OUCH! | Februarie 2015

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Verificări preliminare**
- **Dispozitive pierdute sau furate**
- **Accesul wireless**
- **Calculatoare cu acces public**

Securitatea lucrului la distanță în deplasare

Introducere

În acest buletin informativ vom vedea cum vă puteți conecta în siguranță la Internet pentru a putea lucra la distanță când sunteți în deplasare.

Editor Invitat

Steve Armstrong director tehnic la CyberCPR și Logically Secure, instructor certificat și autor de cursuri SANS. Este activ pe Twitter la **@Nebulator** și pe Google Plus: **+SteveArmstrongSecurity**.

Verificări preliminare

Dacă rețelele de-acasă sau de la serviciu pot fi considerate sigure, atunci când călătoriți trebuie să considerați orice rețea la care vă conectați ca fiind lipsită de siguranță. Nu puteți ști cine mai este conectat în același timp și ce pericole comportă asta. Câteva verificări prealabile, înainte de plecare, pot asigura protecția datelor personale în deplasare. Astfel, cu o săptămână sau două înainte de călătorie:

- Identificați datele de care nu aveți nevoie pe dispozitivele pe care le luați cu dumneavoastră și ștergeți-le pe cele care nu sunt necesare. Aceasta ajută semnificativ la reducerea impactului pe care-l poate avea pierderea dispozitivelor, furtul sau reținerea lor la controalele de securitate vamale. Dacă veți călători în interes de serviciu, întrebați-vă superiorii dacă se impune folosirea de echipamente special alocate pentru lucrul în deplasare.
- Atunci când călătoriți în altă țară, verificați tipul surselor de alimentare cu electricitate specifice țării respective, pentru că va fi necesar să vă luați adaptoare pentru reîncărcarea dispozitivelor. Suplimentar, verificați cu furnizorul de servicii de telecomunicații planul tarifar pe care-l aveți. Adesea furnizorii facturează la prețuri mai mari traficul de date folosit internațional, astfel că ați putea vrea să dezactivați accesul de date pe mobil atunci când călătoriți în altă țară sau să vă modificați planul tarifar când sunteți plecați.
- Instalați un program de monitorizare pentru a urmări locul unde se află dispozitivele mobile, sau chiar pentru a putea șterge de la distanță datele stocate, în caz că sunt pierdute sau furate. Majoritate dispozitivelor mobile au deja această funcționalitate inclusă, rămâne doar s-o activați (rețineți că acestea au nevoie de conectivitate Internet pentru a funcționa).

Cu o zi-două înainte de plecare:

- Actualizați-vă dispozitivele, aplicațiile și programele antivirus, ca să fiți siguri că folosiți cea mai recentă versiune a acestora.
- Activați funcțiile de protecție corespunzătoare, cum ar fi aplicațiile de tip firewall.

Securitatea lucrului la distanță în deplasare

- Blocați-vă dispozitivele mobile folosind parole puternice. În acest fel, dacă pierdeți vreun dispozitiv sau vă este furat, altcineva nu va putea să acceseze informațiile conținute.
- Criptați datele astfel încât dacă dispozitivele sunt pierdute să nu poată fi accesate. Unele dispozitive, cum ar fi iPhone, fac asta automat, odată ce ați configurat o parolă de acces.
- Faceți copii de siguranță ale datelor de pe aceste dispozitive. În felul acesta, dacă se întâmplă ceva cât sunteți în deplasare, aveți toate datele salvate la loc sigur.

Esențial pentru păstrarea securității atunci când lucrați în deplasare este să vă securizați dispozitivele înainte de plecare, să le păstrați în siguranță și să știți permanent unde se află și să criptați toate activitățile online.

Dispozitive pierdute sau furate

Odată plecați în călătorie, asigurați-vă de protecția fizică a dispozitivelor personale. Spre exemplu, nu le lăsați niciodată la vedere în mașină, deoarece infractorii pot sparge mașina ca să fure orice găsesc valoros. O variantă este să folosiți un cablu de siguranță cu care să legați calculatorul portabil atunci când îl lăsați nesupravegheat. Deși infracțiunile reprezintă un risc deloc de neglijat, s-ar putea să nu vă dați seama că e mult mai probabil să pierdeți un dispozitiv mai degrabă decât să vă fie furat. Potrivit unui studiu efectuat de compania Verizon pe un interval de zece ani, probabilitatea ca un dispozitiv să fie pierdut este de 15 ori mai mare decât cea de a fi furat. Aceasta înseamnă că trebuie să verificați de fiecare dată că aveți toate echipamentele atunci când călătoriți, cum ar fi atunci când treceți punctele de control la aeroport, când coborâți din taxi sau plecați dintr-un restaurant sau când părăsiți camera de hotel ocupată ori când coborâți din avion.

Accesul wireless

Accesarea Internetului atunci când călătoriți implică adesea folosirea punctelor de acces public wireless, cum ar fi cele din hoteluri, cafenele sau aeroporturi. Problema cu aceste puncte de acces wireless destinate publicului e nu numai că nu știm niciodată cine le-a configurat, dar nu știm nici cine este simultan conectat la ele. În consecință, nu trebuie să fie considerate de încredere căci, de altfel, acesta este motivul pentru care ați parcurs toți pașii pregătitori descriși mai sus, pentru securizarea dispozitivelor proprii înainte de plecare. De asemenea, accesul wireless folosește undele radio pentru comunicația dintre dispozitivele proprii și punctul de acces. Astfel, oricine se află în proximitatea dumneavoastră ar putea intercepta și monitoriza această comunicație.

Acesta este motivul pentru care, dacă folosiți puncte de acces wireless publice, trebuie să vă asigurați că traficul de date făcut este criptat. De exemplu, atunci când vă conectați la un website, verificați dacă conexiunea este criptată (adresa începe cu https:// și este afișat simbolul unui lacăt încuiat în dreptul ei). Suplimentar, ați putea avea deja un cont de acces VPN (Virtual Private Network — rețea privată de date peste Internet) care permite accesul criptat pentru toată activitatea

Securitatea lucrului la distanță în deplasare

online. Acesta poate v-a fost pus la dispoziție de la serviciu sau puteți achiziționa un serviciu VPN pentru uz personal. Dacă aveți rețineri legate de accesare unui punct de acces wireless public, atunci puteți lua în considerare folosirea unui smarphone ca mijloc de acces la Internet. (Atenție! Așa cum am menționat deja, aceasta poate avea costuri însemnate atunci când călătoriți în altă țară, așa că verificați cu furnizorul dumneavoastră înainte de plecare).

Calculatoare cu acces public

Nu folosiți calculatoare cu acces public, cum ar fi cele din holurile hotelurilor, biblioteci sau cafenele Internet. Nu aveți de unde ști cine a folosit calculatorul înaintea dumneavoastră și dacă l-a infectat, accidental sau voit. Ori de câte ori e posibil, folosiți numai dispozitivele asupra cărora aveți control şi sunt de încredere pentru activitatea online. Dacă trebuie să folosiți un calculator public, nu accesați servicii care necesită autentificare sau cer parole de acces.

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

Despre parole:	http://www.securingthehuman.org/ouch/2013#may2013
Verificări în doi pași:	http://www.securingthehuman.org/ouch/2013#august2013
Despre criptare:	http://www.securingthehuman.org/ouch/2014#august2014
Securizarea tabletei nou cumpărate:	http://www.securingthehuman.org/ouch/2013#december2013

Raportul de investigație Verizon despre incidentele de securitatea datelor pe 2014:
http://www.verizonenterprise.com/DBIR/2014/

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