proofpoint

TRADITIONSREICHE UNIVERSITÄT GEHT CYBERSICHERHEIT PROAKTIV AN

HERAUSFORDERUNG

- Abwehr von Ransomware-, Spam- und Phishing-Angriffen, bevor diese in die Postfächer der Benutzer gelangen können
- Verbesserung des E-Mail-Reputationsfaktors der Universität
- Besseres Sicherheitsbewusstsein
- Minimierung des Zeitaufwands für die Behebung von Cyberbedrohungen zugunsten proaktiverer Projekte

LÖSUNG

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection und Integration mit Palo Alto Networks WildFire

ERGEBNISSE

- Stoppt 300.000 bis 500.000 Ransomware-Angriff pro Woche
- Reduziert die Zahl der Phishing-E-Mails und Klicks erheblich
- Verringert die Zahl kompromittierter Konten von 200 pro Monat auf weniger als 12
- Bietet detaillierte Übersicht über Bedrohungen, Auswirkungen und Trends

Wie kann eine traditionsreiche Universität mit mehr als 16.000 Studierenden und Stipendiaten, mehr als 4.000 Fakultätsmitgliedern und vielen Programmen, Fachbereichen und zugehörigen Organisationen umfassenden Schutz bieten? Mit einem proaktiven Cybersicherheitsansatz und präventiver Bedrohungsabwehr.

Als im Jahr 2011 ein neuer CISO (Chief Information Security Officer) seine Arbeitsstelle bei der Universität antrat, stellte er fest, dass ein E-Mail-Gateway der Enterprise-Klasse nötig war. Er suchte bei Gartner um Rat und las den Review zu Proofpoint. Dadurch wurde er auf diesen Anbieter und die beeindruckenden Kundenreferenzen aufmerksam. Und er entschied sich für Proofpoint Email Protection.

ERGÄNZUNG DER CLOUD

Die Universität verlegte außerdem einige der Systeme in die Cloud. So migrierte das E-Mail-System zu Microsoft Office 365, um die Kosten, Supportanforderungen und den durch Exchange-Server entstehenden Rechenzentrum-Ressourcenbedarf zu reduzieren. Proofpoint Email Protection wurde zwischen die bereits vorhandene Lösung Palo Alto Networks WildFire und Office 365 integriert. Dadurch erhält das Sicherheitsteam deutlich besseren E-Mail-Schutz und einen besseren Einblick in die Sicherheitslage.

„Die Veränderungen waren enorm“, sagte der CISO. Spam verschwand in den immer besser optimierten Spam-Filtern der Hochschule. Anschließend wurde der ausgehende Schutz aktiviert, um die dauerhaften Reputationsprobleme zu beseitigen.

„Der Unterschied war gewaltig“, betont er.

GEZIELTE PHISHING-ABWEHR

Nach dem Aktivieren des ausgehenden E-Mail-Schutzes konzentrierte sich das Sicherheitsteam auf die Reduzierung der Phishing-Angriffe und ihrer Folgen. Zu diesem Zeitpunkt führten Phishing-E-Mails jeden Monat zu mehr als 200 kompromittierten Konten. Der CISO sprach sich für die Implementierung von Proofpoint Targeted Attack Protection (TAP) aus. Diesem Vorschlag wurde schnell zugestimmt und die Universität integrierte TAP über eine einfache API-basierte Aktivierung mit Palo Alto Networks WildFire. Durch die Kombination der zwei Lösungen können die Cloud-basierten Malware-Analysen der beiden Anbieter den Schutz über das Proofpoint-E-Mail-Gateway und die Palo Alto Networks-Firewall automatisch miteinander abstimmen.

Dank TAP ging die Zahl der jeden Monat kompromittierten Konten von 200 auf weniger als 12 zurück. Für die wenigen „durchgeschlüpften“ Phishing-E-Mails öffnete die Hochschule ein Support-Ticket bei Proofpoint, damit diese E-Mails dokumentiert und zum TAP-Schutz hinzugefügt werden konnten. Davon profitieren alle.

„Wenn sich jemand über eine eingegangene Phishing-E-Mail beschwert, kann ich gern die Zahlen dahinter zeigen“, sagt der CISO. „So verzeichnen wir zum Beispiel 200.000 Phishing-Versuche pro Monat, aber nur 21 sind tatsächlich in ein Postfach gelangt.“

„Proofpoint leistet uns gute Dienste und hält Ransomware zuverlässig von unseren Systemen fern. Wir freuen uns darüber, dass Proofpoint uns so effektiv vor dieser großen Menge an Ransomware schützt.“

Chief Information Security Officer, traditionsreiche Universität

STOPPEN VON RANSOMWARE

Ab 2016 verzeichnete die Hochschule eine Flut von Ransomware-Angriffen. Das Sicherheitsteam entdeckte jede Woche 300.000 bis 500.000 Ransomware-Angriffe, die in das Netzwerk einzudringen versuchten. Mitte 2016 lag die Zahl in nur sieben Tagen bei 500.000 Angriffen. Proofpoint isoliert verdächtige E-Mails sofort, führt Sandbox-Analysen durch und stellt so fest, ob sie tatsächlich schädlich sind.

„Proofpoint leistet uns gute Dienste und hält Ransomware zuverlässig von unseren Systemen fern“, erklärt der CISO. „Wir freuen uns darüber, dass Proofpoint uns so effektiv vor dieser großen Menge an Ransomware schützt.“

TRANSPARENZ FÜR EFFEKTIVE MASSNAHMEN

Wenn es in der Vergangenheit zu einem Phishing-Angriff kam, sendete das Sicherheitsteam eine Nachricht an die gesamte Hochschule und fragte nach, ob irgendjemand auf die E-Mail geklickt hat. Es war schwierig, die Folgen einer bestimmten E-Mail genau einzuschätzen.

Die Berichtsfunktionen von Proofpoint bieten dem Team nun sofortige Transparenz – einschließlich detaillierter Daten, die eine schnelle Reaktion ermöglichen. Wenn jetzt eine Phishing-E-Mail durchgeht, weiß das Team genau, wer diese E-Mail erhalten hat und wie viele Personen insgesamt betroffen sind. Sie können jeden Empfänger kontaktieren oder die Konten aus Sicherheitsgründen sperren. Proofpoint bietet die Möglichkeit, die Phishing-Folgen zu kontrollieren, sofort an genau der richtigen Stelle zu reagieren und so Zeit und Benachrichtigungsaufwand zu sparen. Kompromittierte Konten sind jetzt eine seltene Ausnahme. Dank dieser Veränderung hat das Sicherheitsteam nun die Freiheit, sich mit komplexeren Sicherheitsmaßnahmen zu beschäftigen.

„Proofpoint ist taktisch und präzise“, beschreibt der CISO. „Die Reaktion auf Zwischenfälle bereitet keine Bauchschmerzen mehr. Der Umgang mit der Technologie ist sehr komfortabel. Die Navigation ist einfach, ich finde genau die richtigen Informationen und kann Berichte generieren sowie Trends überwachen.“

AUSWIRKUNGEN AUF DIE ZUKUNFT

Obwohl das Sicherheitsteam die Universität rund um die Uhr schützt, bereitet die wachsende Zahl und Vielfalt der Bedrohungen große Sorgen. Zudem richten sich diese Angriffe auch gegen Hochschulen, Unternehmen und Strafverfolgungsbehörden.

„Manchmal finden die Menschen Sicherheitsbedenken übertrieben“, sagt der CISO. „Doch in einigen Fällen entwickeln sich Situationen, die sehr ernst und folgenschwer sind. Wir müssen reagieren. Wir können nicht abwarten, bis jemand herausfindet, warum wir angegriffen werden. Wir müssen eine Abwehr aufstellen und die Universität schützen. Proofpoint unterstützt uns dabei.“

Der CISO ärgert sich darüber, dass kriminelle Akteure ehrbare Institutionen angreifen, die gute Dienste für die Gesellschaft leisten. Er sieht seine Verantwortung darin, sein neues Wissen weiterzugeben, damit Hochschulen die Cyberbedrohungen gemeinsam effektiver abwehren können. Er empfiehlt seinen Kollegen an anderen Instituten, sich Proofpoint genauer anzusehen, da er die Effektivität aus eigener Erfahrung kennt.

INFORMATIONEN ZU PROOFPOINT
Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.