



AUDIT DE SÉCURITÉ DES SYSTÈMES

L'objectif d'un audit de sécurité des systèmes est de vérifier en profondeur les applications, les configurations et les paramètres des systèmes d'information actuellement en place. Cet audit est donc une démarche exhaustive exécutée en suivant une méthodologie précise, efficace et reconnue pour obtenir les résultats visés. Pendant un audit de sécurité, les systèmes (les serveurs et les postes de travail de votre entreprise) seront tous scrutés à la loupe.

EN TROIS TEMPS

Dans ce contexte, **Gardien Virtuel** a segmenté sa méthodologie d'audit en trois (3) phases, soit :

- 1. La phase de « Collecte des données »** : En premier lieu, **Gardien Virtuel** effectuera divers tests d'intrusion à l'aide d'outils spécialisés, des tests manuels ainsi que des vérifications visuelles. Tout ceci sera fait afin de déceler les potentielles faiblesses, failles et vulnérabilités de sécurité de vos systèmes. Notez qu'une partie de cette première phase peut être effectuée par le client s'il le désire. **Gardien Virtuel** fournira la procédure à suivre aux responsables désignés. Il en résultera une baisse de 25% de la facture totale.
- 2. La phase d'« Analyses des données »** : Depuis le siège social, les experts de **Gardien Virtuel** procéderont à l'analyse de toutes les informations recueillies et des résultats générés par les divers outils utilisés. Cette phase peut être plus ou moins longue, selon la quantité et la complexité des systèmes analysés.
- 3. La phase « Rapport d'évaluation et recommandations »** : Finalement, **Gardien Virtuel** prépare un rapport qui détaille les failles identifiées et les classe en utilisant un code de sévérité extrêmement compréhensible. De plus, pour chaque faiblesse découverte, nos experts présenteront leurs recommandations et solutions pour corriger ou mitiger ces dernières.

LE LIVRABLE

Suite à cette démarche, un rapport comprenant les éléments suivants sera émis:

- La description des configurations actuelles des systèmes analysés;
- La description détaillée des insuffisances et des vulnérabilités constatées durant l'audit;
- Les résultats complets de l'ensemble des tests réalisés;
- Des recommandations à mettre en place pour augmenter le niveau de sécurité des systèmes analysés;
- Un sommaire exécutif sous la forme d'un tableau (voir verso).

Le coût et le délai de livraison du mandat dépendent du nombre de serveurs et de postes de travail qui seront analysés. **Gardien Virtuel** se base donc sur son expérience pour soumettre un prix au client.

Contactez-nous dès aujourd'hui pour une évaluation gratuite du projet qui répondra à toutes vos attentes !

LA SYNTHÈSE GRAPHIQUE : UNE EXCLUSIVITÉ GARDIEN VIRTUEL

Développé par **Gardien Virtuel**, le graphique de synthèse est un excellent outil pour permettre au client d'avoir un aperçu global de l'état de la sécurité de ses systèmes d'information. Vous trouverez ci-dessous un exemple du graphique en question :

RAPPORT D'ÉVALUATION DE SÉCURITÉ INTERNE

Fichier	Fichier .xls		Permissions for file system x.dcl		Users.dcl		Dumpreg.txt		TCPView.txt		Passprop.txt		Pinfo.txt		Fichiers .MBSA				Streams.txt				
	ANTIVIRUS	LOGICIEL À JOUR	FICHERS STANDARDS	FICHERS SYSTEMES	TOTAL EVERYONE	# UTILISATEURS	MOT DE PASSE NEXISTE PAS ?	# DE PROGRAMMES AU DÉMARRAGE	# ÉLÉMENTS À NOTER	# TCP	# UDP	MOT DE PASSE COMPLEXE ?	COMPTE ADMIN PEUT-ÊTRE VERROUILLÉ	PERFORMANCES	ESPACE DISQUE (-20%)	MAJ INSTALLÉES	PROGRAMMES INSTALLÉS	MAJ MANQUANTES	ZONES IE DÉFINIES	/RESTREINT AUX ADMINS	VULNÉRABILITÉS OFFICE ?	FLUX ALTERNATIFS SUSPECTS	
#	SYSTÈME																						
1	✓	⚠	26	2	27	86	17	3	---	45	59	✓	✗	✓	79	24	39	✓	✗	---	---	⚠	
2	✓	⚠	107	6	13	7	7	6	---	24	21	✓	✗	✓	115	50	31	✗	---	---	---	✓	
3	✓	⚠	305	6	11	7	6	4	---	27	31	✓	✗	✓	7	50	92	✗	---	---	⚠	✓	
4	✓	⚠	6039	12	6051	8	8	7	---	44	18	✓	✗	✓	7	45	92	✗	---	---	---	✓	
5	✓	⚠	13	C*	\13	6	6	2	---	20	22	✓	✗	✓	84	22	28	✗	---	---	---	✓	
6	✓	⚠	9	2	11	86	16	2	---	29	50	✓	✗	⚠	34	16	24	✓	✗	---	---	⚠	
RÉFÉRENCES																							
SECTION		---	4.1	4.2	4.3	4.4	4.5	4.6	4.7	4.8	4.9	4.10	4.11	4.12	4.13	4.14	---	---	---	---	---	---	---
PAGE		---	7	7	8	8	8	9	9	9	10	10	10	11	11	11	---	---	---	---	---	---	---

* : l'analyse des permissions pour cet ordinateur a permis de déjouer qu'une restriction d'accès n'est pas présente sur le lecteur C:\ L'accès total au lecteur est possible pour "Everyone" .

LÉGENDE :

- ✓ = L'élément concerné est sécuritaire. Aucune vulnérabilité n'a été trouvée.
- ✗ = Une vulnérabilité est présente. Une réaction corrective immédiate est recommandée.
- ⚠ = Ce point requiert votre attention. En fonction de la colonne, la signification peut changer.

