Ransomware:
het draait om het vertrouwen van de klant

Er is niet veel nodig om uw bedrijf lam te laten leggen door ransomware. Een ‘onschuldige’ klik op een verdachte advertentie of een link in een e-mail. Zelfs een bezoek aan een legitieme website kan u problemen bezorgen als de site besmet is met software die gebruikers doorsluist naar een kwaadaardige website. Als dat gebeurt, worden al uw bedrijfsbestanden versleuteld en komt er een eis voor losgeld. Nadat u hebt betaald, krijgt u uw bestanden terug, of niet, zoals een aantal bedrijven ontdekte tijdens een recente ransomwareaanval.

Wereldwijd wordt elke 40 seconden een bedrijf getroffen en een op de vijf MKB-bedrijven krijgt hun gegevens niet terug, ook niet nadat ze het losgeld hebben betaald.[1]

Ransomware is kwaadaardige software die dreigt de gegevens van het slachtoffer te publiceren of die voorgoed de toegang tot de gegevens blokkeert, tenzij er losgeld wordt betaald. Soms is ransomware nog kwaadaardiger: uw gegevens worden vernietigd, ook als u betaalt.[2]

40%
van bedrijven wereldwijd werd in 2015 getroffen door een ransomware-incident.[3]

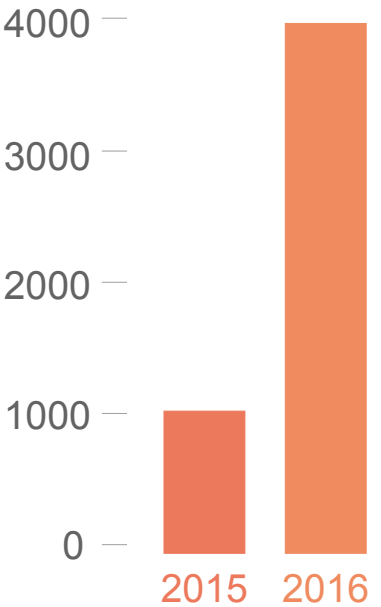
60%
van ransomwareaanvallen wereldwijd eiste minimaal $ 1.000.[3]

$ 1 miljard
is het geschatte bedrag dat cyberdieven in 2016 binnenhaalden.[4]

Als u denkt dat uw bedrijf veilig is omdat het te klein is om de aandacht van een cyberdief te trekken, dan hebt u het mis.

Volgens schattingen van de FBI (het Amerikaanse Federal Bureau of Investigation) zijn dagelijkse ransomwareaan-vallen sinds 2015 met gemiddeld 300% toegenomen.[5]

Aantal ransomwareaanvallen per dag



Resultaten van de WannaCry-ransomwareaanval in mei 2017:[6]

150
landen getroffen

300.000
apparaten geïnfecteerd

200.000
bedrijven getroffen

Het punt is dat ransomware geen respect heeft voor u of voor uw bedrijf. Geen enkel bedrijf is immuun, maar kleine en middelgrote bedrijven (MKB-bedrijven) zijn kwetsbaarder vanwege hun budgetbeperkingen en lagere uitgaven aan IT-infrastructuren en -beveiliging.

Wat kunnen MKB-bedrijven doen om hun beveiliging tegen ransomwareaanvallen te verbeteren?

Sommige experts raden bedrijven aan om zich te verzekeren tegen cyberaanvallen.[7] Dat kan duur zijn en voorkomt de aanval niet. Daarnaast kan een verzekering helpen met de kosten van het losgeld en andere IT-uitgaven die het gevolg zijn van de schade, maar er is geen garantie dat u uw gegevens kunt herstellen.

Als het gaat om ransomware, is preventie de beste remedie.

Dit zijn een aantal stappen die uw bedrijf kan zetten om blootstelling aan aanvallen te verminderen:

1. Train werknemers op wat wel en niet te doen bij een ransomwareaanval. Een eenvoudige aandachtspunt is om nooit te klikken op ongevraagde links of e-mailbijlagen.
2. Zorg voor een beveiligingsprotocol dat uw werknemers kan beschermen als zij onderweg zijn en mobiele apparaten, zoals laptops, gebruiken.
3. Installeer een virtueel beveiligingssysteem dat problemen detecteert en inperkt. Dit systeem kan uw netwerken voortdurend in de gaten houden, malware-exploitkits identificeren en voorkomen dat de malwarecode wordt uitgevoerd. Het zal ook kwaadaardig command-and-control verkeer en kwaadaardige bestanden en URL's in e-mails blokkeren.
4. Verminder het risico op infectie door een proactief beveiligingsplan te ontwikkelen dat draait om een meerlaagse verdediging, met voorspellende intelligentie om te begrijpen waar aanvallen op het internet optreden en daarnaast ook voortdurend uw netwerkhygiëne verbetert en uw beveiligingspostuur evalueert.
5. Zorg dat u een actueel plan hebt voor de bedrijfscontinuïteit. Maak regelmatig back-ups van al uw cruciale gegevens. Test de integriteit van de back-ups en zorg ervoor dat het herstelproces altijd werkt. Back-ups mogen niet verbonden zijn met uw systeemnetwerken en moeten worden opgeslagen in de cloud of offline in een fysieke opslag.
6. Voer een jaarlijkse kwetsbaarheidsbeoordeling uit waarin ook gesimuleerde cyberaanvallen zijn opgenomen.
7. Zorg dat er consistente en uitgebreide processen zijn voor patchbeheer.
8. Kleinere bedrijven die zich geen intern IT-team kunnen veroorloven, kunnen externe beveiligingsexpertise inhuren en controle van IT-systemen delegeren aan providers van beheerde services (MSP's).

Voor veel MKB-bedrijven heeft beveiliging de hoogste prioriteit als het gaat om het inkopen van een technologische infrastructuur voor het bedrijf.

– IDC-onderzoek in opdracht van Cisco[8]

MKB-bedrijven zijn zich beter bewust van de noodzaak zich te beschermen tegen ransomware- en andere cyberaanvallen. De MKB-bedrijven die deelnamen aan de IDC-studie zeiden ook dat zij vertrouwen op oplossingen van bekende merken die zij betrouwbaarder vinden en die genoeg ingebouwde beveiliging bieden.

Uw bedrijf mag niet in het ongewisse blijven.

Bij Cisco weten we dat klantgegevens de essentie zijn van uw bedrijf. Over het beveiligen van deze informatie valt niet te onderhandelen. Uiteindelijk is het behoud van het vertrouwen van de klant de beste reden voor een MKB-bedrijf om te investeren in een sterke reeks oplossingen voor cyberbeveiliging.
Leer hoe Cisco voor het MKB u daarbij kan helpen.

1. ‘The Cost of Cryptomalware: SMBs at Gunpoint’, Kaspersky Lab, 7 sep 2016.

2. Robert Hackett, ‘Why You Shouldn’t Pay the Petya Ransomware’, Fortune, 28 jun 2017.

3. ‘40 Percent of Enterprises Hit by Ransomware in the Last Year’, Security Magazine, 4 aug 2016.

4. David Fitzpatrick en Drew Griffin, ‘Cyber-extortion losses skyrocket, says FBI’, CNN Money, 15 apr 2016.

5. ‘How to Protect Your Networks from Ransomware’, Federal Bureau of Investigation.

6. ‘Stop Ransomware in Its Tracks’, Cisco Umbrella.

7. ‘Extreme cyber attack could cause $120bn in damage’, Lloyd’s, 16 jul 2017.
(Gedetailleerde bevindingen van deze studie worden binnenkort gepubliceerd.)