

Les tests de vulnérabilité informatique



Évaluer les risques d'intrusion dans votre système d'information

Prérequis à l'audit de sécurité, l'évaluation des risques d'intrusion s'effectue par une série de tests de vulnérabilité en conditions simulées et réelles, et sur la base de cas concrets.

Notre offre

Test d'intrusion (ou pentest – penetration test)

- Réaliser une cartographie concrète des vulnérabilités techniques.
- Évaluer la capacité d'un cybercriminel à tirer parti des vulnérabilités détectées.
- Hiérarchiser les vulnérabilités (mineures, majeures et critiques) avec pour chacune une recommandation adaptée.

Red Team (test de pénétration sans que la Blue Team de votre entreprise ne soit prévenue)

- En adoptant la posture des cybercriminels, mesurer la capacité de réaction de votre organisation à détecter et à répondre aux cyberattaques.
- Mettre en place des actions préventives à partir des faiblesses identifiées.

Simulation de phishing (hameçonnage par un fraudeur pour usurper une identité)

- Évaluer le niveau de maturité de votre défense face à une menace de phishing.
- Réduire les risques en sensibilisant vos collaborateurs à la détection de ce type de menaces et préparer la réponse à y opposer.

Les bénéfices des tests de vulnérabilités pour votre entreprise

Les tests permettent d'identifier les vulnérabilités de l'entreprise et d'en prendre conscience. Ce sont des prérequis à la définition du dispositif de cyber sécurité et du plan de résilience. Ils permettent en outre de :

- Mesurer l'exposition aux risques de tout l'ensemble du système d'information.
- Sécuriser le système d'information pour l'entreprise et ses parties prenantes (clients, fournisseurs).

Notre engagement

Vous aider à maîtriser les risques cyber pour votre entreprise et ses parties prenantes et à garantir la conformité des pratiques au regard des règles de l'art.

Contact