

Les données de santé et les objets connectés seront dans la ligne de mire des cybercriminels en 2015

x	Les données de santé et les objets connectés seront dans la ligne de mire des cybercriminels en 2015
---	--

« 2014 a été une année riche en innovations. L'apparition des vêtements connectés et le développement de l'Internet des objets retiennent bien sûr toutes les attentions et promettent une année 2015 tout aussi riche. Il reste pourtant toujours une ombre au tableau : la cybercriminalité. Nos données personnelles sont plus exposées que jamais et les gouvernements ne semblent pas décidés à mettre en vigueur les lois pour y remédier. »

2014, une année faite de hauts...

« En 2014, Le Cloud et les technologies mobiles ont contribué à rendre nos vies plus faciles, plus productives et plus agréables. Quant aux appareils mobiles, ils représentent aujourd'hui plus de 30 % du trafic Internet, soit deux fois plus qu'il y a 18 mois.

Les technologies mobiles elles-mêmes continuent d'évoluer. Je pense notamment aux vêtements et aux accessoires connectés, comme les Google Glass ou les montres. Mais aussi tendance soient-elles, ces technologies ne sont rien comparé au Cloud. Plus de 90% des entreprises et 90% des internautes comptent désormais sur le Cloud pour disposer d'un accès facile, abordable et permanent à leurs données et leurs services favoris. Internet n'est plus un moyen de connexion à l'information, mais bien le lieu où on la stocke. »

... Et de bas !

« Malheureusement, innovations et risques sont indissociables. On a pu s'en rendre compte avec la succession d'attaques informatiques de grande envergure qui ont touché les entreprises de tous les secteurs cette année.

Nos adversaires ne sont plus seulement des criminels et des hacktivistes. La sophistication et le nombre croissants d'attaques sont autant d'indices qui pointent du doigt les Etats, nouveaux acteurs de la cyberguerre. Et ces pratiques douteuses ont commencé à provoquer des crises diplomatiques dans le monde réel. Je pense notamment aux tensions qui se sont accentuées entre les États-Unis et la Chine.

Quelques gouvernements à travers le monde tentent d'endiguer le phénomène mais rares sont les progrès qui valent la peine d'être mentionnés. Les révélations d'Edward Snowden en 2013 ont continué de polariser le débat sur la vie privée et de freiner les efforts législatifs, pourtant nécessaires. Dans ce contexte, que pouvons-nous prévoir en 2015 ? »

Les cyber-attaques au niveau national continueront d'évoluer et d'augmenter, mais les dommages seront davantage supportés par le secteur privé

« En 2014, des états du monde entier ont repoussé les limites acceptables de la cyber-attaque pour contrôler leurs propres populations et espionner d'autres états. Parce que personne ne s'est attelé activement au développement de normes de comportement numérique acceptables – une Convention de la Haye ou de Genève du numérique pour ainsi dire – nous pouvons nous attendre à ce que cette guerre numérique secrète se poursuive. Cependant, les sociétés du secteur privé seront de plus en plus souvent entraînées dans cette guerre soit en tant que victime visée soit en tant qu'instrument involontaire d'une attaque contre d'autres sociétés. »

Le débat sur la vie privée va mûrir

« Nous commençons à constater un assouplissement de l'actuel environnement polarisé aux États-Unis et en Europe au fur et à mesure que les gens comprennent que leur vie privée est attaquée et défendue par un ensemble d'acteurs plus varié et complexe que les débats actuels ne le porteraient à croire. L'idée s'impose que la vie privée n'est pas un concept monolithique et qu'elle ne peut pas survivre indépendamment de la sécurité. Un débat plus pragmatique et équilibré sur la manière de sécuriser notre vie privée se poursuivra en 2015 et les perspectives de voir une politique de protection de la vie privée et une législation sur le partage de renseignement susceptibles de mieux nous protéger pourraient s'éclaircir. Cette prédiction se vérifiera si la Réglementation générale sur la protection des données de l'EU, qui devrait être finalisée 2015, entre en vigueur. »

Le secteur de la distribution est la cible actuelle et les renseignements personnels sur la santé (RPS) sont dans le collimateur

« Suite aux nombreuses failles dans le secteur de la distribution et des services financiers en 2014, les entreprises qui gèrent les données des cartes de paiement renforcent leurs défenses et réduisent la fenêtre d'opportunité pour les cybercriminels, ce qui les rend moins lucratives en tant que cibles. Malheureusement, le secteur de la distribution est massif et d'envergure mondiale, et il continuera à être un environnement riche en cibles. En 2015, toutefois, les cybercriminels bien organisés se tourneront de plus en plus vers le vol d'un autre type de données moins bien sécurisées, très lucratives à monétiser dans l'économie du cyber-crime, et largement détenues par des entreprises ne disposant pas de moyens de défense contre les attaques sophistiquées : les informations personnelles détenues par les prestataires de services de santé. Hélas, il est probable que nous assistions à une autre série de hacks tant que les fournisseurs n'auront pas renforcé leur sécurité pour lutter efficacement contre ces menaces. »

L'identité des objets (connectés)

« Malgré le battage autour des vulnérabilités des logiciels et des systèmes, elles deviennent moins lucratives pour les criminels que l'ingénierie sociale et d'autres « trust exploits » plus faciles à exécuter. J'ai lu cet année un tweet qui disait à peu près ceci : « pas besoin de Zero Days quand on a la stupidité ». L'accentuation de l'interaction homme-machine et machine-machine ne fera qu'aggraver cette situation. De ce fait, l'authentification et la gestion des identités des personnes et des objets connectés qui accèdent à nos réseaux et nos données, seront un élément de sécurité de plus en plus critique en 2015. Tenez-vous prêt pour le Botnet des objets. Si l'on considère cette tendance, la forte croissance de l'Internet des objets dans le secteur de la santé, et ma prédiction sur les renseignements personnels sur la santé (RPS), les ramifications sont vraiment effrayantes.

Bien que nous ayons assisté à un changement à la présidence du Sénat de États-Unis, je ne suis pas optimiste quant aux chances de voir évoluer les projets de législation sur la cyber-sécurité en 2015. Bien que cette question soit d'une importance critique pour l'avenir de toutes les nations, elle est complexe et les avancées seront difficiles dans le climat géopolitique actuel. En l'absence de législation complète, les régulateurs de l'industrie interviendront pour combler le vide en créant une mosaïque de nouvelles exigences de conformité potentiellement incompatibles (hélas...)

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire...

Source : <http://www.globalsecuritymag.fr/Art-Coviello-Executive-Chairman-de,20150107,49869.html>