Contrer les menaces e-mail sophistiquées :

Protégez vos données et votre marque

Présentation

Depuis les années 1990, l'e-mail a évolué : d'un simple outil principalement utilisé par la communauté technique et les chercheurs, il est devenu l'épine dorsale de la communication au sein des entreprises. Plus de 100 milliards de messages électroniques professionnels s'échangent chaque jour.[1] La sécurité est logiquement devenue une priorité, mais elle ne se limite plus aux grandes campagnes de spam. Aujourd'hui, le spam et les programmes malveillants ne sont que les composantes d'un problème plus complexe :

- Les menaces venues de l'extérieur (entrantes) sont mieux organisées, plus ciblées et plus profondes.
- Dans le même temps, le risque de fuite vers l'extérieur est grand et peut avoir des effets dévastateurs sur la réputation et la situation financière de l'entreprise.

Les solutions de sécurité e-mail Cisco® offrent plusieurs avantages pour contrer ces menaces :

- Système de protection avancée
- Sécurité accrue des données
- Gestion simplifiée

Des menaces entrantes en pleine expansion

Les attaques par e-mail ont gagné en complexité et en sophistication.

Mieux organisées

Des criminels habiles s'associent désormais afin de créer des programmes malveillants, découvrir des failles à exploiter, élaborer des kits d'installation pour les programmes malveillants, et vendre des réseaux de robots (botnets) et des services d'attaque par déni de service distribué (DDoS). D'autres monnaient leurs services pour rendre ces activités encore plus fructueuses. Afin d'optimiser la portée des charges et des liens malveillants, les criminels proposent des programmes qui testent le spam sur des filtres open source ainsi que des réseaux de spambot dont le faible volume leur permet d'échapper à la vigilance des services de listes noires.

Plus ciblées

Les attaques sont également devenues beaucoup plus personnelles. En ratissant les sites de médias sociaux, les criminels trouvent des informations sur les victimes visées et s'en servent pour élaborer des e-mails de harponnage (spear-phishing). Ces messages pertinents, destinés à des individus ou des catégories de population, contiennent des liens vers des sites hébergeant des kits d'exploitation. Selon le *rapport annuel 2015 de Cisco sur la sécurité*, « les messages de harponnage, la spécialité des cybercriminels pendant plusieurs années, ont évolué à un tel point que même les utilisateurs les plus expérimentés ont du mal à détecter les faux messages parmi ceux qu'ils reçoivent ».[2]

Le rapport note également que volume de spam, principale méthode de diffusion des messages liés à des programmes malveillants, a augmenté de 250 % entre janvier et novembre 2014.[3]

Plus profondes

Il fut un temps où les employés consultaient leurs e-mails au format texte sur une station de travail à l'abri du pare-feu de l'entreprise. Mais aujourd'hui ils travaillent avec des messages HTML enrichis sur une multiplicité d'appareils, de partout et à tout moment. Le format HTML offre de véritables boulevards pour les attaques combinées, et l'ubiquité d'accès crée de nouveaux points d'entrée qui brouillent les lignes autrefois instaurées par la segmentation des couches de sécurité. Sans le savoir, les destinataires des messages liés à des programmes malveillants propagent l'attaque en ouvrant une pièce jointe ou en cliquant sur une URL, mettant ainsi en danger d'autres employés et infrastructures.

Risques posés par les e-mails sortants

Outre la protection contre les menaces, la sécurité des données est un enjeu majeur pour la plupart des entreprises. La quantité croissante de données sensibles et personnelles envoyées par e-mail accentue le risque de fuites. En juillet 2014, par exemple, la banque d'investissement Goldman Sachs Group a informé ses clients d'une faille survenue lorsqu'un sous-traitant a envoyé par erreur des données personnelles, dont des « informations hautement confidentielles sur des comptes de titres » à l'adresse Gmail d'un inconnu. Le nombre de clients concernés par cette faille n'a pas été révélé.[4]

[1] *Email Statistics Report*, The Radicati Group, Inc. ; 2012–2016. ; [2] *Cisco 2015 Annual Security Report*, Cisco, janvier 2015. ; [3] Ibid. ; [4] « Chronology of Data Breaches », Privacy Rights Clearinghouse, actualisé le 31 décembre 2013.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ce document Cisco est confidentiel. Réservé aux partenaires de distribution. Diffusion en interne uniquement. (1110R)

Dans de nombreux pays, tous les e-mails contenant des données personnelles doivent être chiffrés avant l'envoi. Si une personne non autorisée peut lire des e-mails non chiffrés, c'est que l'entreprise concernée ne respecte pas les normes ou réglementations applicables à son secteur d'activité (PCI DSS, HIPAA, GLBA ou SOX, par exemple). Le nombre et la diversité des textes en vigueur ajoutent à la complexité et justifient l'importance donnée au contrôle des e-mails sortants. La plupart des solutions de sécurité n'offrent aucun moyen aux expéditeurs pour rappeler un message dévoilant des informations personnelles ou savoir si les destinataires l'ont effectivement lu.

Enfin, les comptes de messagerie infectés peuvent propager un virus en émettant des rafales de spams sortants. En conséquence, le domaine de messagerie de l'entreprise est placé sur liste noire, même si les messages sont signés.

Le coût d'une protection inadaptée

Compte tenu de la généralisation des mesures de protection de base contre les e-mails malveillants ou non sollicités, les entreprises peuvent estimer qu'elles sont convenablement protégées. Mais de nouvelles méthodes sont sans cesse mises au point pour contourner ce niveau de défense. Le coût engendré par les failles de sécurité annule les économies à court terme réalisées sur une solution de base.

Des centaines de banques de trente pays différents ont perdu des centaines de millions de dollars (et pourraient perdre encore plus en frais connexes) parce que des pirates avaient usé de botnets pour envoyer des e-mails contenant des programmes malveillants à leurs employés, qui ne se méfiaient pas.[5] Lorsque ces derniers ont ouvert les messages par inadvertance, les pirates ont pu prendre le contrôle des systèmes bancaires à l'aide des informations d'authentification des employés.[6]

Les erreurs dues aux e-mails sortants peuvent également entamer le capital de marque, la confiance des clients et la réputation des e-mails provenant de l'entreprise. Un franc-tireur en interne peut radicalement brider les capacités de l'entreprise à envoyer des messages à des destinataires légitimes. Les bévues risquent également d'être sanctionnées comme des infractions à la réglementation, et entraîner d'autres pertes financières. Une attaque de phishing visant un sous-traitant aurait provoqué, en 2013, la violation de données subie par la société Target Corp. et qui avait exposé les données personnelles et coordonnées de cartes bancaires de plus de 110 millions de consommateurs.[7] En février 2015, les frais encourus par cette société de détail américaine atteignaient 162 millions de dollars.[8]

Défis

Pour être efficace, la protection des e-mails impose d'adopter une vision mondiale et multiprotocole des menaces et une infrastructure qui couvre tout le cycle de l'attaque : avant, pendant et après. L'évolutivité est également un impératif, de même que des fonctions de conformité et de chiffrement flexibles sur les e-mails sortants et la capacité à éviter les charges trop lourdes pour l'infrastructure.

La solution de sécurité e-mail Cisco offre un **système de protection avancée**, une **plus grande sécurité des données** et une **gestion simplifiée**, tout en réduisant le coût total de possession et les tâches administratives.

Système de protection avancée

Protection complète et rapide des e-mails grâce à un réseau exceptionnel de détection des menaces

Le système de protection avancée de Cisco repose en premier lieu sur les travaux de Cisco Talos Security Intelligence and Research Groupe (Talos). Talos, qui réunit des chercheurs de premier plan, constitue la principale source d'informations sur les menaces de l'écosystème de sécurité adaptative collective de Cisco (CSI). Cet écosystème se compose des unités TRIAD (Threat Response, Intelligence and Development), Managed Threat Defense et Security Intelligence Operations. Cisco CSI couvre de multiples solutions de sécurité et fournit d'excellents niveaux de protection et d'efficacité.

[5] Jose Pagliery, « What We Know About the Bank Hacking Ring–And Who's Behind It », CNN Money, 16 février 2015. ; [6] Ibid. ;
[7] Bryan Krebs, « Email Attack on Vendor Set Up Breach at Target », blog KrebsOnSecurity, 12 février 2014. ; [8] John Fontana, « Breach costs at $162 million, Target reports », ZDNet, 17 février 2015.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ce document Cisco est confidentiel. Réservé aux partenaires de distribution. Diffusion en interne uniquement. (1110R)

Talos mobilise un volume inégalé de données télémétriques, regroupant des milliards de requêtes web et d'e-mails, des millions d'échantillons de programmes malveillants, des jeux de données open source et des millions d'intrusions réseau, afin d'établir une vision holistique des menaces. Cette capacité se traduit par l'exceptionnelle efficacité des solutions de sécurité Cisco. Notre cloud de sécurité adaptative génère une mine de renseignements et produit des analyses de réputation qui permettent de suivre les menaces à la trace sur les réseaux, les terminaux fixes et mobiles, les systèmes virtuels, le web et la messagerie e-mail.

Talos surveille en permanence plus de 200 paramètres, notamment :

- Listes de réputation des domaines, URL, adresses IP et fichiers à bloquer
- Pièges à spams qui interceptent les e-mails susceptibles de passer au travers des appliances Cisco
- Dispositifs « honeypot » qui détectent les auteurs d'attaques pour que Cisco puisse analyser leurs méthodes
- Robots qui arpentent le web afin de repérer les contenus malveillants
- Inspection approfondie des fichiers doublée d'une analyse permettant de détecter les contenus malveillants
- Informations de domaines et de WHOIS utilisées pour établir une base de données des domaines malveillants

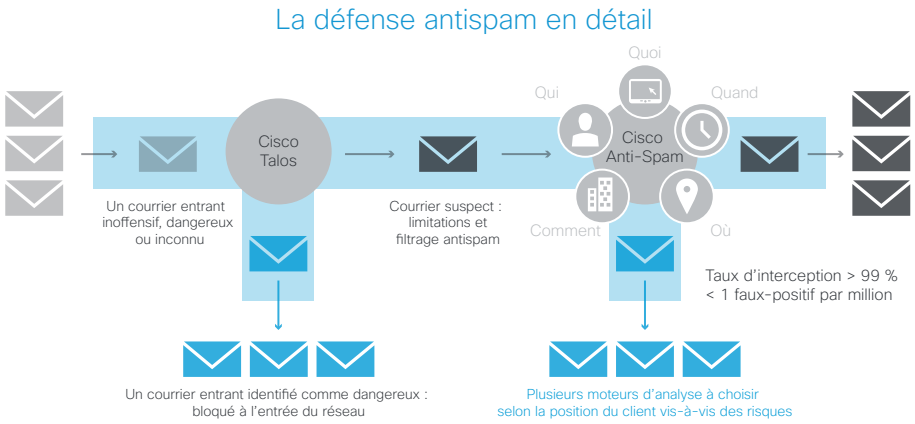
Défenses antispam

Le spam est un problème complexe qui exige une solution multicouche sophistiquée. Cisco Anti-Spam affiche le meilleur taux de capture des spams, avec un taux de faux-positifs inférieur à 1 par million, l'un des plus bas du marché.

Pour bloquer le spam avant même qu'il n'atteigne les boîtes de réception, Cisco Anti-Spam combine une couche extérieure de filtrage basée sur la réputation de l'expéditeur et une couche intérieure de filtrage qui analyse le message en profondeur. Le filtrage par réputation bloque 90 % des spams avant qu'ils ne pénètrent sur le réseau, ce qui permet de faire évoluer la solution en analysant une charge beaucoup plus réduite. Le reste est analysé par le moteur Cisco Anti-Spam, avec les critères suivants : qui a envoyé le message, quelles sont ses caractéristiques et à quel moment a-t-il été livré ? Depuis combien de temps le domaine de messagerie est-il actif ? Si le message contient une URL, où mène-t-elle ?

Dans Cisco Anti-Spam, la réputation et la catégorie de l'URL font partie des paramètres déterminants. La figure 1 illustre le fonctionnement de Cisco Anti-Spam.

Figure 1. Cisco Anti-Spam



Protection contre les virus et programmes malveillants

La seule solution antivirus Zero-Hour qui ait véritablement fait ses preuves sur le marché et qui protège contre les nouveaux virus en moins de 60 minutes.

Module complémentaire Advanced Malware Protection

Cisco Advanced Malware Protection (AMP) complète la solution de sécurité e-mail Cisco avec des fonctions de détection et de blocage des programmes malveillants, d'analyse en continu et d'alertes rétrospectives. Cisco AMP tire parti des vastes réseaux de sécurité adaptative cloud de Talos pour fournir une protection renforcée sur tout le cycle de l'attaque : avant, pendant et après.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ce document Cisco est confidentiel. Réservé aux partenaires de distribution. Diffusion en interne uniquement. (1110R)

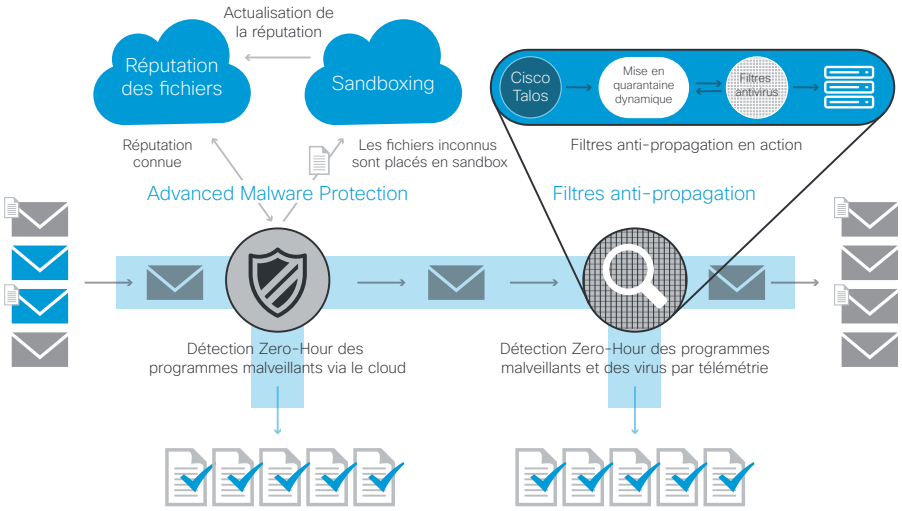
Cisco AMP combine la réputation des fichiers, le sandboxing et l'analyse rétrospective pour identifier et stopper les menaces à tous les stades du cycle de l'attaque. En voici les principales caractéristiques :

- **L'analyse de réputation** collecte une empreinte de chaque fichier transitant par la passerelle de sécurité e-mail Cisco et interroge le réseau de sécurité adaptative via le cloud d'AMP sur sa réputation. En fonction de la réponse, vous pouvez bloquer automatiquement les fichiers malveillants et appliquer les politiques définies par l'administrateur. Les solutions de sécurité e-mail et web de Cisco offrent des interfaces utilisateur identiques, et les structures de rapports sur les politiques sont semblables à celles que vous connaissez déjà.
- **L'analyse sandboxing** vous permet de contrôler les fichiers inconnus transitant par la passerelle de sécurité e-mail Cisco. Dans un environnement en sandbox hautement sécurisé, AMP peut recueillir des informations précises sur le comportement d'un fichier et les associer à une analyse humaine et automatique des données afin de déterminer le niveau de menace que représente le fichier. Cette indication est ensuite transmise au réseau Talos et utilisée pour mettre à jour et développer dynamiquement le jeu de données cloud du module AMP afin de renforcer la protection.
- **L'analyse rétrospective** résout les problèmes liés aux fichiers malveillants qui franchissent les défenses périmétriques, mais qui sont ensuite identifiés comme des menaces. Même les méthodes les plus pointues échouent parfois à identifier des programmes malveillants au niveau périmétrique. En effet, certaines techniques très efficaces, telles que le polymorphisme, le brouillage et les minuteurs de veille, peuvent empêcher toute détection. Les programmes malveillants attendent simplement d'être à l'intérieur du réseau pour agir.

  C'est à ce stade que l'analyse rétrospective entre en jeu. Elle surveille en continu les fichiers qui ont franchi la passerelle de sécurité et exploite en temps réel les informations régulièrement transmises par Talos afin de suivre l'évolution des tactiques. Dès qu'un fichier représentant une menace est identifié, AMP alerte les administrateurs et les informe sur les utilisateurs du réseau susceptibles d'être infectés et sur l'heure de l'infection. Ainsi, AMP vous aide à identifier et traiter rapidement les attaques avant qu'elles ne puissent se propager.

Les filtres antipropagation de Cisco établissent une première ligne de défense contre les nouvelles attaques, avec en moyenne 13 heures d'avance sur les signatures utilisées par les solutions antivirus réactives classiques. Le Cisco Threat Operations Center (TOC) analyse les données Talos et émet des règles de mise en quarantaine pour les messages suspects dans le monde entier (figure 2). À mesure que le TOC réunit des connaissances sur la propagation d'une attaque, il peut modifier les règles et lever la quarantaine des messages en conséquence. Les messages avec pièces jointes restent en quarantaine jusqu'à ce que Sophos ou McAfee publie une signature à jour.

Figure 2. Protection Cisco contre les virus et les programmes malveillants

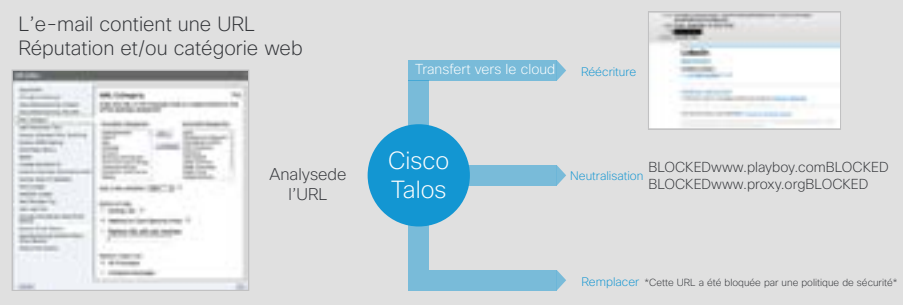


Les filtres antipropagation de Cisco protègent également contre les menaces combinées ou les attaques ciblées grâce au filtrage des URL dans les messages suspects. La sécurité e-mail Cisco peut réécrire l'URL de manière automatique ou manuelle afin de :

- rediriger le destinataire via le proxy de sécurisation du web de Cisco ; le contenu du site web fait alors l'objet d'une analyse active et le module de filtres antipropagation affiche un message pour avertir l'utilisateur que le site contient un programme malveillant ;
- « neutraliser » l'URL pour empêcher l'utilisateur de cliquer dessus ;
- remplacer l'URL ; elle est entièrement retirée et un message informe l'utilisateur qu'une partie de l'e-mail a été bloquée.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ce document Cisco est confidentiel. Réservé aux partenaires de distribution. Diffusion en interne uniquement. (1110R)

Figure 3. Les filtres antipropagation protègent contre les menaces combinées et les attaques ciblées



Sécurité accrue des données

Simplicité, précision et efficacité de la mise en application des politiques de prévention des pertes de données et du chiffrement des e-mails

Prévention des pertes de données : mise en conformité totale en 60 secondes

Les solutions de sécurité e-mail Cisco comprennent des filtres de prévention des pertes de données (DLP, Data Loss Prevention). Grâce à un partenariat avec RSA Security, leader de la technologie DLP, notre solution fournit plus de 100 politiques prédéfinies couvrant les réglementations applicables aux secteurs public et privé ainsi que les règles personnalisées de l'entreprise. Plusieurs options de remédiation sont proposées : chiffrement, ajout de pieds de page et d'avis de non-responsabilité, ajout d'adresses en copie cachée, notification, mise en quarantaine, etc. L'équipe de recherche en politique et classification des informations de RSA Security crée et met automatiquement à jour des politiques prédéfinies en s'appuyant sur des méthodologies éprouvées afin d'atteindre un degré de précision exemplaire. Avec un filtre tel que HIPAA, GLBA ou DSS, les e-mails sortants peuvent être automatiquement analysés et chiffrés en conséquence.

Si l'entreprise a besoin d'une politique complexe, les composants nécessaires à la personnalisation sont immédiatement disponibles et facilitent le processus.

Chiffrement : Contrôle total au niveau expéditeur, sans surcharge

La sécurité e-mail Cisco est la seule solution à proposer la révocation des clés de chiffrement par message et par destinataire qui peut être réalisée par l'expéditeur ou l'administrateur. L'expéditeur d'un message chiffré reçoit un accusé de réception lorsqu'un destinataire ouvre un message. Les réponses et les transferts de ce message sont automatiquement chiffrés pour préserver la confidentialité et le contrôle de bout en bout. Pour rappeler un message, l'expéditeur peut verrouiller ou invalider la clé de chiffrement à tout moment.

Le service de recommandés Cisco fournit des fonctions d'enregistrement et d'authentification des utilisateurs sous la forme d'un service géré hautement disponible, sans que les clients aient besoin de déployer d'infrastructure supplémentaire. Pour renforcer la sécurité et réduire les risques, seule la clé est stockée dans le cloud. Le contenu du message passe directement de la passerelle de l'expéditeur à la messagerie du destinataire.

Gestion simplifiée

Un contrôle total, mis à jour en permanence

Un tableau de bord centralisé, personnalisable et consolidé permet de consulter l'état du système et des files d'attente, la mise en quarantaine et la propagation des attaques, et d'autres indicateurs essentiels. Le système de quarantaine centralisé offre un point d'accès unique par lequel les utilisateurs peuvent autogérer la mise en quarantaine des spams, et les administrateurs superviser les contrôles DLP et les politiques.

Les règles de détection des messages dangereux et les mises à jour s'appliquent automatiquement sans aucun temps d'arrêt ni aucune intervention humaine. Résultat : la gestion est optimale et la protection renforcée.

> « Avec Cisco, une réduction significative du coût total de possession et les nouvelles fonctions de lutte contre les virus et le spam [sont] une réalité. »
>
> – Kenichi Tabata, responsable de département, Komatsu Ltd.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ce document Cisco est confidentiel. Réservé aux partenaires de distribution. Diffusion en interne uniquement. (1110R)

Conclusion

Cisco fournit des solutions de pointe parfaitement évolutives en s'appuyant sur une méthode adaptée à votre entreprise.

Cisco offre des solutions sur site avec appliance, des solutions cloud et des solutions hybrides :

- **Appliance de sécurité e-mail Cisco (ESA)** : conserve les données sensibles sur le site, avec d'excellentes performances et des modalités de gestion simples.
- **Appareil virtuel de sécurité de la messagerie électronique (ESAv)** : offre un déploiement plus rapide, une évolutivité à la demande et des gains d'efficacité opérationnelle en s'appuyant sur les investissements existants.
- **Sécurité e-mail via le cloud Cisco** : propose un modèle de déploiement flexible pour garantir la sécurité des e-mails à tout moment et en tous lieux.
- **Sécurité e-mail hybride Cisco** : renforce le contrôle des messages sur site tout en profitant de la simplicité et de la rentabilité de la sécurisation par le cloud.
- **Sécurité e-mail gérée Cisco** : combine la performance et la sécurité d'un appliance ESA sur site avec la fiabilité de la gestion Cisco TOC.

Pour en savoir plus

Pour en savoir plus, rendez-vous sur www.cisco.com/go/emailsecurity. Consultez un conseiller commercial, un partenaire ou un ingénieur système Cisco afin de déterminer les produits Cisco les mieux adaptés à vos besoins.

© 2015 Cisco et/ou ses filiales. Tous droits réservés. Ce document Cisco est confidentiel. Réservé aux partenaires de distribution. Diffusion en interne uniquement. (1110R)