proofpoint.

KUNDENBERICHT

Bildungsministerium von Neuseeland schützt tausende Schulen mit Proofpoint

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Die Herausforderung

- Schutz von Schülern und Lehrkräften vor Bedrohungen
- Berücksichtigung individueller Schulanforderungen bei einem standardisierten Ansatz
- E-Mail-Sicherheit bei minimalen Kosten für Schulen

Die Lösung

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection

Die Ergebnisse

- Aktuelle E-Mail-Sicherheit minimiert hochentwickelte Bedrohungen
- Verbesserte E-Mail-Sicherheit für proaktive Sicherheit
- Proofpoint erlaubt reibungslose Integration in verschiedene Umgebungen

Die Behörde

Wie lässt sich ein landesweites Schulsystem mit mehr als 900.000 Schülern und Lehrkräften absichern? Für das Bildungsministerium von Neuseeland beginnt das mit dem Schutz der E-Mail-Kommunikation. Die Behörde gibt die Richtung für Behörden und Anbieter vor und unterstützt die Regierung dabei, ihre Bildungsziele zu erreichen.

Die Herausforderung

Landesweiter Schutz der Kommunikation von Schülern und Lehrkräften
In Neuseeland müssen Schulen und Kura Kaupapa Māori (staatliche Schulen für Māori-Kultur und -Werte) ständig einen Kompromiss zwischen ihren lokalen Anforderungen und nationalen Standards suchen. Sie haben ihren eigenen Schulträger, der meist lokal gewählt wird und viele der anzuwendenden Regeln und Prozesse festlegt. Aktuelle E-Mail-Bedrohungen lassen sich jedoch nicht von geografischen Grenzen aufhalten. Daher erkannte das neuseeländische Bildungsministerium, dass es eine standardisierte Option zum Schutz von Schülern, Lehrkräften und Mitarbeitern anbieten muss.

„Vor einigen Jahren gab es eine relativ schwerwiegende Cybersicherheitsverletzung bei einer unserer regionalen Gesundheitsbehörden“, erklärt Andrew Hood, Chief Advisor of Cybersecurity beim Bildungsministerium von Neuseeland. „Wir wurden gefragt, wie wir die Cybersicherheit der neuseeländischen Schulen verbessern können.“

Schulen in Neuseeland können ihre Produktivitätssoftware flexibel wählen und entscheiden sich meist für Google mit Workspace Plus oder Microsoft 365 – oder sogar für eine Kombination aus beiden Lösungen. Das Bildungsministerium übernimmt die Lizenzkosten, während die Schulen individuelle Mandanten-umgebungen konfigurieren.

„Auf unsere Schulen verteilen sich etwa 3.500 unterschiedliche Google- und Microsoft-Mandantenumgebungen“, erklärt Hood. „Sorgen bereitete uns, dass die standardmäßige Konfiguration nicht genug Schutz vor E-Mail-Bedrohungen bieten würde, die wir an Schulen erwarteten. Wir hatten keinen Überblick über die Bedrohungen in den jeweiligen Mandantenumgebungen, gleichzeitig war uns jedoch bewusst, dass Anwender kompromittiert wurden. Beispielsweise wurden Postfächer missbraucht, um Phishing-Kampagnen und Angriffe gegen andere Schulen sowie gegen die allgemeine Bevölkerung zu führen. Wir waren also ziemlich sicher, dass etwas im Argen lag, hatten jedoch keine konkreten Daten.“

Das Bildungsministerium wollte eine zentralisierte Lösung bereitstellen, mit der Schulen ihre E-Mails filtern konnten. Das würde nicht nur die Risiken erheblich verringern, sondern der Behörde auch einen besseren Überblick über die auftretenden Bedrohungen geben.

„Wir wollten eine Statistik zu den Aktivitäten und zum Angriffsaufkommen, um Schulen besser zu Abwehrmaßnahmen beraten zu können“, so Hood. „Dazu benötigten wir ein Tool, das einerseits differenziert und gleichzeitig kollektiv arbeitet und zudem tausende unterschiedliche Mandanten unterstützt.“

„Proofpoint Email Protection hat sich beim Blockieren schädlicher E-Mails als sehr effektiv erwiesen. Die Lösung zeigt uns die Art der Angriffe und gibt uns die Sicherheit, dass unsere Schulen gut davor geschützt sind.“

Andrew Hood, Chief Advisor of Cybersecurity, Bildungsministerium von Neuseeland

Die Lösung

Eine zentralisierte und flexible Lösung für Schulen

Im Rahmen des Beschaffungsprozesses führte das Bildungsministerium eine umfassende Marktanalyse durch, um die beste Lösung für Schulen zu finden. Nach Berücksichtigung von Faktoren wie Kompatibilität mit den Google- und Microsoft-Produktivitätstools, die in den Schulen eingesetzt wurden, sowie Kosten und Performance entschied sich das Ministerium für Proofpoint Email Protection.

„Bei unserer Marktanalyse erwies sich Proofpoint als Gewinner“, betont Hood. „Für die Implementierung der Lösung in Schulen arbeiten wir mit dem staatlichen Unternehmen Network for Learning (N4L) zusammen, das im Auftrag des Bildungsministeriums digitale Dienstleistungen für die Schulen unseres Landes bereitstellt. N4L installiert die Proofpoint-Software in den Schulen und agiert als Ansprechpartner für die Service-Funktionen.“

Mit Proofpoint Email Protection können Schulen alle eingehenden E-Mails mithilfe mehrschichtiger Erkennungstechniken absichern und kontrollieren, sodass schädliche E-Mails erkannt und blockiert werden. Die Lösung kann auch die neuesten Bedrohungen und Massenmailings dynamisch klassifizieren. Die Bereitstellung der Lösung durch N4L war ein kosteneffizienter und unkomplizierter Ansatz, mit dem eine Vielzahl von Schulen schnell geschützt werden konnte.

„Bei etwa 2.500 Schulen stellt N4L bereits Services wie Netzwerke und Firewalls bereit, sodass wir Proofpoint als einen ergänzenden Service konzipierten“, sagt Hood. „Schuldirektoren haben bereits ein umfangreiches Aufgabenpensum. Ihnen sollte nicht auch noch die E-Mail-Sicherheit aufgebürdet werden. Wir informierten sie darüber, dass wir diese Aufgabe übernehmen und zentralisieren können.“

Die Zusammenarbeit von Proofpoint und N4L bei der Bereitstellung verlief absolut reibungslos und das Bildungsministerium arbeitete eng mit dem Unternehmen zusammen, um Schulen bei der Anpassung für ihre individuellen Umgebungen und Produktivitätsanwendungen zu unterstützen. Die Schulen können sich jederzeit für Proofpoint Email Protection registrieren, dessen Hauptzweck bei der klassischen E-Mail-Filterung liegt, also der Erkennung und Blockierung gefährlicher Bedrohungen, die per E-Mail eingehen.

Proofpoint Targeted Attack Protection (TAP) spielt als Teil der Lösung ebenfalls eine wichtige Rolle. Die Komponente schützt vor Business Email Compromise (BEC), schädlichen Anhängen sowie Cloud-basierten Bedrohungen und bietet einen Überblick über deren Ziele, sodass das Ministerium strategisch planen kann.

„Eine unserer Herausforderungen war, dass Schulen ihre Mandantenumgebungen eigenständig verwalten können und wir somit keinen Einblick in die spezifischen Google- und Microsoft-Konfigurationen der einzelnen Standorte hatten“, so Hood. „Um einen zuverlässigen Service zu wählen, mussten wir daher verschiedene Szenarien darauf testen, was die Schulen wahrscheinlich benötigen würden. Für N4L bedeutete das eine enorme Anzahl zusätzlicher Variantentests, was mehrere Monate in Anspruch nahm. Nachdem diese Tests abgeschlossen waren, konnten wir den Service bei einigen Schulen im Pilotbetrieb einführen, um anschließend die breite Implementierung mit vollem Tempo zu starten. Innerhalb von neun Monaten hatten sich bereits 60 % der Schulen für den Service registriert.“

Die Ergebnisse

Besserer Schutz und umfangreicher Überblick

Da immer mehr Schulen Proofpoint Email Protection implementieren, verfügt das Bildungsministerium über zuverlässige Informationen über die Anzahl und Arten der Bedrohungen, die die Schulen ins Visier nehmen – und kann sie proaktiv stoppen, bevor sie Schüler und Lehrkräfte erreichen.

„Anhand der Zahlen sehen wir, wie wichtig Proofpoint ist“, betont Hood. „Jeden Monat durchlaufen 80–100 Millionen E-Mails die Plattform. Die meisten werden als unwichtiger Spam blockiert, doch bei einer beunruhigenden Zahl von 80.000 bis 100.000 Nachrichten handelt es sich um Bedrohungen, die in der Proofpoint-Sandbox auffallen. Hier finden wir schädliche URLs und Inhalte, die umfassendere Scans erfordern, und hier spielt Proofpoint seine Stärken aus. Der größte Erfolg war dabei, dass wir nun über konkrete Zahlen zu jeder blockierten Bedrohung verfügten, die kein Postfach erreichte und keinen Anwender zum Klicken verleiten konnte.“

Proofpoint Email Protection schützt neuseeländische Schulen mit stärkerer E-Mail-Sicherheit. „Wir haben keine negativen Rückmeldungen von Lehrkräften und Mitarbeitern zu Verzögerungen oder Geschwindigkeitsproblemen erhalten“, berichtet Hood.

Proofpoint blockiert nicht nur Bedrohungen sofort bei ihrem Auftauchen, sondern unterstützt das Bildungsministerium und die Schulen zudem beim Wechsel zu einem proaktiveren Sicherheitsansatz.

„N4L überwacht die Plattform und arbeitet eng mit Proofpoint an der API-Integration. Dadurch können wir die Proofpoint-Protokolle in unserem eigenen SOC (Security Operations Center) verarbeiten“, freut sich Hood. „Dabei sucht N4L nach ungewöhnlichen Verhaltensweisen und Mustern, z. B. plötzlichen Aktivitätsspitzen bei bestimmten Angriffstypen. Diese Informationen zeigen uns, ob eine Schule mit einer potenziell schädlichen E-Mail interagiert. In diesem Fall können wir die entsprechende Schule proaktiv kontaktieren und darauf hinweisen, dass sie gerade etwas tun, das wahrscheinlich sehr gefährlich ist, und dass sie dringend Maßnahmen ergreifen sollten.“

Mit der zentralisierten Lösung konnte das Bildungsministerium Lehrkräfte und Mitarbeiter entlasten, damit diese sich auf den Lehrbetrieb statt auf Cybersicherheit konzentrieren können.

Der von Proofpoint Targeted Attack Protection erstellte Proofpoint Attack Index hilft dem Bildungsministerium bei der Identifizierung der am häufigsten angegriffenen Personen (Very Attacked People™, VAPs), sodass diese proaktiv vor Gefahren gewarnt werden können.

„Mit einem Blick auf die VAP-Liste können wir die angegriffenen Personen mit öffentlichen Quellen von E-Mail-Adressen für Schulen korrelieren und erhalten Einblicke in das Angreiferverhalten“, so Hood.

„Proofpoint bietet uns eine kostengünstige Möglichkeit zur E-Mail-Filterung, die den Schulen diese Arbeit abnimmt“, ist Hood begeistert. „Die einzelnen Bildungseinrichtungen müssen sich nicht um die Konfiguration und ihre ständige Aktualisierung kümmern oder sich Sorgen über die neuesten Bedrohungen machen. Sie können darauf vertrauen, dass es eine Lösung gibt, die sie zuverlässig schützt.“

MEHR ERFAHREN

Weitere Informationen finden Sie unter **proofpoint.com.de**.