



SIMPLY
SECURE

NETWERK BEVEILIGING ZONDER ACHTERPOORTJES

IT-BEVEILIGING VOOR DE COATINGINDUSTRIE

KLANT

- Sector: Industriële coating
- Land: Duitsland
- Grootte: 240 werknemers
- Netwerk: Windows-server, desktopcomputers, notebooks en Android-toestellen

UITDAGINGEN

- Industriële spionage en nieuwe bedreigingen voor de IT-infrastructuur
- Onbedoelde malware-infecties binnen het bedrijf

ONZE OPLOSSING

- Geen achterpoortjes
- Uitstekend detectiepercentage voor malware
- Eenvoudige implementatie

VOORDELEN

- Beveiliging tegen criminelen en spionage
- Gemoedsrust: geen zorgen over gegevensbeveiliging
- Minder tijd nodig voor implementatie en beheer



VOGLER

Eenvoudige malware was lange tijd de grootste digitale dreiging, maar die tijd is voorbij. Zowel concurrenten als hackers in opdracht van de overheid hebben het gemunt op industriële bedrijven en willen hun handelsgeheimen stelen en activiteiten verstoren.

Vogler GmbH & Co. KG werd in 1990 opgericht als full-service industrieel coatingbedrijf. Het levert coatingdiensten aan de meest uiteenlopende sectoren, van de automobiellindustrie tot fabrikanten van industriële apparatuur. Vogler telt 240 werknemers, beschikt over een volledig automatisch magazijn met hoge stellingen en richt zich op efficiënte kwaliteitsproducten die voldoen aan de eisen van het kwaliteitslabel "Made in Germany".

Om ervoor te zorgen dat bestellingen tijdig kunnen worden verwerkt, wordt de IT-infrastructuur van Vogler voortdurend bewaakt en geoptimaliseerd. Clients worden beveiligd tegen malware en een restrictief beleidsbeheer zorgt ervoor dat gebruikers het netwerk niet onopzettelijk kunnen infecteren met malware met een geïnfecteerde USB-stick. Het risicolandschap verandert echter voortdurend. "De onthullingen over de NSA hebben ons doen beseffen aan welke gevaren onze IT-infrastructuur wordt blootgesteld", vertelt Timo Erlemann, manager van de IT-afdeling van Vogler. "Naast de

bekende risico's van virussen en andere malware, vormt industriële spionage een steeds grotere bedreiging." Malware is niet langer het enige digitale gevaar waarmee bedrijven van elke grootte te maken krijgen.

Beveiligingsproblemen in software of zelfs in beveiligingsoplossingen zelf kunnen worden misbruikt om toegang te krijgen tot computersystemen. Vooral dat laatste is problematisch. Sommige landen dwingen ontwikkelaars om hun beveiligingsoplossingen te voorzien van achterpoortjes voor de overheid. Hoewel dit vaak wordt gerechtvaardigd door te verwijzen naar de strijd tegen criminelen of



"AAN ONZE IT-BEVEILIGING STELLEN WE DEZELFDE KWALITEITSEISEN ALS AAN ONZE EIGEN PRODUCTEN. DAAROM HEBBEN WE VOOR G DATA GEKOZEN."

Timo Erlemann, manager van de IT-afdeling

terroristen, kunnen deze zwakke plekken gemakkelijk voor industriële spionage worden gebruikt.

DE OPLOSSING: BEVEILIGING MET EEN GESTROOMLIJNDE INTERFACE, ZONDER ACHTERPOORTJES

"Aan onze IT-beveiliging stellen we dezelfde kwaliteitseisen als aan onze eigen producten. Daarom hebben we voor G DATA gekozen", zegt Erlemann. De beveiligingsoplossingen van G DATA voldoen aan de Duitse privacy-wetgeving, een van de strengste ter wereld. Bedrijven hoeven zich geen zorgen te maken over geheime achterpoortjes, omdat de oplossingen van G DATA er geen bevatten. De Duitse



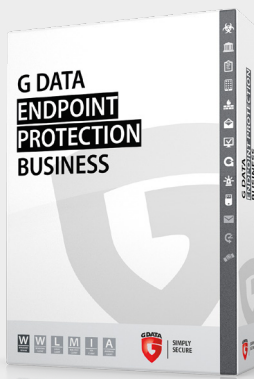
overheid kan bedrijven niet dwingen om hun producten te voorzien van achterpoortjes. Dat is bijzonder geruststellend voor bedrijven die zeker willen zijn dat hun beveiligingsoplossing hun gevoelige gegevens in elk opzicht beschermt. Niet alleen de ontwikkeling van de software gebeurt in Duitsland, ook de servers van G DATA bevinden zich daar.

G DATA ENDPOINT PROTECTION BUSINESS bleek de perfecte oplossing voor Vogler. De oplossing voldeed aan alle beveiligingseisen en bood tegelijk een bijzonder gebruiksvriendelijke interface, waardoor Vogler deze zelf kon implementeren en geen geld hoefde te besteden aan externe consultants en technici. De configuratie van de verschillende gebruikersgroepen, gebruikersrechten en update-instellingen werd door medewerkers van Vogler uitgevoerd.

DE VOORDELEN

"ENDPOINT PROTECTION BUSINESS is een doordachte en goed gestructureerde oplossing die perfect op onze behoeften kan worden afgestemd", vertelt Daniel Bölling, IT-beheerder bij Vogler. G DATA biedt het bedrijf beveiliging op alle niveaus en zorgt ervoor dat gewone criminelen, concurrenten en hackers in opdracht van de overheid, op geen enkele manier toegang krijgen tot gevoelige gegevens. Ook hun technische ondersteuning was uitstekend, zo vertelt Erlemann: "Tot nu toe hebben we amper technische ondersteuning nodig gehad, maar de enkele keren dat dat toch het geval was, werden onze problemen snel opgelost tot onze volledige tevredenheid."

G DATA ENDPOINT PROTECTION BUSINESS



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**