GUIDE DES SOLUTIONS PHISHING

ACENSI CYBERSECURITY

Tour Black Pearl, 14 rue du général Audran – 92400 Courbevoie – www.acensi.fr

Sommaire

Introduction	**Page 3**
Le constat	**Page 5**
Web proxy	**Page 6**
Email gateway	**Page 8**
Les employés	**Page 10**
Que faire ?	**Page 11**
Conclusion	**Page 12**
About ACENSI	**Page 13**

Introduction

Le phishing est-il un problème toujours d'actualité ?

L'implémentation des plateformes NEXTGEN de SEG avec AI, plus rapides, plus intelligentes, plus puissantes, va-t-elle vraiment faire une différence ?

Au cours des derniers mois, il est très probable que vous ayez été inondés de mails faisant part de l'augmentation des attaques de phishing depuis le début de la crise du Covid-19... Certains rapports annoncent que ces attaques ont doublé, d'autres seraient jusqu'à 6 fois plus élevées.

La question ne devrait pas être de savoir quel est le pourcentage d'augmentation mais plutôt pourquoi. Malgré toutes les solutions de sécurité déployées, il s'agit toujours du principal vecteur d'attaques réussies au sein des organisations. Certaines analyses indiquent que 90 % des vols de données proviennent d'attaques de phishing.

Le phishing

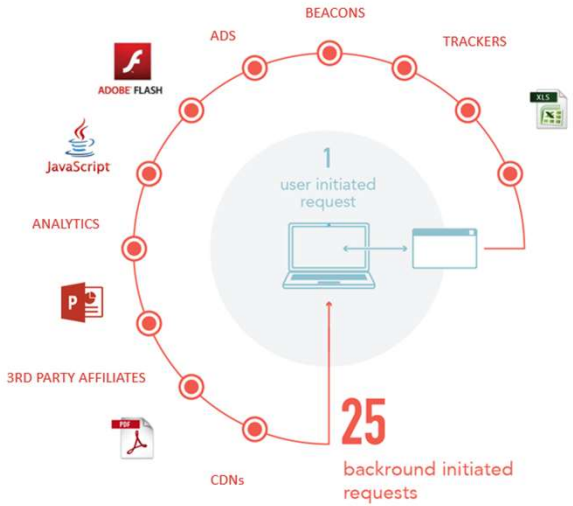
L’adage selon lequel on ne peut pas continuer à faire les mêmes choses et s'attendre à des résultats différents est on ne peut plus pertinent.

Il est évident que les business ne peuvent fonctionner sans messagerie et sans utilisation du web. Au contraire, les surfaces d'attaques augmentent et il s’agit de déployer des contrôles aussi vite que l'évolution de l'environnement de travail.

L’idée est de partager quelques concepts et déploiements réalisés ces dernières années pour éventuellement envisager ce problème d'une manière différente.

Les briques s'articulent autour de trois piliers : **WEB PROXY / EMAIL GATEWAY / LES EMPLOYES**

Les protections avancées actuelles ne protègent pas contre les logiciels malveillants !



Le constat

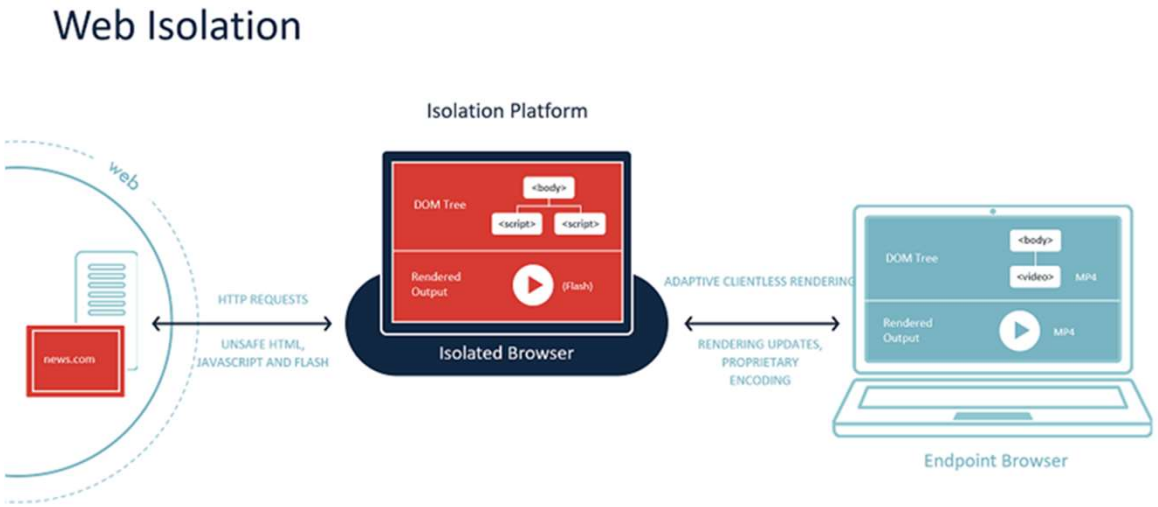
Typiquement, tout repose sur les équipes de sécurité qui définissent les politiques, établissent les règles et les exceptions tout en essayant de limiter les intrusions avec les solutions en place. Le business (les utilisateurs finaux) s'attend à ce que la messagerie et le web "fonctionnent" et si ce n'est pas le cas, cela peut très fortement affecter leur travail quotidien. Ces utilisateurs feront alors des tickets au service informatique. Le service informatique devra analyser des sites internet pour leur potentielle ouverture, mettre à jour les « white » et « black » listes et effectuer les remédiations lors de mails frauduleux.

Ce travail quotidien ne diminue pas ! Il n'y a pas assez d'heures dans une journée, de personnes ou de ressources disponibles pour augmenter de manière substantielle la sécurité des entreprises et ce d'autant que les hackeurs disposent d'outils bon marché et très sophistiqués...

Il n'y a pas de solution magique : ACENSI vous propose néanmoins d'envisager cette problématique sous un nouvel angle.

Web proxy

Le proxy web est une nécessité dans toute entreprise. Imaginons la possibilité d'intégrer un reverse proxy dans la DMZ. Cela permettrait d'isoler les utilisateurs du web, de les protéger des sites web à risque, des téléchargements en drive by download et même des vols d'identité. L'idée n'est pas nouvelle. Elle s'est néanmoins heurtée à la complexité de mise en œuvre avec les environnements Citrix pour obtenir une expérience utilisateur neutre ainsi qu'un coût de déploiement astronomique.



Web proxy

Il y a cinq ans, ACENSI a commencé à travailler avec une société dont la plupart d'entre vous n'ont probablement pas entendu parler. Le concept était simple : isoler les utilisateurs avec une technologie brevetée unique de « rendering » qui offre à l'utilisateur une expérience native et pouvant être déployée à très grande échelle. En d'autres termes, c'est comme visiter un aquarium : vous regardez les requins à travers une vitre épaisse qui vous protège de risques ne pouvant vous atteindre. Au début, comme dans de nombreuses start-ups, la technologie a connu des réajustements. Elle est maintenant déployée auprès de services financiers et d'industriels français (jusqu'à 50 000 utilisateurs). Nous avons également vu son déploiement au sein de grandes entreprises telles que JPMorgan Chase, HSBC, AMEX, US Minister Of Defense, etc… Après des années de déploiement pas un seul n'a connu de faille de sécurité. L'éditeur propose d'ailleurs une garantie financière en cas d'attaque réussie qui, à ce jour n'a jamais été réclamée.

Email gateway

Les techniques actuelles de détections des mails à risque sont basées sur les signatures (phishing, domaines connus, etc...) pour créer et mettre à jour des « black » et « white » listes.

Ces technologies bloquent environ 70 % des emails malveillants. L'investigation des sources prend en moyenne 30 minutes par mail à un analyste, sans compter la remédiation pour supprimer les mails similaires existant sur les boîtes mails d'autres utilisateurs ainsi que la mise à jour des « white » et « black » listes.

70 % pour la plupart des organisations n'est pas un résultat acceptable. Les entreprises déploient donc des couches de sécurité pour faire face à une attaque réussie mais nous pouvons tous convenir que le moyen le plus efficace de prévenir une brèche est de l'arrêter avant qu'elle ne passe par la SEG.

Que pouvons-nous donc faire pour améliorer l'efficacité des SEG et rendre le processus d'analyse et de remédiation plus efficace ?

Email gateway

Si nous supposons que 30 % des mails malveillants parviennent à l'utilisateur, nous avons quatre voies d'améliorations :

- La première option est d'enquêter sur un plus grand nombre d'e-mails, en donnant des outils plus efficaces à votre analyste avant qu'ils n'atteignent l'utilisateur ;

- La deuxième option est de transformer vos utilisateurs en analystes ;

- La troisième serait de fournir une auto-remédiation à travers toute l'infrastructure de messagerie pour immuniser les boîtes aux lettres le plus rapidement possible ;

- La quatrième est de faire partie d'une « communauté de confiance » où se partagent les nouvelles signatures et les versions polymorphes de la même attaque. Utiliser ces informations permet d'automatiser la mise à jour les « black » listes, bloquer les mails frauduleux et automatiser la remédiation.

En combinant ces stratégies, il est possible d'obtenir une augmentation significative de la réduction des mails malveillants. Imaginez un SOC assistant virtuel dans chaque boite mail, imaginez faire partie d'une communauté d'analystes qui partage ses conclusions d'analyses des attaques. Vos analystes ont à disposition des outils leur permettant de prendre de meilleures décisions et d'agir en conséquence très rapidement. Imaginez pouvoir effectuer les remédiations d'un clic, même d'un smartphone !

Les employés

Il est courant d'entendre que les employés devraient faire partie de la solution et non du problème. C'est un peu marketing et sûrement ce à quoi aspirent toutes les DSI et les RSSI. Si nous regardons la réalité en face, les utilisateurs font partie du problème. Même avec une formation continue de sensibilisation, des attaques de phishing simulées… ils cliqueront toujours ! Et ce d'autant plus que les attaques sont de plus en plus sophistiquées et réalistes.

Avec les SEG, la majorité des e-mails de phishing et des e-mails malveillants seront bloqués, qu'il s'agisse d'un add-on APT de Proofpoint ou de Microsoft. Cependant, en moyenne 20 à 30 % des attaques ciblées passent encore. Finalement, les attaques ciblées qui passent ont plus de chances d'être cliquées car les utilisateurs voient moins « d'attaques de base » et baissent leurs gardes.

Que faire ?

Les techniques d'isolation permettent de répondre à cette problématique. Aucun lien cliqué ne pourra affecter le réseau puisque les liens sont isolés. Il est même possible d'éviter les vols d'identité. Les attaques ciblées telles VIP qui n'ont aucun lien sont plus subtiles. Il existe des techniques utilisant le machine learning qui adressent ce problème.

Au-delà des solutions techniques, le constat d'échec de la formation des employés est clair. Il s'agit plus d'être règlementaire que d'apporter un réel changement. C'est pourquoi aujourd'hui les entreprises se tournent vers des solutions d'aides aux changements des comportements à hauts risques. Pouvoir faire du reporting sur l'amélioration des comportements et de la culture sécurité au sein de l'entreprise permet de mieux maîtriser sa « security posture ». C'est d'autant plus pertinent que les employés ont plus de flexibilité dans leur mode de travail. Ce n'est pas en lisant des pdf ou en visualisant des vidéos que les comportements vont évoluer.

Conclusion

Quelle que soit la taille de votre entreprise et votre appétit en cyber sécurité, les problèmes sont similaires. Néanmoins, les priorités et budgets peuvent fortement varier.

Pour certains, la priorité est de répondre aux exigences règlementaires. Il est clair que les solutions qui présentent un tel niveau d'efficacité ont un coût supérieur à celui d'un SEG/SWG ou d'un proxy classique. Cependant, lorsque nous définissons le coût réel, nous devons intégrer le coût de fonctionnement du maintien des systèmes traditionnels et, comme toujours, l'impact en cas de problème.

Il faut également noter que le marketing est une question de perception par rapport à la fonctionnalité du produit. Il est important de savoir avant toute acquisition que la complexité et les délais de déploiement peuvent aller de quelques heures à plusieurs mois - cela dépend de multiples facteurs (taille, architecture, intégration avec des tiers, etc..). Nos équipes ACENSI vous accompagnent dans ce processus.

Imaginez un monde où mail et web ne seraient plus un problème. Ce que cela signifierait pour vos entreprises qui sont des cibles constantes, avec d'énormes surfaces d'attaque. Peut-être est-ce le bon moment d'envisager une stratégie similaire ?

Si vous êtes intéressé pour échanger, contactez l'équipe à l'adresse suivante : acensicyber@acensi.fr

About ACENSI

ACENSI Cyber est un incubateur de sécurité informatique de premier plan qui teste des centaines de solutions chaque année afin de pouvoir aligner la technologie et les services d'ACENSI sur les besoins clients. Nous sommes l'un des rares incubateurs technologiques mondiaux en France et au BENELUX qui dispose de compétences techniques et de support dans le pays, englobant des solutions cyber, des services professionnels, des formations, du support et des offres de service managés.