proofpoint.

TÉMOIGNAGE CLIENT

Le ministère de l'Éducation néo-zélandais protège des milliers d'établissements scolaires avec Proofpoint

MINISTRY OF EDUCATION
TE TĀHUHU O TE MĀTAURANGA

Le défi

- Protéger les élèves et les professeurs contre les menaces email
- Répondre aux besoins de chaque établissement scolaire tout en conservant une approche standardisée
- Proposer aux établissements scolaires une solution de protection de la messagerie à prix réduit

La solution

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection

Les résultats

- Réduction des menaces avancées grâce à une protection constamment actualisée de la messagerie
- Sécurité plus proactive grâce à une visibilité améliorée sur les emails
- Intégration fluide dans divers environnements

L'organisation

Comment protéger un système éducatif national comprenant plus de 900 000 élèves et membres du personnel ? Pour le ministère de l'Éducation néo-zélandais, cela commence par la protection des communications par email. L'organisation est le principal conseiller du gouvernement en ce qui concerne le système éducatif du pays. Elle définit les orientations pour les agences et les prestataires afin d'aider le gouvernement à atteindre ses objectifs en matière d'éducation.

Le défi

Protéger les communications des élèves et des professeurs dans l'ensemble du pays
En Nouvelle-Zélande, les établissements primaires et secondaires et les Kura Kaupapa Māori (écoles publiques où sont enseignées les cultures et les valeurs maories) doivent constamment trouver un équilibre entre les besoins locaux et les standards nationaux. Les établissements scolaires néo-zélandais ont leur propre conseil scolaire, qui est élu localement et qui définit la plupart des règles et des modes de fonctionnement des établissements. Les menaces email modernes peuvent toutefois facilement s'étendre au-delà des limites géographiques, et le ministère de l'Éducation néo-zélandais s'est rendu compte qu'il devait proposer une solution standardisée pour protéger ses élèves, ses professeurs et son personnel.

« Il y a quelques années, l'un des conseils de santé de district néo-zélandais a été victime d'un incident de cybersécurité relativement important », explique Andrew Hood, conseiller principal en cybersécurité au sein du ministère de l'Éducation néo-zélandais. « On nous a donc demandé ce que nous pouvions faire pour améliorer la maturité de la cybersécurité des établissements scolaires néo-zélandais. »

Les établissements scolaires néo-zélandais ont la liberté de choisir leurs outils de productivité de bureau et optent généralement pour Google en association avec Workspace Plus ou Microsoft 365, ou une combinaison des deux. Le ministère de l'Éducation paie les licences, tandis que les établissements configurent les locations.

« Environ 3 500 locations Google et Microsoft différentes sont réparties entre nos établissements », précise M. Hood. « Nous craignions que leur configuration par défaut ne suffise pas à les protéger contre le type de menaces email par lequel nous pensions qu'ils étaient visés. Nous n'avions aucun moyen de déterminer quelles menaces ciblaient nos locations, mais nous constations que des utilisateurs étaient compromis.

Par exemple, nous savions que des boîtes email étaient utilisées pour lancer des attaques et des campagnes de phishing contre d'autres établissements et contre la communauté plus large. Nous étions donc convaincus que quelque chose se tramait, mais nous n'avions aucune visibilité sur les menaces. »

Le ministère de l'Éducation souhaitait proposer une solution centralisée permettant aux établissements de filtrer leurs emails. Non seulement cette solution éliminerait un risque majeur pour les établissements, mais elle offrirait également à l'organisation une meilleure visibilité sur les menaces.

« Nous souhaitions pouvoir visualiser statistiquement ce qui se passait et le volume d'attaques lancées, afin de mieux conseiller les établissements sur les défenses à mettre en place contre ces menaces », ajoute Andrew Hood. « Nous avions besoin d'un outil qui puisse fonctionner de manière isolée mais collective, et qui prendrait également en charge des milliers de locations différentes. »

« Proofpoint Email Protection est très efficace pour bloquer les emails malveillants. Il nous permet de visualiser les types d'attaques et de savoir que nos établissements scolaires sont protégés contre ceux-ci. »

Andrew Hood, conseiller principal en cybersécurité, Ministère de l'Éducation néo-zélandais

La solution

Une solution centralisée mais flexible pour les établissements scolaires

Dans le cadre de sa procédure de passation de marchés, le ministère de l'Éducation a procédé à une étude approfondie du marché afin de choisir la meilleure solution pour ses établissements. Après avoir pris en compte des facteurs tels que les coûts, les performances et la compatibilité avec les outils de productivité Google et Microsoft utilisés par les établissements, il a opté pour Proofpoint Email Protection.

« Nous avons réalisé une étude du marché et Proofpoint en est ressorti gagnant », explique M. Hood. « Pour déployer la solution dans les établissements, nous travaillons avec Network for Learning (N4L), une entreprise appartenant à l'État et financée par le ministère de l'Éducation pour fournir des services numériques aux établissements scolaires néo-zélandais. N4L déploie la solution dans les établissements et est leur interlocuteur pour la capacité de service. »

Proofpoint Email Protection aide les établissements scolaires à sécuriser et à contrôler leurs emails entrants grâce à des techniques de détection multicouches afin d'identifier et de bloquer les messages malveillants. Il propose également une classification dynamique des menaces et nuisances les plus récentes. La distribution de la solution via N4L constituait une approche économique et pratique pour protéger un grand nombre d'établissements scolaires en un court laps de temps.

« Près de 2 500 établissements étant déjà en relation avec N4L pour des services tels que la mise en réseau et les pare-feux, Proofpoint vient compléter cette approche », explique Andrew Hood. « Les chefs d'établissement ont déjà bien assez de problèmes à gérer. La protection de la messagerie ne doit pas en faire partie. Nous leur faisons savoir que nous pouvons centraliser cette protection et nous en charger à leur place. »

Le déploiement en collaboration avec Proofpoint et N4L a été d'une fluidité incroyable, et le ministère de l'Éducation a travaillé main dans la main avec l'organisation pour permettre aux établissements scolaires de prendre facilement en charge leurs environnements et leurs applications de productivité spécifiques. Les établissements scolaires peuvent s'inscrire à tout moment pour utiliser Proofpoint Email Protection, qui propose principalement un filtrage classique des emails, à savoir l'extraction et le blocage des menaces à haut risque qui arrivent par email.

Proofpoint Targeted Attack Protection (TAP) joue également un rôle important dans le cadre de la solution. Il prévient le piratage de la messagerie en entreprise (BEC, Business Email Compromise), les menaces cloud et basées sur des pièces jointes, tout en fournissant des informations et une visibilité sur les cibles, pour aider le ministère à effectuer une planification plus stratégique.

« Étant donné que les établissements peuvent gérer leurs propres locations, nous ignorions quelle était la configuration Google et Microsoft existante de chaque site spécifique, ce qui représentait un défi », précise M. Hood. « Nous devions tester un certain nombre de situations selon ce que nous estimions que les établissements devaient faire pour nous assurer que nous disposions d'un service fiable. N4L a donc dû tester de nombreuses variations. Cela lui a pris quelques mois, au bout desquels nous avons commencé à lancer une version pilote du service dans certains établissements. Nous avons ensuite entamé un processus de montée en charge rapide. En seulement neuf mois, 60 % des établissements étaient inscrits au service. »

Les résultats

Protection et visibilité accrue

À mesure qu'un nombre croissant d'établissements scolaires adoptent Proofpoint Email Protection, le ministère de l'Éducation acquiert une visibilité approfondie sur le volume et les types de menaces auxquelles les établissements sont confrontés — et les bloque de manière proactive avant qu'elles ne puissent atteindre les élèves ou le personnel.

« Les chiffres sont la preuve de la valeur ajoutée que nous offre Proofpoint », explique Andrew Hood. « Nous traitons entre 80 et 100 millions de messages par mois grâce à la plate-forme. La plupart sont bloqués car considérés comme du spam peu sophistiqué, mais un nombre inquiétant de messages (entre 80 000 et 100 000 environ) sont des menaces que nous extrayons des chambres de détonation de Proofpoint. Les contenus et URL malveillants détectés requièrent une analyse plus avancée, et c'est exactement ce que fait Proofpoint. Le principal avantage est que nous sommes en mesure de fournir des preuves chaque fois qu'une menace a été bloquée et qu'elle n'a pas atteint une boîte email et cherché à piéger un utilisateur. »

Proofpoint Email Protection protège les établissements scolaires néo-zélandais grâce à une protection plus efficace de la messagerie. « Ni les professeurs ni le personnel ne nous ont fait part de retards ou de problèmes de performances », affirme M. Hood.

Non seulement Proofpoint bloque les menaces dès leur apparition, mais il permet également au ministère de l'Éducation et aux établissements sous sa responsabilité d'adopter une approche de sécurité plus proactive.

« N4L se charge de surveiller la plate-forme et a beaucoup travaillé avec Proofpoint sur l'intégration des API. Il peut même intégrer les journaux de Proofpoint à son centre SOC », ajoute Andrew Hood. « Il recherche des comportements et des modèles inhabituels, comme des pics soudains du volume de certains types d'attaques. Ces informations nous permettent également de déterminer si un établissement a interagi avec un email potentiellement malveillant. Nous pouvons ainsi informer l'établissement que nous pensons qu'il a effectué une activité à haut risque et qu'il devrait prendre certaines mesures. »

Grâce à sa solution centralisée, le ministère de l'Éducation permet aux équipes pédagogiques et aux administrateurs de se concentrer davantage sur l'apprentissage plutôt que sur la cybersécurité.

Proofpoint Attack Index, fourni par Proofpoint TAP, facilite également l'identification des VAP (Very Attacked People™, ou personnes très attaquées) afin d'aider le ministère à identifier les cibles principales et à les tenir à l'écart des menaces.

« La possibilité de passer en revue la liste des VAP et de mettre en corrélation les personnes attaquées et les sources publiques d'adresses email pour les établissements scolaires nous fournit des informations sur le comportement des cybercriminels », déclare M. Hood.

« Proofpoint nous offre une solution de filtrage des emails plus économique, tout en déchargeant l'établissement scolaire de cette responsabilité », explique Andrew Hood. « Les établissements n'ont pas à s'inquiéter de la configuration et du maintien à jour de la solution, ni à se préoccuper des dernières menaces. Ils savent qu'une solution est en place, qu'elle les protège et qu'elle est extrêmement efficace. »

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 85 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.

©Proofpoint, Inc. Proofpoint est une marque commerciale de Proofpoint, Inc. aux États-Unis et dans d'autres pays. Toutes les autres marques citées dans ce document sont la propriété de leurs détenteurs respectifs.