La valeur ajoutée du test d'intrusion

S'il y'a une chose sur laquelle tout le monde s'entend, c'est l'augmentation croissante du nombre d'attaques de sécurité. Ceci s'explique en partie par le nombre grandissant de systèmes et d'utilisateurs interconnectés. Fraude, cyber espionnage, vol d'identité, les motivations varient et les auteurs de ces attaques sont de mieux en mieux organisés. Beaucoup d'entreprises, de tous gabarits, sont ciblées ou choisies au hasard pour des actes de piratage informatique.

Selon *techradar.com* : « Indeed, research commissioned by the Department for Business, Innovation and Skills last year found that 93 per cent of large businesses in the UK suffered a computer security breach in the previous 12 months, while 87 per cent of small businesses also suffered attacks. »

Chaque année le rapport "Internet Security Threat Report " produit par Symantec ainsi que le rapport DBIR "Data Breach Investigation Report" par Verizon en collaboration avec une cinquantaine d'organisations, Publient des statistiques intéressantes sur les types de menaces et leurs occurrences. En examinant ces rapports nous arrivons vite à la conclusion que les attaques sont de plus en plus nombreuses et les fuites de données abondantes. Même son de cloche du côté de l' ITRC (Identity theft ressource center) qui compile les violations de données rapportées depuis 2005. Même si les chiffres et statistiques de ces rapports sont faramineux, ils ne représentent que les violations et attaques détectées et rapportées. Ces chiffres ne sont qu'un indicateur de la situation globale.

Je dégage ici quelques faits qu'il me semble intéressant de partager.

- 232M de fuites d'identité (connues) en 2013 soit 4 fois plus qu'en 2012.
- Dans les faits, 72% des violations de données investiguées par l'unité " Verizon Communications' forensic analysis" ciblaient des compagnies de moins de 100 employés
- Un record de 23 0days (Failles non connues et non corrigées par le fournisseur) ont été découvertes en 2013 et utilisées dans des attaques de type watering hole («Infection par site Web », autrement appelée «Drive-By Download »).
- Les attaques sont de plus en plus sophistiquées et les attaquants de plus en plus déterminés.
- Selon le rapport Symantec, 1 site sur 8 souffre d'une vulnérabilité critique non corrigée
- 568 700 attaques web bloquées en 2013 versus 464 100 en 2012
- De plus en plus d'attaques visent les utilisateurs d'appareils mobiles
- Les appareils Android sont touchés par 97% des menaces ciblant les mobiles

La liste pourrait s'allonger encore et encore. Vous vous demandez où je veux en venir avec tous ces chiffres et statistiques. En fait, je tente de dégager une image globale de l'état actuel de la sécurité des entreprises. L'analyse des données contenues dans ces rapports, nous permet de comprendre dans quelle proportion les entreprises risquent d'être attaquées et par quels types de menaces. Un

regard sur les années passées, nous aide à anticiper les menaces contre lesquelles nous devrons nous protéger. Une attention particulière devrait être accordée aux appareils mobiles qui sont principalement ciblés par les développeurs de malwares. Même si le nombre de menaces peut sembler énorme, 100 000 incidents analysés sur une période de 10 ans révèlent que 92% des incidents peuvent être regroupés en 9 modèles :

- Intrusions en point de vente
- Cyber-espionnage
- Attaques d'application Web
- Abus de privilèges
- Erreurs diverses
- Logiciels criminels
- Fraudes à la carte bancaire
- Vols physiques et fuites de données
- Attaques par déni de service

Je vous entends maintenant dire « Quel est le lien avec le titre de cet article ? »

Ce à quoi je réponds;

Vous vous dites que je prêche pour ma paroisse et vous n'avez pas tort. Toutefois, si un test d'intrusion et/ou de vulnérabilités applicatives était systématiquement effectué à certaines étapes du développement et du déploiement, bon nombre de failles ne passeraient pas le filet (par ex. Heartbleed). Même chose pour les autres éléments de l'infrastructure. Je ne cherche pas à vous dire qu'il faille effectuer des tests d'intrusion sur tout et continuellement mais si la sécurité est adressée dès le départ, nous obtiendront une infrastructure et une application avec des contrôles de sécurité adéquats. Ce sont ces contrôles que doit cibler un test d'intrusion. Bien-sûr, un test d'intrusion n'est pas une pilule anti-piratage et certains types d'attaques ne pourront pas être évités par celui-ci (DDOS, Watering Hole). Néanmoins, il s'agit d'une valeur ajoutée pour protéger vos actifs et réduire vos risques d'entreprise.

Certaines entreprises ne voient pas la nécessité d'investir sur un projet difficilement quantifiable. Comment justifier le coût du test d'intrusion? La réponse se trouve dans la question suivante : Votre entreprise peut-elle faire face, entre autres) au risque de perte de confiance de ses clients? Et à combien se chiffre ce risque?

Bien que de très grandes entreprises (iPhoneDevSDK, Facebook, Twitter, Apple, and Microsoft curieusement toutes en février 2013 (DBIR)) ont faits les frais de pirates et ont dû rapporter des violations. Les dernières données indiquent une augmentation significative des attaques sur les entreprises de plus petite taille. La fausse impression de sécurité peut-être trompeuse pour une entreprise, un jour ou l'autre ses systèmes seront sous attaques. Rappelez-vous, il y a mille et une bonnes raisons pour pirater vos données.

Dany Ouellet OSCP, MCSA security, Comptia Sec +

www.securecom.ca
T : 514 544-0442
Contact : info@securecom.ca

SECURECOM Services Conseils inc.