OUCH! | Septembrie 2014

Buletinul informativ lunar de sensibilizare asupra securității pentru utilizatorii de calculatoare

OUCH!

În această ediție…

- **Generalități**
- **Alegerea unui ofertant de servicii Cloud**
- **Securizarea datelor**

Utilizarea în siguranță a tehnologiei Cloud

Generalități

Tehnologia Cloud este o tehnologie puternică pe care atât companiile cât și persoanele private o adoptă rapid. „Cloud“ poate însemna lucruri diferite pentru persoane diferite, dar în esență este vorba de utilizarea unui ofertant de servicii prin Internet pentru stocarea și administrarea datelor proprii. Unul dintre avantajele tehnologiei Cloud este că nu numai că permite accesul ușor și sincronizarea datelor pe mai multe dispozitive conectate de oriunde în lume, dar oferă și posibilitatea partajării acestor informații cu oricine doriți. Motivul pentru care aceste servicii se numesc „Cloud“ (i.e. Nor) este că cel mai adesea nu știm precis unde sunt stocate fizic datele în cauză. Exemple de utilizare a tehnologiei Cloud pot include crearea de documente în portalul Google Docs, distribuirea de fișiere prin intermediul Dropbox, configurarea unui server personalizat pe platforma Amazon Cloud sau stocarea de fișiere multimedia — muzică și fotografii — prin serviciul Apple iCloud. Aceste servicii online au potențialul de a vă face mult mai productivi, dar ele comportă, de asemenea, anumite riscuri specifice. În acest buletin informativ vom vedea cum se poate pune în valoare în siguranță potențialul tehnologiei Cloud.

Editor Invitat

James și Kelli Tarala (**@isaudit** / **@kellitarala**) sunt consultanți principali la Enclave Security, fiind autori a numeroase cursuri de instruire SANS, printre care se numără și SANS Audit 566: Implementarea și auditarea celor 20 de controale de securitate și MGT 415: O introducere practică în evaluarea riscurilor.

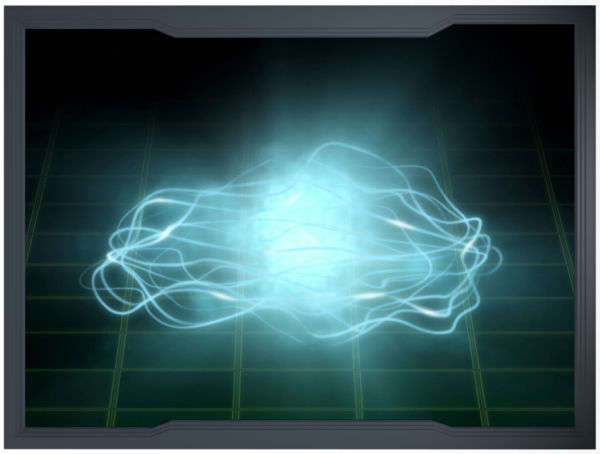
Alegerea unui ofertant de servicii Cloud

Tehnologia Cloud nu este nici bună nici rea, este o unealtă menită să ajute la realizarea multor lucruri, atât la serviciu cât și acasă. Cu toate astea însă, atunci când folosiți acest tip de servicii în fapt puneți la dispoziția unor necunoscuți datele personale, așteptându-vă ca aceștia să le mențină în siguranță și accesibile. Drept consecință, veți dori să vă asigurați că ați făcut o alegere înțeleaptă. În ce privește calculatoarele și informațiile de la serviciu, întrebați-vă superiorul ierarhic dacă puteți folosi servicii de tip Cloud. Dacă vă este permis, confirmați numele serviciilor de tip Cloud care sunt acceptate și care sunt politicile aplicabile pentru utilizarea lor. Dacă luați în calcul utilizarea unui serviciu de tip Cloud pentru nevoile personale, atunci aveți în vedere următoarele:

1. **Suport**: Cât de ușor este să obțineți ajutor sau răspuns la o întrebare? Există un număr de telefon la care puteți suna, sau o adresă de email de contact? Există și alte opțiuni pentru obținerea de suport, cum ar fi grupurile de discuții publice sau listele de întrebări frecvente afișate pe site-ul ofertantului de servicii?
2. **Simplitate**: Cât de ușor este să folosiți serviciul respectiv? Cu cât este mai complicat serviciul cu atât e mai probabil ca să faceți o greșeală și să expuneți sau să pierdeți datele proprii. Folosiți un serviciu Cloud pe care-l înțelegeți ușor și-l puteți configura și utiliza cu ușurință.

Utilizarea în siguranță a tehnologiei Cloud

3. **Securitate**: Cum ajung datele de pe calculatorul personal în mediul de stocare Cloud, este conexiunea dintre acestea securizată prin criptare? Cum este stocată informația pe platforma Cloud, este criptată și dacă da, puteți s-o decriptați?
4. **Condițiile de utilizare a serviciului**: Luați-vă un răgaz pentru citirea Condițiilor de utilizare a serviciului (deseori surprinzător de ușor de înțeles). Confirmați cine vă poate accesa datele și care vă sunt drepturile conferite de legislația în vigoare.



Tehnologia Cloud poate oferi o accesibilitate sporită informației, cât și o productivitate mai mare, dar trebuie să fiți atenți cum stocați și distribuiți această informație.

Securizarea datelor

Odată ce ați ales un serviciu Cloud, pașii următori sunt aceia prin care vă asigurați că folosiți acest serviciu în mod adecvat. Felul cum vă accesați și partajați datele poate avea cel mai adesea un impact mult mai mare decât orice altceva asupra securității lor. Câțiva pași esențiali pe care trebuie să-i parcurgeți sunt:

1. **Autentificare**: Folosiți o parolă puternică, unică, pentru autentificarea în contul personal din serviciul Cloud. Dacă ofertantul de servicii Cloud vă pune la dispoziție un mecanism de autentificare în doi pași, vă recomandăm insistent să-l folosiți.
2. **Partajarea fișierelor**: Tehnologia Cloud face partajarea și distribuirea datelor foarte ușoară, uneori chiar prea facilă. Într-o situația ipotetică nedorită puteți, în mod accidental, să faceți accesibile oricui în Internet fișierele personale sau chiar întreaga arhivă de date. Cel mai bun mod de a vă proteja este ca în mod implicit să nu faceți accesibile nimănui datele proprii. Apoi, în funcție de necesități, puteți să acordați drepturi de acces pentru anumite persoane sau grupuri specifice de persoane. Atunci când cineva nu mai are nevoie de acces la fișierele dumneavoastră, ștergeți-le. Ofertantul de servicii Cloud trebuie să vă pună la dispoziție modalități ușoare pentru a verifica cine are acces la fișierele personale.
3. **Partajarea fișierelor prin intermediul adreselor Web**: O facilitate frecvent pusă la dispoziția utilizatorilor de servicii Cloud este posibilitatea de a crea o adresă Web care dă acces la fișierele proprii. Această funcționalitate vă permite să partajați fișierele cu cine doriți trimițându-le această adresă web specifică. Această abordare însă este lipsită de securitate, deoarece oricine cunoaște această adresă poate avea acces la datele dumneavoastră. Dacă trimiteți adresa respectivă unei singure persoane acea persoană o poate trimite altora, sau adresa poate apărea în rezultatele unui motor de căutare online. Dacă partajați informația folosind o astfel de adresă, atunci asigurați-vă că ați dezactivat-o odată ce accesul pe care-l conferă nu mai e necesar, sau, cel puțin, protejați-o cu o parolă.
4. **Configurare**: Înțelegeți elementele de parametrizare a configurației de securitate ce vă sunt oferite de furnizorul serviciului Cloud. Spre exemplificare, dacă partajați o arhivă de date cu cineva, pot aceștia la rândul lor să partajeze informația la care le-ați dat acces cu altcineva, fără știința dumneavoastră?

Utilizarea în siguranță a tehnologiei Cloud

5. **Antivirus**: Asigurați-vă că aveți instalată cea mai recentă actualizare a programului antivirus de pe calculatorul propriu dar și pe oricare alt dispozitiv de pe care accesați datele proprii. Dacă un fișier pe care-l partajați este infectat cu un virus, alte calculatoare ce accesează acel fișier pot fi infectate, de asemenea.
6. **Copii de siguranță (backup)**: Chiar și dacă furnizorul serviciului Cloud folosit face copii de siguranță ale datelor, este recomandabil să vă faceți propriile copii de siguranță în mod regulat. Nu numai că aceasta vă protejează datele în eventualitatea că furnizorul își încetează activitatea sau are serviciile inaccesibile temporar, dar este și mult mai ușor să recuperați volume mari de date dintr-o copie de siguranță personală mai degrabă decât să descărcați aceste date din Cloud. De asemenea, confirmați frecvența cu care furnizorul serviciului face copii de siguranță ale datelor și dacă permite recuperare unor versiuni anterioare a fișierelor stocate și durata pentru care menține copiile de siguranță accesibile.

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 parole puternice:	http://www.securingthehuman.org/ouch/2013#may2013
Despre programele de gestiune a parolelor:	http://www.securingthehuman.org/ouch/2013#october2013
Despre copiile de siguranță (backup):	http://www.securingthehuman.org/ouch/2013#september2013
Termeni specifici din domeniul securității informației:	http://www.securingthehuman.org/resources/security-terms

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

