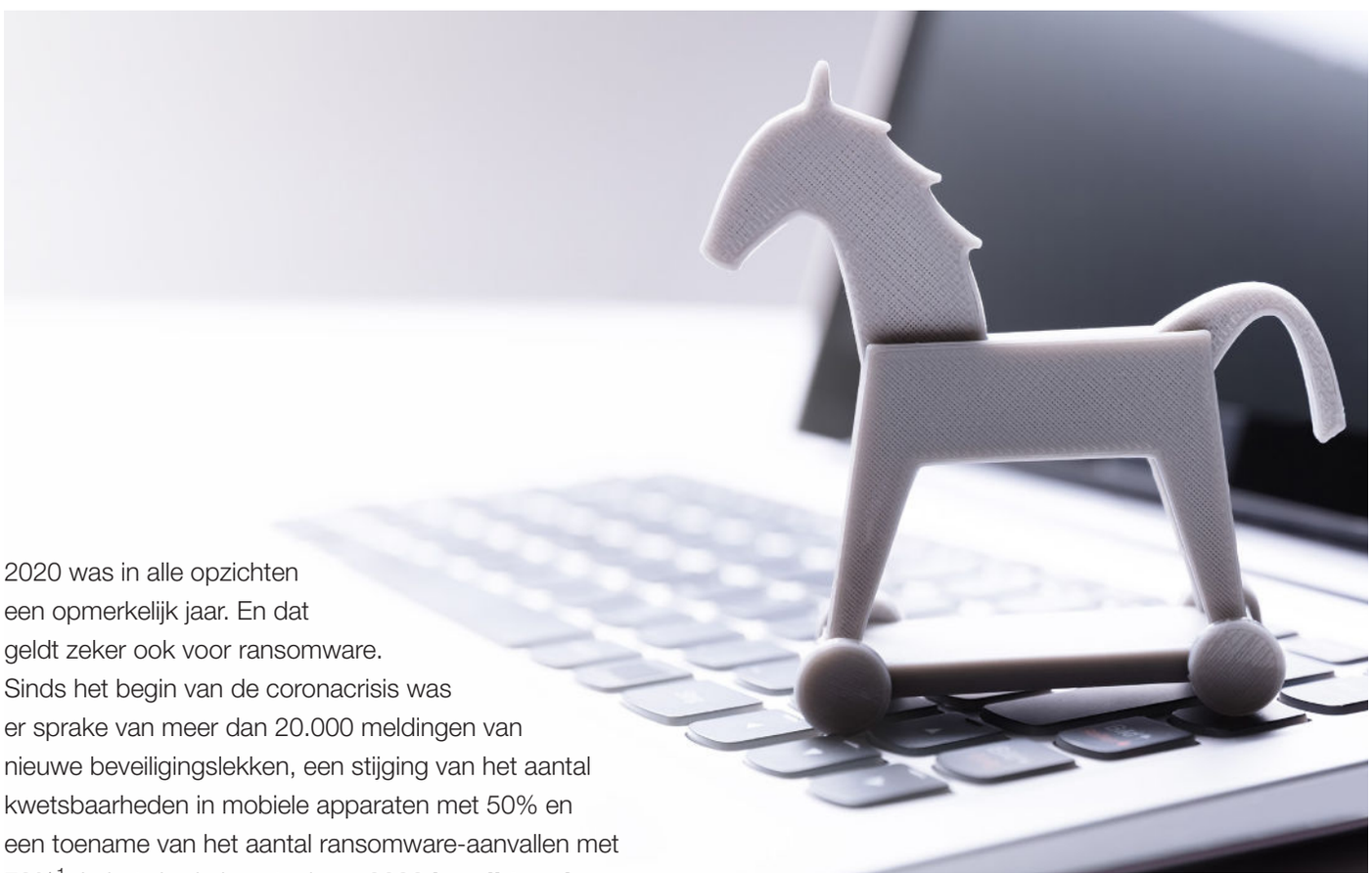
FAST LTA

Feitencheck

Welke kosten zijn er met een ransomware-aanval gemoeid?



2020 was in alle opzichten een opmerkelijk jaar. En dat geldt zeker ook voor ransomware. Sinds het begin van de coronacrisis was er sprake van meer dan 20.000 meldingen van nieuwe beveiligingslekken, een stijging van het aantal kwetsbaarheden in mobiele apparaten met 50% en een toename van het aantal ransomware-aanvallen met 72%[1]. In het derde kwartaal van 2020 **bereikten de losgeldeisen van cybercriminelen een hoogtepunt** met een gemiddeld bedrag van 230.000 dollar. In het vierde kwartaal zetten die weer een lichte daling in[2].

Voor veel succesvolle ransomware-aanvallen op bedrijven is het niet publiekelijk bekend hoeveel losgeld de slachtoffers betaalden. **Het is echter duidelijk dat de totale kosten als gevolg van een ransomware-aanval vele malen hoger uitvallen dan het losgeldbedrag.** Ook als het incident in kwestie niet in een kostenpost van 50 miljoen dollar resulteert, zoals aan de bedrijfsbalans van Universal Health Services, Inc (UHS) af te lezen valt[3].

We hebben de vijf grootste financiële risico's in kaart gebracht die een ransomware-aanval met zich mee kan brengen voor bedrijven, overheidsorganisaties en zorginstellingen.

Publicatiedatum: april 2021

#1

Downtime van de IT-omgeving

Het leeuwendeel van alle communicatie, verwerking, opslag en facturering verloopt tegenwoordig via digitale weg. Daarom resulteert elke dag zonder een functionerende IT-omgeving direct in financiële verliezen. **En hoe langer een bedrijf "offline" is, des te voelbaarder het omzetverlies en de annuleringen.**

En dan bestaat er nog het gevaar van een langdurige nasleep, bijvoorbeeld wanneer onderhoudsovereenkomsten niet kunnen worden nageleefd. Uit diverse onderzoeken blijkt dat de kosten als gevolg van downtime **tot 50 keer hoger uitvallen dan het gevraagde losgeld**[4].

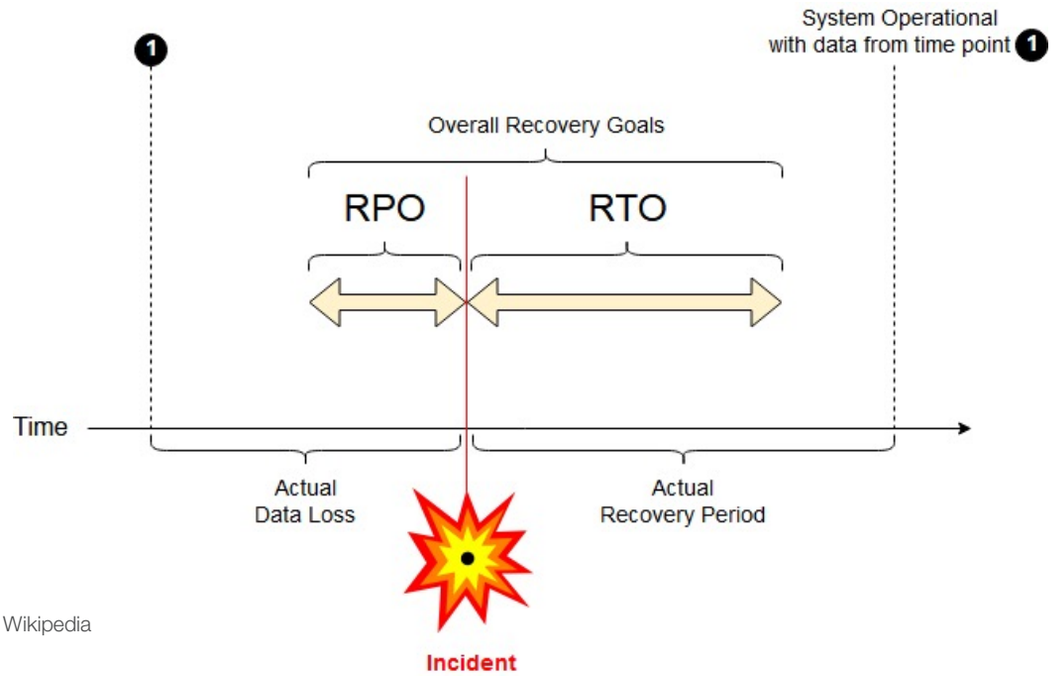
Gemiddeld duurt het drie weken voordat een door ransomware getroffen organisatie weer operationeel is[5]. Er zijn echter ook voorbeelden te vinden waarbij het opschonen en herstellen van de IT-infrastructuur aanmerkelijk langer in beslag nam. Incidenten zoals die bij aluminiumgigant Norsk Hydro, die 2019 **meer dan drie maanden** offline was[6], komen echter maar weinig voor. Bij dit Noorse concern werden in uiterst korte tijd 22.000 computers op 170 locaties in 40 landen met ransomware besmet. **Alle 32.000 werknemers waren maandenlang aangewezen op pen en papier**. Dit bezorgde de onderneming uiteindelijk een kostenpost van ruim 70 miljoen dollar[7].

Wat te doen?

Het is van essentieel belang om de tijd tot de hernieuwde beschikbaarheid van alle diensten en systemen te verkorten. Dit wordt uiteraard moeilijker naarmate er meer systemen met ransomware zijn besmet. Er is echter een aspect dat cruciaal is om een succesvolle aanval te overleven: **veilige, goed geconfigureerde back-ups**.

Hoewel back-ups behoren tot de maatregelen voor gegevensbescherming die elk bedrijf en elke overheidsinstelling nemen, is de manier waarop het back-upproces wordt vormgegeven wat het grote verschil maakt. Moderne ransomware valt tegenwoordig gericht back-ups aan. Als er dus alleen netwerk- en online-back-ups beschikbaar zijn, kan de vermeende bescherming al snel in rook opgaan.

Back-ups die op geen enkele manier door ransomware kunnen worden gemanipuleerd zijn daarmee een basisvereiste. Dergelijke back-ups moeten lokaal beschikbaar zijn, want het eerste wat je immers in een noodgeval doet is alle internetverbindingen verbreken. Verder mogen de back-ups niet met het primaire netwerk zijn verbonden, omdat ze anders eveneens een doelwit voor de ransomware vormen. Daarnaast moeten ze in overeenstemming met de specifieke eisen en financiële mogelijkheden van de organisatie worden geconfigureerd. De twee cruciale parameters waarmee elke IT-beheerder bekend is, zijn de RTO en RPO[8]:



Afbeelding: Wikipedia

- **RTO - Recovery Time Objective** - de tijd die het herstel van alle data uit de back-ups maximaal in beslag mag nemen.

- **RPO - Recovery Point Objective** - de mate van gegevensverlies die acceptabel is als gegevens moeten worden hersteld op basis van back-ups verder in het verleden

Het mooiste zou natuurlijk zijn dat beide parameters een waarde van nul hebben. Dat is technisch gezien echter geen haalbare kaart. Al naar gelang het budget is het daarom zaak om te zorgen voor een **aanvaardbaar compromis** tussen regelmatige back-ups die snel terug gezet kunnen worden en de kosten van de back-upinfrastructuur.

Bij een succesvolle ransomware-aanval gaat er tijdens het herstellen van gegevens ook tijd op aan het opsporen van de malware, het opschonen van alle componenten en het opnieuw installeren of vervangen van servers en pc's. Pas dan kan er een beroep worden gedaan op de back-ups. **Hierbij is echter bijzondere voorzichtigheid geboden**: ransomware kan zich weken- of maandenlang binnen de IT-omgeving verspreiden alvorens van start te gaan met het versleutelen van gegevens. Het is daarom belangrijk om erop toe te zien dat de gegevens die uit de back-ups worden hersteld geen malware bevatten.

Een specifiek op de onderneming, overheidsorganisatie of zorginstelling gerichte back-upstrategie die voorziet in **meerdere back-up stappen (trefwoord: de 3-2-1-regel), offline kopieën (ook wel air gapping genoemd) en lokale back-uparchieven** is daarom onontbeerlijk.

Onze tip

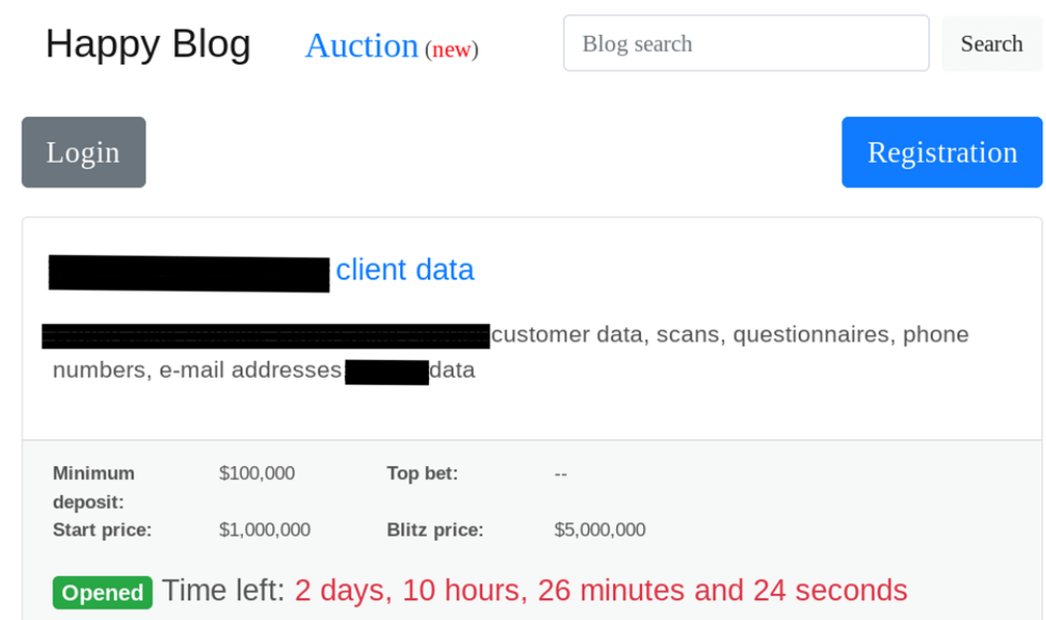
Zoals altijd geldt dat een back-up slechts zo goed is als de herstelprocedure. Een recent onderzoek door back-upspecialist Veeam wees erop dat **ruim de helft van alle herstelpogingen mislukt**[9]. Hoe u een uitgebreide en complete back-upstrategie kunt vormgeven met de software van Veeam en de flexibele Silent Bricks voor secundaire opslag leest u in onze Veeam Mini Guides[10].

#2

Dubbele afpersing

De ervaring van de afgelopen jaren leert daarnaast dat cyberaanvallen een steeds gerichter karakter krijgen. Cybercriminelen richten hun vizier speciaal op grote bedrijven, overheidsinstellingen en zorginstellingen. En als reactie op de **vanuit hun optiek slechte betaalmoraal** van slachtoffers passen ze een tweede afpersingstechniek toe. Alvorens tot encryptie over te gaan verzamelen moderne ransomware-varianten als DoppelPaymer, Ryuk en Egregor enorme hoeveelheden data uit de getroffen systemen. Cybercriminelen **dreigen vervolgens om deze bedrijfskritische informatie of persoonsgegevens openbaar te maken**. Dit gaat vaak gepaard met bijzonder hoge losgeldeisen (die soms in de miljoenen kunnen lopen) en extra tijdsdruk. **Als de afpersers niet direct betaald krijgen, maken ze geleidelijk aan meer gegevens openbaar en verdubbelen ze de losgeldeis.**

Hiervan zijn tal van voorbeelden te vinden uit de afgelopen maanden. De kans is echter groot dat slechts een fractie van alle succesvolle ransomware-aanvallen openbaar is gemaakt. Prominente slachtoffers waren onder meer de Japanse gameproducent CAPCOM[11], het Portugese energiebedrijf EDP[12], en de Duitse softwaregigant software AG[13]. Dit laatste concern moest uiteindelijk toegeven dat er "**gegevens van servers en notebooks**" van zijn medewerkers waren gedownload. De hackers achter de hierbij betrokken CLOP-ransomware vroegen **20 miljoen dollar** aan losgeld, dat vermoedelijk niet werd betaald.



Bron: Crowdstrike

Afbeelding: Microsoft

Wat te doen?

Wat de preventie van de versleuteling en het naar buiten smokkelen van gevoelige data door ransomware betreft is de focus binnen het bedrijfsleven verschoven naar het **'zero trust'-model**. Security Insider beschrijft dit als volgt: "Het zero trust-model is een beveiligingsconcept dat is gebaseerd op het principe dat **geen enkel(e) apparaat, gebruiker of dienst binnen of buiten het netwerk wordt vertrouwd**. Dit vraagt om uitgebreide maatregelen voor de authenticatie van alle gebruikers en diensten, plus inspectie van het netwerkverkeer."[14]

In tijden van thuiswerken en externe toegang tot bedrijfsnetwerken via VPN-verbindingen zijn er strengere veiligheidsmaatregelen nodig. Daarom is het van cruciaal belang dat niet alle werknemers directe toegang hebben tot gevoelige informatie en persoonsgegevens (of idealiter niet via hun standaardacccount), dat **back-ups en archieven in versleutelde vorm** worden opgeslagen op gegevensdragers voor offline gebruik die zijn beveiligd op basis van het **Write Once, Read Many (WORM)**-principe. Deze maatregelen zijn vaak ook nodig voor het waarborgen van overeenstemming met de AVG, die opslag "volgens de laatste stand der techniek" voorschrijft.

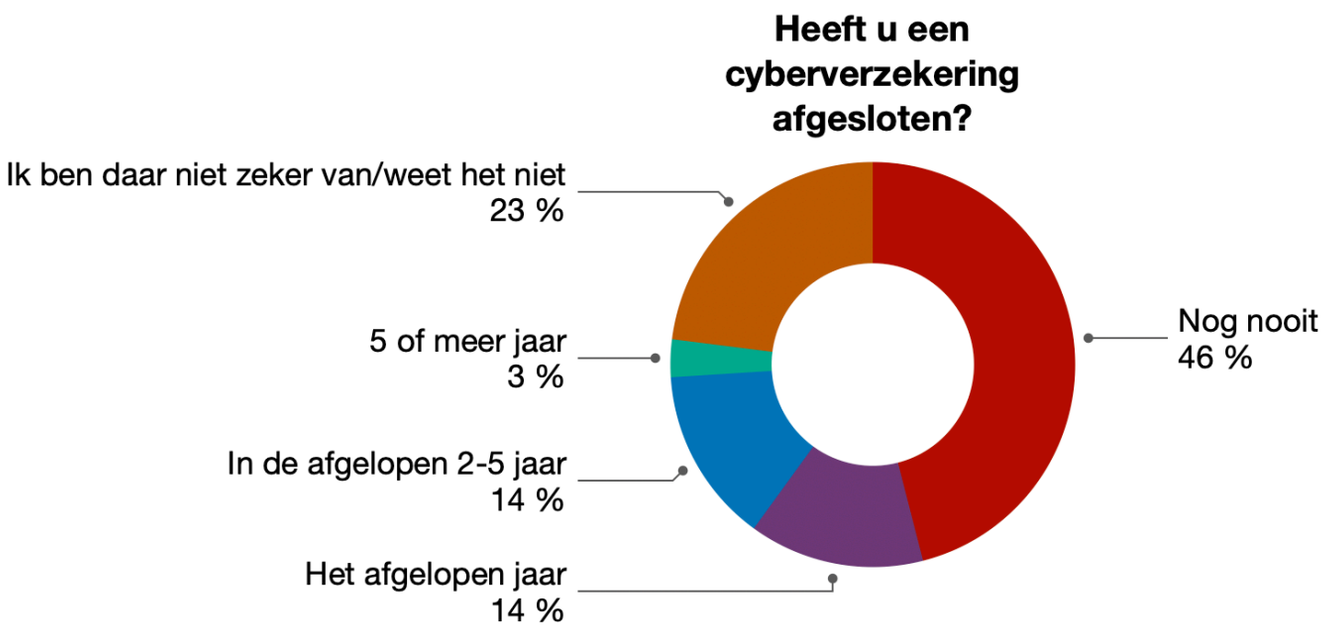
#3

Herstelkosten

Als een bedrijf eenmaal slachtoffer is geworden van een ransomware-aanval, betekent het herstellen van de normale gang van zaken niet alleen een tijdrovend proces: het gaat ook gepaard met **hoge kosten vanwege de noodzaak van investeringen in personeel en nieuwe IT-systemen**. Om nieuwe besmettingen te voorkomen moeten uiteraard eerst alle veiligheidslekken worden gedicht en alle getroffen systemen worden opgeschoond of opnieuw geïnstalleerd. Daarnaast moet de integriteit van de laatste bruikbare back-ups worden gecontroleerd. En last but not least moeten de gegevens uit deze back-ups in het gehele bedrijf worden hersteld. In theorie zou de organisatie na deze ingrepen weer operationeel moeten zijn.

Veel bedrijven, maar ook overheidsorganisaties en zorginstellingen, proberen echter de levensduur van hun bestaande IT-systemen zo lang mogelijk te rekken. Ze **investeren onvoldoende** in interne expertise en schuiven **softwareupdates en hardwareupgrades** op de lange baan. Dit wreekt zich echter des te meer in het geval van een succesvolle ransomware-aanval, omdat alle benodigde updates en upgrades dan gelijktijdig moeten worden uitgevoerd met het gegevensherstel, en bovendien onder enorme tijdsdruk. Vooral de vaak benodigde externe experts zijn kostbaar. Jake Williams, de oprichter van een cybersecurity-bedrijf, zegt daarover het volgende: “**Noodhulp en overuren vertegenwoordigen een veelvoud van de kosten** van het werk dat moet worden geleverd om het probleem te verhelpen. Met andere woorden: upgrades die op basis van het normale budget misschien 100.000 dollar hadden gekost, kunnen in noodgevallen 300.000 dollar of meer kosten.”

Dat zelfs een overstap naar de cloud geen bescherming biedt tegen hoge vervolgkosten, blijkt wel uit een incident bij de gemeente van Atlanta in de Amerikaanse staat Georgia. De betrekkelijk gematigde losgeldeis van 50.000 dollar stond in geen verhouding tot de uiteindelijke **totale kosten van ruim 2,6 miljoen dollar**[15]. De gemeente moest in totaal acht noodovereenkomsten sluiten voor het vinden en dichten van beveiligingslekken, investeringen in extra personeel en het aantrekken van Microsoft-gerelateerde **cloud-expertise**. Deze overeenkomsten hielden direct verband met het herstel van de gegevens die door de cybercriminelen waren versleuteld. Daarnaast ging er nog eens 650.000 dollar op aan crisiscommunicatie.



Bron: NinjaRMM

Het grootste probleem:

nalatigheid met updates

De praktijk wijst uit dat schrikwekkend veel bedrijven en overheidsinstellingen nalaten om **belangrijke updates** tijdig te installeren. Dat kan alleen maar worden uitgelegd als een gebrek aan deskundigheid. Een onzorgvuldige omgang met software- en firmware-updates vertegenwoordigt de belangrijkste zwakke schakel in de beveiliging van organisaties. Het loont daarom de moeite om het **spannende verhaal van Marcus Hutchins**, de jonge hacker die de **WannaCry**-aanval eigenhandig een halt toeriep, te lezen (of bekijken). Tal van bedrijven in alle delen van de wereld vielen ten prooi aan deze ransomware. WannaCry maakte misbruik van een **beveiligingslek in Windows** waarvoor Microsoft reeds een beveiligingsupdate had uitgebracht. Dit lek kon met behulp van de door de NSA ontwikkelde malware EternalBlue worden misbruikt[16] [17] [18].

Tegenmaatregelen

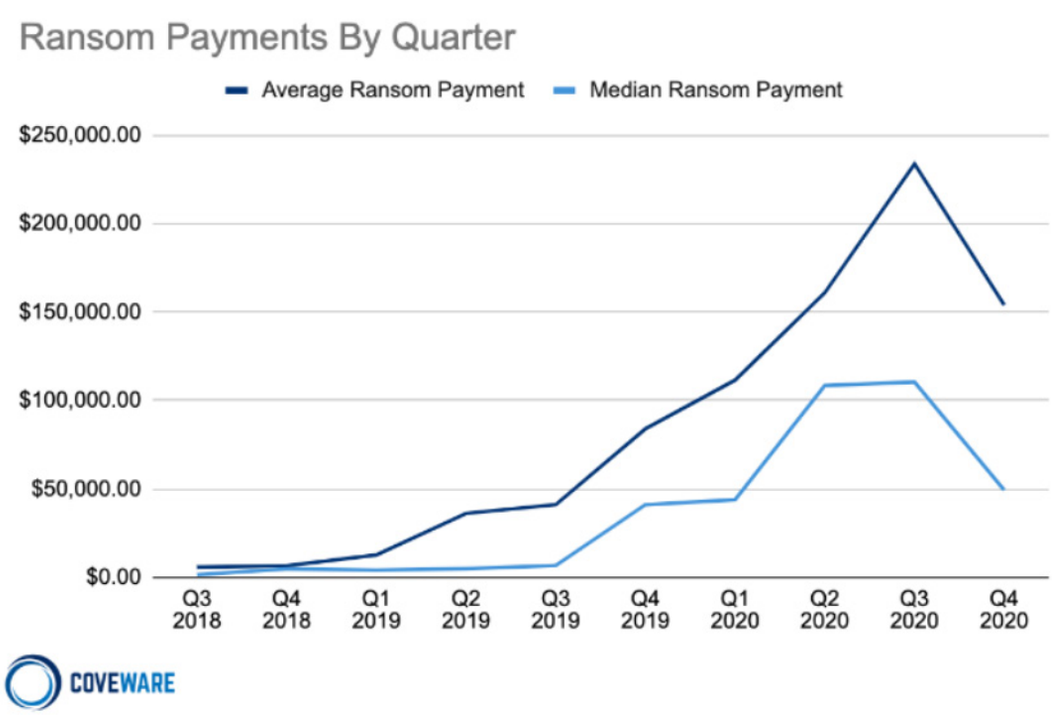
De belangrijkste maatregel voor het minimaliseren van de herstelkosten is daarom het installeren van **alle beveiligingsupdates** op pc's, servers en andere apparaten (switches, NAS, firewalls enzovoort). Dit vraagt om het opbouwen van interne expertise of op zijn minst het inschakelen van een betrouwbare IT-dienstverlener. Het valt daarnaast absoluut aan te raden om een **cyberverzekering af te sluiten** die in noodsituaties het leeuwendeel van de herstelkosten dekt. In 2020 had echter bijna de helft van alle IT-dienstverleners geen cyberverzekering[19].

#4

Losgeld

En ja – ook de losgeldeisen worden hoger. De gemiddelde losgeldeis steeg van 84.000 dollar in het vierde kwartaal van 2019 tot ruim 230.000 dollar in het derde kwartaal van 2020, hoewel dit bedrag in het vierde kwartaal van 2020 weer was gedaald tot iets boven de 150.000 dollar. Blijkbaar was de **pijngrens bereikt** waarop bedrijven zich nog net konden veroorloven om het losgeld op te hoesten[20].

Als men het gemiddelde voor deze periode beziet, blijkt dat er sprake is van een hoop **uitschieters naar boven**. Cybercriminelen voerden minder aanvallen uit op grote ondernemingen en overheidsinstellingen, maar de aanvallen die ze wél uitvoerden kregen een steeds gerichter karakter. Dit in combinatie met de techniek van dubbele afpersing zorgde ervoor dat er in veel gevallen sprake was van hoge losgeldeisen. Die liepen soms **tot in de miljoenen**.



Bron: Coveware

Er zijn op het internet talloze lijsten te vinden met "**de hoogste losgeldeisen van 2020**". Van de vele incidenten valt de aanval op Garmin, de leverancier van GPS-navigatie en draagbare outdoor-technologie, misschien nog wel het meeste op. Zeker omdat die vanwege de bekendheid van het merk iets meer voor het publieke oog plaatsvond. De experts zijn het erover eens dat Garmin naar alle waarschijnlijkheid de **geëiste 10 miljoen dollar heeft betaald**, of in ieder geval een groot deel daarvan. Er bestaat namelijk geen universele decryptiesleutel voor de ransomware WastedLocker waardoor het werd getroffen. Dat Garmin na vier dagen downtime weer volledig operationeel was, kan maar één ding betekenen: er is een functionerende sleutel aangeschaft[21].

Recentelijk baarde een nieuw recordbedrag opzien: de computerfabrikant ACER kreeg een claim van 50 miljoen aan zijn broek nadat er sprake bleek van misbruik van een beveiligingslek in een **Exchange-mailserver**[22]. De cybercriminelen stelden zich daarbij flexibel op: ze boden 20 procent korting op het losgeld als dat binnen drie dagen werd betaald. Ze dreigden echter om het bedrag te **verdubbelen tot 100 miljoen dollar** als de betaling meer dan twee weken op zich liet wachten. Of er wel of niet is betaald, is helaas niet duidelijk.

Tegenmaatregelen

Veel bedrijven en overheidsinstellingen verkeren in de veronderstelling dat ze de downtime van hun IT-omgeving aanmerkelijk kunnen verkorten door het betalen van losgeld. Sophos stelt in het rapport "The State of Ransomware 2020" dat 26% van alle ondervraagde bedrijven overging tot het betalen van losgeld[23]. Het geval wil alleen dat de totale kosten als gevolg van de ransomware-aanval stegen met bijna hetzelfde bedrag als het gevraagde losgeld. **Het betalen van losgeld heeft dus in de meeste gevallen geen invloed** op het leeuwendeel van de overige kosten die zich als gevolg van een aanval voordoen. Het dringende advies luidt dus om **geen losgeld te betalen** zolang er een of andere mogelijkheid bestaat om gegevens te herstellen, iets waartoe de helft van de respondenten in staat was met behulp van back-ups.

#5

Reputatieverlies

Iets wat nauwelijks in exacte cijfers valt uit te drukken, maar een niet minder pijnlijk gevolg is van een succesvolle ransomware-aanval, is **vergaande reputatieverlies**. Als gevolg van downtime worden er deals misgelopen en kunnen onderhoudsovereenkomsten niet worden nageleefd. Het blijkt bovendien dat twee derde van alle klanten spontaan naar de concurrentie overstapt. En uit een onderzoek door Arcserve[24] blijkt dat **60% van alle respondenten bedrijven mijdt die het niet zo nauw blijken te nemen met de beveiliging**. Hoewel veel beveiligingslekken zoals voorheen kunnen worden verzwegen, is het een stuk moeilijker om succesvolle aanvallen en datalekken voor de buitenwereld verborgen te houden.

Beursgenoteerde ondernemingen zijn overigens sowieso verplicht om factoren die van invloed zijn op het bedrijfsresultaat openbaar te maken, zoals in het geval van software AG. Dat geldt ook voor overtredingen van de AVG. En cybercriminelen dragen ook hun steentje bij door **succesvolle aanvallen openbaar te maken** om de druk op de getroffen organisatie op te voeren.

Bron: Arcserve

Tegenmaatregelen

Als bedrijven slecht of helemaal niet communiceren, neemt de internetgemeenschap het stokje over. En uiteraard voeren mensen die ooit slechte ervaringen met het bedrijf in kwestie opdeden daarbij de boventoon. De discussie gaat dan al snel niet meer over de aanval zelf, maar over de reputatie van het getroffen bedrijf. Dit blijkt onder meer uit de discussies op Reddit over het eerder genoemde incident bij ACER[25]. Het probleem hiermee is dat deze discussies bovenin de zoekresultaten voor bedrijven kunnen opduiken. Dit kan voor flinke reputatieschade zorgen.

Zorg in dit soort gevallen daarom altijd voor transparante en uitgebreide communicatie.

Conclusie

De grootste kostenpost bij ransomware-aanvallen wordt veroorzaakt door **downtime van de IT-omgeving**. De kosten als gevolg van omzetverlies, boetes van toezichthouders, het herstel van IT-systemen en het inhuren van externe specialisten vallen hoger uit dan de eveneens stijgende losgeldeisen, waar u in geen geval gehoor aan zou moeten geven.

De beste bescherming tegen hoge kosten is een samenhangende **back-upstrategie** die voortdurend wordt geëvalueerd en voorziet in restores die ook zonder verbinding met de buitenwereld tot volledig herstel leiden. Een **cyberverzekering** kan eveneens helpen om in noodsituaties torenhoge IT- en personeelskosten te voorkomen. Uiteindelijk komt het erop aan om **goed voorbereid** te zijn. Want de experts zijn het erover eens: het is niet langer de vraag of organisaties slachtoffer worden van een ransomware-aanval, maar **wanneer**.

Bild: Darknet Diaries

Aanrader: het verhaal achter NotPetya, de ergste hack aller tijden

Ook overheden kunnen dader zijn of slachtoffer worden van ransomware-aanvallen. Een voorbeeld daarvan is de vermoedelijk Russische aanval op de infrastructuur van de Oekraïne met de ransomware NotPetya. Hierbij kaapten de daders de updateserver van de besturingssoftware die binnen vrijwel het hele land werd gebruikt. De ransomware verspreidde zich vervolgens als een lopend vuurtje door de Oekraïne. Omdat de staatshackers niet uit waren op losgeld, maar maximale chaos wilden verzaken, was er geen gemakkelijke uitweg. Voor het spannende en aanbevelenswaardige achtergrondverhaal kunt u terecht op Youtube[26] of een speciale podcast beluisteren[27].

Bronvermeldingen

1 https://www.skyboxsecurity.com/trends-report/
2 https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
3 https://healthitsecurity.com/news/uhs-ransomware-attack-cost-67-million-in-recovery-lost-revenue
4 https://www.datto.com/blog/downtime-the-true-cost-of-a-ransomware-attack
5 https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020#costs
6 https://www.bbc.com/news/business-48661152
7 https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/
8 https://de.wikipedia.org/wiki/Disaster_Recovery
9 https://www.veeam.com/de/news/cxo-research-58-percent-of-data-backups-are-failing-creating-data-protection-challenges-and-limiting-digital-transformation-initiatives.html
10 https://fastlta.com/veeam-de
11 https://www.zdnet.com/article/capcom-confirms-ransomware-attack-potential-theft-of-customer-employee-data/
12 https://www.zdnet.com/article/edp-energy-confirms-cyberattack-ragnar-locker-ransomware-blamed/
13 https://secure-technology.de/news/interne-daten-der-software-ag-nach-ransomware-angriff-veroeffentlicht/
14 https://www.security-insider.de/was-ist-ein-zero-trust-modell-a-752389/
15 https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/
16 https://www.youtube.com/watch?v=yewkv8pTAu0
17 https://www.youtube.com/watch?v=vveLaA-z3-o
18 https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/
19 https://www.ninjarmm.com/de/blog/der-ransomware-report-2020/
20 https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
21 https://www.bleepingcomputer.com/news/security/confirmed-garmin-received-decryptor-for-wastedlocker-ransomware/
22 https://www.security-insider.de/ransomware-angriff-acer-soll-50-millionen-us-dollar-zahlen-a-1010194/
23 https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf
24 https://info.arcserve.com/en/thank-you-ransomwares-stunning-impact-on-consumer-loyalty-and-purchasing-behavior
25 https://www.reddit.com/r/worldnews/comments/ma8a54/computer_giant_acer_hit_by_50_million_ransomware/
26 https://www.youtube.com/watch?v=KODpP29AHD4
27 https://darknetdiaries.com/episode/54/

COMEX

FAST LTA

Publicatiedatum: april 2021

COMEX | Vogt 21 | NL-6422 RK Heerlen | office@comex.eu | **www.comex.eu**

FAST LTA | Ruedesheimer Str. 11 | 80686 Munich, Germany | info@fast-lta.de | **www.fast-lta.com**