HOE ZIET EEN RANSOMWARE-AANVAL ERUIT EN WAT KUN JE ERTEGEN DOEN?

tectrade

Ransomware vormt een steeds grotere bedreiging doordat hackers steeds sluwer opereren. Voorheen werd vaak maar één enkele laptop door gijzelsoftware aangetast. Alle aanwezige bestanden werden versleuteld en daarna stuurde de hacker het verzoek om (bijvoorbeeld) bitcoins over te maken. Inmiddels vormen cybercriminelen goed georganiseerde professionele groepen, die doelgericht complete bedrijfstakken aanvallen. De schade blijft niet meer beperkt tot honderden of duizenden euro's maar kan in de miljoenen lopen.

De digitale criminelen richten zich liefst op bedrijven met een financiële achtergrond – hier valt het meest te halen. Daarnaast kijken ze ook naar organisaties met een grote maatschappelijke impact -zodat deze organisaties sneller genoodzaakt zijn te betalen voor de sleutel om bestanden mee te decoderen. Ook bedrijven die hun security niet goed op orde hebben zijn een geliefd doelwit. Een organisatie waar deze drie elementen samenkomen, loopt uiteraard de meeste kans op een dergelijke aanval.

Udo Brok is senior solution architect bij Tectrade. Hij legt aan de hand van een recent praktijkvoorbeeld bij de Universiteit Maastricht uit, wat ransomware precies inhoudt en wat je ertegen kunt doen.

Hoe ransomware werkt

Malware

Brok: "Ransomware is een vorm van malware. Malware gebruiken hackers om computersystemen te verstoren, gevoelige informatie te verzamelen, of om toegang te krijgen tot private computersystemen. Ransomware is er specifiek op gericht om je computer te vergrendelen, om te voorkomen dat je er toegang tot hebt. Totdat het losgeld, meestal in de vorm van bitcoins, is betaald. Een ransomware-aanval begint bijvoorbeeld bij een poging om via phishing-mails, in het systeem van het bedrijf te komen."

De masterkey

Brok vervolgt: "Daarna zoeken hackers naar zwakke plekken, met als doel: het kraken van de directory service. De directory service is te vergelijken met een hotel dat verschillende kamers heeft. De beheerder is in het bezit van de masterkey. De hackers trachten deze masterkey in handen te krijgen. Als dit lukt, kunnen ze op alle servers en werkstations binnendringen."

De aanval

"Hierna nemen de hackers vaak even de tijd", vertelt Brok. "Ze proberen de impact zo groot mogelijk te maken én wachten daarom een vervelend moment af om toe te slaan. Bijvoorbeeld tijdens de feestdagen. Zo wordt de encryptie die dan plaatsvindt minder goed opgemerkt en vindt het herstel logischerwijs ook minder snel plaats. En hoe meer bestanden de hackers raken met de ransomware, hoe meer losgeld ze kunnen vragen."

Casus: ransomware-aanval bij Universiteit Maastricht

“Een medewerker van de Universiteit Maastricht ontving op 15 oktober 2019 een phishingmail. Hierin stond een link naar bestanden op OneDrive. De gebruiker klikte hierop, merkte dat er iets niet klopte en belde netjes de service-desk”, vertelt Brok. “Na onderzoek heeft de service-desk de link in het netwerk geblokkeerd, zodat deze geen kwaad meer zou kunnen mocht hij ook naar anderen worden verstuurd. Vervolgens werd de laptop van de gebruiker ook in beslag genomen.”

“Hierna kreeg een andere gebruiker een nieuwe, soortgelijke, link. De service-desk was in de veronderstelling dat deze al was geblokkeerd en ondernam geen actie meer. Op het moment dat de gebruiker op de link klikte, kregen de hackers toegang tot het systeem”, legt Brok uit. “Tijdens hun speurtocht naar een zwakke plek, zijn de hackers tegen een drietal verouderde servers aangelopen. Dat was op 21 november. De hackers zijn toen in de systemen op deze servers binnengedrongen, die toevallig ook gebruikt werden door de beheerders. Toen de beheerder op één van deze systemen inlogde, konden de criminelen de masterkey kraken. Zo hebben ze volledig toegang gekregen tot het domein.”

“De hackers begonnen op 19 december met het installeren van een stukje software dat later de ransomware over het hele netwerk kon distribueren. Deze activiteit werd gesignaleerd door een virusscanner die op de server waar de hackers opereerden actief was. Een melding kwam bij de service-desk terecht, die de software verwijderde. De service-desk heeft verder geen onderzoek gedaan naar hoe de software überhaupt op de server terecht kon komen. Dit gaf de hackers de gelegenheid om met de masterkey de virusscanner onschadelijk te maken. Hierna hebben ze alsnog de software geïnstalleerd.”

“De hackers voorzagen op 23 december alle 267 servers van ransomware. Alle gegevens die op deze servers stonden, werden tegelijkertijd versleuteld. Dit heeft in totaal 50 minuten geduurd. Hierna waren ook alle online back-ups versleuteld.”

“Omdat salarissen niet konden worden uitbetaald, en tentamens niet afgenomen konden worden, besloot Universiteit Maastricht de sleutel te kopen van de criminelen. Dit kostte de universiteit 30 bitcoins, gelijk aan 197.000 euro”, besluit Brok.

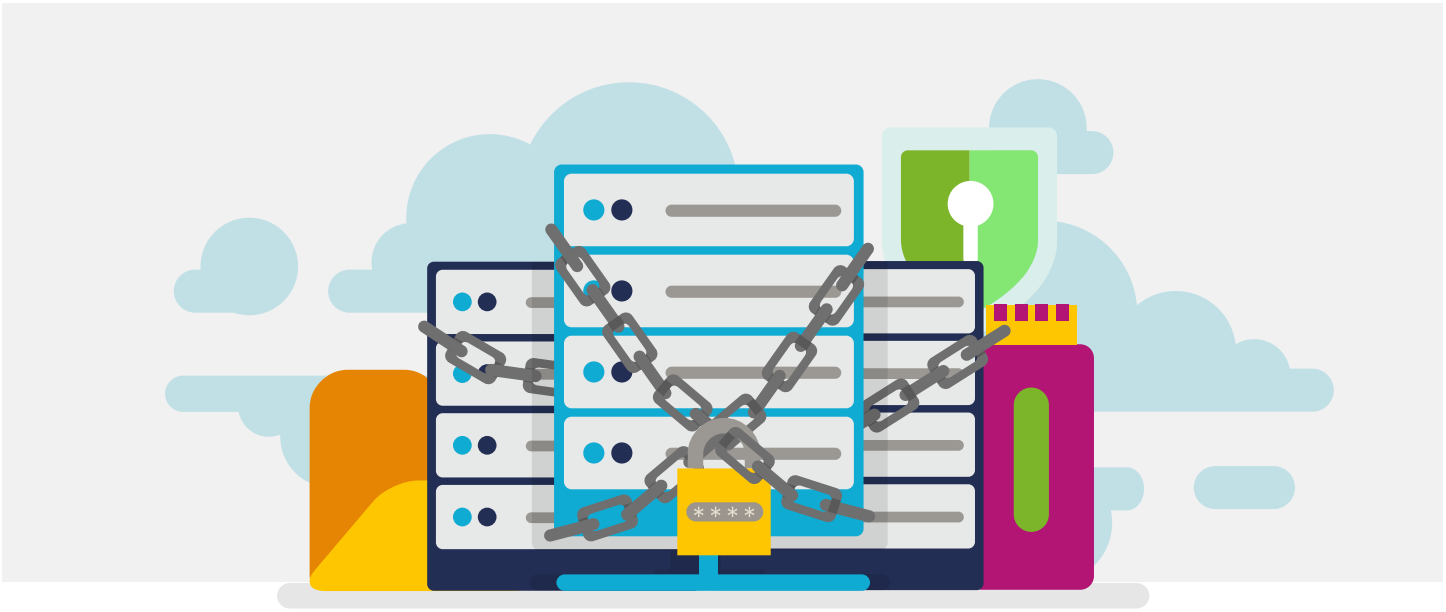
Ik word aangevallen! En nu?

Trek geen stekkers uit het stopcontact

De eerste neiging bij een aanval is vaak om alle stekkers uit het stopcontact te trekken. Een grote fout, omdat hiermee alle digitale sporen worden gewist. Brok: “Deze sporen zijn nodig om goed onderzoek te kunnen doen naar de details van de aanval. Bovendien gaat de aanval gewoon weer door wanneer de systemen worden opgestart.”

Sluit je netwerk af

“Hetzelfde geldt voor de encryptie. Wanneer het proces van encryptie loopt en je stopt het, kan het zelfs zo zijn dat het niet eens meer valt te decoderen. Wat je wel kunt doen, is je netwerk afsluiten van het internet zodat de hackers niet meer mee kunnen kijken en dus niet meer zien wat er gebeurt. Dan kunnen ze ook niet meer verder gaan,” vertelt Brok.



De gevolgen van een aanval

Datalek

Op het moment dat je met ransomware te maken hebt, is er ook sprake van een datalek. In dat geval ben je voor de wet verplicht om dit te melden. Als je deze melding doet, moet je ook aangeven wat de schade is, welke data in potentie op straat ligt. Dat is bijzonder moeilijk. Het kan zijn dat de data enkel versleuteld is en de hacker hier verder niets mee heeft gedaan.

Diepgaand onderzoek

Brok: “Er is diepgaand onderzoek nodig om vast te kunnen stellen wat de impact van de aanval op de data is. Meestal beschikt een organisatie niet over de kennis om dit zelf uit te voeren. Er is dan externe partij nodig die kan herkennen welke criminele organisatie achter de aanval zit. Een expert die op basis van de digitale sporen een rapport kan maken, met een overzicht van de data die is aangetast.”

Imagoschade

“Wanneer de gelekte data informatie bevat over personen, moeten deze mensen op de hoogte worden gebracht. Imagoschade is hierdoor een voor de hand liggend gevolg” vertelt Brok. “Een van de kernwaardes van Universiteit Maastricht is openheid. Toen zij werden aangevallen, heeft de universiteit hierin volledige openheid gegeven. Voor hen is de imagoschade dus juist niet groot. Maar je kunt je voorstellen, dat dit voor een financiële instelling een andere zaak is.”

Financiële schade

“Wat je niet wilt (ook moreel gezien) is betalen aan deze criminelen. Je wilt liever niet een dergelijke organisatie financieren. Maar omdat de impact groot kan zijn, is het vaak in het bedrijfsbelang om dit toch te doen, zoals in het geval van Universiteit Maastricht. Anders konden salarissen niet worden betaald en konden er geen tentamens worden afgenomen”, aldus Brok. “Naast de kosten die een organisatie betaalt voor de sleutel, heb je ook te maken met kosten voor het digitale recherchewerk en strikte maatregelen om dit in het vervolg te voorkomen.”

> “ **Door de ransomware-aanval binnen Universiteit Maastricht zijn 19.000 studenten en 4.200 personeelsleden geraakt.”**

Niet operationeel

“Het kan ook zijn dat je als organisatie door deze gebeurtenis een paar weken niet operationeel kunt zijn. De data die versleuteld is, kan ook een belangrijke database treffen waardoor bedrijfsapplicaties niet meer werken en je bijvoorbeeld geen orders meer kunt doorvoeren”, vertelt Brok.

De oplossing: krachtige security, bewustwording en back-up

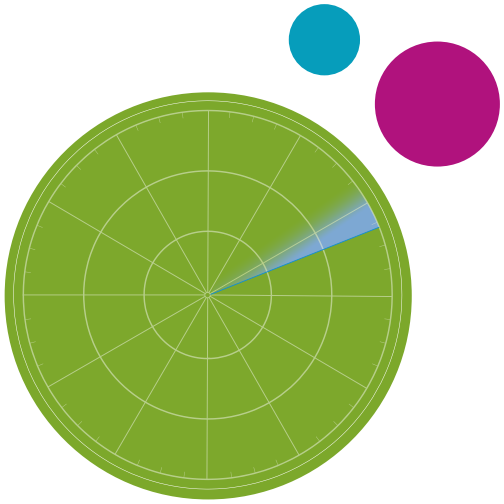
Het belangrijkste aspect om een aanval te voorkomen is krachtige security. Daarnaast is het belangrijk dat er interne bewustwording is van de gevaren. Zodat medewerkers bij iets verdachts dit melden aan de servicedesk.

Tot slot is het van belang om ook een ransomware bestendige backup klaar te hebben staan wanneer een dergelijke aanval plaatsvindt. Dit kan heel veel schelen in de kosten: niet alleen is er geen sleutel meer nodig om de data te decoderen, ook is je organisatie weer sneller up en running.

Hoe Tectrade helpt een aanval te voorkomen

Tectrade helpt klanten in een goede voorbereiding. Dit doen we door:

- ✓ Klanten bewust te maken van de gevaren.
- ✓ Advies te geven over eventuele zwakheden binnen de installed base.
- ✓ Nieuwe back-up oplossingen aan te bieden die tegen ransomware-aanvallen bestand zijn.



Met jarenlange netwerk- en beveiligingexpertise, helpt Tectrade u een datacenter te realiseren dat niet alleen klaar is voor de toekomst, maar ook volledig beschermd. Ook wel het Next Generation Datacenter.

Heeft u vragen over wat Tectrade voor u kan betekenen of wilt u meer informatie?

Mail naar info@tectrade.nl of bel +31(0)345 547040.
Of vul het contactformulier in.

tectrade