KVC Health Systems
people matter

KVC HEALTH SYSTEMS ÉLIMINE LES INCIDENTS DE SÉCURITÉ LIÉS AUX EMAILS AVEC VADE FOR M365

L'adoption de Vade for M365 a amélioré le niveau de protection de KVC de plus de 15% par rapport aux solutions précédentes.

À PROPOS DE KVC HEALTH SYSTEMS

KVC Health Systems est une organisation privée à but non lucratif disposant de 35 bureaux à Kansas City, mais aussi dans le Kentucky, dans le Missouri, dans le Nebraska et en Virginie-Occidentale. Fondée en 1970, KVC propose des services de santé comportementale, de protection de l'enfance, et de santé et bien-être destinés aux enfants et à la communauté, ainsi que des services de conseil en matière de santé auprès d'organisations gouvernementales et non gouvernementales.

ENJEUX

KVC Health Systems emploie 1 600 personnes et accompagne 63 000 enfants et familles dans 5 États. L'étendue et la nature de son activité en fait ainsi une cible de choix pour les cybercriminels. « Les données de santé sont celles qui se monnaient le plus cher », explique Erik Nyberg, Vice-président du service informatique de KVC. « La divulgation de ces informations nuirait à notre réputation, voire à notre organisation tout entière. »

Avant la fin de l'année 2018, KVC recevait de nombreux emails de phishing et de spear phishing. Après sa migration vers Microsoft 365, les attaques perpétrées par ce biais ont en effet connu une croissance exponentielle. « Je recevais au moins un message par semaine de nos dirigeants qui m'informaient qu'un email avait passé nos défenses », poursuit-il. « Nous avons toujours eu ce problème, mais la situation s'est aggravée lors de notre passage à Microsoft 365. »

Les années précédentes, ces attaques par email visaient les dirigeants de KVC, mais comme dans de nombreuses organisations, la tendance a changé. « Nos dirigeants maîtrisent maintenant bien ce sujet », affirme Erik Nyberg. « Ils ne tombent pas souvent dans le panneau. » Il explique que désormais, les hackers se renseignent sur KVC via les médias sociaux et d'autres données en ligne pour savoir quels employés ont accès aux systèmes informatiques de l'organisation, notamment ceux qui concernent la finance, les RH et la sécurité.

En plus d'emails de phishing classiques, KYC reçoit des emails extrêmement sophistiqués et ciblés conçus pour leurrer spécifiquement les employés de l'organisation. « L'objectif de notre organisation est avant tout d'aider les autres », détaille Erik Nyberg. « Lorsqu'une personne nous demande de l'aide par email, nous pouvons beaucoup plus facilement nous faire avoir. »

L'organisation a eu beau multiplier les produits de

POURQUOI KVC A CHOISI VADE

- ✓ Taux de détection amélioré
- ✓ Déploiement simple
- ✓ Intégration native
- ✓ Gestion des emails facilitée

VALEUR AJOUTÉE DE VADE FOR M365

En 3 mois, Vade a bloqué presque 18 000 menaces envoyées par email ciblant les employés de KVC.

Type de menace	Nombre total de menaces détectées par Vade
Phishing	2,751
Spear phishing	593
Malware	145
Spam	13,138
Scam	1,266
Total	17,893

Parmi ces 18 000 menaces, presque 5 600 sont passées entre les mailles du filet d'EOP.

Type de menace	Nombre de menaces uniques détectées par Vade
Phishing	714
Spear phishing	243
Malware	31
Spam	4,435
Scam	175
Total	5,598

sécurité de l'email au fil des ans, aucun ne présentait un niveau de protection suffisant pour protéger Microsoft 365. « Aucune solution de sécurité de l'email ne me satisfaisait », poursuit Erik Nyberg. « Un système de protection qui arrête 80 % des balles ne suffit pas. »

SOLUTION

KVC savait qu'il lui fallait une nouvelle solution, mais ne pensait pas qu'il existait un produit de sécurité de l'email capable de renforcer la protection d'Microsoft 365 de manière significative. « Je connaissais tous les produits du marché et je savais qu'aucun ne proposait un taux de détection supérieur à 80/90 % ». Après avoir rencontré les représentants de Vade, Erik Nyberg a accepté de mettre en place une preuve de concept. « Ils affirmaient pouvoir faire mieux que 90 %. Je leur ai répondu "OK, montrez-moi ça." »

La solution de sécurité de l'email Vade for M365 est basée sur une IA et s'intègre nativement à Microsoft 365. À la différence des passerelles de messagerie sécurisées, elle se place au sein d'Microsoft 365 et vient compléter Microsoft Exchange Online Protection (EOP), tout en étant transparente pour les utilisateurs et indétectable par les hackers.

La technologie anti-phishing de Vade for M365 fait appel à l'intelligence artificielle, et notamment à l'apprentissage automatique (supervisé et non supervisé) ainsi qu'à l'apprentissage approfondi (vision numérique) pour analyser les URL et pages Web en temps réel. En analysant l'origine, le contenu et le contexte des emails et des pages Web, les modèles d'apprentissage automatique reconnaissent les techniques d'obfuscation sophistiquées que les hackers utilisent pour contourner les filtres de messagerie, notamment les alias créés à l'aide d'outils de raccourcissement des URL, la redirection de pages Web légitimes vers des pages de phishing, la modification des logos des marques et l'usurpation d'adresses email.

Pour bloquer les attaques de spear phishing, les modules de détection non supervisée des anomalies et de traitement du langage naturel repèrent les modèles et anomalies courants dans les emails de spear phishing et avertissent l'utilisateur à l'aide d'une bannière personnalisable.

Par ailleurs, la fonction Auto-Remediate de Vade for M365 vient renforcer la détection des menaces et simplifier la réponse aux incidents et les analyses. Les menaces par email ayant initialement réussi à contourner le filtre sont automatiquement retirées des boîtes de réception et déplacées dans un dossier désigné par l'administrateur. En outre, le moteur d'IA ne cesse d'apprendre et de s'améliorer en s'appuyant sur les retours des utilisateurs et les données sur les menaces.

RÉSULTATS

Le volume de menaces stoppées par Vade for M365 a surpris Erik Nyberg. « Vade atteint des taux de détection de l'ordre de 90 à 95 %. Je ne pensais pas que c'était possible. » En plus, Vade for M365 bloque de nombreux emails qui passent au travers de la sécurité de l'email native d'Microsoft 365. En 2019, sur une période de seulement 3 mois, Vade a ainsi détecté pas moins de 5 600 emails manqués par EOP.

Un autre atout ayant joué dans le choix du produit réside dans son intégration native à Microsoft 365 et sa simplicité de déploiement, notamment liée à sa configuration rapide et son interface épurée. « d'un point de vue informatique, nous apprécions beaucoup la simplicité de Vade », détaille Erik Nyberg. « L'accès au portail d'administration d'Microsoft 365 pour ajouter des adresses en liste blanche ou noire est un processus pénible, qui peut prendre de 10 à 15 minutes. Avec Vade, 5 secondes suffisent. Vade est 90 % plus simple à utiliser qu'Microsoft 365. »

> ***"Le taux d'interception de Vade for Microsoft 365 est au moins 15 % supérieur à celui des filtres de messagerie que j'ai testés. Vade intercepte les emails que Microsoft laisse passer."***
>
> **Erik Nyberg, Vice-président du service**