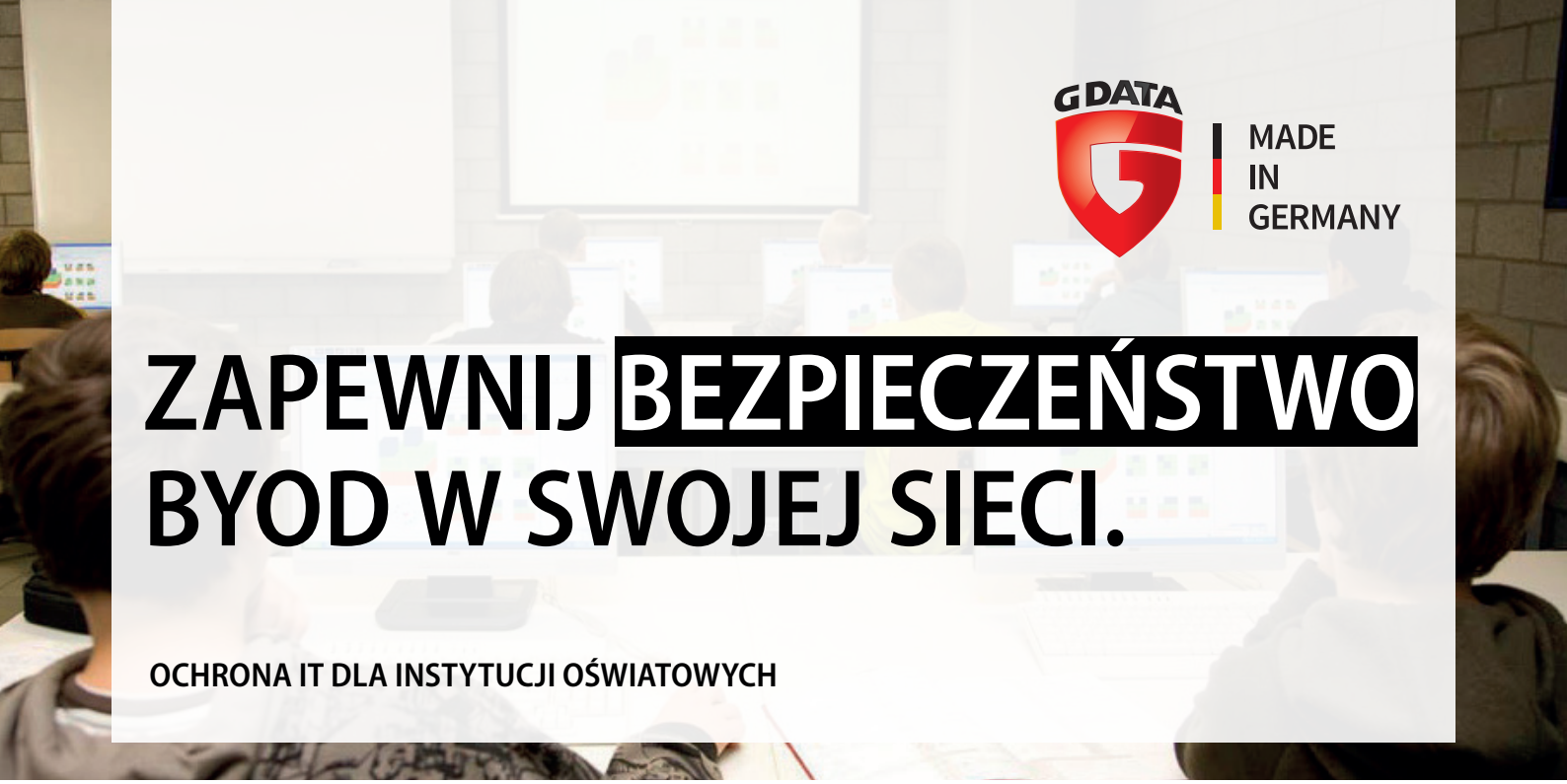


G DATA MADE IN GERMANY

ZAPEWNIJ BEZPIECZEŃSTWO BYOD W SWOJEJ SIECI.

OCHRONA IT DLA INSTYTUCJI OŚWIATOWYCH

KLIENT

- Branża: Edukacja
- Kraj: Holandia
- Wielkość: 6000 uczniów
- Sieć o wielu lokalizacjach i BYOD

WYZWANIA

- Wgląd w bieżący stan bezpieczeństwa sieci
- Zapobieganie zakażeniu sieci przez urządzenia BYOD

NASZE ROZWIĄZANIE

- Doskonały wskaźnik wykrywania złośliwego oprogramowania
- Bezproblemowe włączenie ochrony urządzeń BYOD do systemu ochrony sieci
- Ograniczenia w korzystaniu z aplikacji, urządzeń i internetu

KORZYŚCI

- Mniej przypadków zakażenia złośliwym oprogramowaniem
- Skuteczne zabezpieczenie urządzeń BYOD z Androidem
- Oszczędność dzięki konkurencyjnym cenom

ROC Kop van Noord-Holland

scholen aan zee ONDERWIJS VAN NIVEAU

Sieci szkolne są narażone na wiele rodzajów ataków – nie tylko ze strony złośliwego oprogramowania pochodzącego z komputerów szkolnych, ale i coraz częściej z prywatnych laptopów, smartfonów i tabletów uczniów.

Szkoła ROC Kop van Noord-Holland i zespół szkół Scholen aan Zee to instytucje zajmujące się edukacją ponadpodstawową, zawodową i kształceniem dorosłych w ośmiu placówkach w Den Helder, Schagen i Julianadorp (w Holandii). Obie szkoły prowadzą szeroko zakrojoną edukację przy wykorzystaniu technologii cyfrowych, w związku z czym zainwestowały sporo w potrzebne środowisko i infrastrukturę IT.

Dwa lata temu szkoła Scholen aan Zee jeszcze bardziej rozwinęła tę formę kształcenia, wdrażając projekt Flex-IT, w ramach którego zachęca się uczniów do przynoszenia do szkoły własnych laptopów. W 2005 roku nastąpiło połączenie działów IT ROC Kop van Noord-Holland i Scholen aan Zee i obecnie nowo utworzony pion zarządza środowiskiem informatycznym obu instytucji, a także obsługuje ponad 6000 uczniów i kursantów.

Do niedawna szkoły zabezpieczały swoją sieć za pomocą produktów jednego z wiodących dostawców oprogramowania ochronnego. „Poprzednie rozwiązanie dawało nam fałszywe poczucie bezpieczeństwa" – uważa administrator IT, Raymond Bernaert. „Bardzo rzadko wysyłało nam jakiekolwiek powiadomienia, więc myśleliśmy, że nasza sieć jest bezpieczna."

Okazało się, że największym wyzwaniem są laptopy uczniów. Szkoły natychmiast zaczęły doświadczać zmasowanych ataków złośliwego oprogramowania, których źródło można było zlokalizować w sprzęcie przynoszonym przez uczniów w ramach polityki „Przynieś swoje własne urządzenie" (Bring Your Own Device, BYOD). „Nasza baza Active Directory została zaatakowana. Szkodliwe oprogramowanie próbowało się do niej zalogować przy użyciu różnych haseł. Po trzech nieudanych próbach zablokowały się konta. W ciągu kilku minut mieliśmy więc na głowie setki zablokowanych kont w naszej bazie danych i musieliśmy ręcznie aktywować każde z nich" – opowiada Bernaert. „Cały personel szkoły i uczniowie siedzieli przez ten czas bezczynnie, a to oznaczało nieakceptowalną stratę czasu." Ponadto przekonanie uczniów do tego, aby zainstalowali na swoich komputerach dobre oprogramowanie ochronne, okazało się niezwykle trudne. A ponieważ laptopy stanowią własność uczniów, szkoły nie mogą ich objąć ich swoją własną licencją.

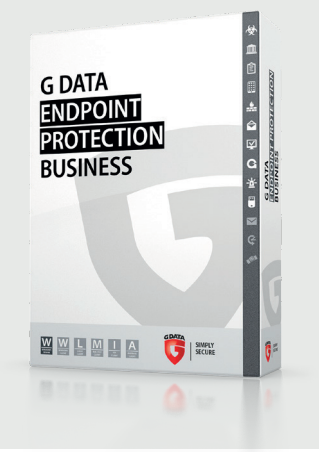
150244_GD_CaseStudy_ROCKop_2015_PL_04 • 2811051115

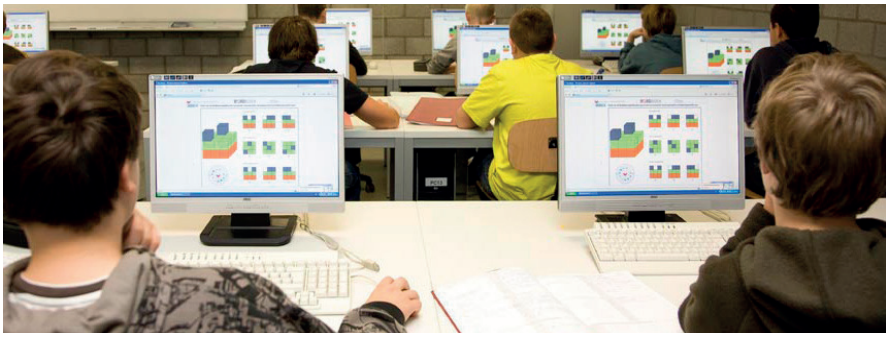
„NASZA SIEĆ JEST ODCZUWALNIE LEPIEJ CHRONIONA I ROZWIĄZALIŚMY PROBLEMY Z URZĄDZENIAMI BYOD. A DO TEGO MOŻEMY LICZYĆ NA ŚWIETNĄ POMOC TECHNICZNĄ, ŚWIADCZONĄ PRZEZ E-MAIL, TELEFON LUB SKYPE." Raymond Bernaert, administrator IT

ROZWIĄZANIE: BEZPROBLEMOWE WŁĄCZENIE OCHRONY URZĄDZEŃ BYOD DO SYSTEMU OCHRONY SIECI

Wówczas szkoły postanowiły znaleźć nowe rozwiązanie w zakresie ochrony IT, spełniające następujące wymogi: wysoka wykrywalność szkodliwych programów, możliwość objęcia ochroną prywatnych urządzeń uczniowskich a także opłacalny koszt licencji. Dział IT szybko znalazł ofertę G DATA. „Zaczęliśmy testować ich produkty i natychmiast odnotowaliśmy wyższą wykrywalność szkodliwego oprogramowania w porównaniu z wynikami poprzedniego antywirusa" - mówi Raymond Bernaert. „Poza tym firma G DATA przedstawiła nam rozwiązanie, pozwalające zredukować zagrożenie infekcji ze strony

G DATA ENDPOINT PROTECTION BUSINESS





laptopów uczniów – ofertę zniżki na zakup licencji dla urządzeń prywatnych naszych uczniów i pracowników. Od przyszłego roku wdrożymy oprogramowanie G DATA, które okazało się bezkonkurencyjne, na wszystkich laptopach w naszej sieci. Później będzie musiał je mieć zainstalowane każdy komputer, który zechce uzyskać dostęp do naszej sieci."

Po wybraniu rozwiązania G DATA, Raymond Bernaert wziął też udział w jednym z bezpłatnych szkoleń technicznych, organizowanych przez dostawcę. Podczas szkolenia jego uwagę przykuł moduł Policy Manager, będący elementem całościowego oprogramowania G DATA w pakiecie ENDPOINT PROTECTION BUSINESS. „Policy Manager pomoże nam uporać się z problemem, z którym zmagamy się każdego dnia. Uczniowie często zdają na swoich laptopach szkolne testy, przy czym nauczyciele zabraniają im korzystania z niektórych aplikacji, takich jak sprawdzanie pisowni w Wordzie, czy dostęp do internetu. Przy pomocy modułu Policy Manager można łatwo zablokować wybrane funkcje, aby nauczyciele nie musieli przez cały czas kontrolować wszystkich laptopów podczas testów."

KORZYŚCI

Choć szkoły nie wdrożyły jeszcze wszystkich opcji pakietu ENDPOINT PROTECTION BUSINESS, już odczuwają korzyści, jakie zapewnia im to rozwiązanie. Jak przyznaje Raymond Bernaert: „Nasza sieć jest odczuwalnie lepiej chroniona i rozwiązaliśmy problemy z urządzeniami BYOD. A do tego możemy liczyć na świetną pomoc techniczną, świadczoną przez e-mail, telefon. Mam numery telefonów komórkowych niemal wszystkich pracowników z G DATA. Obiecali nawet, że odbiorą telefon w nocy, ale na szczęście dla nich nie musiałem jeszcze korzystać z tej opcji!"

WWW.GDATA.PL

G DATA MADE IN GERMANY

150244_GD_CaseStudy_ROCkop_2015_PL_04 • 2811051115