OUCH! | Juin 2016

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

OUCH!

Dans ce numéro...

Le chiffrement

Qu'est-ce que le chiffrement?

Vous devez probablement entendre les gens utiliser le terme "chiffrement" et entendre parler de la manière de l'utiliser pour vous protéger vous ainsi que vos informations. Cependant, la notion de chiffrement peut sembler déroutante et vous devez être conscient de ses limites. Dans ce numéro, nous expliquons en termes simples ce qu'est le chiffrement, comment il vous protège et comment l'appliquer correctement.

Editeur invité

Francesca Bosco (**@francibosco**) est chercheuse et responsable de projet notamment dans la gestion de projets liés à la cybercriminalité, à la cybersécurité et à la mauvaise utilisation de la technologie. Elle travaille à l'Institut interrégional de recherche des Nations Unies sur la criminalité et la justice et elle a également co-fondé le Tech et le Law Center.

Vous disposez d'une énorme quantité d'informations sensibles sur vos appareils, tels que des documents personnels, des photos et des e-mails. Si vous deviez avoir un de vos appareils perdus ou volés, toutes vos informations sensibles pourraient être accessibles par quiconque les possèderaient. En outre, vous pouvez effectuer des transactions en ligne sensibles, comme consulter vos comptes bancaires ou faire du shopping. Si quelqu'un devait surveiller ces activités, il pourrait voler vos informations, tels que vos comptes bancaires ou les numéros de votre carte de crédit. Le chiffrement vous protège de ces situations en s'assurant que des personnes non autorisées ne puissent pas accéder ou modifier vos informations.

Le chiffrement existe depuis des milliers d'années. Aujourd'hui, il est beaucoup plus sophistiqué, mais son objectif reste le même : faire passer un message secret d'un endroit à un autre en faisant en sorte que ceux qui sont autorisés à lire le message puissent y accéder. Lorsque l'information n'est pas chiffrée, elle est appelée texte brut. Cela signifie que toute personne peut facilement la lire ou y accéder. Le chiffrement consiste à convertir ces informations dans un format non lisible appelé chiffrement texte. Le chiffrement d'aujourd'hui fonctionne à l'aide d'opérations mathématiques complexes et grâce à une clé unique permettant de convertir vos informations en texte chiffré. La clé est ce qui verrouille ou déverrouille vos informations. Dans la plupart des cas, votre clé est un mot de passe ou un code d'accès.

Que peut-on chiffrer?

En général, il existe deux types de données à chiffrer, les données au repos (telles que les données stockées sur votre appareil mobile) et les données en mouvement (telle que la récupération de courrier électronique ou de messagerie d'un ami).

Le chiffrement

Le chiffrement des données au repos est essentiel pour protéger les informations en cas de vol ou perte de votre ordinateur ou appareil mobile. Les appareils d'aujourd'hui sont extrêmement puissants et détiennent une énorme quantité d'informations, mais sont également très faciles à perdre. En outre, d'autres types de médias mobiles peuvent contenir des informations sensibles, comme un lecteur flash USB ou des disques durs externes. Le Full Disk Encryption (FDE) est une technique de chiffrement largement utilisée qui chiffre l'intégralité du disque dans votre système. Cela signifie que tout le système est automatiquement chiffré pour vous, vous n'êtes pas obligé de décider de ce qui doit ou ne doit pas être chiffré. Aujourd'hui, la plupart des ordinateurs intègrent FDE, mais vous pouvez avoir à l'activer manuellement. Sur les ordinateurs Mac, il est appelé FileVault tandis que sur les ordinateurs Windows, selon la version, vous pouvez utiliser BitLocker ou Device Encryption. La plupart des appareils mobiles supportent également FDE. iOS sur les iPhones et iPads permettent automatiquement FDE une fois qu'un mot de passe a été défini. A partir d'Android 6.0 (Marshmallow), Google exige que FDE soit activé par défaut, à condition que le matériel réponde à certaines normes minimales.

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

L'information est également vulnérable quand elle est en mouvement. Si les données ne sont pas chiffrées, elles peuvent être surveillées, modifiées et capturées en ligne. Ceci est la raison pour laquelle vous voulez vous assurer que toutes les transactions et les communications en ligne sensibles soient chiffrées. 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 chiffré. Recherchez des https:// dans l'URL, vous verrez une icône de verrouillage sur votre navigateur ou votre barre d'URL devenir verte. Un autre exemple est lorsque vous envoyez ou recevez un email. La plupart des clients de messagerie offrent des capacités chiffrées que vous pourriez avoir à activer. Un troisième exemple de chiffrement de données sont les données transitant entre deux utilisateurs chattant ensemble avec des outils tels que iMessage, Wickr, Signal, WhatsApp ou Telegram. Des applications comme celles-ci utilisent un chiffrement de bout-à-bout qui empêchent des personnes tierces d'accéder aux données qui sont transférées d'un système à l'autre. Cela signifie que seulement vous et votre interlocuteur pouvez lire ce qui est envoyé.

Faire les bons choix

Pour être sûr d'être protégé lorsque vous utilisez le chiffrement, il est primordial de l'utiliser correctement.

Le chiffrement

- Votre chiffrement est aussi fort que votre clé. Si quelqu'un devine ou compromet votre clé, il aura alors accès à vos données. Vous devez par conséquent protéger votre clé. Si vous utilisez un mot de passe ou un mot de passe pour votre clé, assurez-vous qu'il soit fort et qu'il s'agisse d'un mot de passe unique. Plus votre mot de passe sera fort, plus il sera difficile pour un attaquant de le deviner. Ne pas oublier votre mot de passe, sans votre clé, vous ne pouvez plus décrypter vos informations. Si vous ne pouvez pas se souvenir de tous vos mots de passe, nous vous recommandons d'avoir recours à un gestionnaire de mot de passe.
- Votre chiffrement est aussi fort que la sécurité de vos appareils. Si votre appareil a été compromis ou est infecté, les cyberattaquants peuvent contourner votre chiffrement. Voilà pourquoi il est si important de prendre d'autres mesures pour sécuriser votre appareil, y compris à l'aide d'anti-virus, des mots de passe en les maintenant à jour.
- De nombreuses applications mobiles et applications informatiques offrent maintenant un chiffrement fort pour protéger vos données et vos communications. Si l'application que vous envisagez ne supporte pas le chiffrement, envisagez une alternative.

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.answer.ch et http://answersecurity.com/

Sources

Le chiffrement expliqué : http://www.howtogeek.com/howto/33949/htg-explains-what-is-encryption-and-how-does-it-work/

Les phrases de passe : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_fr.pdf

Les gestionnaires de mots de passe : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201510_fr.pdf

Qu'est-ce qu'un Malware : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_fr.pdf

Sécuriser votre nouvelle tablette : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_fr.pdf

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley

Traduit par : Marilyn Combet