Les habitudes de sécurité que chacun devrait adopter (ou abandonner) cette année

2018 est déjà bien avancé, et pour beaucoup, les bonnes résolutions du réveillon sombrent déjà dans l'oubli. Mais chez WatchGuard, nous pensons qu'il n'est jamais trop tard de commencer à adopter de bonnes habitudes en matière de sécurité des informations, ou à en abandonner de mauvaises. Donc notre équipe d'analystes a compilé une liste de choses à faire et à ne pas faire qui aidera à la fois les administrateurs de réseau et les utilisateurs finaux à rester en ligne en toute sécurité cette année.

Si vous êtes un administrateur préoccupé par la sécurité de votre réseau, vous trouverez ci-dessous plusieurs voies à suivre pour l'améliorer. Et si vous êtes un simple utilisateur effaré par toutes les menaces et autres attaques qui font la une des journaux (Vol de bitcoins ! Failles dans les puces Intel ! Espionnage d'Etat !), vous trouverez plus bas quelques mesures simples à prendre pour améliorer sensiblement votre niveau de sécurité digitale sans impacter votre vie de tous les jours.

Pour les administrateurs de réseau

1 Mettez en place un système d'authentification multi facteurs pour toute votre entreprise.

Beaucoup d'employés utilisent des mots de passe ultra simples, ou adoptent les mêmes pour leurs comptes professionnel et personnel. Des vols massifs de mots de passe ont largement exacerbé ce problème. Les systèmes d'authentification multi facteurs sont la solution. Ils étaient auparavant trop complexes et trop coûteux pour la plupart des entreprises, mais ce n'est plus le cas. La mise en place de tels systèmes est désormais chaudement recommandée pour protéger les accès aux réseaux d'entreprise, aux applications dans le cloud, aux VPNs, etc.

2 Créez et testez un plan de reprise après désastre (PRA).

Même s'il paraît futile d'investir dans un plan que l'on espère ne jamais utiliser, trop d'entreprises ont perdu des millions d'Euros et un temps considérable en raison d'incidents de sécurité tels que des ransomwares. Pour les hôpitaux par exemple, ces problèmes ont pu avoir des conséquences vitales. Evidemment, les sauvegardes représentent une partie importante de ce plan, mais il est important d'y intégrer les services et les ressources informatiques en plus des données.

3 Proposez des formations régulières aux bonnes pratiques de sécurité.

Certains administrateurs de réseau disent qu'il existe des situations sans espoir, mais ce n'est pas vrai. L'éducation est le remède à l'ignorance. Certes, des sessions de formation ne veulent pas dire que vos employés deviendront parfaits et ne feront plus jamais d'erreurs, mais elles veulent dire que statistiquement ils feront moins d'erreurs, produisant ainsi moins d'incidents à gérer. Les technologies de défense sont indispensables, mais certains risques ne peuvent être circonscrits sans l'assistance active des utilisateurs.

4 Donnez votre avis sur les réglementations anti cyber criminalité.

La cyber sécurité est devenue un sujet d'actualité majeur. Du piratage d'élections aux piratages de grande ampleur, en passant par la découverte de nouvelles vulnérabilités et les réglementations sur les objets connectés, les législateurs dans la plupart des pays développés sont en pleine réflexion sur les meilleures façons de traiter les problèmes liés aux cyber attaques. Toutefois, ces législateurs ne sont pas experts de ce domaine. Vous l'êtes. Faites entendre votre voix et participez au débat public chaque fois que cela est possible

5 Ne définissez pas votre stratégie de sécurité sans concertation.

La cyber sécurité et les politiques fixées par le service informatique affectent l'ensemble de l'entreprise. La direction générale voudra jouer un rôle plus actif dans le processus, car elle connait désormais les conséquences stratégiques que peut avoir une cyber attaque. Plus important encore, d'autres départements peuvent avoir des informations utiles sur la destination de certaines données et d'autres risques non répertoriés. En tant qu'administrateur, vous avez donc tout intérêt à impliquer les chefs de département dans leurs plans de sécurité, et ce, dès les premières étapes.

6 Ne concentrez pas vos investissements uniquement sur des technologies préventives.

Traditionnellement, les professionnels de la sécurité consacrent l'essentiel de leur budget à des solutions conçues pour stopper les attaques. Ces investissements sont certes indispensables, mais la technologie ne stoppera jamais la totalité des attaques. Mieux vaut donc équilibrer vos investissements avec des technologies qui identifient et éradiquent rapidement les menaces lorsqu'elles pénètrent dans votre réseau.

7 Ne soyez ni complaisant ni découragé.

Aujourd'hui les cyber attaques et les failles de sécurité envahissent continuellement l'actualité. Dans ces conditions, il est facile de se montrer défaitiste ou fataliste. Toutefois, les

risques sont souvent moins sévères qu'il n'y parait. La bonne attitude consiste à rester vigilant et à se tenir constamment au courant de l'évolution des menaces.

Pour les utilisateurs finaux

1 Privilégiez les systèmes d'authentification forte (en deux étapes).

Les simples mots de passe offrent un faible niveau de sécurité, et ne sont souvent pas utilisés correctement. La meilleure défense est l'authentification multi facteurs. La plupart des grands sites et des services cloud proposent ce type d'authentification, donc aucune excuse de na pas les utiliser s'ils sont disponibles.

2 Utilisez un gestionnaire de mots de passe.

L'authentification multi facteurs est la meilleure option, mais si un site ne la propose pas, vous devez respecter de bonnes pratiques concernant les mots de passe. Ceci dit, se souvenir d'une quantité de mots de passe aléatoires est impossible. Les gestionnaires de mots de passe sont là pour résoudre ce problème. Parfois ils sont même intégrés dans votre système d'exploitation. Utilisez-les !

3 Investissez dans un matériel ou logiciel de sécurité, quelle que soit la plate-forme que vous utilisez.

Conserver un PC sans logiciel de sécurité est comme nager dans un égout avec une plaie ouverte. Si vous êtes sous Windows vous êtes probablement déjà équipé. Toutefois, les Mac ont également besoin de suites de sécurité, de même que les terminaux mobiles sous Android par exemple.

4 Faites des sauvegardes.

La plupart des gens disent qu'ils les font, mais les font-ils réellement ? Si tout le monde sauvegardait ses données correctement, les ransomwares cesseraient d'exister. Si vous effectuez des sauvegardes, les avez-vous déjà testées ? Assurez-vous que les données que vous pensez avoir sauvegardées le sont réellement, sinon vous perdez votre temps.

5 Faites régulièrement les mises à jour.

Pour tous les utilisateurs de PC en situation normale, mieux vaut toujours configurer le système d'exploitation afin qu'il télécharge les mises à jour automatiquement et les installe immédiatement.

6 N'envoyez pas de paiements sur la base de simples SMS ou emails.

On constate un nombre croissant d'attaques de phishing via des emails ou des messages texte demandant à leurs victimes d'effectuer des virements bancaires. Même si ces messages paraissent parfois provenir de votre patron ou d'une personne connue, ce n'est quasiment jamais le cas. Avant de procéder au paiement demandé, Il est indispensable de toujours valider de tels messages en échangeant avec le demandeur via un canal de communication différent.

7 Ne cliquez pas à tort et à travers.

Vous voyez passer chaque jour un grand nombre d'emails et de posts sur les médias sociaux comportant des liens hypertexte. Certaines occasions paraissent dignes d'intérêt, mais avez-vous vraiment besoin de cliquer ? Efforcez-vous d'éviter de cliquer sur des liens provenant de communications non sollicitées. Visitez plutôt les sites concernés directement, ou si vous devez cliquer sur quelque chose, examinez d'abord le lien, et utilisez des outils pour interpréter les liens raccourcis.

8 Ne vous connectez pas sur des réseaux WiFi ouverts ou publics sans protection.

Tout d'abord, équipez-vous d'un logiciel de sécurité. Et plus important encore, s'il s'agit d'un réseau ouvert, ne l'utilisez jamais sans un VPN.

9 Méfiez-vous des offres gratuites. Beaucoup d'applications et de produits que l'on trouve sur Internet sont mentionnées comme « gratuites ». Au mieux, beaucoup d'entre eux vous seront livrés avec des publicités intermittentes ou un logiciel espion. Au pire, ils seront susceptibles d'infecter votre ordinateur. Même si certaines applications 'open source' sont dignes d'intérêt, méfiez-vous toujours des offres gratuites.

10 Ne laissez jamais votre ordinateur ouvert en public.

Même dans des environnements que vous contrôlez, installez un écran de verrouillage sur votre ordinateur, et réglez un délai d'expiration assez court (quelques minutes).

Souvenez-vous, pour les entreprises comme pour les particuliers, une bonne sécurité dépend souvent plus du respect continu de certains comportements que de n'importe quelle décision ou erreur. Si vous respectez les bonnes habitudes citées plus haut, et si vous vous les remettez en mémoire de temps en temps, votre niveau de sécurité digitale pourrait bien s'améliorer en 2018.

Pascal Le Digol, Country Manager France de WatchGuard

A propos de WatchGuard Technologies, Inc.

WatchGuard® Technologies, Inc. est un leader mondial dans le domaine de la sécurité réseau, et fournit une gamme complète de solutions UTM (Unified Threat Management), Firewall de Nouvelle Génération, WiFi sécurisé, d'intelligence réseau et de services associés à plus de 80.000 clients à travers le monde. La mission de la société est de rendre les solutions de sécurité les plus performantes accessibles à des entreprises de tous types et de toutes tailles grâce à un haut niveau de simplicité, ce qui rend les solutions WatchGuard idéales pour les entreprises distribuées et les PME. WatchGuard a son siège à Seattle, Washington, et possède des bureaux dans toute l'Amérique du Nord, en Europe, en Asie Pacifique et en Amérique latine. Pour en savoir plus, visiter WatchGuard.com, or www.secplicity.org.