PENTEST - 4 points à maitriser avant de vous lancer

Guide spécial - Membres du

Les techniques d'attaque évoluent chaque année, et votre surface d'exposition aussi.
Dans ce contexte, un pentest est un outil de pilotage du risque.
Voici ce que tout RSSI devrait avoir vérifié avant de signer — et ce que nous examinons systématiquement avec nos clients.

CE QUE VOUS DEVEZ VÉRIFIER AVANT DE FAIRE UN PENTEST

1) Ne choisissez pas un prestataire sans lui poser ces questions

Qui conduit la mission — un expert certifié ou un outil automatisé ? Le rapport inclura-t-il des preuves d'exploitation reproductibles ? Un pentester manuel s'adapte à votre environnement, contourne vos défenses et simule un attaquant réel. La méthodologie de votre pentest est un gage de qualité.

2) Définissez votre périmètre en amont

Répondez d'abord à ces questions :

- Où sont vos actifs critiques et mes données sensibles ?
- Quel est mon niveau d'exposition sur Internet ?
- Quel est l'objectif du test — réglementaire, proactif, post-incident ?
- Vos utilisateurs ont-ils des pratiques à risque ?

Ces réponses vous permettront d'identifier le bon périmètre de votre test d'intrusion.

3) Exigez un livrable à 3 niveaux

Un bon rapport s'adresse à plusieurs audiences : une synthèse lisible par votre COMEX, un volet technique avec des preuves d'exploitation reproductibles, et un plan de remédiation priorisé avec délais réalistes. Posez aussi la question de l'après : si vous n'avez pas les ressources pour corriger en interne, votre prestataire doit pouvoir vous accompagner.

4) Un pentest ponctuel protège — un pentest régulier transforme

Les techniques d'attaque évoluent chaque année. De nouveaux vecteurs émergent en permanence — infostealers, faux captchas, supply chain. Et chaque migration, chaque nouveau projet ouvre de nouvelles surfaces d'exposition. Ce qui était sûr il y a 18 mois ne l'est peut-être plus aujourd'hui. Planifiez au minimum un test par an, et après chaque changement structurant de votre SI.

Un pentest bien cadré, c'est aussi l'argument le plus concret pour convaincre votre direction d'investir dans la sécurité.

Vous souhaitez en savoir plus ? Contactez-nous : **contact@aisi.fr**
AISI - 1 avenue Alphand - 94160 Saint-Mandé