



## Insight helpt BCC proactief aan sterke en gebruiksvriendelijke e-mail- en websitebeveiliging

### Story Snapshot

BCC had de beveiliging van website en e-mail prima op orde, maar wenste al langer een gebruiksvriendelijker programma. Op het moment dat Insight kennisnam van een compleet nieuwe oplossing, werd BCC direct ingelicht. De Proof of Concept (POC) werd uitgevoerd en bezorgde iedereen zeer waardevolle inzichten.



Retail

### Achtergrond

BCC is een Nederlandse retailer in consumentenelektronica. Het bedrijf telt 61 fysieke winkels en de website trekt vele miljoenen bezoekers per maand, hetgeen goed is voor een substantieel deel van de bedrijfsinkomsten.

### Uitdaging

Voor de beveiliging van de website en het e-mailverkeer maakte BCC al langere tijd gebruik van Azure Front Door-mogelijkheden van Microsoft voor WAF en DDoS-mitigatie, en Microsoft 365 voor e-mailbescherming. Dit bood hen echter niet het gebruikersgemak die ze wensden.

“We gebruikten Azure Front Door, die hadden we zelf ingericht. Het werkte vrij statisch, maar dat volstond lange tijd. De wens was er wel om het fijnmaziger in te richten, maar we wisten ook dat dit het IT-team veel werk zou gaan kosten, nu en in de toekomst. We keken dan ook uit naar iets dat gebruiksvriendelijker zou zijn, terwijl het tegelijkertijd ook proactief cyberdreigingen kon detecteren. En zolang dat er niet was, bleven de dingen zoals ze waren. Het is typisch zo’n onderwerp dat tijdens mijn gesprekken met Maarten Burgmeijer van Insight de revue passeert. We hadden het er al tijdje niet meer over gehad, maar op het moment dat Maarten kennis had genomen van een nieuwe oplossing, belde hij me enthousiast op,” vertelt Corine Bos, IT-directeur bij BCC.

*“We gebruikten Azure Front Door, die hadden we zelf ingericht. Het werkte vrij statisch, maar dat volstond lange tijd. De wens was er wel om het fijnmaziger in te richten, maar we wisten ook dat dit het IT-team veel werk zou gaan kosten, nu en in de toekomst. We keken dan ook uit naar iets dat gebruiksvriendelijker zou zijn, terwijl het tegelijkertijd ook proactief cyberdreigingen kon detecteren.”*

Corine Bos

IT-directeur, BCC Elektro-speciaalzaken BV

*“We zijn allemaal megadruk, dat Maarten hier uit zichzelf mee kwam, dat is wat je wil van een IT-partner. Dat ze weten wat de klant zoekt en nodig heeft. Ik ben blij met die extra paar oren en ogen.”*

Corine Bos  
IT-directeur, BCC Elektro-speciaalzaken BV



“We zaten midden in de pandemie, een tijd waarin mensen massaal online zijn gaan winkelen en we ook de cyberaanvallen zagen toenemen. Een concurrent van BCC was vrij recent getroffen door Ransomware, logisch dus dat Corine voor BCC een strengere maar ook gebruiksvriendelijke tooling wenste. Barracuda had me net laten zien hoe hun nieuwe applicatie werkte. Een compleet nieuwe oplossing die webwinkels beschermt tegen onder andere scraperbots en DDoS-aanvallen. Scraperbots zijn geautomatiseerde bots die websites afstruinen om prijs- en productinformatie te verzamelen en te vergelijken. Het kan concurrenten een voordeel opleveren. DDoS-aanvallen, zoals het bekende Ransomware, zorgen ervoor dat je website plat komt te liggen, met alle gevolgen van dien. Barracuda’s presentatie was zo overtuigend en de SaaS-applicatie werkte zo eenvoudig, ik wist direct dat dit de oplossing was die BCC zocht,” zegt Maarten Burgmeijer, Executive Account Manager bij Insight.

## Oplossing

Insight bracht BCC en Barracuda in coronatijd virtueel samen voor een gesprek en al vrij snel volgde het draaien van een ‘proof of concept’ (POC) voor zowel de beveiliging van e-mail als de website. Op die manier kon BCC direct ervaren wat de oplossing voor de organisatie kon betekenen.

“Op het moment dat we de Web Application Firewall van Barracuda gingen testen, was het heel even schrikken voor ons e-commerce-team. Die zag ineens de webtraffic flink dalen. Toen we vervolgens zagen dat de conversie op de website gelijk bleef en zelfs ging stijgen, wisten we dat het goed zat. Ook de POC met hun Email Protection maakte duidelijk dat er meer dan genoeg winst te behalen viel voor ons. Kortom, de tooling deed zijn werk meer dan goed en het maakte voor de gehele organisatie heel inzichtelijk wat voor aanvallen er zoal waren geweest. Dit samen met de feestdagen in het vooruitzicht en de hack bij de concurrent zorgde ervoor dat er vrijwel direct budget vrijgemaakt werd om de beveiliging van website en e-mail te kunnen optimaliseren met behulp van de oplossingen van Barracuda,” vervolgt Corine.

“Naast voorkomen dat je website stilvalt, wil je ook zorgen dat de website zo goed mogelijk werkt. Bots en scrapers zorgen vaak voor vertraging en dat kan hinderlijk zijn tijdens het bezoeken van zo’n webshop. Naast vertraging zorgen die bots en scrapers ook voor veel meer traffic op de website dan nodig is. Bedenk dat je Azure vaak afneemt op basis van het aantal users, dan kun je wel nagaan wat het wegvallen van al dat overbodige en schadelijke verkeer op dat vlak doet met de kosten,” vervolgt Maarten.



## Resultaat

De nieuwe oplossingen van Barracuda hebben nog een tijdje naast Azure Front Door gedraaid bij BCC. Op het moment dat alles helemaal naar wens was ingericht, werd Front Door uitgezet.

“Bij Barracuda zitten ze er bovenop. Is er een nieuwe bedreiging, dan wordt het in een mum van tijd opgenomen in de beveiliging. We zien dat we op dagelijkse basis worden aangevallen, maar ook dat dit dus proactief wordt tegengehouden, zonder dat het onze IT-afdeling zeeën van tijd kost. We zijn allemaal megadruk, dat Maarten hier uit zichzelf mee kwam, dat is wat je wil van een IT-partner. Dat ze weten wat de klant zoekt en nodig heeft. Ik ben blij met die extra paar oren en ogen,” besluit Corine.

## HIGHLIGHTS

- Proactieve mindset Insight
- Risico’s minimaliseren van DDoS-aanvallen en scraperbots
- Gebruiksvriendelijke beveiligingsoplossing
- Barracuda WAF-as-a-Service en Email Protection