

THÉMA TEST D'INTRUSION



DES « FANS » DES TESTS D'INTRUSION AUX NÉOPHYTES...



Raphaël Illouz, NES

Raphaël Illouz, DG de NES, distingue deux types de comportement vis-à-vis de la SSI. La première catégorie concerne les sociétés pour lesquelles la culture de la sécurité est ancrée depuis des années et pour lesquelles il constate une réelle évolution de la sécurité d'années en années. Ces sociétés, principalement dans

le domaine BFA, possèdent une équipe dédiée à la sécurité et réalisent des tests d'intrusion sur leur système d'information plusieurs fois dans l'année. Le niveau de sécurité de leur SI a donc globalement augmenté, malgré la publication de plus en plus croissante de vulnérabilités, dans le domaine applicatif notamment.

En ce qui concerne la seconde catégorie, la prise de conscience de la sécurité est bien réelle, mais elle n'offre que peu d'importance à l'élévation du niveau de sécurité de leur SI. Ainsi, elle ne souhaite pas attribuer de budget, ni même aux équipes dédiées à la sécurité quand il y en a. Cette situation se traduit par une stagnation, voire une baisse du niveau de sécurité au niveau des infrastructures (réseau, système), mais aussi et surtout au niveau applicatif, qui représente à ce jour 80% des points d'entrées dans le système d'information interne dans le cadre d'un test d'intrusion externe. C'est un peu le même constat pour



Frédéric Charpentier, XMCO Partners

Frédéric Charpentier, Directeur Technique d'XMCO Partners, « le niveau de sécurité s'est amélioré pour les entreprises qui ont déjà effectué des tests d'intrusion en 2008/2009. Par contre, il est faible pour celles qui réalisent leur premier test d'intrusion. Il identifie plusieurs tendances positives et négatives d'après les résultats

de centaines de tests d'intrusion réalisés en 2010 (ban-

ques, assurances, industriels) :

Tendances positives :

- Le patch management des systèmes Microsoft Windows est désormais adopté par les entreprises.

- Les entreprises emploient de plus en plus de frameworks applicatifs (Struts, Hibernate, ...) pour le développement de leurs applications Web. Ces frameworks proposent des bases très solides en termes de sécurité.

Tendances négatives :

- La présence de mots de passe par défaut sur les interfaces d'administration est toujours aussi répandue qu'en 2008/2009, en particulier sur les briques applicatives tierces.

- La responsabilité de la sécurité est de plus en plus diluée entre les différents acteurs : équipe production, agence Web, développeurs, DBA, hébergeur, PSP, etc. Nous constatons lors des soutenances de tests d'intrusion qu'il est difficile pour le RSSI d'obtenir un inventaire et une vision globale de la sécurité de tous les composants d'une plateforme donnée. Rappelons-le, les pirates informatiques ne ciblent pas une couche en particulier, ils cherchent la faille la plus facile à exploiter, quelle qu'elle soit. Le modèle de défense en profondeur basé sur des DMZ successives, selon une analogie militaire, ne s'applique plus aujourd'hui.

- Les entreprises déploient désormais des Web Services (architecture SOA), accessibles sur le Web, qui permettent à leurs partenaires d'accéder à des applications et à des données métier. Ces Web Services sont encore très peu sécurisés. Nous l'avons clairement constaté en 2010 dans nos tests d'intrusion orientés Web Services ».

PENETRATION TESTING

PENETRATION TESTING: TWO-TIER SECURITY

INTERVIEW BY MARC JACOB AND EMMANUELLE LAMANDÉ



French enterprises have two-tier security levels, according to our nine experts in penetration testing. If for some, they see a marked improvement, for others, especially those who undertake tests for the first time, the situation is rather alarming ...