

Case Sanofi | Beveiliging SCADA-netwerken

Stabiele SCADA-netwerken cruciaal voor bedrijfsvoering én volksgezondheid

Sanofi is één van de grootste farmaceutische bedrijven ter wereld. Zij houden zich bezig met onderzoek, ontwikkeling en productie van geneesmiddelen. Van zelfzorgmiddelen als paracetamol tot middelen voor de behandeling van zeldzame ziekten. Het productieproces luistert nauw. Een storing, hack of virus in het netwerk kan niet alleen bedrijfsmatig gevolgen hebben, maar ook gevolgen voor de volksgezondheid.

“Voor Sanofi geldt bijvoorbeeld dat meetsystemen ontregeld kunnen worden. Dan worden medicijnen met een verkeerde samenstelling geproduceerd en kun je een hele batch vernietigen. Het gaat letterlijk om leven of dood. Stabiele, veilige netwerken zijn écht cruciaal”, vertelt consultant Arjan Speelman.

SCADA-netwerken door lange levensduur verouderd en niet veilig meer

De productieomgeving van Sanofi bestaat uit SCADA-netwerken: Supervisory Control and Data Acquisition. Het verzamelen, doorsturen, verwerken en visualiseren van meet- en regelsignalen van verschillende machines in grote industriële systemen. Arjan: “Bij SCADA kun je ook denken aan drinkwaternetwerken, rioolwater-systemen en olie- en gaspijpleidingen. Een incident kan grote gevolgen hebben. Zoals een stroomuitval in stedelijke gebieden, een ontploffing van gasleidingen of gevaren voor de volksgezondheid. Organisaties lopen dan grote financiële schade op.”



De SCADA-netwerken en de reguliere netwerken liepen bij Sanofi dwars door elkaar heen. Arjan: “Netwerken waren verouderd en niet beveiligd volgens de nieuwste standaarden. SCADA-systemen hebben een lange levensduur. Twintig jaar is geen uitzondering. Ze draaien vaak op verouderde operating systems. Maar ze worden wél via het netwerk ontsloten voor onder andere remote beheer. Oude SCADA-systemen draaien bijvoorbeeld op *proprietary* hardware en software, zijn geïsoleerd van andere IT-systemen geïnstalleerd en draaien op verschillende locaties onafhankelijk van elkaar. Nieuwere SCADA-systemen gebruiken open standaarden, zijn vaak Windows-based en worden juist steeds meer geïntegreerd met IT-systemen en kantoornetwerken. Dat laatste verhoogt wel weer het cybersecurityrisico.”

Domeinscheiding SCADA- en kantoornetwerk door firewalls

“Er zijn een aantal opties voor beveiliging: een domeinscheiding van de kantoor- en SCADA-netwerken, DeMilitarized Zones (DMZ), Intrusion Prevention Systems (IPS), Remote Support Access, redundancy in oplossing en logging en monitoring. Sanofi had de primaire keuze al gemaakt voor een scheiding van de netwerken. Daarin heb je nog verschillende oplossingen, zoals een fysieke of logische scheiding of het

aanbrengen van firewalls. Voor dat laatste is gekozen omdat het de meeste voordelen oplevert. Er is remote monitoring en management mogelijk. De SCADA- en reguliere netwerken maken gebruik van dezelfde hardware waar mogelijk én gescheiden hardware waar nodig”, vertelt Arjan.

Uitrol op vijftig locaties in vijftientig landen

Er zijn firewalls aangebracht tussen de SCADA-netwerken en kantoornetwerken op circa vijftig locaties in ongeveer vijftientig landen in de Azië, Europa en Amerika. Dat gaat om twee tot twintig firewalls voor tien tot tienduizend gebruikers per locatie. Dit is het proces dat werd gevolgd:

- Kwalificeerbaar maken SCADA-systemen voor audits: voldoen aan alle geldende richtlijnen;
- SCADA-compliant maken van de rule-base: verkeersstromen specifiek maken;
- Rule-base maken voor firewalls: verkeersstromen in kaart brengen en regels maken;
- Migreren van VLAN: migratie van netwerksegmenten;
- Installeren en configureren van firewalls per locatie.



‘Sanofi heeft nu stabiele netwerken die minder gevoelig zijn voor invloeden van buitenaf’

“Wat ik één van de grootste uitdagingen vond was het kwalificeerbaar maken van alle SCADA-systemen. Zodat ze voldoen aan de richtlijnen voor audits. Standaarden die wij hebben gebruikt zijn ISA-88, die uit modellen en termen bestaat die het productieproces logisch indelen en de besturing van het machinepark regelen. De ISA-95, internationale standaard voor de integratie van kantoor- en productieautomatiseringssystemen. En ISA/IEC-62443, een internationale standaard voor de beveiliging van productieautomatiserings- en controlesystemen.

Ook was het contact houden met de locaties wereldwijd cruciaal. Goed communiceren was een must. Bijvoorbeeld wanneer en hoe lang er een downtime van het systeem wordt verwacht. Maar ook: testen. Zowel voor als na de migratie zoveel mogelijk testen of alles werkt. Doen de firewalls wat is beoogd? Voldoen ze aan de kwalificatie-eisen? Uiteindelijk hebben wij voor Sanofi écht stabiele netwerken gecreëerd die volgens de laatste standaarden werken en minder gevoelig zijn voor invloeden van buitenaf”, sluit Arjan af.

NiVo network architects is een ingenieursbureau gespecialiseerd in ICT-infrastructuur. Opdrachtgevers worden ondersteund in de complete levenscyclus van hun technologie en diensten. NiVo is actief in de expertisegebieden [networking](#), [datacenters](#), [cybersecurity](#), mobile, [unified communications](#) en [beheer & tooling](#).

Meer weten? [Neem contact op met NiVo](#)