PrÃ©dictions 2014 : Quelles tendances pour la CybersÃ©curitÃ© ?
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 16/12/2013 15:00:00

La cybersÃ©curitÃ© nâ□□est plus le domaine privilÃ©giÃ© des Ã©quipes techniques ou de sÃ©curitÃ© rÃ©seau. De nos jours, câ□□est devenu un sujet qui concerne tous les aspects dâ□□une entreprise avec un impact potentiel direct sur le business, les clients de lâ□□entreprise, sa rÃ©putation, ses revenues.
Voici quelques tendances qui selon nous vont fortement se dÃ©velopper durant lâ□□annÃ©e 2014 :

1. En 2014, les projets de cyber sÃ©curitÃ© seront de plus en plus souvent discutÃ©s et pilotÃ©s par la direction de lâ□□entreprise

Je passe beaucoup de temps avec nos clients et quel que soit le domaine, finance, Ã©ducation, santÃ©, Ã©nergie, transports et autres, ces entreprises reconnaissent les risques liÃ©s aux menaces de cyber sÃ©curitÃ© mais elles admettent quâ□□elles ont encore beaucoup de progrÃ¨s Ã faire pour Ã©valuer correctement les coÃ»ts liÃ©s Ã ces risques.

Certaines entreprises cotÃ©es en bourse vont mÃªme jusqu'Ã citer les risques liÃ©s aux menaces nouvelles dans leurs rapports publiques trimestriels. L'annÃ©e passÃ©e a vu une augmentation de plus de 100% de ce type de mentions comme facteur de risques.

A cause de leurs impacts potentiels sur lâ□□image de marque dâ□□une entreprise et sur ses revenues, les sujets liÃ©s Ã la cyber sÃ©curitÃ© vont basculer du domaine informatique Ã la direction de lâ□□entreprise. Nous recommandons aux responsables sÃ©curitÃ© de se prÃ©parer Ã des discussions Ã un plus haut niveau et Ã rÃ©pondre aux questions de la direction.

2. Partager les informations et les recherches sur les nouvelles menaces devient une nÃ©cessitÃ© pour les entreprises

Avec un volume de trafic sur les rÃ©seaux qui double chaque annÃ©e, les problÃ¨mes de sÃ©curitÃ© rÃ©seaux sont en augmentation constante et les outils de sÃ©curitÃ© traditionnels qui nÃ©cessitent Ã©normÃ©ment de taches manuelles sont dÃ©passÃ©s.

Nous entrons dans une nouvelle Ã¨re pour la sÃ©curitÃ© rÃ©seau basÃ©e sur un modÃ¨le ou des processus de recherches automatisÃ©s, le renforcement de l'intelligence sur les menaces nouvelles et plus que tout, le partage de cette intelligence entre entreprises devient crucial.

Le besoin dâ□□automatisation et dâ□□Ã©limination des tÃ¢ches manuelles est particuliÃ¨rement aigu pour tous les secteurs tels que le gouvernement, l'Ã©ducation, la santÃ© et les services publics. Leurs Ã©quipes de sÃ©curitÃ© rÃ©seau ont un personnel limitÃ© et ont besoin dâ□□outils les plus performants - par exemple, des logiciels de sÃ©curitÃ© qui leur donnent une visibilitÃ© et un contrÃ´le complet de leur trafic rÃ©seau.

3. Les menaces nouvelles sur les centres de donnÃ©es ciblent les systÃ¨mes de contrÃ´le pÃ©riphÃ©riques

Depuis plusieurs annÃ©es, les entreprises ont pris des mesures de plus en plus draconiennes pour renforcer la protection de leurs centres de donnÃ©es. Mais elles ont rarement fait de mÃªme pour les systÃ¨mes pÃ©riphÃ©riques qui contribuent au bon fonctionnement du centre. Cela laisse l'ensemble du centre de donnÃ©es vulnÃ©rable aux menaces nouvelles.

Les centres de donnÃ©es ne peuvent rester opÃ©rationnels et rÃ©pondre aux plus hauts niveaux de fiabilitÃ© sans que tous les Ã©lÃ©ments, des serveurs de stockage, Ã lâ□□alimentation Ã©lectrique, et aux systÃ¨mes dâ□□air conditionnÃ© et de refroidissement, soient entiÃ¨rement protÃ©gÃ©s contre les vulnÃ©rabilitÃ©s et les cyber attaques et rÃ©pondent aux mÃªmes cahiers des charges en terme de fiabilitÃ©.

Rappelez-vous ce qui s'est passÃ© en Australie en dÃ©but dâ□□annÃ©e quand les bureaux locaux Google et leur centre de donnÃ©es local ont Ã©tÃ© piratÃ©s en passant par les systÃ¨mes de contrÃ´le du bÃ¢timent. Nous nous attendons Ã ce que ce type d'attaques â□□ ou les pirates sâ□□attaquent aux systÃ¨mes les moins protÃ©gÃ©es et ciblent les Ã©lÃ©ments pÃ©riphÃ©riques dâ□□une infrastructure â□□ soient de plus en plus frÃ©quentes.

4. La validation des systÃ¨mes de sÃ©curitÃ© par les organismes nationaux tels que lâ□□ANSSI, procurera plus de confiance aux entreprises

En 2014, un retour Ã plus de confiance dans le cyberespace et encore plus dans les systÃ¨mes de sÃ©curitÃ© qui y seront intÃ©grÃ©s, passera nÃ©cessairement par la validation par des organismes nationaux, comme par exemple lâ□□ANSSI et la certification CSPN pour la France.Par Isabelle Dumont, Directrice Marketing de la division Industrie de Palo Alto Networks

Les prÃ©dictions IT/sÃ©curitÃ© de Palo Alto Networks pour 2014 :

â□¢ La sÃ©curisation des dispositifs mobiles sera inextricablement liÃ©e Ã la sÃ©curisation des rÃ©seaux
â□¢ L'Ã©cosystÃ¨me des OS mobiles s'avÃ©rera trop grand pour assurer sa protection dans son ensemble
â□¢ Lâ□□augmentation du nombre de dÃ©ploiements de Cloud hybrides (publics et privÃ©s)
â□¢ Une refonte des systÃ¨mes de sÃ©curitÃ© dÃ©diÃ©s au Cloud
â□¢ La diminution des durÃ©es de dÃ©tection
â□¢ La cyber sÃ©curitÃ© deviendra encore plus une prÃ©occupation business, gÃ©rÃ©e et pilotÃ©e par la direction de lâ□□entreprise
â□¢ La sÃ©curitÃ© entrainera la fiabilitÃ© Ã©tant donnÃ© que les attaques visent les systÃ¨mes de contrÃ´le
â□¢ La demande de cyber sÃ©curitÃ© et de compÃ©tences IR atteindra de nouveaux sommets
â□¢ Les rÃ©vÃ©lations de la NSA entraineront une hausse dramatique du cryptage et de sÃ©curisation SSL
â□¢ Les malwares financiÃ¨rement motivÃ©s effectueront leur retour et la frontiÃ¨re entre APT et le crime organisÃ© sera floue
â□¢ La validation des systÃ¨mes de sÃ©curitÃ© par des organismes nationaux renforcera la confiance des entreprises