



Niko automatiseert cloudbeveiliging met Sophos Cloud Optix

Niko startte in 1919 met de productie van schakelmateriaal en stopcontacten. Inmiddels is het bedrijf, met het hoofdkantoor in Sint-Niklaas (België) marktleider op dit vakgebied. Verder produceert Niko oplossingen voor toegangscontrole, lichtsturing, energiebeheer en huisautomatisering. Naast hoogwaardige technologie zet het bedrijf volop in op een doordacht design, kwalitatief hoogstaande producten en een milieuvriendelijk productieproces. Deze strategie heeft geleid tot innovatie en groei. De Niko groep bestaat momenteel uit zo'n 750 medewerkers verspreid over meerdere vestigingen waaronder Denemarken, Duitsland, Frankrijk, Nederland, Slowakije en Zwitserland.

CUSTOMER-AT-A-GLANCE



Niko

Industry
Services

Website
www.niko.eu

Aantal medewerkers
750

Sophos-oplossingen
COPX

“We ondersteunen onze bedrijfsvoering en R&D met een on-premise-omgeving van zo’n 250 servers. De laatste jaren hebben we ook de stap naar de cloud gezet om onze flexibiliteit te vergroten en kosten te verlagen”



Innovatie staat centraal in de bedrijfsvoering van Niko. In het streven om gebouwen beter voor mensen te laten werken, ontwikkelen hun experts geavanceerde oplossingen die gebouwen slimmer maken. Hierbij gaan technologie, design en gebruiksgemak hand in hand. Het aanbod bestaat onder andere uit slimme schakelaars en sensoren voor verlichting, oplossingen voor toegangscontrole en energiebeheer, en een compleet Home Control-systeem. Het doel is steeds dat oplossingen naadloos integreren en een ideaal woon- of werkklimaat creëren in gebouwen die klaar zijn voor de toekomst. De bedrijfsprocessen en R&D-activiteiten vereisen dat de IT-omgeving van Niko, zowel on-premise als in de cloud goed inzichtelijk, beheersbaar en beveiligd is.

Stap naar de cloud

“We ondersteunen onze bedrijfsvoering en R&D met een on-premise-omgeving van zo’n 250 servers. De laatste jaren hebben we ook de stap naar de cloud gezet om onze flexibiliteit te vergroten en kosten te verlagen”, stelt Jan Van Moere, Network & Security Engineer bij Niko en verantwoordelijk voor de infrastructuur, netwerk en cybersecurity van het Belgische bedrijf. “Momenteel hebben we 150 servers in de cloud draaien, verdeeld over Amazon Web Services en Microsoft Azure. Vanuit het verleden hebben we een goed overzicht en stevige grip op onze on-premise omgeving. Dit geldt minder voor onze resources in de cloud. Het is een voordeel dat mensen van verschillende afdelingen zelf snel capaciteit in de cloud afnemen en aan de slag kunnen. Dit leidt echter wel tot iets minder controle op en zichtbaarheid van deze cloudactiviteiten.”

Risico’s automatisch in kaart

Sophos Partner SWITCHPOINT NV/SA ondersteunt Niko al jaren met de beveiliging van de IT-omgeving. Beide partners voeren regelmatig gesprekken over de ontwikkelingen in de markt en de vertaalslag naar de beveiliging bij Niko. De zichtbaarheid en beveiliging van cloud-activiteiten kwam aan bod tijdens een gesprek over security analytics & intelligence. “Het gesprek kwam op security-oplossingen die niet alleen cloudactiviteiten inzichtelijk maken, maar ook kwetsbaarheden en risico’s in kaart brengen. SWITCHPOINT NV/SA gaf aan dat Sophos Cloud Optix activiteiten in de cloud niet alleen visualiseert, maar ook geautomatiseerd kan beveiligen.”

Hoewel Niko zeker geïnteresseerd was in de mogelijkheden van Sophos Cloud Optix, is het bedrijf zeer kritisch met de validatie van nieuwe tools. Van Moere: “We bepalen de meerwaarde van tools aan de



hand van dagelijkse praktijk. Daarom doen we geen proof of concept in een testomgeving. Op die manier voorkomen we dat tools in productie anders reageren dan in de testomgeving. Door de oplossing in de productieomgeving te testen, krijgen we een inkijk in wat een product écht voor onze omgeving doet en wat de meerwaarde is."

Snelle installatie en inrichting

Samen met SWITCHPOINT NV/SA startte Niko de installatie van Cloud Optix voor hun AWS- en Azure-cloud. Het was een voordeel dat de installatie en inrichting zeer eenvoudig waren. Ook dat sluit goed aan bij de wensen van Niko, aldus Van Moere. "De inrichting duurde maar een paar uur en vervolgens bood het dashboard heel snel waardevolle informatie over hoe onze clouds functioneren. Het dashboard geeft een complete visualisatie van onze activiteiten bij beide cloudleveranciers. Dat is nuttig omdat we

zo een goed beeld hebben van de resources die we afnemen en hoe we deze benutten. Dit inzicht helpt ons kosten te optimaliseren." Maar dat is een bijkomend voordeel, geeft Van Moere aan.

"Het is vooral belangrijk dat we inzicht hebben in de security-maatregelen in de cloud en hoe die toegepast worden."

Automatische detectie

De inzet van Machine Learning zorgt verder dat Sophos Cloud Optix het ingestelde beleid analyseert. "Afwijkingen in gedrag of configuraties worden automatisch gedetecteerd. Bijvoorbeeld als bepaalde toegangsactiviteiten tot een server ongebruikelijk zijn. Stel dat een beheerder een activiteit in de Amazon Web Services cloud uitvoert en hiervoor iemand uit een ander land inhuurt. Als deze inlogt, wordt dit gesignaleerd. Hierdoor kunnen we eenvoudig een check doen en eventuele risico's proactief voorkomen." Ook toegangsrechten worden nauwlettend in de gaten gehouden en getoetst tegen het geldende beleid. "In het dashboard zien we bijvoorbeeld welke gebruikers met een gewoon wachtwoord zonder multi-factor authentication toegang hebben. Of dat gebruikers meerdere toegangscodes hebben. Als dat zichtbaar wordt, kunnen we daar meteen actie op ondernemen."

Focus op innovatie en groei

Door de inzet van Sophos Cloud Optix kan Niko optimaal profiteren van de flexibiliteit en schaalbaarheid van de cloud zonder concessies aan de beveiliging. Van Moere tot slot: "Onze medewerkers kunnen de cloudresources van Amazon Web Services en Microsoft Azure flexibel en veilig inzetten. We hebben altijd een compleet overzicht van de activiteiten. Bovendien hoeven we alleen de gesignaleerde afwijkingen in ons dashboard te monitoren om ook het beveiligingsniveau te bewaken. Met Sophos Cloud Optix is de beveiliging altijd up-to-date en gewaarborgd. Hierdoor kunnen we al onze energie en aandacht besteden aan verdere innovatie en groei van onze organisatie."

