CASO CLIENTE

proofpoint

UNA UNIVERSITÀ STORICA ADOTTA UN APPROCCIO PROATTIVO ALLA SICUREZZA INFORMATICA

LA SFIDA

- Bloccare attacchi ransomware, spam e phishing evitando che raggiungano le caselle di posta degli utenti
- Migliorare il punteggio di reputazione dell'email dell'università
- Accrescere la giusta percezione della situazione
- Recuperare il tempo impiegato per porre rimedio all'impatto delle minacce informatiche per dedicarlo a progetti più proattivi

LA SOLUZIONE

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection e integrazione con Palo Alto Networks Wildfire

I RISULTATI

- Bloccati da 300.000 a 500.000 elementi di ransomware alla settimana
- Riduzione significativa delle email di phishing e dei relativi clic
- Diminuita violazione degli account da 200 al mese a meno di 12
- Raggiunta visibilità dettagliata su minacce, impatto e tendenze

Come può una storica università con più di 16.000 studenti e studiosi, oltre 4.000 membri di facoltà e un'ampia gamma di programmi, dipartimenti e organizzazioni affiliate proteggere la propria attività? Adottando un approccio proattivo alla sicurezza informatica e alle minacce che la colpiscono.

Quando un responsabile della sicurezza delle informazioni dell'ente scolastico è arrivato nel 2011, ha capito di aver bisogno di un gateway email di livello enterprise. Si è rivolto a Gartner per un consiglio. Quando ha visto la recensione di Gartner relativa a Proofpoint e ricevuto maggiori informazioni, tra cui referenze di clienti ragguardevoli, ha scelto Proofpoint Email Protection.

COMPLEMENTARE AL CLOUD

L'università stava anche effettuando la migrazione di alcuni dei suoi sistemi nel cloud. Aveva spostato il suo sistema di posta elettronica passando a Microsoft Office 365 per ridurre i costi, i requisiti di supporto e l'impronta del data center associati ai server Exchange. Proofpoint Email Protection si posiziona dietro la soluzione Palo Alto Networks Wildfire dell'università e davanti a Office 365. Tale collocazione offre al team di sicurezza una maggiore difesa dell'email e una migliore percezione della situazione.

"Il cambiamento è stato notevole", ha affermato il responsabile della sicurezza delle informazioni. Lo spam è scomparso quando l'ateneo ha messo a punto i filtri di identificazione dello spam. Quindi ha attivato la protezione in uscita per eliminare i problemi persistenti del punteggio di reputazione.

"Ha fatto un'enorme differenza", ha affermato.

COLPIRE I PHISHER

Con la protezione dell'email in uscita, il team di sicurezza si è concentrato sulla riduzione degli attacchi di phishing e dei relativi effetti. Fino ad allora, le email di phishing avevano portato a oltre 200 account compromessi al mese. Il responsabile della sicurezza delle informazioni ha fatto pressione per usare Proofpoint Targeted Attack Protection (TAP); la sua richiesta è stata approvata rapidamente. L'università ha integrato TAP con Palo Alto Networks WildFire utilizzando un'attivazione basata su una semplice chiave API. Combinando le due soluzioni, l'analisi del malware basata su cloud di entrambe le aziende è in grado di allineare automaticamente la protezione tra il gateway email di Proofpoint e il firewall di Palo Alto Networks.

Immediatamente, TAP ha ridotto le violazione degli account da 200 al mese a meno di 12. Per le poche email di phishing che riescono a passare, l'ateneo ha aperto un ticket di supporto con Proofpoint in modo che l'email venga documentata e aggiunta alla protezione TAP a beneficio di tutti.

"Se qualcuno si lamenta di aver ricevuto un'email di phishing, posso mostrargli i calcoli", ha affermato il responsabile della sicurezza informatica. "Come esempio, abbiamo osservato 200.000 tentativi di phishing questo mese, e solo 21 sono riusciti a passare".

“Proofpoint ci aiuta a tenere il ransomware alla larga dai nostri sistemi. Siamo soddisfatti della quantità di ransomware da cui Proofpoint ci protegge con efficacia”.

Responsabile della sicurezza delle informazioni, storica Università

BLOCCARE IL RANSOMWARE

A partire dal 2016, l’ateneo ha osservato un’impennata degli attacchi ransomware. Il team della sicurezza osserva da 300.000 a 500.000 elementi di ransomware alla settimana che cercano di entrare nella rete dell’università. In un periodo di soli 7 giorni a metà 2016, ne ha ricevuti quasi 500.000. Proofpoint mette immediatamente in quarantena l’email sospetta, ne effettua il sandboxing e quindi stabilisce se è dannosa.

“Proofpoint ci aiuta a tenere il ransomware alla larga dai nostri sistemi”, ha commentato il responsabile della sicurezza delle informazioni. “Siamo soddisfatti della quantità di Ransomware da cui Proofpoint ci protegge con efficacia”.

VISIBILITÀ PER UN’AZIONE EFFICACE

In passato, quando si verificava un attacco di phishing, il team addetto alla sicurezza girava per tutta l’università a chiedere se qualcuno avesse effettivamente fatto clic sull'email. Era difficile valutare con precisione l'impatto di una determinata email.

Le funzionalità di reporting di Proofpoint offrono al team visibilità immediata con dati dettagliati per una risposta rapida. Ora se arriva un'email di phishing, il team sa esattamente chi e quanti l’hanno ricevuta. Possono contattare chiunque sia stato colpito o bloccare i loro account per sicurezza. Proofpoint consente al team di controllare l'impatto del phishing, reagire immediatamente esattamente nel posto giusto ed evitare sprechi di tempo e comunicazioni. Gli account violati sono ora una rara eccezione. Questo cambiamento ha permesso al team di sicurezza di lavorare su progetti di sicurezza più avanzati.

"Proofpoint è tattico e preciso", ha affermato il responsabile della sicurezza delle informazioni. "Ha reso la risposta agli incidenti un evento gestibile. Mi sento molto a mio agio nell’utilizzare la tecnologia. Per me è semplice navigare, trovare esattamente ciò che cerco, generare report e studiare le tendenze nel tempo”.

L’IMPATTO SUL FUTURO

Sebbene il team di sicurezza protegga l'università 24 ore al giorno, il crescente volume e la varietà di minacce rappresentano ancora una preoccupazione enorme. E stanno anche attaccando altri istituti di istruzione superiore, aziende e forze dell'ordine.

"A volte le persone ritengono che i problemi di sicurezza siano sovradimensionati", ha affermato il responsabile della sicurezza delle informazioni. “Ma a volte si sviluppano condizioni che sono gravi e che hanno un forte impatto. Dobbiamo rispondere. Non possiamo semplicemente rimanere seduti finché qualcuno non capirà perché queste forze vogliono attaccarci. Dobbiamo approntare delle difese e proteggere l’attività dell'università. Proofpoint ci aiuta in tal senso”.

Il responsabile della sicurezza delle informazioni odia vedere i malintenzionati attaccare le istituzioni che fanno un ottimo lavoro a vantaggio della società. Sente la responsabilità di condividere ciò che ha appreso, in modo che, insieme, gli istituti di istruzione superiore possano collaborare per combattere in modo più efficace le minacce informatiche. Incoraggia i suoi colleghi presso altre istituzioni a valutare Proofpoint perché sa in prima persona quanto sia efficace.