Barracuda : La sÃ©curitÃ© informatique en 2012, les menaces
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 11/1/2012 13:00:00

2012 - Regardons dans la boule de cristal de la sÃ©curitÃ© Informatique!. Il yÂ a eu de **nombreux changements dans l'industrie de la sÃ©curitÃ© informatique** depuis la crÃ©ation du premier virus en 1971.

Les menaces virtuelles ont Ã©voluÃ© afin de s'adapter aux changements du monde de l'entreprise, oÃ¹ l'on est passÃ© du stockage sur disquettes 3.5 pouces au Cloud Computing, proposant un dÃ©bit bien plus Ã©levÃ©.

Ces quarante derniÃ¨res annÃ©es nous ont montrÃ© que le secteur de la sÃ©curitÃ© informatique devrait perpÃ©tuellement faire face Ã de nouveaux challenges au lieu de devancer la criminalitÃ© virtuelle. Il y a une foule de facteurs que les entreprises devraient prendre en compte, voici donc 8 questions qui devraient Ãªtre au top 10 des interrogations des dÃ©partements IT en 2012 :

1- La guerre criminelle continue dans le monde entier :

Les attaques des Cyber Criminels ont Ã©voluÃ© d'attaque d'ordinateurs personnels Ã des attaques bien plus ciblÃ©es, organisÃ©es par des Cyber Criminels, des activistes ou encore des hackers ou pire encore, d'autres pays essayant de voler des secrets d'Ã©tats. Tant et si bien que le soucis est remontÃ© Ã la tÃªte des Ã tats, qui maintenant placent le crime virtuel au mÃªme niveau que le terrorisme International !

Plus tÃ´t cette annÃ©e, le gouvernement franÃ§ais a Ã©tÃ© victime d'une attaque virtuelle majeure, venant de jeune hackers qui avaient utilisÃ© une adresse Internet Chinoise. L'infraction, qui ciblait des documents d'affaires Ã©conomiques internationales, a Ã©tÃ© considÃ©rÃ©e comme une attaque nationale et a Ã©tÃ© Ã©talÃ©e dans la presse. Afin de contrer ce type d'attaques en 2012, le gouvernement franÃ§ais a triplÃ© le budget de l'Anssi pour atteindre 90 millions d'euros. Afin de remporter un tel dÃ©fi, l'Anssi devra s'entourer des meilleurs fournisseurs de sÃ©curitÃ© afin de dÃ©velopper des solutions pour faire face aux derniÃ¨res menaces virtuelles.

Les fournisseurs de sÃ©curitÃ© et le gouvernement ont du pain sur la planche afin d'obtenir les niveaux de sÃ©curitÃ© suffisants dans les diffÃ©rentes rÃ©gions. Beaucoup d'entreprises demandent aujourd'hui quels sont les sources et les sites Internet dans lesquels ils peuvent avoir confiance. Plus de restrictions et la mise en place de clÃ©s personnelles vont devenir des solutions essentielles pour Ã©viter que de tels soucis reprennent en 2012.

2- Le dÃ©ploiement du Cloud en perspective - les problÃ¨mes liÃ©s Ã la sÃ©curitÃ© avec.

Les fournisseurs de SaaS (Software as a service) et PaaS (Platform as a service) sont souvent considÃ©rÃ©s comme plus sÃ©curisÃ©s que des systÃ¨mes traditionnels, car l'information est stockÃ©e Ã distance, dans le nuage. Aussi, le cloud gagne en rÃ©putation auprÃ©s des entreprises franÃ§aises dans lesquelles il y a eu beaucoup de faille de systÃ¨me. Google a Ã©tÃ© forcÃ© de s'excuser auprÃ¨s de ses clients, mondialement, lorsque son service Gmail s'est effondrÃ©. Salesforce.com a aussi Ã©tÃ© victime d'une attaque virtuelle en 2007 en forÃ§ant les utilisateurs Ã rÃ©vÃ©ler leur mot de passe.

Au fur et Ã mesure que le Cloud computing gagne en rÃ©putation, il devient une cible privilÃ©giÃ©e pour les cyber-criminels qui cherchent Ã dÃ©rober des informations contre paiement. L'analyste David Bradshaw du groupe IDC rÃ©sume parfaitement la situation : Â« Le plus riche est la base de donnÃ©e, au plus de moyens le fournisseur de Cloud doit fournir pour les protÃ©ger. Â» Le conseil aux entreprises utilisant le Cloud est de suivre les recommandations de David.

3- Le vol de donnÃ©es par les employÃ©s va augmenter.

Les affaires juridiques concernant le vol des donnÃ©es par des employÃ©s sur leur lieu de travail ont considÃ©rablement augmentÃ© selon le cabinet AMW. Cette tendance est malheureusement due, pour parti, Ã la crise Ã©conomique actuelle, qui met une pression financiÃ¨re sur le dos des employÃ©s suite Ã la perte de leur emploi. Dans une Ã©tude rÃ©cente, 42% des dÃ©cisionnaires IT considÃ¨rent que les employÃ©s, rÃ©cemment licenciÃ©s, reprÃ©sentent une menace pour la sÃ©curitÃ© des donnÃ©es de l'entreprise, menace bien plus Ã©levÃ©e que celle d'une attaque extÃ©rieure potentielle. Se tourner vers des technologies de sÃ©curitÃ© et contrÃ´ler les accÃ¨s USB/VPN est indispensable en 2012 pour les entreprises qui souhaitent se prÃ©munir.

4- Un nouveau type de hackers dÃ©diÃ© Ã tester la sÃ©curitÃ© des entreprises et des gouvernements.

Une nouvelle gÃ©nÃ©ration de hackers est dÃ©diÃ©e Ã l'attaque des entreprises et des gouvernements en 2012. Ã la diffÃ©rence des hackers d'autrefois, ces nouveaux hackers ont grandi avec les toutes derniÃ¨res nouveautÃ©s technologiques. Ceci les rend encore plus dangereux. De plus, beaucoup d'entres eux ont des motivations plus politiques que financiÃ¨res. Le pire Ã©tant que ces groupes gagnent chaque jour en popularitÃ©. En France le piratage a augmentÃ© de 29% en 2011 et la tendance indique que ces chiffres ne vont pas diminuÃ©s en 2012.

Le groupe d'activistes Anonymous a aujourd'hui des membres dans le monde entier. Le groupe a entrepris de l'Hacktivisme au niveau international avec le but de promouvoir la libertÃ© d'expression et la libertÃ© sur Internet. Le mois dernier, le groupe a rendu public des donnÃ©es qu'ils disent avoir volÃ© au groupe de dÃ©fense AmÃ©ricain Booz Allen Hamilton. Le dossier qui contient plus de 90 000 adresses emails, avec leurs mots de passe, noms d'utilisateurs et toutes les informations qui y sont relatives, a Ã©tÃ© mis en ligne sur le site de partage Pirate Bay. Les dÃ©partements IT doivent rester vigilants et alerter les autoritÃ©s s'ils pensent avoir Ã©tÃ© victimes d'un de ces groupes.

5- Les Smartphone sont des outils professionnels indispensables mais sont aussi un vrai casse-tÃªte pour la sÃ©curitÃ©.

La distribution des numÃ©ros de tÃ©lÃ©phone portable est en hausse constante. Il y a aujourd'hui plus de 5 milliards de forfaits tÃ©lÃ©phoniques dans le monde. C'est presque 5 fois le nombre de PC! Les employÃ©s utilisent de plus en plus leur tÃ©lÃ©phone portable pour accÃ©der au rÃ©seau de l'entreprise, laissant ainsi les dÃ©partements IT fassent Ã des soucis de sÃ©curitÃ© sur comment protÃ©ger les donnÃ©es relatives Ã l'entreprise. Il est intÃ©ressant de noter que plus de la moitiÃ© des utilisateurs de Smartphone pensent que la sÃ©curitÃ© de leur appareil n'est pas de leur ressort et que lorsqu'ils reÃ§oivent un virus, ils incriminent leur opÃ©rateur, qui selon-eux ne les protÃ¨ge pas suffisamment. En le sachant, en 2012, les entreprises ont besoin de dÃ©cider comment limiter l'accÃ¨s via les mobiles (avec un risque de limiter la productivitÃ©) ou de cloisonner leurs rÃ©seaux - ou mieux d'utiliser une combinaison des deux.

6- Les applications mobiles - Un danger grandissant pour les entreprises et les particuliers.

Le dernier rapport de sÃ©curitÃ© sur les mobiles nous montre que 69% des utilisateurs de Smartphones sont catÃ©goriques sur le fait que les failles autour de la vie privÃ©e sur leur Smartphone sont inacceptables, aujourd'hui plus des Â¾ d'entres eux n'ont pas lu les conditions gÃ©nÃ©rales relatives au tÃ©lÃ©chargement sur iTunes ou l'Android Market.

Des jeux trÃ¨s populaires, comme Angry Birds, sont connus pour accÃ©der aux informations privÃ©es des utilisateurs (dont la position gÃ©ographique, le nom....) et pour les partager avec de tierces personnes, entreprises, dont des publicitaires. Publicitaires qui considÃ¨rent ceci comme normal car l'application est gratuite ou Ã prix rÃ©duit, mais si les utilisateurs n'ont pas lu les conditions gÃ©nÃ©rales de vente de l'application, ils ne sont probablement pas au courant des risques qu'ils ont prit. MÃªme si les risques liÃ©s Ã ce genre de pratiques sont de moins en moins frÃ©quents, les utilisateurs de Smartphones (et les entreprises pour lesquels ils travaillent) doivent faire de plus en plus attention aux risques et mettre en place des moyens afin de protÃ©ger leurs donnÃ©es.

7- Les gouvernements devraient jouer un plus grand rÃ´le dans la protection des particuliers et des entreprises.

En France, **le gouvernement a lancÃ© un site dÃ©diÃ©** Ã l'information du grand public en matiÃ¨re de risques liÃ©s Ã la sÃ©curitÃ© informatique et aux moyens mis en place pour les Ã©viter . Les particuliers et les entreprises doivent tirer parti des informations disponibles sur ces supports pour rester informÃ©s des risques et solutions disponibles.

8- Les rÃ©seaux sociaux Ã la source de nouveaux risques en 2012.

La popularitÃ© des mÃ©dias sociaux, mÃªme en entreprise, amÃ¨ne de nouveaux risques et rendent les entreprises vulnÃ©rables. Quand les virus traditionnels ennuient les utilisateurs en dÃ©truisant leurs donnÃ©es, il y a de nouvelles menaces qui elles sont liÃ©es au vol d'identitÃ© virtuelle et au vol d'informations personnelles.

Les virus les plus sophistiquÃ©s aujourd'hui sont dÃ©veloppÃ©s dans le but de mettre hors service les anti-virus traditionnels. Limiter l'utilisation de ces rÃ©seaux sociaux en entreprises limite les risques liÃ©s Ã ces derniers et sera probablement une solution essentielle pour cette nouvelle annÃ©e.