Mail Protection
- SANDBOX -

LE PROFIL CLIENT

Le client est la plus grande banque d'un pays d'Afrique centrale, leader de son secteur. L'institution offre des services de banque de détail et de banque de dépôt. Sa clientèle est composée de grands comptes privés, d'institutions, de PME et de particuliers. Elle s'est implantée dans tout le pays, y compris dans des zones relativement enclavées.

SONEMA accompagne le client depuis plus de 10 ans en fournissant de la connectivité VSAT pour ses principales agences bancaires, en plus de services à valeur ajoutée d'hébergement de serveurs virtualisés, de visioconférence, de téléphonie IP, d'optimisation de bande passante et d'infogérance de ses firewalls.

LE CHALLENGE

Les collaborateurs du client se sont plaints auprès de leur DSI de fortes lenteurs sur la réception des emails. Ce dernier demandait donc régulièrement à SONEMA, de procéder au rajout manuel de nouvelles règles de blocage d'adresses email mises en cause comme source de spams importante. Compte tenu de l'inefficacité de ce filtrage, SONEMA a réalisé un audit de la connexion Internet et des flux d'emails entrants afin d'identifier la source des emails frauduleux.
L'analyse effectuée par les équipes techniques de SONEMA a révélé un problème de spams récurrent (80% du trafic était du spam). Le filtrage de contenu au niveau du firewall Internet était devenu inefficace car la majorité des messages indésirables était chiffrée entre les serveurs spammeurs et le serveur mail du client, et ces spams passaient à travers le firewall, occasionnant la congestion du lien Internet.

LA SOLUTION SONEMA

SONEMA a proposé au client la mise en place de sa solution « *Mail Protection* » de filtrage d'emails entrants. Cette solution permet d'analyser les mails, qu'ils soient transmis en clair ou chiffrés, et de bloquer les virus, malware, et spams à signature connue, mais aussi les malware à signature inconnue de type zero-day, grâce à l'option associée « *Sandbox* ».
A travers cette offre, SONEMA a mis en place les solutions adéquates afin de protéger la messagerie du client, en redirigeant le flux de mails entrants vers les infrastructures de SONEMA à Fréjus, en France, où il est filtré et analysé, avant de le retransmettre vers le serveur mail de l'entreprise.

Par ailleurs, « *Mail Protection* » convient parfaitement au client qui ne souhaitait pas investir dans une solution onéreuse, et ne disposait pas d'experts en sécurité capables de mettre en place et suivre ce genre de solutions. En souscrivant au service, le client délègue à SONEMA la mise en place et la gestion de cette solution, en contrepartie d'un abonnement mensuel basé sur le nombre de boîtes emails à protéger.

Pour sa mise en œuvre, **un serveur mail proxy a été déployé entre le réseau de SONEMA et le serveur de messagerie de la banque**, pour analyser les messages électroniques entrants avant qu'ils n'atteignent le serveur mail de la banque, et ne soient livrés à l'utilisateur final.

Le filtrage se fait ici en 3 étapes :

- **Etape 1 :** Le flux email est redirigé vers le serveur de relais mail. Celui-ci réalise un premier filtrage, aux niveaux antivirus, protection contre les intrusions (IPS), base de connaissance des IP réputées comme spammeuses (IP réputation), et filtrage d'URL. Le relais email étant la terminaison de la connexion, il est donc en mesure de déchiffrer le contenu des messages afin d'y appliquer l'ensemble de ces mesures de protection.

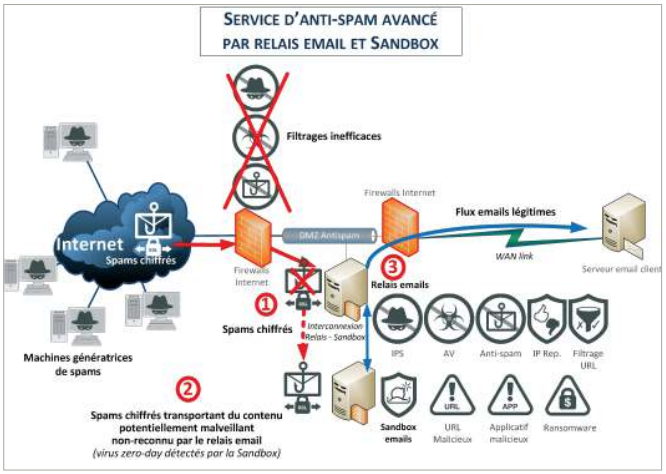

Figure 1 - Exemple de filtrage Sandbox

- **Etape 2 :** Dans le cas où le message contient une URL ou un fichier attaché, il est transféré par un canal sécurisé à la *Sandbox*. Le message y est exécuté dans un environnement virtuel similaire à celui d'un poste de travail. Lors de l'exécution du fichier ou de l'URL dans cet environnement de test, l'ensemble des « comportements » présents sur la machine sont enregistrés et analysés automatiquement par la *Sandbox*.

  En cas d'évènements suspects (effacement de fichiers, modification de paramètres systèmes, connexions à distance, etc.), la *Sandbox* bloque le message, puis le détruit ou le met en quarantaine.

  Cette deuxième étape permet de filtrer les messages contenant des codes malveillants de type zero day créés 'sur-mesure' pour exploiter des failles logicielles non encore connues des éditeurs de solutions antivirus.

- **Etape 3 :** Une fois ces filtrages réalisés, les emails légitimes sont renvoyés par le relais mail au serveur email du client.

Au-delà d'améliorer la sécurité de la messagerie, ce processus complet a permis **d'éliminer en moyenne environ 80% du trafic de messagerie sur le lien Internet du client**.

CONCLUSION

L'expérience est très positive pour le client. Cette solution lui a permis de bénéficier des améliorations suivantes :

1. Protection avancée de la messagerie avec les dernières technologies de filtrage de mails;
2. Réduction des coûts opérationnels, le client n'ayant pas à dédier des ressources techniques ni à investir dans une plateforme dédiée ;
3. Bénéfice d'une plateforme évolutive (licences, software, hardware) ;
4. Temps de mise en place réduit (autour de 15 jours) par rapport à une solution basée sur des boîtiers (à commander, installer, configurer) ;
5. Modèle de facturation simple, basé sur le nombre de boîte aux lettres, et le nombre de mails entrants ;
6. Décongestion du lien Internet au serveur mail client grâce au filtrage du trafic messagerie entrant ;
7. Améliorations des performances (espace disque, processeur, mémoire vive) du serveur mail par la réduction du trafic entrant.

Pour plus d'information :
sales@sonema.com

A propos de Sonema

Partenaire proactif de nos clients, nous développons des solutions télécom sur mesure et évolutives pour les accompagner au quotidien dans leurs projets. Notre état d'esprit d'engagement fondé sur une forte compréhension de leurs enjeux, leur permet de se concentrer sur leur coeur de métier et leurs innovations business.

Plus d'information?

Contactez notre équipe commerciale:
+377 93 15 93 15 ou
sales@sonema.com

SONEMA

7, Avenue d'Ostende
98000 Monaco
www.sonema.com