uniserver

Paniekvoetbal of zorgvuldig geplande herstel-acties

Alles wat je moet weten over **ransomware**

We leven in een snel veranderende wereld. Digitale technologie transformeert markten, soms disruptief, soms gestaag. Het levert kansen op voor bedrijven om efficiënter te worden, makkelijker samen te werken. Sneller dingen te realiseren. Veel onbekender dan de kansen, zijn de bedreigingen die digitalisering met zich meebrengt voor ondernemingen. Maar 'Cybercrime' groeit hard en is na fraude volgens het 2016 Economic Crime Survey van PwC inmiddels de op een na grootste gerapporteerde economische misdaad.

Ransomware, het nieuwe soort cybercrime

Aanvallen op data en andere waardevolle bedrijfsonderdelen zijn niets nieuws. Wat wél nieuw is, is dat data in gijzeling wordt gehouden door criminelen, ransomware genoemd. Stel je eens voor: van het ene op het andere moment kun je niet meer bij al je bedrijfsgegevens. Van de administratie tot en met e-mails, cliëntgegevens en misschien wel intellectueel eigendom of andere waardevolle data. Dan heb je het niet alleen over bedrijfsgegevens. Het gaat over je hele bedrijfsvoering. De vraag is: wat is het je waard om die toegang terug te krijgen?

Ransomware: wat is het eigenlijk en welke soorten zijn er?

Kort gezegd is ransomware een chantagemethode op internet waarbij gebruik wordt gemaakt van malware; schadelijke en ongewenste software. Letterlijk vertaald betekent ransom: losgeld. Ransomware is een programma dat een computer (of gegevens die erop staan) blokkeert en vervolgens van de gebruiker geld vraagt om de computer weer te 'bevrijden'. Er zijn verschillende types ransomware. We onderscheiden hier de twee meest voorkomende: Locker- en Crypto ransomware.

1. Locker ransomware: wordt ook wel computer locker genoemd. Het Locker virus 'lockt' een computer of device. Het geeft zich uit als een officiële justitiële instantie en geeft aan dat de computer geblokkeerd is omdat het onderdeel is van justitieel onderzoek. Bijvoorbeeld vanwege copyright overtredingen of zelfs illegale pornografische praktijken. Een 'boete' moet betaald worden om weer toegang tot de eigen computer of device te krijgen.

2. Crypto ransomware (data locker): is erop gericht mensen de toegang tot data te ontzeggen, vaak door gebruik van data-encryptie.

   a. CryptoLocker was de eerste grote crypto ransomware. De locker maakt gebruik van een bijna onbreekbare data-encryptie om mappen, bestanden en dataopslag te blokkeren voor de gebruiker. Hij is zo goed dat zelfs in gevallen waar de malware is verwijderd, bestanden en folders gelockt zijn gebleven. Het ergste is dat een gebruiker het virus vaak zelf heeft binnengehaald door bestanden te openen uit zorgvuldig opgezette en betrouwbaar ogende e-mails van wat bijvoorbeeld een logistiek bedrijf lijkt.

   b. CrypJoker is een relatief nieuwe vorm van ransomware, ontdekt in januari 2016. Het gebruikt een ingewikkeld algoritme (AES-256) om bestanden van een gebruiker te encrypten en vraagt vervolgens om losgeld voor de vrijlating ervan.

Naast het gijzelen van data zijn er ook andere toepassingen van ransomware bekend, zoals het wissen van datakopieën. Op die manier is het niet mogelijk om vanuit een back-up data te herstellen. Uiteindelijk hebben slachtoffers dan vaak maar twee opties: herstellen uit een beschikbare back-up of het geld betalen om de toegang terug te krijgen. En zelfs dan is er vaak geen garantie dat de gijzelnemers de juiste code verschaffen om de data weer beschikbaar te maken.

Cybercrime is meer dan een IT-uitdaging

Cybercrime cijfers zijn dus enorm gestegen en naar verwachting zullen ze ook blijven stijgen. Er zijn inmiddels zelfs websites waar 'whitelabel' ransomware wordt verkocht aan criminelen. Gelukkig begint dit besef ook steeds meer door te dringen bij de besluitvormers in het bedrijfsleven en wordt ransomware niet alleen meer als een IT-probleem, maar juist als een serieus bedrijfsrisico aangemerkt. Toch heeft nog geen 1 op de 3 bedrijven een 'cyber incident response plan'.

De cybercrime nul-test

Om voorbereid te zijn op eventuele ransomware aanvallen, is een goede basisgezondheid van je data-omgeving de eerste stap. Stel jezelf om te beginnen de volgende vragen:

1. Waar staat je data? En is het veilig? Analyseer je data-ecosysteem. Weet waar alle data is opgeslagen en welke servers of systemen de data ondersteunen. Breng ook in kaart waar de 'points of entry' zijn, en zorg dat je ze sluit.
2. Wanneer was je laatste back-up, en heb je het getest? Ok, je hebt recentelijk een back-up gemaakt. En er kwamen geen errors naar boven. Maar wanneer heb je voor het laatst echt bestanden teruggehaald uit de back-up? Testen is een belangrijk onderdeel van het beveiligen van je data.
3. Zijn je 'end-points' veilig en gesegmenteerd? Hoe zorg je er, met een groei aan 'bring your own device' en werken op afstand, voor dat on site- en remote data en back-ups veilig staan?
4. Hoe goed is je netwerk beveiligd? Je netwerk is de levensader van je data in- en outflow. De juiste segmentatie is daarom essentieel voor de veiligheid om risico's te managen.
5. Heb je controle over datatoegang? Een 'access control list' (ACL) is een goede manier om de toekenning van toegangsrechten bij te houden. Houd back-up data bijvoorbeeld zuiver door slechts een aantal mensen toegang te geven.

Vergeet vooral niet de dialoog te starten in je organisatie over cybercrime en ransomware. Criminelen gebruiken vaak technisch en sociaal handige technieken om te zorgen dat mensen hun malware installeren. Uiteindelijk is ransomware vaak een 'eigen doelpunt' omdat een van de medewerkers, of iemand anders met toegang, (onbewust) een virus binnenlaat.

Voorkomen is beter dan genezen: wat kun je doen?

De eerste relatief makkelijke actie om te ondernemen is het gebruik van goede anti-malware software. Hiermee kun je je data tegen bekende ransomware technieken beschermen. Maak ook gebruik van de pop-upblocker functies in webbrowser(s). Maar zorg er daarnaast vooral voor dat medewerkers zich bewust zijn van de risico's en de waarschuwingen die ze tegenkomen. Bijvoorbeeld met betrekking tot phishing e-mails zijn er een paar simpele regels die je een hoop schade kunnen besparen:

- Open geen e-mailbijlagen van afzenders die onbekend of onverwacht zijn.
- Klik niet op links in e-mails van onbekende afzenders. Klik pas op de links in e-mails van bekenden als je er met je cursor overheen hebt bewogen en je ziet dat het doeladres iets is wat niet verdacht is. Google bij twijfel het adres.
- Zorg dat je bestanden regelmatig worden geback-upt. Hoewel dit geen ransomware aanval tegengaat, zal het de schade aanzienlijk beperken in het geval van een aanval.
- Licht je organisatie goed voor over deze risico's! Dit lijkt voor de hand liggend, maar communicatie hierover is essentieel.

Een simpele regel om ransomware tegen te gaan

Je wil er toch eigenlijk niet aan denken dat je 's ochtends vroeg op kantoor komt en dat de belangrijkste bestanden die je gebruikt voor je werk gelockt en encrypted (versleuteld) zijn door een ransomware aanval. Wat zou er dan gebeuren: zou het totale paniek opleveren of maak je een kop koffie en los je het op?

Om voor de tweede, toch wat meer ontspannen, optie te kunnen gaan, moet je goed voorbereid zijn. Dat kan onder andere door de 3-2-1 back-up regel toe te passen.

DRaaS – Disaster Recovery as a Service

Voorkomen is beter dan genezen. De bewustwording en training van personeel met betrekking tot cybercrime is daarom van essentieel belang. Maar zorg er daarnaast dus voor dat áls er iets gebeurt, je daar goed op voorbereid bent. Een efficiënte en betaalbare manier om snel een back-up te maken van essentiële bedrijfsdata en cruciale systemen te herstellen is DRaaS: de 'as a Service' variant van Disaster Recovery. Dit is een cloud-based service die je organisatie een uitwijkmogelijkheid geeft in geval van calamiteiten. Cruciale systemen zijn vaak al binnen 15 minuten weer beschikbaar.

De 3-2-1 back-up regel

- Zorg voor tenminste 3 kopieën van de belangrijkste corporate data
- Deze kopieën moeten op ten minste 2 verschillende media opgeslagen zijn
- Tenminste 1 van deze media moet off-site blijven

Wanneer je werkt aan databeveiliging en back-up oplossingen, dan zal de 3-2-1 back-up regel je helpen opgewassen te zijn tegen welke vorm van een ransomware attack dan ook. Maak dus een goed back-up plan. Dit zal ervoor zorgen dat je altijd de regie kan houden en gebruikers-, user- en andere data altijd kan herstellen. Zo wordt 'Disaster Recovery' geen paniekvoetbal, maar een zorgvuldig geplande opvolging van herstel-acties.

Nieuwsgierig?

Neem gerust eens contact op. We praten graag met je verder over mogelijkheden van DRaaS die bij jouw organisatie passen. Uniserver levert sinds 2000 cloudhostingdiensten en gelooft dat samenwerking leidt tot de beste resultaten. De missie van Uniserver is: IT simpel maken. Met een partnernetwerk van meer dan 100 IT-partners en jarenlange ervaring en kennis over de cloud, profiteer je van (cloud en business) oplossingen op basis van efficiency, kwaliteit en innovatie. Wij denken graag met je mee over een passende oplossing.

uniserver

Uniserver Internet B.V.
Robijnstraat 3
1812 RB Alkmaar

+31(0) 72 572 56 46
sales@uniserver.nl
www.uniserver.nl