OUCH! | Noiembrie 2016

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Generalități**
- **Alegerea furnizorului de servicii Cloud**
- **Securizarea datelor proprii**

Utilizarea securizată a serviciilor Cloud

Generalități

„Cloud“ poate desemna lucruri diferite pentru persoane diferite, dar în mod uzual acesta înseamnă folosirea unui furnizor de servicii prin Internet pentru stocarea și administrarea sistemelor de calcul și / sau a datelor în numele dumneavoastră. Un avantaj al serviciilor Cloud este acela că puteți accesa și sincroniza datele proprii de pe mai multe dispozitive oriunde în lume și că puteți de asemenea partaja informațiile cu oricine doriți. Numim aceste servicii „Cloud“ pentru că deseori nu știți unde sunt stocate fizic datele. Exemple de servicii Cloud includ crearea de documente folosind Google Docs, partajarea fișierelor prin intermediul Dropbox, configurarea unui server propriu pe platforma Amazon Cloud, stocarea datelor clienților folosind Salesfore sau arhivarea muzicii sau fotografiilor personale folosind serviciul Apple iCloud. Aceste servicii online vă pot face mult mai productiv, dar ele sunt însoțite de anumite riscuri specifice. În acest buletin informativ vom vedea cum puteți beneficia la maxim de serviciile Cloud într-un mod securizat.

Editor Invitat

Dave Shackleford (**@daveshackleford**) este un consultant profesionist, deținătorul Voodoo Security și autor a numeroase cursuri SANS, printre care se numără SANS Security 579: Virtualizarea și Securitatea Serviciilor Cloud Private și Security 524: Fundamentele Securității Serviciilor Cloud.

Alegerea furnizorului de servicii Cloud

Serviciile Cloud nu sunt nici bune nici rele, ele sunt o unealtă menită să servească pentru realizarea multor lucruri, atât la serviciu cât și acasă. Cu toate astea, atunci când folosiți aceste servicii vă puneți datele personale la dispoziția altora și vă așteptați ca aceștia să le păstreze în siguranță și accesibile. În consecință, vreți să fiți siguri că vă alegeți furnizorul de servicii cu înțelepciune. În cazul calculatoarelor de la serviciu și a informațiilor legate de acesta, întrebați superiorul ierarhic pentru a vedea dacă vă este permisă în companie folosirea serviciilor Cloud. Dacă vă este permisă folosirea serviciilor Cloud, confirmați tipul de servicii Cloud pe care le puteți folosi și care sunt politicile privitoare la utilizarea acestora. Dacă luați în calcul folosirea unui serviciu Cloud pentru nevoi personale, țineți cont de următoarele:

1. **Asistență**. Cât de ușor puteți obține asistență sau răspuns la o întrebare? Există o adresă de email pentru contact, grupuri de discuții publice în care puteți formula întrebări sau o listă de Întrebări și Răspunsuri Frecvente pe site-ul furnizorului?
2. **Simplitate**. Cât de ușor de folosit este serviciul? Cu cât serviciul este mai complex, cu atât mai probabil este să faceți greșeli, să expuneți sau să pierdeți accidental informațiile proprii. Alegeți un furnizor ale cărui servicii Cloud le găsiți ușor de înțeles, de configurat și de folosit.

Utilizarea securizată a serviciilor Cloud

3. **Securitate**. Ce date personale despre dumneavoastră sunt colectate, dacă este cazul? Cum ajung datele personale de pe calculatorul propriu pe platforma de servicii Cloud și cum sunt stocate acolo; sunt criptate și, dacă așa e, cine le poate decripta?
4. **Condiții de furnizare a serviciilor**. Luați-vă un răgaz de timp pentru a parcurge Condițiile de furnizare a serviciilor (acestea sunt deseori surprinzător de ușor de citit). Confirmați cine poate avea acces la datele dumneavoastră și care sunt drepturile legale pe care le aveți cât și responsabilitățile privind securitatea ce revin furnizorului sau dumneavoastră.

Serviciile Cloud pot face informațiile personale mult mai ușor accesibile și pe dumneavoastră mai productivi, dar fiți atenți cum accesați și partajați aceste informații.

Securizarea datelor proprii

Odată ce ați ales un furnizor de servicii Cloud, următorul pas este să vă asigurați că folosiți corect serviciile acestuia. Modul cum accesați și partajați datele proprii poate uneori avea un impact mult mai mare decât orice altceva asupra fișierelor personale. Câțiva pași importanți pe care-i puteți parcurge includ:

1. **Autentificarea**: Folosiți propoziții-parolă unice, puternice, pentru a vă autentifica în propriul cont Cloud.
2. **Partajarea de fișiere / cataloage de fișiere**: Serviciile Cloud fac foarte ușoară partajarea, uneori chiar prea simplă. În cel mai rău caz puteți avea convingerea că partajați fișierele cu o persoană anume când, accidental, puteți face accesibile oricui e conectat la Internet fișierele sau chiar cataloage întregi de fișiere personale. Cel mai bun mod în care vă puteți proteja este să nu partajați niciun fișier cu nimeni în mod implicit. Permiteți apoi numai anumitor persoane (sau grupuri de persoane) accesul la fișiere specifice sau cataloage de fișiere în baza unei nevoi reale de acces la ele. Atunci când cineva nu mai are nevoie să acceseze fișierele, revocați accesul. Furnizorul serviciilor Cloud trebuie să ofere un mecanism facil de urmărire a accesului la fișierele și cataloagele de fișiere personale.
3. **Partajarea de fișiere sau cataloage de fișiere folosind adrese web**. O funcționalitate frecvent oferită de unele servicii Cloud este abilitatea de a crea o adresă web care trimite la fișierele sau cataloagele de fișiere proprii. Această funcționalitate vă permite să partajați fișiere cu oricine doriți prin simpla trimitere a respectivei adrese web. Cu toate astea, abordarea aceasta oferă foarte puțină protecție, oricine știe adresa putând avea acces la fișierele și cataloagele dumneavoastră de fișiere. Dacă trimiteți această adresă unei anumite persoane, această persoană poate să o trimită altora, sau adresa poate apărea în rezultatele unui motor de căutare online. Dacă partajați date folosind o adresă asigurați-vă că o dezactivați atunci când nu mai e necesară configurând un termen de valabilitate sau, dacă se poate, protejând-o cu o parolă.

Utilizarea securizată a serviciilor Cloud

4. **Parametri de configurare**. Înțelegeți parametrii de configurare a securității puși la dispoziția dumneavoastră de furnizorul serviciilor Cloud. De exemplu, dacă partajați un catalog de fișiere cu cineva, pot aceștia partaja la rândul lor datele cu altcineva fără știința dumneavoastră? De asemenea, vedeți dacă există mecanisme ce vă permit să vedeți cine și când a accesat datele pe care le-ați partajat. Puteți restricționa accesul la simpla vizualizare, în loc să permiteți drepturi de citire și scriere, ceea ce înseamnă că alții pot să și modifice fișierele?
5. **Programe antivirus**. Asigurați-vă că cea mai recentă versiune de program antivirus este instalată pe calculatorul personal sau orice alt calculator folosit pentru accesarea și partajarea datelor personale. Dacă un fișier pe care-l partajați este compromis, alte calculatoare care accesează același fișier pot de asemenea să fie infectate.

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

Verificarea în doi pași:	https://securingthehuman.sans.org/ouch/2015#september2015
Propoziții-parolă:	https://securingthehuman.sans.org/ouch/2015#april2015
Programe de gestiune a parolelor:	https://securingthehuman.sans.org/ouch/2015#october2015
Ce sunt programele malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Cursul SANS SEC524: Fundamentele securității serviciilor Cloud:	https://sans.org/sec524

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