OUCH! | Februarie, 2017

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

Vă dorim să beneficiați pe deplin de tehnologii tot timpul, inclusiv atunci când călătoriți. În acest buletin informativ discutăm cum vă puteți conecta la Internet și cum vă puteți folosi dispozitivele într-o manieră securizată atunci când sunteți în deplasare.

Editor Invitat

Mark Williams este Enterprise Security Architect la compania BlueCross Blueshield din Tennessee. El este de asemenea instructor SANS și președintele filialei ISSA din Chattanooga. A călătorit mult și înțelege problemele întâlnite atunci când e în deplasare însoțit de tot felul de dispozitive hi-tech.

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 ar putea face. Iată câteva măsuri de securitate simple cu un efect foarte bun asupra protecției dumneavoastră și a datelor personale, înainte de plecarea în călătorie:

- Cea mai sigură informație e cea pe care nu o aveți. Identificați datele de care nu aveți nevoie pe dispozitivele pe care le luați cu dumneavoastră și ștergeți-le. 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 superiorul ierarhic dacă sunt disponibile echipamente special alocate pentru lucrul în deplasare.
- Blocați-vă dispozitivele mobile folosind parole sau coduri de acces puternice. În acest fel, dacă pierdeți vreun dispozitiv sau vă este furat, altcineva nu va putea să acceseze informațiile conținute. În plus, activați sau instalați un program de criptare a datelor de pe dispozitivele mobile sau calculatoarele portabile. Pentru majoritatea lor aceasta este activată atunci când folosiți funcția de blocare a ecranului.
- Instalați un program de monitorizare pentru a urmări locul unde se află dispozitivul dumneavoastră mobil, sau chiar pentru a putea șterge de la distanță datele stocate, în caz că s-a pierdut sau a fost furat.
- Actualizați-vă dispozitivele, aplicațiile și programele antivirus înainte de plecare, ca să fiți siguri că folosiți cea mai recentă versiune a acestora. Multe atacuri se concentrează asupra sistemelor ce au programe neactualizate.
- 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.
- Atunci când călătoriți în altă țară, verificați cu furnizorul de servicii de telecomunicații planul tarifar pe care-l aveți.

© SANS Institute 2017

Securitatea lucrului la distanță în deplasare

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 cumpărați la fața locului o cartelă SIM preplătită.

Pentru a vă păstra securitatea atunci când călătoriți, protejați-vă dispozitivele înainte de plecare, țineți-le în siguranță și criptați toată activitatea 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 răufăcătorii pot sparge geamul ca să fure orice obiect de valoare găsit. Deși infracțiunile reprezintă un risc deloc de neglijat, un studiu realizat recent de compania Verizon relevă că există o probabilitate de 100 de ori mai mare ca să pierdeți un dispozitiv mai degrabă decât să vă fie furat. Aceasta înseamnă că trebuie să verificați de fiecare dată că încă 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. Nu uitați să verificați buzunarul scaunului din față, în 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. Sunt două probleme cu aceste puncte de acces public wireless: nu știm niciodată cine le-a configurat și nu știm nici cine este conectat la ele. Prin urmare, nu trebuie să fie considerate de încredere. De fapt ăsta e și motivul pentru care ați luat măsurile de securitate de mai sus, înainte de plecare. În plus, accesul wireless folosește undele radio pentru comunicație, deci oricine se află în proximitatea dumneavoastră ar putea intercepta și monitoriza această comunicație. Din aceste motive, 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 site web, verificați dacă conexiunea este criptată. Puteți verifica asta dacă 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 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 luat 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 mai întâi.

© SANS Institute 2017

Securitatea lucrului la distanță în deplasare

Calculatoare cu acces public

Nu folosiți calculatoare cu acces public, cum ar fi cele din holurile hotelurilor sau cafenele Internet pentru a vă accesa contul și informații personale sensibile. Nu aveți de unde ști cine a folosit calculatorul înaintea dumneavoastră și dacă l-au infectat, accidental sau voit. Ori de câte ori e posibil, folosiți numai dispozitivele asupra cărora aveți control și sunt de încredere. În cel mai bun caz, calculatoarele cu acces public sunt utile pentru accesare de informații publice, cum ar fi prognoza meteo sau ultimele știri. Autentificarea în orice cont, cum ar fi cel personal Google, pot fi o invitație pentru răufăcătorii care ar putea în acest timp să stea la pândă.

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

Propoziții-parolă:	https://securingthehuman.sans.org/ouch/2015#april2015
Copiile de siguranță:	https://securingthehuman.sans.org/ouch/2015#august2015
Despre Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Criptarea:	https://securingthehuman.sans.org/ouch/2016#june2016
Arhiva buletinelor informative OUCH:	https://securingthehuman.sans.org/ouch/archives

OUCH! este publicat de SANS, Securing The Human și distribuit sub licența Creative Commons BY-NC-ND, versiunea 4.
Sunteți liberi să distribuiți acest buletin informativ sau să-l folosiți în programele de instruire proprii atât timp cât nu-i modificați conținutul.
Pentru traduceri sau informații suplimentare scrieți la ouch@securingthehuman.org

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