Les tendances 2016 en cyber-sécurité

Les tendances 2016 en cyber-sécurité

Comme la plupart des professionnels de la sécurité informatique, je souhaite vraiment que mes prédictions ne se réalisent pas. Je préférerais que les entreprises ne soient ni piratées ni victimes de failles. Mais en prédisant la prochaine vague de menaces, nous espérons aider les entreprises à rester au fait de l'évolution des tactiques et des méthodes que les criminels vont utiliser pour les cibler. Voici dix menaces et tendances que nous devrions constater au cours de 2016 en matière de sécurité informatique.

Si une semaine peut sembler longue en politique, comme l'a observé l'ancien Premier ministre britannique Harold Wilson, une année dans le domaine de la cyber-sécurité peut ressembler à une éternité. Malgré les changements rapides, beaucoup de choses restent cependant constantes. Les trois principales menaces prévues par Check Point pour 2015 étaient la croissance rapide des logiciels malveillants inconnus, les menaces mobiles et les vulnérabilités critiques dans les plates-formes couramment utilisées (Android, iOS et autres). Ces prédictions se sont pleinement réalisées et ces menaces continueront certainement de poser nombreux problèmes. Le jeu du chat et de la souris qui a caractérisé la cyber-sécurité au cours des dernières années se poursuit. Les pirates tentent de trouver sans cesse de nouvelles manières d'attaquer les réseaux, comme le montrent les failles de cette année chez Anthem, Experian, Carphone Warehouse, Ashley Madison et TalkTalk.

Logiciels malveillants « sniper »
Les plus grandes failles de 2016 seront le résultat de logiciels malveillants conçus sur mesure pour franchir les défenses d'entreprises spécifiques, telles que lors des attaques menées contre TV5 Monde. Les attaques génériques à champ large continueront de menacer les utilisateurs individuels et les petites entreprises, et les pirates amélioreront leurs méthodes d'attaque contre les grandes entreprises qui disposent de postures de sécurité plus sophistiquées. Ils utiliseront des méthodes de phishing plus approfondies et plus sophistiquées, et d'autres astuces d'ingénierie sociale pour accéder aux systèmes et aux données qu'ils souhaitent.

Les terminaux mobiles en 1ère ligne des attaques
Le nombre d'attaques mobiles continue d'augmenter à mesure que les appareils mobiles prennent place dans l'entreprise et offrent aux pirates un accès direct et potentiellement lucratif aux données personnelles et professionnelles. D'après une étude que nous avons menée en 2015, 42% des entreprises ont subi des incidents de sécurité mobile leur coûtant plus de 200 000 €, et 82% s'attendent à une augmentation du nombre d'incidents. Cette année a également été le témoin de l'émergence de plusieurs vulnérabilités mobiles critiques, notamment Certifigate impactant des centaines de millions d'appareils Android, et XcodeGhost – première infection malveillante à grande échelle ciblant des appareils Apple iOS non jailbreakés. Nous nous attendons à d'importantes vulnérabilités mobiles similaires l'année prochaine.

La bataille contre les menaces les plus dangereuses
Dans la bataille continue entre les pirates et les professionnels de la sécurité, les agresseurs déploient des variantes personnalisées de logiciels malveillants existants et d'attaques encore inconnues (« zero-day ») de plus en plus sophistiquées, capables de contourner la technologie de sécurité traditionnelle. Ces nouveaux vecteurs d'attaque exigent des solutions plus proactives et plus avancées pour stopper ces logiciels malveillants. Des innovations comme le sandboxing au niveau du CPU, capable d'identifier les menaces les plus dangereuses avant qu'elles ne parviennent à échapper à la détection des outils traditionnels et infecter les réseaux, seront plus que jamais nécessaires en 2016 pour faire face à ces nouvelles menaces.

Les infrastructures critiques plus que jamais en ligne de mire
En décembre 2014, une aciérie en Allemagne a été frappée par des pirates qui ont réussi à accéder au réseau de production de l'usine et causer des dommages « massifs ». Le département américain de la sécurité intérieure a découvert que le Trojan « Havex » était parvenu à compromettre les systèmes de contrôle industriel de plus de 1 000 entreprises du secteur de l'énergie en Europe et en Amérique du Nord. Les cyber-attaques menées contre des services publics et des processus industriels clés se poursuivront, à l'aide de logiciels malveillants ciblant les systèmes SCADA qui contrôlent ces processus. Comme ces systèmes de contrôle sont de plus en plus connectés et offrent une surface d'attaque plus étendue, une meilleure protection sera nécessaire pour les défendre. Ces risques sur les infrastructures critiques sont particulièrement sensibles dans un contexte de menaces terroristes accrues.

Les objets connectés : futur terrain de jeu des hackers ?
L'Internet des objets en est encore à ses balbutiements, et il est peu probable qu'il ait un fort impact en 2016. Néanmoins, les entreprises doivent réfléchir à la manière dont elles peuvent protéger les appareils intelligents et se préparer à une plus vaste adoption de l'IoT. Les utilisateurs doivent se demander « où leurs données sont transmises » et « ce qui se passerait si quelqu'un mettait la main sur ces données ». L'année dernière, nous avons découvert une faille dans des routeurs équipant des TPE dans le monde entier, qui pourrait permettre à des pirates de les détourner pour lancer des attaques sur tous les appareils qui leur sont connectés. Nous nous attendons à plus de vulnérabilités similaires dans les appareils connectés.

Les wearables c'est beau … mais pas très sécurisé !
Les wearables tels que les montres intelligentes font leur entrée dans l'entreprise, présentant de nouveaux risques et défis pour la sécurité. Les données stockées dans les montres intelligentes et les autres appareils personnels intelligents sont vulnérables et pourraient même être utilisées par des pirates pour capturer de l'audio et de la vidéo via des Trojans d'accès à distance. Les entreprises qui autorisent l'utilisation de ces appareils doivent assurer leur protection via des mots de passe et des technologies de chiffrement renforcées.
Trains, avions et véhicules connectés… autant de portes d'entrée pour les hackers !

2015 est l'année de l'émergence du piratage de véhicules : leurs logiciels embarqués sont détournés afin de prendre le contrôle des véhicules. En juillet, Fiat Chrysler a rappelé 1,4 millions de véhicules Jeep Cherokee aux États-Unis après que des chercheurs aient découvert qu'ils pouvaient être piratés via le système de divertissement connecté. Avec plus de gadgets et de systèmes connectés que jamais dans les véhicules modernes, nous devons protéger ces systèmes. Il en va de même pour les systèmes complexes des avions de ligne, des trains et autres formes de transport public.

Véritable sécurité pour les environnements virtuels
La virtualisation a été rapidement adoptée par les entreprises au cours des dernières années, que ce soit via SDN, NFV ou le Cloud. Les environnements virtualisés sont complexes et créent de nouvelles couches réseau. C'est seulement maintenant que nous comprenons réellement comment protéger ces environnements. Lorsque les entreprises migrent vers des environnements virtualisés, la sécurité doit être conçue dès le départ pour offrir une protection efficace.

Nouveaux environnements, nouvelles menaces
2015 était également l'année du lancement de plusieurs nouveaux systèmes d'exploitation, tels que Windows 10 et iOS 9. La majeure partie des attaques menées contre les entreprises ces dernières années ciblaient Windows 7, en raison de la faible adoption de Windows 8. Mais avec Windows 10 et son offre de téléchargement gratuit, les cybercriminels vont donc tenter d'exploiter ce nouveau système d'exploitation. Ses mises à jour sont plus fréquentes et les utilisateurs maîtrisent moins son environnement.

La consolidation de la sécurité pour la simplifier !
Pour se protéger contre les menaces multiformes, les professionnels de la sécurité sont susceptibles de se tourner vers des solutions d'administration centralisée de la sécurité. Les grandes entreprises qui possèdent pléthore de différents produits de sécurité sur leur réseau verront la consolidation comme un moyen de réduire à la fois coût et complexité. La multitude de solutions et de produits individuels devient rapidement ingérable et peut effectivement entraver la sécurité plutôt que l'améliorer. La consolidation de la sécurité fournit un moyen efficace de réduire la complexité afin que les nouvelles menaces ne s'égarent pas entre les mailles des différents systèmes.

Réagissez à cet article
Source : http://www.globalsecuritymag.fr/La-cyber-securite-en-2016-Check,20151204,58072.html