Pete Linforth de Pixabay

Une messagerie française (ou européenne) sécurisée

Si vous voulez que votre entreprise soit attaquée par un malware, que votre directeur général se fasse cyber-escroquer ou encore que votre département recherche soit l'objet de l'espionnage de vos concurrents, choisissez donc une messagerie sans anti-spams, sans possibilité de chiffrement de message et non hébergée en France ou en Europe. C'est un bon début. Par Juliette Paoli

Vous affinerez plus tard vos choix en permettant, par exemple, à vos employés de fournir leur adresse e-mail professionnelle pour recevoir des avis de passage de livraison de colis chez eux, et cela afin que quantité de spams viennent leur demander de remplir un formulaire en scannant un QR code pour finaliser une commande, car l'adresse de livraison était censée être manquante (lire encadré sur le *phishing* par QR code)… Très, très bonne idée de mélanger professionnel et personnel, vous êtes décidément ingénieux. Ces pratiques coûteront à votre PME ou ETI environ 665 000 euros quand elle se fera attaquer par e-mail – très rapidement – selon une étude de Barracuda. Félicitations, vous avez gagné le gros lot !

Pour **Hélène Madar**, directrice générale banque de proximité et assurance Banque Populaire et Caisse d'Épargne, c'était une évidence : *« Face aux défis cyber auxquels sont confrontés nos clients en termes de protection de leurs données et de leurs activités, il était important d'accompagner et d'encourager tous nos clients professionnels et entreprises à se saisir du risque cyber. »* Le groupe BPCE vient en effet de signer un partenariat au mois d'octobre avec Mailinblack, une société française qui édite une messagerie du même nom, afin de proposer ses solutions – messagerie et sensibilisation à ses dangers – à leurs clients professionnels et entreprises (lire encadré). *« Les organisations doivent se protéger sur le plan technologique mais aussi humain. 90 % des incidents de sécurité sont liés à une erreur humaine. Il est devenu crucial de former et d'accompagner les collaborateurs aux cyber-menaces grandissantes »*, renchérit **Thomas Kerjean**, P-DG de Mailinblack. •••

Interview de Christophe Malapris, vice-président Sales France Vade, Hornetsecurity Group.

Solutions numériques et cybersécurité – Pouvez-vous expliquer pourquoi la sécurité des e-mails est si critique aujourd'hui ?

C. M. – Le courrier électronique est le principal point d'entrée des cyberattaques, des tentatives d'hameçonnage ou d'escroquerie aux rançongiciels et autres. Les cybercriminels évoluent constamment, exploitant les vulnérabilités humaines et utilisant l'IA pour rendre leurs attaques plus efficaces. La combinaison d'approches IA pour prédire et bloquer ces menaces est donc devenue cruciale.

SNC – Qu'est-ce qui distingue Vade (Hornetsecurity Group) sur le marché ?

C. M. – Vade (Hornetsecurity Group) se démarque par sa détection des menaces et son analyse comportementale basées sur l'IA. Nous utilisons un filtrage collaboratif pour prédire et bloquer les attaques inconnues en analysant les schémas de millions de boîtes de réception. Cela nous permet d'identifier les menaces en temps réel. À cela s'ajoute notre service de sensibilisation permanente à la sécurité, automatisé et alimenté par l'IA pour la gestion des risques humains.

SNC – Comment Vade (Hornetsecurity Group) garde-t-il une longueur d'avance sur les cybercriminels ?

C. M. – L'innovation est au cœur de notre stratégie. Nous disposons de notre propre laboratoire de sécurité Hornetsecurity et nous investissons également dans l'apprentissage automatique et l'intelligence en temps réel, ce qui permet à notre système de s'adapter aux nouvelles menaces.

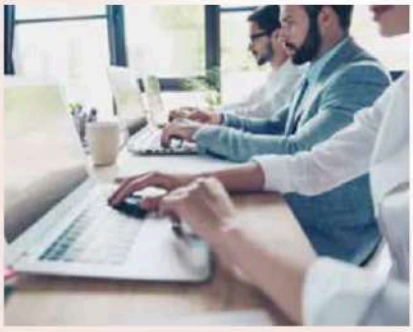
SNC – Comment répondez-vous aux préoccupations liées à la gestion des autorisations dans la sécurité des e-mails ?

C. M. – La gestion des permissions est un défi essentiel pour les RSSI, à la fois pour la sécurité et la gouvernance. Sans contrôles appropriés, les données sensibles peuvent être compromises. Vade intègre des fonctions robustes de gestion des permissions permettant aux administrateurs de définir des contrôles d'accès précis. Cela garantit que seuls les utilisateurs autorisés accèdent aux informations sensibles, réduisant ainsi le risque de fuite de données.

Avant de déployer des outils comme Copilot, les entreprises doivent s'assurer que les bonnes permissions sont en place. Nous recommandons le principe du moindre privilège : les utilisateurs n'accèdent qu'aux données nécessaires à leur rôle, conformément à des normes telles que ISO 27001.

SNC – Quelle valeur ajoutée Vade (Hornetsecurity Group) apporte-t-il aux entreprises ?

C. M. – Vade propose une défense multicouches combinant détection des menaces IA, gestion des permissions et une formation continue de sensibilisation à la sécurité. Les entreprises se concentrent souvent sur les menaces externes mais la gouvernance interne est tout aussi critique. Nos solutions aident à gérer efficacement les accès internes, assurant la conformité réglementaire et prévenant les partages non autorisés, surtout avec l'adoption croissante d'outils collaboratifs et d'environnements cloud.



SNC – Comment vos solutions aident-elles les RSSI à gérer la conformité ?

C. M. – Pour les RSSI, gérer la gouvernance dans les environnements cloud est complexe. Vade fournit des outils pour contrôler l'accès, appliquer des politiques et auditer les activités de messagerie afin de garantir la conformité avec des réglementations comme le RGPD. Nos fonctions permettent aux équipes de vérifier et d'ajuster les permissions en temps réel, assurant une conformité continue.

SNC – Comment Vade s'intègre-t-il dans la stratégie globale d'Hornetsecurity Group ?

C. M. – La mission de Hornetsecurity Group est de fournir une sécurité complète pour le cloud, avec un accent particulier porté sur Microsoft 365. En tant que membre du groupe, nous offrons un portefeuille robuste de solutions allant de la protection des e-mails à la sauvegarde et à la conformité, fournissant une protection de bout en bout pour les entreprises, le tout gérable à partir d'une console unique. ■

HORNETSECURITY
vade

••• L'e-mail, la porte d'entrée des cyberattaquants

La messagerie électronique est un canal de communication omniprésent et *a priori* de confiance pour ses utilisateurs, ce qui en fait une cible de prédilection pour les cybercriminels, que ce soit chez les particuliers, les entreprises ou les collectivités. Diverses études montrent que 9 cyberattaques sur 10 commencent par un e-mail. C'est dire l'importance de protéger la boîte e-mail de l'entreprise. E-securemail, de Secuserve, spécialiste français de la sécurité et de la messagerie collaborative, aurait le filtre anti-spams le plus complet du marché, avec 16 technologies complémentaires. Une version dédiée à M365 est également proposée par l'éditeur.

› La solution Mailo pour les collectivités

Vade, start-up française créée en 2009 et faisant partie depuis cette année du groupe allemand Hornetsecurity, propose une protection alimentée par l'IA contre les menaces les plus avancées en matière de *phishing*, de *spear phishing* et de logiciels malveillants. Ses offres de sécurité de la messagerie électronique comprennent divers services qui peuvent être proposés dans une offre packagée selon les besoins : cryptage TLS empêchant les tiers d'espionner l'e-mail en cours de transmission, filtre anti-phishing et anti- •••

Gare au phishing basé sur des QR codes

Selon cybermalveillance.gouv.fr, le *phishing*, ou « hameçonnage » en français, reste la principale menace pour toutes les catégories de public et, dans 73 % des cas, il arrive via la messagerie.

Une méthode de plus en plus populaire consiste à envoyer des e-mails contenant des QR codes qui dirigent les utilisateurs vers des sites malveillants lorsqu'ils sont scannés – et les chercheurs ont maintenant trouvé une variante dans laquelle ces QR codes sont construits à l'aide de caractères ASCII et Unicode disposés en HTML au lieu d'images statiques.

Réseaux Barracuda

Barracuda explique que cette technique, parfois appelée *quishing*, vise à contourner les filtres de sécurité dotés de capacités de reconnaissance optique de caractères (OCR) pour détecter le QR code à l'intérieur des images, puis inspecter les URL vers lesquelles ils pointent. La méthode ASCII rend la détection basée sur l'OCR inutile car une chaîne de caractères spéciaux dans les e-mails n'aura aucun sens pour un moteur OCR et ne pourra pas être distinguée d'un QR code pour un humain.

Les attaquants utilisent également de plus en plus d'URL dites « blob » (*binary large object*) qui ne s'ouvrent que dans le navigateur local pour afficher les pages de *phishing* au lieu d'utiliser des URL qui pointent vers des pages externes qui pourraient être mises sur liste noire par les logiciels de sécurité.

« Il y a un an, le volume d'attaques de phishing *basées sur des QR codes a soudainement augmenté,* ont déclaré des chercheurs de Barracuda Networks dans un rapport dédié à la question. *Les données montrent qu'environ 1 boîte aux lettres sur 20 a été ciblée par des attaques par QR code au cours du dernier trimestre 2023. »*

Ces e-mails de *phishing* se font généralement passer pour des notifications automatiques de services légitimes et incluent un QR code que l'utilisateur peut scanner avec son appareil mobile pour accéder à une ressource, telle qu'une facture, un document ou une page de suivi d'expédition.

••• spams, analyse et test de pièces jointes malveillantes dans un environnement virtuel (Sandbox). Des solutions de cyber-protection sont spécifiquement adaptées à Microsoft 365 et Google Workplace.

Des services souverains, conçus et hébergés en France

Chez Cheops Technology, la messagerie, qui comprend un espace de travail, se nomme Mail in France. Sortie en avril 2023, elle se définit comme *« une messagerie dans un cloud français »*. Tous les composants applicatifs sont *open source*. Elle s'adresse aussi bien aux PME et ETI qu'aux collectivités locales et établissements publics. Car, bien entendu, ces derniers sont eux aussi confrontés aux mêmes risques cyber. Il existe des solutions qui leur sont spécifiquement dédiées comme Mailo Collectivités, à destination des mairies, communautés de communes et collectivités territoriales.

Pour les élus et agents, Mailo Collectivités est un service de messagerie et de cloud personnalisable avec de multiples fonctionnalités qui vient de s'enrichir d'agendas de ressources et de listes de distribution. La messagerie est dotée d'un anti-spams, d'un tri intelligent des messages et de fonctionnalités avancées (envoi différé, e-mail recommandé, envoi de fichiers par lien, alias, listes de distribution, chiffrement des messages par PGP, etc.). À cela s'ajoutent agenda, gestion des emplois du temps et des occupations des salles (avec agendas de ressources), envoi d'invitations, notifications par SMS, partage d'agendas et carnet d'adresses : organisation et partage de contacts, le cloud et une suite collaborative (stockage de documents, partage et coédition de documents texte, tableurs ou présentations en ligne). Enfin, elle propose un chat et un outil de visioconférence, Rainbow, pouvant accueillir jusqu'à 120 participants. *« En hébergeant ses données en France, le service n'est pas soumis aux législations extraterritoriales comme le Cloud Act ou le Foreign Intelligence Surveillance Act (FISA) américains. Mailo Collectivités est également disponible sur l'hébergement SecNumCloud d'Outscale Dassault Systèmes et référencée au catalogue de l'UGAP »*, explique l'éditeur. Rappelons que la qualification SecNumCloud de l'ANSSI s'adresse aux prestataires de services cloud souhaitant démontrer un niveau de sécurité parmi les plus élevés du marché. ■

Les banques BPCE proposent la messagerie Mailinblack à leurs entreprises clientes

Au travers d'un partenariat avec l'entreprise marseillaise Mailinblack, la Banque Populaire et la Caisse d'Épargne proposent des solutions de protection de messagerie aussi bien sur le volet technologique que sur le volet humain, actuellement la principale vulnérabilité que rencontrent entreprises et professionnels.

Ainsi, pour protéger au quotidien leurs messageries électroniques, les clients des banques du groupe BPCE peuvent compter sur une première solution permettant de filtrer les cyberattaques transitant par e-mails (en 2023, Mailinblack a permis le blocage de 143 millions de cyberattaques). Et pour sensibiliser les salariés des entreprises clientes au risque cyber, une seconde solution de simulation d'attaques est également disponible. À travers l'envoi régulier, personnalisé et inopiné de fausses attaques par e-mail, cet outil sensibilise régulièrement les clients aux bons réflexes cyber de manière concrète.

Sécuriser la messagerie : les 10 bonnes pratiques selon Secuserve

1. Vérifiez la conformité DNS de votre domaine de messagerie.
2. Appliquez et suivez votre politique de sécurité DMARC pour rejeter les usurpations d'identité, améliorer votre délivrabilité et votre réputation.
3. Soyez vigilant si l'expéditeur affiché ne correspond pas à l'émetteur du message.
4. Méfiez-vous des QR codes et des images pouvant cacher des menaces.
5. Analysez en profondeur la structure des pièces jointes pour vous prémunir des cyber-menaces cachées et des malwares inconnus.
6. Effectuez une levée de doutes grâce à l'identification de l'émetteur du message.
7. Prévisualisez vos messages en quarantaine en toute sécurité.
8. Empêchez l'utilisateur de suivre des liens malveillants.


© Gino Crescoli de Pixabay

« Secuserve a complètement intégré les conformités DNS à ses solutions de cybersécurité. »

Stéphane Bouché est fondateur et président de Secuserve, éditeur français de solutions SaaS de sécurisation des messageries. Il nous décrit les dernières évolutions des attaques visant les boîtes e-mail et nous explique comment s'en prémunir.

› **Stéphane Bouché**, fondateur et président de Secuserve.

SNC – Quelles sont les menaces qui pèsent sur les messageries des entreprises ?

S. B. – Contrairement à une idée répandue, la messagerie reste l'application n° 1 des entreprises et la principale porte d'entrée des attaquants, dans 91 % des cas. Ces derniers utilisent des mécanismes toujours plus subtils et complexes pour atteindre leur cible grâce à l'ingénierie sociale. Il y a 20 ans, la priorité était de détecter les virus. Puis le spam est devenu un problème, aujourd'hui relégué au rang de simple nuisance. Ce que l'on voit maintenant, c'est surtout du *phishing*, du *spear phishing* et du *quishing* (utilisation d'un QR code malveillant). Idem pour le *spoofing*, soit le fait que la personne qui vous envoie un e-mail se fait passer pour quelqu'un d'autre, soit à partir d'un serveur qui n'a rien à voir avec l'entreprise en question, soit en compromettant une boîte e-mail légitime, ce qui est beaucoup plus subtil puisque l'attaquant utilise alors un vrai serveur d'entreprise. On doit la dernière innovation en date à l'intelligence artificielle. Il y a encore quelques années, les e-mails de *phishing* étaient souvent truffés de fautes d'orthographe, utilisaient un logo qui n'était pas le bon, en mauvaise résolution ou de la mauvaise couleur… Grâce à ou à cause de l'IA, les e-mails de *phishing* sont désormais propres, employant un niveau de langue adapté, sans fautes, avec le logo approprié.

SNC – Comment Secuserve s'y adapte-t-il ?

S. B. – Nous faisons de la R&D depuis 21 ans, c'est la clé ! Nous devons faire évoluer en permanence nos méthodes, nos parades, pour nous adapter aux attaquants. Dernièrement, nos innovations les plus importantes portaient sur l'IA, avec le développement et l'intégration de moteurs d'IA à nos solutions pour accélérer la détection d'attaques évoluées. Secuserve, c'est plus de 10 000 organisations utilisatrices de secteurs divers et variés et dans le monde entier ainsi que des millions d'e-mails traités chaque heure. Cela nous permet de bien avancer sur l'entraînement de nos modèles. Cette année, nous avons également fait un grand bond sur les techniques d'authentification. Je parle ici des « protocoles » autour de DNS, liés aux noms de domaines de messagerie, tels que SPF, DKIM, DMARC, ARC et BIMI qui permettent de s'assurer qu'un expéditeur utilisant un nom de domaine donné vient bien du bon serveur, avec les bons certificats. Ces protocoles sont de plus en plus répandus, c'est un cercle vertueux : plus ils sont utilisés, mieux les messageries seront sécurisées. Secuserve a complètement intégré les conformités DNS à ses solutions et, mieux encore, nous ne sommes pas seulement collecteurs de rapports DMARC mais aussi émetteurs.

SNC – La conformité DNS, c'est quelque chose qui parle aux utilisateurs ?

S. B. – Les entreprises devraient s'en préoccuper car il s'agit de la délivrabilité de leur messagerie et de la réputation de leurs marques. Je pense que la conformité DNS est aussi un critère de choix pour NIS 2 et pour la majeure partie des réglementations en France et en Europe. Surtout en s'appuyant sur une solution qui respecte les standards et les normes, ça rassure. D'autant que nous pouvons nous dire souverains : notre R&D est faite en France, nos solutions sont hébergées en France, par des équipes localisées en France et toutes nos infrastructures sont visitables.

SNC – Comment votre implémentation de DMARC permet-elle aux entreprises de renforcer leur sécurité ?

S. B. – Les rapports DMARC permettent d'identifier les e-mails qui utilisent votre domaine de messagerie. Imaginons qu'un attaquant se fasse passer pour vous mais n'envoie pas son e-mail de *phishing* depuis le bon serveur. Si vous avez une bonne politique DMARC, le message sera rejeté par tous les opérateurs sérieux. Secuserve présente ces rapports DMARC à l'administrateur du domaine, qui va pouvoir vérifier s'il y a des rejets, les IP qui sont liées à ces rejets et détecter des utilisations frauduleuses de son nom de domaine au niveau du serveur. On peut ainsi repérer des tentatives d'attaques contre le domaine, lorsque les rejets remontent en flèche dans ces rapports. Puisque nous sommes intégrés à la plupart des SIEM du marché, notre solution e-securemail peut remonter automatiquement ces éléments vers le SIEM. D'ici quelques mois, on pourra même ajouter une couche d'orchestration et de chiffrement avec MTA-STS et DANE/DNSSEC. Secuserve a été parmi les premiers à implémenter des politiques multi-domaines et granulaires fondées sur les contraintes techniques et sécuritaires et les usages. E-securemail voit tout ce qui entre et tout ce qui sort : on peut bloquer, alerter l'administrateur en cas d'anomalie, lancer des contrôles complémentaires, placer en quarantaine, demander une authentification, etc. La sécurité, c'est bien, l'administration de la sécurité, c'est mieux ; c'est ça la cybersécurité (« cyber » est tiré du mot grec *kubernân* signifiant « gouverner ») ! ■

Pour en savoir plus : https://secuserve.fr/