OUCH! | Août 2014

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

Chiffrement

Qu'est-ce que le chiffrement?

Vous devez probablement entendre les gens utiliser le terme «chiffrement» et entendre parler de la manière pour l'utiliser afin de vous protéger vous ainsi que vos informations. Cependant, la notion de chiffrement peut sembler déroutante. En outre, le chiffrement ne peut pas vous protéger de tout, il a ses limites. Dans ce numéro, nous expliquons en termes très simples ce qu'est le chiffrement, pourquoi vous devriez l'utiliser et comment l'appliquer correctement.

Editeur invité

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) est un consultant basé dans l'Etat de Washington. Il est l'instructeur principal des cours Mobile Device Security et Ethical Hacking (SEC575) au SANS Institute et auteur de l'incident Response Team Management (MGT535).

Vous disposez d'une énorme quantité d'informations sensibles sur vos appareils, tels que des documents financiers, des images, e-mails, ou encore des dossiers médicaux. Si vous deviez avoir un de vos appareils perdus ou volés, toutes ces informations très sensibles pourraient être consultées par quiconque les possèderait. En outre, vous pouvez effectuer des transactions sensibles en ligne, tels que les services bancaires en ligne ou faire du shopping. Si un cyber attaquant devait surveiller vos activités en ligne, il pourrait voler toutes vos informations, tels que votre compte bancaire ou numéros de carte de crédit. Le chiffrement vous protège de ces situations en s'assurant que des personnes non autorisées ne peuvent pas accéder ou modifier vos informations.

Lorsque l'information n'est pas chiffrée, elle est appelée texte brut. Cela signifie que n'importe qui peut facilement la lire ou y accéder. Le chiffrement convertit ces informations dans un format non lisible appelé texte chiffré. Le chiffrement fonctionne en utilisant des opérations mathématiques complexes et une clé unique pour convertir vos informations en texte chiffré. La clé sert à verrouiller et à déverrouiller votre information, tout comme une clé peut verrouiller ou déverrouiller une porte. Par exemple, une clé est très souvent un mot de passe, seules les personnes qui ont ce mot de passe peuvent décrypter et accéder à vos informations. Pour protéger vos informations chiffrées, vous avez besoin de votre clé. Dans les travaux de chiffrement généraux, il existe deux façons de procéder : vous pouvez soit chiffrer les données (telles que les données stockées sur votre ordinateur portable) soit chiffrer les données à la volée (comme la transmission d'informations en ligne).

Le chiffrement d'informations

L'objectif principal du chiffrement est de protéger les renseignements dans le cas où votre ordinateur ou appareil mobile soit perdu ou volé. Il y'a quinze ans, ce n'était pas un problème, car la plupart des ordinateurs étaient grands, les appareils

Chiffrement

de bureau encombrants étaient très difficiles à déplacer. Aujourd'hui, de nombreux ordinateurs portables ne pèsent que quelques kilos et un appareil mobile peut peser à peine quelques grammes. Ces dispositifs sont extrêmement puissants et détiennent une quantité énorme d'informations, mais sont également très faciles à perdre. En outre, d'autres dispositifs mobiles peuvent contenir des informations sensibles, comme un lecteurs flash USB ou CD-ROM. Une technique courante pour chiffrer des informations sur ces dispositifs est appelée Full Disk Encryption (FDE). Cela signifie que tout le système est automatiquement chiffré, vous n'avez pas à décider de ce qui ou quoi doit être chiffré. La plupart des systèmes d'exploitation sont de nos jours intégrés avec Full Disk Encryption, il vous suffit de l'activer. Par exemple, Mac OS X comprend FileVault tandis que certaines versions de Windows incluent Bitlocker. Si votre ordinateur prend en charge Full Disk Encryption, nous vous recommandons fortement de l'activer. En outre, la plupart des téléphones mobiles soutiennent Full Disk Encryption pour leurs périphériques de stockage interne. Par exemple iOS, le système d'exploitation pour les iPhones et iPads, applique automatiquement Full Disk Encryption une fois qu'un mot de passe a été défini. Pour savoir si votre ordinateur ou appareil mobile de travail soutient Full Disk Encryption, demandez à votre service d'assistance ou à votre superviseur. Pour vos ordinateurs personnels, veuillez contacter le fabricant de votre ordinateur ou consultez la documentation en ligne.

Le chiffrement est un puissant moyen de sécuriser vos informations, mais il n'est pas aussi fort que votre clé.

Le chiffrement d'informations à la volée

L'information est également vulnérable quand elle est en mouvement. Si les données ne sont pas chiffrées, elle peut être surveillée et capturée en ligne. C'est pourquoi vous voulez vous assurer que toutes les communications en ligne sensibles, tels que les services bancaires en ligne, l'envoi de courriels ou peut-être même l'accès aux sites de médias sociaux sont cryptés. Le type de chiffrement en ligne le plus commun est HTTPS. Cela signifie que tout le trafic entre votre navigateur et un site web est crypté. Rechercher des https:// dans l'URL, vous verrez un verrou sur votre navigateur ou votre barre d'adresse devenir verte. Il s'agit de signes qui prouvent que la communication est cryptée. En fonction de votre navigateur et du site Web, vous pouvez voir tous les trois en même temps. En outre, chaque fois que vous vous connectez à un réseau Wi-Fi public, assurez-vous d'utiliser également le chiffrement lorsque cela est possible. Enfin, lors de l'envoi ou la réception de courriels, assurez-vous que votre client de messagerie est configuré pour transmettre votre e-mail via un canal chiffré. La plupart des clients de messagerie permettent le chiffrement, de plus, votre ISP peut être en mesure de vous aider à activer le chiffrement sur votre client de messagerie.

Chiffrement

Mise en œuvre correcte du chiffrement

Quel que soit le type de chiffrement que vous utilisez ou la façon dont vous l'utilisez, presque toutes les formes de chiffrement comportent des étapes communes afin de l'utiliser correctement.

- Votre chiffrement est aussi fort que votre clé. Si quelqu'un devine ou compromet votre clé, il aura accès à vos données. Vous devez par conséquent protéger votre clé.
- Si vous utilisez un mot de passe ou mot de passe pour votre clé, assurez-vous qu'il soit long et sécurisé et veillez à ne pas le perdre ou l'oublier. Si vous l'oubliez, vous n'aurez plus accès à vos propres données.
- Votre chiffrement est aussi fort que la sécurité de votre ordinateur. Si votre ordinateur a été compromis ou infecté, les cyberattaquants peuvent contourner votre chiffrement. En tant que tel, soyez sûr de garder votre ordinateur ou appareil mobile sécurisé aussi.
- Si vous disposez de différentes options de chiffrement, choisissez toujours la méthode la plus forte.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients.

Pour en savoir plus, veuillez vous référer aux liens suivants :

http://www.answersolutions.ch et http://answersecurity.com/

Ressources

OUCH! Attaques par Phishing:	http://support.apple.com/kb/HT4790?viewlocale=fr_FR
OUCH! Attaques par harponnage:	http://support.apple.com/kb/HT4175?viewlocale=fr_FR&locale=en_US
Termes communs de sécurité:	http://www.androidauthority.com/how-to-encrypt-android-device-326700/
OUCH! Attaques par Phishing:	http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7
OUCH! Attaques par harponnage:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201212_fr.pdf
Termes communs de sécurité:	http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201310_fr.pdf

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet