PrÃ©voir lâ□□imprÃ©visible en matiÃ¨re de cyber-attaques avancÃ©es
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 18/12/2013 15:00:00

Lâ□□annÃ©e 2013 fÃ»t une annÃ©e Ã©prouvante sur le plan de la sÃ©curitÃ© informatique : tandis que les entreprises devaient faire face Ã de nouvelles formes dâ□□attaques ciblÃ©es et de plus en plus sophistiquÃ©es, la protection des donnÃ©es et de la vie privÃ©e a Ã©tÃ© sÃ©rieusement remise en cause suite Ã la rÃ©vÃ©lation de pratiques douteuses de la part de certains gouvernements.
Pour relever ces dÃ©fis liÃ©s Ã la cyber-sÃ©curitÃ©, une campagne internationale de sensibilisation Ã la sÃ©curisation des donnÃ©es sensibles est lancÃ©e par les organisations et les Ã©diteurs de sÃ©curitÃ© afin de limiter ces attaques et notamment les consÃ©quences parfois irrÃ©versibles quâ□□elles engendrent. CyberArk propose de se projeter dans les bonnes pratiques de lâ□□annÃ©e 2014 en 10 points clÃ©s :

1. Surveiller les attaques commanditÃ©es par les Ã□tats qui deviendront plus frÃ©quentes

Les rÃ©vÃ©lations sur lâ□□existence de programmes d'espionnage par la NSA, le GCHQ britannique, ou encore d'autres agences de renseignements, ont crÃ©Ã© un prÃ©cÃ©dent sur la maniÃ¨re dont les gouvernements utilisent Internet et les technologies pour la dÃ©fense nationale. De plus en plus de pays adopteront cette approche et iront mÃªme au-delÃ , que ce soit en termes de surveillance passive ou de campagnes de cyber-attaques agressives. Les principaux acteurs gÃ©opolitiques (les puissances occidentales, l'Iran, la Chine et la Russie) vont continuer de renforcer leurs efforts en matiÃ¨re de cyber-sÃ©curitÃ©, ce qui aura un impact majeur sur les pouvoirs des Etats malveillants et les groupes terroristes quâ□□ils soutiennent.Â

Comme nous lâ□□avons vu avec Stuxnet, ces attaques sont dÃ©mantelÃ©es, analysÃ©es et rÃ©-exploitÃ©es â□□ elles se banalisent et deviennent par consÃ©quent plus facilement utilisables par des acteurs malveillants. Davantage d'attaques de cette nature vont Ã©merger dans le futur, pour des raisons Ã la fois Ã©conomiques, politiques et terroristes.

2. Tout encoder/encrypter

Les consÃ©quences des rÃ©vÃ©lations dâ□□Edward Snowden continueront dâ□□avoir un impact

majeur sur tout ce que nous faisons. Alors que des entreprises telles que Google appellent Ã tout encrypter, de nouvelles normes dâ□□encodage vont Ã©merger. Le dÃ©veloppement de nouvelles mÃ©thodes conduira au passage de nouvelles frontiÃ¨res en termes de cryptage et dâ□□interception dâ□□attaques, que ce soit Ã travers des mÃ©thodes mathÃ©matiques innovantes ou grÃ¢ce Ã un matÃ©riel informatique dÃ©diÃ©.

3. Renforcer la prÃ©vention des malwares

On parle de la mort de la sÃ©curitÃ© pÃ©rimÃ©trique depuis plus de 10 ans. Bien quâ□□il y ait un marchÃ© Ã venir pour ces remparts technologiques, nous sommes confrontÃ©s Ã une dÃ©sillusion de taille quant Ã lâ□□infaillibilitÃ© de technologies telles que les pare-feu de nouvelle gÃ©nÃ©ration, les navigations sÃ©curisÃ©es (sandboxing), etc. principalement en raison du fait que de plus en plus dâ□□entreprises seront victimes dâ□□attaques ciblÃ©es en dÃ©pit de de ces solutions.

4. Augmenter les dÃ©penses pour la prÃ©vention des menaces internes

La menace interne est constamment prÃ©sente et concerne toutes les entreprises. Lâ□□incident Edward Snowden continue de rÃ©sonner Ã travers les industries. Câ□□est pourquoi 2014 sera lâ□□annÃ©e oÃ¹ lâ□□accent sera mis sur lâ□□aspect humain de la prÃ©vention de la menace interne. Les entreprises dÃ©penseront plus dâ□□argent et de temps Ã suivre et surveiller leurs employÃ©s, avec une attention toute particuliÃ¨re sur les postes et les contrats externalisÃ©s. Il en sera de mÃªme en ce qui concerne la surveillance et le contrÃ´le des comptes Ã privilÃ¨ges.

5. Renforcer la protection de lâ□□ingÃ©nierie sociale

Lâ□□ingÃ©nierie sociale a toujours Ã©tÃ© lâ□□un des meilleurs outils Ã la disposition des cyber-attaqueurs pour violer les pÃ©rimÃ¨tres de sÃ©curitÃ©. Des emails canulars aux faux sites web, les hackers utilisent le Â« facteur humain Â» pour outrepasser les pÃ©rimÃ¨tres de sÃ©curitÃ© et rÃ©pandre leur charge malveillante directement sur le rÃ©seau. Ainsi, de plus en plus de faux profils vont Ã©merger au sein de rÃ©seaux sociaux sous la forme de jeunes femmes attirantes se faisant passer pour de jeunes recrues Ã la recherche de conseils auprÃ¨s de la gente masculine dâ□□un service IT, ou encore de faux chasseurs de tÃªtes, incitant les employÃ©s Ã dÃ©voiler des informations utiles sans le savoir, et laissant ainsi le champ libre pour perpÃ©trer une attaque. Tandis que la gestion des identitÃ©s en ligne est Ã prÃ©sent Ã©troitement liÃ©e aux rÃ©seaux sociaux, la sophistication des attaques Â« dâ□□ingÃ©nierie sociale Â» va se dÃ©cupler.

6. ProtÃ©ger la chaÃ®ne logistique

Les hackers ont dÃ©ployÃ© une stratÃ©gie similaire en 2012 et en 2013 en ciblant des fournisseurs de technologies (spÃ©cialement dans la sÃ©curitÃ©) dans le but de mettre en place des portes dÃ©robÃ©es ou de dÃ©tourner la sÃ©curitÃ© des clients de lâ□□entreprise. Ces types dâ□□attaques vont sâ□□amplifier en 2014 avec lâ□□augmentation des infiltrations de cyber-attaquants au niveau de la chaÃ®ne logistique, notamment grÃ¢ce Ã lâ□□implantation de codes malveillants dans des logiciels qui seront installÃ©s plus tard sur le rÃ©seau dâ□□une entreprise cible.

7. ContrÃ´ler la maison connectÃ©e

Les chercheurs ont montrÃ© quâ□□on pouvait utiliser les mots de passe codÃ©s en dur et par dÃ©faut comme portes dÃ©robÃ©es de nombreuses entreprises et produits de consommation. Cette annÃ©e, nous verrons les chercheurs (ou les hackeurs) dÃ©montrer avec quelle facilitÃ© on peut hacker les compteurs intelligents grÃ¢ce aux mots de passe par dÃ©faut. De cette maniÃ¨re, les hackers seront en mesure de prendre le contrÃ´le des appareils connectÃ©s dâ□□une maison.

Cela pourrait Ãªtre le cas, par exemple, des compteurs intelligents dâ□□Ã©lectricitÃ© prÃ©sents dans lâ□□ensemble des foyers franÃ§ais, et qui pourraient devenir un point sensible de la sÃ©curitÃ© des citoyens et par extension des entreprises en cas de sÃ©curisation non-adaptÃ©e.

8. Surveiller le crime organisÃ©

La capacitÃ© du crime organisÃ© Ã atteindre le cyber espace nâ□□existe pas quâ□□au cinÃ©ma. 2014 mettra en lumiÃ¨re la capacitÃ© dâ□□organisation des cybercriminels, notamment contre les rÃ©seaux de services rÃ©pressifs, afin de dÃ©rober des informations sur les enquÃªtes en cours dans le but de toujours garder une longueur dâ□□avance sur la loi.

9. Le marchÃ© noir du cyber-espace

Il existe bien un marchÃ© noir pour les cybers criminels oÃ¹ sont mis en vente malwares, outils de piratage ainsi quâ□□un ensemble dâ□□autres outils de hacking du mÃªme type. En 2014, les mots de passes administratifs et les accÃ¨s Ã privilÃ¨ges deviendront les incontournables des marchÃ©s noirs. Nous avons dÃ©jÃ pu le constater en 2013 lors de la mise en examen du hacker et entrepreneur du marchÃ© noir Andrew James Miller. Il y a fort Ã parier quâ□□une telle manne financiÃ¨re dÃ©cuple les efforts des hackers pour sâ□□emparer de toutes ces informations sensibles et confidentielles de grande valeur.

10. Temps nuageux Ã venir

Ce nâ□□est quâ□□une question de temps avant quâ□□un fournisseur de services Cloud ne soit lui aussi victime dâ□□une attaque ciblÃ©e Ã grande Ã©chelle causant ainsi un temps dâ□□arrÃªt et des perturbations majeures. La prÃ©vention reste donc de mise. Par Jean-Christophe Vitu, Professional Service Manager North Europe & Africa chez CyberArk