

Maîtriser l'impact des technologies sur la sécurité du système d'information

Audits Techniques de Sécurité

Avant de s'engager dans des projets lourds et structurants, il faut s'assurer de la maturité des technologies sous-jacentes les plus critiques. Les consultants de Bull proposent d'assister leurs clients pour analyser l'impact des technologies sur la sécurité de leur S.I. et déterminer le niveau de confidentialité, d'intégrité et de disponibilité des solutions dont ils ont besoin.

Les consultants et experts de Bull Réseau et Sécurité accompagnent leurs clients dans tous les processus d'évaluation des risques liés aux technologies.

Audits d'architecture

L'objectif est d'obtenir un diagnostic de la sécurité d'une plate-forme ou solution : définir les points faibles et forts des maillons composant la chaîne applicative, recenser, qualifier les vulnérabilités, trouver les parades techniques pour y remédier.

Tests de vulnérabilité

Ils permettent de lister les failles présentes sur une ou plusieurs « machines » (serveur, routeur, etc.). Ils peuvent être effectués en interne ou en externe et être réalisés sur une seule cible jusqu'à plusieurs milliers.

Tests d'Intrusion

Ils visent à qualifier le niveau de sécurité du système d'information depuis l'extérieur ou l'intérieur de l'entreprise. Ils s'appuient sur une méthodologie rigoureuse pour garantir des prestations de qualité constante, assurant le non-débordement, la traçabilité des actions menées, le bon niveau des livrables, etc.

Audits de code

La « relecture » du code source d'une application sous l'angle de la sécurité permet d'identifier :

- Les techniques de programmation n'assurant pas une sécurité suffisante ;
- La présence de vulnérabilités susceptibles d'entraîner des problèmes de sécurité.

Les mauvaises pratiques de programmation sont ainsi relevées. L'audit de code permet aussi de vérifier l'absence de « porte dérobée », déposée intentionnellement ou non dans l'application.

Bull Réseau et sécurité, la maîtrise de la complexité

Bull Réseau et Sécurité est une entité qui regroupe, au sein d'une même communauté d'experts, les compétences nécessaires pour accompagner de bout en bout les entreprises dans la conception, la réalisation et l'exploitation de leurs infrastructures de communication. Son objectif : proposer des solutions conciliant haute technicité et services d'accompagnement pour aider les entreprises à maîtriser la complexité de leurs nouvelles infrastructures complexes.

BULL RESEAU ET SECURITE



Architect of an Open World™

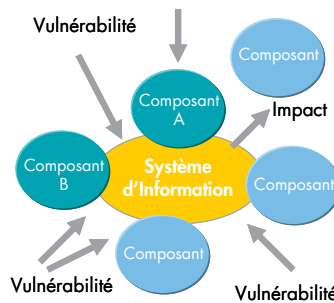
Audits d'architecture et de configuration

Les audits d'architectures techniques s'appuient sur des modules intégrés dans une offre de gestion du risque : V2SI (Validation de la Sécurité du Système d'Information).

Nos experts analysent l'architecture technique de la solution du point de vue sécuritaire pour identifier d'éventuelles failles de conception. Par exemple, dans le cadre d'une application Extranet, les points suivants seront abordés :

- système d'authentification
- architecture « back-office »
- architecture du système DNS
- architecture connexions Internet
- architecture des DMZ
- mécanismes de chiffrement.

Chaque composant sensible de l'architecture est ensuite analysé brique par brique.



L'analyse de configuration

Élément clef de l'audit d'architecture, elle permet de détecter les vulnérabilités locales d'une brique élémentaire. Par exemple, un routeur correspond à une brique élémentaire seule, alors qu'un serveur Web est une brique fonctionnelle composée de trois

Contact
Pôle Conseil et Audit en Réseau et Sécurité
Bull-Conseil-Audit@Bull.net
+33 (0)130 80 32 96

bricks élémentaires : le système d'exploitation, l'application Web et le développement spécifique réalisé par le client. Les paramètres critiques de la configuration de chaque brique élémentaire sont validés par rapport aux référentiels existants du client et aux guides de sécurisation de Bull.

Les livrables synthétisent l'analyse des points forts et faibles de la configuration. Les vulnérabilités sont présentées sous une forme permettant de mesurer le degré d'urgence de la mise en œuvre des actions correctives.

Une offre modulaire

<p>Test de Validation : interconnexion Internet</p> <p>Il comporte 3 phases permettant une approche progressive et détaillée du système cible, comme le ferait un « hacker » depuis le réseau Internet :</p> <ul style="list-style-type: none"> • une phase de reconnaissance : identification des cibles et collecte d'informations ; • une phase d'acquisition : exploration des points d'entrée possibles ; • une phase d'attaque : recherche et qualification des vulnérabilités. <p>Test de Vulnérabilité Interne</p> <p>Il a pour objectif de dégager les vulnérabilités affectant une ou plusieurs machines identifiées depuis un point interne du réseau, à l'aide d'une machine pré-configurée et dédiée à la réalisation de ce type de test. Les principaux sujets traités sont :</p> <ul style="list-style-type: none"> • le recensement des machines actives et l'identification des services accessibles sur les principales machines ; • l'identification des systèmes, plates-formes et applications utilisées ; • l'établissement d'une liste des vulnérabilités des serveurs et des matériels actifs identifiés. 	<p>Test de Visibilité</p> <p>L'objectif est de dégager la visibilité offerte par le réseau, à partir d'un poste de travail banalisé spécialement préparé, connecté en interne.</p> <p>Il existe 3 types de test de visibilité :</p> <ul style="list-style-type: none"> • à partir d'un poste standard : aucune modification n'est apportée au poste client ; • à partir d'un poste modifié : le poste client standard est modifié par l'ajout de logiciels et outils de tests ; • à partir d'un poste préconfiguré et dédié à la réalisation de ce type de test. <p>Test de Validation : accès RTC</p> <p>L'objectif est d'évaluer la visibilité des systèmes d'accès du client au travers du Réseau Téléphonique Commuté (RTC). Les 3 phases « Reconnaissance, Acquisition, Attaque » de notre démarche sont mises en œuvre dans ce cadre.</p>
---	--

Boîte noire ou boîte blanche ?

Les tests d'intrusion peuvent être effectués en mode 'boîte noire' (les informations données sur la cible des tests sont minimales) ou en mode 'boîte blanche' (les tests sont réalisés après prise de connaissance des caractéristiques de la cible).

Quelle démarche faut-il privilégier ?

Réponse d'un expert de Bull :

« Les deux approches sont complémentaires. Tout dépend de l'objectif de l'audit. Si le but est de vérifier qu'une équipe d'experts sécurité n'est pas en mesure de pénétrer le système dans un temps raisonnable, alors des tests en aveugle sont suffisants. Mais si on veut avoir un minimum de garanties sur le niveau de sécurité d'une solution et sa pérennité, il est indispensable de combiner les tests de sécurité avec un audit 'boîte blanche' qui permettra d'évaluer l'ensemble des risques. »