

● Back-uppen moet! ●

Rein de Jong

De back-up is de veiligste manier om je voor van buiten komend onheil te behoeden. Naast malware en corrupte opslagmedia vormen wij zelf de grootste bedreiging voor onze persoonlijke data door het per ongeluk weggooien of overschrijven van bestanden. De back-up vrijwaart ons voor dataverlies. Je zult maar een belangrijke brief, een scriptie of foto's van je pasgeboren (klein)kind kwijt zijn. Een met regelmaat uitgevoerde back-up, die brand- en diefstalveilig is opgeslagen, is het beste middel om je daartegen te wapenen.



Daarvan was geen back-up, maar wel een papieren exemplaar van ruim een week geleden. Dankzij mijn inspanningen met een herstelprogramma kon ik een versie van een paar dagen daarvoor herstellen. Samen met de papieren versie en een nacht doorwerken kon de scriptie een dag later worden ingeleverd. Wel was de familie een aantal recente foto's kwijt. Deze mensen maken nu dagelijks een veiligheidskopie in de Cloud bij Livedrive (Backupmypc.nl). Die back-up heeft hen al vaak voor meer ellende behoed. En scripties? Die zijn ze nooit meer kwijtgeraakt.

Een soortgelijk verhaal had ik ook met een predikant die op zaterdagmiddag opeens zijn preek kwijt was. Daarvan vond ik een werkexemplaar terug. Uiteindelijk heeft hij deze de preek grotendeels uit het hoofd gedaan. Dit tot genoegen van veel oudere kerkleden.

Oorzaak B. Laptop gestolen



Een stel hier uit de buurt gaat altijd overwinteren in Spanje. Natuurlijk gaat de laptop mee op vakantie. Al is het alleen maar voor de contacten met thuis en als opslag voor de gemaakte foto's. Op de weg naar huis sloeg het noodlot toe. Tijdens een koffiestop is er in de auto ingebroken. Daarbij is de laptop ontvreemd. Tja, en dan ben je veel kwijt. Mij werd gevraagd of ik uit dropbox nog foto's kon redden.

Dropbox was immers de plek waar de foto's zouden moeten staan? Helaas kon ik daar alleen foto's vinden die met de

mobiel waren gemaakt. Op de fotokaart van de camera was met behulp van Recuva ook nog wat te redden, maar veel, heel veel foto's van die vakantie waren ze kwijt. De mail van de vakantie was behouden gebleven doordat er gebruik gemaakt werd van een IMAP-verbinding. Had een back-up hen kunnen helpen?

Wel als ze tijdens de vakantie een externe harde schijf gebruikt zouden hebben voor opslag van nieuwe foto's en documenten. En wanneer die schijf op een veilige plek zou zijn opgeslagen tijdens de terugreis. Of ... wanneer de foto's waren opgeslagen op het internet. Alleen zijn aan dat laatste vaak hoge kosten verbonden in verband met dataverbruik onderweg en in het buitenland.

Oorzaak C. Slachtoffer van malware

Een pc van een bekende werd ruim een jaar geleden gebracht met de mededeling dat documenten niet meer leesbaar waren. Toen de pc werd gestart, verscheen direct na inloggen de mededeling dat alle documenten geëncrypt waren en dat er nog 72 uur tijd was om € 300,- te betalen waarna een sleutel zou worden verstrekt om de bestanden weer toegankelijk te maken. Ik heb de pc direct uitgezet en de schijf uitgebouwd om te kijken of er nog wat te redden was. Met de toen bekende programma's is mij dat deels gelukt. Gelukkig werd er dagelijks een back-up gemaakt op een externe harde schijf.

Deze werd opgehaald. Doordat de back-upschijf altijd aan die pc hing en schrijfbaar was vanuit het gebruikte account, waren ook die documenten versleuteld. Zelfs de bestanden op de NAS waren geëncrypt. Deze man heeft na aangifte en afraden door de politie toch de € 300 betaald, maar nooit een sleutel ontvangen! Dus én de data kwijt én 300 euro!



Wat kan er gebeuren?

In mijn omgeving heb ik als helper een aantal malen meegemaakt dat mensen data waren kwijtgeraakt. Daarvoor werd mijn hulp dan ingeroepen. Dikwijls is het mij gelukt hen te helpen. Helaas was mijn hulp ook een aantal keren vergeefs. Drie verhalen over hoe het kan lopen.

Oorzaak A. Harde schijf defect



Mij werd gevraagd te helpen bij een pc die niet meer wilde starten. Het systeem werd gebracht, en al snel werd duidelijk dat de harde schijf was gecrasht. Op mijn vraag of er een back-up was, werd mij verteld dat er wel e.e.a. op een externe schijf was geplaatst, maar dat het al weer een tijdje geleden was. Het ergste was dat de eindexamenscriptie van de oudste dochter ook op de pc stond.

Back-uppen moet!

Wat back-up je?

Hoewel het verleidelijk is om de inhoud van je complete harde schijf veilig te stellen is dat, naast ruimte verslindend, ook vaak overbodig. Je hoeft immers alleen datgene veilig te stellen wat uniek is op je eigen pc. Daarbij kun je denken aan je persoonlijke gegevens en unieke instellingen zoals:

- Eigen documenten
- Foto's en films
- Favorieten
- E-mail/adresboek
- Programma-instellingen en sleutels
- Back-ups van andere apparaten, zoals telefoon en navigatieapparaat
- Overige eigen unieke bestanden.

Onnodig zijn gedownloade bestanden zoals publieke: films, muziek en installatiebestanden. Deze kun je immers al tijd weer van het internet ophalen. Vergeet niet de films en muziek die je hebt aangeschaft.

Hoe back-up je?

Je kunt op verschillende manieren back-uppen.

- Gewoon simpel, met een gratis back-upprogramma, telkens kopieën op een fysiek andere plek zetten. Daarvandaan kun je de veiligheidskopie weer terugzetten. Dit alles heeft echter als nadeel dat een beschadigd bestand over een kopie heen kan worden geschreven voordat je er erg in hebt.
- Een tijdelijback-up die meerdere versies van een bestand opslaat zodat je terug kunt gaan in de tijd om een bepaalde versie te herstellen. Dit is de veiligste back-up.
- Dan zijn er nog kretten als incrementeel en differentieel¹. En grootvader-, vader-, zoon-systemen, die je met meerdere media kunt bereiken.

Waar sla je de back-up op?

Die vraag wordt veel gesteld. Ik merk in de praktijk dat we heel graag de back-up in eigen beheer willen houden. Alleen houden we de discipline die dat vraagt vaak niet vol. Wie maakt er da-

gelijks een back-up op een externe schijf die vervolgens veilig en buitenshuis wordt opgeborgen? Ik zie drie mogelijkheden met elk hun eigen voor- en nadelen.

1. Op DVD's

Nadeel is dat er vaak heel veel nodig zijn om je persoonlijke data op te slaan. Wanneer je echter alleen de gewijzigde en nieuwe bestanden opslaat valt het over het algemeen wel mee. Berg ze wel op een veilige plek op. Houd ook rekening met de levensduur van DVD's. Waar men vroeger dacht dat deze heel lang mee zouden gaan, blijkt in de praktijk dat zelf gebrande DVD's vaak al na een paar jaar slecht benaderbaar worden.

2. Externe schijf, USB-stick of NAS

Dit wordt door velen omarmd omdat het makkelijk is. Het is eenvoudig te automatiseren. Ook al maak je hier een tijdelijback-up, dan is er nog het nadeel dat de externe schijf en zeker een NAS zich in huis bevinden



Niet veilig voor brand, blikseminslag en diefstal. Daarnaast, wanneer via het 'normale' gebruikersaccount de back-up wordt gemaakt, zijn je bestanden, bij een aangekoppelde schijf, niet veilig voor ransomware. Wil je tegen een gijzelvirus beschermd zijn, dan moet je back-uppen met een speciaal account dat jouw bestanden kan lezen en kan schrijven op de back-uplocatie. Je eigen account mag alleen maar kunnen lezen op de back-uplocatie.

3. In de Cloud.

Op een internetserver (de Cloud) staan je back-ups het veiligst. Daar staan je bestanden veilig, beschermd tegen brand, diefstal en, omdat het meestal



timelineback-ups betreft, ook veilig voor gijzelvirussen. Daarnaast is de veiligheidsafdeling van een back-up-provider veel beter toegerust om je bestanden te beschermen dan jij zelf op je privécomputer ooit kunt. Mocht je de bestanden 100% afgeschermd willen, dan kan dat bij KPN; daar kun je de bestanden met een eigen sleutel encrypten zodat jouw bestanden ook voor de beheerders niet te ontsleutelen zijn.

Back-up bij KPN² kost €87,12 per jaar voor een pc waarbij je net zoveel data mag uploaden als je wenst. Een goedkopere oplossing is BackupMyPC³ voor € 25,- per jaar (Voor HCC-leden € 10,- per jaar⁴), waar je onder een account een onbeperkt aantal pc's mag back-uppen en ook daar geldt dat het databeslag onbeperkt is. De data gaat over een versleutelde verbinding naar de Livedrive-servers in Engeland. Beide providers bieden een tijdelijback-up, zodat je ook na verloop van tijd je bestanden kunt terugplaatsen.

Tot Slot

Vind je een back-up te prijzig? En betaal je wel voor je antivirus? Bedenk dan dat een back-up je beter tegen de gevolgen van virussen en malware beschermt dan enig ander product. Wil je goedkoop beveiligen tegen malware, dan blijft mijn advies een basale scanner, b.v. Microsoft Defender in combinatie met de second opinion scanner HitManPro die wekelijks wordt uitgevoerd.

Daarnaast beschermt de back-up je natuurlijk ook tegen defecte opslagmedia.

En nu maar hopen dat niemand mij meer nodig heeft om gegevens te herstellen ;-)



Links

- | | |
|--------------------------|---|
| 1 Back-upmethodieken | https://nl.wikipedia.org/wiki/Back-up |
| 2 KPN Back-up | https://zakelijk.kpn.com/zakelijk/cloud/cloudstore/3992/Back-up-Online.htm |
| 3 BackupMyPC | https://backupmypc.nl/ |
| 4 Back-up via HCC | https://www.hcc.nl/backup |
| Datarecovery | http://www.digirec.nl/ |
| Online storage providers | http://storageproviders.nl/ |