OUCH! | August 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Wat en wanneer back-ups maken**
- **Hoe een back-up maken**
- **Recovery**
- **Belangrijke punten**

Back-up & Recovery

Overzicht

Vroeg of laat zal er iets misgaan en verlies je hierdoor jouw persoonlijke bestanden, documenten of foto's. Bijvoorbeeld door per ongeluk bestanden te verwijderen, hardware problemen, door jouw laptop te verliezen of door een virusinfectie op jouw computer. Uitgerekend op deze momenten is een back-up dé manier om jouw digitale leven terug op te bouwen. In deze nieuwsbrief leggen we uit wat back-ups zijn, hoe je een back-up neemt en hoe je een juiste strategie voor jezelf kan kiezen.

Gastredacteur

Heather Mahalik is een gerenommeerde forensisch expert met als specialiteit smartphone forensics. Ze is coauteur van Mobile Forensics, technisch redacteur van Learning Android Forensics en is coauteur van de cursussen FOR585 Advanced Smartphone Forensics en FOR518 Macintosh Forensics van het SANS-instituut. Volg Heather via **smarterforensics.com** en op Twitter via **@heathermahalik**.

Wat en wanneer een back-up maken

Back-ups zijn kopieën van jouw gegevens die je ergens bewaart. Wanneer je belangrijke gegevens verliest, kan je deze herstellen van de back-ups. Het probleem is echter dat veel mensen geen back-ups maken, wat een jammere zaak is aangezien dit simpel en goedkoop kan. Om te beslissen welke gegevens je precies dient te voorzien in een back-up, zijn er twee opties: (1) bepaalde gegevens die belangrijk voor jou zijn, of (2) alles, inclusief jouw besturingssysteem. Met de eerste optie bespaar je schijfruimte, maar de tweede optie is eenvoudiger en completer. Indien je niet weet wat je moet back-uppen, kies dan voor een volledige back-up.

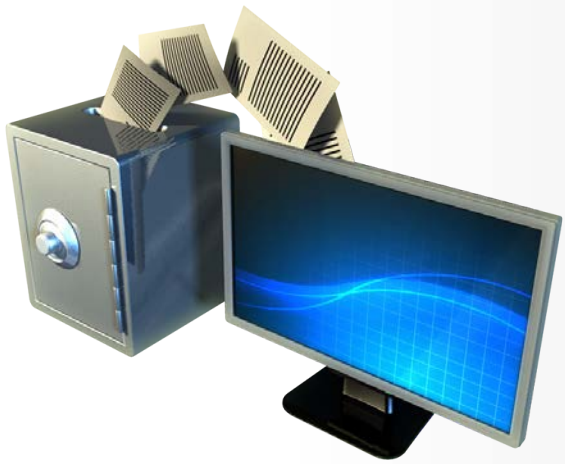
Een andere beslissing die je moet nemen, is de frequentie van de back-ups. Gangbare opties hier zijn uurlijks, dagelijks, wekelijks, etc. Voor thuisgebruik zijn persoonlijke back-up programma's als Apple's Time Machine of Microsoft Windows Backup en Restore goed om automatische back-up schema's in te stellen. Deze oplossingen zullen in de achtergrond een back-up maken van jouw gegevens tijdens de dag terwijl je jouw computer gebruikt of afwezig bent. Andere oplossingen bieden een continue bescherming aan waarbij gewijzigde bestanden meteen in back-up gaan zodra deze worden gesloten. We raden aan om een dagelijkse back-up te nemen. De vraag die je jezelf moet stellen hier is: exact hoeveel gegevensverlies is acceptabel minstens als ik een herstel dien uit te voeren vanuit mijn back-up.

Hoe een back-up maken

Er zijn twee manieren om een back-up te maken van jouw gegevens: via een fysiek opslagapparaat of via cloud-gebaseerde opslag. Fysieke media verwijst naar elke type hardware, zoals DVDs, USB-sticks of externe harde schijven. Wat je ook kiest,

Back-up & Recovery

doe nooit een back-up op hetzelfde toestel dat de originele bestanden bevat. Het probleem met fysieke opslag is dat wanneer je een probleem hebt (zoals brand of diefstal) je niet enkel jouw computer kwijt bent maar ook de back-ups. Net hierdoor dien je een goed plan te hebben om jouw back-ups op een veilige manier op een andere plaats te bewaren. Indien je ze ergens anders bewaart, voorzie dan een etiket met daarop een omschrijving van welke gegevens en wanneer de back-up is genomen. Voor extra veiligheid kan je best jouw back-ups voorzien van encryptie.



Geautomatiseerde en betrouwbare back-ups zijn vaak de laatste verdediging bij het beschermen van jouw gegevens.

Cloud-gebaseerde oplossingen zijn anders, dit is een dienst waarbij jouw gegevens worden opgeslagen ergens op het Internet. Afhankelijk van de grootte van jouw back-ups, kan dit een betalende dienst zijn. Je dient hiervoor een bepaald programma te installeren die dan automatisch back-ups neemt van jouw bestanden. Het voordeel hier is dat wanneer er een probleem voorvalt met jouw woning, jouw back-ups steeds veilig zijn. Bovendien heb je nog toegang tot jouw back-ups, vaak zelfs individuele bestanden vanaf overal, zelfs wanneer je op reis bent. Het nadeel is dat Cloud-gebaseerde back-ups (en herstel) mogelijk trager zijn, zeker als je veel gegevens hebt. Indien je niet zeker bent welke back-up oplossing het beste voor jou is (fysieke opslag of Cloud), realiseer je dan dat je altijd beide kunt combineren.

Ten slotte, vergeet je mobiele toestellen niet. Het voordeel met mobiele toestellen is dat de meeste van jouw gegevens reeds in de Cloud staan, zoals jouw e-mail, kalender gebeurtenissen of contactpersonen. Maar je hebt ook gegevens die niet in de Cloud staan, zoals de instellingen van jouw toestel, recente foto's en systeem voorkeuren. Door een back-up te maken van jouw mobiel toestel, bewaar je niet enkel deze gegevens, maar is het makkelijker om jouw toestel terug in te stellen wanneer je een upgrade doet of een nieuw toestel koopt. Een iPhone/iPad kan automatisch back-ups voorzien via Apple's iCloud. Met Android en andere mobiele toestellen is dit afhankelijk van de service provider of fabrikant. In sommige gevallen dien je mobiele apps aan te kopen die speciaal ontworpen zijn om back-ups te nemen.

Recovery

Back-ups nemen zijn maar een deel van de oplossing, je dient ook zeker te zijn dat je een recovery kunt uitvoeren. Test maandelijks jouw back-ups door een bestand te recoveren en de bestandsinhoud te valideren. Zorg ook dat je een volledige systeem back-up maakt voor dat je een belangrijke upgrade uitvoert (zoals migreren naar een nieuwe computer of mobiel toestel) of voor een reparatie (zoals het vervangen van een harde schijf) en ga na of je de data kunt herstellen via recovery.

Back-up & Recovery

Belangrijke punten

- Automatiseer het nemen van back-ups en test ze regelmatig.
- Wanneer je een systeem opnieuw installeert vanaf een back-up, installeer dan zeker de meeste recente security patches en updates vooraleer je het systeem gebruikt.
- Oude en overbodige back-ups kunnen een risico worden, deze moeten worden verwijderd om ongeoorloofde toegang door anderen te voorkomen.
- Als je een Cloud-oplossing gebruikt, lees dan hun gebruiksvoorwaarden en lees wat andere gebruikers ervaren bij deze oplossing. Bijvoorbeeld, worden de back-ups geëncrypteerd bewaard? Wie heeft er toegang tot de back-ups? Maken ze gebruik van sterke authenticatie als tweestapsverificatie?

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.

Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Passphrases:	http://www.securingthehuman.org/ouch/2015#april2015
Two-Step Verification:	http://www.securingthehuman.org/ouch/2013#august2013
Cloud Security:	http://www.securingthehuman.org/ouch/2014#september2014
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Tip of the Day:	http://www.sans.org/tip_of_the_day.php

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