Innovatie in supply chain security

Slimme technologie voor een veiligere en efficiëntere toekomst

De veiligheid van transport en logistiek is zowel voor de sector zelf als voor de overheid een van de absolute topprioriteiten. En terecht, want cyberaanvallen, drugstrafiek en ladingdiefstallen komen quasi wekelijks in het nieuws. Maar zo divers de uitdagingen zijn, zo uiteenlopend zijn ook de mogelijke oplossingen. Dat blijkt uit de nieuwste innovaties op het vlak van transport- en logistieke veiligheid.

Ken Schepers, Product & Solutions manager bij Proximus NXT bij de introductie van Video Surveillance as a Service: "Videobewaking neemt steeds meer de vorm aan van slimme, cloudgebaseerde systemen."

Bij het innovatiecentrum Log!Ville in Niel stellen elf bedrijven innovatieve technieken voor die transporteurs en logistieke spelers moeten helpen de end-to-end veiligheid van hun processen te verhogen. Voorbeelden zijn vrachtwagens met allerlei slimme sensoren en camerabeveiliging in de laadruimtes, of dekzeilen die insnijdingen detecteren en intelligente testbanken die controleren of goederen op een veilige manier gestapeld zijn voor het transport. De innovaties focussen op een breed scala aan risico's. Er is bescherming tegen cyberaanvallen, toegangscontrole, de opvolging van personen op bedrijventerreinen, beveiliging van ladingen, ongevallenpreventie, enzovoort.

Een allesomvattende oplossing die de veiligheidsrisico's van de transport- en logistieke keten naar nul herleidt, blijft echter een utopie. De beveiliging van supply chains omvat immers tal van aspecten. De toekomst ligt in een geïntegreerde aanpak waarbij technologische innovaties samenwerken om de veiligheidsrisico's op alle fronten te bestrijden: van slimme containers en drones tot het gebruik van AI en blockchain. Die innovaties zijn niet langer een luxe, maar van vitaal belang voor bedrijven om hun concurrentievoordeel te behouden en de veiligheid van de logistieke keten te vrijwaren.

Niet 'of', maar 'wanneer'

De sector van transport en logistiek groeide de voorbije jaren uit tot een geliefkoosd doelwit voor ransomware-aanvallen. Geen toeval, want het disruptieve effect ervan valt niet te overzien. Vooral het aantal cyberaanvallen op de maritieme sector steeg in 2024 naar een recordhoogte. Het voorbeeld van Maersk – dat in 2017 ten prooi viel aan een ransomware-aanval die het bedrijf tien dagen lang gijzelde en maar liefst 300 miljoen dollar schade berokkende – toont aan dat werkelijk elk bedrijf, ongeacht zijn omvang en middelen, een potentieel slachtoffer is.

Hoewel het aantal cyberaanvallen almaar verder toeneemt en cybercriminelen inventiever te werk gaan, laat de beveiliging van IT-systemen nog vaak te wensen over. Bedrijven moe-

ten zich voorbereiden op een aanval, zo klinkt het in de sector. Het gaat er niet om óf er ooit een cyberaanval komt, maar wannéér. Preventiemaatregelen zoals multifactorauthenticatie, offline back-ups, software-updates en netwerksegmentatie zijn in die context no-brainers. Een end-to-end benadering is in de context van cybersecurity eveneens van belang: zekerheid dat ook alle externe softwareleveranciers het nodige doen op het vlak van cyberveiligheid, want net dat bleek bij Maersk de achilleshiel te zijn. Met de NIS2-wetgeving wil de Europese Unie daar alvast sterker op inspelen.

Video Surveillance as a Service

Waar bedrijfsnetwerken het geliefkoosde doelwit van ransomware-criminelen vormen, zijn logistieke sites aan allerlei fysieke risico's blootgesteld. In dat segment van de beveiligingsmarkt zijn tal van nieuwe technologieën aan een opmars bezig, waaronder videobewaking. Proximus NXT speelt daarop in met een oplossing voor 'Video Surveillance-as-a-Service', kortweg VSaaS. Een combinatie van clouddiensten en artificiële intelligentie zorgt voor de automatische detectie van verdachte activiteiten. Slimme camera's leren daarbij het onderscheid te maken tussen normale patronen en anomalieën, zoals een vrachtwagen met een bepaalde nummerplaat die een afwijkende route volgt op het haventerrein. Volgens Ken Schepers, Product & Solutions manager bij Proximus NXT, zal videobewaking in de toekomst steeds meer de vorm aannemen van slimme, cloudgebaseerde systemen.

'Cloud native' camera's zijn belangrijk in dat verhaal. Waar traditionele camera's hun videodata lokaal op een harde schijf opslaan, sturen cloud based camera's alle gegevens rechtstreeks naar de cloud. "Dat gebeurt via een 'edge gateway'-apparaat of 'bridge', dat alle videodata uit de camera haalt en vervolgens doorstuurt. Een groot voordeel is dat er minder internetbandbreedte nodig is aangezien het apparaat de beelden niet streamt", aldus Ken Schepers. Net zoals bij andere cloud devices is ook eenvoudiger infrastructuurbeheer mogelijk, met eenvoudige aanpassingen en integraties, regelmatige updates en externe toegang vanaf elke locatie.

Lagere drempel

Die toegang verloopt via het web, waarbij gebruikers met de juiste toegangsrechten naar een onlineplatform surfen en daar inloggen. Ken Schepers benadrukt de toegankelijkheid van de oplossing vanaf het moment van implementatie: "De cloudverbinding van de camera is volledig geëncrypteerd en traint zichzelf gedurende veertien dagen om abnormaal gedrag te leren herkennen." Het systeem laat ook open integraties toe door middel van API's, waardoor je als beheerder verschillende systemen in een naadloze end-to-end workflow kunt samenvoegen. "VSaaS verlaagt de drempel om een camerabewakingssysteem op te zetten of op te schalen", aldus Ken Schepers.

"Ook het gebruik van beelden wanneer het systeem verdachte gedragingen detecteert en vastlegt, verloopt zo een pak vlotter. Beheerders geven een zoekterm in en het systeem toont alle mogelijke resultaten die aan de ingegeven parameters voldoen. Achteraf kun je een beveiligde link met de beelden genereren. Dat biedt onder andere het voordeel dat je sneller kunt schakelen als je bijvoorbeeld bewijzen moet aanleveren."

Toch draait de oplossing vooral rond het verbeteren van bedrijfsactiviteiten: bezettingsgraden in kaart brengen, heatmaps genereren, nummerplaatherkenning, enzovoort. Bij zijn lancering zal het VSaaS-platform beheerders toelaten meteen 100.000 gebruikers en devices aan te sluiten. In de toekomst wil Proximus NXT dat aantal nog verder uitbreiden.

Fysiek en digitaal

Een goed voorbeeld van hoe fysieke en digitale beveiliging hand in hand gaan, vinden we bij de Haven van Antwerpen-Brugge, een belangrijke logistieke hub die jaarlijks 290 miljoen ton goederen verwerkt. Het gebruik van drones, sensoren en een digital twin van het havengebied, gecombineerd met een sterke digitale ruggengraat, zorgt ervoor dat de haven continue monitoring kan garanderen. Bovendien speelt IT een sleutelrol in het fysieke beheer van de haven, waarbij data uit diverse bronnen, zoals camera's en sensoren, in één centraal platform samenkomen: APICA (Advanced Port Information and Control Assistant). Dat platform stelt teams in staat incidenten in real time op te volgen en zelfs toekomstige risico's te voorspellen door middel van data-analyse met historische data.

Een andere innovatie in de haven is het Inbound Release Platform en het Certified Pickup-systeem. "Het Inbound Release Platform zorgt voor een veilige en efficiënte vrijgave van inkomende containers door middel van gestandaardiseerde en volledig gedigitaliseerde processen", zegt Mieke Laethem, manager Trade Facilitation, Mobility & Digital Cargo Community Services bij de Haven van Antwerpen-Brugge. "Dat maakt het mogelijk de administratieve afhandeling van containerverplaatsingen aanzienlijk te versnellen, terwijl het risico op fouten en fraude vermindert." Het systeem biedt ook een hogere mate van transparantie door alle stappen van de vrijgaveprocedure te monitoren.

Mieke Laethem, manager Trade Facilitation, Mobility & Digital Cargo Community Services bij de Haven van Antwerpen-Brugge: "Oplossingen als het Inbound Release Platform en het Certified Pickup-systeem versnellen de administratie binnen de haven en verminderen tegelijk het risico op fouten en fraude."

Veilige toegang tot containers

Het Certified Pickup-systeem is een sleuteltechnologie voor de beveiliging van vrachtbewegingen binnen de haven. "Het systeem is ontwikkeld in samenwerking met stakeholders uit de sector. Het vervangt het traditionele pincodesysteem dat nodig was voor het ophalen van containers. Het genereert en wijst digitale sleutels gecontroleerd en beveiligd toe, waardoor containers pas vrijkomen wanneer aan alle voorwaarden is voldaan." Omdat het elke stap in het proces volledig opvolgt, is er in principe geen ongeoorloofde toegang of manipulatie meer mogelijk. "Zo stijgen de veiligheid en de operationele efficiëntie aanzienlijk, met minder vertragingen en administratieve fouten."

Tot slot is de bewustwording rond veiligheid van groot belang. De Haven van Antwerpen-Brugge heeft daarom geïnvesteerd in een 'cyber security awareness'-programma, zodat medewerkers leren omgaan met bedreigingen, zoals phishing mails. Die aanpak kan als voorbeeld dienen voor andere bedrijven in de sector, aangezien de menselijke factor vaak een zwakke schakel vormt in het beveiligingsbeleid. Alleen met een geïntegreerde aanpak die zowel technologie als menselijk gedrag omvat, kunnen bedrijven zich wapenen tegen de groeiende dreiging van cybercriminaliteit en fysieke beveiligingsrisico's.

EE