OUCH! | September 2014

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Overzicht
- Een Cloud Provider kiezen
- Jouw gegevens beveiligen

Veilig omgaan met de Cloud

Overzicht

‘De cloud’ is een krachtige technologie die momenteel door meer en meer organisaties en mensen wordt gebruikt. Het woord Cloud kan verschillende betekenissen hebben, maar in het algemeen betekent het een dienstprovider op het Internet, die gegevens voor jou beheert en bewaart. Niet enkel heeft de Cloud als voordeel, dat je jouw gegevens van meerdere toestellen makkelijk raadplegen en synchroniseren van overal. Met de Cloud kan je jouw gegevens delen met wie je maar wil. De reden waarom we deze diensten de Cloud noemen, is dat je niet weet op welke locatie de gegevens fysiek zijn opgeslagen. Het bewerken van documenten via Google Docs, het delen van bestanden via Dropbox, jouw eigen server opzetten op Amazon Cloud of het bewaren van muziek of afbeeldingen op Apple’s iCloud zijn enkele voorbeelden van Clouddiensten. Deze online diensten bieden het potentieel om productiever te zijn, maar brengen ook nieuwe risico’s. In deze editie beschrijven we hoe je veilig kan omgaan met de Cloud.

Gastredacteur

James en Kelli Tarala (@isaudit / @kellitarala) zijn principal consultants bij Enclave Security en hebben bijgedragen tot verscheidene SANS trainingen, waaronder SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls en MGT 415: A Practical Introduction to Risk Assessments.

Een Cloud Provider kiezen

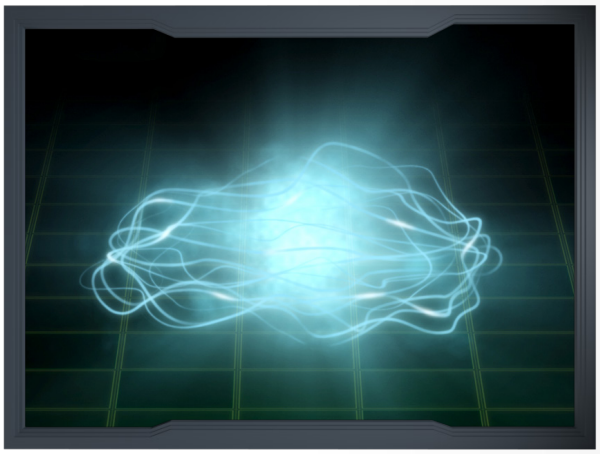
De Cloud is op zich noch goed, noch slecht, het is een instrument om al jouw zaken te regelen, zowel op het werk als thuis. Maar wanneer je deze diensten gebruikt, overhandig je jouw gegevens aan een vreemde partij waarvan je verwacht dat ze de gegevens beschikbaar stellen en beveiligen. Daarom moet je je ervan verzekeren dat je een goede partij kiest. Wil je de Cloud gebruiken op het werk, raadpleeg dan eerst jouw leidinggevende om te zien of dit wel mag. Indien je de Cloud mag gebruiken, vraag dan welke Clouddiensten zijn toegestaan en wat de gebruiksrichtlijnen zijn. Indien je zelf een Clouddienst wil gebruiken, houdt dan rekening met de volgende aspecten:

1. **Ondersteuning**: Kan je eenvoudig hulp krijgen of een antwoord krijgen op jouw vragen? Is er een telefoonnummer of emailadres voor hulp? Zijn er andere mogelijkheden zoals een publiek forum of is er een sectie met veelgestelde vragen op hun website?
2. **Gebruiksgemak**: Is de dienst eenvoudig in gebruik? Des te complexer de dienst, des te sneller je fouten zal maken en per

Veilig omgaan met de Cloud

ongeluk jouw gegevens kan verliezen of openstellen. Gebruik daarom een Clouddienst die je gemakkelijk kan onder knie hebben, instellen en gebruiken.

3. **Beveiliging**: Hoe krijg je de gegevens van jouw computer op de Cloud? Is het via een beveiligde verbinding? Hoe worden jouw gegevens bewaard in de Cloud? Worden ze geëncrypteerd en wie allemaal kan de gegevens decrypteren?
4. **Dienstvoorwaarden**: Neem een moment om de dienstvoorwaarden te lezen (vaak zijn ze verrassend genoeg in begrijpbare taal). Kijk na wie jouw gegevens kan raadplegen en welke rechten je hebt als gebruiker.



De Cloud maakt je productiever door jouw gegevens toegankelijker te maken, maar wees voorzichtig met hoe je de gegevens bewaart en deelt.

Jouw gegevens beveiligen

Eens je een Clouddienst hebt gekozen, is de volgende stap ervoor zorgen dat je de dienst juist gebruikt. De manier waarop je de gegevens raadpleegt en deelt, hebben vaak een grotere invloed op de beveiliging van jouw gegevens dan wat dan ook. Enkele belangrijke aspecten hierin zijn:

1. **Authenticatie**: Gebruik een sterke en unieke wachtwoordzin om te authenticeren tot jouw Cloud account. Indien jouw Cloud provider authenticatie in twee stappen aanbiedt, raden we aan deze te gebruiken.
2. **Delen van Bestanden en Mappen**: de Cloud maakt het zeer makkelijk om te delen, soms zelfs iets te makkelijk. In het ergste geval, kan je zelfs jouw bestanden of hele mappen onopzettelijk delen met het hele Internet. De beste manier om je te beschermen, is om standaard niets te delen. Vervolgens voeg je enkel specifieke personen toe (of groepen van personen) tot bepaalde bestanden of mappen. Wanneer iemand niet langer toegang vereist, verwijder je de toegang. Jouw Cloud provider voorziet normaal een eenvoudige manier om te bepalen wie er toegang heeft tot jouw bestanden en mappen.
3. **Delen van bestanden en mappen via links**: Een veelvoorkomende functie van Clouddiensten is dat je een weblink kan maken die naar jouw bestanden en mappen verwijst. Met deze functie kan je makkelijk bestanden of mappen delen via een weblink. Deze methode biedt echter weinig beveiliging, want iedereen die de link heeft, kan aan jouw gegevens of bestanden. Als je de link stuurt naar één persoon, kan deze persoon de link delen met andere personen. Als je iets deelt via een link, zorg er dan voor dat de link vervalt als deze niet langer nodig is en dat je de link beveiligt met een wachtwoord.

Veilig omgaan met de Cloud

4. **Instellingen**: Begrijp de beveiligingsinstellingen die jouw Cloud provider voorziet. Bijvoorbeeld wanneer je een map deelt met iemand, kan hij deze map dan zelf delen zonder dat je het weet?
5. **Antivirus**: Zorg ervoor dat je de meest recente antivirus versie hebt geinstalleerd op jouw computer, ook op iedere andere computer die je gebruikt om gegevens te delen. Indien een bestand dat je wilt delen besmet is, kunnen de computers die het bestand raadplegen ook besmet raken.
6. **Backup**: Zelfs indien jouw Cloud provider backups voorziet van jouw gegevens, overweeg dan om zelf regelmatig backups te maken. Dit beschermt jouw gegevens indien jouw Cloud provider ermee stopt, of om een andere reden niet beschikbaar is. Het is tevens veel makkelijker om grote hoeveelheden gegevens via lokale backups te nemen dan ze te downloaden vanuit de Cloud. Bekijk ook hoe frequent jouw Cloud provider backups neemt. Is het bijvoorbeeld mogelijk om eerdere versies van bestanden te raadplegen en exact hoe lang houden ze de backups beschikbaar?

Meer Weten?

Ga naar http://www.securingthehuman.org om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Nederlandse Editie

Cegeka is een full-service ICT-bedrijf: u kan bij ons terecht voor advies, detachering, softwareontwikkeling, bouw van websites, on-site en remote beheer van ICT-infrastructuur en outsourcing. Voor meer informatie: http://www.cegeka.com of volg ons op Twitter via @cegeka.

Bronnen (Engels)

Sterke wachtwoorden:	http://www.securingthehuman.org/ouch/2013#may2013
Password Managers:	http://www.securingthehuman.org/ouch/2013#october2013
Backups:	http://www.securingthehuman.org/ouch/2013#september2013
Security begrippen:	http://www.securingthehuman.org/resources/security-terms

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Sven Jacobs, Tom Palmaers