenea, și în complexitate. Ritmul în care aceasta evoluează poate fi o sursă de confuzie atunci când încercăm să păstrăm pasul cu recomandările de securitate. Se pare că există în permanență noi sfaturi privitoare la ce e sau nu de făcut. Cu toate astea, în timp ce detaliile pot să se schimbe, există câteva lucruri fundamentale pe care le putem face pentru a ne proteja. Indiferent de tehnologia sau locul unde aceasta este folosită, recomandăm urmarea celor cinci elemente de bază de mai jos.

Editor Invitat

Lenny Zeltser se concentrează pe asigurarea securității clienților la NCR Corp și predă tehnici de combatere a programelor malware în cadrul SANS Institute. Lenny este activ pe Twitter la **@lennyzeltser** și scrie despre securitatea informației pe blogul său **blog.zeltser.com**.

Cinci elemente de bază

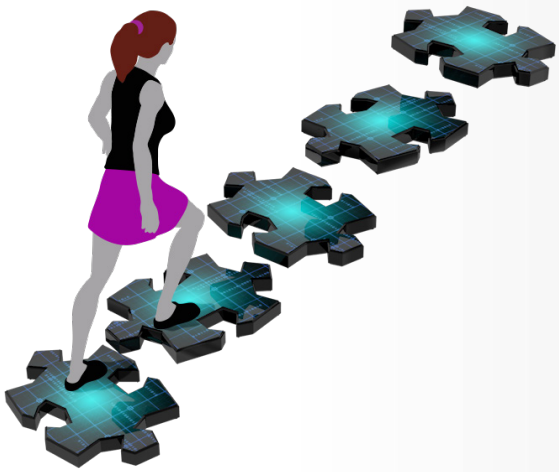
Fiecare dintre cele cinci elemente de mai jos sunt descrise sumar. Pentru a afla mai multe despre fiecare în parte consultați secțiunea Resurse suplimentare de la sfârșitul acestui buletin informativ.

1. **Dumneavoastră**: În primul rând și înainte de toate, rețineți că tehnologia singură nu vă poate proteja. Răuvoitorii au realizat că cel mai ușor mod de a ocoli majoritatea tehnologiilor de protecție este atacându-vă direct. Dacă vor să vă afle parola sau numărul cardului de credit atunci cel mai simplu le este să vă determine, păcălindu-vă, să le dați Dumneavoastră aceste informații. De exemplu, vă sună pretinzând că sunt de la serviciul de asistență Microsoft, susținând că aveți calculatorul infectat, când de fapt ei sunt niște escroci care urmăresc să le dați acces la calculator. Sau poate vă trimit un mesaj email în care spun că nu vi se poate livra un colet și că trebuie să dați clic pe o anumită adresă Web, când în realitate ei urmăresc să vă determine să vizitați un site cu malware care va infecta calculatorul Dumneavoastră. În ultimă instanță, cea mai bună defensivă în fața răufăcătorilor sunteți Dumneavoastră. Fiți suspicioși, căci simțul realității ajută la depistarea și stoparea majorității atacurilor.

2. **Actualizarea**: Asigurați-vă că toate calculatoarele, dispozitivele mobile, aplicațiile și tot ce este conectat la o rețea rulează cele mai recente versiuni de software. Răufăcătorii caută în permanență vulnerabilități în tehnologiile pe care le folosiți. Atunci când descoperă o slăbiciune folosesc programe special concepute să exploateze acea vulnerabilitate pentru a pătrunde în rețeaua, calculatorul sau dispozitivul mobil pe care-l aveți, indiferent ce tehnologie folosește. În paralel, companiile care au conceput tehnologiile pe care le folosiți se străduie să le actualizeze. Odată ce o vulnerabilitate este depistată ei dezvoltă o actualizare ce o înlătură și fac publică această actualizare. Asigurându-vă că propriile

Cinci elemente de bază pentru păstrarea securității

calculatoare și dispozitive mobile au aceste actualizări reduceți numărul de vulnerabilități cunoscute, făcând astfel mult mai dificil accesul răufăcătorilor. Pentru a fi la zi, activați opțiunea de actualizare automată, ori de câte ori e posibil. Această regulă este aplicabilă pentru aproape orice tehnologie conectată la o rețea, incluzând televizoarele conectate la Internet, sistemele de monitorizare a copiilor, echipamentele domestice de dirijare a traficului de rețea, consolele pentru jocuri electronice și, într-o bună zi, cel mai probabil că și autoturismul personal. Dacă sistemul de operare a calculatorului personal, dispozitivul mobil sau orice altă tehnologie pe care o folosiți nu mai beneficiază de suportul producătorului și nu va mai primi actualizări atunci recomandăm să le înlocuiți cu modele mai noi care sunt în garanție.



Urmând acești cinci pași esențiali veți fi într-o mai mare măsură protejați, în timp ce profitați de avantajele celei mai noi tehnologii.

3. **Parolele**: Următorul lucru pe care trebuie să-l faceți pentru a vă proteja este folosirea de parole puternice, unice, pentru fiecare dintre dispozitivele, conturile online sau aplicațiile folosite. Cuvintele cheie aici sunt *puternic* și *unic*. O parolă puternică înseamnă că aceasta nu poate fi ghicită de răufăcători sau de către programele lor. În locul unui singur cuvânt folosiți o frază lungă, formată din mai multe cuvinte, împănată cu numere și caractere speciale pentru mau multă complexitate. Unic înseamnă folosirea de parole diferite pentru fiecare dispozitiv sau cont online. Astfel, dacă o parolă este compromisă, celelalte conturi și dispozitive vor fi neafectate. Nu puteți memora toate aceste parole complexe și unice? Nu vă îngrijorați, nici noi. Acesta este motivul pentru care vă recomandăm folosirea unui program de gestiune a parolelor, adică o aplicație dedicată pentru smartphone sau calculator personal care stochează în siguranță toate parolele într-un format criptat. În final, dacă oricare dintre conturile folosite oferă posibilitatea autentificării în doi pași, recomandăm insistent activarea permanentă a acestui mecanism deoarece este una dintre cele mai sigure căi de protecție a contului.

4. **Criptarea**: Un al treilea element de protecție pe care-l recomandăm este criptarea. Criptarea garantează accesul la informație numai pentru Dumneavoastră și persoanele de încredere. Datele pot fi criptate în două stadii: stocate fiind sau în tranzit. Criptarea datelor stocate înseamnă protejarea acestora atunci când sunt salvate sub formă de fișiere pe un disc fix sau un dispozitiv mobil de stocare conectat prin USB. Majoritatea sistemelor de operare permit criptarea automată a tuturor datelor folosind facilități cum ar fi Criptarea Exhaustivă a Discului (Full Disk Encryption). Vă recomandăm să activați această funcție dacă este posibil. Criptarea datelor în tranzit înseamnă criptarea acestora atunci când sunt transmise de la calculatorul propriu la altele, ca atunci când faceți operațiuni bancare online. O modalitate simplă de verificare este să vă asigurați că atunci când accesați un site adresa acestuia începe cu „https“ și că alături de aceasta apare o ideogramă cu un lacăt încuiat.

Cinci elemente de bază pentru păstrarea securității

5. **Copiile de siguranță**: Uneori, oricât de atenți sunteți, unul dintre dispozitivele sau conturile proprii poate fi compromis. Dacă se întâmplă asta, adesea singura opțiune pentru a scăpa de malware este să ștergeți complet conținutul dispozitivului și să îl reinițializați. Atacatorul ar putea chiar să vă blocheze accesul la datele personale, fotografii sau alte informații stocate pe sistemul compromis. Singura opțiune pe care ați putea-o avea la dispoziție este să recuperați toate datele personale dintr-o copie de siguranță. Asigurați-vă că faceți copii de siguranță cu regularitate pentru orice informație importantă și verificați că le puteți recupera. Majoritatea sistemelor de operare și a dispozitivelor mobile permit crearea automată a copiilor de siguranță.

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

Cegeka este o companie de servicii IT integrate cu peste 2100 de angajați, prezentă în Benelux, Franța, Polonia și România. Clienții beneficiază de consultanță, dezvoltare de software și aplicații Web, administrarea infrastructurii IT la distanță sau la sediile proprii, sau servicii de externalizare complexe. Având propriile centre de date moderne, Cegeka deține expertiza și tehnologiile ce garantează agilitatea și inovația necesare rezolvării celor mai complexe cerințe ale clienților. Pentru mai multe informații accesați www.cegeka.com sau urmăriți-ne pe Twitter @cegeka

Resurse suplimentare

Despre atacurile de tip phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Despre securitatea tabletelor:	http://www.securingthehuman.org/ouch/2013#december2013
Despre parolele puternice:	http://www.securingthehuman.org/ouch/2013#may2013
Despre programele de gestiune a parolelor:	http://www.securingthehuman.org/ouch/2013#october2013
Despre autentificarea în doi pași:	http://www.securingthehuman.org/ouch/2013#august2013
Despre criptare:	http://www.securingthehuman.org/ouch/2014#august2014
Despre copiile de siguranță:	http://www.securingthehuman.org/ouch/2013#september2013

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