Door Anita Hestens

HOE WEERSTAAN ONDERNEMERS CYBERCRIMINELEN?

‘VOORBEREIDING IS ALLES’

Wat kun je als ondernemer wél en beter niet doen na een cyberincident? TLN werkt samen met IT-securityspecialisten Tesorion en Reqon om ondernemers hierin te ondersteunen.

Cyberdreigingen in de maatschappij nemen toe, ook in de logistieke sector. Veel ondernemers weten niet dat zij doelwit zijn van cybercriminelen en gaan er soms vanuit dat de digitale beveiliging goed geregeld is, terwijl dat in de praktijk niet altijd het geval is. Als een cyberincident zich voordoet, weten veel ondernemers niet wat zij moeten doen. Daarom zijn er webinars opgezet om extra bewustwording te creëren in de logistieke sector en de weerbaarheid te vergroten. Cybercriminelen spelen vaak in op actueel nieuws. Zo verwijzen zij in bijvoorbeeld een mail naar corona om de ontvanger van de mail te verleiden om door te klikken en vertrouwelijke gegevens prijs te geven. Bedrijven die (nog) niet worden getroffen door cybercriminaliteit, versloffen vaak in het toetsen in de praktijk van hun maatregelen.

VOORBEREIDING

Sommige criminelen zijn alleen uit op informatie door bijvoorbeeld de website of het hele organisatiesysteem te hacken. Anderen proberen alles wat geld oplevert te ontvreemden.

1

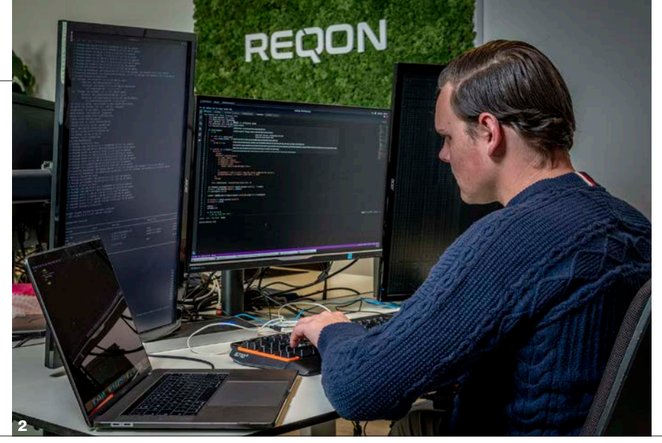
Cybercriminelen denken minder fysieke risico’s te lopen door een cyberaanval in te stellen met ransomware. Lodi Hensen is hoofd van het Computer Emergency Response Team (Cert) bij Tesorion, een soort digitale brandweer of arrestatieteam. Hij geeft het advies om voor de digitale beveiliging naar de fysieke wereld te kijken. “Wij trekken vaak de volgende parallel: als je je huis wilt beveiligen kun je kiezen voor een muur om je tuin, in de digitale wereld een firewall. Maar criminelen klimmen daar overheen, Zo biedt een muur dus meestal niet voldoende beveiliging. Je kunt een waakhond in de tuin zetten, in de digitale wereld geautomatiseerde detectie en gaan testen of de beveiliging voldoende is. Beveiliging is een continuproces. Vraag je af hoe de aanvaller te werk gaat. Voorbereiding is alles.”

ONGOING PROCESS

Belangrijk is om een tweestaps-identificatie te hebben bij het inloggen op systemen. “Een aanvaller gaat gegevens verzamelen – bijvoorbeeld verkregen via phishing – of malafide software installeren, na digitaal te zijn binnengedrongen. Het beste is om dan geautomatiseerde detectie – een digitale waakhond – te hebben of in ieder geval een melding in te stellen van het binnendringen van de indringer”, aldus Hensen die het ongoing process een ‘incident life circle’ noemt: voorbereiding, detectie & analyse en oplossen. Bij de oplossing van cyberincidenten kan Tesorion in actie komen, zoals toegelicht in de volgende casus.

GIJZELSOFTWARE

In deze casus had de situatie grote impact op de continuïteit van de bedrijfsprocessen. Hensen werd gebeld door een nieuwe klant, die vertelde dat



2

alle bestanden versleuteld waren en de systemen platlagen. “Er was in dit geval sprake van ransomware, ook wel gijzelsoftware genoemd. Er werd losgeld geëist om weer bij de systemen en bestanden te kunnen komen. Wij werden ingeschakeld om te analyseren wat er gebeurd was en de systemen van de klant weer online te brengen. De complete IT was uitbesteed en de leverancier had steken laten vallen. Zo bleek dat er geen afspraken waren gemaakt over incidenten. Geïnfecteerde systemen moeten bij een aanval worden geïsoleerd, zodat de infectie zich niet verder over het netwerk verspreidt. In dit geval was het echter al te laat en was het hele bedrijfsnetwerk in handen van de aanvaller. Er werden alleen onlineback-ups gemaakt, wat bij veel bedrijven gebruikelijk is, maar die waren door de aanvaller verwijderd. Tapes en offlineback-ups waren afgeschaft. Er was daardoor geen andere manier om het bedrijf up-and-running te krijgen dan door het losgeld te betalen.” Dit is overigens iets dat Tesorion te allen tijde afraadt, omdat op deze manier het ‘criminele businessmodel’ in stand blijft. Maar er is in sommige gevallen geen keus, en wordt er in goed overleg met diverse stakeholders een besluit genomen. “Wij hebben het proces van het ontsleutelen van data begeleid en parallel mitigatie- en detectiesystemen geïnstalleerd. Hiermee zijn wij een paar weken bezig geweest. Uiteraard is er ook aangifte bij de politie gedaan en is het onderzoeksrapport gedeeld voor het strafrechtelijke onderzoek.”

WACHTWOORDEN GERADEN

Wat valt uit deze casus te leren? Hensen: “Wees kritisch op de IT-leverancier waar je mee samenwerkt. Wij zien regelmatig dat bij de cyberaanval wachtwoorden worden geraden en dat daar geen stop of detectie op zit. Hierdoor kan de aanvaller uiteindelijk inloggen, binnen 24 uur het wachtwoord raden en het hele netwerk platleggen. Zorg daarnaast voor gedegen detectie op systemen en pas netwerk segmentatie toe. Regel verder offlineback-ups, naast onlineback-ups. Verder geldt altijd: wees up-to-date, kijk naar je zichtbaarheid online en wees voorbereid! En last but not least: kom je als ondernemer er niet uit? Raadpleeg dan experts.”

COLLECTIEF TESTEN

Harm Blankers, ethisch hacker en medeoprichter van Reqon, benadrukt het belang van goed testen van de IT-systemen. Volgens de privacywet AVG is het voor ondernemers verplicht om data adequaat te beveiligen. Tijdens een IT-beveiligingsonderzoek voert Reqon zogeheten pentesten uit, waarbij het onderzoekt in hoeverre een kwaadwillende een IT-omgeving kan binnendringen. De resultaten van deze testen geven inzicht in de aanwezige kwetsbaarheden en de bijbehorende beveiligingsrisico’s. Na afronding van het onderzoek stelt Reqon een advies op. Aan de hand van dit advies kunnen ondernemers maatregelen nemen om het beveiligingsniveau van de IT-omgeving te verhogen. Blankers benadrukt dat er tijdens het testen niets kapot wordt gemaakt. “Wanneer verschillende organisaties software van dezelfde leverancier afnemen, is het raadzaam om samen de benodigde IT-beveiligingsonderzoeken uit te laten voeren.”

1. Lodi Hensen: “Kijk voor de digitale beveiliging naar de fysieke wereld.”
2. Harm Blankers: “Het is belangrijk om IT-systemen goed te testen.”