proofpoint

UNE UNIVERSITÉ AU PASSÉ LÉGENDAIRE ADOPTE UNE APPROCHE PROACTIVE DE LA CYBERSÉCURITÉ

DÉFI

- Empêcher le spam et les attaques par phishing et par ransomware d'atteindre les boîtes de réception des utilisateurs
- Améliorer la réputation des domaines et interfaces publiques de la messagerie de l'université
- Améliorer la connaissance sur le niveau de sécurité
- Réallouer à des projets plus proactifs le temps autrefois consacré à la réponse aux incidents

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection et intégration avec Palo Alto Networks WildFire

RÉSULTATS

- Blocage de 300 000 à 500 000 ransomwares par semaine
- Réduction significative du nombre d'e-mails de phishing et de clics
- Réduction du nombre de comptes compromis de 200 à moins de 12 par mois
- Visibilité détaillée sur les menaces, leur impact et les tendances

Comment une université historique comptant plus de 16 000 étudiants et chercheurs, plus de 4 000 enseignants et un large éventail de programmes, de départements et d'organismes affiliés peut-elle protéger ses activités ? En adoptant une approche proactive de la cybersécurité et des menaces auxquelles elle est exposée.

Lorsque le responsable de la sécurité des systèmes d'information de la faculté est arrivé sur le campus en 2011, il s'est rendu compte qu'elle avait besoin d'une passerelle de messagerie d'entreprise. Il s'est alors adressé à Gartner pour obtenir des conseils. Après avoir lu l'évaluation de Proofpoint dressée par Gartner et s'être renseigné davantage, notamment sur les références clients impressionnantes, son choix s'est porté sur Proofpoint Email Protection.

UN COMPLÉMENT AU CLOUD

À l'époque, l'université avait également entamé la migration de certains de ses systèmes vers le cloud. Elle avait transféré son système de messagerie vers Microsoft Office 365 afin de réduire les coûts, les besoins en matière de support et les ressources serveurs consommées par Exchange dans leur datacentre. Proofpoint Email Protection est déployé derrière la solution Palo Alto Networks WildFire et devant Office 365. Cette configuration assure à l'équipe de sécurité une bien meilleure protection de la messagerie et une connaissance sur les menaces hors pair.

« Le changement a été spectaculaire », affirme le RSSI. Le spam a disparu à mesure que la faculté affinait les filtres d'identification du spam. L'équipe de sécurité a ensuite activé la protection des e-mails sortants pour éliminer de manière définitive la réputation de leurs interfaces IP publiques.

« Cela a tout changé », a-t-il déclaré.

CIBLAGE DES ATTAQUES PAR PHISHING

Une fois la protection des e-mails sortants en place, l'équipe de sécurité s'est concentrée sur la réduction des attaques par phishing et de leurs conséquences. À l'époque, plus de 200 comptes étaient compromis chaque mois au moyen d'e-mails de phishing. Le RSSI a plaidé pour le déploiement de Proofpoint Targeted Attack Protection (TAP) et a vu sa demande approuvée rapidement. L'université a intégré TAP avec la solution Palo Alto Networks WildFire au moyen d'une API simple activée par une clé. En combinant les deux solutions, les fonctionnalités d'analyse des malwares dans le cloud des deux entreprises peuvent aligner automatiquement la protection sur la passerelle de messagerie de Proofpoint et le pare-feu de Palo Alto Networks.

Suite au déploiement de TAP, le nombre de comptes compromis est immédiatement tombé de 200 par mois à moins de 12. Pour les quelques e-mails de phishing qui parviennent à passer, la faculté a ouvert un ticket de support auprès de Proofpoint afin que les e-mails soient documentés et ajoutés à la protection TAP dans l'intérêt de tous.

« Si quelqu'un se plaint d'avoir reçu un e-mail de phishing, je peux lui montrer les chiffres », explique le RSSI. « À titre d'exemple, nous avons recensé 200 000 tentatives de phishing ce mois-ci, et seuls 21 e-mails ont réussi à passer ».

« Proofpoint est très utile, car il bloque l'accès des ransomwares à notre environnement système. Nous sommes enchantés de l'efficacité de la protection de Proofpoint contre les ransomwares. »

Responsable de la sécurité des systèmes d'information, Université au passé légendaire

NEUTRALISATION DES RANSOMWARES

Depuis 2016, l'équipe de sécurité de la faculté a constaté une augmentation considérable des attaques par ransomware. Chaque semaine, 300 000 à 500 000 ransomwares tentent d'infiltrer son réseau. Mi-2016, l'équipe a recensé près de 500 000 tentatives d'attaques par ransomware sur une période de sept jours seulement. Proofpoint met instantanément en quarantaine les e-mails suspects, les analyse dans un environnement sandbox et détermine s'ils sont malveillants.

« Proofpoint est très utile, car il bloque l'accès des ransomwares à notre environnement système », affirme le RSSI. « Nous sommes enchantés de l'efficacité de la protection de Proofpoint contre les ransomwares. »

VISIBILITÉ POUR UNE ACTION EFFICACE

Auparavant, lorsqu'une attaque par phishing se produisait, l'équipe de sécurité se disséminait dans toute la faculté pour demander si quelqu'un avait cliqué sur l'e-mail. Il était extrêmement difficile de mesurer avec précision l'impact d'un e-mail donné.

Les fonctions de génération de rapports de Proofpoint offrent à l'équipe une visibilité instantanée et des données détaillées pour une réponse rapide. Aujourd'hui, si un e-mail de phishing parvient à se frayer un chemin jusqu'à la boîte de réception, l'équipe sait exactement qui et combien de personnes l'ont reçu. Elle peut contacter les personnes concernées ou verrouiller leurs comptes par mesure de sécurité. Proofpoint permet à l'équipe de contrôler l'impact du phishing, d'intervenir immédiatement au bon endroit et d'éviter les pertes de temps et les communications inutiles. Les comptes compromis constituent désormais une exception. Cette évolution a permis à l'équipe de sécurité de se consacrer à des tâches de sécurité plus avancée.

« Proofpoint est tactique et précis », affirme le RSSI. « Il simplifie considérablement l'intervention sur incident. Je suis très à l'aise avec leur outil. Je peux facilement m'orienter, trouver exactement ce que je cherche, générer des rapports et étudier l'évolution des tendances au fil du temps. »

IMPACT SUR L'AVENIR

Bien que l'équipe de sécurité protège l'université 24 heures sur 24, le volume croissant et la diversité des menaces continuent de susciter de vives inquiétudes. D'autant qu'elles ciblent également d'autres établissements d'enseignement supérieur, les entreprises et les forces de l'ordre.

« Parfois, les gens considèrent que les risques de sécurité sont surestimés », explique le RSSI. « Mais il arrive que des problèmes sérieux surviennent et leurs conséquences peuvent être graves. Nous devons agir. Nous ne pouvons pas rester les bras croisés en attendant que quelqu'un découvre pourquoi ces forces malveillantes veulent nous attaquer. Nous devons mettre en place des défenses et protéger la mission de l'université. Proofpoint nous y aide. »

Le RSSI déteste voir des acteurs malveillants s'attaquer à des institutions qui réalisent un travail utile et honorable qui profite à la société. Il estime qu'il est de son devoir de partager ce qu'il a appris, afin que les établissements d'enseignement supérieur puissent s'unir pour lutter plus efficacement contre les cybermenaces. Il encourage ses collègues d'autres établissements à examiner la technologie Proofpoint de plus près parce qu'il sait d'expérience combien elle est efficace.