Tests d'intrusion ou tests de pénétration

Dans un contexte grandissant des attaques de cybersécurité et en application de la directive du Secrétariat du Conseil du trésor sur la nécessité de mettre en place un plan de détection des vulnérabilités (NVD19), les tests d'intrusion (ou test de pénétration) sont maintenant un prérequis à l'obtention de la certification Trousse globale de vérification (TGV) pour tous les produits ou services technologiques utilisant des données personnelles, de santé et de services sociaux.

Ces tests doivent être réalisés par des prestataires de services indépendants dans le domaine de la cybersécurité et de la protection des renseignements personnels qui sont spécialisés dans les tests d'intrusions et de vulnérabilités.

Considérant la complexité liée à la réalisation de tests d'intrusion de qualité, le Bureau de certification et d'homologation (BCH) fournit dans les sections suivantes quelques orientations à suivre par le fournisseur du produit ou service technologique (PST) pour l'aider dans son choix de prestataire de service et à bien définir la portée des tests.

Couverture ou portée des tests d'intrusion :

1- Les tests d'intrusion doivent être inspirés des standards reconnus, des meilleures pratiques du domaine, des techniques éprouvées garantissant des tests réalistes et pertinents (ex. : National Vulnerability Database (NVD), Open Web Application Security Project (OWASP), Open Source Security Testing Methodology Manual (OSSTMM), National Institute of Standards and Technology (NIST), etc.).

2- Les tests doivent être réalisés dans un environnement de production ou un environnement équivalent à l'environnement de production.

3- Tous les rôles[1] (acteurs du système) doivent être identifiés et testés dans leur contexte d'utilisation prévue, et ce, qu'ils soient accessibles depuis le Web ou non.

   a. Test en boîte blanche (acceptée dans tous les cas).
   b. Test en boîte grise acceptée seulement dans le cas de certains PST non sensibles et pour lesquels il n'est pas prévu un déploiement provincial.
   c. ~~Test en boîte noire~~ (non acceptée par le BCH, donc à éviter si on veut obtenir certification TGV).

4- Identifier et tester toutes les failles en lien à des mises à jour logicielles non effectuées.

5- Identifier et tester les vulnérabilités en lien avec le mode de déploiement du PST.

   a. Installé dans l'environnement du client (ex. test applicatif).

---

[1] Un test d'intrusion peut inclure des tests en boîte noire, en boîte grise ou en boîte blanche.

1. Boite noire : tests permettant de déterminer si les mécanismes de sécurité en place sont fonctionnels et de s'assurer qu'aucune erreur évidente n'est présente. Ils sont donc en lien avec la surface d'attaque accessible à n'importe quel attaquant externe.
2. Boite grise : Boite noire + tests visant à déterminer si les mesures de sécurité s'exécutent comme il se doit. Pour cela, il faut vérifier des éléments disponibles à des clients, des partenaires ou des salariés d'une entreprise.
3. Boite blanche : Boite grise + confirmation sur une base continue et cohérente. Ce test permet d'analyser le niveau de sécurité en disposant des mêmes accès qu'un administrateur du système.

b. Hébergé par le fournisseur (ex. : test sur son réseau).
c. Hébergé dans un environnement infonuagique (ex. : service infonuagique).

6- Identifier les vecteurs d'attaque (points d'entrée) possibles en fonction des criticités du PST (plateforme Web, applications mobiles, infrastructures et réseaux, etc.) et monter des scénarios de tests pour détecter les vulnérabilités.
7- Toute autre vérification jugée pertinente pour aider à la découverte de vulnérabilités dans l'utilisation du PST.

Caractéristiques des prestataires de services (firmes) autorisés par le BCH

Le BCH acceptera les résultats des tests d'intrusion ou tests de pénétration provenant uniquement d'un prestataire de service répondant minimalement aux exigences suivantes :

1. avoir des représentants légalement autorisés au Canada;
2. être minimalement spécialisé en cybersécurité et en protection de renseignements personnels avec du personnel possédant des certifications reconnues en test d'intrusion ou de vulnérabilités;
3. être en mesure de fournir des preuves d'antécédents criminels pour le personnel effectuant lesdits tests parce qu'ils sont appelés à accéder à de l'information extrêmement sensible;
4. être responsable et imputable des résultats desdits tests qu'elle utilise les services de sous-traitants ou non;
5. être en mesure, avec l'accord de son client, de fournir sans frais le rapport des tests en français au BCH;
6. être en mesure de réaliser des tests dans un environnement de production ou un environnement équivalent en tenant compte des risques ou enjeux d'affaires du client.

Caractéristiques d'un rapport de test d'intrusion

Le rapport d'un test d'intrusion ou de pénétration doit permettre au BCH d'appuyer ses décisions relatives à l'acceptation ou non du PST. Dans ce contexte, le rapport doit présenter minimalement les informations suivantes :

1. contexte - Objectifs et Portée du test d'intrusion;
2. méthodologie d'évaluation des risques et d'identification des vulnérabilités;
3. description de chacun des tests effectués, concluants ou non, et les résultats obtenus;
4. documentation détaillée de chaque vulnérabilité identifiée et risques associés;
5. déterminer et documenter les forces et les faiblesses des mesures de sécurité examinées;
6. documenter les vulnérabilités potentiellement présentes qui n'ont pu être exploitées;
7. recommandations spécifiques aux vulnérabilités majeures ou critiques et recommandations générales;

8. produire une synthèse, de type sommaire de gestion, complet et d'interprétation facile (peut être inclus à même le rapport ou un rapport indépendant).