VIVALTEK | INTERNAL NETWORK EVALUATION

Auditer son réseau interne, c'est détecter les équipements vulnérables avant les attaquants et renforcer sa sécurité durablement.

INTRODUCTION

Un réseau interne mal maîtrisé ou insuffisamment sécurisé peut entraîner de graves interruptions de service et favoriser la propagation d'attaques telles que les ransomwares.

Réaliser un audit permet de **garantir la continuité de votre activité et l'intégrité de vos données.**

Investir dans des audits préventifs, c'est **limiter les risques et éviter les conséquences financières** d'un arrêt soudain de vos opérations.

OBJECTIFS

Cet audit a pour but principal d'évaluer la qualité, la sécurité et l'efficacité du réseau interne de votre entreprise.

- **Inventaire complet parc informatique**
- **Identifier les vulnérabilités (via CVE[1]), forces et faiblesses du réseau**
- **Analyse les performances et la disponibilité du réseau**
- **Evaluer la résilience face aux attaques**

LES CHIFFRES CLÉS*

70 %

des ransomwares réussis tirent parti de mouvements latéraux dans le réseau interne, en réutilisant des protocoles comme SMB, RDP ou LDAP[2].

62 %

des attaques ciblées se propagent à cause de configurations réseau trop faibles ou de droits excessifs sur les partages internes.

88 %

des attaques « hands-on keyboard » utilisent une phase de reconnaissance réseau pour identifier les périphériques et escalader les privilèges.

4,5

millions d'euros, c'est le coût moyen d'un incident interne lorsque l'attaque provoque une indisponibilité des systèmes métiers ou une perte de données.

**Toutes les sources sont disponibles sur notre site internet, dans la fiche produit correspondante.*

CONTACTEZ NOTRE EXPERT 02 52 61 46 75 | contact@vivaltek.com

Comment fonctionne Internal Network Evaluation ?

Le module **évalue un réseau complet ou une plage d'adresses IP** au sein de votre infrastructure.

Celui-ci commence par lancer une **phase de reconnaissance et de découverte**, durant laquelle il **identifie tous les équipements connectés** : serveurs, postes de travail, périphériques réseau, objets IoT[3] et autres composants de l'infrastructure.

Pour ce faire, il réalise des scans afin de détecter les adresses IP actives, les ports ouverts et les services exposés. Cette étape permet d'établir un **inventaire exhaustif du réseau interne**.

Il poursuit ensuite par une **analyse des vulnérabilités**, en confrontant les versions des logiciels et services identifiés aux bases de données de vulnérabilités connues (CVE). Cela facilite la détection rapide des systèmes obsolètes ou mal configurés, susceptibles d'être exploités par un attaquant.

Ce processus commence par **une phase de reconnaissance pour identifier tous les équipements connectés au réseau.** Il poursuit avec des **scans techniques** afin de recenser les IP actives, ports ouverts et services exposés. Enfin, il **analyse les vulnérabilités en comparant les logiciels détectés aux bases CVE**, afin d'identifier les failles potentielles.

Sur quoi s'appuie le scan d'un domaine avec Internal Network Evaluation ?

- Des tests ciblés permettent de **vérifier la robustesse des configurations**, la gestion des accès et des authentifications, ainsi que la segmentation du réseau. Ils visent à détecter d'éventuels chemins de propagation exploitables **en cas d'attaque interne.**

- La réalisation d'un inventaire, synthétisant les constats techniques, les failles identifiées et leur niveau de criticité permettant de **corriger les vulnérabilités**, renforcer la sécurité du réseau interne et optimiser son efficacité.

Pourquoi effectuer le scan d'un domaine avec Internal Network Evaluation ?

1. **Évaluer la résistance du réseau interne aux risques d'intrusion,** de propagation d'attaques et de compromission des données sensibles. Il offre à l'entreprise une vision précise et complète des équipements, des services en fonctionnement et des vulnérabilités potentielles, afin de corriger ces failles avant qu'elles ne soient exploitées.

2. **Préserver la disponibilité et les performances** du Système d'Information en détectant les anomalies ou éléments pouvant perturber les opérations quotidiennes.

3. **Répondre aux exigences de conformité réglementaire** et aux standards de sécurité en garantissant que le réseau interne est maîtrisé et bien documenté, réduisant ainsi les risques de sanctions ou de pertes contractuelles.

4. **Renforcer la confiance des clients et partenaires,** en attestant que l'entreprise contrôle efficacement la sécurité de ses infrastructures critiques.

Le module Internal Network Evaluation

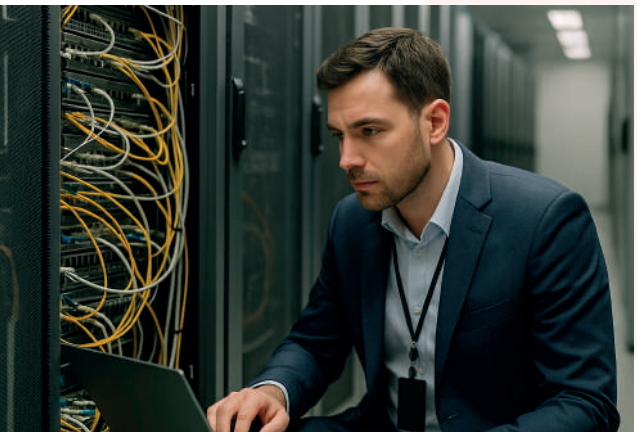
Il vise avant tout à **protéger l'activité et les actifs stratégiques de l'entreprise**. Il permet d'**identifier les failles techniques** susceptibles de compromettre des données sensibles ou d'interrompre les opérations.

Sur quelle fréquence évaluer vos réseaux et périphériques internes ?

Chez VIVALTEK, nous recommandons d'effectuer une **évaluation du réseau interne et des périphériques en continu**. Ce suivi régulier permet de **détecter rapidement toute nouvelle faille** introduite par un changement de configuration, un ajout de périphérique ou une mauvaise pratique interne.

Cette démarche préventive vous offre une vision claire de votre surface d'exposition, vous permet de **renforcer votre posture de sécurité, de protéger vos actifs critiques et de rassurer vos partenaires et clients**.

Passer à ue évaluation régulière du réseau, c'est faire le choix d'une cybersécurité **durable, maîtrisée et conforme** aux standards les plus exigeants.



Cet audit a pour but principal d'**évaluer la qualité, la sécurité et l'efficacité du réseau interne de votre entreprise.**

Lexique

[1]**CVE :** Identifiant unique donné à une faille de sécurité informatique connue. Chaque CVE permet de nommer, suivre et corriger rapidement une vulnérabilité dans un logiciel ou un système.

[2]**LDAP :** Protocole utilisé pour accéder et gérer les informations dans un annuaire d'entreprise, comme les comptes utilisateurs, les mots de passe ou les droits d'accès.

[3]**IoT (Internet des Objects) :** Désigne tous les objets connectés à Internet capables de collecter, transmettre ou recevoir des données, sans intervention humaine directe.

Consultez notre lexique complet à l'adresse suivante : https://vivaltek.com/lexique-complet

VIVALTEK
2, Impasse Johannes Gutenberg, Z.A Les Acacias III 85430 La Boissière des Landes
02 52 61 46 75 | contact@vivaltek.com