

Backupinformatie, -tips en -instructies

Het doel van deze informatie is om de opdrachtgever te informeren over backups, om tips te geven en om de meest gangbare instructies te geven. De informatie dekt echter niet alle mogelijkheden, beschrijft niet alle situaties en is dan ook niet volledig of als zodanig bedoeld. Deze hieronder verstrekte informatie dient dan ook als algemene richtlijnen beschouwd te worden waaraan geen rechten ontleend kunnen worden.

Backupinformatie

Bij ernstige storingen aan de soft- of hardware, virus- en/of malware infecties maar ook bij onbedoelde fouten door medewerkers van EQUA en/of medewerkers van de opdrachtgever kan het nodig zijn om backups geheel- of gedeeltelijk terug te zetten. Goede backups zijn dan ook uitermate belangrijk en het ontbreken van goede en recente backups kan tot forse bedrijfsschade of erger leiden. Het meewerken aan goede en veilige backups beschouwen we dan ook als een kerntaak van EQUA. EQUA kan dit echter niet zonder medewerking van de opdrachtgever. Bij een lokale backup is het uitermate van belang dat de datadragers waarop de backups gemaakt worden na elke succesvolle backup gewisseld en op een veilige plaats opgeslagen worden. Omdat het uitvoeren van deze handeling niet binnen de SLA valt en EQUA hiervoor niet kan zorgen valt dit onder de verantwoordelijkheid van de opdrachtgever. Bij een lokale backup is de opdrachtgever verantwoordelijk voor:

- het zo spoedig mogelijk wisselen van de datadragers na een geslaagde backup;
- het monitoren van de ontvangen backupmeldingen;
- het signaleren als er geen backupmeldingen ontvangen worden;
- het bewaren van de backupdragers op een veilige plaats.

In veel gevallen zal EQUA ook meldingen krijgen als de backups niet goed werken en pro-actief actie ondernemen. Omdat niet gegarandeerd kan worden dat meldingen in alle gevallen daadwerkelijk verstuurd en ontvangen worden rekent EQUA erop dat niet alleen alle fouten maar ook het ontbreken van meldingen dat de backup succesvol afgerond is, door de opdrachtgever schriftelijk of per e-mail aan EQUA gemeld wordt. EQUA laat de opdrachtgever per email weten als de melding opgepakt en afgehandeld is.

EQUA controleert minimaal 2x per jaar handmatig of backups volledig zijn en of deze ingelezen kunnen worden. Op verzoek van de klant kan deze controle vaker plaatsvinden. De aan deze, op verzoek van de opdrachtgever, extra controles bestede tijd wordt afgeschreven van het urencontract dat elke klant bij EQUA heeft. Verder biedt EQUA, indien technisch mogelijk, extra backupdiensten aan zoals: een backup naar een lokatie buiten het pand van de klant (*cloudbackup*); replicatie naar een virtuele server van de klant in het datacenter van EQUA of in een extern datacenter, het plaatsen van een fysieke server van de klant in het datacenter van EQUA of in een extern datacenter (*huren rackspace*). De mogelijkheden van extra backupmogelijkheden zijn legio en wij helpen en adviseren dan ook graag bij het maken van deze keuze.

Backuptips

Van belang is om een onderscheid te maken tussen backups- en archivering. Het doel van backups is om snel de meest recente informatie terug te kunnen halen in het geval van een storing. De te herstellen data kan bestaan uit bestanden maar ook uit de volledige herinstallatie van één of meerdere servers. Bij een ernstige calamiteit zal EQUA in het algemeen in staat zijn om de ICT van de opdrachtgever binnen 24 uur na aanvang van de herstelwerkzaamheden weer operationeel te hebben. Hoe lang EQUA daadwerkelijk nodig heeft voor een volledige herinstallatie is afhankelijk van de hoeveelheid data die teruggezet moet worden, de snelheid van de datadragers en de snelheid van de apparatuur waarop de backups teruggezet gaan worden. Als vuistregel mag 4-6 uur (installatie- en opbouwtijd) + 1 uur voor elke 100GB aan data aangehouden worden.

Hoeveel backupdragers hebt u nodig?

We beschouwen 3 backupdrages als het absolute minimum en we zijn van mening dat een dergelijke backup alleen geschikt is voor kleine netwerken en in die gevallen waarin het verloren gaan van gegevens niet tot onherstelbare schade en/of ernstige hinder zal leiden.

Één van de mogelijke backupstrategiën bij 3 backupdragers is om 2 van deze backupdragers te voorzien van het label 'even' en 'oneven' en de derde backupdrager van het label 'vrijdag'. De 'even/oneven' gelabelde datadragers worden om de dag gewisseld (waarbij de datum van de dag gebruikt wordt om de juiste datadrager te indentificeren. De met 'vrijdag' gelabelde datadrager wordt maar één keer per week (op een vrijdag) gebruikt.

De meeste EQUA klanten met een lokale backup gebruiken minimaal 6 datadragers ('Maandag t/m Donderdag' en 'Vrijdag Even' / 'Vrijdag Oneven'). Met 6 datadragers waarop een succesvolle en recente backup staat kunnen we minimaal 3 (storing op één maandag) en maximaal 14 dagen terug (storing op een vrijdag). Bij het bepalen van de dagen zijn ook de zaterdag en zondag meegeteld.

Archiveren

Het doel van archivering is om backups langdurig te bewaren. Dat kan zijn met het oog op wettelijke voorgeschreven 'bewaartermijnen' maar ook met het doel om data te kunnen terughalen die per abuis of opzettelijk verwijderd is en waarvan het ontbreken pas na lange tijd (maanden/jaren) ontdekt wordt. Verder beschermt archivering tegen nieuwe dreigingen zoals langzaam werkende crypto besmettingen ('Ransomware') waarbij bestanden versleuteld worden en waarbij vaak 'losgeld' geëist wordt. Een spraakmakende en succesvolle 'ransomware' haalde in december 2019 het nieuws toen de universiteit in Maastricht hiermee te maken kreeg en bijna 200.000 EURO aan losgeld moest betalen. De daadwerkelijke schade was echter veel hoger. Door een goede combinatie van goede backups- en archivering kan de schade en hinder beperkt worden.

Een belangrijke voorwaarde voor een goede backup is dat deze losgekoppeld ('airgap backup') van het interne netwerk bewaard wordt. Een backup naar een NAS is geen airgap backup en volstaat derhalve absoluut niet als dit de enige backup is. Van belang is om te weten dat alle op het interne netwerk aangesloten apparatuur (bijvoorbeeld: USB schijven, tapes, RDX apparatuur, lokale replicaties) bij een infectie of 'hack' kwetsbaar zijn en dat de daarop aanwezige informatie volledig en onherstelbaar verloren kan gaan. Hoewel een NAS of andere permanent op het LAN aangesloten systemen vaak prima als secundaire backup of voor archivering gebruikt kunnen worden dient u zich de kwetsbaarheid van deze systemen te realiseren. De via VPN gekoppelde systemen zijn in principe net zo kwetsbaar als aan het LAN gekoppelde systemen.

Ons advies:

Lokale backup

Minimaal 6 datadragers voor de dagelijkse backup en minimaal 2 – 4x per jaar alle data te archiveren naar een USB schijf die u op dan op een veilige plaats bewaard of die EQUA kosteloos, maar zonder aansprakelijkheid, voor u bewaard.

Een extra backup naar NAS en/of archiveren naar een NAS kunnen we ook adviseren met nogmaals de opmerking dat een NAS kwetsbaar is.

Combinatie van lokale en cloud backup

Hebt u niet de mogelijkheid om dagelijks de backup te wisselen? In dat geval is een combinatie van een permanent gekoppelde lokale backup in combinatie met een backup naar de cloud een goede oplossing. Indien mogelijk zullen we de lokale backup gebruiken maar in het geval de lokaal gekoppelde backup om wat voor een reden dan ook niet bruikbaar is kunnen we terugvallen op de backup in de cloud. Het nadeel van een cloudbackup is dat het terughalen van grote hoeveelheden data lang kan duren (tussen de 10 – 80 GB per uur, gemiddeld ca. 40GB per uur) en dat er een goede stabiele en snelle internetverbinding vereist is. Verder hebben wij bij een externe backup geen invloed op de beschikbaarheid van de data. Indien naar het datacenter van EQUA gebackuppeld wordt hebben we geen hinder van vertraging door het downloaden van internet al zal ook dan de gebackupte data nog naar een geschikt medium gekopieerd moeten worden.

Hoge beschikbaarheid en calamiteitenplan

In het geval dat het van belang is om bij een uitzonderlijke ernstige storing weer snel online te zijn kan gekozen worden voor een goede lokale backup in combinatie met replicatie naar eigen servers, virtuele en eventueel nog een *offsitebackup* van deze servers. Dit is echter maatwerk en als dit voor u van belang is dan denken wij graag met u mee om de best mogelijk oplossing te ontwikkelen.

Voorbeeld:

Een van onze best beveiligde klanten maakt dagelijks 2 backups: één backup naar RDX en één backup naar NAS. Verder wordt elke server gerepliceerd naar een eigen replicaserver en deze replicaserver repliceert op zijn beurt weer naar een externe replicaserver in het datacenter van EQUA. Tenslotte exporteren we elke 3 maanden alle virtuele servers naar een extern medium dat permanent bewaard wordt. Met deze opzet is aan alle voorwaarden voldaan:

1. Er zijn recente backups op RDX en NAS;
2. Data wordt gearhiveerd;
3. Bij uitval van een fysieke server kan de replica de taken snel overnemen;
4. Bij een ernstige calamiteit zoals brand, langdurige uitval van stroom, ernstige waterschade staat er een 'up-to-date' kopie van de belangrijkste servers bij EQUA klaar.

De kosten van een dergelijke oplossing zijn natuurlijk hoger dan een simpele (en vaak afdoende) lokale backup maar nog steeds prima betaalbaar, zeker gezien het feit dat bij uitval van de ICT bij deze klant een schadepost van meer dan 5000,00 per uur ontstaat.

Backupinstructies

Als u als opdrachtgever kiest voor een lokale backup dan is het van belang dat u de datadrager pas wisselt nadat u de melding ontvangen hebt dat de backup succesvol afgerond is. Als meerdere servers gebackuppeld worden dan zult u in het algemeen (afhankelijk van de gebruikte software) van elke server een separate backupmelding krijgen. Zorg ervoor dat u weet welke servers gebackuppeld moeten worden en vraag dit bij enige twijfel altijd na bij EQUA. Van belang is dat u ook het uitblijven van backupmeldingen direct bij EQUA meldt.

Versleuteling van backups

De standaard bij Windows inbegrepen backupsoftware versleutelt de backups niet. Dat betekent dat iedereen met enige kennis van IT de op de datadrager aanwezige informatie kan gebruiken en inzien. EQUA kan uw hele IT omgeving met de informatie op de backupdrager herstellen en anderen kunnen dat dan ook. Als u een veilige opslag, transport en opbewaren van de datadrager niet kunt garanderen dan is het verstandig om gebruik te maken van (optionele) backupsoftware die de data wel kan versleutelen. Als extra voordeel comprimeert deze software ook en dat levert naast andere voordelen ook meer backupcapaciteit en een hogere backupsnelheid op.

100% Zekerheid bestaat niet dus ook als u gebruik maakt van een versleutelde backup is het aan te raden om deze veilig te transporteren en op te slaan. De versleuteling moet beschouwd worden als een laatste verdedigingslinie.

Bewaar minimaal 1 maar liefst meerdere recente backups op een veilige plaats buiten het pand. Brandwerende datakluisen beschermen maar een bepaalde tijd tegen hoge temperaturen en de kans dat de backup bij brand, diefstal of waterschade verloren gaat is een reële mogelijkheid. Wij adviseren u dan ook om hier niet volledig op te vertrouwen.