BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS

Option : Solutions d'infrastructure, systèmes et réseaux

U6 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES
SESSION 2023

CAS VILLE DU PARC
PROPOSITION DE CORRIGÉ

DOSSIER A	**Évaluation des risques**	**28 points**

Question A1.1
Rédiger une courte note rappelant au moins quatre obligations en matière de collecte et traitement de données personnelles.

Citer le RGPD qui, depuis le 25 mai 2018, définit les obligations légales est attendu.

- Obligation d'information de l'internaute quant aux traitements qui seront effectués sur les données.
- Obligation pour l'organisation de nommer un correspondant RGPD.
- Obligation de recenser les traitements (registre des traitements).
- Lister les données « particulièrement sensibles » : nécessité de consentement explicite, libre, spécifique et univoque.
- Toute mesure de sécurisation pertinente pour l'accès aux données et leur stockage (mot de passe, chiffrement, sauvegardes, etc.).
- Définir la durée de conservation des données.
- Etc.

Question A1.2
Exposer deux conséquences pour la Mairie et deux conséquences pour ses usagers, d'un vol de données relatives au service de l'état-civil.

Pour la mairie :

- pour le domaine de l'état-civil, toute intrusion pourrait amener, au mieux, à des retards dans les traitements, au pire à du vol de données, des usurpations d'identité, voire des créations de faux papiers ;
- la responsabilité pénale et/ou civile du Maire peut être engagée (au titre de manquements à l'obligation de sécurité ou du détournement de finalités d'un traitement de données personnelles) ;
- dysfonctionnement des services, arrêt des services tels que réservation de cantine scolaire, services sociaux, bibliothèque, activités sportives, etc.
- dégradation de l'image de marque du service public, perte de confiance des administrés envers l'administration ;
- etc.

Pour les usagers :

- retard dans les traitements de demandes administratives, que ce soit le renouvellement de papiers d'identité, demandes de permis de construire, publication des bans pour les mariages, etc. ;
- possibilité d'usurpation d'identité pour les usagers si leurs données sont exfiltrées ;
- utilisation des données personnelles des usagers à des fins commerciales (démarchage) ou malveillantes ;
- etc.

Question A2.1
Lister au moins cinq éléments déjà mis en œuvre pour favoriser la résilience des services de la ville.

Eléments favorisant la résilience du SI de la ville :

- doublement des datacenters et de l'infrastructure globale ;
- doublement des liaisons WAN ;
- redondance des routeurs pares-feux ;
- redondance de l'infrastructure de virtualisation ;
- module HA activé sur les ESX (haute-disponibilité des VM) ;
- redondance des liens entre cœur de réseau et commutateurs (RSTP activé) ;
- redondance des SAN ;
- disques mis en RAID50 (disponibilité des données et intégrité) ;
- double climatisation ;
- etc.

Des éléments ne favorisant pas la résilience doivent être sanctionnés.

Question A2.2
a) Evaluer les conséquences en termes de disponibilité, d'intégrité et de confidentialité sur le SI de la ville d'une attaque par rançongiciel sur les serveurs.

En termes de disponibilité : coupure des activités de nombreux services, données inaccessibles, arrêt des services, etc.

En termes d'intégrité : les données sont altérées par le chiffrement frauduleux. Par ailleurs, les personnes malveillantes ayant eu accès aux données, celles-ci ont pu également être modifiées (même celles qui n'ont pas été chiffrées).

En termes de confidentialité : accès aux données de façon non autorisées (par la rançongiciel) donc problème de confidentialité.

La qualification des 3 éléments est nécessaire.

Question A2.2
b) Identifier le niveau de gravité et le niveau de vraisemblance de l'attaque et en déduire le scénario de risque indiqué dans la matrice.

Gravité = 4

Fournir un service pour les actes d'état-civil (passeport, carte nationale d'identité…)	*Perte ou destruction des données concernant les usagers*	▪ *Impacts sur les missions et services de la mairie* ▪ *Impacts sur l'image et la confiance* ▪ *Impacts juridiques, etc.*	***4/4***

Vraisemblance = 4

Un groupe de pirate envoie un courriel d'hameçonnage à un utilisateur du réseau et infecte un poste informatique avec un rançongiciel	*Très vraisemblable (4/4)*

Le risque peut être classifié en R2 (stratégie de traitement des risques).

Question A2.2
c) Lister les mesures déjà prises pour limiter ce risque.

Surveillance renforcée des flux entrants et sortants	R2, R3
Sensibilisation à l'hameçonnage	R2, R3
Audit de sécurité de l'ensemble du SI	R1, R3, R2

Le listage d'autres mesures non présentes dans le tableau mais cohérentes (comme l'analyse anti-spam) est accepté.
Le listage d'une mesure à lancer peut être considérée comme prise.

Question A2.3
Indiquer l'impact sur la gravité et sur la vraisemblance de chacune des solutions « Bac à sable » et « Application Guard » pour le risque induit par un rançongiciel. Justifier la réponse.

Le **bac à sable** permet de travailler dans un environnement isolé mais il faut l'activer. La probabilité de cliquer sur un lien frauduleux et d'installer un malware reste identique si l'utilisateur ne l'utilise pas mais il n'y aura aucune conséquence si l'utilisateur l'active.

- La gravité du risque est moindre si l'utilisateur l'active.
- La vraisemblance reste identique si l'utilisateur ne l'utilise pas.

Application Guard limite les risques de cliquer sur un lien corrompu dans un mail ou un fichier frauduleux en empêchant l'accès au site pirate.

- La gravité du risque reste identique.
- La vraisemblance du scénario sera diminuée car même si l'utilisateur clique sur un lien frauduleux ou ouvre un fichier Microsoft Office, le système bloquera l'accès au site. Par contre si l'utilisateur clique sur un autre type de fichier (.pdf, .jpg, etc), Application Guard ne sera d'aucune utilité.

L'utilisation du bac à sable est une action volontaire de l'utilisateur contrairement à Application Guard qui est intégré au navigateur usuel.

DOSSIER B	**Mesures de protection supplémentaires face aux menaces**	**37 points**

Question B1.1
a) Expliquer, en fonction du type de compte, les impacts d'une stratégie de changement de mot de passe avec une durée très courte (inférieure à un mois par exemple) par rapport à une stratégie de changement sur une durée très longue, voire illimitée.

Compte sans privilège :

- un délai d'expiration de mot de passe très court est contre-productif. Il incite l'utilisateur à construire des stratégies pour retenir son mot de passe comme par exemple l'ajout d'un compteur à la fin d'un mot de passe toujours identique ;
- un délai d'expiration très long : pas d'impact si le mot de passe est robuste, sauf s'il est divulgué.

Compte à privilège :

- un délai d'expiration de mot de passe très court est contre-productif. Il incite l'utilisateur à construire des stratégies pour retenir son mot de passe comme par exemple l'ajout d'un compteur à la fin d'un mot de passe toujours identique ;
- un délai d'expiration très long, voire illimité peut présenter un risque si le mot de passe est divulgué. Son utilisation frauduleuse pourra avoir lieu durant une longue période.

Question B1.1
b) Préconiser un délai d'expiration de mot de passe pour les comptes à privilèges.

Il est nécessaire de mettre en place un délai d'expiration pour les comptes à privilège.
L'ANSSI préconise une durée de 1 à 3 ans. (*On attend que le candidat propose une durée comprise entre ces 2 bornes*).

On valorisera une durée différente (raisonnablement plus courte) correctement argumentée.

Question B1.2
Adapter le script Powershell afin de permettre de lister les comptes à privilèges appartenant au groupe « Administrateurs de l'entreprise » dont le mot de passe n'a pas été modifié depuis plus d'un an.

Il suffit d'adapter le script :

- en changeant le nom de groupe ;
- en modifiant l'attribut récupéré et éventuellement le nom de la variable ;
- en modifiant la limite ;
- en adaptant le message affiché.

```
$groupe = "Administrateurs de l'entreprise"

$membres = Get-ADGroupMember -Identity $groupe -Recursive
foreach($un_membre in $membres)
{
      $id = $un_membre.samaccountname
      $user = Get-ADUser -Identity $id -properties *
      $dateDernier = $user.PasswordLastSet
      $limite = (get-date).AddDays(-365)
      if($dateDernier -lt $limite)
      {
            Write-Host "$id mot de passe modifié le $dateDernier"
      }
}
```

On accepte entre 360 et 366 jours …
`$limite = (get-date).AddYears(-1)` est également accepté

Le nom de la variable $dateDernier n'a pas d'importance mais doit être identique partout.

La réponse est valide même si le script n'est que partiellement recopié.

Question B2.1
Justifier le recours à la solution HAProxy pour renforcer la haute-disponibilité et la sécurité des services en ligne de la mairie et préciser l'importance de doubler les serveurs HAProxy.

Dans cette configuration, le HAProxy assure la répartition de charge sur les serveurs Web. De plus, en cas de défaillance d'un serveur Web le HAProxy dirigera les requêtes vers un serveur web fonctionnel.

La fonction de HA proxy peut aussi détecter les attaques de type DDos ou force brute.

En cas de défaillance du HAProxy actif, le HAProxy secondaire prend le relais et garantit ainsi la haute disponibilité. Le HAProxy secondaire est passif**.**

Les fonctions de répartition de charge de HAProxy assurent la disponibilité des services et des applications. Elles permettent une certaine maîtrise du trafic pendant les pics de charge, les pannes ou la maintenance des serveurs (PCA). Le HAProxy actif répartit le trafic entre l'ensemble des serveurs web, en cas d'augmentation permanente du trafic, l'ajout de serveurs supplémentaire sera facilité.

Question B2.2
Expliquer pourquoi il est obligatoire pour une Mairie d'utiliser un certificat TLS issu d'une autorité publique dans les échanges avec les administrés.

Notions à retrouver dans la réponse :

- Tiers de Confiance qui gère la validité publique des certificats.
- Le certificat de l'autorité de certification, installé sur tous les postes permet de vérifier la signature du certificat serveur.
- Certificat serveur automatiquement validé par le navigateur ➔ pas d'erreur de certificat.

On n'exige pas systématiquement ces 3 notions mais la compréhension d'une autorité de certification publique.

Question B2.3
Expliquer, pour chaque stratégie, sur quelles machines mettre en place les certificats et indiquer jusqu'où seront chiffrées les communications

Stratégie A – Les certificats des serveurs sont installés sur les serveurs HAProxy. La connexion entre les HAProxy et les serveurs Web n'est pas chiffrée.

Stratégie B - Le certificat reste installé sur les serveurs Web. Le serveur HAProxy fait juste une « redirection ». Les communications sont chiffrées jusqu'aux serveurs Web.

Une troisième stratégie est possible (certificat sur Proxy + serveur Web). On ne pénalise pas un candidat qui explique cette solution

Question B2.4
Ajouter les nouvelles règles de filtrage nécessaires pour que les serveurs HAProxy aient accès aux serveurs *web*.

Solution 1

N° règle	Action	Protocole	Source	Port source	Destination	Port destination
1	Block	any	MachineC2-525-CobaltStrike (IP : 193.29.13.201)	any	Firewall-out	any
…	…	…	…	…	…	…
9	Pass	TCP	VLAN-DSI (10.100.0.0/16)	any	Reseau_Dir_GS (10.10.0.0/16)	ssh (22)
10	Pass	TCP	Reseau_Dir_GS (10.10.0.0/16)	any	Reseau_DMZ (172.16.0.0/16)	https (443)
11	**Pass**	**TCP**	**HAProxy principal 172.16.0.10**	**Any**	**Serveur web 10.55.2.1**	**https (443)**
12	**Pass**	**TCP**	**HAProxy principal 172.16.0.10**	**Any**	**Serveur web redondé 10.55.2.2**	**https (443)**
13	**Pass**	**TCP**	**HAProxy secondaire 172.16.0.20**	**Any**	**Serveur web 10.55.2.1**	**https (443)**
14	**Pass**	**TCP**	**HAProxy secondaire 172.16.0.20**	**Any**	**Serveur web redondé 10.55.2.2**	**https (443)**

Les règles peuvent être placées avant la règle 9.
Le filtrage sur le port 80 (http) est accepté.
Solution 2

N° règle	Action	Protocole	Source	Port source	Destination	Port destination
1	Block	any	MachineC2-525-CobaltStrike (IP : 193.29.13.201)	any	Firewall-out	any
…	…	…	…	…	…	…
9	Pass	TCP	VLAN-DSI (10.100.0.0/16)	any	Reseau_Dir_GS (10.10.0.0/16)	ssh (22)
10	Pass	TCP	Reseau_Dir_GS (10.10.0.0/16)	any	Reseau_DMZ (172.16.0.0/16)	https (443)
11	**Pass**	**TCP**	**HAProxy principal 172.16.0.10**	**Any**	**Réseau serveurs Web 10.55.2.0/24**	**https (443)**
12	**Pass**	**TCP**	**HAProxy secondaire 172.16.0.20**	**Any**	**Réseau serveurs Web 10.55.2.0/24**	**https (443)**

Les règles peuvent être placées avant la règle 9.
Une solution utilisant l'adresse de réseau de la DMZ est acceptable.
Un sous réseau de /25 à /30 est accepté.
Le filtrage sur le port 80 (http) est accepté.

Question B3.1
a) Identifier les événements observés dans la capture de trames et donner une cause possible du problème.

- L'attaquant 10.15.0.5 envoie une multitude de paquets de type TCP SYN qui oblige le serveur à approuver la connexion, utilisant sa mémoire et ses ressources processeurs.
- Attaque « inondation TCP SYN » ou « TCP SYN flood » à partir de l'adresse 10.15.0.5
  L'attaquant semble se trouver sur le **même** réseau que le serveur.
- Il s'agit d'une attaque de type déni de service (DoS)

Le terme TCP SYN n'est pas obligatoirement attendu pour une bonne maitrise.

Question B3.1
b) Mettre en avant les conséquences sur les services fournis par la bibliothèque.

L'objectif final de l'attaquant est de saturer le serveur de la bibliothèque et d'empêcher les accès légitimes. Si l'attaque est fructueuse, le serveur ne sera plus accessible par les utilisateurs de la bibliothèque. Les prêts de livres risquent de ne plus être possible et le travail des salariés de la bibliothèque plus difficile.

Question B3.2
a) Lister les actions à entreprendre sur le commutateur de la bibliothèque afin de sécuriser les 42 prises murales.

- Fermer les ports 39 à 42.
- Ouvrir les ports 1 à 38 à une seule adresse MAC en dynamique.
- Configurer le blocage des adresses MAC inconnues.
- *Démarrer immédiatement les PC autorisés afin d'enregistrer automatiquement la bonne adresse MAC (non imposé car ce n'est pas une action sur le commutateur).*

Ne pas oublier la sauvegarde de la start-up config à la fin de l'intégration.

Question B3.2
b) Écrire les commandes à saisir sur le commutateur pour réaliser ces actions.

La commande pour fermer les ports sera :

```
Switch(config)# interface range fa0/39-42
Switch(config-if))# shutdown
```

Pour ouvrir un port à une seule adresse MAC en dynamique, on utilise le mode « *sticky* ».
Ne pas oublier la sauvegarde de la start-up config à la fin de l'intégration :

```
Switch(config)#interface range fa0/1-38
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security sticky
```

Dernière commande pour bloquer les adresses MAC inconnues :

```
Switch(config-if))# switchport port-security violation protect
On accepte aussi le shutdown a la place du protect.
```

Ne pas oublier de sauvegarder la config obtenue après connexion de TOUS les postes :

```
Switch# copy running-config startup-config
Ou Switch# copy run start
Ou write memory
```

La sauvegarde de la configuration n'est pas demandée.

L'ordre de configuration des différentes interfaces n'a pas d'importance.

DOSSIER C	**Réponse à un incident de sécurité**	**15 points**

Question C1.1
Rédiger un compte-rendu pour la phase d'investigation numéro 2 (identification) en précisant :
a) la cause première probable de l'incident ;

Cause première probable : clic sur un lien malveillant (contenu dans un courriel d'hameçonnage).

Cause possiblement confirmée par les déclarations de l'utilisateur et les journaux systèmes.

Question C1.1
Rédiger un compte-rendu pour la phase d'investigation numéro 2 (identification) en précisant :
b) la qualification de l'alerte de sécurité (incident de sécurité confirmé ou faux positif) en indiquant les indicateurs de compromission ;

Qualification de l'incident : incident de sécurité confirmé. Tentative d'infection par un virus de type rançongiciel (processus d'infection non terminé : virus rançongiciel non déployé sur le poste).

Indicateurs de compromission (IoC) :

- fichier P64.exe et fichier compos1524.txt présents dans le dossier PerfLogs de la machine infectée. (Noms de fichiers et répertoire (dossier PerfLogs) couramment utilisés par le groupe UNC1878) ;
- adresse IP du serveur de commande et contrôle (C&C), utilisé par le maliciel BazarLoader, contacté par la machine infectée (d'après les logs du proxy).

Toutefois, pas de hash du virus Ryuk (MD5 : 544900a527328f2e4fe7598985bc688f) trouvé sur le poste (certainement parce que l'utilisateur a déconnecté assez rapidement sa machine du réseau ; il faut entre 3 heures et 5 jours pour être infecté par un virus tel que Ryuk ; virus qui était certainement destiné au poste de l'utilisateur d'après le groupe identifié). Et pas de clé de registre (de persistance du virus) trouvée.

Question C1.1
Rédiger un compte-rendu pour la phase d'investigation numéro 2 (identification) en précisant :
c) la liste des autres machines du SI de la ville qui auraient pu être impactées par cet incident.

Toutes les machines contenant des partages réseaux accessibles par le poste de travail infecté.

On ne pénalisera pas un candidat qui limiterait l'impact aux ordinateurs ayant Microsoft Windows comme système d'exploitation.

Question C1.2
Lister des mesures à prendre pour éradiquer la menace présente sur la machine de l'utilisateur et retrouver un poste sain (phases d'éradication et de retour à la normale).

Mesures d'éradication possibles :

- supprimer le courriel malveillant ;
- supprimer tous les fichiers malveillants (issus des indicateurs de compromission publics) ;
- supprimer les éventuelles clés de registre malveillantes ;
- vérifier les partages réseaux à l'aide de différents anti-virus et anti-malwares ;
- passer le disque à l'analyse de différents anti-virus et anti-malwares ;
- supprimer d'éventuelles tâches planifiées (utilisées pour la persistance).

Toutefois, la mesure la plus efficace et la plus pertinente sera d'opter pour le mode « restauration ou réinstallation » :

- formater le disque de la machine infectée ;
- procéder à la réinstallation du système et des applications ;
- restaurer les données (si des données sont stockées sur le poste et non sur les serveurs) à partir d'un jeu de sauvegarde sain.

Une réponse comportant toutes les étapes d'une réinstallation correctement expliquées est suffisante.

Question C1.3
Lister trois autres mesures complémentaires à mettre en œuvre pour réduire davantage le risque d'hameçonnage et/ou ses conséquences.

Mesures complémentaires pour réduire le risque :

- sauvegarder régulièrement les données ;
- appliquer les correctifs réguliers pour diminuer les vulnérabilités des postes ;
- limiter au maximum les privilèges d'administration ;
- supervision des postes (connexions TCP, activité, etc.) ;
- organiser des exercices de simulation d'attaque et de réponse à incident pour entraîner les techniciens ;
- créer une procédure de signalement pour contacter rapidement le pôle PSIR en cas d'hameçonnage ou suspicion (politique de gestion des incidents) ;
- procéder à une analyse post-incident pour chaque incident et alimentation de la gestion des problèmes ;
- paramétrer le pare-feu des machines pour interdire les communications entre les postes (limitant ainsi les mouvements latéraux et/ou la propagation d'une menace) ; d'une façon générale : autoriser (au niveau du pare-feu) les flux uniquement nécessaires (strict minimum) ;
- mettre en place des VLAN privés (*private VLAN*) ;
- renforcer la veille cyber des employés de la DSI (nouvelles méthodes d'attaque, IoC, virus « du moment » : on retrouve souvent les mêmes virus à certaines périodes, outils ou techniques de protection ;
- etc.