

NOS MODULES D'AUDIT

Analyse - Accompagnement - Sérénité - Sécurité

Audit Technique

Audit des serveurs

Mise à jour, vulnérabilités classiques

Respect des politiques de mots de passe

Contrôle des accès à distance (filtrage)

Contrôle sur les élévations de privilèges

Fuites d'informations (techniques/métier) en local, à partir de profils non privilégiés

Audit niveau de sécurité des postes de travail

Audit du niveau de sécurité globale (Niveau de cohérence des OS, patchs et mises à jour)

Résistances aux attaques par ingénierie sociale. Firewall personnels et/ou HIPS, exfiltration de données

Audit des flux réseaux (les flux critiques sont il chiffrés, évaluer les risques d'écoute par exemple)

Recensement et évaluation de la criticité des flux non chiffrés présents (accès à distance type Telnet, mais aussi applicatif comme du HTTP par exemple)

Vérification de l'impact des attaques man in the middle sur les protocoles chiffrés, évaluation de la solidité des chiffrements, gestion des certificats et cryptographie asymétrique

Audit Organisationnel

Audit de la PSSI

Audit de la PSSI sous forme de document déjà réalisé

Audit de la PSSI sous forme de règles non formalisées

Audit concernant l'exfiltration des données (connexions sortantes et canaux cachés)

Traçabilité et Marquage de l'information

Connexions sortantes

Périphériques amovibles

Segmentation de la donnée sur les serveurs de fichiers ou sur certaines applications à forte connotation métier (qui a accès à quoi ? et dans quelle mesure ces accès sont légitimes)

Applications métier : Perméabilité entre les différents profils

Serveurs de fichiers (Windows), Groupes, ACL et segmentation de l'information

Les échanges de données sont ils correctement effectués ou sont ils trop laxistes

Audit Organisationnel

Traçabilité des événements (accès aux données par ex)

Présence de logs, niveau de détail et pertinence

Sauvegarde des logs et intégrité de ceux-ci

Capture d'information par des éléments réseaux autres que ceux qui contiennent l'information (par exemple en cas de compromission avancé cela permet d'avoir une meilleure garantie de l'intégrité des logs)

Audit/Vérification PCA/PRA

Vérification de la fréquence, et de l'intégrité des sauvegardes. Vérification de la cohérence des données sauvegardées

Simulation de mise en situation réelle du PRA/PCA, réplication sur les serveurs de secours, et évaluation du temps de remise en services réel

Audit « théorique » de l'architecture et/ou des choix technologiques

Audit des applicatifs internes

Audit des applicatifs internes et développements internes (intranet par exemple, ou autre logiciels réalisés/maintenus en interne)

Test applicatif sur les logiciels internes (intrusif non exhaustif)

Audit du code source des logiciels internes (vulnérabilités classiques : buffer Overflow, injection SQL, XSS, mais aussi chiffrement, authentification, bugs algorithmiques)

Sylvain Martin, Directeur Commercial
Mail : Sylvain.Martin@nbs-system.com



NBS System
140 Boulevard Haussmann
75 008 Paris
Tel : 01.58.56.60.80, Fax : 01.58.56.60.81

<http://www.nbs-system.com>