

Il Ministero dell'Istruzione della Nuova Zelanda protegge migliaia di istituti scolastici con Proofpoint



MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

La sfida

- Proteggere gli studenti e i docenti dalle minacce email
- Rispondere alle esigenze dei singoli istituti scolastici mantenendo un approccio standardizzato
- Offrire agli istituti scolastici una soluzione di sicurezza dell'email a un prezzo contenuto

La soluzione

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection

I risultati

- Riduzione delle minacce avanzate grazie a una protezione aggiornata dell'email
- Sicurezza più proattiva grazie a una miglior visibilità sulle email
- Integrazione senza problemi con diversi ambienti

L'ente

Come proteggere un sistema scolastico nazionale con più di 900.000 tra studenti e membri del personale? Per il Ministero dell'Istruzione della Nuova Zelanda la risposta parte dalla protezione delle comunicazioni via email. L'ente è il principale consulente del governo in merito al sistema educativo nazionale. Stabilisce l'orientamento delle agenzie e dei fornitori per aiutare il governo a raggiungere i suoi obiettivi in termini di istruzione.

La sfida

Proteggere le comunicazioni degli studenti e dei docenti a livello nazionale

In Nuova Zelanda, le scuole primarie e secondarie e le Kura Kaupapa Māori (scuole pubbliche in cui vengono insegnate la cultura e i valori Maori) devono continuamente bilanciare le esigenze locali con gli standard nazionali. Gli istituti scolastici in Nuova Zelanda hanno il proprio consiglio scolastico, che viene eletto a livello locale e definisce la maggior parte delle regole e delle modalità operative delle scuole. Le minacce email moderne possono facilmente andare oltre i confini geografici, e il Ministero dell'Istruzione della Nuova Zelanda si è reso conto di dover offrire un'opzione standardizzata per proteggere gli studenti, i docenti e il personale.

“Qualche anno fa, uno dei consigli sanitari distrettuali ha subito un incidente di sicurezza informatica piuttosto importante” ha spiegato Andrew Hood, Chief Advisor of Cybersecurity del Ministero dell'Istruzione della Nuova Zelanda. “Perciò ci è stato chiesto come potessimo migliorare il livello di sicurezza informatica degli istituti scolastici nel nostro Paese”.

Gli istituti scolastici della Nuova Zelanda hanno la libertà di scegliere i propri strumenti di produttività per l'ufficio e generalmente optano per Google con Workspace Plus o Microsoft 365, o una combinazione dei due. Il Ministero dell'Istruzione paga le licenze, mentre gli istituti configurano i tenant.

“Abbiamo circa 3.500 tenant Google e Microsoft diversi ripartiti nei nostri istituti”, ha precisato Hood. “Temevamo che la loro configurazione di default non fosse sufficiente a proteggerli dal tipo di minacce email che pensavamo li stessero prendendo di mira. Non avevamo alcun modo di stabilire quali minacce colpivano i nostri tenant, ma vedevamo che alcuni utenti venivano compromessi. Per esempio, sappiamo che delle caselle email sono state utilizzate per lanciare attacchi e campagne di phishing contro altri istituti scolastici e la comunità in generale. Eravamo perciò piuttosto sicuri che stesse accadendo qualcosa, ma non avevamo alcuna visibilità sulle minacce”.

Il Ministero dell'Istruzione desiderava offrire una soluzione centralizzata che permettesse agli istituti scolastici di filtrare le email. Non solo questa soluzione eliminerebbe un rischio importante per gli istituti scolastici, ma fornirebbe all'ente una migliore visibilità sulle minacce.

“Volevamo essere in grado di vedere statisticamente cosa accadeva e il volume degli attacchi sferrati, per consigliare meglio gli istituti scolastici su come proteggersi da queste minacce”, ha aggiunto Hood. “Avevamo bisogno di uno strumento che potesse funzionare in modo separato ma collettivo e con migliaia di tenant diversi”.

“Proofpoint Email Protection ha bloccato in modo molto efficace le email dannose. Ci permette di visualizzare i tipi di attacchi e sapere che i nostri istituti scolastici sono protetti”.

Andrew Hood, Chief Advisor of Cybersecurity, Ministero dell'Istruzione della Nuova Zelanda

La soluzione

Una soluzione centralizzata ma flessibile per gli istituti scolastici

Come parte di questo processo di procurement, il Ministero dell'Istruzione ha condotto un'approfondita valutazione di mercato per scegliere la miglior soluzione per i suoi istituti. Dopo aver preso in considerazione fattori come la compatibilità con gli strumenti di produttività Google e Microsoft utilizzati dagli istituti, i costi e le prestazioni, ha scelto Proofpoint Email Protection.

“Abbiamo condotto una valutazione di mercato e Proofpoint ne è uscita vincente” spiega Hood. “Per implementare la soluzione negli istituti, lavoriamo con l'azienda Network for Learning (N4L), un'azienda statale finanziata dal Ministero dell'Istruzione per fornire servizi digitali agli istituti scolastici della Nuova Zelanda. N4L li implementa negli istituti e agisce come punto di contatto per la capacità di servizio”.

Proofpoint Email Protection aiuta gli istituti scolastici a proteggere e controllare le loro email in arrivo, utilizzando tecniche di rilevamento multilivello per identificare e bloccare i messaggi dannosi. Inoltre, offre una classificazione dinamica delle minacce e problematiche più recenti. La distribuzione della soluzione tramite N4L si è rivelato un approccio economico e pratico per proteggere un grande numero di istituti scolastici, rapidamente.

“Circa 2.500 istituti hanno già instaurato una relazione con N4L per servizi come il networking e i firewall e Proofpoint completa tale approccio” ha commentato Hood. “I presidi degli istituti hanno già numerosi problemi da gestire. La sicurezza dell'email non dovrebbe essere uno di questi. Facciamo sapere loro che possiamo centralizzare tutto e farcene carico per loro conto”.

L'implementazione in collaborazione con Proofpoint e N4L è stata estremamente fluida, e il Ministero dell'Istruzione ha lavorato a stretto contatto con l'azienda per permettere agli istituti scolastici di supportare facilmente le loro applicazioni di produttività e i loro ambienti specifici. Gli istituti scolastici possono registrarsi in qualsiasi momento per utilizzare Proofpoint Email Protection, che offre un filtraggio classico delle email, rimuovendo e bloccando le minacce ad alto rischio che arrivano via email.

Proofpoint Targeted Attack Protection (TAP) gioca un ruolo altrettanto importante come parte della soluzione. Previene le violazioni dell'email aziendale (BEC, Business Email Compromise), le minacce cloud e basate sugli allegati, fornendo informazioni e visibilità sulle vittime, per aiutare il Ministero a pianificare in modo più strategico.

“Poiché gli istituti possono gestire i loro tenant, noi non sapevamo quale sarebbe stata la configurazione Google e Microsoft esistente di ogni sito specifico” ha sottolineato Hood. “Dovevamo testare diverse circostanze in base a ciò che ritenevamo dovessero fare gli istituti scolastici per essere certi di disporre di un servizio affidabile. Per questo motivo N4L ha dovuto condurre numerosi test di variazioni. Ciò ha richiesto qualche mese, alla fine dei quali abbiamo iniziato a lanciare una versione pilota del servizio in alcuni istituti. Abbiamo quindi avviato un processo di accelerazione. In soli nove mesi, il 60% degli istituti erano iscritti al servizio”.

I risultati

Maggior protezione e visibilità

Man mano che un numero crescente di istituti scolastici adotta Proofpoint Email Protection, il Ministero dell'Istruzione acquisisce una visibilità approfondita sul volume e i tipi di minacce che gli istituti devono affrontare, bloccandole proattivamente prima che possano raggiungere gli studenti o il personale.

“I numeri ci confermano il valore aggiunto offerto da Proofpoint” ha commentato Hood. “Generalmente analizziamo da 80 a 100 milioni di messaggi al mese grazie alla piattaforma. La maggior parte viene bloccata perché considerata come spam di basso livello, ma un allarmante numero di messaggi (tra 80.000 e 100.000) sono minacce che estraiamo dalle camere di detonazione di Proofpoint. Il rilevamento di alcuni URL dannosi e certi contenuti pericolosi richiede un'analisi più avanzata, ed è proprio ciò che fa Proofpoint.

Il principale vantaggio è la possibilità di dimostrare ogni volta che una minaccia è stata bloccata e non ha raggiunto la casella email né indotto un utente a fare clic”.

Proofpoint Email Protection protegge gli istituti scolastici della Nuova Zelanda grazie a una sicurezza dell'email più efficace. “Né i docenti né il personale hanno segnalato ritardi o problemi di prestazioni” ha affermato Hood.

Proofpoint non solo blocca le minacce nel momento in cui si manifestano, ma permette al Ministero dell'Istruzione e agli istituti sotto la sua responsabilità di adottare un livello di sicurezza più proattivo.

“N4L si è fatta carico del monitoraggio della piattaforma e ha lavorato con Proofpoint per l'integrazione delle API. Possono anche integrare i log di Proofpoint all'interno del loro SOC” ha aggiunto Hood. “Vanno alla ricerca di comportamenti e modelli insoliti, come picchi improvvisi del volume di alcuni tipi di attacchi. Queste informazioni ci consentono anche di stabilire se un istituto ha interagito con un'email potenzialmente dannosa. Possiamo comunicare proattivamente all'istituto che pensiamo abbiano effettuato un'azione a alto rischio e che è necessario intervenire”.

Grazie alla sua soluzione centralizzata, il Ministero dell'Istruzione ha permesso a docenti e amministratori di concentrarsi di più sull'insegnamento invece che sulla sicurezza informatica.

Proofpoint Attack Index, fornito da TAP, facilita anche l'identificazione dei VAP (Very Attacked People™) ovvero le persone più attaccate) per aiutare il Ministero a identificare i principali obiettivi e tenerli informati sulle minacce.

“La possibilità di consultare l'elenco dei VAP e correlare le persone attaccate con le fonti pubbliche di indirizzi email per gli stabilimenti scolastici ci offre informazioni sul comportamento dei criminali informatici” ha dichiarato Hood.

“Proofpoint ci offre una soluzione di filtraggio delle email più economica, eliminando tale responsabilità dall'istituto scolastico” ha commentato Hood. “Gli istituti scolastici non devono preoccuparsi della configurazione né degli aggiornamenti della soluzione né delle minacce più recenti. Sanno che c'è una soluzione in essere che li protegge e che è molto efficace”.

PER SAPERNE DI PIÙ

Per maggiori informazioni visita il sito proofpoint.com/it.

INFORMAZIONI SU PROOFPOINT

Proofpoint è un'azienda leader nella cybersecurity e nella conformità, che protegge dai rischi il patrimonio più importante di un'azienda: le persone. Con una suite integrata di soluzioni basate su cloud, Proofpoint aiuta le aziende di tutto il mondo a bloccare le minacce mirate, a salvaguardare i propri dati e a proteggere gli utenti dagli attacchi IT. Aziende di ogni dimensione, tra cui l'85% delle Fortune 100, si affidano alle soluzioni di sicurezza e di conformità incentrate sulle persone di Proofpoint per mitigare i rischi di sicurezza veicolati via email, cloud, social media e web. Per ulteriori informazioni: www.proofpoint.com/it.

©Proofpoint, Inc. Proofpoint è un marchio commerciale di Proofpoint, Inc. negli Stati Uniti e negli altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.