Integrieren Sie BYOD-Sicherheit in Ihr Netzwerk

IT-Sicherheit für Bildungseinrichtungen.

Foto: Dicide

Kunde

- Branche: Bildung
- Land: Niederlande
- Umfang: 6.000 Lernende
- Netzwerk: Mehrere Standorte, auch mit BYOD-Geräten

Die Herausforderung

- Die Netzwerksicherheit stets im Blick behalten
- Infizierungen des Netzwerks durch BYOD-Geräte verhindern

Die Lösung

- Hervorragende Malware-Erkennungsrate
- Nahtlose Integration von BYOD-Sicherheit in die Netzwerksicherheit
- Beschränkung der Anwendungs-, Geräte- und Internetnutzung

Die Vorteile

- Weniger Malware-Infektionen
- Effizient abgesicherte BYOD-Geräte
- Geringere Kosten dank wettbewerbsfähiger Preisgestaltung

Schulnetzwerke zählen zu den besonders gefährdeten Zielscheiben für Malware-Attacken – Gefahr geht dabei nicht nur von den schuleigenen Computern aus, sondern zunehmend auch von den privaten Notebooks, Smartphones und Tablets der Schüler.

Die niederländischen Berufskollegschulen „ROC Kop van Noord-Holland“ und „Scholen aan Zee“ bieten an acht Standorten in Den Helder, Schagen und Julianadorp Unterricht im Sekundarstufenbereich sowie Unterricht in der Berufs- und Erwachsenenbildung. Beide Bildungseinrichtungen sind stark auf digitales Lernen ausgerichtet und haben große Summen in digitale Lernumgebungen und -infrastrukuren investiert.

Vor zwei Jahren beschleunigte die „Scholen aan Zee“ diese Entwicklung durch Einführung des sogenannten Flex-IT-Projekts, das die Schüler ermutigte, ihr eigenes Notebook mit zur Schule zu bringen. Im Jahr 2005 wurden die IT-Abteilungen von „ROC Kop van Noord-Holland“ und „Scholen aan Zee“ zusammengelegt. Die neue Abteilung verwaltet die IT-Umgebung beider Einrichtungen und unterstützt mehr als 6.000 Lernende. Bis vor kurzem sicherten die Schulen ihre Netzwerke mit Produkten eines führenden Herstellers von Sicherheitslösungen. „Diese Lösung wog uns in falscher Sicherheit“, erklärt IT-Administrator Raymond Bernaert. „Die Software erstellte kaum Benachrichtigungen, weshalb wir fälschlicherweise dachten, dass unser Netzwerk sicher sei.“

Die Notebooks der Schüler erwiesen sich als die größte Herausforderung. Die Schulen hatten bereits Erfahrungen mit Malware-Ausbrüchen, deren Ursache auf die BYOD-Regelung der Schule zurückgeführt werden konnte. „Unser Active Directory wurde angegriffen. Die Malware versuchte immer wieder sich mit verschiedenen Passwörtern anzumelden. Accounts werden nach drei vergeblichen Versuchen gesperrt, wodurch wir innerhalb weniger Minuten mit Hunderten von gesperrten Active Directory-Accounts konfrontiert waren, die alle manuell entsperrt werden mussten“, so Raymond Bernaert. „Mitarbeiter und Schüler saßen herum und konnten nicht arbeiten w eine ungeheure Zeitverschwendung.“ Zudem erwies es sich als schwierig, die Schüler zu überzeugen, dass sie auf ihren Rechnern eine anständige Sicherheitslösung installieren müssen. Da die

„Unser Netzwerk ist nachweislich besser geschützt. Wir haben unsere BYOD-Probleme gelöst. Wir können uns auf einen hervorragenden Support per E-Mail, Telefon oder Skype verlassen.“

Raymond Bernaert, IT-Administrator

Notebooks Privateigentum der Schüler sind, können Schulen ihre Softwarelizenzen nicht zur Verfügung stellen.

Die Lösung: Nahtlose Integration von BYOD in die Netzwerksicherheit

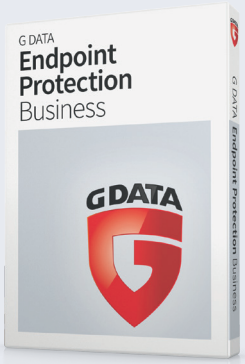
Die Schulen suchten daraufhin nach einer neuen Sicherheitslösung. Sie sollte hohe Malware-Erkennungsraten sowie die Möglichkeit bieten, sie auch auf privaten Geräten zu implementieren. Zudem gab es die Anforderung, dass sich die Lizenzgebühren in einem angemessenen Rahmen bewegen. Die IT-Abteilung stieß schon bald auf G DATA. „Wir haben die Produkte getestet und im Vergleich zur alten Lösung sofort die viel höheren Malware-Erkennungsraten festgestellt“, erläutert Raymond Bernaert. „Darüber hinaus hatte G DATA auch einen Vorschlag, wie man die Risiken der Schüler-Notebooks in den Griff bekommt. Man unterbreitete uns ein Angebot mit Lizenzvergünstigungen für die privaten Geräte aller Schüler und Mitarbeiter. Schon bald wird G DATA standardmäßig auf allen von uns zur Verfügung gestellten Notebooks installiert sein. Dann muss jeder PC, der auf das Netzwerk zugreifen möchte, mit der dieser Sicherheitslösung ausgestattet sein.“

Nach dem Kauf besuchte Raymond Bernaert eines der kostenfreien technischen G DATA Seminare. Dort weckte der PolicyManager sein Interesse. Ein optionales Modul der G DATA Endpoint Protection Business. „Der PolicyManager behebt ein Problem, mit dem wir täglich zu tun haben. Unsere Schüler schreiben auf ihren Notebooks oft Klassenarbeiten, doch einige Anwendungen sind dabei verboten, z. B. die Word-Rechtschreibprüfung sowie der Internetzugang. Mit dem PolicyManager werden diese Anwendungen ganz einfach blockiert.“

Die Vorteile

Die Vorteile, so Raymond Bernaert, sind bereits jetzt deutlich: „Unser Netzwerk ist nachweislich besser geschützt. Wir haben unsere BYOD-Probleme gelöst, können uns auf hervorragenden Support per E-Mail, Telefon oder Skype verlassen und ich kann G DATA selbst nachts anrufen. Das war aber noch nie der Fall!“

G DATA
Endpoint Protection Business



Mehr Informationen:

www.gdata.de

TRUST IN GERMAN SICHERHEIT