



Audit de sécurité



Reconnaître les déficiences de sécurité et minimiser efficacement les risques

Le problème

La question primordiale est:
„Ma sécurité est-elle sécurisée?“

Seul des tests systématiques avec les conseils attenants vous éclairciront quand l'usages de termes comme intégrité, confidentialité ou disponibilité sont de rigueur.

L'audit de Sécurité – toujours à la hauteur du challenge.

La demande

Sans doute avez-vous déjà beaucoup lu sur le sujet, voir vous avez suivi un cours ou participé à un séminaire sur la question. Vous avez même sûrement mis des mesures en places pour la sécurité de votre entreprise!

Mais avez-vous déjà tester vos mesures de sécurités par des attaques actives, de façon à juger de l'efficacité de vos contre-mesures en environnement réel?

Notre solution

Nous vous proposons nos services pour la localisation des risques de votre sécurité avec une analyse complète des dangers potentiels et les contres-mesures attenante qui peuvent être intégré dans la police de sécurité de votre entreprise.

- Test de pénétration et Hacking
- Analyse des configurations
- Social Engineering
-

Audit de Sécurité: une sécurité testée

Indépendamment des actions effectuées: il n'existe pas de sécurité à 100%! Cependant, des audits réguliers de votre sécurité vous permettront de vous approcher de ce chiffre. Nos services dans ce domaine vont de l'analyse théorique, en passant par les test des risques connus, jusqu'aux tests de pénétration avec des scénarios d'attaques réalisés par nos spécialistes qualifiés en sécurité. Le contrôle manuel des faiblesses potentielles excluent les « false positive » (sécurité apparentes) et garantissent donc une grande qualité dans l'analyse des risques potentiels.



Reconnaître les déficiences de sécurité

Apparition et cause

Notre expérience dans ce domaine nous permet d'affirmer que la plus part des déficiences dans la sécurité ont les causes suivantes: manquement dans les mises à jour des updates de sécurité des applications et systèmes d'exploitation, installations standards avec une insuffisance dans les paramétrages de sécurité, activation de services qui ne sont pas nécessaires, perte d'intégrité ayant pour origine une insuffisance d'authentification et même la conservation d'utilisateurs standards avec des mots de passes par défaut. Les causes sont bien souvent dues à l'aide à l'installation contenue dans les programmes combinés à la complexité grandissante de l'interaction des programmes.

Une autre déficience de la sécurité provient très souvent de règles et polices de sécurité rendues complexes par le temps ainsi que les modifications dues aux tests et installations provisoires qui ont été réalisés au fil des années et n'ont pas été retirés. NewNet Technology vous propose un check unique ou, dans le cadre d'un contrat de maintenance de façon plus régulière, de réviser et de juger votre dispositif de sécurité.



Des prestations flexibles et modulaires

Par une approche structurée en liaison avec les modules variables de prestation nous garantissons à nos clients une grande flexibilité et qualité dans l'optique de la sécurité de l'entreprise. Les modules sont les suivant :

- **Security BASIC (information Gathering)**

Nous trouvons les portes dérobées – Part des contrôles des accès usuels ou dérobés qu'empruntent les programmes d'attaques et les hackers, nous faisons un premier check des points sensibles des systèmes atteignables. Selon les résultats nous fournissons un catalogue de mesure et les explications attenantes au risques découverts pour vous permettre de prendre les mesures qui s'imposent.

- **Penetration et Hacking**

„On réalise avec succès les attaques!“ – Par des scénarios d'attaques actives, nous analysons les points faibles qui présentent des risques potentiels. Pour cela nous utilisons une quantité non négligeable de tools pour mettre à jour l'intégrité et l'anonymité des systèmes.

- **Analyse des polices**

On a bien mis en place des polices et fait divers tests, mais qu'est-ce qui doit rester ? – Souvent, on teste des connections ou on autorise provisoirement des services, mais êtes vous bien sûre de ne pas avoir oublié d'enlever tout ce qui est inutile et qui fait autant de portes dérobés dans votre système ? Nous vérifions les polices de sécurité après avoir analysé quels sont vos besoins réels et contrôlons que seul ce qui doit passer est autorisé à le faire.

- **Analyse de configuration**

L'analyse des configurations pour mettre à jour le manque de sécurité en local! – Nous vérifions les paramétrages ayant un rapport avec la sécurité, les règles de droits d'accès, les concepts d'authentification et d'encryption ainsi que les droits des utilisateurs externes et internes.

- **Social Engineering**

Il est difficile de croire combien les employés donnent d'informations quand on les aborde de façon convaincante et persuasive. Par exemple, lors d'une attaque par simulation voir d'une demande de mot de passe pour la maintenance. Nous nous infiltrons dans leur confiance en nous glissant dans la peau d'une personne connue ou compétente. Et même dans la peau des instituts de nettoyage pour trouver les mots « passes inscrit sur des Post-Its sous les claviers au autres objets, voir les informations confidentielles, qui finissent dans les corbeilles à papier ! Les résultats garantissent une plus grande attention de la part de vos collaborateurs dans leur vie de tous les jours.

- **Faiblesses repérées – Solutions conseillés**

Les résultats sont condensés dans un rapport écrit sur les problèmes de sécurité et priorisés selon le potentiel de danger qu'ils représentent. De ce rapport résulte les mesures nécessaires à prendre avec les conseils et les solutions pour minimiser les risques. La répétition régulière de l'audit garantie un haut niveau de sécurité.

Sécurité = Processus

La sécurité est à considérer comme un processus dynamique et non comme une solution statique. Seul un contrôle continu et les adaptations des statu quo garantissent un niveau de sécurité suffisant.

Sécurité de l'information

Mais comment?

Avec une analyse des risques pour définir avec succès le dispositif actuel de sécurité.

- Unique – avec l'attaque active en utilisant des scénarios qui ont souvent réussi.
- Périodiquement – par la répétition régulière des attaques pour un plus grand niveau de sécurité.

Les bénéfices

- Repérage des trous dans la sécurité
- Mise à jour des risques d'erreurs
- Minimiser les risques potentiels
- Vérification des concepts de sécurité

Security Assessment Process

