WHITEPAPER BACK-UP POLICY

EVEN EEN BACK-UPJE MAKEN. SIMPEL TOCH?

Door het grote aantal ransomware uitbraken dat in de afgelopen periode heeft plaatsgevonden, wordt er de laatste tijd veel gesproken over het belang van het hebben van een goede back-up policy. En dat is goed.

WHITEPAPER

EVEN EEN BACK-UPJE MAKEN. SIMPEL TOCH?

Het hebben van een back-up is het laatste redmiddel wanneer alle andere proactieve hulpmiddelen, zoals endpoint beveiliging, niet afdoende zijn. Ga maar na. Wanneer uw data centraal op een laptop staan opgeslagen en deze wordt gestolen, dan is een back-up de enige manier om deze data terug te halen.

Het maken van een back-up heeft als doel om na een veiligheidsincident terug te kunnen vallen op de reservekopie van uw data, een situatie of een omgeving. Om de continuïteit van uw bedrijf te waarborgen. Dus maakt u even een back-upje. Maar van wat eigenlijk? En hoe? En voor hoe lang?

De juiste back-up

Er hangt veel af van het maken van de juiste back-up. Helaas is niet iedere ondernemer op de hoogte van de verschillende soorten back-ups die er zijn. We kennen genoeg voorbeelden van mensen die voor een onaangename verrassing komen te staan als na een incident blijkt dat alle vakantiefoto's op de laptop bewaard zijn gebleven maar wel het hele CRM is weggevaagd.

We nemen u in deze whitepaper daarom mee in het proces om tot een goede back-up policy te komen. Aan de hand van een aantal vragen krijgt u inzicht in wat u moet doen om ervoor te zorgen dat u, indien nodig, terug kunt vallen op data die voor u van belang is.

Welke soorten data zijn er?

Voordat u een back-up kunt maken, moet u eerst beslissen van welke data u een back-up wilt maken. Er zijn verschillende soorten data.

- Gebruikersbestanden.

Dit zijn unieke, losse bestanden in Word, Excel etc. of foto's. Waardevolle bestanden.

- Databases.

Een database is een grote bulk digitale data die door een databaseapplicatie gelezen kan worden. Omdat er intelligentie zit in de manier waarop deze data is opgeslagen, kan deze data snel vanuit diverse invalshoeken worden geraadpleegd.

WAAR DIENT U OP TE LETTEN?

De BrainCheck is o.a. opgesteld aan de hand van fouten die bedrijven regelmatig maken. Deze punten zijn van belang voor ieder bedrijf, ongeacht grootte of branche. Met de opkomst van cybercriminaliteit is men geneigd om, gedreven door paniek en publieke opinie, de nadruk hier op te leggen. Echter, voor een bedrijf dat zijn algehele digitale veiligheid goed op orde wil hebben, is het van belang deze top 10 punt voor punt door te lopen.

- Systeemdata

Dit zijn de gegevens van een computer of een randapparaat die voor de werking van dat apparaat zorgen, zoals het operating system van een server, werkstation, firewall of router.

De keuze voor een back-up van een van bovenstaande soorten data is o.a. afhankelijk van uw werkwijze en van die van uw medewerkers en daarmee voor ieder bedrijf verschillend. In overleg met een IT-afdeling of adviseur kunt u hier een overweging in maken.

Waar bevindt zich de data waarvan u een back-up wilt maken?

Wanneer u weet welke soort data u wilt beveiligen, brengt u in kaart waar deze data zich bevindt. De locatie van de data is afhankelijk van de soort data.

- Gebruikersbestanden staan opgeslagen op de pc, het netwerk/de server of in de cloud.
- Databases staan (bijna) altijd op een server opgeslagen (on-premise of in de cloud).
- Systeemdata staan altijd op de machine zelf opgeslagen.

Het onderscheid tussen de soorten data en verschillende locaties van deze data illustreert dat het ‘maken van een back-upje’ iets gecompliceerder is dan het lijkt.

Van welke data moet er een back-up gemaakt worden?

Nu kunt u gaan bepalen welke data wel of niet geback-upt moet worden. Dit gebeurt op basis van de wijze waarop de data is opgeslagen. Hierbij onderscheiden we twee manieren van opslaan.

- Gesynchroniseerde data

Voor data die zowel op een pc als op een gemeenschappelijk plek staan (bijvoorbeeld op een server) en automatisch worden gesynchroniseerd, volstaat het om alleen een back-up van de server te maken. De server is de bron van deze data. Hetzelfde geldt voor gegevens die in de cloud zijn opgeslagen (Waar wacht u nog op? Ga werken in de cloud!). Overigens moet er goed gekeken worden dat data niet dubbel geback-upt wordt.

- Niet-centraal opgeslagen data

Steeds meer mensen werken onderweg (en op kantoor) op een laptop. De data op deze laptop wordt vaak lokaal en niet op een centrale plek opgeslagen. Voor het opslaan en delen van bestanden met collega’s of klanten worden Dropbox of OneDrive gebruikt. Maar deze File Sync & Share (FSS) oplossingen vormen géén back-up oplossing om de eenvoudige reden dat deze data corrupt kan raken (of zelfs kan verdwijnen). Hier dient u rekening mee te houden en ook voor deze data dient daarom een back-up gemaakt te worden. Hetzelfde geldt voor gegevens die in de cloud zijn opgeslagen (Waar wacht u nog op? Ga werken in de cloud!).

Er bestaan endpointoplossingen die data op werkstations automatisch naar de cloud back-uppen als er een internetverbinding is of lokaal naar een externe harddisk (meestal niet geheel automatisch). Ook zijn er FSS-oplossingen die wel een echte back-up maken van de data, de zogenaamde File Sync, Share & Back-up oplossingen voor endpoints.

Kort samengevat levert dit de volgende back-up jobs op:

Soort data	Back-up
Centrale data op server (on-premise of in de cloud)	Alles
Databases (on-premise of in de cloud)	Alles
Data op endpoints/werkstations	Alleen wat uniek op die machine staat
Systeemdata	Gehele machine minus de gebruikersdata en databases
Overige endpoints zoals routers en firewalls	Firmware en configuratie

Hoe lang moet de data bewaard blijven?

Wanneer bepaald is welke data veiliggesteld moet worden, moet u beslissen hoe lang de data bewaard moet blijven. Ook dit is afhankelijk van de soort data. Bij het maken van een back-up van een database bijvoorbeeld, heeft het weinig zin om een back-up voor een langere periode te bewaren. Bij het gebruik van een database wijzigt er tussentijds zoveel, dat een back-up al snel onbruikbaar wordt.

Bij systeemdata (die voor de werking van apparaten zorgt) is het alleen nodig deze te back-uppen als er iets gewijzigd is in de configuratie. In dat geval kan vanaf een bepaald punt alles weer in werking worden gezet en moeten de back-up van de database en gebruikersbestanden worden teruggezet. De IT-afdeling en de gebruikers moeten daarom samen bepalen wat er gewenst is in welke situatie.

Tot slot nog een gouden tip. Zorg ervoor dat geregeld getest wordt of de back-up wel werkt. Uit ervaring weten wij dat dit vaak vergeten wordt.

De moraal van dit verhaal

Digitale onveiligheid krijg veel aandacht in de media. Terecht, want ondanks het feit dat we er de mond van vol hebben, weten (zo blijkt uit alle consternatie) de meeste bedrijven niet wat ze zelf kunnen doen aan het beveiligen van hun IT-omgeving.

Het hebben van een goede back-up policy is essentieel bij het optimaliseren van de beveiliging van uw automatisering. Want als de boot lek is, de peddels kwijt zijn en de boei al overboord is dan is het heel fijn dat u in ieder geval kunt zwemmen.

Doe de BrainCheck

Om u inzicht te geven in uw huidige niveau van digitale beveiliging en veiligheid, heeft BrainCap de BrainCheck ontwikkeld. De back-up policy is hier onderdeel van.

De BrainCheck behandelt een 10-tal punten die essentieel zijn met betrekking tot ICT-beveiliging en de veiligheid van de gegevens binnen een bedrijf en bestaat uit de volgende lijst van vragen en aandachtspunten:

- Back-up policy
- Gebruikersrechten
- Patchmanagement
- Wachtwoordpolicy
- Cloud Bestandsdeling en Synchronisatie
- Awareness
- Toegang van buitenaf
- Endpoint beveiliging
- Versleuteling van data
- Security Network Monitoring

Zegt niet alles u iets? Geen paniek, daar zijn wij voor. Nadat deze cruciale aandachtspunten besproken zijn, volgt er een rapportage met uw score op het gebied van digitale beveiliging en een aanbeveling. Met dit rapport kunt u zelf beslissen hoe u verdere invulling geeft aan een veilig ICT-beleid, waar we u uiteraard graag en vakkundig in adviseren. Neem contact met ons op via services@braincap.nl of bel ons op 088-2754800.

BRAINCAP
SOFTWARE & SERVICES