« 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/