BREVET DE TECHNICIEN SUPÉRIEUR
SERVICES INFORMATIQUES AUX ORGANISATIONS

Option : Solutions d'infrastructure, systèmes et réseaux

U6 – CYBERSÉCURITÉ DES SERVICES INFORMATIQUES

SESSION 2023

_____

Durée : 4 heures
Coefficient : 4

_____

Matériel autorisé :
Aucun matériel ni document n'est autorisé.

Dès que le sujet vous est remis, assurez-vous qu'il est complet.

Le sujet comporte 19 pages, numérotées de 1/19 à 19/19.

CAS VILLE DU PARC

Ce sujet comporte 19 pages dont un dossier documentaire de 12 pages.

Barème

DOSSIER A	**Évaluation des risques**	28 points
DOSSIER B	**Mesures de protection supplémentaires face aux menaces**	37 points
DOSSIER C	**Réponse à un incident de sécurité**	15 points
	TOTAL	80 points

Dossier documentaire

Présentation du contexte

Située en région parisienne, la ville du Parc[1] est une commune de taille moyenne de 50 000 habitants. La mairie, implantée dans le bâtiment de l'hôtel de ville, est l'appareil administratif de la ville. Ses attributions sont multiples : état-civil, voirie, logements, écoles, aides sociales, etc.

La mairie est organisée en différents services : dont le cabinet du maire, la direction générale des services, la direction voirie et espace public, la direction des espaces verts, la direction des systèmes d'information (DSI), etc.

Pour mener à bien leurs missions, les agents de la mairie doivent manipuler une grande quantité d'informations dans des domaines variés. Cela inclut des données à caractère personnel (des habitants[2], des employés, des entreprises localisées dans la ville ou partenaires, etc.) ou des données sensibles concernant l'activité générale de toute municipalité.

L'activité de la ville repose sur un système d'information (SI) administré par la DSI. Ce service, dirigé par M. Guy Aurat, s'articule autour de 4 pôles :

- le pôle sécurité et infrastructure réseaux (PSIR) composé de : 1 administratrice réseaux et sécurité et 4 techniciens réseaux et sécurité (dont un apprenti) ;
- le pôle infrastructure systèmes (PIS) composé de : 1 responsable d'exploitation, 1 administrateur systèmes et 2 techniciens systèmes ;
- le pôle support aux utilisateurs (PSU) composé de : 1 responsable support *Helpdesk* et 6 techniciens support ;
- le pôle applications métiers (PAM) composé de : 1 chef de projets et 2 développeurs.

Vous travaillez en tant que technicien(ne) réseaux et sécurité dans le pôle PSIR de la DSI.

La DSI gère plus de 60 sites (bâtiments), répartis dans toute l'agglomération, reliés au réseau « ville » par des liaisons en fibre optique appartenant à la commune. Parmi ces sites, on retrouve le site principal de l'hôtel de ville, le site de la DSI, les sites des écoles municipales, le site de la bibliothèque municipale, le site de la maison des associations, etc.

Le système d'information de la ville compte plus de 1 200 postes de travail et 1 300 comptes utilisateurs gérés par un annuaire *Microsoft Active Directory*.

Du fait de son statut de collectivité territoriale et dans le cadre du développement de l'administration électronique, la ville du Parc recourt de plus en plus aux usages numériques. Afin d'offrir des services publics continus et sûrs pour ses habitants, la ville se doit d'améliorer son système d'information contre les accidents pouvant survenir et de le sécuriser face à d'éventuels actes malveillants ou menaces sérieuses.

Vous vous appuierez sur le dossier documentaire mis à votre disposition.

[1] Pour des raisons de confidentialité, le nom de la ville et toutes les données s'y référant ont été modifiées.
[2] Un habitant de la ville peut également être désigné par les termes usager ou administré.

Dossier A – Évaluation des risques

Mission A1 – Identifier des données personnelles et sensibles

Via son site *web*, la ville propose à ses habitants de multiples services destinés à faciliter leurs démarches pour des actes d'état civil (demande ou renouvellement d'une carte d'identité, déclaration de naissance ou de décès), mais aussi les prises de rendez-vous. L'accès à ces services en ligne nécessite une inscription (création d'un compte personnel) et la saisie de nombreuses données personnelles ou sensibles telles que le nom, l'adresse postale, le numéro de téléphone, l'adresse de courriel, les noms et dates de naissance des enfants, les revenus ou encore le numéro de carte bancaire (utilisé pour le paiement de certaines prestations).

Lors de la dernière séance du conseil municipal, un élu a évoqué les risques grandissants dans le domaine de la sécurité informatique et cité plusieurs exemples de municipalités ayant fait l'objet de vols de données avec des conséquences importantes pour la ville et les administrés.

Monsieur Aurat vous demande, afin qu'il puisse préparer un « audit de sécurité des données personnelles » qui sera présenté lors de la prochaine séance du conseil municipal, de recenser les obligations auxquelles la ville est soumise.

Question A1.1

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

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.

Mission A2 – Évaluer les risques numériques

La DSI a déjà mis en place différentes solutions augmentant la résilience (capacité de résistance aux pannes) du système d'information de la ville en cas d'incidents, comme la panne d'un commutateur ou la défaillance d'un disque dur utilisé pour le stockage des données.

Question A2.1

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

Monsieur Aurat souhaite mener une analyse des risques pesant sur son système d'information pour identifier les principales mesures de sécurité et de sûreté à mettre en œuvre et ainsi renforcer son niveau de défense. Il a choisi de suivre la méthode EBIOS RM de l'agence nationale de la sécurité des systèmes d'information (ANSSI). Cette analyse s'est déroulée sur plusieurs semaines et a regroupé de nombreux acteurs, notamment la DSI, le maire, les élus et les responsables des différents services de la ville. Toutefois, certains éléments concernant les impacts et les mesures de sécurité à mettre en œuvre n'ont pas été étudiés en totalité.

Question A2.2

a) Évaluer les conséquences en termes de disponibilité, d'intégrité et de confidentialité sur le SI de la ville d'une attaque par rançongiciel[3] (*ransomware*) sur les serveurs.
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.
c) Lister les mesures déjà prises pour limiter ce risque.

Afin de limiter les risques liés à un rançongiciel, M. Aurat vous demande d'analyser deux solutions pour les postes de travail intégrées au système d'exploitation Windows : « Application Guard » et « Sandbox » (bac à sable).

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.

[3] Technique d'attaque courante de la cybercriminalité, le rançongiciel consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement. (source : ANSSI)

Dossier B – Mesures de protection supplémentaires face aux menaces

Mission B1 – Améliorer la stratégie des mots de passe

L'administrateur du PSIR a étudié la dernière version du guide de l'ANSSI relatif à l'authentification et aux mots de passe.

Il a relevé que les recommandations relatives au délai d'expiration des mots de passe avaient évolué.

En vérifiant la configuration de la stratégie de mots de passe du domaine *Active Directory*, il s'est rendu compte qu'aucun délai d'expiration n'est actuellement défini.

Il vous charge d'étudier la modification de cette stratégie.

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.

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

Avant de modifier la stratégie de mots de passe du domaine, l'administrateur veut connaitre l'impact de la mise à jour sur les utilisateurs. Il voudrait notamment connaitre la liste des utilisateurs à privilèges qui devront renouveler leur mot de passe.

Vous prenez en charge la récupération de cette information en utilisant un script *Powershell*. Un script ayant une autre fonction vous est présenté dans le dossier documentaire.

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.

Mission B2 – Renforcer la haute-disponibilité des services *web*

Le portail *web* de la ville, à partir duquel les habitants peuvent accomplir des démarches en ligne, est hébergé sur un serveur *web* situé en zone démilitarisée (DMZ). À certaines périodes, le site *web* de la ville subit des pics de trafic ralentissant considérablement le service. L'indisponibilité du portail *web* constituerait un incident majeur pour la mairie.

Devant l'augmentation des usages ainsi que dans le cadre de son plan de continuité d'activité (PCA), l'administrateur du PSIR réfléchit à une solution permettant d'améliorer la disponibilité des services *web*. La solution HAProxy serait privilégiée.

Le serveur mandataire HAProxy serait placé dans la zone démilitarisée (DMZ) publique de la mairie à la place des serveurs *web* qui seraient déplacés dans un nouveau réseau local virtuel (VLAN) spécifique pour les serveurs *web* (VLAN 55).

Un schéma de la nouvelle infrastructure de la zone démilitarisée a été élaboré et est présenté dans le dossier documentaire.

Votre responsable vous demande de valider cette solution.

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.

Le serveur *web* est protégé par un certificat acquis auprès d'un organisme agréé afin d'assurer la sécurité des connexions via le protocole HTTPS des habitants.

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.

Les serveurs HA proxy ont été installés, mais l'administrateur du PSIR s'interroge sur la stratégie de certificats à mettre en œuvre. Ces stratégies sont décrites dans le dossier documentaire.

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

L'installation des deux répartiteurs de charge HAProxy dans la zone démilitarisée (DMZ) a entraîné le déplacement des deux serveurs *web* dans un nouveau réseau local virtuel (VLAN) spécifique pour les serveurs *web* (VLAN 55 SERVEURS_WEB). En conséquence, l'adressage IP des serveurs *web* a été modifiée.

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

Mission B3 – Sécuriser le réseau local de la bibliothèque

La bibliothèque municipale met à disposition de ses abonnés une quarantaine de postes informatiques en libre-service. Le pôle PSIR a remarqué que des abonnés débranchaient les ordinateurs des prises RJ45 murales pour y brancher leur propre machine portable.

La modification des branchements des prises RJ45 peut entraîner des risques si un abonné a des intentions malveillantes et voit ses attaques facilitées par sa présence physique sur le réseau (par exemple une attaque par usurpation DHCP – *DHCP spoofing –)*.

La bibliothèque municipale a conservé dans ses murs un serveur qui lui sert pour l'application de gestion des prêts et pour partager des fichiers entre les employés de cette bibliothèque. Le pôle PSIR a été prévenu que ce serveur semblait parfois saturé et mettait du temps à répondre. Il l'a mis sous surveillance et a réalisé des captures de trames pour analyse.

Question B3.1
a) Identifier les évènements observés dans la capture de trames et donner une cause possible du problème.
b) Mettre en avant les conséquences sur les services fournis par la bibliothèque.

Sur les 42 prises, 38 sont utilisées (prises B01 à B38) pour les postes PC de la bibliothèque et 4 sont inutilisées (prises B39 à B42). Toutes sont brassées sur les ports d'un commutateur (situé dans une baie de brassage) en respectant le numéro de la prise et le numéro de l'interface (prise B0<u>5</u> brassée sur l'interface fa0/<u>5</u> du commutateur).

L'administrateur du pôle PSIR a décidé de sécuriser les ports en limitant l'accès aux seules machines de la bibliothèque sans avoir à collecter manuellement l'ensemble des adresses MAC.

Question B3.2
a) Lister les actions à entreprendre sur le commutateur de la bibliothèque afin de sécuriser les 42 prises murales.
b) Écrire les commandes à saisir sur le commutateur pour réaliser ces actions.

Dossier C – Réponse à un incident de sécurité

Ce dossier ne comporte qu'une seule mission.

Mission C1 – Analyser et investiguer l'incident

Le pôle PSIR a été alerté par un utilisateur du service de l'état civil qui a cliqué, par mégarde, sur un lien suspect présent dans un courriel. Grâce à la campagne de sensibilisation à l'hameçonnage (*phishing*) menée auprès du personnel, l'utilisateur a eu le réflexe de déconnecter le poste informatique du réseau.

En tant que technicien(ne) du pôle sécurité, vous prenez en charge cette alerte en menant les investigations adéquates et intervenez directement dans la phase d'identification.

Lors des premières investigations, les journaux d'évènements de la machine ont été extraits. Les journaux des connexions HTTP et HTTPS ont été extraits du serveur mandataire (*proxy*) et ont révélé des connexions vers l'adresse IP 34.217.209.239. Toutefois, aucune empreinte (*hash* ou condensé) de virus connus (tel que Ryuk) ou création de clé de registre n'a été relevée sur le poste de travail.

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 ;
b) la qualification de l'alerte de sécurité (incident de sécurité confirmé ou faux positif) en indiquant les indicateurs de compromission ;
c) la liste des autres machines du SI de la ville qui auraient pu être impactées par cet incident.

Le poste compromis a été rapidement isolé du réseau pour empêcher la propagation de l'attaque et contenir la menace. Il faut désormais tenter d'éliminer les éléments d'infection.

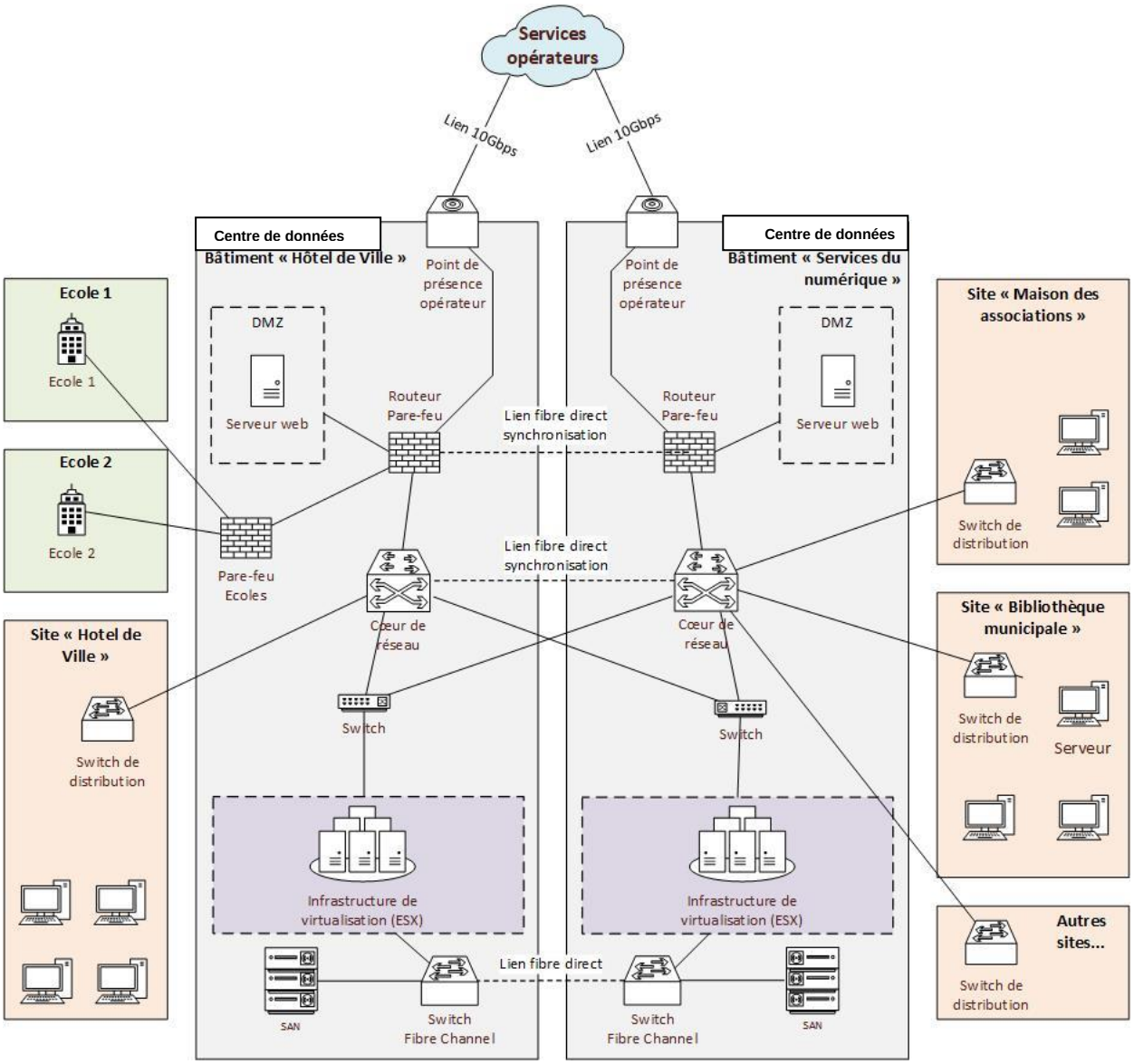
Question C1.2
Lister des mesures à prendre pour éradiquer la menace présente sur la machine de l'utilisateur et retrouver un poste sain (phases d'éradication et de retour à la normale).

Lors d'une précédente évaluation des risques, la DSI avait mis en évidence le risque d'hameçonnage et avait, comme mesure principale, choisi la formation et la sensibilisation des utilisateurs.

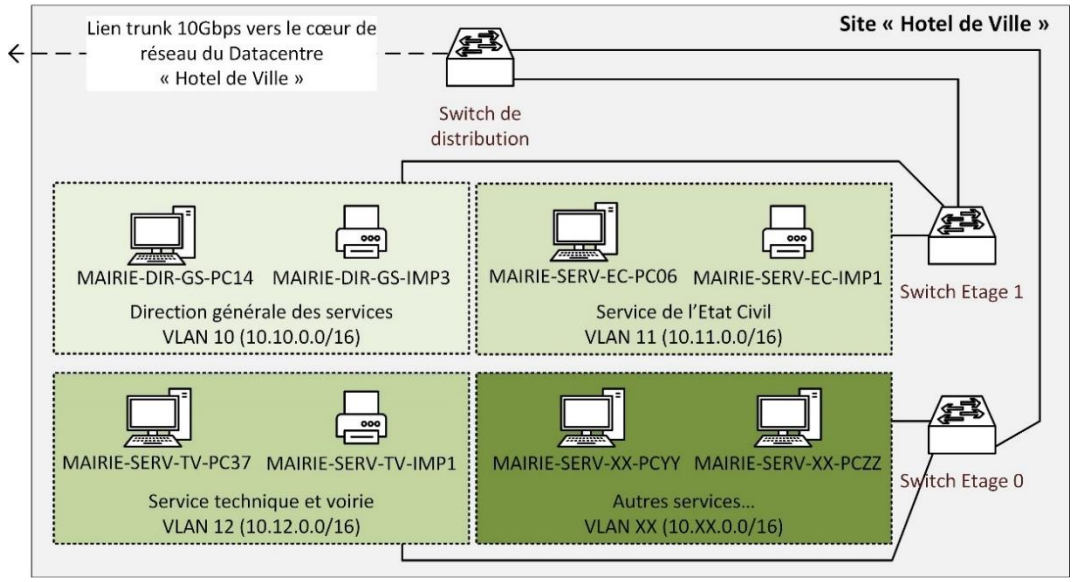
La phase n° 6 « Enseignements » du plan de réponse à incident amène à tirer les conclusions sur l'incident et les actions de formations déjà menées. Vous participez à la réunion d'analyse post-incident et devez proposer des recommandations de sécurité.

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

Document 1 : Schéma de l'infrastructure réseau de la ville



Document 2 : Schéma (extrait) de l'infrastructure du site « hôtel de ville »



Les noms des machines sont donnés à titre d'exemples.

Document 3 : Éléments complémentaires sur l'infrastructure du SI de la ville

- **Infrastructure de niveau 2 privilégiée**

La ville dispose de son propre réseau fibre optique (réalisé lors de travaux il y a quelques années). Les 60 sites géographiques gérés par la DSI sont reliés avec des liaisons en fibre optique longues distances et sont considérés comme faisant partie du réseau local (LAN). Il s'agit d'une infrastructure de type Metro Ethernet (réseau de niveau 2 sur une zone géographique étendue). Tous les réseaux locaux virtuels (VLAN) sont routés sur le cœur de réseau (qui analyse les étiquettes 802.1q) via des liens 10 Gbps.

- **Infrastructure redondée**

Dans le cadre d'un plan de continuité de l'activité (PCA), l'infrastructure réseau a été redondée avec 2 salles serveurs et 2 cœurs de réseau répartis sur 2 sites géographiques différents : un à l'hôtel de ville et un dans le bâtiment « Services du numérique ».

- **Services exposés**

Tous les services exposés sur internet (comme le site *web* de la ville) sont regroupés dans une zone démilitarisée (DMZ).

Adresse réseau de la zone démilitarisée : 172.16.0.0/16.

- **Serveurs**

6 serveurs physiques dotés de l'hyperviseur ESX (3 dans chaque centre de données), configurés en grappe (*cluster*) avec une fonctionnalité de basculement en cas d'incident sur un des serveurs physiques, virtualisent plus de 60 serveurs (serveurs de fichiers, serveurs LDAP *Active Directory*, serveurs DNS, serveurs de supervision, serveurs de gestion du service informatique, serveurs de messagerie, etc.).

- **Disponibilité des données**

Les données sont stockées dans 2 baies de stockage SAN (200 To x 2) configurées selon la technologie RAID de niveau 50. Chaque baie est reliée en fibre optique aux serveurs de virtualisation via un commutateur *Fibre Channel*. Les données sont répliquées (par un lien de synchronisation fibre) entre les 2 centres de données (*datacenters*).

- **Disponibilité dans le réseau local (LAN)**

Le protocole RSTP (*Rapid Spanning Tree Protocol*) est activé sur tous les commutateurs afin d'avoir une topologie redondante sans boucle.

- **Locaux sécurisés**

Les salles serveurs sont équipées de portes avec accès par badge et biométrie, d'un système de vidéosurveillance, d'un dispositif alarme-incendie, d'une double climatisation et d'un courant fort ondulé.

- **Sauvegardes**

Les sauvegardes sont gérées par 2 équipements de la solution *VeeamBackup* (sauvegardes complètes et incrémentielles). Les sauvegardes sont chiffrées. Une empreinte (*hash ou condensé*) est effectuée pour l'intégrité. Les jeux de sauvegardes sont stockés sur 2 sites géographiques différents, sur des supports déconnectés du réseau et nécessitent une habilitation pour accéder au contenu. Des exercices de restauration sont réalisés régulièrement pour éprouver les procédures et vérifier les sauvegardes.

- **Pare-feu (*firewall*) et anti-virus**

Les contrôles de flux (ainsi que l'analyse anti-spam) sont assurés par plusieurs pare-feux (*firewalls*) et serveurs mandataires (*proxies*). L'accès réseau aux écoles est contrôlé par un pare-feu supplémentaire et configuré spécialement pour protéger les utilisateurs mineurs.

L'analyse anti-virus repose sur une solution professionnelle.

- **Serveur de centralisation des journaux (logs)**

Les journaux des serveurs, commutateurs, routeurs et pares-feux sont centralisés sur une machine de centralisation (adresse IP : 10.50.1.100, appartenant au réseau local virtuel *VLAN* 50 « SERVEURS »).

Document associé au dossier A

Document A1 : Extraits de l'analyse de risques EBIOS RM pour le SI de la ville

Rappel de l'objectif : EBIOS RM (expression des besoins et identification des objectifs de sécurité – *risk manager*) est une méthode d'appréciation et de traitement des risques numériques publiée par l'ANSSI. Elle permet d'identifier les mesures de sécurité à mettre en œuvre pour les maîtriser et définir un niveau de sécurité à atteindre pour un service. Elle se base sur différents scénarios et se concentre sur les menaces intentionnelles. La méthode est décomposée en 5 « ateliers ».

ATELIER 1 : CADRAGE ET SOCLE DE SECURITÉ

Cette étape a recensé les valeurs métier (informations et processus importants) susceptibles d'être attaquées, les besoins de sécurité associés (en termes de disponibilité, confidentialité, intégrité, etc.) et les biens supports (éléments du SI sur lesquels les valeurs métier reposent) ; ensuite, les évènements redoutés sont identifiés et la gravité caractérisée.

Extrait :

VALEUR MÉTIER	ÉVÈNEMENT REDOUTÉ	IMPACTS	GRAVITÉ
Fournir un service pour les actes d'état-civil (passeport, carte nationale d'identité, etc.)	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**
Fournir un service de santé avec le centre municipal de santé	Perte ou destructions des données de santé des habitants	▪ Impacts sur les missions et services de la mairie ▪ Impacts sur l'image et la confiance ▪ Impacts juridiques, etc.	**4/4**

ATELIER 2 : SOURCES DE RISQUES

Cette étape a permis d'identifier les sources de risques les plus pertinentes et leurs objectifs visés.

Extrait :

SOURCES DE RISQUE	OBJECTIFS VISÉS	MOTIVATION	RESSOURCES	ACTIVITÉ	PERTINENCE
Cyber-terroriste	Voler les informations personnelles des usagers dans un but financier	**+ +**	**+ + +**	**+**	**Moyenne**
Cyber-terroriste	Bloquer le SI avec demande de rançon sans exfiltrer les données	**+ + +**	**+ + +**	**+ +**	**Haute**
Usager malveillant	Accéder à des données sensibles sans autorisation en exploitant une faille	**+**	**+**	**+**	**Faible**

ATELIER 3 : SCÉNARIOS STRATÉGIQUES

Cette étape a permis d'identifier les parties prenantes externes les plus vulnérables et de bâtir des scénarios stratégiques (chemins d'attaques que pourrait emprunter une source de risque pour atteindre son objectif).

Extrait :

PARTIE PRENANTE	CHEMINS D'ATTAQUE STRATÉGIQUES	MESURES DE SECURITÉ	MENACE INITIALE	MENACE RÉSIDUELLE
Prestataire informatique	Vol d'informations en passant par le prestataire informatique	Accroître la maturité cyber du prestataire. Solutions à investiguer : audit de sécurité, etc.	2/5	1,2/5

ATELIER 4 : SCÉNARIOS OPÉRATIONNELS

Cette étape a détaillé les scénarios opérationnels, c'est-à-dire les modes opératoires que pourraient mettre en œuvre les sources de risque pour réaliser les scénarios stratégiques.

Extrait :

CHEMINS D'ATTAQUES STRATÉGIQUES (ASSOCIÉS AUX SCÉNARIOS OPÉRATIONNELS)	VRAISEMBLANCE GLOBALE
Une personne malveillante (pirate) compromet un logiciel fourni par un prestataire et utilisé dans le SI de la mairie (vol de données par une porte dérobée)	Peu vraisemblable (2/4)
Un groupe de pirates envoie un courriel d'hameçonnage à un utilisateur du réseau et crée une porte dérobée pour exfiltrer des données	Très vraisemblable (4/4)
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)

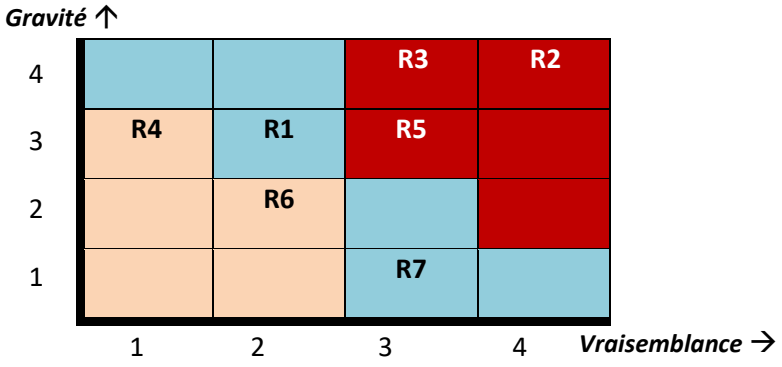
ATELIER 5 : TRAITEMENT DU RISQUE

Cette dernière étape (inachevée) permettra de définir une stratégie de traitement du risque avec une série de mesures de sécurité à mettre en œuvre.

Extrait de la synthèse des scénarios de risques :

- *R1 : un utilisateur du réseau tente d'accéder à des données sans autorisation*
- *R4 : un utilisateur ne respecte pas l'interdiction et se connecte au réseau de la ville avec sa propre machine (infectée par un virus)*
- *[…]*

Matrice des scénarios de risques dans le cadre du SI de ville :



Stratégie de traitement des risques dans le cadre du SI de ville :

Extrait :

MESURE DE SÉCURITÉ	SCÉNARIOS DE RISQUES ASSOCIÉS	RESPONSABLE	FREINS ET DIFFICULTÉS DE MISE EN OEUVRE	COÛT / COMPLEXITÉ	ÉCHÉANCE	STATUT
Sensibilisation à l'hameçonnage	R2, R3	DSI, entreprise spécialisée		+	3 mois	Terminée
Audit de sécurité de l'ensemble du SI	Rx	DSI, pôle PSIR	Nécessite une cartographie complète et à jour	+ + +	6 mois	En cours
Surveillance renforcée des flux entrants et sortants	R2, R3	Pôle PSIR	Besoin de veille (signes d'infection - IOC à surveiller)	+	1 mois	En cours
Protection renforcée des données	R1, R2, R3	Pôle PIS		+	1 mois	À lancer
Analyse des journaux d'évènements à l'aide d'un outil	R1, R2, R3, R4	Pôle PSIR	Quantité de logs	+ +	2 mois	À lancer
Renforcement du PCA	Rx	DSI	Prévoir une solution cloud	+ + +	12 mois	À lancer
…	…	…	…	…	…	…

Rx = Tous les scénarios de risques
Source : d'après le « Guide EBIOS Risk Manager » de l'ANSSI

Document A2 : Applications de protection

Le logiciel « *Application Guard* » permet d'isoler les sites non définis par l'entreprise. L'administrateur définit les sites *web* approuvés, les ressources en nuage (*cloud*) et les réseaux internes. Tout ce qui ne figure pas sur la liste est considéré comme non approuvé. Si un employé se rend sur un site non approuvé via un navigateur *Microsoft Edge*, *Firefox* ou *Google Chrome*, le navigateur ouvre le site dans un conteneur isolé.

Le logiciel « *Application Guard* » empêche les fichiers *Word*, *PowerPoint* et *Excel* non fiables d'accéder aux ressources fiables. Il ouvre les fichiers non approuvés dans un conteneur isolé. Le conteneur isolé est distinct du système d'exploitation hôte.

Le bac à sable (*sandbox*) intégré au système *Windows* depuis la version 10 est un secteur isolé du reste du système d'exploitation. Cet environnement offre les mêmes fonctions qu'une version classique de *Windows*. Lorsque l'utilisateur l'active, le bac à sable fonctionne comme un nouvel ordinateur sans application ou programme installé.

Dans cet environnement virtuel, il est possible d'installer et d'exécuter un programme non vérifié. Si le logiciel est malveillant et contient un virus, cela n'a aucun impact sur le système d'exploitation. Lorsque le bac à sable de *Windows* est fermé, tous les programmes et les données qu'il contient sont automatiquement et définitivement supprimés.

Documents associés au dossier B

Document B1 : Recommandations relatives à l'authentification multifacteur et aux mots de passe (extraits)

Délai d'expiration des mots de passe

Le choix d'imposer ou non un délai d'expiration fixe est un sujet qui a évolué ces dernières années. Fixer un délai d'expiration sur des moyens d'authentification est une bonne mesure en général mais s'avère souvent contre-productif dans le cas des mots de passe. […]

Pour des comptes peu sensibles, imposer un délai d'expiration trop court (3 à 6 mois par exemple) peut se révéler contre-productif étant donné les comportements des utilisateurs observés lorsqu'ils sont soumis à ce type de contrainte. En revanche, pour les comptes très sensibles comme les comptes à privilèges, conserver un délai d'expiration des mots de passe reste une bonne mesure à mettre en œuvre.

R24 : Ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles
Si la politique de mots de passe exige des mots de passe robustes et que les systèmes permettent son implémentation, alors il est recommandé de ne pas imposer par défaut de délai d'expiration sur les mots de passe des comptes non sensibles comme les comptes utilisateur.

R25 : Imposer un délai d'expiration sur les mots de passe des comptes à privilèges
Il est recommandé d'imposer un délai d'expiration sur les mots de passe des comptes très sensibles comme les comptes administrateurs. Ce délai d'expiration peut par exemple être fixé à une durée comprise entre 1 et 3 ans.

En cas d'incidents de sécurité (comme une suspicion de compromission de la base de données contenant des mots de passe), une expiration immédiate des mots de passe des comptes concernés doit être imposée.

Source : d'après le « Guide de recommandations relatives à l'authentification multifacteur et aux mots de passe » de l'ANSSI

Document B2 : Script PowerShell de surveillance des comptes

Un domaine « *Active Directory* » dans une architecture *Microsoft Windows* dispose automatiquement d'un certain nombre de groupes de niveau « Administrateur » ; l'utilisation normale consiste à créer des comptes dans le groupe « Admins du domaine ». Toutefois d'autres groupes de niveau administrateur existent, notamment le groupe « Administrateurs de l'entreprise ».

Le script suivant permet de détecter les comptes appartenant au groupe « Admins du domaine » **ne s'étant pas connectés depuis plus de 6 mois (180 jours)**.

```
01 # définition du groupe à traiter
02 $groupe = "Admins du domaine"
03
04 # Sélection de la liste des membres d'un groupe
05 $membres = Get-ADGroupMember -Identity $groupe -Recursive
06
07
08 # Affichage des utilisateurs n'ayant pas été logués depuis plus de 6 mois
09 # La collection $membres contient la liste des utilisateurs
10 foreach($un_membre in $membres)
11 # Boucle automatique parcourant la liste
12 {
13       $id = $un_membre.SamAccountName
14       # identifiant / login de l'utilisateur
15
16       $user = Get-ADUser -Identity $id -properties *
17       # Récupération des propriétés de l'utilisateur
18
19       $dateDerniere = $user.LastLogonDate
20       # Date de dernière ouverture de session
21
22       $limite =(get-date).AddDays(-180)
23       # Calcul de date système moins 6 mois
24
25       # Test pour déterminer si la date est antérieure
26       # à la limite de 180 jours
27       if($dateDerniere -lt $limite)
28       # Plus petit que, lower than, noté "-lt"
29       {
         Write-Host "$id connecté le $dateDerniere"
         # Affichage de l'id et de la date de connexion
         }
}
```

Exemples de propriétés de l'objet « utilisateur »

`AccountExpirationDate`	Date d'expiration du compte
`CannotChangePassword`	Si true = impossible de modifier le mot de passe
`LastLogonDate`	Date de dernière connexion
`LogonCount`	Nombre de connexions du compte
`PasswordLastSet`	Date de dernière modification du mot de passe
`PasswordNeverExpired`	Si true = Le mot de passe n'expire jamais

Opérateurs en Powershell

`-lt` : lower than, plus petit que

`-gt` : greater than, plus grand que

`-eq` : equal, égal à

`-ne` : not equal, différent de

Document B3 : Présentation de la solution HAProxy

HAProxy est un logiciel libre (*open source*), sous Linux, offrant des solutions de serveur mandataire (*proxy*) et de répartition de charge TCP/HTTP. Il assure la disponibilité des serveurs et applications même pendant des pics de charge, des pannes ou des périodes de maintenance, en répartissant les requêtes sur de multiples serveurs.

Une infrastructure basée sur la solution HAProxy enlève les points de défaillance unique (*single point of failure - SPOF*).

De plus, la solution HAProxy peut détecter et stopper les attaques de type déni de service distribué (DDoS) ou force brute. Une journalisation avancée permet d'identifier les intrusions et d'assurer la conformité aux protocoles réseaux.

La solution comprend 2 parties :

- une partie dite ***Frontend*** : cette partie écoute sur un port (par exemple le port HTTPS 443) et réceptionne les requêtes avant de les transmettre à la partie *Backend*.
- une partie dite ***Backend*** : cette partie désigne les serveurs qui recevront les requêtes transmises par la partie *Frontend* ; la répartition entre les serveurs de la partie *backend* sera faite selon l'algorithme de répartition choisi (souvent *Round-Robin* qui transmet les requêtes à chaque serveur à tour de rôle).

Source : d'après haproxy.com

Document B4 : Certificats et solution HAProxy

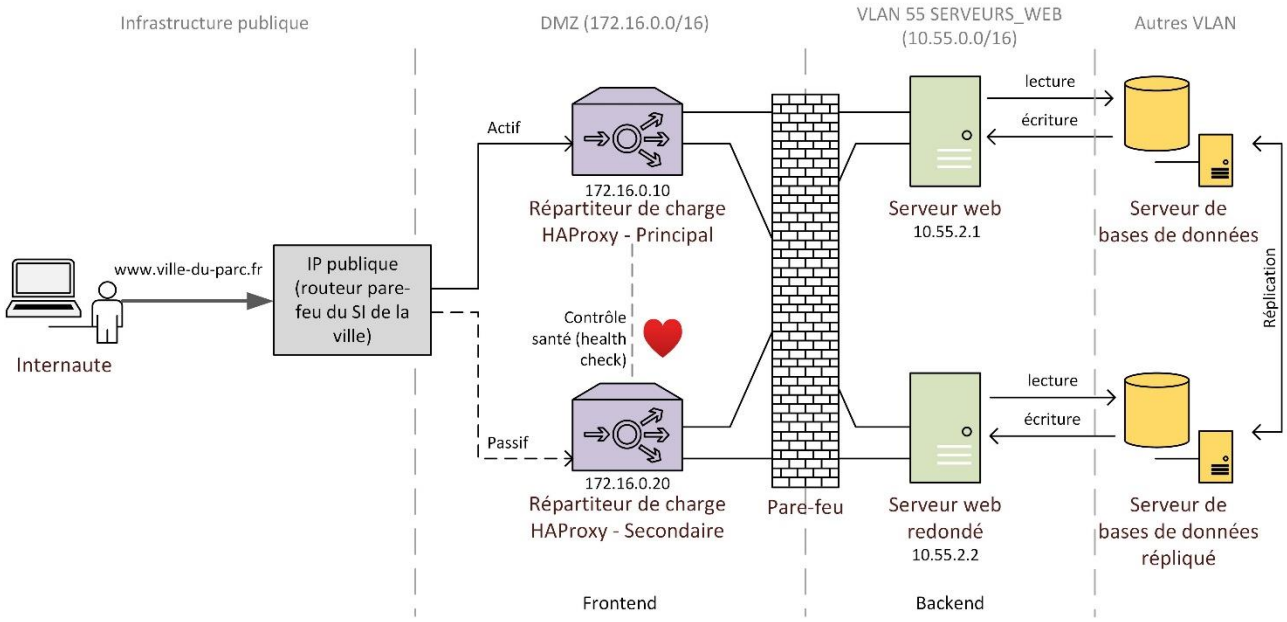
Une configuration simple d'un serveur voit généralement la connexion TLS d'un client déchiffrée par le serveur recevant la demande.

Il existe deux stratégies principales lorsque l'on met un équilibreur de charge entre un client et un ou plusieurs serveurs.

A : la terminaison TLS est la pratique consistant à terminer/déchiffrer une connexion TLS au niveau de l'équilibreur de charge et à envoyer des connexions non chiffrées aux serveurs principaux. Cela signifie que l'équilibreur de charge est responsable du déchiffrage d'une connexion TLS.

B : la terminaison TLS « *Pass-Through* » permet que la connexion soit simplement acheminée via l'équilibreur de charge vers les serveurs.

Document B5 : Schéma de principe d'infrastructure de la zone démilitarisée (DMZ) du SI de la ville avec la solution HAProxy



Document B6 : Extrait de la table de filtrage du pare-feu de périmètre

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)
…	…	…	…	…	…	….

Remarques : la règle de blocage total par défaut est implicite.

Il s'agit de filtrage en mode « *stateful* », les règles de retour sont donc implicites.

Document B7 : Capture de l'analyseur de trames Wireshark de l'activité sur le serveur de la bibliothèque (extrait)

Adresse IP du serveur : 10.15.0.253/16.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.15.0.5	10.15.0.253	TCP	60	1948 → 445 [SYN] Seq=0 Win=64 Len=0
2	0.000000	10.15.0.5	10.15.0.253	TCP	60	1949 → 445 [SYN] Seq=0 Win=64 Len=0
3	0.000000	10.15.0.5	10.15.0.253	TCP	60	1950 → 445 [SYN] Seq=0 Win=64 Len=0
4	0.000000	10.15.0.5	10.15.0.253	TCP	60	1951 → 445 [SYN] Seq=0 Win=64 Len=0
5	0.000093	10.15.0.253	10.15.0.5	TCP	58	445 → 1948 [SYN, ACK] Seq=0 Ack=1 Win=65392
6	0.000156	10.15.0.253	10.15.0.5	TCP	58	445 → 1949 [SYN, ACK] Seq=0 Ack=1 Win=65392
7	0.000242	10.15.0.253	10.15.0.5	TCP	58	445 → 1950 [SYN, ACK] Seq=0 Ack=1 Win=65392
8	0.000321	10.15.0.253	10.15.0.5	TCP	58	445 → 1951 [SYN, ACK] Seq=0 Ack=1 Win=65392
9	0.000573	10.15.0.5	10.15.0.253	TCP	60	1952 → 445 [SYN] Seq=0 Win=64 Len=0
10	0.000573	10.15.0.5	10.15.0.253	TCP	60	1953 → 445 [SYN] Seq=0 Win=64 Len=0
11	0.000573	10.15.0.5	10.15.0.253	TCP	60	1954 → 445 [SYN] Seq=0 Win=64 Len=0
12	0.000573	10.15.0.5	10.15.0.253	TCP	60	1955 → 445 [SYN] Seq=0 Win=64 Len=0
13	0.000573	10.15.0.5	10.15.0.253	TCP	60	1956 → 445 [SYN] Seq=0 Win=64 Len=0
14	0.000573	10.15.0.5	10.15.0.253	TCP	60	1957 → 445 [SYN] Seq=0 Win=64 Len=0
15	0.000573	10.15.0.5	10.15.0.253	TCP	60	1958 → 445 [SYN] Seq=0 Win=64 Len=0
19	0.000666	10.15.0.253	10.15.0.5	TCP	58	445 → 1952 [SYN, ACK] Seq=0 Ack=1 Win=65392
20	0.000704	10.15.0.253	10.15.0.5	TCP	58	445 → 1953 [SYN, ACK] Seq=0 Ack=1 Win=65392
21	0.000744	10.15.0.253	10.15.0.5	TCP	58	445 → 1954 [SYN, ACK] Seq=0 Ack=1 Win=65392
22	0.000816	10.15.0.253	10.15.0.5	TCP	58	445 → 1955 [SYN, ACK] Seq=0 Ack=1 Win=65392
23	0.000893	10.15.0.253	10.15.0.5	TCP	58	445 → 1956 [SYN, ACK] Seq=0 Ack=1 Win=65392
24	0.000936	10.15.0.253	10.15.0.5	TCP	58	445 → 1957 [SYN, ACK] Seq=0 Ack=1 Win=65392
25	0.000984	10.15.0.253	10.15.0.5	TCP	58	445 → 1958 [SYN, ACK] Seq=0 Ack=1 Win=65392
27	0.001156	10.15.0.5	10.15.0.253	TCP	60	1959 → 445 [SYN] Seq=0 Win=64 Len=0
28	0.001156	10.15.0.5	10.15.0.253	TCP	60	1960 → 445 [SYN] Seq=0 Win=64 Len=0
29	0.001156	10.15.0.5	10.15.0.253	TCP	60	1961 → 445 [SYN] Seq=0 Win=64 Len=0
30	0.001156	10.15.0.5	10.15.0.253	TCP	60	1962 → 445 [SYN] Seq=0 Win=64 Len=0
31	0.001156	10.15.0.5	10.15.0.253	TCP	60	1963 → 445 [SYN] Seq=0 Win=64 Len=0
32	0.001156	10.15.0.5	10.15.0.253	TCP	60	1964 → 445 [SYN] Seq=0 Win=64 Len=0

Des milliers de lignes identiques sont présentes dans la capture.

Document B8 : Procédure de connexion via le protocole TCP

1. Un client souhaitant établir une connexion au serveur envoie un paquet SYN (de l'anglais *synchronize*, signifiant synchroniser).
2. Lorsque le serveur reçoit le segment, il approuve la connexion en renvoyant un paquet SYN-ACK (de l'anglais *acknowledgement*, signifiant confirmation).
3. Pour finir, le client confirme la réception du paquet SYN-ACK en envoyant un paquet ACK.
4. Les échanges de données peuvent débuter.

Ces échanges sont appelés « *3-Way Handshake* » ou « poignée de main en trois temps ». Sans le dernier échange (ACK), le serveur « réserve » la connexion pour chaque paquet SYN reçu.

Document B9 : Commandes de sécurisation des ports pour les commutateurs CISCO

Commandes courantes :

Commande (par l'exemple)	Description
`Switch(config)# interface fa0/1`	Accéder à l'interface fastEthernet 0/1 du commutateur
`Switch(config)# interface range fa0/1-42`	Accéder aux interfaces de fa0/1 à fa0/42
`Switch(config-if))# shutdown`	Éteindre l'interface sélectionnée préalablement

Commandes sur les ports pour limiter l'accès à certaines adresses MAC (soit en enregistrant manuellement l'adresse MAC soit en prenant comme adresse MAC autorisée celle de la machine qui se connectera en premier) :

Commande (par l'exemple)	Description
`Switch# show port-security`	Voir la politique de sécurité
`Switch# show port-security address`	Voir les adresses MAC autorisées sur chacun des ports sécurisés
`Switch# show port-security interface fa0/1`	Voir en détail la sécurité de l'interface fa0/1

`Switch(config)# int fa0/1`
`Switch(config-if)# switchport mode access`
`Switch(config-if)# switchport port-security`
`Switch(config-if)# switchport port-security maximum 10`
`Switch(config-if)# sw port-sec mac-add AAAA.AAAA.0001`
(commande fonctionnelle écrite en abrégé)
	Sécuriser manuellement l'interface fa0/1
	- avec 10 adresses MAC maximum
	- pour l'adresse MAC AA:AA:AA:AA:00:01

`Switch(config)# int fa0/1`
`Switch(config-if)# switchport mode access`
`Switch(config-if)# switchport port-security`
`Switch(config-if)# switchport port-security maximum 10`
`Switch(config-if)# switchport port-security sticky`
	Sécuriser automatiquement l'interface fa0/1
	- avec 10 adresses MAC maximum

Configuration de la réaction en cas de violation de la sécurité :

- *shutdown* : désactive l'interface
- *protect* : bloque les adresses MAC inconnues
- *restrict* : alerte SNMP envoyée et compteur de violation incrémenté

Commande (par l'exemple)	Description
`Switch(config-if))# switchport port-security violation protect`	Passer la sécurité du port en mode protect

Source : it-connect.fr

Documents associés au dossier C

Document C1 : Le plan de réponse à incident

La réponse à incident suit généralement un modèle bien défini. Le SANS Institute (qui regroupe les plus grands professionnels de la cybersécurité) a publié son manuel de prise en charge des incidents (*Handler's Handbook*) il y a quelques années. Il reste la référence en matière de plans de réponse aux incidents. Il s'agit d'un cadre en 6 étapes ou phases, utilisable pour établir un plan adapté à chaque organisation.

Phase n°1 - Préparation

Pour garantir une réponse réussie à un incident, il est essentiel de s'y préparer en pratiquant des exercices simulant des attaques (attaques DDoS, logiciels malveillants, menaces internes, accès non autorisés, hameçonnage, etc.). Les procédures doivent être testées sur les personnes et les équipes qui seront en charge de la réponse.

Phase n°2 - Identification

Pour mettre fin à une menace de sécurité, il faut connaître la taille et la portée de l'incident. En trouvant le premier appareil à avoir été compromis, l'objectif est de comprendre la cause première. Mais il est possible que la menace se soit répandue latéralement. Un incident n'est réellement identifié que lorsque l'on recueille des signes d'infection (IOC) utiles. Plutôt que de réinitialiser le premier appareil infecté, il faut chercher à identifier tout signe d'infection unique, pouvant être utilisé ensuite pour analyser l'infrastructure à la recherche d'autres signes d'infection. Si l'incident est lié à une infection de logiciel malveillant (*malware*), il faut se poser les questions suivantes : quelles connexions réseau le malware génère-t-il ? Le logiciel malveillant (*malware*) s'est-il connecté à des domaines en particulier ? Quels fichiers ont été créés sur le disque ? Quels processus d'exécution ont été créés ? Des clés de registre uniques ont-elles été créées ? Ces données peuvent ensuite être utilisées pour rechercher d'autres traces d'infection et identifier les autres machines infectées sur le réseau.

Phase n°3 - Confinement

Une fois que la portée de l'incident a bien été identifiée, le processus de confinement peut démarrer. Les appareils compromis dans l'infrastructure sont alors isolés du reste du réseau pour arrêter la progression de l'attaque. Un confinement à court terme peut être utilisé pour isoler un appareil ciblé par le trafic de l'attaque. Le confinement à long terme peut être nécessaire lorsqu'une analyse approfondie est requise, ce qui peut prendre du temps. Cela peut vouloir dire faire une sauvegarde d'image système de l'appareil et analyser le disque dur en profondeur. Ces recherches sont susceptibles de révéler d'autres signes d'infection, ce qui signifie répéter l'étape d'identification.

Phase n°4 - Éradication

Après avoir contenu l'incident, la phase d'éradication de la menace peut commencer. Celle-ci dépend de la cause d'infection de l'appareil. Souvent, il faut appliquer des correctifs sur les appareils, désarmer un logiciel malveillant, désactiver les comptes compromis, etc.

Phase n°5 - Retour à la normale

Le but de cette phase est de ramener tous les services de l'entreprise à un fonctionnement normal. Si des sauvegardes propres sont disponibles, elles peuvent être utilisées pour restaurer le service. Autrement, tout appareil compromis devra être réinitialisé pour assurer une restauration propre. Il faudra peut-être mettre en place une surveillance supplémentaire des appareils affectés.

Phase n°6 - Enseignements

Une fois que la menace est définitivement écartée, la phase suivante consiste à répondre à la question : comment fait-on pour éviter que cela ne se reproduise ? Une réunion qu'on appelle analyse post-incident (*Post Incident Review*) doit avoir lieu avec les représentants de toutes les équipes concernées. C'est le moment d'aborder ce qui s'est bien passé pendant la réponse à l'incident et ce qui peut être amélioré. Le plan de réponse aux incidents peut alors être modifié suite aux conclusions de cette réunion. Les procédures et les exercices de simulation sont également modifiés pour refléter tout changement validé.

Source : d'après Varonis (éditeur de solutions de sécurité)

Document C2 : Rançongiciel Ryuk

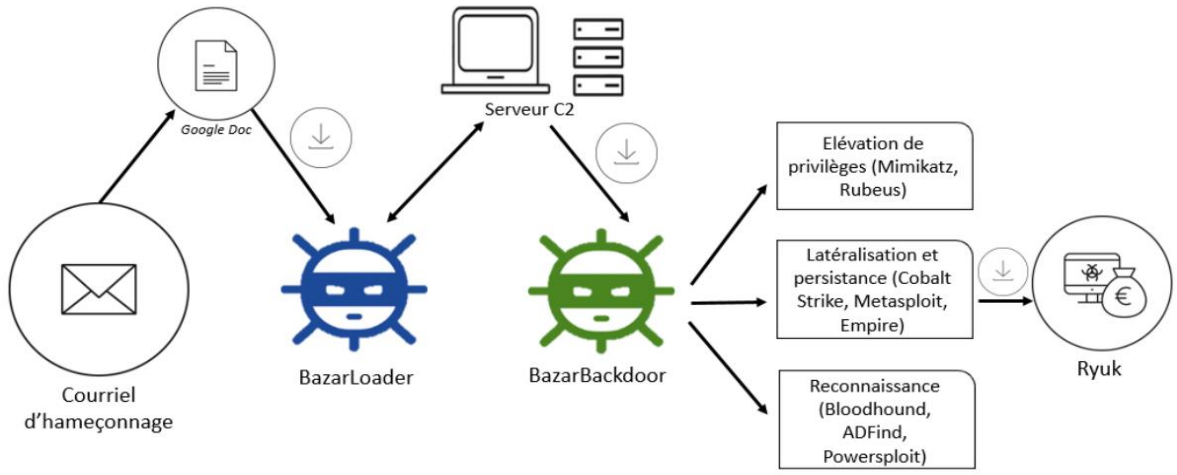
Ryuk est un rançongiciel attribué au groupe de pirates *Wizard Spider* qui a compromis, depuis août 2018, de nombreuses entités telles que des gouvernements, des universités, des établissements de santé et diverses entreprises.

Lorsque le rançongiciel Ryuk infecte un système, il tente d'arrêter 180 services et 40 processus connus (notamment ceux liés aux logiciels anti-virus et aux sauvegardes).

La persistance de l'échantillon Ryuk présent sur la machine est réalisée en faisant pointer la clé de registre «HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\svchost» vers son chemin disque. Il utilise également une tâche planifiée pour se lancer automatiquement.

Ryuk chiffre tous les fichiers en AES256 à l'aide d'une clé (chiffrement symétrique). Puis la clé AES est à son tour chiffrée au moyen d'une clé publique RSA contenue dans le programme Ryuk. Les navigateurs internet ainsi que les composants de base du système d'exploitation sont laissés intacts pour permettre aux victimes de lire la demande de rançon, d'acheter des cryptomonnaies et de payer la rançon. Ryuk ajoute l'extension « .RYK » aux fichiers chiffrés et dépose la note de rançon dans un fichier nommé « RyukReadMe.txt » dans chaque dossier chiffré.

Au niveau réseau, Ryuk recherche la présence de partages réseaux pour étendre son objectif. Pour ce faire, certaines plages d'adresses privées sont scannées : 10.0.0.0/8, de 172.16.0.0/16 à 172.31.0.0/16 et 192.168.0.0/16. Il génère toutes les adresses IP possibles des réseaux locaux et envoie un ping ICMP sur chacune. Ensuite il énumère tous les partages ouverts sur les IP trouvées, monte chacun et tente de chiffrer le contenu. La propagation se fait en utilisant un compte privilégié du domaine.



Déroulé simplifié de la chaîne d'infection Bazar-Ryuk :

Ryuk repose sur un courriel contenant un lien malveillant, qui télécharge le maliciel BazarLoader. Ce dernier contacte ensuite son serveur de commande et contrôle (C2) pour télécharger un autre programme qui créé une porte dérobée (*backdoor*). Ensuite, une élévation de privilèges est réalisée afin d'obtenir un droit administrateur et lancer le programme Ryuk qui chiffrera tous les fichiers.

Ce virus est caractérisé par plusieurs éléments :

- un vecteur d'infection qui repose sur des courriels d'hameçonnage contenant des liens ;
- une rapidité d'exécution, le délai entre l'infection initiale et le chiffrement s'étalant entre 3 heures et 5 jours ;
- l'absence d'exfiltration d'informations depuis le SI de ses victimes.

D'après FireEye (entreprise de sécurité informatique américaine), un cinquième des intrusions liées à des rançongiciels en 2021 sont dues à Ryuk. Et 83 % des infections dues à Ryuk sont le fait du groupe UNC1878 (groupe de cybercriminels).

Indicateurs de compromission (marqueurs du programme Ryuk) :

- Nom : xxx.exe, taille : 552960
- MD5 : 544900a527328f2e4fe7598985bc688f

Source : D'après CERT-FR - Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (cert.ssi.gouv.fr)

Document C3 : Indicateurs de compromission du logiciel malveillant BazarLoader

BAZARLOADER TRAFFIC :

- 172.67.205.11 port 80 - meronekis.space - GET /222g100/index.php
- 172.67.205.11 port 80 - meronekis.space - GET /222g100/main.php
- 34.217.209.239 port 443 - 34.217.209.239 - GET /www/html/var/generic/doc
- 103.208.86.5 port 443 - 103.208.86.5 - GET /www/html/var/generic/doc
- 103.208.86.5 port 443 - 103.208.86.5 - POST /www/html/var/generic/doc

Source : Github de Brad Duncan (analyste des menaces cyber pour l'US Air Force et Palo Alto Networks)

Document C4 : Indicateurs de compromission du rançongiciel Ryuk par le groupe UNC1878

# FQDN des serveurs de commande et contrôle (C2)	**#Répertoires courants**	**# Nom de fichiers courants**
updatemanagir.us cmdupdatewin.com scrservallinst.info winsystemupdate.com jomamba.best updatewinlsass.com winsysteminfo.com …	C:\PerfLogs\ C:\share$\ …	comps[1-9999].txt COPY.bat P64.exe vVv.exe xxx.exe 1234.zip …

Source 1 : Github de Aaron Stephens (analyste des menaces cyber pour Mandiant Security)

Source 2 : CISA (cybersecurity and infrastructure security agency), organisation gouvernementale des USA

Document C5 : Extrait des journaux d'évènements du poste de travail concerné par l'alerte

Nom du journal : Security
Source : Microsoft-Windows-Security-Auditing
Date : 04/05/2022 13:47:53
ID de l'évènement : 4663
Catégorie de la tâche : File System
Niveau : Information
Mots clés : Succès de l'audit
Utilisateur : N/A
Ordinateur : MAIRIE-SERV-EC-PC06
Description :
Une tentative d'accès à un objet a été effectuée.

Sujet :
- ID de sécurité : VILLE-PARC\lvadot
- Nom du compte : lvadot
- Domaine du compte : VILLE-PARC
- ID d'ouverture de session : 0xAAF61C4

Objet :
- Serveur de l'objet : Security
- Type d'objet : File
- Nom de l'objet : C:\PerfLogs\P64.exe
- ID du handle : 0x31a0
- Attributs de ressource : S:AI

Informations sur le processus :
- ID du processus : 0x2f34
- Nom du processus : C:\Windows\explorer.exe

Informations sur la demande d'accès :
- Accès : Lecture données
- Masque d'accès : 0x1

Nom du journal : Security
Source : Microsoft-Windows-Security-Auditing
Date : 04/05/2022 13:48:27
ID de l'évènement : 4663
Catégorie de la tâche : File System
Niveau : Information
Mots clés : Succès de l'audit
Utilisateur : N/A
Ordinateur : MAIRIE-SERV-EC-PC06
Description :
Une tentative d'accès à un objet a été effectuée.

Sujet :
- ID de sécurité : VILLE-PARC\lvadot
- Nom du compte : lvadot
- Domaine du compte : VILLE-PARC
- ID d'ouverture de session : 0xAF434E4

Objet :
- Serveur de l'objet : Security
- Type d'objet : File
- Nom de l'objet : C:\PerfLogs\comps1524.txt
- ID du handle : 0x2cf0
- Attributs de ressource : S:AI

Informations sur le processus :
- ID du processus : 0xd64
- Nom du processus : C:\Windows\explorer.exe

Informations sur la demande d'accès :
- Accès : ReadAttributes
- Masque d'accès : 0x80