



PACK SÉRÉNITE

+33 6 34 63 06 75
contact@procybex.fr
Siège social
26 Chaussée Marcadé
80100 ABBEVILLE

AUDIT 360 INTÉGRAL

Un état des lieux de la sécurité du système d'information, et l'identification des 80/20 : les 20% d'efforts qui vont faire **gagner 80% de sécurité** ! Nos experts se basent sur les indicateurs validés par les principaux référentiels cybersécurité et l'ANSSI.

Un panorama global de la sécurité de votre infrastructure informatique : une **analyse des points forts et des points faibles** du périmètre de votre système d'information. Les axes d'améliorations seront ainsi relevés et notés dans un **rapport qui inclut un plan d'actions** pour atteindre un niveau de protection le plus élevé possible. Ce rapport vous aidera à mieux piloter l'enjeu majeur : **la gestion des risques de votre organisation.**

- ✓ Prestation sur site
- ✓ Gestion RH (*procédures entrées/sorties des collaborateurs*)
- ✓ Vulnérabilités du site web et des accès internet IP publiques
- ✓ Présence d'informations confidentielles sur le Web/DeepWeb
- ✓ Politique d'authentification et de gestion des accès
- ✓ Sécurité du réseau (*Switch, Firewall, Wifi, etc..*)
- ✓ Sécurité des postes (*Antivirus, Systèmes d'exploitation, etc..*)
- ✓ Sécurité de l'administration (*Accès distants, physiques, & Active Directory*)
- ✓ Gestion du nomadisme (*Chiffrement, etc..*)
- ✓ Politique de mises à jour (*Serveurs, PC, etc..*)
- ✓ Politique de sauvegarde
- ✓ Rapport intégral et précis

CAMPAGNE DE FAUX PHISHING

- ✓ Réunion de lancement : définition du contexte et élaboration du scénario
- ✓ Conception du courriel de type phishing
- ✓ Boîte aux lettres de test
- ✓ Intégration d'un listing des adresses emails cibles (*max. 50*)
- ✓ Adresse email source crédible, externe à l'entreprise
- ✓ Page web sur un serveur dans notre lab pour collecter les données sensibles
- ✓ Configuration de votre/vos anti-spam avec votre prestataire informatique
- ✓ Simulation en conditions opérationnelles
- ✓ Envoi réel de l'email d'hameçonnage et collecte des informations sensibles
- ✓ Statistiques de clics
- ✓ Synthèse sur la récupération de données, identifiants et mots de passes
- ✓ Rapport intégral et précis

Nous utilisons des méthodes d'évaluation de la sécurité de votre système informatique face à **une attaque basée sur les failles humaines**. Nous testons la réaction de vos collaborateurs face à une **simulation d'attaque** par ingénierie sociale, pour comprendre comment une personne malveillante extérieure pourrait impacter votre système. **91% des cyberattaques commencent par un email innocent !**

Réalisé par un expert en cybersécurité certifié, sur des collaborateurs non informés de sa mise en œuvre, nous utilisons des **emails d'hameçonnage**, typiques des cybercriminels (*phishing*), imitant les messages reçus au quotidien pour **simuler une collecte de données sensibles.**

SCANS DE VULNÉRABILITÉS

Un test à distance des vulnérabilités visibles depuis Internet vers votre système d'information*. Réalisé par notre équipe d'experts en cybersécurité à partir de notre lab, nous organisons une réunion de débriefing avec la remise d'un rapport.

Nous effectuons un **transfert de connaissances** et communiquons les éléments nécessaires à la mise en place d'un **plan d'action**.

* Fréquence des tests en fonction du contrat.

Confidentialité et éthique :

Chacun de nos collaborateurs a signé une « charte éthique et déontologique » et une « clause de discrétion » dans lesquelles il s'engage à respecter la plus grande confidentialité, intégrité et honnêteté. D'autre part, nous nous engageons à supprimer les données collectées lors de cette prestation une fois celle-ci terminée.

- ✓ Scan de vulnérabilité à partir de notre lab
- ✓ Standard PCI DSS
- ✓ Scan des IP's publiques
- ✓ Scan de vulnérabilité externe
- ✓ Scan de vulnérabilité Active Directory
- ✓ Scan de vulnérabilité site internet (*hors E-Commerce*)
- ✓ Plan d'action pour la correction des vulnérabilités
- ✓ Réunion bilan avec transfert de connaissances
- ✓ Rapport intégral et précis