Ransomware:

Hoe het risico te beheersen

AIG®

Ransomware: wat het is en hoe het werkt

Hoe het werkt

Ransomware is ontworpen om bestanden of systemen binnen te dringen en deze te gijzelen. Een veelgebruikte methode is het sturen van misleidende berichten via e-mail, sociale media, of pop-ups die de ontvanger nietsvermoedend opent. Door het klikken op links of het openen van bijlagen, krijgt de ransomware toegang tot alle verbonden bestanden, netwerken of systemen en worden deze geblokkeerd.

Mogelijke gevolgen

De mogelijke gevolgen van een besmetting met ransomware zijn verlies van gevoelige informatie, storingen van IT systemen, reputatieschade en bedrijfsschade (financieel verlies). Het betalen van losgeld garandeert echter niet dat de versleutelde bestanden weer worden vrijgegeven. Sterker nog, het kan zelfs tot gevolg hebben dat de bankgegevens van het slachtoffer openbaar worden gemaakt. Zelfs decodering hoeft niet in te houden dat de ransomware besmetting ook daadwerkelijk is verwijderd.

Wat is ransomware?

Ransomware, oftewel gijzelsoftware, is kwaadaardige of schadelijke software die bestanden of systemen binnendringt en vervolgens de toegang daartoe blokkeert. De aangetaste bestanden, of zelfs gehele apparaten, worden dan gegijzeld en de toegang is geblokkeerd door het te versleutelen. Pas als het slachtoffer losgeld heeft betaald, wordt het wachtwoord vrijgegeven om de versleutelde delen weer toegankelijk te maken.

Grote aanvallen met ransomware

Ransomware blijft het cyberveiligheids-landschap in 2019 en 2020 domineren. Bedrijven van groot tot klein betalen miljoenen om versleutelde bestanden te decoderen en weer beschikbaar te maken. Enkele van de tot nu toe bekende zwaarste ransomware-aanvallen zijn: NotPetya (2017), WannaCry (2016), Petya (2016), LOcky (2016), CryptoWall (2014) en CryptoLocker (2014). Maar ook in Nederland kennen we voorbeelden, zoals recent met de Universiteit van Maastricht.

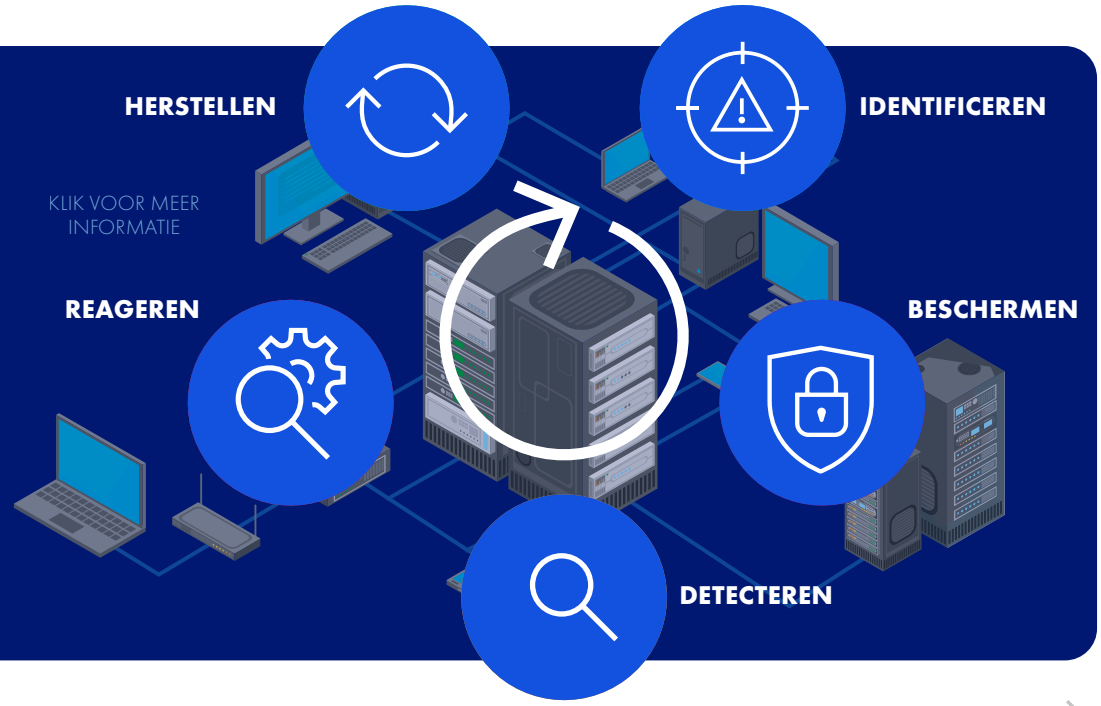
Ransomware ontwikkelingen

Cybercriminelen zijn de laatste jaren steeds professioneler geworden en hebben professionele dienstverleningsprogramma's opgezet rondom de verspreiding van malware/ ransomware. Hier zitten vaak complete teams achter met zogenaamde call centers en helpdesks om de slachtoffers te 'helpen' bij het terugkrijgen van de data.

Beheersing van het risico van ransomware besmettingen

Het raamwerk voor cyberveiligheid van het 'National Institute of Standards and Technology' (NIST) beschrijft vijf belangrijke stappen in het voorkomen en beheersen van een aanval met ransomware: Identificeren, Beschermen, Detecteren, Reageren en Herstellen.

Om klanten van AIG te informeren hebben we dit raamwerk gebruikt als systematische basis voor het voorkomen en beheersen van een ransomware-aanval, waaronder een koppeling met onze Cyber Impact Scans en analyses en de preventieve diensten die gekoppeld zijn aan onze cyberverzekering.



Een besmetting voorkomen:

IDENTIFICEREN

Het voorkomen van een besmetting begint met het identificeren van...

- De belangrijkste bedrijfsmiddelen van de organisatie, zowel fysiek als de data en de software, maar ook de bedrijfsomgeving die de organisatie ondersteunt. Denk aan de rol van de organisatie in de supply chain en de plaats die de organisatie inneemt in de kritieke infrastructuur van de sector.
- Kwetsbaarheden van IT systemen, software, data of andere bedrijfsmiddelen en bedreigingen voor de organisatie en de vaardigheden gericht op het reageren op risico's.
- Factoren met betrekking tot de betrouwbaarheid, beschikbaarheid en bruikbaarheid van de IT en OT moeten in acht worden genomen op de gehele inventarisatie inclusief apparatuur die mogelijk onbeheerd is.

AIG en onze partners kunnen u helpen bij dit identificatieproces en hebben hiervoor een aantal diensten beschikbaar

AIG Cyber Impact Scan/Analyse*

AIG's prijswinnende technologie helpt een organisatie haar profiel met betrekking tot cyberrisico's te bepalen, geeft inzicht in de prioriteiten voor de meest effectieve beveiligsmaatsregelen en helpt beter te investeren in het programma voor cyberbeveiliging als geheel. Ook bij het aanschaffen van een cyberverzekering. Daarnaast geeft het een goed inzicht in de mogelijke financiële impact van een cyberincident op de organisatie. De Cyber Impact Scan kan zelfs al worden aangevraagd voordat er een verzekering bij AIG is afgesloten.

BitSight technologie***

BitSight genereert beoordelingen voor organisaties om zo hun eigen netwerk en dat van hun externe leveranciers te meten en te controleren. De beoordelingen worden onopvallend gegenereerd, doordat BitSight continue de van buitenaf waarneembare, vrij toegankelijke gegevens meet. Organisaties met een cyberverzekering van AIG komen in aanmerking voor een gratis BitSight Security Rating rapport om hun prestaties op het gebied van bedrijfsbeveiliging te meten.

Security Scorecard***

Het cyberveiligheidsrisico van partners, leveranciers en verkopers is een belangrijk aandachtsgebied van bedrijven. De Security Scorecard levert een overzicht dat organisaties in staat stelt om de beveiliging van hun netwerk en die van verkopende derden te meten en te monitoren. Hierdoor krijgen organisaties controle over het ecosysteem van derden (leveranciers en/of afnemers) en kunnen ze hun meest risicovolle leveranciers bepalen.

AIG Cyber Services inventarisatiegesprek**

Een gesprek van een uur met een AIG Cyber Risk Expert of Engineer waarin eventuele vragen over het risicoprofiel en aanbevelingen uit de Cyber Impact Analyse aan de orde komen. Daarnaast maakt u kennis met de (gratis) diensten van AIG en haar partners waarmee u de cyberrisico's die u loopt kunt verkleinen.

Executive Threat Briefing****

De AIG Cyber Risk Advisory's Executive Threat Brief is een workshop met als doel uw organisatie te helpen beter inzicht te krijgen in de huidige specifieke cyberveiligheidsrisico's van uw sector. Daarnaast krijgt u informatie over de huidige methoden die aanvallers gebruiken, zodat u uw bedrijf beter kunt verdedigen.

Axio Cyber Risk Quantification / Dependencies****

Kwantificering van de blootstelling aan cyberrisico's in een workshop van een dag door onze partner Axio. Dit kan worden ingepland als één volledige dag, of kan worden opgedeeld in meerdere bijeenkomsten.

* Gratis voor klanten van de AIG cyberverzekering | ** Gratis voor klanten de AIG cyberverzekering met een premie van meer dan €5.000,--
*** Gratis toegang voor de verzekerde onderneming | **** Neem contact op met AIG voor informatie over beschikbaarheid

Een besmetting voorkomen:

BESCHERMING

Het voorzien in effectieve bescherming houdt in dat er een reeks maatregelen voor de beveiliging van informatie wordt genomen en er processen en procedures worden ingesteld ter beveiliging van informatiesystemen en -middelen. Hierbij moet er rekening worden gehouden met verschillende aspecten, waaronder:

- Het updaten van IT en OT.
- Het maken en testen van online en offline back-ups van gegevens en systeeminformatie, opgeslagen op verschillende locaties.
- Netwerksegmentatie en systeem 'hardening' om zo veel mogelijk veiligheidsrisico's te elimineren.
- Betrokkenheid van de werknemers creëren door middel van bewustwording en training, inclusief het specifiek opleiding van gebruikers van kritische systemen.

AIG en onze partners kunnen u met een reeks aan diensten helpen bij het implementeren van beveiligingsmaatregelen.

TechGuard SHIELD**

Awareness trainingen voor medewerkers inclusief phishingtraining en simulaties. Een unieke opleidingsmethode gericht op Beoordelen (assess), Opleiden (educate), Versterken (reinforce) en Meten (measure) zijn de vier belangrijkste componenten van een succesvol opleidingsprogramma om het bewustzijn van cyberveiligheid te verhogen. Een demo of proefversie is op aanvraag beschikbaar.

Bandura Threat Intelligence Gateway (TIG)**

De Bandura PoliWall is een hardwarecomponent die u in het bezit krijgt en gebruik maakt van IP- en domeinblokkades. Dit is een snelle en eenvoudige oplossing voor vergaande beveiliging. Hiermee worden mogelijke aanvallen tot 90% teruggedrongen.

Office of the CISO powered by Optiv****

Optiv biedt op afroep toegang tot virtuele, interim en persoonlijke expertise van een CISO, maar ook toegang tot essentiële diensten op het gebied van veiligheidsadvies die zijn afgestemd op de behoefte van uw specifieke organisatie.

BitSight technologie en Security Scorecard***

Externe veiligheidsbeoordeling.

* Gratis voor klanten van de AIG cyberverzekering | ** Gratis voor klanten de AIG cyberverzekering met een premie van meer dan €5.000,--
*** Gratis toegang voor de verzekerde onderneming | **** Neem contact op met AIG voor informatie over beschikbaarheid

Een besmetting voorkomen:

DETECTEREN

Het detecteren van afwijkingen en incidenten is de derde stap in het succesvol voorkomen van een besmetting met ransomware. Dit houdt in:

- Het implementeren van 'Security Continuous Monitoring' om cyberincidenten continu te monitoren en de doeltreffendheid van de beveiligingsmaatregelen, met inbegrip van de netwerk- en fysieke activiteiten, te verifiëren.
- Het in stand houden van detectieprocessen om de aandacht te vestigen op afwijkende gebeurtenissen.

Het zorgen voor snelle detectie begint met het opzetten van 'Security Information and Event Management' (SIEM) of zelfs een 'Security Operation Center' (SOC) met goede informatie over dreigingen. Een goede netwerk infrastructuur en het inzicht in alle werkstations (waaronder laptops en telefoons) helpt uw organisatie om de detectie te vergemakkelijken.

AIG en onze partners kunnen u met onze dienstverlening helpen bij het detecteren van eventuele voorvallen:

TechGuard Securities Vulnerability Scan**

- Identificeer, kwantificeer en classificeer de kwetsbaarheden binnen uw computeromgeving door gebruik te maken van scans van buitenaf.
- Tot 250 IP-adressen.
- Identificeert huidige kwetsbaarheden en 'fals positives'.
- Een uitgebreid rapport met drie dagen aan scanwerkzaamheden, ondersteuning na de analyse en een herbeoordelingsscan binnen 90 dagen na het originele rapport.

Dark Web Intelligence door BlueVoyant****

Samenvatting van de resultaten van het onderzoek op het Dark Web:

- Scant duizenden bronnen op het Dark Web, inclusief meertalige forums, de zwarte 'cyber' markt, Automatic Vending Machines (AVM's), knip- en plaksites, Instant-messaging / chatplatforms en meer.
- Verzamelt informatie over relevante aanvallers: hun plannen, methoden en gebruikte hulpmiddelen en gelekte klantspecifieke informatie.

RSA NetWitness® Endpoint****

- Geïntegreerde 'endpoint' (laptops, tablets, telefoons) detectie en passende response-oplossing.
- Helpt SOC- en IT-teams inzicht te krijgen in de volledige omvang van een aanval voor zowel het netwerk als 'endpoints'

BitSight technologie en Security Scorecard***

Externe veiligheidsbeoordeling.

* Gratis voor klanten van de AIG cyberverzekering | ** Gratis voor klanten de AIG cyberverzekering met een premie van meer dan €5.000,--
*** Gratis toegang voor de verzekerde onderneming | **** Neem contact op met AIG voor informatie over beschikbaarheid

REAGEREN

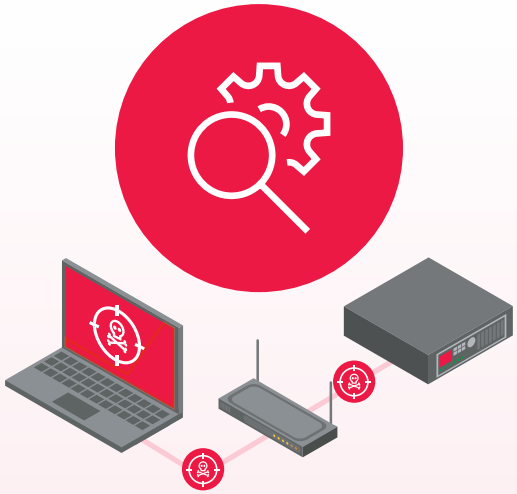
voor en na een besmetting

Voordat een besmetting plaatsvindt, is een goed ontwikkeld reactiemechanisme binnen de organisatie onmisbaar en helpt die tijdens een besmetting met ransomware om de potentiële schade te beperken. Dit kan inhouden:

- Maatregelen die worden uitgevoerd om uitbreiding na een voorval te voorkomen en om het incident op te lossen.
- Het implementeren van verbeteringen voortgekomen uit de lessen die zijn geleerd van eerdere incidenten en activiteiten gericht op detectie en reactie.
- Dit alles vereist de oprichting van een CSIRT (Cyber Security Incident Response Team) dat een getest Incident Response Plan heeft ontwikkeld om de reactie op voorvallen te beschrijven.

Na een besmetting, moeten reactief maatregelen worden genomen, waaronder:

- Zorgdragen voor een goed uitgevoerde Response Planning tijdens en na een incident.
- Het managen van de communicatie met interne stakeholders, wetshandhavingsinstanties en externe stakeholders tijdens en na een incident.
- Het uitvoeren van een analyse om te zorgen voor een doeltreffende reactie en ondersteuning van herstelactiviteiten, zoals forensische analyse en het bepalen van de gevolgen van incidenten.



AIG en onze partners kunnen u met onze dienstverlening helpen bij het reactieproces:

RSA Incident Response Retainer****

Incident Response retainers zijn proactieve beveiligingsmaatregelen die de tijd van een aanvaller aanzienlijk kunnen verkorten en de gevolgen van een cyberincident aanzienlijk kunnen verminderen.

Incident Simulatie Workshop****

Het doel van de AIG Cyber Risk Incident Simulatie Workshop is tweeledig. Enerzijds helpt het ervoor te zorgen dat uw incident response plan uw organisatie doeltreffender laat reageren wanneer zich een cyberincident voordoet. Anderzijds helpt het om het AIG claims proces beter te begrijpen.

* Gratis voor klanten van de AIG cyberverzekering | ** Gratis voor klanten de AIG cyberverzekering met een premie van meer dan €5.000,--
*** Gratis toegang voor de verzekerde onderneming | **** Neem contact op met AIG voor informatie over beschikbaarheid

HERSTELLEN

na een ransomware aanval

Mocht er toch uitval zijn van systemen, of verlies van data, dan is het van belang om de operationele processen weer zo snel mogelijk op gang te krijgen en de bedrijfscontinuatieplannen uit te voeren. Dit alles ondersteunt een tijdige hervatting van de normale bedrijfsvoering om de gevolgen van een besmetting met ransomware te verkleinen.

Organisaties moeten de herstelprocessen en -procedures uitvoeren om systemen en/of bedrijfsmiddelen die zijn getroffen door incidenten te herstellen door (offsite) backups terug te zetten om de bedrijfsvoering zo spoedig mogelijk te hervatten.

AIG en onze partners kunnen u als onderdeel van onze ondersteuning bij claims helpen in het geval van cyberincidenten:

AIG: Cyber Hotline*

Onze CyberEdge Claims Hotline is 24/7/365 beschikbaar. Het Cyber Claims Team overlegt met u over het implementeren van uw reactieplan en het inschakelen van de noodzakelijke forensisch IT, juridisch en/of crisiscommunicatie dienstverleners. Hierdoor kunnen directe bedreigingen worden geïdentificeerd en kan er worden begonnen met het herstel- en terugzetproces.

Incident response: forensisch IT

Als onderdeel van de First Response binnen de AIG cyberverzekering heeft u toegang tot forensisch IT experts.

Incident response: juridisch

Als onderdeel van de First Response binnen de AIG Cyberverzekering heeft u toegang tot juridische experts.

Incident response: Crisiscommunicatie en PR

Als onderdeel van de First Response binnen de AIG Cyberverzekering heeft u toegang tot experts op het gebied van PR en crisiscommunicatie.

* Gratis voor klanten van de AIG cyberverzekering | ** Gratis voor klanten de AIG cyberverzekering met een premie van meer dan €5.000,--
*** Gratis toegang voor de verzekerde onderneming | **** Neem contact op met AIG voor informatie over beschikbaarheid

AIG Europe S.A., Netherlands Branch
Crystal Building B
Rivium Boulevard 216-218
2909 LK Capelle aan den IJssel

GBL00003649 0220