SIMPLY SECURE

INTEGREER BYOD-BEVEILIGING IN UW NETWERK.

IT-BEVEILIGING VOOR ONDERWIJSINSTELLINGEN

KLANT

- Sector: Onderwijs
- Land: België
- Grootte: Meer dan 3000 studenten
- Netwerk: 1100 pc's in twee subnetwerken

UITDAGINGEN

- Beschermen tegen malware
- BYOD-toestellen beveiligen
- Geen invloed op systeemprestaties

ONZE OPLOSSING

- Uitstekend detectiepercentage voor malware
- BYOD-beveiliging naadloos integreren in netwerkbeveiliging
- Intuitieve beheer-interface

VOORDELEN

- Minder malware-infecties
- Goed beveiligde BYOD-toestellen
- Verbeterde efficiëntie

campus de helix
waar talent thuiskomt

Wanneer een IT-afdeling van drie personen verantwoordelijk is voor de beveiliging van een netwerk met meer dan 1100 PC's is de kwaliteit van de malware-beveiliging van essentieel belang. Vooral als dit netwerk een scholengemeenschap met ruim 3000 leerlingen en cursisten bedient, waar meegebrachte USB-sticks en harde schijven een grote bedreiging vormen.

Campus de helix is een samenwerkingsverband tussen de vier vroegere katholieke scholen van Maasmechelen (België). Campus de helix heeft in het secundair onderwijs ruim 1.900 leerlingen in 31 verschillende studierichtingen. Het volwassenenonderwijs heeft ruim 1.200 cursisten. De meeste leerlingen en cursisten brengen veel tijd door op de pc's op de campus en op hun zelf meegebrachte laptops (Bring Your Own Device).

De IT-omgeving is opgedeeld in twee subnetwerken; één voor de leerlingen en één voor het personeel. De leerlingen hebben op hun netwerk beperkte rechten. Zij kunnen niets installeren, maar het is wel toegestaan om eigen datadragers te gebruiken, zoals USB-sticks en harde schijven. Vooral dat laatste leverde vaak problemen op. ICT-coördinator Marc Majzik vertelt: "De beveiligingssoftware die wij voorheen gebruikten, van een grote Amerikaanse aanbieder, liet regelmatig virussen en andere malware van die meegebrachte datadragers toe op het netwerk. Daardoor hebben wij als IT-afdeling van slechts drie man sterk al heel wat monsterklussen moeten klaren om het netwerk weer schoon en werkend te krijgen. En dat terwijl het pakket vrij duur was en daarbij niet eens zo prettig in het beheer." Toen het contract op zijn einde liep, vond Majzik het dan ook tijd om op zoek te gaan naar een alternatief.

DE OPLOSSING: BYOD-INTEGRATIE EN UITSTEKENDE MALWARE-BEVEILIGING

Het voorkomen van malware-infecties was het belangrijkste criterium, maar tegelijkertijd vond Majzik een lage systeembelasting en een absoluut minimum aan meldingen van de software aan de gebruiker ook essentieel. Tevens was het belangrijk dat de gekozen beveiligingssoftware in staat was om de van huis meegebrachte toestellen enerzijds te beschermen

150237_GD_CaseStudy_CampusDeHelix_NL • 0011280715

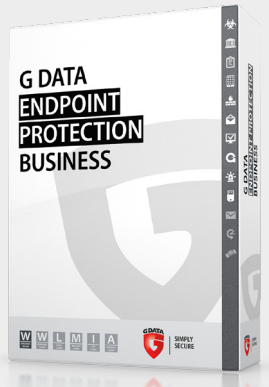
"ONS NETWERK IS, SINDS WIJ VIER JAAR GELEDEN MET G DATA STARTTEN, VOLLEDIG MALWARE-VRIJ GEBLEVEN." Marc Majzik, IT Manager

tegen malware en anderzijds te controleren voordat deze het campusnetwerk betreden. Verder was het noodzakelijk dat de software gemakkelijk was in het beheer, gezien de bescheiden omvang van het IT-team. Tot slot was het van essentieel belang dat de prijs van de oplossing binnen het budget zou passen.

In de zoektocht naar een geschikte beveiligingsoplossing bezocht Majzik een evenement waar verschillende aanbieders van beveiligingssoftware zich presenteerden. "De eerlijkheid gebiedt mij te zeggen dat ik in de eerste plaats werd getrokken door de zeer aantrekkelijke prijzen die G DATA onderwijsinstellingen kan

bieden. Naar aanleiding daarvan ben ik G DATA gaan researchen op internet. Ik kwam al gauw zeer veel positieve berichten tegen over het constant hoge detectieniveau dat G DATA biedt en de positieve ervaringen die andere gebruikers hebben met de software en de service van G DATA. Dit heeft ons doen besluiten om contact op te nemen met G DATA." Tijdens het testen van de software viel op dat de installatie erg gemakkelijk verliep en dat de interface heel intuïtief is. "Al snel besloten wij definitief met G DATA in zee te gaan." De installatie van de software op het gehele netwerk kostte nog geen twee uur tijd, een fractie van de installatie van het vorige beveiligingspakket.

G DATA ENDPOINT PROTECTION BUSINESS



DE VOORDELEN

Inmiddels heeft Campus de helix al vier jaar ervaring met G DATA ENDPOINT PROTECTION en kan met veel zekerheid een aantal conclusies worden getrokken. Majzik: "Ons netwerk is, sinds wij vier jaar geleden met G DATA startten, volledig malware-vrij gebleven. Via de management console en via e-mail krijgen we nu alle meldingen van gestopte virussen binnen. We hoeven zelfs niet meer om te kijken naar installaties: door de integratie met Active Directory wordt het pakket automatisch op nieuw geïnstalleerde computers gezet. En dat alles terwijl wij minder kosten hebben. Doordat wij met G DATA veel efficiënter zijn in de strijd tegen malware hebben wij nu veel meer tijd voor onze andere taken."

WWW.GDATA.NL / WWW.GDATA.BE

© Copyright 05/2015 G DATA Software AG. Alle rechten voorbehouden. Dit document mag noch volledig, noch gedeeltelijk worden gekopieerd of gereproduceerd zonder de schriftelijke toestemming van G DATA Software AG Duitsland.

Microsoft, Windows, Outlook en Exchange Server zijn gedeponeerde handelsmerken van The Microsoft Corporation. Alle overige handelsmerken en merknamen zijn eigendom van hun respectieve eigenaars en moeten daarom als dusdanig worden behandeld.

SIMPLY SECURE

150237_GD_CaseStudy_CampusDeHelix_NL • 0011280715