PlatformOne
MANAGED BY VISOLITY

Cyber Recovery Vault

Is uw IT-omgeving beschermd tegen cyberaanvallen en ransomware?

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 zelfs al vaak zonder dat we het doorhebben.
Hoe heeft het zover kunnen komen, en belangrijker:
wat kunnen bedrijven ertegen doen?

Denial of service

Veel mensen denken dat cyberaanvallen stammen uit het internettijd-perk. In werkelijkheid begon het 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 verschoof door de introductie van internet vooral naar Denial-of-Service en datadiefstal. Denk hierbij aan het onbruikbaar maken van een website, diefstal van identiteit, creditcardinformatie of het stelen en delen van intellectuele eigendommen. Dit resulteert niet direct in het verlies of vernietiging van data. Daarmee was zo'n aanval weliswaar vervelend, maar had het weinig invloed op het functioneren van de organisatie. Het leidde wel tot de implementatie van afweersystemen als encryptie, het beperken van rechten, en firewalls om data te beschermen.

Cyber Recovery Vault

Cyberaanval of Ransomeware? Is uw ICT omgeving beschermd?

Cyber destructie & cyber afpersing

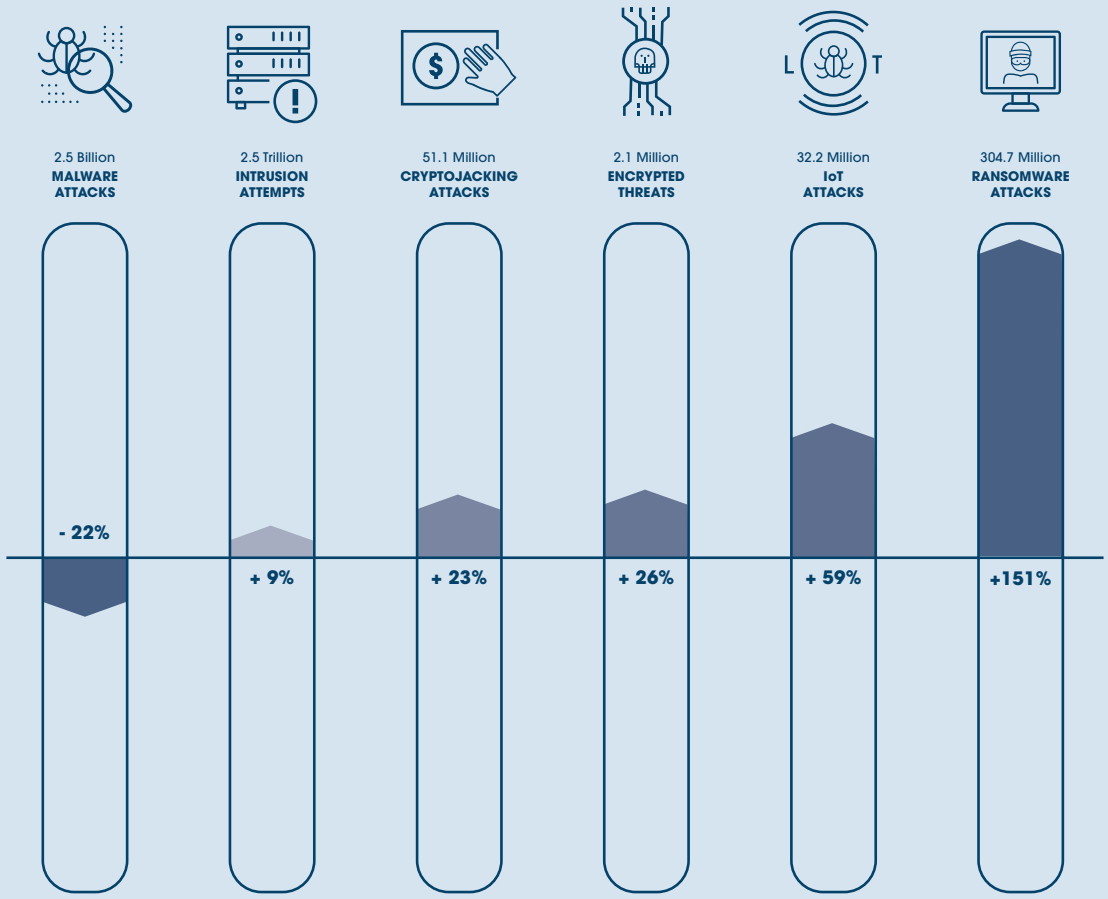
In het laatste decennium veranderde de aard van cyberaanvallen. De huidige bedreigingen zijn op dit moment voornamelijk malware en ransomware. Malware is ontworpen voor cyberdestructie en is gericht op het vernietigen van primaire data en back-updata. Ransomware versleutelt data totdat de getroffen partij losgeld betaalt: cyberafpersing. Kortom: data is het nieuwe goud van iedere organisatie geworden.

Een bekend voorbeeld is de Sony Pictures-cyberaanval uit 2014. Voordat Sony's IT-beheerders de aanval konden stoppen had de malware alle data overschreven op de helft van alle desktops en servers.

Om er zeker van te zijn dat niets hersteld kon worden, werd de data op zeven verschillende manieren overschreven. Vervolgens vernietigde de malware ook de opstartsoftware van de systemen, wat ze totaal onbruikbaar maakte, en verspreidde het nog niet uitgebrachte films op het internet.

Na onderzoek bleek dat de hackers al maanden op het interne netwerk actief waren en de informatie en rechten hadden verzameld om de aanval effectief te kunnen uitvoeren. Het kostte maanden en vele honderden miljoenen dollars om de schade te herstellen: een duidelijk teken dat cyberaanvallen steeds geavanceerder werden.

Global Cyberattack Trends 2021



Mid-Year Update: 2021 SonicWall Cyber Threat Report | 2021 Global Cyberattack Trends

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

Ook ontvangen organisaties na betaling vaak niet de decryptiesoftware en is de kans groot dat er na een tijd een tweede aanval wordt gedaan: de aanvaller weet immers dat er weer wordt betaald.

Cyber Recovery Vault

Cyberaanval of Ransomeware? Is uw ICT omgeving beschermd?

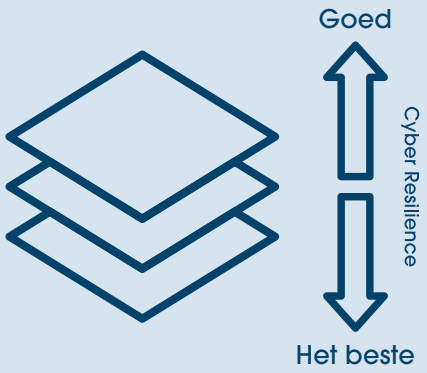
Voorkomen is beter dan genezen

De toename van security-incidenten bewijst 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 zero-day-code kan dus nog niet worden opgemerkt door detectiesystemen. Het is daarom slechts een kwestie van tijd voordat bedrijven te maken krijgen met malware of ransomware.

Dan is er ook de toenemende populariteit van Ransomware-as-a-Service, waarmee het eenvoudig als dienst is af te nemen.

Dit zorgt ervoor dat het aantal incidenten de komende jaren alleen nog maar verder toeneemt. Voorkomen is daarom beter dan genezen.



Het is dus beter om de back-upsystemen specifiek per product te beveiligen door bijvoorbeeld een firewall aan te zetten, geen gebruik te maken van CIFS- of NFS-shares, of onnodige services uit te schakelen.

Daarnaast is het verstandig om back-updata te versleutelen voor het over het netwerk te versturen en retentie-locks met aparte security-credentials en tweestaps-authenticatie te gebruiken.

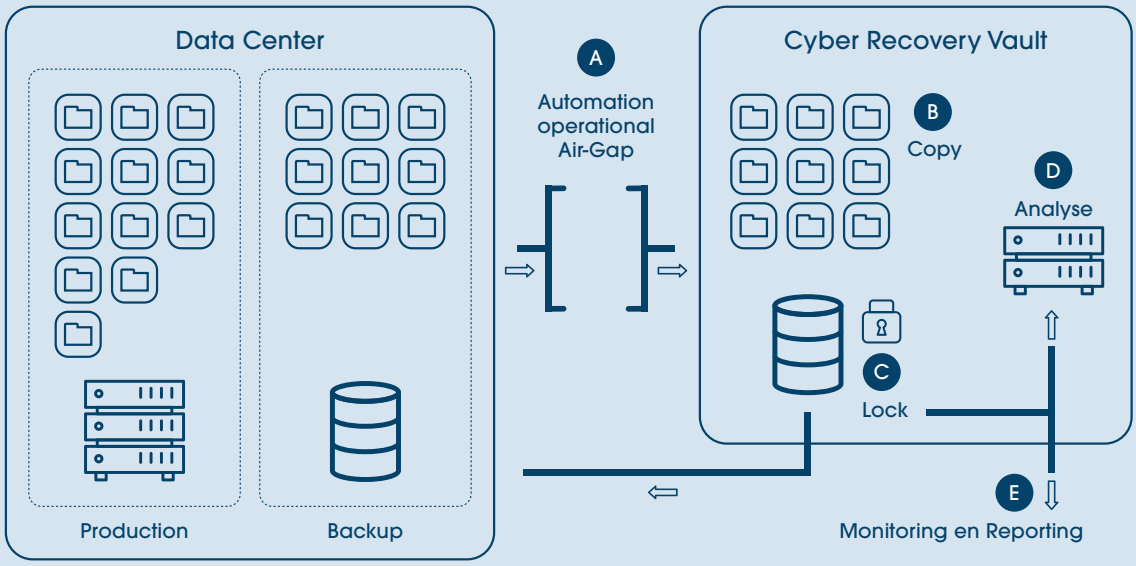
Cyber Recovery Vault

Cyberaanval of Ransomeware? Is uw ICT omgeving beschermd?

Isoleren bespaart op de langere termijn

De beste en veiligste oplossing is een onveranderbare (immutable) kopie van 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 een Data Domain dat beperkte tijd vanuit de kluis met het productienetwerk wordt verbonden om een kopie van back-updata en catalogus te ontvangen.

Beheer kan alleen in de vault uitgevoerd worden door personen met de juiste rechten. De beheerder van de productieback-up heeft geen rechten op dit systeem en de back-upkopie is niet zichtbaar in de applicatie voor de productieback-up.

Maar: controle blijft onvermijdelijk

Het bewaren van data in een kluis is de juiste aanpak, maar niet de oplossing voor alles. Anders zou back-up op een tape immers ook voldoen. Je moet de opgeslagen data continu blijven analyseren op verdachte veranderingen die duiden op malware of ransomware. Want wanneer weet je dat data geïnfecteerd is?

Onze cyber recovery software analyseert de data in de kluis automatisch op verdachte veranderingen zoals aangepaste bestandsextensies, bestandsgrootte, beschadigde bestandsstructuur en corrupte of versleutelde content. Vervolgens ontvangt de beheerder direct een rapport.

Met deze aanpak kan ongeïdentificeerde malware of ransomware eerder worden gedetecteerd. Het is mogelijk om binnen de kluis in een 'clean room' de data te controleren zonder invloed van buitenaf en daarna de getroffen productiesystemen te herstellen.

Visolity biedt deze service aan vanuit haar redundant uitgevoerde datacenter

Onze Cyber Recovery Vault is volledig geïsoleerd van de klant zijn eigen infrastructuur en beschikbaar 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