OUCH! | Octombrie 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- Tu
- Parole
- Actualizări
- Copii de siguranță

Patru pași pentru a rămâne în siguranță

Prezentare generală

Pe măsură ce tehnologia capătă un rol din ce în ce mai important în viețile noastre, aceasta crește și în complexitate. Gândindu-ne la cât de repede se schimbă tehnologia, menținerea unui nivel permanent actualizat al consultanței privind securitatea poate crea confuzii. Par să existe mereu noi și noi indicații cu privire la ce trebuie sau nu trebuie să faci. Chiar dacă detaliile modului în care poți rămâne în siguranță se pot schimba în timp, există unele lucruri fundamentale care se pot face pentru a fi protejat. Indiferent ce tehnologie folosești sau unde te afli atunci când o folosești, noi recomandăm următorii patru pași cheie. Petru a afla mai multe despre fiecare dintre pașii de mai jos, consultați secțiunea Resurse, de la sfârșitul acestui articol.

Editor Invitat

Ryan Johnson își concentrează activitatea pe pregătirea organizațiilor pentru a răspunde breșelor de securitate inevitabile, predă cursul Advanced Network Forensics la Institutul SANS și este activ pe Twitter cu numele de utilizator **@ForensicRJ**.

1. **Tu**: Mai presus de toate trebuie să ții minte că tehnologia în sine nu va putea să te protejeze în totalitate. Atacatorii au învățat că cel mai simplu mod de a trece și de cea mai avansată tehnologie de securitate este să te atace pe tine. Dacă îți vor parola, datele personale sau ale cardului de credit, cel mai ușor lucru pentru ei este să te păcălească să le dai tu însuți aceste informații. De exemplu, te pot suna pretinzând că sunt de la departamentul de suport tehnic Microsoft să îți spună că ți s-a infectat computerul când, în realitate sunt doar infractori care vor ca tu să le dai acces la computer. Sau îți pot trimite un email în care să explice că pachetul pe care l-ai comandat nu poate fi livrat și să îți ceară să accesezi un anume site pentru a confirma adresa poștală, când, de fapt vor să te păcălească să accesezi un site infectat care îți va compromite securitatea calculatorului personal. Așa încep atacurile de tip ransomware sau CEO: în ultimă instanță, cea mai bună apărare împotriva atacatorilor ești tu însuți. Fii suspicios. Dacă îți folosești logica poți identifica și opri majoritatea atacurilor.

2. **Parole**: Următorul pas în a te proteja implică folosirea unei parole puternice și unice pentru fiecare dintre computerele, telefoanele și conturile online pe care le deții. Cuvintele cheie aici sunt *puternică* și *unică*. O parolă puternică înseamnă o parolă care nu poate fi ghicită ușor de atacatori sau de programele lor automate. Ai obosit de atâtea parole complicate, greu de ținut minte și complicat de tastat? Încearcă să folosești o propoziție-parolă. În locul unui singur

Patru pași pentru a rămâne în siguranță

cuvânt complex folosește o serie de cuvinte care va fi ușor de rememorat, cum ar fi „Unde îmi e cafeaua?“ Cu cât propoziția-parolă va fi mai lungă, cu atât va fi mai puternică. O parolă unică înseamnă folosirea unei parole diferite pentru fiecare computer, telefon sau cont online. În acest fel, dacă una dintre parole este compromisă, toate celelalte conturi și dispozitive vor rămâne în siguranță. Nu îți poți aminti toate acele parole puternice și unice? Nu îți face griji, nici noi nu ne facem. De aceea și recomandăm folosirea unui program de gestiune a parolelor, care este o aplicație specializată pentru mobil sau computer, ce poate stoca toate parolele într-un format criptat.

Prin urmarea acestor patru pași cheie, vei face mult pentru a te proteja, folosind cea mai recentă tehnologie.

În final, unul dintre cei mai importanți pași pe care îi poți face pentru a îți proteja orice cont este activarea unei verificări în doi pași. Parolele sigure nu mai sunt suficiente pentru a proteja conturile, toți avem nevoie de ceva mai puternic. Verificarea în doi pași este mult mai puternică. Aceasta folosește parola dar adaugă și un al doilea pas, fie ceva ce ține de ce/cine ești (biometrică), fie ceva ce deții (cum ar fi un cod trimis către telefonul inteligent sau o aplicație pe telefon care îți generează acest cod). Selectează această opțiune pentru fiecare cont la care o poți face, inclusiv la programul de gestiune a parolelor, dacă este posibil. Verificarea în doi pași este probabil singurul pas cel mai important pe care îl poți face pentru a te proteja și este mult mai ușor decât ai crede.

3. **Actualizare**: Asigură-te că toate computerele, telefoanele, aplicațiile și orice altceva conectat la Internet utilizează cea mai recentă versiune de software. Răufăcătorii caută întotdeauna noi vulnerabilități în programele folosite de echipamentele tale. Atunci când descoperă vulnerabilități, folosesc programe speciale pentru a le exploata și a pătrunde în sistemul pe care îl folosești. În acest timp, companiile care au creat programele pentru acel dispozitiv lucrează din greu să acopere respectivele vulnerabilități prin lansarea de actualizări. Dacă te asiguri că telefoanele mobile și computerele tale își instalează ultimele actualizări, va fi mult mai greu ca unui infractor să îi reușească un atac. Pentru a fi întotdeauna la zi, selectează opțiunea de actualizare automată oriunde este posibil. Această regulă se aplică aproape tuturor tehnologiilor conectate la o rețea, inclusiv televizoarelor conectate la Internet, monitoarelor pentru bebeluși, echipamentele de rețea casnice, consolelor de jocuri și, poate într-o zi, chiar propriei tale mașini. Dacă sistemele de operare sau unitățile sunt vechi și nu mai pot ține pasul cu actualizările de securitate, recomandăm înlocuirea lor cu unele care pot suporta aceste actualizări.

Patru pași pentru a rămâne în siguranță

4. **Copiile de siguranță**: Uneori, indiferent cât de atent ești, un atac poate reuși. Dacă se întâmplă asta, de multe ori, singura soluție pentru a te asigura că dispozitivul mobil sau computerul nu mai conțin malware este ștergerea completă și reinstalarea de la zero a sistemului de operare. Atacatorul te poate chiar împiedica să îți accesezi fișierele personale, pozele sau alte informații stocate pe sistemul atacat. De multe ori, singura cale de a îți recupera datele, este din copia de siguranță. Asigură-te că îți faci în mod regulat copii de siguranță ale informațiilor importante și verifică dacă acestea pot fi recuperate din acele copii. Majoritatea sistemelor de operare și dispozitivelor mobile suportă copiile de siguranță automate. În plus, recomandăm păstrarea acestor copii de siguranță fie în Cloud, fie offline, pentru le proteja împotriva atacatorilor cibernetici.

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 securingthehuman.sans.org/ouch/archives

Versiunea în limba română

Cegeka este un furnizor independent de servicii IT&C ce își ajută clienții din întreaga Europă în transformarea lor digitală, dezvoltarea de aplicații folosind metodologiile Agile, soluții de încredere de tip Cloud și managementul serviciilor 24/7. Cegeka este prezentă în Austria, Belgia, Republica Cehă, Franța, Germania, Italia, Olanda, Polonia, România și Republica Slovacă, având 3600 de angajați. Cegeka a realizat o cifră de afaceri de 368 milioane de euro în 2015. Pentru mai multe informații vizitați www.cegeka.com.

Resurse

Despre Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Despre programele de gestiune a parolelor:	https://securingthehuman.sans.org/ouch/2015#october2015
Verificarea în doi pași:	https://securingthehuman.sans.org/ouch/2015#september2015
Propoziții parolă:	https://securingthehuman.sans.org/ouch/2015#april2015
Despre copiile de siguranță:	https://securingthehuman.sans.org/ouch/2015#august2015

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