Bildungswerk der Niedersächsischen Wirtschaft nutzt Next Generation Firewall von Palo Alto Networks™ – Effektiver Schutz gegen Attacken von außen und IT-Sicherheitsgefahren von innen

BACKGROUND

Das Bildungswerk der Niedersächsischen Wirtschaft gemeinnützige GmbH (BNW) bietet berufliche Orientierungshilfe, Vermittlungsunterstützung und Fortbildungsprogramme. Rund 1.100 Mitarbeiter arbeiten an über 140 Standorten daran, Menschen mit dem wichtigsten Rohstoff Deutschlands zu versorgen: Wissen. Moderne Informationstechnologie übernimmt hierbei eine Doppelrolle als Mittel und Zweck – sie vermittelt Inhalte und trägt dazu bei, den alltäglichen Umgang mit zeitgemäßen Technologien zu erhalten oder zu vertiefen. Die Sicherheit der IT-Infrastruktur ist für das BNW daher von zentraler Bedeutung. Um gegen Angriffe von außen wie auch gegen IT-Security-Gefahren von innen gewappnet zu sein, hat sich das Bildungswerk für die Next Generation Firewall von Palo Alto Networks entschieden.

IT-BASIERTES LERNEN BEIM BNW

Das BNW ist einer der größten Bildungsdienstleister Niedersachsens. Die „Schüler" des aus 24 Trägern gebildeten Bildungswerks können auch Führungskräfte mit viel Berufserfahrung sein. Doch, egal ob jung oder alt, scheint den Menschen hin und wieder die Lust auf Abwechslung im Lernalltag zu überkommen – und IT-basierte Lernplätze mit Internetzugang bieten hier viele Ablenkungsmöglichkeiten: „Einer unserer Mitarbeiter rief mich an und teilte mir mit, dass in einem der Schulungsräume das Computerspiel ‚Call of Duty' gespielt würde. Und er fragte, ob wir dagegen nichts unternehmen könnten", so Markus Köhler, der beim BNW als Leiter der IT-Abteilung und als Supportverantwortlicher tätig ist. „Dem Kollegen war nach fünf Minuten geholfen. Einige wenige Klicks im Dashboard der Palo Alto Networks Firewall haben mich zur Steam Application geführt, die ich sofort geblockt habe."

Nachdem der Status der Anwendung auf Deny gesetzt wurde, konnten die Rechner keine Verbindung mehr zum Server herstellen. „Die Teilnehmer haben das Spielen daraufhin eingestellt", fügt Köhler mit einem Schmunzeln hinzu. „Wir helfen den Lehrern und Trainern also dabei, dass die Schüler ihre Aufgaben erledigen." Neben dem rigorosen Blocken einzelner Anwendungen gibt es dabei elegante Alternativen. So lässt sich mit der Firewall über die Quality of Services die Bandbreite für einzelne Anwendungen festlegen. „Wir können so zum Beispiel für fachfremde Anwendungen die Geschwindigkeit drosseln. Youtube macht keinen Spaß, wenn für ein Frame mehrere Sekunden Ladezeit nötig sind", erläutert Matthias Canisius, Regional Sales Manager, Palo Alto Networks. „Außerdem ermöglichen sogenannte Time Tables, Anwendungen nur zu bestimmten Uhrzeiten zu erlauben. Die Kursteilnehmer des BNW können also in der Mittagspause durchaus ihren Freunden auf Facebook mitteilen, was sie vormittags gelernt haben – und danach ist die Anwendung wieder geblockt." Hier zeigt sich der technische Vorteil des Konzepts: Die Firewall nutzt keinen Paketfilter mehr, sondern analysiert die Anwendungen unabhängig vom Port.

ORGANISATION:
Bildungswerk der Niedersächsischen Wirtschaft gemeinnützige GmbH (BNW)

BRANCHE:
Education

HERAUSFORDERUNG:
Attacken von außen wie durch den Conficker-Wurm abwehren und so Bedrohungen vom Netz des BNW abwenden. Verhindern, dass Schüler Zugriff auf Webinhalte wie Spiele haben, die sie vom Unterricht ablenken.

LÖSUNG:
Implementierung einer Next-Generation Firewall von Palo Alto Networks.

ERGEBNIS:
Einzelne Anwendungen können rigoros geblockt werden. Zudem lässt sich mit der Firewall über die Quality of Services die Bandbreite für einzelne Anwendungen festlegen. Sogenannte Time Tables ermöglichen darüber hinaus, Anwendungen nur zu bestimmten Uhrzeiten zu erlauben. Attacken auf das Netz des BNW können jetzt isoliert werden. Die verbesserte Sicherheit durch die Firewall von Palo Alto Networks hat auch indirekt positive Auswirkungen – dem IT-Support-Team des BNW bleibt mehr Zeit, um echte Support-Fälle zu betreuen, anstatt sich vornehmlich um die Schulungsräume zu kümmern.

paloalto NETWORKS
the network security company™

VOM ÄRGERNIS ZUM REALEN BEDROHUNGSSZENARIO

Bis hierhin waren die Beispiele des BNW eher der Kategorie Ärgernisse zuzuordnen. Abgesehen von den negativen Auswirkungen auf den gewünschten Lernerfolg, kann dies heutzutage Konsequenzen nach sich ziehen, die über den Einzelnen hinausreichen, denn gerade aus Administratorensicht gibt es Schlimmeres als unaufmerksame Kursteilnehmer: Gezielte oder zufällige Angriffe von außen auf das Rechnernetz könnten den gesamten Weiterbildungsbetrieb lahmlegen. „Zweimal infizierte eine Version des Conficker-Wurms Schulungsräume, die zwar nicht vom BNW betreut werden, aber auch an unserem Netz hängen“, erzählt Markus Köhler weiter. „Die Firewall hat es uns glücklicherweise ermöglicht, die Attacke zu isolieren. Damit war die Bedrohung von unserem Netz abgewendet.“

Schadsoftware im Web ist für 76 Prozent der Befragten einer aktuellen Umfrage des „eco Verbands der deutschen Internetwirtschaft“ das wichtigste technische Sicherheitsthema – und damit an Platz eins der Bedrohungsszenarien. Trotz neuer Trends wie Cloud Security ist damit das Web nach wie vor das entscheidende Sicherheitsrisiko. Die Antworten auf diese Bedrohungen waren bisher meist das Kumulieren unterschiedlicher Systeme, von Paketfiltern über VPN-Gateways bis hin zu Content-Filtern. Das Ergebnis war eine heterogene Sicherheitsinfrastruktur mit all den bekannten Nachteilen von Insellösungen: Die Wartung- und Lizenzkosten sind vergleichsweise hoch und die Bedienung ist wegen der vielen unterschiedlichen Oberflächen komplex. Darüber hinaus sind die Latenzzeiten lang, denn die Systeme interagieren nicht optimal. Diese Liste ließe sich noch fortsetzen. „Wir haben daher einen Ansatz gewählt, der die Applikation in den Mittelpunkt stellt, unabhängig von Port, Protokoll oder Verschleierungsmethoden“, erklärt Canisius die Idee des Palo Alto Networks-Konzepts. „Daher werden wir auch von Gartner als einziger Anbieter einer echten „Next Generation Firewall“ eingestuft. Unser Lösungsansatz vereinigt die Identifikation von Anwendung, Benutzer und Inhalt.“

„Zweimal infizierte eine Version des Conficker-Wurms Schulungsräume, die zwar nicht vom BNW betreut werden, aber auch an unserem Netz hängen. Die Firewall hat es uns glücklicherweise ermöglicht, die Attacke zu isolieren. Damit war die Bedrohung von unserem Netz abgewendet.“

Markus Köhler
Leiter IT-Abteilung
der IT-Abteilung beim BNW

„Auch wenn die Anforderungen, die an uns als IT-Abteilung gestellt werden, in Sachen ‚sicherer Zugriff auf das Unternehmensnetzwerk' immer größer und herausfordernder werden, habe ich mit Palo Alto Networks als Partner ein gutes Gefühl für die Zukunft."

Markus Köhler
Leiter IT-Abteilung
der IT-Abteilung beim BNW

MEHR ZEIT FÜR WIRKLICHE SUPPORT-FÄLLE

Die verbesserte Sicherheit durch die Firewall von Palo Ato Networks hat auch indirekt positive Auswirkungen. So bleibt dem sechsköpfigen IT-Support-Team des BNW um Markus Köhler zum Beispiel mehr Zeit, um echte Support-Fälle zu betreuen anstatt sich vornehmlich um die Schulungsräume zu kümmern. „Wir hatten sehr viele Anfragen von Dozenten, ob wir Anwendungen blocken können, da Kursteilnehmer abgelenkt waren", bestätigt Köhler. „Wir können jetzt ohne Black Lists arbeiten. Damit sind wir nun in der Lage, proaktiv zu arbeiten. Zum Beispiel können wir jetzt in regelmäßigen Abständen das Control Center checken." Nicht wenige der Schulungsteilnehmer des BNW sind sehr technikaffin, sodass die Administratoren selbst immer wieder neue, ihnen zuvor unbekannte Anwendungen entdecken. Mit der neuen Firewall kann die IT-Mannschaft nach einem vorherigen Check im Netz Anwendungen blocken, noch bevor Anfragen entstehen.

In Zukunft plant das BNW weiterhin mit der Palo Alto Networks-Lösung zu wachsen – Köhler sieht hier insbesondere die zunehmende Anzahl mobiler Mitarbeiter als nächste Aufgabe für die Netzwerksicherheit, denn immer mehr Kollegen möchten von außen auf das Netz zugreifen. „Auch wenn die Anforderungen, die an uns als IT-Abteilung gestellt werden, in Sachen ‚sicherer Zugriff auf das Unternehmensnetzwerk' immer größer und herausfordernder werden, habe ich mit Palo Alto Networks als Partner ein gutes Gefühl für die Zukunft", resümiert Köhler.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com