

## TEST DE SÉCURITÉ INTERNE

### ***Vos employés peuvent-ils voler vos données ou endommager votre système informatique ?***

Un test de sécurité interne (TSI) vous permettra de répondre à cette question. De plus, ce test permet de démasquer les vulnérabilités menaçant vos actifs informationnels. Pour la portée du TSI, deux options se présentent à vous : le test peut être réalisé « à l'aveugle » ou avec l'assistance de vos administrateurs.

Lors d'un test « à l'aveuglette », les experts de **Gardien Virtuel** se connectent directement sur votre réseau interne et tentent de compromettre celui-ci. L'objectif principal des spécialistes de **Gardien Virtuel** est d'identifier les façons de compromettre la confidentialité, l'intégrité et la disponibilité de vos informations et de vos équipements. Le TSI peut aussi être effectué en collaboration avec les administrateurs de vos systèmes, c'est-à-dire que le client fournit les accès (mots de passe par exemple) nécessaires pour accéder à vos systèmes. Nos experts ont alors le même niveau d'accès que les employés et ils pourront rapidement trouver les failles que pourraient exploiter ces derniers.

Ce test permet par ailleurs de classer très facilement et rapidement les menaces. Suite au TSI, **Gardien Virtuel** vous fournira un rapport détaillant les vulnérabilités trouvées sur vos systèmes. Ce rapport comportera aussi une liste de recommandations pour mitiger les menaces trouvées et mettre au point des défenses pour votre système d'information. En option, un rapport « VIP » pour votre comité de direction peut être rédigé afin, par exemple, de venir compléter une démarche budgétaire. Ce rapport « VIP » explique en termes très peu techniques les tenants et aboutissants, les risques et les impacts des failles recensées.

## MÉTHODOLOGIE DE GARDIEN VIRTUEL POUR SES TSI

### ***Étape 1 : Prise de connaissance et évaluation de l'environnement et du contexte***

Les premiers éléments à réviser sont les politiques de sécurité. Celles-ci devraient décrire les objectifs de sécurité de l'organisation et les moyens choisis pour atteindre ceux-ci. **Gardien Virtuel** pourra prendre connaissance de ces documents afin de comparer la situation réelle de l'organisation et les objectifs de contrôle que celle-ci s'est fixée.

**Gardien Virtuel** utilise les normes ISO 27002 (17799) et COBIT comme guides de référence des bonnes pratiques et pour l'évaluation des objectifs de contrôle.

### ***Voici les principaux critères d'évaluation de l'environnement utilisés dans le TSI :***

- La ou les politiques de sécurité;
- L'organisation de la sécurité de l'information;
- Les contrôles et la classification des actifs informationnels (gestion des biens);
- La sécurité liée aux ressources humaines;
- La sécurité physique et environnementale;
- La sécurité des opérations et des communications;
- Les contrôles d'accès;
- La gestion du développement et la maintenance des systèmes;
- La gestion des incidents liés à la sécurité de l'information;
- Les processus de continuité des affaires;
- La conformité des pratiques de l'organisation.



## Étape 2 : Balayage automatisé des ports

Cette étape est intrusive et peut être rapidement détectée compte tenu de la grande quantité de tentatives de connexion générées. Tous les ports sont balayés (65535 ports TCP et autant en UDP), à la recherche des services accessibles à partir d'ordinateurs distants. Ce type de balayage permet également de vérifier la configuration des coupe-feu utilisés. À cette étape on obtient :

- La liste complète des ports ouverts (chaque port ouvert est une entrée potentielle dans l'entreprise qui pourrait devenir une éventuelle vulnérabilité);
- L'identification des services et des logiciels actifs;
- La version des logiciels utilisés dans l'entreprise (dans le but de cibler les vulnérabilités présentes);
- Des moyens de contourner le coupe-feu.

## Étape 3 : Balayage automatisé des vulnérabilités

Ce second balayage va beaucoup plus en profondeur que le premier et est par conséquent considéré comme très intrusif. Non seulement cherche-t-il à identifier les services qui lui sont accessibles, mais de plus, il tente de les percer grâce à une liste exhaustive d'attaques reconnues. Dépendant de vos désirs et besoins, les tests pouvant entraîner une interruption de service peuvent être laissés de côté. Une autorisation écrite explicite est nécessaire pour que **Gardien Virtuel** exécute ceux-ci.

## Étape 4 : Tests d'intrusion manuels

Suite aux résultats obtenus dans les étapes précédentes, des tests manuels seront réalisés. Les tests manuels sont importants puisque certaines configurations ne posent pas un risque en elles-mêmes, mais lorsque combinées à d'autres, elles peuvent avoir une incidence plus élevée. Ces configurations fournissent alors des moyens aux pirates informatiques d'arriver à leurs fins. Voici une liste d'exemples de vérifications manuelles exécutées suite aux vulnérabilités découvertes aux étapes précédentes :

- Valider qu'il n'y ait pas de faux positifs, c'est-à-dire, déterminer que les vulnérabilités rapportées par les outils sont réellement présentes;
- Valider qu'il n'y ait pas de faux négatifs, c'est-à-dire, déterminer les vulnérabilités existantes qui n'ont pas été découvertes par les logiciels de balayages automatisés;
- Exploiter certaines vulnérabilités pour obtenir des accès supplémentaires permettant la découverte d'autres vulnérabilités;
- Rechercher de façon plus poussée pour découvrir des failles ou des problèmes rattachés aux applications et aux systèmes informatiques qui nécessitent une attention particulière.

## Étape 5 : Analyse de l'architecture et des choix technologiques

Chaque organisation possède une culture d'entreprise qui lui est propre. Les choix technologiques reflètent cette culture. Nous procéderons à une évaluation des configurations, mais aussi des forces et faiblesses de l'architecture technologique, de sa mise en place et de sa gestion. **Gardien Virtuel** procédera également à une évaluation des risques liés aux composantes réseaux et à leurs supports, tels que :

- Vérification des règles de filtrage des coupe-feu;
- Évaluation des restrictions et séparation des réseaux;
- Évaluation des restrictions et permission de protocoles tels que définis dans la politique de sécurité;
- Vérification du contrôle des accès et de l'authentification des utilisateurs, des tentatives d'obtenir des mots de passe et de la possibilité d'attaques par rejeu (« replay »);
- Validation des protocoles utilisés pour la gestion réseau tels que NTP, SMB, SNMP, etc.;
- Évaluation des systèmes de surveillance, des journaux d'événements système, ainsi que la protection utilisée pour protéger ceux-ci.

## SOMMAIRE DES VULNÉRABILITÉS

Zone	Vulnérabilités / Code de sévérité					Total vuln.
	0	1	2	3	4	
STATIONS DE TRAVAIL	0	3	11	26	6	46
SERVICES / SERVEURS	0	26	39	26	6	97
<b>TOTAUX</b>	<b>0</b>	<b>29</b>	<b>50</b>	<b>52</b>	<b>12</b>	<b>143</b>

Le sommaire des vulnérabilités sera inclus dans le rapport final.

Avez-vous besoin d'évaluer la **résistance de votre système d'information ?**  
**Contactez-nous dès aujourd'hui pour une évaluation gratuite de vos besoins !**