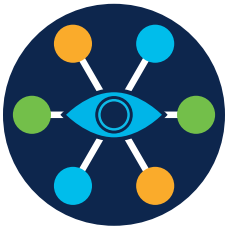
Bornego College: 90 procent minder cyberincidenten door Cisco Umbrella

Ongekende groei van data, een sterke toename van gebruikers die met eigen mobiele apparaten werken, en een open cultuur waarin samenwerken en data delen heel gewoon is. Een combinatie die organisaties kwetsbaar maakt voor cyberaanvallen. Het Friese Bornego College kan erover meepraten, want het kreeg te maken met DDos-aanvallen die van binnen en buiten kwamen. Ondanks uitgebreide securitymaatregelen, ontbrak het tot voor kort aan goed zicht op internetverkeer. Dit gat in de beveiliging is nu succesvol gedicht met Cisco Umbrella: binnen twee weken daalde het aantal cyberincidenten met ruim 90 procent.

Het Bornego College is een onderwijsinstelling voor vmbo-t, havo, atheneum en gymnasium. De hoofdvestiging staat in Heerenveen. Dat de scholengemeenschap vijf locaties telt en tweeduizend eindgebruikers, betekent dat er pittige eisen worden gesteld aan het netwerk. Toen de school in 2013 iPad-onderwijs wilde invoeren, bleek dat dit niet goed mogelijk was zonder de IT-infrastructuur te vernieuwen. Er kwamen onder meer nieuwe switches en wireless access points en met Cisco CleanAir beschikt de instelling over een oplossing die verstoringen van het wifi-signaal elimineert. Het aantal securitymaatregelen werd stapsgewijs opgevoerd, op verschillende netwerklagen.



De uitdaging: meer zicht krijgen op internetverkeer

Desondanks vond de netwerkbeheerder dat hij nog altijd onvoldoende inzicht had in alle internetverkeer. Het IT-team zag het aantal incidenten oplopen. En mede door DDoS-aanvallen kwam het functioneren van het netwerk in het gedrang.

Daar komt bij dat leerlingen door de jaren heen steeds meer devices zijn gaan gebruiken, waardoor het steeds lastiger is om het netwerk goed te monitoren. Verder signaleert de school dat leerlingen steeds vaker een VPN-verbinding opzetten, om de beveiliging te omzeilen. Die wordt in dit geval gebruikt om toegang te krijgen tot bestemmingen waarvoor de school geen toestemming geeft. De firewall is als het ware blind voor zo'n verbinding.

Voor de school waren deze ontwikkelingen ongewenst, omdat ze het risico op een cyberaanval vergroten. Er ontstond vrees voor een datalek en voor de boetes, reputatieschade en claims die daarmee gepaard kunnen gaan. Het Bornego College moet immers net als iedere andere organisatie voldoen aan strenge wet- en regelgeving rondom bescherming van privacygevoelige data.

De driekoppige IT-afdeling riep daarom de hulp in van kennispartner aaZoo. Deze dienstverlener was al betrokken bij de vernieuwing, beheer en onderhoud van het netwerk. Het was tijd om voorzorgsmaatregelen te nemen, om de beschikbaarheid van het netwerk te kunnen garanderen.

De oplossing: Cisco Umbrella

Eén van de mogelijkheden die aaZoo aandroeg om het zicht op wat er op het netwerk allemaal gebeurt te vergroten, was de implementatie van Cisco Umbrella. De naam zegt het eigenlijk al: Umbrella is een paraplu of schild tegen dreigingen. Een cloudoplossing die eenvoudig gezegd gebruikmaakt van een database, met daarin een enorme hoeveelheid bestemmingen die als 'verdacht' zijn aangemerkt. Als iemand daar contact mee zoekt, komt de verbinding eenvoudigweg niet tot stand.

Tevens is Umbrella in staat om VPN's te blokkeren die niet zijn toegestaan. Ook op die manier wordt voorkomen dat kwaadwillende software het netwerk bereikt. De check vindt altijd daar plaats waar data het pand in- en uitgaat, meestal de internet gateway. Met Umbrella is het dus mogelijk om bijvoorbeeld een firewall of wifipunten te beveiligen.

De database van Umbrella is altijd actueel, doordat Cisco beschikt over een team van meer dan 250 technici (Talos). Dat volgt dagelijks alle ontwikkelingen op het gebied van cyberdreigingen op de voet.

Resultaten: minder incidenten, meer notificaties

Een proof of concept verzorgd door aaZoo leverde direct resultaat op. Umbrella bracht aan het licht dat een alarmerend groot aantal geïnfecteerde mobiele devices ongehinderd het draadloze netwerk op kon. In 80 procent van de gevallen ging het daarbij om malware. Geen enkele security-oplossing sloeg erop aan. Voor Bornego was dit de bevestiging dat er meer zicht moest komen op internetverkeer. “We ontdekten dat een firewall met IPS niet genoeg bescherming biedt”, zegt systeembeheerder Atze Zandstra.

Volgens Jeroen Melis, security-specialist bij Cisco, denken veel organisaties ten onrechte dat hun security goed geregeld is. “De technologie die bij cyberaanvallen wordt gebruikt is zó vooruitstrevend dat een firewall echt niet meer alles tegenhoudt. Pas als dit zichtbaar wordt, is duidelijk dat het tijd is om de manier waarop je netwerk is beveiligd te heroverwegen.”

Het Bornego College boekte door Umbrella nog meer resultaat:

- Binnen twee weken liep het aantal security-incidenten met meer dan 90 procent terug.
- De oplossing genereerde in deze tijd 54 notificaties.

Het grootste deel van deze signalen had te maken met verdachte apparaten, zoals smartphones, die verbinding met het netwerk probeerden te maken. Maar IT werd ook geattendeerd op pogingen om de elektronische leeromgeving te hacken.

Security naar een hoger niveau door integratie

Behalve een beter zicht op dreigingen, had de scholengemeenschap nog een paar redenen om voor deze oplossing te kiezen. De prijs speelt een rol, maar ook het feit dat het relatief eenvoudig is om met Umbrella aan de slag te gaan. Omdat het een cloudoplossing is, hoeft er niets te worden geïnstalleerd. De implementatie is meestal een kwestie van minuten. Bovendien kon de IT-afdeling in dit proces leunen op aaZoo, dat zich sinds februari 2020 Cisco Advanced Security Partner mag noemen.

Een groot voordeel van Cisco is dat het sterk is in integratie van hard- en software, waardoor oplossingen als één geheel werken. Dat is ook het geval als deze van andere leveranciers afkomstig zijn. De school geeft aan dat het hierdoor beschikt ‘over een efficiënt werkend en eenvoudig te managen security-platform.’ Melis: “Er wordt vaak verondersteld dat individuele oplossingen ingrijpen, bijvoorbeeld als een geïnfecteerd apparaat wordt gedetecteerd. Maar dat blijkt in de praktijk vaak niet zo te zijn. De grote kracht van Cisco is dat wij ervoor zorgen dat componenten elkaar begrijpen en daardoor wel tot actie overgaan.”

Umbrella fungeert volgens Melis als een extra ‘wasstraat’ tegen verdacht internetverkeer, als toevoeging op de firewall. Zo til je netwerksecurity naar een hoger niveau, omdat Cisco Umbrella dreigingen al een halt toeroept voordat ze het netwerk bereiken.

Meer weten over wat Cisco Umbrella voor jouw organisatie kan betekenen?
Kijk dan op https://umbrella.cisco.com of https://umbrella.cisco.com/products/cloud-security-service.