Straffe klant

LINEAS

SPOORVRACHTBEDRIJF WAPENT ZICH TEGEN CYBERAANVALLEN

STRAFFE KLANT LINEAS

Computersystemen die niet meer werken, gecompromitteerde gegevens of vrachttreinen die niet kunnen uitrijden? De impact daarvan is enorm. Niet alleen op de bedrijven die hun vrachten niet krijgen geleverd, maar ook op het spoorwegnet en de economie. Reden genoeg voor Lineas, de grootste private spoorvrachtoperator in Europa, om op zoek te gaan naar een sterke samenwerking voor zijn cyberbeveiligingsbeleid.

"Toen ik een jaar geleden aan boord kwam bij Lineas was er nog geen formeel proces rond cyberbeveiliging. De integriteit van ons computernetwerk werd meteen mijn eerste prioriteit", zegt Chief Information Security Officer (CISO) Christophe Rome van Lineas. "Systemen die door een cyberaanval uitvallen, zijn een nachtmerrie. Als onze treinen niet meer rijden, heeft dat een directe impact op de bevoorradingsketen van onze klanten. Als een van de grootste private spoorvrachtbedrijven creëren we mogelijk een opstopping die gevolgen heeft voor het hele spoorwegnet."

GAT IN BELEID OPGEVULD

"Bij mogelijke aanvallen kwamen er wel alarmmeldingen binnen in iemand zijn mailbox of op een gsm-nummer, maar daar werd niets systematisch mee gedaan. De logs werden niet centraal bijgehouden, waardoor je geen overzicht had. Mijn eerste zorg was dan ook al die logbestanden centraliseren. Maar we hadden een tool nodig die verder gaat dan de traditionele security information & event management (SIEM)-oplossingen. Die tool moest niet alleen onze logbestanden analyseren en er besluiten uit trekken. Ik wilde alleen meldingen overhouden die echt nagekeken moeten worden omdat ze een reële bedreiging zijn."

"Lineas had ook geen formeel security operations center (SOC) om op incidenten te reageren. Ook dat zochten we extern omdat we niet over de juiste profielen beschikken en cyberbeveiligingsexperts moeilijk te vinden zijn. De combinatie van die technologie en die extra service om op incidenten te reageren, vonden we bij Telenet Business en NVISO. Hun Managed Detection & Response (MDR) vervolledigt ons beveiligingsbeleid", gaat Christophe Rome verder.

ZELFLERENDE SOFTWARE

"Ik had al contacten met NVISO. Zij staan voor mij momenteel met stip bovenaan als een van dé beveiligingspartners met de meeste kennis in België. Mensen uit mijn netwerk die de beveiligingsmarkt kennen, vertelden me dat Telenet Business aan het bekijken was hoe het een innovatieve managed service-oplossing op de markt kon zetten, gebruikmakend van Exabeam als onderliggend platform. Bovendien werd al snel duidelijk dat NVISO mee zou instaan voor de respons, het tweede luik van de oplossing. Voor mij was dat een puzzel die samenviel. Detectie zonder adequate respons heeft totaal geen zin."

Telenet Business koos bewust voor Exabeam. De detectietechnologie gebruikt machine learning om te leren uit cyberdreigingen en zichzelf slimmer te maken. "Met een traditionele, manuele aanpak loop je als bedrijf constant achter de feiten. Die is ook onhoudbaar omdat er nu eenmaal te weinig beveiligingsexperts rondlopen", zegt Cybersecurity Expert Willem Janssens van Telenet Business. "Concreet bekijkt de software wat computers en gebruikers doen. Daaruit maakt hij gedragspatronen van mensen en systemen. Hij leert wat normaal is, herkent zo risico's en geeft weer wanneer gedrag afwijkt", verduidelijkt Kris Bogaerts, Principal Security Consultant van Telenet Business.

VERTROUWEN IS DE SLEUTEL

"Onze relatie met Telenet Business en NVISO is een strategisch partnerschap dat ik verder wil uitbouwen. Want zeker in beveiliging draait alles om vertrouwen. Je hebt een partner nodig waar je altijd op kan rekenen. Het kan faliekant aflopen als je iemand belt die de voorgeschiedenis, je bedrijf en je netwerk niet kent", gaat Christophe Rome verder. Willem Janssens beaamt: "Bij een cyberaanval heb je snel hulp nodig. Krijg je die niet, dan verlies je kostbare tijd en wordt de impact alleen maar groter."

"Daarom garanderen wij incident response voor de MDR-klanten", vult Solution Lead Kris Boulez van NVISO aan. "Elke maand zitten we met Telenet Business en de klant samen. We bekijken dan wat de bedreigingen zijn, wat er eventueel kan gebeuren, in welke mate we ze al detecteren en hoe we nog kunnen verbeteren. Daardoor kennen we de omgeving van de klant en kunnen we proactief sturen en heel snel reageren."

LEERRIJKE TESTPERIODE

"We hebben onze Managed Detection & Response 3 maanden lang bij Lineas getest tijdens een proof of concept", geeft Willem Janssens nog mee. "Daaruit bleek dat de samenwerking ook voor ons heel nuttig is. Lineas gaf ons bijvoorbeeld advies om bepaalde zaken anders aan te pakken. Uit wat we leerden, halen ook onze andere klanten voordeel."
Christophe Rome bevestigt: "Die testperiode bewees hoe cruciaal het is om de netwerkomgeving en bedrijfsprocessen van je klant te kennen. Er kwamen soms meldingen binnen die geen bedreigingen waren. Maar nu zijn we zeker dat we bij de definitieve opstart alleen nog meldingen krijgen die er echt toe doen."

"Omdat we de omgeving van de klant kennen, kunnen we proactief sturen en snel reageren."
Kris Boulez

OVER LINEAS

Lineas is de grootste private spoorvrachtoperator in Europa met vestigingen in Frankrijk, Duitsland, Nederland, Italië en Spanje. Het hoofdkantoor bevindt zich in België. Het bedrijf wil goede spoorproducten en -diensten aanbieden zodat bedrijven het transport van hun goederen van de weg naar het spoor verschuiven. Zo verbeteren ze hun bevoorradingsketen en verminderen ze de negatieve impact van hun activiteiten op het klimaat, de mobiliteit en luchtkwaliteit.

Het belangrijkste product van Lineas is het Green Xpress Network, dat elke dag snelle en betrouwbare spoorverbindingen tussen Europese hubs aanbiedt. Het bundelt daarbij verschillende soorten vrachten tot één trein.

Lineas telt meer dan 2.100 werknemers en heeft een vloot van meer dan 250 locomotieven en 7.000 wagons.

GESLAAGDE SAMENWERKING

"Ik zocht een technologie om cyberbedreigingen te detecteren en te analyseren, met daarbovenop een service die ons zo veel mogelijk werk uit handen neemt", vertelt Christophe Rome van Lineas. "Die combinatie vond ik bij het intelligente, zelflerende platform Exabeam en de concrete hulp bij cyberbedreigingen van NVISO."

Kris Bogaerts van Telenet Business ziet meerdere voordelen bij deze samenwerking: "We combineren de technologie om logs te centraliseren en te analyseren met reactie op cyberaanvallen door experts. Die concrete hulp is een grote meerwaarde voor onze klanten."

Kris Boulez van NVISO gaat daar verder op in: "We gaan op locatie om bedrijven te helpen en doen dat in hun eigen taal. Lokaal samenwerken levert veel betere resultaten op dan een telefoontje met een expert in een ver land die je bedrijf en netwerk niet kent, de taal niet spreekt en niet ter plaatse kan helpen. Dankzij onze lokale samenwerking krijg je meldingen waar je iets aan hebt en loop je niet het risico dat echte bedreigingen niet worden opgemerkt."

V.l.n.r.: Christophe Rome (Lineas), Kris Boulez (NVISO),
Kris Bogaerts (Telenet Business) en Willem Janssens (Telenet Business).

DE CASE SAMENGEVAT

UITDAGINGEN

- Organisatie van beveiligingsmeldingen;
- Centralisering van logbestanden;
- Automatische analyse van logbestanden;
- Reële meldingen filteren.

OPLOSSINGEN

- Slimme detectie van potentiële gevaren met UEBA via Telenet Business;
- Expert knowledge en Incident Response via NVISO;
- Lokale aanwezigheid en expertise.

VOORDELEN

- Outsourcing;
- Betere en efficiëntere beveiliging;
- Minder kosten.