SIDN CyberSterk | case study

Van Donge en De Roo (D&R) is sinds 1977 een expediteur die het vervoer van goederen organiseert en ook coördineert. Er worden op jaarbasis ruim 630.000 containers verwerkt op verschillende locaties. Dennis de Roo (managing director) zag om zich heen het ene na de andere grote- maar ook midden- en kleinbedrijf slachtoffer worden van een hack. En ging daarom op zoek naar een partij die kon helpen om dat vooruitzicht te voorkomen.

Het hoofdkantoor van D&R is gevestigd in Rhoon, vlak bij de terminal in Rotterdam. Daarnaast beschikt D&R ook over een terminal in Antwerpen, waar onder andere containers worden overgeslagen, gerepareerd en gewassen. Het vervoer van al die containers loopt via vrachtschepen, vliegtuigen, vrachtwagens, treinen en binnenvaartschepen. Daarnaast heeft het bedrijf met ruim 340 medewerkers een eigen douaneafdeling.
Door in te loggen op de website van D&R kunnen klanten inzien waar een container zich bevindt in de ‘pijplijn’ en tegelijkertijd kunnen ze de nodige documenten van het betreffende transport inzien. Wat betreft alle klantgegevens – het bestand beslaat tussen de 1000 en 5000 klanten per afdeling – is het volgens De Roo van groot belang dat deze goed beschermd worden.

Wat er vooraf speelde

“We waren in eerste instantie met name aan het kijken naar de beveiliging van ons netwerk,” vertelt De Roo. “Bij andere bedrijven in de haven zagen we heel wat partijen die de dupe werden van cybercriminaliteit. Wij zelf zijn nooit gehackt, maar de gebeurtenissen om ons heen zetten ons wel aan het denken.”
Daarom gingen ze bij D&R op zoek naar een partij die voor al hun facetten – het netwerk en de verschillende websites – de securityrisico’s zo klein mogelijk kon maken. De Roo: “Het is lastig om duidelijk in beeld te krijgen of je website wel of niet goed beveiligd is. Wij maken gebruik van WordPress. En als je kijkt naar wat er gebeurt in de hackerswereld, dan is dat wel een ‘fantastisch programma’ om aan te vallen. Wanneer daar een lek zit, dan gaat het als een lopend vuurtje rond onder alle actieve hackers.”

De oplossing van SIDN CyberSterk

D&R heeft meerdere softwareleveranciers en het netwerk is op dit moment gedeeltelijk gevestigd in de cloud, ten behoeve van de opslag. Het datacenter heeft D&R geplaatst op kantoor; elke nacht wordt er een back-up gemaakt.

Om cyberweerbaar te worden én zicht te krijgen in alle risico’s op het gebied van cybersecurity is D&R in zee gegaan met SIDN CyberSterk, dat inmiddels 107 werkplekken (seats) en één website bewaakt. “En vanuit daar willen we deze oplossing steeds verder uitrollen,” vertelt De Roo. “Doordat onze website op afstand wordt gescand én door de plaatsing van de SIDN CyberSterk-box die 24/7 meekijkt met ons verkeer, hebben we al een aantal risico’s inzichtelijk gekregen. Zo waren er bijvoorbeeld een paar routers in het pand aanwezig waarvan we eigenlijk niet meer op de hoogte waren. Maar deze ‘achteruitgangen’ konden wel mogelijke gevaren opleveren.” Over de implementatie vertelt De Roo het volgende: “De implementatie van de SIDN CyberSterk-box ging ook super. Erg snel. Eigenlijk was de box in amper een kwartiertje geïnstalleerd.”

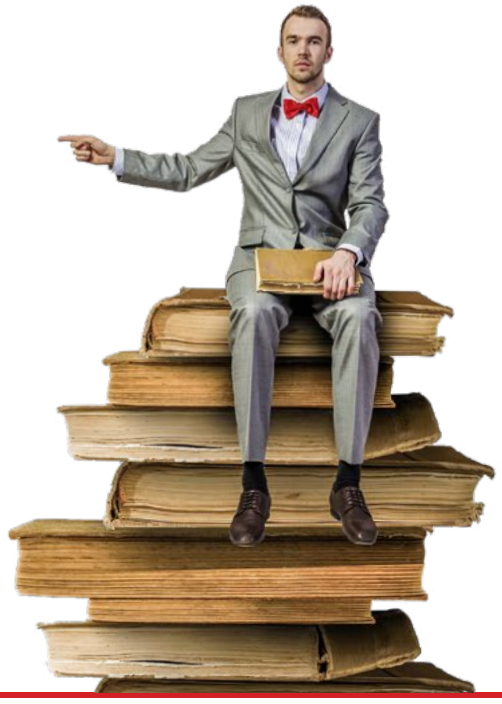
Het behaalde resultaat

“Door de maatregelen rondom de coronacrisis hebben we op een snelle manier de thuiswerkomgeving moeten inrichten. Maar we wilden dit uiteraard op zo’n manier bewerkstelligen dat er geen extra risico’s op de loer kwamen te liggen. Daarom wordt er onder andere gewerkt met een twee-factorauthenticatie, waarbij je twee stappen succesvol moet doorlopen om ergens toegang toe te krijgen. Daarnaast zijn we erg blij met het feit dat nu – met de oplossing van SIDN CyberSterk – het verkeer op ons netwerk ook in de gaten wordt gehouden wanneer we niet op kantoor werken.”
Concluderend zegt De Roo het volgende over de oplossing: “Het geeft mij een comfortabel gevoel dat ons netwerk 24/7 in de gaten wordt gehouden en dat daarbij ook de website wordt meegenomen met een wekelijkse website scan.
Ik raad SIDN CyberSterk zeker ook aan vanwege het stukje bewustwording van de potentiële gevaren op het gebied van cybercriminaliteit. Het krijgen van inzicht in die risico’s vind ik van grote toegevoegde waarde.”

Meer weten?
Neem contact op met alex.vanwijhe@sidn.nl

SIDN CyberSterk is een product van SIDN Business B.V., onderdeel van SIDN | KvK 75364689 | BTW NL860254252B01

Bedankt voor uw interesse in Cybersterk!



Hopelijk heeft dit document u de benodigde informatie en inzicht gegeven waar u op zoek naar was.

Andere tools die uw organisatie weerbaarder maken

ProteQtor IT Security is niet alleen reseller partner van SIDN Cybersterk, maar biedt nog meer cybersecurity tools aan om uw organisatie zo weerbaar mogelijk te maken.

Hieronder tools die wellicht interessant zijn ter bescherming van uw organisatie:

- Bescherm uw gegevens met **SentinelOne endpoint protection**
- Liever een Europese endpoint protection & EDR tool? Kies **Reaqta**
- Beveilig uw e-mail met **Proofpoint email security**
- Train uw medewerkers met laagdrempelige **Wizer security awareness trainingen**
- Bescherm het inloggen met **Watchguard Authpoint multi-factor authenticatie**
- Voorkom bezoeken aan ongewenste websites met **NSOC360 Safeweb webfiltering**
- Herstel verloren data met **NSOC360 Safedata online backup**

ProteQtor
Next-Gen IT Security

Laat hackers uw bedrijfscontinuïteit niet in gevaar brengen!

Cyberaanvallen bedreigen privacy, bedrijfskritische data, de reputatie en andere 'kroonjuwelen' die cruciaal zijn voor de continuïteit van uw organisatie. De vraag is allang niet meer 'of' uw organisatie aangevallen wordt, maar 'wanneer' uw organisatie (weer) aangevallen wordt. Het is essentieel om cyberaanvallen te voorkomen en de gevolgen van cyberaanvallen tot een minimum te beperken. Het feit dat u deze pdf leest, toont dat u dat belang inziet.

Vanwege de grootte, de complexiteit en de diversiteit van moderne cyberaanvallen is een multidisciplinaire aanpak nodig. We helpen u graag met praktische adviezen en effectieve oplossingen om deze aanpak te realiseren.

Met de juiste trainingen, tools en support helpen wij u hackers het hoofd te bieden en er voor te zorgen dat alles wat voor uw organisatie van waarde is, beschermd blijft.

Hulp nodig? Bel 088-0660770 of plan een afspraak in

ProteQtor
Next-Gen IT Security

Telefoon : +31 (0)88 066 0770
E-mail : contact@proteqtor.nl
Website : proteqtor.nl