OUCH! | Augustus 2017

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- **Back-ups: Wat, Wanneer en Hoe**
- **Herstel**
- **Belangrijke Aandachtspunten**

Back-up & Herstel

Overzicht

Als je een computer of mobiel toestel lang genoeg gebruikt, zal je vroeg of laat een probleem ervaren waardoor je jouw persoonlijk bestanden, documenten of foto's verliest. Zo kan je bijvoorbeeld per ongeluk bestanden verwijderen, een hardware probleem hebben, een toestel verliezen of besmet worden met een malware zoals ransomware. In deze gevallen is een back-up vaak de enige oplossing om jouw digitale leven te herstellen. In deze nieuwsbrief leggen we uit wat back-ups zijn, hoe je jouw gegevens back-upt en hoe je een makkelijk strategie kan ontwikkelen voor jezelf.

Gast redacteur

Keith Palmgren is een cyberbeveiliging professional met meer dan 30 jaar ervaring in het IT-beveiligingsgebied. Hij is een Senior SANS-instructeur en auteur van SANS SEC301 "Inleiding tot Informatiebeveiliging". Keith leidt een security consulting onderneming en is op Twitter via **@kpalmgren**.

Back-ups: Wat, Wanneer en Hoe

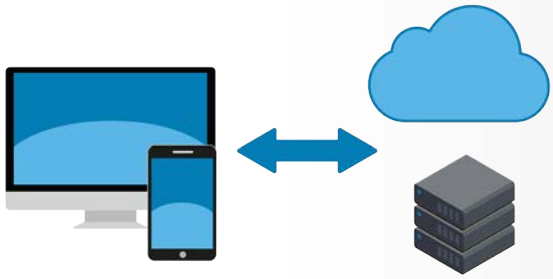
Back-ups zijn kopieën van jouw gegevens die je op een andere plaats bewaart dan jouw computer of mobiel toestel. Wanneer je data verliest, kan je deze herstellen vanaf jouw back-ups. Jammer genoeg zijn er veel mensen die niet slagen in het nemen van back-ups, ook al is het eenvoudig en goedkoop. Bij de eerste stap, beslis je wat je precies wil back-uppen. Hier kan je kiezen uit 2 verschillende methodes: (1) specifieke data die belangrijk voor je is of (2) alles, inclusief jouw hele besturingssysteem. De meeste back-upoplossingen zijn ingesteld om de eerste methode te gebruiken, ze nemen enkel een back-up van de meest gebruikte mappen. In de meeste gevallen volstaat dit. Weet je niet precies wat je allemaal nodig hebt, wees dan extra voorzichtig en ga voor een volledige back-up.

Ten tweede dien je te beslissen hoe vaak je de data back-upt. Ingebouwde back-up toepassingen zoals Apple's Time Machine of Microsoft Windows Back-up en Restore laten toe om een automatisch schema toe te passen. Opties zijn ieder uur, dagelijks, wekelijks etc. Andere oplossingen bieden continue bescherming aan waarbij iedere nieuwe of gewijzigde bestand meteen wordt geback-upt wanneer je deze wijzigt. We raden aan om minstens iedere dag een back-up te nemen.

Ten slotte moet je beslissen hoe je de back-up neemt. Er zijn 2 manieren om een back-up te nemen: via een fysiek opslagapparaat of via cloud-based opslag. Iedere aanpak heeft zijn voor- en nadelen. Ben je niet zeker welke aanpak het beste is, dan kan je beide toepassen. Fysieke opslagapparaten zijn toestellen zoals externe USD-schijven of netwerkapparaten. Het voordeel met deze is dat je snel grote hoeveelheden aan data in back-up kunt nemen. Het nadeel is dat wanneer je

Back-up & Herstel

besmet raakt met malware, zoals ransomware, het mogelijk is dat jouw back-ups ook besmet raken. Wanneer je een noodgeval hebt, zoals een brand of diefstal, is het mogelijk dat je jouw back-ups verliest. Indien je deze toestellen gebruikt, bewaar ze dan op een andere locatie en zorg ervoor dat deze voorzien zijn van een duidelijk label.



Automatische en betrouwbare back-ups zijn vaak het laatste middel om jouw data te beveiligen.

Cloud-gebaseerde oplossingen zijn onlinediensten die jouw bestanden opslaan op het Internet. Dit gebeurt door een toepassing te installeren op jouw toestel. De toepassing plaatst de bestanden automatisch in back-up naargelang het gekozen schema of telkens wanneer je ze wijzigt. Een voordeel van een cloudoplossing is het gebruiksgemak. De back-ups zijn automatisch en zorgen ervoor dat je van elke plek aan jouw bestanden kunt. Omdat jouw data in de cloud zit, zijn noodgevallen als een woningbrand of diefstal minder drastisch en hebben geen effect hebben op jouw back-up. Ten slotte, cloud back-ups kunnen je helpen om te herstellen van malware besmettingen als ransomware. Veel cloudoplossingen laten het toe om te herstellen van vorige versies. Het nadeel is dat het lang duurt om een back-up te nemen of grote hoeveelheden aan data te herstellen. Vergeet ook de privacy en beveiliging niet. Weet je of de back-up dienst sterke securitymaatregelen neemt zoals het versleutelen van jouw gegevens en het toepassen van twee-staps-verificatie?

Vergeet jouw mobiele toestellen niet. Bij mobiele toestellen is de meeste van jouw data zoals email en jouw agenda reeds in de cloud. Echter kunnen de instellingen van jouw apps, recente foto's en systeeminstellingen niet bewaard zijn in de cloud. Met een back-up van jouw mobiel toestel, bewaar je niet enkel deze informatie maar is het makkelijk om data te verplaatsen wanneer je een nieuw of ander toestel gebruikt. Een iPhone/iPad kan automatisch een back-up doen naar Apple's iCloud. Android en andere mobiele toestellen zijn afhankelijk van de leverancier of service provider. In sommige gevallen, moet je zelfs een mobiele app aanschaffen, speciaal ontworpen voor back-ups.

Herstellen

Back-ups nemen is slechts een deel van de puzzel. Je moet ook zeker weten dat je de data kan herstellen. Controleer daarom regelmatig dat de back-ups werken door een bestand te herstellen en te kijken of deze overeenstemt met het origineel. Zorg ook voor een volledige systeemback-up voordat je een grote update doet (zoals een nieuw toestel of computer in gebruik te nemen) of een herstelling (veranderen van een harde schijf) en controleer of het herstelbaar is.

Back-up & Herstel

Belangrijke Aandachtspunten

- Ongeacht de oplossing die je gebruikt om een back-up te nemen, zorg ervoor dat je de back-ups regelmatig controleert.
- Wanneer je back-ups gebruikt om een systeem opnieuw te bouwen, zorg er dan voor dat je de laatste security patches en updates toepast voor gebruik.
- Oude back-ups die je niet meer gebruikt, vormen een risico, vernietig ze om ongeoorloofde toegang te voorkomen.
- Wanneer je een cloudoplossing gebruikt, lees dan de gebruiksvoorwaarden en onderzoek hoe tevreden andere gebruikers zijn, om te kijken of ze aan jouw verwachtingen voldoen. Zo kan je bijvoorbeeld nagaan of ze jouw data wel versleutelen of sterke authenticatie gebruiken zoals twee-staps-verificatie?

Meer Weten?

Ga naar securingthehuman.sans.org/ouch/archives 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 is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen

Passphrases:	https://securingthehuman.sans.org/ouch/2017#april2017
Two-step Verification:	https://securingthehuman.sans.org/ouch/2015#september2015
Cloud Security:	https://securingthehuman.sans.org/ouch/2016#november2016
Encryption:	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016

Redactie: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Vertaald door: Sven Jacobs, Tom Palmaers