De maandelijkse Security Awareness nieuwsbrief voor jou!

Reservekopieën?

Overzicht

Als je een computer of mobiel apparaat lang genoeg gebruikt, gaat er vroeg of laat iets mis. Je kunt per ongeluk de verkeerde bestanden verwijderen, een hardwarestoring hebben of een apparaat verliezen. Erger nog, malware zoals ransomware kan jouw bestanden wissen en/of gevangen houden. In tijden als deze zijn reservekopieën vaak de enige manier om je digitale leven weer op te bouwen.

Wat, wanneer en hoe

Reservekopieen zijn kopieën van jouw informatie die ergens anders dan op jouw computer of mobiele apparaat zijn opgeslagen. Wanneer je waardevolle gegevens verliest, kun je jouw gegevens herstellen vanuit reservekopieën. De eerste stap is het bepalen van wat je wilt kopiëren, (1) specifieke gegevens die voor jouw belangrijk zijn; of (2) alles, inclusief jouw hele besturingssysteem. Veel reservekopie-oplossingen zijn standaard geconfigureerd om de eerste benadering te gebruiken, ze maken een reservekopie van de meest gebruikte mappen. Als je niet zeker weet wat je moet kopiëren of extra voorzichtig wilt zijn, maak dan een reservekopie van alles.

Ten tweede, beslis hoe vaak je een reservekopie wilt maken. Met ingebouwde reservekopieprogramma's zoals Apple's Time Machine of Windows Backup and Restore kun je een automatisch "set it and forget it"-schema maken. Veelgebruikte opties zijn onder meer uurlijks, dagelijks, wekelijks, enz. Andere oplossingen bieden "continue bescherming" waarin nieuwe of gewijzigde bestanden onmiddellijk een reservekopie maken wanneer je een document opslaat. Wij raden je minimaal aan om dagelijks een automatische reservekopie te maken van kritische bestanden.

Bepaal tenslotte hoe je een reservekopie gaat maken. Er zijn twee manieren: lokale of cloud-gebaseerde opslag. Lokale reservekopieën zijn afhankelijk van apparaten die je bestuurt, zoals externe USB-schijven of voor Wi-Fi toegankelijke netwerkapparaten. Het voordeel van lokale reservekopieën is dat je hiermee snel een reservekopie en herstel van grote hoeveelheden gegevens kunt maken. Het nadeel is dat als je geïnfecteerd raakt met malware, zoals Ransomware, de infectie zich kan verspreiden naar jouw reservekopieën. Ook in geval van een ramp, zoals brand of diefstal, kan dit ertoe leiden dat je niet alleen jouw computer maar ook de reservekopieën verliest. Als je externe apparaten gebruikt voor het maken van reservekopieën, bewaar dan een kopie off-site op een veilige locatie en zorg ervoor dat jouw reservekopieën van de juiste labels zijn voorzien.

Cloud-gebaseerde oplossingen zijn online diensten die jouw bestanden opslaan op het internet. Meestal installeer je een toepassing op jouw computer, de toepassing maakt dan automatisch een reservekopie van jouw bestanden, hetzij volgens een schema, hetzij terwijl je ze wijzigt. Een voordeel van cloud-oplossingen is hun eenvoud, reservekopieën zijn vaak automatisch en

je kunt jouw bestanden meestal overal benaderen. Ook, omdat jouw gegevens zich in de cloud bevinden, zullen thuis rampen zoals brand of diefstal geen invloed hebben op jouw reservekopieën. Tot slot kunnen cloud reservekopieën je helpen herstellen van malware-infecties zoals Ransomware. De nadelen is jouw vermogen om een reservekopie te maken en te herstellen, afhankelijk van de hoeveelheid gegevens waarvan je een reservekopieën hebt gemaakt en de snelheid van jouw netwerk. Weet je niet zeker of je lokale of cloud-gebaseerde reservekopieën wilt gebruiken? Wees extra veilig en gebruik beide.

Met mobiele apparaten zijn de meeste van jouw gegevens al in de cloud opgeslagen. Het is echter mogelijk dat de configuraties van jouw mobiele app, recente foto's en systeemvoorkeuren dat niet zijn. Door een reservekopie te maken van jouw mobiele apparaat bewaar je niet alleen deze informatie, maar het is ook gemakkelijker om jouw gegevens over te dragen wanneer je een upgrade naar een nieuw apparaat uitvoert.

Belangrijkste punten

- **Het maken van een reservekopie van je gegevens is slechts de helft van de strijd; je moet er zeker van zijn dat je deze kunt herstellen. Test regelmatig of je reservekopieën werken door een bestand op te halen en te openen.**
- **Als je een systeem herbouwt vanaf een reservekopie, zorg er dan voor dat je de laatste beveiligingspatches en updates opnieuw toepast voordat je het opnieuw gebruikt.**
- **Als je een cloud-oplossing gebruikt, selecteer er dan een die eenvoudig te gebruiken is en onderzoek de beveiligingsopties. Ondersteunen ze bijvoorbeeld verificatie in twee stappen om jouw onlineaccount te beveiligen.**

Reservekopieën zijn een eenvoudige en goedkope manier om jouw digitale leven te beschermen.

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 meer dan 4.200 medewerkers. In 2018 realiseerde Cegeka Groep een omzet van 512 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Matt Bromiley *is een cyberbeveiligings - en incident professional die heeft samengewerkt met organisaties van elke omvang. Hij is ook een SANS-instructeur, die lesgeeft in de geavanceerde host- en netwerkincidentenrespons en zogeheten threat hunting lessen, FOR508 en FOR572. Je kunt hem bereiken op Twitter* @mbromileyDFIR.

Bronnen

Making Passwords Simple:	https://www.sans.org/u/TqR
Stop That Malware:	https://www.sans.org/u/TqW
Creating a Cybersecure Home:	https://www.sans.org/u/Tr1