Cyber Recovery Vault

Is uw IT-omgeving beschermd tegen Cyberaanvallen en ransomware?

Cyber Recovery as a Service managed by:

ACES
IT CONSULTANCY & SERVICES

Waarom Cyber Recovery Vault

Toename van cyberdreiging

Je kunt er nagenoeg niet omheen: iedere dag worden gemeenten, bedrijven of particulieren getroffen door ransomware of malware. Het is helaas niet meer de vraag of je gehackt wordt maar wanneer. Het gebeurt zelfs al vaak zonder dat we het doorhebben. Hoe heeft het zover kunnen komen, en belangrijker: wat kunnen we ertegen doen?

De gevolgen van een security-incident kunnen desastreus voor uw organisatie zijn. Denk aan verlies van omzet en reputatie-schade, dat mogelijk weer leidt tot een vertrouwensbreuk met uw klanten en voor gemeenten met burgers en politiek.

Zowel overheden zelf als bedrijven zijn verplicht om passende maatregelen te nemen om data na een Cyber aanval te kunnen herstellen. Bij overheid is dit met name de BIO en in het algmeen voor alle organisaties de nieuwe Europse richtlijn NIS2.

Bescherm uw bedrijfskritische data met een Cyber Recovery Vault

Veel organisaties en gemeenten hebben de laatste jaren goede stappen gezet voor wat betreft Security. Dit maakt het criminelen lastiger om eenvoudig in te breken. Voor wat betreft back-up zijn ook veelal goede stappen gezet door een Air Gap (offline back-up) te realiseren. Echter dat is niet voldoende.

Want kunt u garanderen dat uw back-up data niet is gecompromiteerd?



ACES IT biedt een innovatieve recovery oplossing die u als totaaloplossing of naast uw bestaande back-upstrategie kunt inzetten. Namelijk een voorziening die dagelijks uw data via een air gapped verbinding naar een verborgen Cyber-Vault verstuurt.
Binnen deze kluis wordt uw data gecontroleerd op bedreigingen. Hierdoor weet u dat u na een ransomware aanval uw omgeving met “schone” data kunt herstellen.

Voorkomen is beter dan genezen

De toename van security-incidenten is een duidelijk bewijs dat lang niet alle malware of ransomware wordt tegengehouden. Zero-day-kwetsbaarheden zijn kwetsbaarheden in software die worden uitgebuit voordat de softwarefabrikant de mogelijkheid heeft om een patch uit te brengen of te implementeren. Deze kwetsbaarheden zijn gevaarlijk voor de veiligheid van uw gegevens, daarom is het belangrijk om deze kwetsbaarheden proactief te detecteren en te verhelpen.

Deze zero-day-code kan nog niet worden opgemerkt door detectiesystemen, daarom is het slechts een kwestie van tijd voordat bedrijven te maken krijgen met malware of ransomware.

De toenemende populariteit van Ransomware-as-a-Service maakt het voor aanvallers eenvoudig om deze dienst af te nemen, waardoor het aantal incidenten de komende jaren alleen maar zal toenemen.

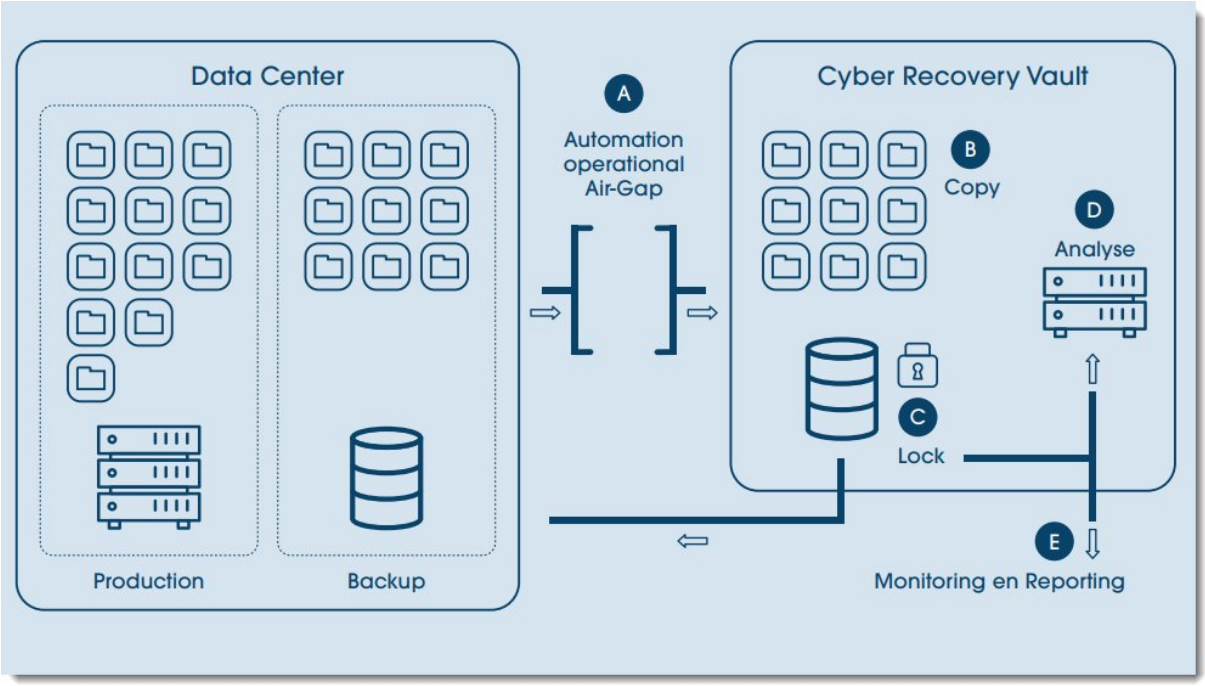
Het is daarom belangrijk om proactief maatregelen te nemen om deze incidenten te voorkomen in plaats van te genezen.

Het is dus beter om technische en organisatorische maatregelen te treffen om de back-upsystemen te beveiligen. Daarnaast is het onder andere verstandig om back-updata te versleutelen voordat het over het netwerk verstuurd word en gebruik te maken van retentie-locks.

Isoleren bespaart op de lange termijn

De beste en veiligste oplossing is een onveranderbare (immutable) kopie van uw back-updata en catalogus in een onzichtbare kluis te stoppen. Deze onzichtbare kluis, ook wel een cyber recovery vault genoemd, is compleet geïsoleerd van uw productieomgeving.

De cyber recovery vault is weergegeven in het onderstaande afbeelding.



In de Cyber Recovery Vault staat de Dell PowerProtect DD back-upvoorziening, welke dagelijks tijdelijk verbonden wordt met het productie-netwerk om een kopie van de back-updata en catalogus te ontvangen.

Beheer van het systeem wordt uitsluitend uitgevoerd door personen met de juiste rechten binnen de vault. De beheerders van de productieback-up hebben geen toegang tot dit systeem en de back-upkopieën zijn niet zichtbaar in de productieback-upapplicatie.

CyberSense

Het immutabel opslaan van data in een kluis is een belangrijke stap in de juiste richting voor de bescherming van uw data tegen ongeïdentificeerde malware of ransomware. Echter, alleen het opslaan is niet voldoende. Continu monitoring en analyse van de opgeslagen data is eveneens essentieel om verdachte veranderingen eerder te detecteren. Daarom bieden wij een optie aan om binnen de kluis een ‘clean room’ te gebruiken waar de data kan worden gecontroleerd zonder invloed van buitenaf. Hierdoor kunnen we getroffen bestanden en productiesystemen sneller herstellen en uw data beter beschermen.

Onze aanpak om data immutabel op te slaan in een kluis, is een belangrijke stap om ongeïdentificeerde malware of ransomware eerder te detecteren. Maar we gaan nog een stap verder. Wij bieden u de optie om binnen de kluis een ‘clean room’ te gebruiken, waar de data kan worden gecontroleerd zonder enige invloed van buitenaf. Hierdoor kunnen we getroffen bestanden en productiesystemen sneller herstellen en uw data beter beschermen. Zo bent u zeker dat uw data altijd veilig is.

De Cyber recovery service wordt aangeboden vanuit een redundant uitgevoerde datacenter.

Onze Cyber Recovery Vault is volledig geïsoleerd van de klant zijn eigen infrastructuur en is beschikbaar op basis van een abonnementsprijs per maand.

Uitwijk

Wij bieden u ook de mogelijkheid om binnen hetzelfde datacenter een uitwijk te realiseren. Deze optionele dienst stelt u in staat om na een aanval of andere calamiteit snel uw IT-omgeving te herstellen. Hiervoor worden er resources gereserveerd in de Cyber Recovery Vault, zodat u altijd beschikt over een betrouwbare oplossing in noodsituaties.

Aan de slag met ACES IT?

ACES IT: een team van passievolle IT specialisten

ACES IT is een landelijk opererende ICT-dienstverlener, gevestigd in Eindhoven. Binnen het gemeentelijke marktsegment en bij een groot aantal MKB-bedrijven is ACES IT bekend als een “trusted advisor” en dé specialist voor professionele ICT-infrastructuren. Ons belangrijkste DNA bestaat uit een combinatie van specialistische kennis, vertrouwen, servicegerichtheid en een grote betrokkenheid bij onze opdrachtgevers. Wij zijn toegewijd aan het leveren van topkwaliteit ICT-diensten en het creëren van waardevolle partnerships met onze klanten.

Informatiebeveiliging

InformatiebeveiligingTegenwoordig zijn een goede continuïteit en informatiebeveiliging steeds belangrijker (lees essentieel) als uitgangspunt in de werkwijze van een IT-partner. Voor overheden een zeer belangrijk onderwerp (denk hierbij aan de bestaande regelgeving en de implementatie van de Baseline Informatiebeveiliging Overheid (BIO)). ACES IT hanteert kwaliteits- en informatiebeveiliging als uitgangspunten. Dit hebben wij in onze organisatie en werkwijzen vastgelegd in ISO9001:2015 en ISO27001:2013 procedures.

ACES IT Consultancy & Services

Dillenburgstraat 49
5652 AM Eindhoven

W: www.aces-it.nl
T: 040 - 264 53 00
E: consultancy@aces-it.nl