LA VILLE ET LA COMMUNAUTÉ URBAINE DE DUNKERQUE COMPLÈTENT LA SÉCURITÉ DE LEURS 2600 BOITES EMAILS MICROSOFT 365, AVEC VADE SECURE

Victime d'attaques ciblées, la DSI choisit la solution Vade Secure for Microsoft 365 pour renforcer la sécurité de la messagerie et protéger ses utilisateurs et infrastructures : plus de 600 attaques bloquées dès le premier mois.

EN RÉSUMÉ

Après une attaque de ransomware subie en 2015, qui aura coûté 5 jours d'arrêt de production, la DSI mutualisée de la ville et de la communauté urbaine de Dunkerque a érigé la sécurité de ses emails au rang de priorité. A l'occasion de la migration de la solution de messagerie existante vers une offre SaaS Microsoft Office 365, la DSI a choisi d'apporter un niveau de sécurité supplémentaire avec la solution Cloud-native Vade Secure s'intégrant directement à Office 365. Et celle-ci a immédiatement montré toutes ses promesses : une migration réussie en 5 minutes et une simplicité d'utilisation absolue ; une économie d'1/2 ETP par semaine grâce à la gestion de la solution à distance par Vade Secure ; mais surtout une acuité de détection des attaques extrêmement avancée, notamment des emails sophistiqués de spear phishing.

ENJEUX

À sa prise de poste, la feuille de route de **Flavien Mailly, le chef du service infrastructure et production fraîchement arrivé à la DSI mutualisée de la ville et de la communauté urbaine de Dunkerque**, était claire : que l'incident vécu en 2015 ne se reproduise plus ! L'incident ? Cinq jours d'arrêt de production dus à une infection par un rançongiciel arrivé dans un email piégé.

À son arrivée, la DSI venait justement de s'engager dans la migration du Lotus Notes historique vers une offre SaaS Microsoft Office 365. C'était évidemment l'occasion d'en profiter pour renforcer la protection contre les emails malveillants.

« La question de conserver le prestataire existant s'est évidemment posée. Mais outre la question du tarif, nous n'étions pas satisfaits de la réactivité de ses équipes de support et de l'absence de francisation du produit. En outre l'éditeur ne proposait qu'une installation locale, sur les postes de travail. Mais quitte à migrer vers une solution email entièrement dans le Cloud, autant que la protection de la messagerie le soit elle aussi ! », se souvient **Flavien Mailly**.

SOLUTION

C'est à l'occasion du Forum International de la Cybersécurité (FIC), que les équipes de la DSI font la connaissance de Vade Secure. Après une présentation de l'offre, il est décidé de lancer un POC pour tester l'efficacité de la solution. A cette époque la solution de Vade Secure est en mode Cloud classique avec des redirections des MX sur son infrastructure pour filtrer les emails, mais l'éditeur assure qu'une version *« Cloud Native intégrée à Office 365 »* arrive, ce qui offre des perspectives très intéressantes et cohérentes avec le projet de migration et les objectifs de la DSI.

« L'installation a été un peu plus complexe qu'elle ne le serait aujourd'hui, car nous étions encore en Cloud classique. Mais une fois installé, tout était particulièrement simple. Et

LES RAISONS DU CHOIX VADE SECURE

- ✓ Simplicité absolue de mise en œuvre, « une migration en 5 min ! » et simplicité d'utilisation
- ✓ Gains financiers et opérationnels offerts par le mode Cloud et le management à distance de Vade Secure (montée en versions, etc.)
- ✓ Une protection avancée contre les attaques, en particulier les attaques sophistiquées et ciblées de spear phishing

LES BÉNÉFICES POUR LA VILLE ET LA COMMUNAUTÉ URBAINE DE DUNKERQUE

Sécurité des emails renforcée
Au-delà de la détection des spams génériques offerte par Microsoft, Vade Secure offre une sécurité bien plus profonde. Vade offre la meilleure acuité de détection du marché, et celle-ci est particulièrement visible sur la détection des emails particulièrement dangereux de spear phishing.

Expérience utilisateur optimisée
Une solution unique, extrêmement simple à installer et à utiliser.

Gain financier et de ressources
Gérer la sécurité plutôt que l'outil, c'est l'une des promesses de Vade Secure. La solution est gérée à distance par Vade Secure et ne requiert qu'une supervision ponctuelle quotidienne par les utilisateurs, leur permettant de gagner du temps, pouvant être mis à profit d'autres tâches stratégiques.

les équipes de support de Vade Secure étaient vraiment très présentes à nos côtés, jusqu'à aller elles-mêmes investiguer dans notre tenant Microsoft pour résoudre des questions de configuration, y compris en collaboration avec les équipes Microsoft lorsque cela était nécessaire », poursuit **Flavien Mailly**. *« Dans un contexte de réduction des effectifs, un tel niveau d'assistance est évidemment le bienvenu ! »*

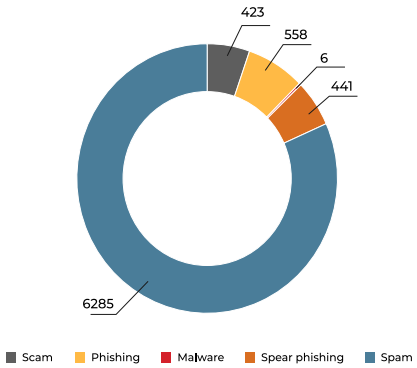
Comme annoncé, la solution Vade Secure devient Cloud native mi-2018 et la DSI de la ville et de la communauté urbaine de Dunkerque décide de migrer sans attendre. *« La migration vers la solution Vade Secure for Microsoft 365 a pris 5mn ! C'était d'une simplicité absolue. Et désormais, tout est géré par Vade Secure, y compris les montées de version. Cela nous change des produits installés localement ! Grâce à cela, nous pouvons réellement nous concentrer sur la gestion de la sécurité plutôt que sur l'outil lui-même »*, explique **Flavien Mailly**. La DSI a ainsi pu constater gain significatif sur le temps d'administration.

Au quotidien, les administrateurs de la solution ne s'y connectent que cinq minutes par jour, le temps de vérifier la présence d'éventuelles alertes (une volumétrie anormale, par exemple) ou de générer occasionnellement les rapports qui serviront à sensibiliser les cadres des autres services. Pour le reste, la solution fait son travail de manière totalement autonome.

RÉSULTATS

Ainsi, sur le mois de mars 2020, la solution a bloqué 6 malwares, 6285 spams, 558 courriers de phishing et, surtout 441 tentatives de spear phishing, les plus sérieuses, car il s'agit de tentatives ciblées, le plus souvent de type « fraude au président ».

Le mois de mars a été un mois propice aux attaques de phishing et spear phishing du fait de la tenue des élections municipales.



Le nombre de spams reçus est particulièrement faible : 6285 spams sur un mois pour 2600 postes protégés, cela fait en moyenne deux spams et demi par mois et par poste.

Cela s'explique par le travail de filtrage réalisé en amont par les différentes infrastructures concernées (notamment au niveau du tenant Microsoft). « Le filtrage natif de Microsoft est efficace contre des spams génériques, mais en revanche, plus on s'approche du spécifique et plus la solution de Vade Secure révèle sa valeur. Car les emails qui passent ainsi à travers les divers filtres standards sont les plus dangereux, les mieux réalisés et ceux qui demandent une tout autre expertise pour les détecter et les bloquer » explique Flavien Mailly, « D'où l'intérêt de compléter la sécurité de la messagerie Office 365 avec la solution protection avancée de Vade Secure ».

C'est pour cela que, paradoxalement, sans même parler des spams grossiers, il y a plus de courriers de spear phishing bloqués que de « simples » emails de phishing, alors qu'ils sont généralement les moins nombreux en valeur absolue.

Pour arriver à un tel résultat, la DSI a choisi d'activer toutes les options proposées par la solution Vade Secure, depuis le graymail (qui permet de classer les emails non prioritaires dans des dossiers spécifiques tels que newsletters, réseaux sociaux, voyages…) jusqu'à l'identification des emails de masse (spam), les messages d'alertes sur les urls suspicieuses ou encore l'intégration de bannières destinées à avertir l'utilisateur si la solution émet un doute sur une tentative de spear phishing, mais choisit d'acheminer malgré tout le courrier.

Pour l'avenir, enfin, la réflexion porte sur l'intégration de la solution à un projet SIEM à venir, afin de bénéficier d'une contextualisation avancée des alertes. Car il n'est pas rare que les infrastructures utilisées pour l'envoi de courriers malveillants soient également utilisées comme serveurs de contrôle pour des bots ou des malwares, par exemple. De l'email au malware, la stratégie sera alors parfaitement unifiée.

> ***« Le filtrage natif de Microsoft est efficace contre des spams génériques, mais en revanche, plus on s'approche du spécifique et plus la solution de Vade Secure révèle sa valeur. Car les emails qui passent ainsi à travers les divers filtres standards sont les plus dangereux, les mieux réalisés et ceux qui demandent une tout autre expertise pour les détecter et les bloquer »***

Flavien Mailly, responsable des infrastructures et de la production, la ville et la communauté urbaine de Dunkerque