SOPHOS

Qui espionne votre messagerie

Ce que vous devez rechercher dans une solution de sécurité de la passerelle de messagerie

Par **Chris McCormack,** Directeur marketing produit

Depuis que le gouvernement américain a révélé collecter d'énormes quantités de données à partir de communications électroniques, la notion de respect de la vie privée en ligne a été sérieusement éprouvée. Mais les fuites ou les pertes de données sensibles ne proviennent pas seulement d'un espionnage de la part du gouvernement ou de l'entreprise. Les messageries représentent le risque le plus élevé en termes d'exposition accidentelle des données, de violation de vie privée ou de non-conformité aux réglementations sur la protection des données. Dans ce livre blanc, nous vous aidons à mieux comprendre les menaces qui pèsent aujourd'hui sur la sécurité des messageries. Nous y expliquons les obstacles à la conformité et démontrons pourquoi il est important de mettre en place une protection de la passerelle de messagerie qui offre plus que le simple chiffrement.

Livre blanc Sophos Novembre 2014

Votre messagerie est un livre ouvert

Presque tout le trafic email transite le réseau public Internet en format de texte brut, sans être chiffré. C'est comme envoyer une carte postale par la Poste. Quiconque y a accès peut, de façon accidentelle ou malveillante, lire son contenu sans que vous ne le sachiez.

Vous vous demandez peut-être qui peut s'intéresser à vos emails. Avez-vous pensé à votre fournisseur d'accès à Internet (FAI) ou à votre fournisseur de messagerie en ligne ? Dans tous les cas, Google l'est certainement. Dans une affaire récente, Google a reconnu que les utilisateurs de Gmail n'ont aucune "attente raisonnable" quant à la confidentialité ou au respect de leur vie privée.[1] Dans le but de régler un recours collectif en mai 2013, Google a déclaré :

> « Tous les utilisateurs de messageries électroniques doivent nécessairement s'attendre à ce que leurs emails soient soumis à un traitement automatique. De la même manière que l'expéditeur d'une lettre à un partenaire commercial ne sera pas surpris que l'assistant du destinataire ouvre la lettre, les individus qui utilisent les messageries Web aujourd'hui ne doivent pas être surpris si leurs emails sont traités par le [fournisseur de messagerie] du destinataire en cours de livraison. En effet, une personne qui s'en remet volontairement à une tierce partie ne doit pas avoir d'attentes légitimes en termes de respect de la vie privée. »[2]

C'est une « déclaration étonnante » selon le groupe de défense des consommateurs américains Consumer Watchdog, qui recommande aux gens soucieux du respect de la vie privée de ne pas utiliser Gmail.[3] Malheureusement, ce n'est pas une solution, car en pratique cela revient à recommander aux gens de ne pas utiliser de messagerie électronique du tout. Même si vous n'utilisez pas Gmail, vous devez correspondre avec vos clients, partenaires ou autres parties prenantes.

Vous avez aussi peut être entendu parler de PRISM, un programme américain de surveillance électronique mis en place par la U.S. National Security Agency (NSA) depuis quelques années. La NSA collecte et stocke des quantités indéfinies de trafic de messagerie à partir de Google, des FAI et autres services de messagerie en ligne comme Yahoo et Hotmail.

Mais les risques qui menacent les messageries ne se limitent pas à l'espionnage intentionnel comme ceux de Google ou de la NSA. Combien de fois avez-vous cliqué sur "Répondre à tous" par accident alors que vous ne souhaitiez répondre qu'à un seul destinataire ? Ou bien envoyé un message à la mauvaise personne à cause de la fonction de saisie semi-automatique de votre client de messagerie ? Ces incidents arrivent tout le temps. Les conséquences suite à l'envoi erroné d'informations sensibles à la mauvaise personne peuvent être dévastatrices : reconnaissance publique de pertes de données, amendes et sanctions, perte de confiance du public, image de marque ternie, et pire encore...

1 http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit

2 http://www.dailytech.com/Google+Yes+we+Read+Your+Gmail/article33184.htm

3 http://www.consumerwatchdog.org/newsrelease/google-tells-court-you-cannot-expect-privacy-when-sending-messages-gmail-people-who-care

Espionnage, spearphising et spam "snowshoe"

A prendre en compte également les attaques de messagerie les plus récentes telles que le phishing, qui continuent à évoluer. Le phishing désigne la tentative d'obtenir des informations telles que noms d'utilisateurs, mots de passe ou coordonnées de cartes bancaires en faisant passer le message pour un email de confiance.

Le phishing réussit souvent en raison du "spoofing", une technique qui consiste à usurper des adresses électroniques. Selon cette technique, les cybercriminels utilisent des adresses dans le champ "De" qui imitent des comptes légitimes tels que ceux des banques, ou même qui utilisent le nom de domaine de votre entreprise pour faire semblant de provenir d'une source interne comme le service informatique.

La dernière tendance est de cibler des groupes ou des individus spécifiques au sein des organisations d'une façon plus personnelle et plus dévouée. C'est ce que l'on appelle le spearphising. Le spearphising est une tactique courante des campagnes de menaces avancées persistantes ("advanced persistent threat" ou APT en anglais), qui visent à pénétrer le réseau d'une entreprise et à obtenir des informations confidentielles.

Enfin, une dernière menace mais non des moindres : le spam classique tel que nous le connaissons tous. Grâce à votre filtre antispam actuel, vous ne le voyez même pas pour la plupart, et les emails suspects des princes nigériens qui tentent leur chance sont facilement identifiables.

Mais les individus sont encore susceptibles de tomber dans le piège et d'ouvrir des pièces jointes malveillantes. Les chercheurs ont trouvé que le spam qui semble provenir d'un site de réseau social tel que Facebook est plus efficace.[4]

Les spammeurs deviennent de plus en plus innovateurs, utilisant des techniques comme le spam "snowshoe" pour échapper aux filtrages antispam. Le spam "snowshoe", comme le terme anglais le sous-entend, propage la charge sur une quantité colossale d'adresses IP. Cela rend le travail difficile pour les filtres antispam et accroît les possibilités qu'un spam atteigne la boîte de réception d'un utilisateur.

Conformité aux réglementations publiques

Sécuriser les données sensibles pour les clients, les partenaires et les employés n'est pas seulement une question de bonnes pratiques à suivre ; c'est souvent la loi qui l'impose. La conformité aux réglementations est une priorité pour les entreprises des secteurs médical, bancaire et financier et les organismes publics. Et même si votre entreprise n'appartient pas à ces secteurs, vous devez penser aux lois qui régissent la protection des données pouvant affecter vos clients.

Il existe un certain nombre de réglementations dans presque chaque pays qui dictent les conditions de conformité et de divulgation en cas de fuite ou de perte de données. Aux États-Unis par exemple, on peut citer les institutions financières GLBA, la norme PCI DSS pour le paiement sécurisé en ligne par carte bancaire, les normes HIPAA et HITECH pour le secteur médical ainsi que de nombreuses réglementations propres à chaque état. En France, il existe plusieurs instruments juridiques telles que la loi Informatique, fichiers et libertés de 1978, la directive 95/46/CE au niveau communautaire ainsi que la Convention n°108 pour la protection des données personnelles du Conseil de l'Europe. Il existe un certain nombre de nouvelles réglementations énoncées dans la Réforme de la législation européenne relative à la protection des données, qui devrait être adoptée par le parlement de l'Union Européenne en 2015.

Leur dénominateur commun est qu'elles exigent toutes de chiffrer les données personnelles qui sont soit stockées ou envoyées électroniquement (par email ou autres). Ces lois prévoient habituellement des sanctions ou des amendes en cas de non-conformité et un devoir de divulgation en cas de fuite ou de violation de données.

4 "Evolving spammers using bogus social media email to fool users," BizReport, August 28, 2013, http://www.bizreport.com/2013/08/evolving-spammers-using-bogus-social-media-email-to-fool-use.html

Trois étapes simples pour garantir la conformité :

1. Commencez par définir une politique et sensibiliser vos utilisateurs

Donnez à vos employés et à toutes les parties prenantes une politique détaillée qui explique les éléments-clés de votre stratégie de DLP. Mentionnez clairement les types de données que vous avez besoin de protéger, vos motivations pour vouloir les protéger, les conséquences si vous ne le faites pas, et les procédures à suivre pour garantir qu'elles sont bien protégées.

2. Déployez une technologie de protection des données dans les messageries

Vos utilisateurs et votre politique doivent être prises en charge par une technologie efficace et transparente. Vous avez besoin d'une solution pour vous protéger contre la perte accidentelle et pour sécuriser vos données sensibles Une passerelle de messagerie sécurisée avec chiffrement basé sur les politiques est un élément-clé de toute solution efficace de conformité et de protection des données.

3. Commencez par l'essentiel puis évoluez en fonction de vos besoins

La protection des données peut vite devenir accablante si l'on ne prend pas la peine d'établir des priorités de ses besoins en protection des données. Commençons par la source la plus courante des fuites de données : les emails. Assurez-vous d'avoir les politiques nécessaires en place pour protéger vos données les plus sensibles sur vos clients, employés et partenaires, telles que les coordonnées bancaires, numéros de sécurité sociale et autres données identifiables. Une fois que ces politiques fonctionnent bien, vous pouvez penser à élargir votre implémentation.

Qu'est-ce qui vous retient ?

Avec toutes ces bonnes raisons pour sécuriser votre messagerie et mettre en place une solution de chiffrement, qu'est ce qui vous retient ?

La complexité : La plupart des solutions de chiffrement sont difficiles à trouver, déployer et administrer. Vous devez réaliser un investissement important pour évaluer et déployer une infrastructure ayant un fort impact dans toute l'entreprise. Cela vous simplifierait la vie s'il existait une solution que vous pourriez installer directement depuis votre fournisseur actuel, une solution qui ne nécessite pas de grand déploiement ni de personnel spécialisé pour être administré.

Le coût : La plupart des solutions de chiffrement coûtent cher à l'achat, sans compter les frais de gestion et maintenance. Ne serait-il pas idéal d'avoir une solution de sécurité des messageries qui offre le chiffrement et le DLP dans le même budget que votre antispam existant ?

L'expérience utilisateur : La plupart des solutions de chiffrement perturbe le workflow des utilisateurs. Elles requièrent des actions explicites de la part des utilisateurs pour chiffrer des emails sensibles et sont donc propices aux erreurs. Autre possibilité : les utilisateurs doivent gérer les emails chiffrés en dehors de leur messagerie habituelle, réduisant ainsi la productivité et augmentant la résistance à l'utiliser. Une meilleure solution doit pouvoir fonctionner en arrière plan, en chiffrant automatiquement les emails basés sur les politiques de DLP, sans impacter les utilisateurs ou nécessiter un nouveau logiciel client.

Ce que vous devez rechercher dans une solution de sécurité de la passerelle de messagerie

Voici la liste des fonctions à rechercher/évaluer dans une solution de sécurité de la passerelle qui protège efficacement vos données

Simplicité et facilité d'utilisation

- Recherchez une solution de protection de la passerelle qui comprend à la fois l'antispam, le DLP et le chiffrement des messageries basé sur les politiques. Une seule solution, un seul fournisseur, une seule console d'administration.
- La solution de votre choix devra inclure des types de données sensibles et pré-définies afin de faciliter la création de politiques de DLP prêtes-à-l'emploi.
- Assurez vous que les politiques de chiffrement des messageries sont assez simples pour que votre personnel puisse facilement créer de nouvelles politiques ou ajuster des politiques existantes sans besoin de formation ni de documentation.
- Choisissez une solution qui ne nécessite pas une administration complexe des clés.

Un environnement utilisateur performant

- Une solution de chiffrement de la messagerie devrait automatiquement analyser les emails et les pièces jointes à la recherche des types de données sensibles avant qu'elles ne quittent l'organisation - de manière automatique et transparente - sans obliger les utilisateurs à marquer leurs emails pour être chiffrés (en cas d'oubli)
- Choisissez une solution de chiffrement des messageries qui ne gêne pas les expéditeurs ni les destinataires. Elle devrait permettre aux utilisateurs d'envoyer des emails de la manière habituelle, en utilisant leur client de messagerie préféré sur leur PC, leur ordinateur portable, leur mobile ou en ligne.
- Votre solution de chiffrement des messageries ne devrait pas nécessiter l'installation d'un logiciel spécifique ou le lancement d'un portail côté destinataire pour qu'il puisse visualiser les emails chiffrés.

Solution économique

- Idéalement, choisissez une solution qui offre le chiffrement des emails et le DLP au prix de votre budget antispam actuel.
- Choisissez une solution qui soit facile à évaluer et à mettre en œuvre, et qui ne requiert ni matériel, logiciel ou formation spécifiques en plus de votre solution antispam existante.

Qui espionne votre messagerie

Sophos SPX Encryption et DLP

Avec notre chiffrement SPX innovant (brevet déposé) et nos politiques de DLP intégrées avec types de données sensibles prédéfinies, Sophos a la réponse à tous vos besoins en matière de protection des données.

Simple à déployer, elle intègre le spam, le chiffrement des emails et le DLP dans une seule appliance sans client logiciel spécifique à installer.

Elle vous permettra de tout administrer depuis une seule console intuitive sans clés ou certificats de chiffrement à gérer et un assistant de DLP utile qui vous rendra opérationnel en quelques minutes.

Notre moteur de DLP contient des centaines de types de données sensibles prédéfinies pour que vous puissiez créer des politiques de DLP efficaces prêtes à l'emploi. Vous pourrez également créer vos propres types personnalisés en toute simplicité.

Il est parfaitement transparent pour les utilisateurs, et leur permet d'utiliser leur client de messagerie préféré (y compris leur mobile). Et il est économique : vous bénéficiez de toutes les fonctionnalités incluses dans notre Sophos Email Appliance et Sophos UTM Email Protection pour le même budget que votre antispam.

Essayez Sophos Email Appliance avec chiffrement SPX intégré

Équipe commerciale France :
Tél. : 01 34 34 80 00
E-mail : info@sophos.fr

Oxford (Royaume-Uni) | Boston (États-Unis)

11.14.wpfr.simple

SOPHOS