DIFFUSION RESTREINTE ADMINISTRATEUR
si renseigné

À le

N° /DR

VISITE DE CONTRÔLE TECHNIQUE DE SÉCURITÉ INFORMATIQUE

APRÈS EXPLOITATION, CE DOCUMENT DEVRA ÊTRE STOCKÉ DANS LE DOSSIER DE SÉCURITÉ INFORMATIQUE DE SITE.
Il SERA DÉTRUIT DÈS RÉCEPTION DU PROCHAIN RAPPORT DE VISITE.

Formation visitée :	
Implantation :	
Responsable informatique :	(PNIA :)
Personnels présents :	(PNIA :)

Contrôle technique effectué le :

Par :	Fonction : Rédacteur SSI	PNIA :
Par :	Fonction :	PNIA :

L'auditeur responsable	Le Directeur de ...

Copies :
- Archive de .....
- Organisme audité

DIFFUSION RESTREINTE ADMINISTRATEUR
si renseigné

Table des matières

1. Informations techniques contextuelles

- Nom du domaine DNS :
- Adresse et masque de réseau :
- Adresse du routeur de site :
- Adresse utilisée par le système contrôleur :
- Type et débit de l'accès à l'Internet :

Adresses et types des systèmes dédiés à la sécurité informatique

- serveur d'antivirus :
  - port d'écoute des clients[1] :
- serveur SUS/WSUS
  - serveur SUS/WSUS de rattachement :
- DMZ
  - parefeu (2 adresses) :

Adresses et types des serveurs locaux de ressources

- fichiers :
- impression :
- domaine ou AD primaire :
- domaine ou AD secondaire :
- WEB :
- messagerie locale :
- SGBD :
- autres :

[1] Pour des clients « officescan » cf. paramètre « CLIENT_LOCALSERVER_PORT » de la section « INI_CLIENT_SECTION » du fichier « ofcscan.ini » ou « clientbindport.ini » du répertoire C:\Program Files\Trend Micro\OfficeScan Client

2. Investigation technique

Les résultats détaillés des investigations techniques peuvent être consultés sur demande.

2.1. Contrôle réseau

Le but est de vérifier l'inventaire informatique détenu dans le dossier de sécurité du site, les trames transitant sur le réseau local et les configurations des équipements ainsi que les applications rendant des services réseaux.

Inventaire informatique

Conforme :

Commentaires :

Analyse des services et protocoles réseau

	GENERALITES	
	Présence de protocoles inutiles au niveau système	0
	Existence de services inutiles au niveau système	0
	CPR	**2**

Commentaires :

Plan d'action :

Id Action	Action	Délais

Configuration des équipements actifs

Commutateurs :

	Commutateurs	
R4	Sauvegarder les configurations sur un support dédié	0
R7	Le choix d'un mot de passe robuste est indispensable	0
R10	Séparation des flux d'administration et de production	0
R11	Désactiver les fonctionnalités non nécessaires	0
R14	Désactiver les ports non utilisés	0
R15	Activer le Trap and Close	0
R17	Désactiver les protocoles inutilisés : STP	0
R18	Désactiver les protocoles inutilisés : CDP – LLDP	0
R19	Désactiver les protocoles inutilisés : DTP	0
R20	Administration à l'aide de SSH	0
	Système d'exploitation à jour des correctifs de sécurité	0
	CPR	**11**

Commentaires :

Plan d'action :

Id Action	Action	Délais

Routeurs :

	Routeurs	
R3	Sauvegarder les configurations sur un support dédié	0
R6	Désactiver les protocoles inutiles ou obsolètes : TCP/IP simples	0
R7	Désactiver les protocoles inutiles ou obsolètes : Finger	0
R8	Désactiver les protocoles inutiles ou obsolètes : Service config	0
R9	Désactiver les protocoles inutiles ou obsolètes : CDP	0
R10	Désactiver les protocoles inutiles ou obsolètes : http server	0
R11	Désactiver les protocoles inutiles ou obsolètes : BOOTP – DHCP	0
R12	Désactiver les protocoles inutiles ou obsolètes : SNMP V1 – V2c	0
R13	Désactiver les protocoles inutiles ou obsolètes : no ip directed broadcast	0
R14	Désactiver les protocoles inutiles ou obsolètes : no ip source route	0
R15	Désactiver les protocoles inutiles ou obsolètes : Information ICMP	0
R16	Désactiver les protocoles inutiles ou obsolètes : Relais ARP	0
R17	Désactiver les protocoles inutiles ou obsolètes : no ip mroute-cache	0
R18	Désactiver les protocoles inutiles ou obsolètes : no ip subnet-zero	0
R19	Désactiver les protocoles inutiles ou obsolètes : no mop enable	0
R22	Utiliser des mots de passe forts	0
R25	Ne pas utiliser Telnet	0
R35	Vérifier l'adéquation des ACL avec la matrice des flux	0
	Système d'exploitation à jour des correctifs de sécurité	0
	CPR	**19**

Commentaires :

Plan d'action :

Id Action	Action	Délais

2.2.Configuration serveur

L'objectif est de vérifier la configuration des serveurs (base de données, web …)

MySql

Analyse générale :

REF	**GENERALITES**	
R1	changement de nom à « root »	0
R2	attribution d'un mot de passe	0
R3	suppression des comptes anonymes sans mot de passe	0
R4	attribution des droits de mysql sur le répertoire « data »	0
R5	suppression de la base « .test »	0
R6	Gestion des fonctionnalités inutiles	0
R7	Restriction des privilèges des utilisateurs	0

R8	Gestion des *logs*	0
CPR		**8**

Commentaires :

Plan d'action :

Id Action	Action	Délais

Accès au serveur :
Commentaires :

Plan d'action :

Id Action	Action	Délais

Apache

Plan d'action :

Id Action	Action	Délais

Domaine Windows

Plan d'action :

Id Action	Action	Délais

2.3.Analyse des vulnérabilités

L'objectif est d'inventorier et de corriger les vulnérabilités résiduelles des systèmes d'exploitation et des applications rendant des services réseaux justifiés.
Des contraintes de sécurité et de temps imposent que cette phase du contrôle ne soit réalisée que sur un échantillon représentatif des systèmes de la formation visitée. Par définition, les actions à mener issues de cette phase (cf. §4) seront à appliquer à l'ensemble des systèmes.
L'échantillon représentatif considéré est le suivant : .....

Actions à mener :

Commentaires :

2.4. Divers

En complément des quatre domaines de contrôle présentés supra, les points particuliers suivants permettent de vérifier certaines conformités réglementaires :

- Présence d'un mot de passe de configuration des imprimantes et copieurs réseau :
- Présence d'un serveur antivirus local :
  - Si oui, est-il abonné au service de mise à jour automatique :
  - Existence de stations ne possédant pas d'antivirus mis à jour automatiquement :
- Existence d'un système de badgeuses :
  - si oui, est-il séparé du réseau local (physique ou logique (VLAN)) :
- Existence, sur le réseau, d'un système supervisé ou administré par une société :
  - si oui, des mesures de sécurité ont-elles été prises :

- Existence d'un système utilisant un moyen radio civil (WIFI, Bluetooth, BLR, etc.) :
- Utilisation de logiciels de prise de contrôle à distance :
  - si oui, les Attestations d'Engagement de Responsabilité (AER) le mentionnent-ils :
  - si oui, la prise de contrôle est-elle validée par l'utilisateur :

:

3. Bilan de la visite précédente

Date de la précédente visite :
Référence du compte-rendu : N° /DR du

Nro	Actions à réaliser	échéance	état

4. Conclusion et actions à mener

Sous la responsabilité du RSSI de la formation, une action visant à améliorer la situation constatée doit être conduite et pilotée par le responsable informatique du site.

Les actes techniques devant être réalisés pour mener à bien cette action ont été montrés et expliqués aux personnels responsables du système d'information contrôlé lors de la visite.

Nro	Actions à réaliser	échéance

RAPPEL : Les méthodes et les outils d'investigation utilisés pour mener à bien ce contrôle sont strictement réglementés. Il est nécessaire de rappeler que seuls les experts SSI formés et désignés sont habilités à les exploiter sous la responsabilité d'un RSSI. En dehors de ce cadre strict, l'utilisation d'outils similaires devrait rester interdite.