Cyber-sécurité : 10 tendances pour 2015

	Cyber-sécurité : 10 tendances pour 2015

L'année 2014 a été particulièrement chargée pour les professionnels de la sécurité informatique. A quoi s'attendre pour 2015 ? Le point avec Thierry Karsenti, directeur technique Europe de Check Point.

Pour l'année 2014, « nous nous attendions à une augmentation des tentatives d'ingénierie sociale, et l'avons bien constatée. Elles ont conduit à d'importantes fuites de données dans plusieurs enseignes bien connues. Les campagnes de logiciels malveillants ciblées se sont également intensifiées. Les attaques de « RAM scraping » et les attaques de rançonneurs ont fait les gros titres. Le nombre de problèmes de sécurité mobile a également continué d'augmenter, indique Thierry Karsenti. Le hic, ce sont les vulnérabilités massives qui ont été découvertes dans des composants informatiques établis, tels que Heartbleed et BadUSB, qui ont touché des dizaines de millions de sites web et d'appareils dans le monde entier. Personne n'y avait été préparé. 2015 verra-t-il les mêmes cyber-risques ?

1. **Les logiciels malveillants « zéro seconde »**

Plus d'un tiers des entreprises auraient téléchargé au moins un fichier infecté par des logiciels malveillants inconnus au cours de l'année dernière. Les auteurs de logiciels malveillants utilisent de plus en plus des outils spécialisés de masquage, afin que leurs attaques puissent contourner les mécanismes de détection des produits antimalwares et infiltrer les réseaux. Efficaces, les bots continueront d'être une technique d'attaque privilégiée, indique Thierry Karsenti.

2. **La mobilité**

Comme vecteurs d'attaque, les appareils mobiles offrent un accès direct à des actifs plus variés et plus précieux que tout autre moyen d'attaque individuel. « C'est également le maillon faible de la chaîne de sécurité, qui donne aux agresseurs un accès à des informations personnellement identifiables, des mots de passe, la messagerie professionnelle et personnelle, des documents professionnels, et l'accès aux réseaux et aux applications d'entreprise », précise le directeur technique.

3. **Les systèmes de paiement mobile**

Le lancement d'Apple Pay avec l'iPhone 6 est susceptible de relancer l'adoption des systèmes de paiement mobiles par les consommateurs, ainsi que d'autres systèmes de paiement concurrents : "Tous ces systèmes n'ont pas été testés pour résister à de réelles menaces, ce qui pourrait signifier d'importantes chances de succès pour les agresseurs qui trouveront des vulnérabilités à exploiter ».

4. **Les failles dans l'open source**

Qu'il s'agisse de Heartbleed (voir l'interview de Patrick Duboys, fondateur d'Alice and Bob http://www.solutions-logiciels.com/actualites.php?actu=14573) ou de Shellshock (voir l'interview vidéo de Vincent Hinderer, expert en cyber-sécurité au Cert du groupe Lexsi http://www.solutions-logiciels.com/actualites.php?actu=15039), les vulnérabilités critiques des plates-formes open source communément utilisées (Windows, Linux, iOS) sont très prisées par les agresseurs car elles offrent d'énormes possibilités. Logiquement, ces derniers vont donc continuer de rechercher des failles pour essayer de les exploiter.

5. **Les attaques sur les infrastructures critiques**

Les systèmes Scada qui commandent les processus industriels devenant de plus en plus connectés, cela va étendre les vecteurs d'attaque qui ont déjà été exploités par des agents logiciels malveillants connus tels que Stuxnet. Près de 70% des entreprises d'infrastructures critiques interrogées par le Ponemon Institute ont subi des attaques au cours de l'année passée.

6. **Les objets connectés**

L'Internet des objets fournit aux criminels un réseau mieux connecté et plus efficace pour lancer des attaques. Les entreprises doivent se préparer à leur impact.

7. **Les réseaux définis par logiciel (SDN)**

La sécurité n'est pas intégrée au concept SDN, « et doit l'être », affirme Thierry Karsenti qui enchérit : « *Avec son adoption croissante dans les centres de données, nous nous attendons à voir des attaques ciblées qui tentent d'exploiter les contrôleurs centraux SDN pour prendre le contrôle des réseaux et contourner les protections réseau* ».

8. **L'unification des couches de sécurité**

Pour lui, les architectures de sécurité monocouche et les solutions isolées provenant de différents fournisseurs n'offrent plus une protection efficace pour les entreprises. Il affirme que de plus en plus de fournisseurs proposeront des protections unifiées issues de développements, de partenariats et d'acquisitions.

9. **Les protections en mode SaaS**

Thierry Karsenti prévoit « une utilisation croissante des solutions de sécurité sous forme de services pour fournir visibilité, contrôle, prévention des menaces et protection des données ». Cette augmentation se fera parallèlement à l'utilisation croissante des services de sécurité externalisés dans le Cloud public.

10. **L'évolution des analyses grâce au Big Data**

Le Big Data va apporter d'énormes possibilités à l'analyse des menaces pour identifier de nouveaux schémas d'attaque, selon l'éditeur. Les fournisseurs intégreront de plus en plus ces capacités analytiques à leurs solutions, et les entreprises devront également investir dans leurs propres systèmes d'analyse pour prendre les bonnes décisions en fonction du contexte et des menaces pesant sur leur activité. Le partage collaboratif de renseignements sur les menaces continuera de se développer, pour proposer des protections à jour qui répondent aux besoins spécifiques des utilisateurs finaux. Le directeur technique de Check Point ajoute que ces possibilités alimenteront à leur tour des solutions de sécurité unifiées capables de fournir automatiquement une protection contre les nouvelles menaces émergentes pour renforcer la sécurité des entreprises.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://www.solutions-logiciels.com/actualites.php?actu=15189&titre=Cyber-securite-10-tendances-pour-2015 Par Juliette Paoli