Bee Ware : les menaces Web de l'annÃ©e 2013
Internet
PostÃ© par : JPilo
PubliÃ©e le : 1/2/2013 13:00:00

Expert en sÃ©curitÃ© applicative et spÃ©cialiste de la sÃ©curisation des flux HTTP, **Bee Ware** revient sur les Ã©volutions techniques dÃ©veloppÃ©es en 2012 entraÃ®nant, pour 2013, de **nouveaux risques sÃ©curitaires.**

L'avÃ¨nement du BYOD

PhÃ©nomÃ¨ne Ã©mergeant de l'annÃ©e 2012, le BYOD (Bring Your Own Device) lÃ©gitimise l'utilisation d'Ã©quipements personnels (ordinateurs portables, Smartphones, etc.) au sein de l'entreprise. Cet accÃ¨s permanent aux ressources professionnelles (agenda, mails, fichiers, etc.) est aujourd'hui devenu indispensable aux organisations qui souhaitent maintenir leur compÃ©titivitÃ©.

Ouvrir ainsi des terminaux personnels au monde professionnel engendre nÃ©anmoins de sÃ©rieux risques d'usurpation d'identitÃ© et de vol de donnÃ©es... Ayant accÃ¨s Ã de nombreuses applications internes sensibles, ces terminaux reprÃ©sentent une possibilitÃ© de rebond parfait Ã destination des systÃ¨mes d'information. Une personne malveillante pourra de ce fait infiltrer l'un de ces terminaux et accÃ©der Ã l'ensemble des donnÃ©es classÃ©es confidentielles de l'entreprise (rapports financiers, propriÃ©tÃ© intellectuelles, etc.).

Bien que de plus en plus banalisÃ©, le BYOD reste aujourd'hui complexe Ã encadrer : rÃ©vision des politiques de sÃ©curitÃ© internes, dÃ©ploiement d'outils sÃ©curitaires adaptÃ©s, Ã©vangÃ©lisation des utilisateurs, etc. Les risques de perte et de vol, conjuguÃ©s Ã la recrudescence d'attaques visant ces pÃ©riphÃ©riques mobiles, feront de ce phÃ©nomÃ¨ne l'une des principales prÃ©occupations des RSSI en 2013.

La dÃ©mocratisation du Cloud Computing

Autre phÃ©nomÃ¨ne Ã©mergeant de ces derniÃ¨res annÃ©es, le Cloud Computing consiste Ã dÃ©porter tout ou partie de vos donnÃ©es et de vos applications sur des serveurs distants. Encore relativement flou pour la majoritÃ© de ses usagers, le Cloud Computing englobe diffÃ©rents types de services utiles aux entreprises :

â¢ La disponibilitÃ© des donnÃ©es sur le rÃ©seaux (DaaS)

â¢ La virtualisation de l'infrastructure (IaaS)

â¢ L'hÃ©bergement d'applications (SaaS)

â¢ Etc.

TrÃ¨s simple d'utilisation, ce concept repose sur le dÃ©veloppement d'APIs, ou interfaces de programmation, permettant de dÃ©lÃ©guer le traitement des donnÃ©es en dehors de leur infrastructure d'origine. Bien qu'il existe d'ores et dÃ©jÃ de nombreuses solutions de sÃ©curitÃ© dÃ©diÃ©es, le Cloud Computing demeure une cible privilÃ©giÃ©e pour accÃ©der aux donnÃ©es sensibles de l'entreprise...

Les APIs, socle commun des technologies de derniÃ¨re gÃ©nÃ©ration

Les APIs constituent le socle commun du BYOD et du Cloud Computing. Ces fonctions, permettant d'accÃ©der aux services d'une application, mettent Ã disposition des utilisateurs des informations de faÃ§on plus ou moins standardisÃ©e (via les langages XML, JSON, etc.). Interfaces directes avec le coeur du systÃ¨me d'information, elles peuvent assurer l'authentification et la gestion des autorisations associÃ©es mais restent vulnÃ©rables Ã de nombreuses attaques :

â¢ Etant liÃ©es entres elles, un dÃ©faut peut entrainer un disfonctionnement en chaine sur d'autres APIs et provoquer d'importants problÃ¨mes de disponibilitÃ©

â¢ Le plus souvent basÃ©es sur le protocole HTTP, elles subissent les mÃªmes types d'attaques que les applications Web (injections SQL, cross-site scripting, DDOS)

â¢ Etc.

OmniprÃ©sentes dans les technologies de derniÃ¨re gÃ©nÃ©ration, ces APIs ne peuvent Ãªtre protÃ©gÃ©es par les protections rÃ©seaux habituellement mises en place... Plus complexes et accessibles via diffÃ©rents consommateurs (navigateurs, pÃ©riphÃ©riques mobiles), elles nÃ©cessitent le dÃ©ploiement de filtrages applicatifs spÃ©cifiques pour garantir un niveau de sÃ©curitÃ© optimal.

Le top 5 des menaces Web 2013

Outre les risques Ã©voquÃ©s ci-dessus, l'annÃ©e 2013 verra le nombre de SPAM/SCAM et les attaques visant les navigateurs Web se multiplier : En constante Ã©volution, les tentatives de phishing (techniques utilisÃ©es pour obtenir des renseignements personnels en vue d'usurper l'identitÃ© d'une personne) augmenteront et seront malheureusement de plus en plus perfectionnÃ©es...

Les problÃ¨mes liÃ©s aux applications Flash, Java et autres accÃ©lÃ©reront le dÃ©ploiement du langage de programmation HTML5 (langage permettant l'affichage de pages Web), extrÃªmement ergonomique mais sujet Ã de nombreuses failles de sÃ©curitÃ©...

Matthieu Estrade, directeur Technique de Bee Ware et spÃ©cialiste en sÃ©curitÃ© informatique nous rÃ©sume en 5 points les principales menaces Web de 2013 :

â¢ Les malwares et les attaques visant les pÃ©riphÃ©riques mobiles : "Le remplacement du poste de travail rÃ©volutionne l'usage des applications d'entreprise et se dÃ©mocratise Ã l'insu des rÃ¨gles de sÃ©curitÃ© Ã©tablies... Cette problÃ©matiques reprÃ©sente pour les RSSI la premiÃ¨re source de menace de l'annÃ©e 2013"

â¢ Les attaques visant les navigateurs Web : "TrÃ¨s vite adoptÃ© par les dÃ©veloppeurs d'applications Web, le langage HTML5 connaitra un succÃ¨s grandissant au cours des prochains mois. Cette utilisation prÃ©coce (NB: la finalisation de ses spÃ©cifications n'est officiellement prÃ©vue qu'en 2014) dÃ©bouchera nÃ©cessairement sur de nombreuses failles de sÃ©curitÃ©..."

â¢ L'abus de fonctionnalitÃ© des APIs : "Rarement standardisÃ©es, les APIs dialoguent directement avec le coeur du systÃ¨me d'information des SociÃ©tÃ©s. DÃ©veloppÃ©es au travers de Framework plus ou moins sÃ©curisÃ©, ces APIs reprÃ©sentent un danger encore mÃ©connu."

â¢ Le vol de donnÃ©es sensibles dans le Cloud : "TrÃ¨s facile d'utilisation, le Cloud hÃ©berge un nombre considÃ©rable de donnÃ©es sensibles et restera en 2013 la cible privilÃ©giÃ©e des hackers. La dÃ©localisation des applications n'implique en aucun cas une diminution des risques d'attaques..."

â¢ Le phishing et vol de donnÃ©es bancaires : "Le contexte Ã©conomique dans lequel nous Ã©voluons actuellement influence Ã©galement le monde de la sÃ©curitÃ© Web... En pÃ©riode de crise, le volume de SPAM/SCAM destinÃ©s Ã rÃ©cupÃ©rer des informations bancaires ou Ã usurper des identitÃ©s se dÃ©veloppe de plus en plus..."