PlatformOne
MANAGED BY VISOLITY

Cyber Recovery Vault

Cyberaanval of Ransomeware?

Is uw ICT omgeving beschermd?

platformone.nl

Bedrijfskritische data beschermen met een Cyber Recovery Vault

Je kunt er nagenoeg niet omheen. Iedere dag worden bedrijven of particulieren getroffen door ransomware of malware. Het is helaas niet meer de vraag of je gehackt wordt maar wanneer; het gebeurt al vaak zonder dat we het door hebben. Uit een rapport van het Nationaal Cyber Security Centrum bleek dat er wereldwijd 1800 bedrijven zijn getroffen door gijzelsoftware. Een aantal daarvan zijn Nederlands. Het werkelijke aantal is waarschijnlijk veel hoger.
Hoe heeft het zover kunnen komen en wat moeten bedrijven er tegen doen? We zetten het voor je op een rij.

Denial of service

Iedereen denkt dat cyber attacks stammen uit het laatste decennium. In werkelijkheid is het begonnen met de introductie van computers ruim 40 jaar geleden. Het eerste wormvirus dateert uit 1971 en was niet schadelijk, maar gaf een onschuldig bericht weer op het scherm van een geïnfecteerd systeem. De focus ging daarna veelal naar denial of service en diefstal van data. Denk hierbij aan het onbruikbaar maken van een website of dienst op internet, diefstal van identiteit, credit card informatie of het stelen en delen van intellectuele eigendommen. Dit resulteerde niet in het verlies of vernietiging van data. Daarmee was het weliswaar vervelend maar had vaak beperkt of geen invloed op het functioneren van de organisatie. Dit heeft ervoor gezorgd dat er afweermechanismen zijn geïmplementeerd zoals encryptie, beperken van rechten en firewalls om data veilig te houden.

Cyber Recovery Vault

Cyberaanval of Ransomeware? Is uw ICT omgeving beschermd?

Cyber destructie & cyber afpersing

Het laatste decennium vond er echter een verandering plaats. De opkomende bedreigingen zijn nu cyber destructie ook wel malware genoemd, het vernietigen van primaire en back-up data, en cyber afpersing ofwel ransomware, het versleutelen van data totdat losgeld is betaald. Waarom? Data is, hoe je het wendt of keert, het nieuwe goud van iedere organisatie.

Een voorbeeld hiervan is de Sony Pictures cyber-attack uit 2014. Voordat Sony's IT beheerders de uitbraak konden stoppen had de malware alle data overschreven op 3262 van de 6797 personal computers en op 837 van de 1555 servers.

Om er zeker van te zijn dat niets hersteld kon worden, werd de data op 7 verschillende manieren overschreven. Vervolgens werd van het besturingssysteem de opstartsoftware vernietigd, wat de systemen totaal onbruikbaar maakten. Tijdens de cyber-attack zijn ook de back-ups op disk aangevallen met het doel om herstel onmogelijk te maken en werden nog niet uitgebrachte films verspreid op het internet.

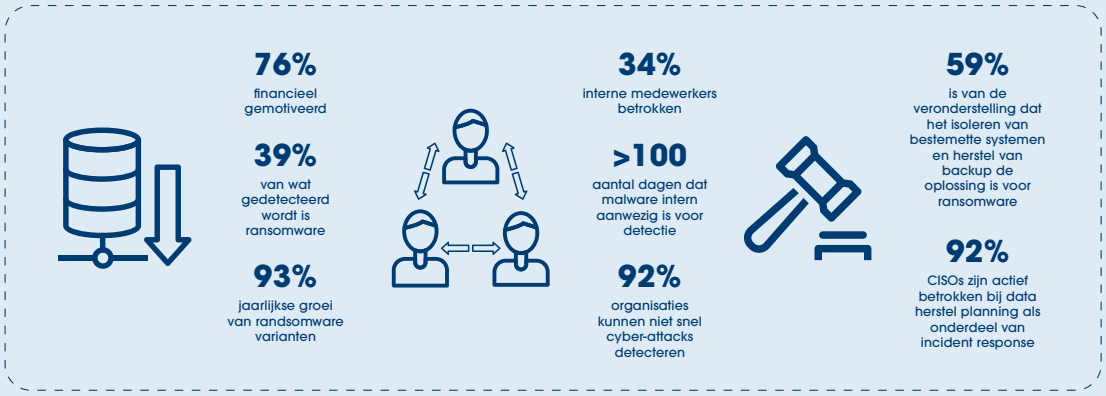
Er is gebleken na onderzoek dat de hackers met ondersteuning van interne medewerkers al maanden op het interne netwerk actief waren en in deze tijd informatie en rechten hadden verzameld om de aanval effectief te kunnen uitvoeren. Het heeft maanden gekost om alles te herstellen met oplopende kosten tot vele honderden miljoenen dollars. De reputatieschade was bijna niet meer te overzien. Dit was ook het begin van steeds geavanceerdere aanvallen op anderegerenom-meerde bedrijven.

Marktonderzoek

Telecomprovider Verizon deed onderzoek naar cyber-aanvallen en daar kwamen opmerkelijke en schrikbarende bevindingen naar boven.

Zo…

- waren 76% van de aanvallen financieel gemotiveerd;
- waren in 34% van de incidenten eigen medewerkers bewust of onbewust betrokken;
- is de malware is meer dan 100 dagen op de interne systemen aanwezig voordat het gedetecteerd wordt;
- is de jaarlijkse groei van ransomware varianten is met 93% enorm;
- kunnen 92% van alles organisaties cyber attacks niet snel detecteren en dus ook niet tijdig ingrijpen;
- En denkt 59% van de ondervraagden te kunnen volstaan met het isoleren van de besmette systemen en herstellen van de back-up.



Bron: 2019 Verizon Data Breach Investigation Report, SecureWorks 2017 State of Cybercrime, Enterprise Strategy Group, Isolated Recovery Opportunity Research, 2018

Bij ransomware wordt er vaak relatief weinig losgeld gevraagd. Dit is slechts een klein deel van de werkelijke totale kosten van de aanval. Zonder data geen bedrijfsvoering is ons motto. De gevolgen van een incident kunnen desastreus voor je organisatie zijn. Denk hierbij aan verlies van omzet en reputatieschade wat mogelijk weer leidt tot een vertrouwensbreuk met uw klanten.

Ook wordt vaak na het betalen van het losgeld niet de decryptie software gegeven en is de kans groot dat na verloop van tijd er een tweede aanval zal worden gedaan. De aanvaller weet immers dat er hoogstwaarschijnlijk weer zal worden betaald.

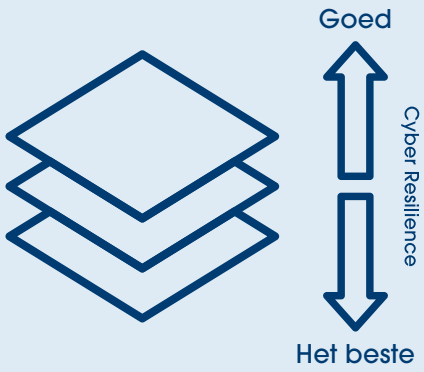
Cyber Recovery Vault

Cyberaanval of Ransomeware? Is uw ICT omgeving beschermd?

Voorkomen is beter dan genezen

Deze toename van incidenten bewijst dat lang niet alle malware of ransomware wordt tegengehouden. Zogenaamde zero-day code kan nog niet worden gedetecteerd door detectiesystemen. Het is daarom slechts een kwestie van tijd voor bedrijven te maken gaan krijgen met malware of ransomware. Dan is er ook de toenemende populariteit van ransomware-as-a-service. Ransomware is daarmee eenvoudig als dienst af te nemen. Zelfs met ondersteuning in verschillende talen. Dit zorgt er mede voor dat het aantal incidenten de komende jaren alleen nog maar verder zal toenemen. Voorkomen is daarom beter dan genezen.

Het beschermen tegen cyber attacks ofwel cyber resilience heeft verschillende lagen. Deze gaan van goed naar beter naar best. Het is goed om data veilig te stellen met een back-up op disk of tape en herhaaldelijk het herstel te testen. Maar kwaadwillenden hebben steeds vaker het doel om naast primaire data ook back-up data te vernietigen of te versleutelen.



Het is dus beter om de back-up systemen product specifiek te ‘hardenen’ door bijvoorbeeld een firewall aan te zetten, geen gebruik te maken van CIFS of NFS shares of onnodige services uit te schakelen. Versleutel daarnaast back-up data voordat het over het netwerk verstuurd wordt en gebruik retentie-locks met aparte security office credentials en twee staps authenticatie.

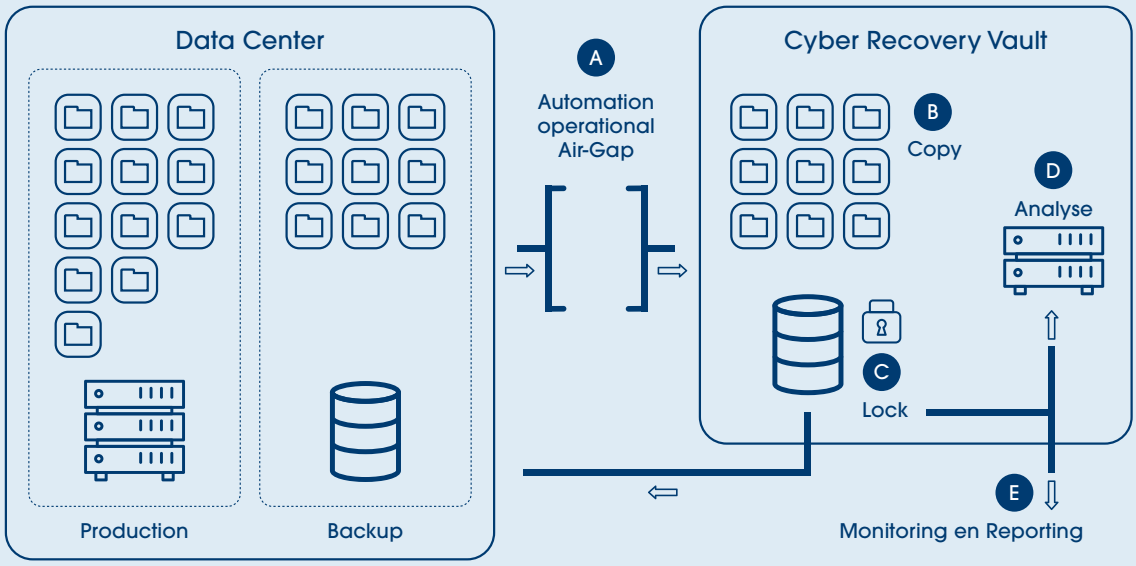
Cyber Recovery Vault

Cyberaanval of Ransomeware? Is uw ICT omgeving beschermd?

Isoleren bespaart op de langere termijn

De beste (en veiligste) oplossing is een onveranderbare kopie (immutable) van back-up data en catalogus in een onzichtbare kluis te stoppen. Deze onzichtbare kluis, ook wel een cyber recovery vault genoemd, is zowel fysiek, als qua netwerk connectiviteit afgesloten van uw productie omgeving.

De cyber recovery vault is weergegeven in het onderstaande afbeelding.



In de cyber recovery vault staat de Data Domain die beperkte tijd vanuit de kluis met het productienetwerk wordt verbonden om een kopie van back-up data en catalogus te ontvangen.

Beheer van en in de vault kan alleen worden uitgevoerd door een speciaal daarvoor aangewezen persoon of meerdere personen. Dit zijn bij Visolity de security officer in combinatie met een aangewezen beheerder en de directie. De productie back-up beheerder heeft geen rechtenop dit systeem en de back-up kopie is niet zichtbaar in de productie back-up applicatie.

Controleren ontkom je niet aan

Het verbergen van data in een kluis is de juiste aanpak, maar niet de oplossing voor alles. Anders zou een tape ook voldoen. Je moet de opgeslagen data ook continu blijven analyseren op verdachte veranderingen die duiden op malware of ransomware.

Want wanneer weet je dat data geïnfecteerd is? Hiervoor wordt met cyber recovery software de data in de kluis automatisch geanalyseerd op verdachte veranderingen zoals aangepaste file extensies, bestandsgrootte, corrupte file structuur, corrupte file content of deels versleutelde bestandsinhoud.

Vervolgens wordt hier direct over gerapporteerd. Met deze aanpak kan nog niet eerder geïdentificeerde malware of ransomware worden gedetecteerd.
Het is mogelijk om binnen de kluis in een "clean-room" de data te controleren zonder invloed van buiten en daarna getroffen productiesystemen te herstellen.

Visolity heeft deze oplossing in haar redundant Datacenter toegepast voor hun klanten

De Cyber Recovery Vault is volledig geïsoleerd van de eigen infrastructuur. De oplossing is op basis van een abonnement per maand.

Vraag vrijblijvend naar de mogelijkheden voor uw organisatie.

PlatformOne
MANAGED BY VISOLITY

platformone.nl

PlatformOne
MANAGED BY VISOLITY

Visolity
James Cookstraat 35
7825 AN Emmen

E info@visolity.nl
T 0591 – 66 82 72

platformone.nl