Scholanova

Apprendre ensemble

BTS Services informatiques aux organisations :

Devoir sur Table

Cas Saint-Jacques

2023-2024

Table des matières

1 Cas Saint-Jacques

1.1 Présentation du contexte

Afin d'assurer ses missions, la mairie de Saint-Jacques-sur-Argens est organisée en services communaux :

- les services principaux réalisant les missions essentielles de toute mairie (état civil, élections, cadastre, urbanisme, marchés publics) ;
- les services aux administrés destinés à satisfaire les demandes des habitants, des associations et des entreprises de la commune (affaires scolaires, culture, sport, médiathèque, police municipale, etc.) ;
- les services de support qui facilitent le travail des deux catégories de services précédentes (accueil, secrétariat, communication, ressources humaines, affaires juridiques, centre technique, archives, etc. et bien sûr le service informatique).

Les missions du maire sont de deux ordres :

- Il représente la commune auprès des tiers. Il est notamment chargé :
  - d'exécuter les délibérations du conseil municipal,
  - d'assurer sa fonction d'administration municipale,
  - d'exercer les pouvoirs de police dans sa commune.
- Il est aussi agent de l'État et doit garantir ses missions liées :
  - aux actes d'état civil (naissances, unions, décès, etc.),
  - aux élections (tenue des listes électorales, organisation des élections, etc.),
  - au recensement citoyen,
  - aux activités judiciaires (sous l'autorité du procureur de la République),
  - à la sécurité civile.

Concernant ce dernier point, la commune doit respecter des contraintes spécifiques en matière de sécurité. En effet, la commune de Saint-Jacques-sur-Argens accueille sur son territoire des sites sensibles classés Seveso 2 :

- un dépôt de carburant et un terminal pétrolier présentant des risques de rejets de boues chargées d'hydrocarbures, d'explosion et d'émanation de gaz toxiques ;
- une entreprise industrielle présentant des risques de rejets d'hydrocarbures, de fluor et de boue hydroxyde.

De plus, comme de nombreuses autres communes du département, Saint-Jacques-sur-Argens est bordé par un fleuve côtier qui déborde régulièrement lors d'épisodes méditerranéens et a donc subi des inondations particulièrement importantes par le passé.

Dans ce contexte, le maire doit s'assurer de la disponibilité des services municipaux jugés comme critiques lors d'une éventuelle crise.

Le service informatique agit non seulement selon le cadre réglementaire numérique des mairies, mais doit aussi tenir compte des spécificités sécuritaires énoncées précédemment. Il doit notamment garantir la continuité des services critiques lors d'une éventuelle attaque informatique ou d'un incident majeur.

Vous venez d'être recruté(e) au sein du service informatique en tant que responsable-adjoint(e) sécurité des systèmes d'information. M. Hopada, le directeur du service informatique, vous a confié l'étude et la réalisation de certaines missions liées à la sécurité du réseau de la mairie.

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

1.2 Dossier A Audit général de la sécurité du réseau

1.2.1 Mission A1 Vérification des accès au réseau

Cette première mission consiste à vérifier la sécurité des différents points d'accès du réseau de la mairie. La mairie dispose d'un certain nombre de services répondant aux besoins de la population (les "administrés"), des entreprises et des associations de la commune.

Il convient de distinguer deux usages des applications :

- d'une part, les applications métier permettant au personnel de la mairie de réaliser leurs différentes missions. Ces applications ne sont accessibles qu'aux personnes habilitées, jamais au public ;
- d'autre part, les applications destinées au public. Elles permettent la consultation, la formulation de demande ou le paiement de certains actes. Elles sont accessibles via le portail internet de la mairie de Saint-Jacques-sur-Argens ou via les postes mis à disposition du public au sein des locaux communaux.

M. Hopada s'interroge sur la sécurité des accès aux ressources informatiques par le public.

Question A1.1
Identifier les différentes façons (emplacements, équipements) par lesquelles le public peut accéder aux applications qui lui sont dédiées.

Réponse :
Les emplacements et équipements par lesquels le public peut accéder aux applications dédiées incluent le portail internet de la mairie et les postes informatiques publics situés dans les locaux communaux. Les points d'accès publics dans un environnement municipal peuvent inclure des bornes interactives, des postes informatiques en libre accès dans des bibliothèques ou des espaces publics, et l'accès Wi-Fi public. La sécurisation de ces points nécessite une attention particulière pour éviter les accès non autorisés au réseau interne de la mairie.
Liste les emplacements et équipements : voir le Document 4 : Matériel utilisateur de chaque service.

Les personnels de la mairie sont considérés comme des utilisateurs loyaux et fiables, ils n'accèdent qu'aux applications et ressources qui leur sont nécessaires pour effectuer leur travail. M. Hopada s'interroge sur la possibilité d'accès malveillant aux données de la mairie par des personnes externes à l'organisation.

Question A1.2
Indiquer au moins trois cas de figure permettant l'accès d'une personne malveillante aux postes de travail ou aux comptes personnels des personnels de la mairie.

Réponse :
Trois cas de figure permettant l'accès malveillant aux données comprennent : l'usage de supports amovibles infectés (clés USB), les attaques de phishing ciblant les employés de la mairie, qui vise à tromper les employés pour qu'ils divulguent des informations sensibles et l'exploitation de vulnérabilités dans les applications publiques ou les systèmes d'exploitation des postes de travail, où des individus ayant un accès légitime abusent de leurs privilèges. On peut rajouter ransomware, MAC spoofing.

L'un des membres du personnel de la médiathèque a récemment ouvert un ticket d'incident contenant les informations suivantes :

- un poste de la médiathèque (destiné au public) semble au premier abord fonctionnel, mais ne permet plus d'accéder à l'application de recherche documentaire ;

- des feuilles portant le message " Hacké par K " ont été trouvées dans les imprimantes de la médiathèque.

Une lecture rapide des journaux d'évènements indiquait que le poste incriminé était à l'origine des impressions. Les réseaux sont actuellement cloisonnés via des réseaux locaux virtuels (VLAN) basés sur les adresses MAC : un " VLAN " pour les services de la mairie et un " VLAN " pour les accès du public.

Question A1.3
Expliquer pourquoi cette stratégie de réseaux locaux virtuels (VLAN) par adresse MAC est insuffisante pour garantir la sécurité du réseau.

Réponse :
La stratégie de VLAN basée sur les adresses MAC est insuffisante car elle peut être contournée par le spoofing d'adresse MAC, permettant ainsi un accès non autorisé à des ressources sensibles. L'utilisation des VLANs est une pratique courante pour segmenter le réseau et limiter l'accès en fonction des besoins de l'utilisateur. Cependant, se baser uniquement sur les adresses MAC pour l'attribution des VLANs peut être risqué car les adresses MAC peuvent être usurpées. L'implémentation d'une authentification supplémentaire, comme 802.1X, peut renforcer la sécurité.

Le technicien s'est rendu compte que l'adresse MAC de la carte réseau du poste concerné a été modifiée, afin que ce dernier appartienne au " VLAN " de la mairie, permettant ainsi l'impression.

Question A1.4
Proposer une nouvelle stratégie permettant de garantir le cloisonnement des ordinateurs de la médiathèque au sein du réseau local virtuel (VLAN) approprié, sans ajouter de matériel d'interconnexion ou de service supplémentaire.

Réponse :
Une stratégie améliorée sans ajout de matériel pourrait inclure l'utilisation de l'authentification 802.1X pour renforcer le contrôle d'accès au réseau, en s'assurant que seuls les appareils authentifiés puissent accéder au VLAN approprié. Authentification : Le 802.1X requiert qu'un dispositif (appelé supplicant) s'authentifie auprès d'un serveur d'authentification (généralement un serveur RADIUS) avant d'accéder au réseau. Cette authentification utilise des identifiants beaucoup plus sécurisés que simplement l'adresse MAC d'un appareil, tels que des certificats numériques, des noms d'utilisateur et des mots de passe, ou des clés pré-partagées. Améliorer la sécurité du réseau sans investir dans du matériel supplémentaire peut impliquer l'utilisation de solutions logicielles ou de configurations réseau existantes plus efficacement. Par exemple, le renforcement des politiques de mot de passe, l'activation de l'authentification à deux facteurs là où c'est possible, et l'utilisation de listes de contrôle d'accès (ACLs) pour gérer finement l'accès au réseau. Aussi, autre solution : Tables ARP statiques. Il est possible de mapper de manière statique toutes les adresses MAC dun réseau à leur adresse IP correcte. Cette méthode est très efficace dans la prévention de ce type dattaque, mais elle ajoute une charge importante de travail aux admin.

1.2.2 Mission A2 Vérification de l'infrastructure prévue en cas de crise

Cette seconde mission vise à vérifier la validité de l'infrastructure et de l'organisation prévue en cas de défaillance majeure. Le réseau de la mairie ayant déjà été spécifiquement la cible d'attaques numériques, M. Hopada souhaite s'assurer de la résilience (capacité de résistance) de son système d'information.

Pour atteindre cet objectif, une infrastructure particulière a été mise en uvre dans un local de la

médiathèque afin de permettre la continuité des activités en cas de défaillance majeure. L'utilité principale de ce " local de secours " est de garantir l'accès aux applications et aux données professionnelles définies comme critiques, c'est-à-dire nécessaires aux activités que doit assurer toute mairie en période de crise.

Ce local est bien entendu inaccessible au public et héberge deux serveurs de virtualisation (SRV-HYPERV3 et SRV-HYPERV4) ainsi qu'un réseau de stockage SAN (SAN-2). En fonctionnement normal, les ressources du site de secours ne sont pas exploitées par les utilisateurs.

Les activités concernées sont la délivrance des états civils, l'établissement de mandats de paiement, la consultation du cadastre et les opérations de paie, répondant à une obligation légale du code des collectivités. La commune doit en toute circonstance être capable d'acheter du matériel en urgence, d'accéder aux plans cadastraux, de dresser des listes d'alerte aux citoyens, d'établir des actes de décès, etc.

Le plan de continuité d'activité reposant beaucoup sur la réplication, M. Hopada se demande si cette stratégie est suffisante.

Question A2.1
Indiquer si la simple réplication des données garantit l'impossibilité de perte de données. Justifier la réponse.

Réponse :
La simple réplication des données ne garantit pas contre la perte de données car elle ne protège pas contre les erreurs de synchronisation, la corruption des données ou les suppressions accidentelles. La réplication assure la disponibilité des données en temps réel ou à des intervalles réguliers, mais elle ne protège pas contre les suppressions accidentelles ou malveillantes ni contre les corruptions de données. Pour cela, il est nécessaire d'implémenter des stratégies de sauvegarde complètes, incluant des sauvegardes incrémentielles et des points de restauration, ainsi que des tests réguliers de restauration pour garantir l'intégrité des données sauvegardées.

Le plan de gestion de crise prévoit qu'en cas d'indisponibilité des postes utilisateurs du site principal de la mairie, les postes de la médiathèque normalement destinés au public soient utilisés pour accéder aux applications du site de secours.

M. Hopada vous demande de comparer cette solution avec l'utilisation de postes dédiés à cette tâche, préparés et stockés dans la salle technique du site de secours.

Question A2.2
Comparer les deux solutions dans un tableau mettant en évidence les trois critères : (1) disponibilité des équipements et rapidité de mise en uvre, (2) sécurité, (3) coût.

Réponse :
La comparaison entre l'utilisation des postes de la médiathèque et des postes dédiés dans la salle technique pour accéder aux applications en cas de crise devrait évaluer la disponibilité, la sécurité, et le coût. Les postes dédiés sont généralement plus sécurisés et rapidement opérationnels, mais impliquent un coût initial plus élevé. La mise en place de postes dédiés dans la salle technique pour accéder aux applications en cas de crise présente plusieurs avantages par rapport à l'utilisation des postes de la médiathèque, notamment en termes de sécurité et de rapidité de mise en uvre. Les postes dédiés peuvent être configurés spécifiquement pour les besoins de la continuité d'activité, avec des droits d'accès et des logiciels appropriés, et ils peuvent être isolés du réseau public pour réduire les risques de sécurité. Cependant, cette solution peut être plus coûteuse en raison du besoin d'équipements supplémentaires et de leur maintenance.

M. Hopada souhaite améliorer son plan de réplication, il vous demande d'en étudier la cohérence. Une attention particulière doit être portée aux applications et données incluses dans le plan, ainsi

qu'aux fréquences de synchronisation

Question A2.3
Identifier au moins deux défauts du plan de réplication actuel, en précisant les problèmes potentiels que ces derniers peuvent engendrer.

Réponse :
Deux défauts du plan de réplication pourraient inclure une fréquence de réplication insuffisante pour certaines données critiques et l'absence de réplication pour certaines ressources importantes, comme les vidéos de surveillance de la police municipale. Un plan de réplication peut présenter des défauts tels qu'une fréquence de réplication inadéquate pour certaines données critiques, ne permettant pas une restauration à un état récent en cas de sinistre, ou l'exclusion de certaines données ou systèmes essentiels de la stratégie de réplication et l'absence de réplication pour certaines ressources importantes, comme les vidéos de surveillance. Il est crucial d'évaluer régulièrement le plan de réplication pour s'assurer qu'il couvre toutes les données essentielles et qu'il est aligné sur les objectifs de temps de récupération après sinistre (RTO) et de point d'objectif de récupération (RPO).

Certaines applications de la mairie ont déjà fait l'objet d'une attaque. Des données ont alors été modifiées. Par chance, cet acte malveillant a été découvert trois jours après et une sauvegarde a pu être utilisée pour restaurer les données. M. Hopada s'interroge sur la durée d'historisation des sauvegardes.

Question A2.4
Indiquer si la fréquence d'historisation est adaptée aux usages de la mairie. Le cas échéant, en proposer une nouvelle. Justifier la réponse.

Réponse :
"les fichiers vidéo de la police municipale (NAS-VIDEO) ne sont pas répliqués ; ces fichiers sont importants en cas denquête diligentée par les autorités." "Une seule sauvegarde complète (la dernière) reste disponible sur le serveur SAN-2." La fréquence dhistorisation des sauvegardes doit être adaptée à la criticité des données et aux exigences légales, en envisageant une stratégie de sauvegarde plus fréquente et diversifiée. La stratégie actuelle de sauvegarde peut ne pas être suffisamment robuste pour répondre aux besoins de la mairie, surtout si les données changent fréquemment ou si elles sont de nature critique. Une approche plus granulaire, avec des sauvegardes complètes hebdomadaires et des sauvegardes incrémentielles quotidiennes, pourrait offrir un meilleur équilibre entre la protection des données et l'utilisation des ressources. De plus, la mise en place d'une politique de rétention des sauvegardes permettrait de s'assurer que les données peuvent être récupérées sur une période conforme aux obligations légales et aux besoins opérationnels.

M. Hopada est aussi soucieux des possibles implications juridiques de ce vol de données.

Question A2.5
Identifier les obligations légales qui s'imposent à la mairie, en matière d'archivage et de protection des données des administrés.

Réponse :
La gestion des archives et la protection des données des administrés par les mairies en France sont régies par plusieurs obligations légales, découlant principalement du Code du patrimoine pour les archives et du Règlement Général sur la Protection des Données (RGPD) ainsi que de la législation nationale pour la protection des données personnelles. Voici un résumé des principales obligations :
1. Archivage
Code du patrimoine (notamment les articles L211-1 et suivants) : Il définit les règles relatives à l'archivage public, incluant les documents produits et reçus par les mairies dans le cadre de leurs activités. Ces règles concernent la conservation, le tri, l'élimination et la communication des archives.

- Conservation : Les archives doivent être conservées dans des conditions qui garantissent leur intégrité, leur sécurité et leur accessibilité, selon leur nature et leur intérêt historique, légal ou administratif.
- Tri et élimination : Un tri doit être effectué pour déterminer les documents à conserver de manière permanente pour leur intérêt historique ou à éliminer selon des règles et des procédures précises.
- Communication : Les archives publiques sont, en principe, communicables au public, sous certaines conditions et délais, à l'exception des documents touchant à la vie privée ou à la sécurité nationale, par exemple.

2. **Protection des données personnelles**
Règlement Général sur la Protection des Données (RGPD) et loi informatique et libertés : Ces textes réglementent le traitement des données personnelles sur le territoire de l'Union européenne et en France.

- Principes de base : Les données personnelles doivent être traitées de manière licite, loyale et transparente. Elles doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités.
- Droits des personnes : Les administrés disposent de droits importants, tels que le droit d'accès, de rectification, d'effacement et de portabilité de leurs données, ainsi que le droit de s'opposer à leur traitement.
- Sécurité des données : La mairie doit mettre en uvre des mesures techniques et organisationnelles appropriées pour garantir un niveau de sécurité adapté au risque, incluant la protection contre l'accès non autorisé, la perte ou la destruction des données.
- Notification des violations de données : En cas de violation de données personnelles, la mairie doit notifier la CNIL (Commission Nationale de l'Informatique et des Libertés) et, dans certains cas, les personnes concernées.

3. **Responsabilités et mise en conformité**

- Désignation d'un délégué à la protection des données (DPO) : Les mairies, en tant que responsables de traitement, sont souvent tenues de désigner un DPO chargé de veiller au respect du RGPD et de la loi informatique et libertés.
- Tenue d'un registre des activités de traitement : Les mairies doivent documenter les traitements de données personnelles qu'elles effectuent, y compris la finalité du traitement, les catégories de données traitées et les destinataires des données.
- Évaluation d'impact relative à la protection des données (EIPD)** : Pour les traitements susceptibles de présenter un risque élevé pour les droits et libertés des personnes, les mairies doivent réaliser une EIPD.

Ces obligations visent à assurer la protection de la vie privée des administrés et la préservation du patrimoine documentaire de la collectivité. Pour une application correcte, il est conseillé aux mairies de se rapprocher de la CNIL et des services des archives départementales compétents.

Dans le plan actuel, le lieu de sauvegarde est unique. Dans le cas d'une éventuelle attaque

simultanée sur le site principal et sur le site de secours, le système d'information serait donc exposé à un risque de perte de données.

Question A2.6
Proposer une solution de stockage complémentaire qui permettrait d'améliorer la conservation des données en cas de défaillance majeure.

Réponse :
Pour améliorer la résilience du système d'information et la conservation des données, une approche multi-couche peut être envisagée, combinant des solutions de stockage locales et dans le cloud. Le cloud offre une flexibilité et une échelle qui peuvent compléter les infrastructures locales, permettant une réplication géographique des données pour protéger contre les sinistres régionaux. De plus, l'utilisation de technologies de stockage immuable ou de services d'archivage spécialisés peut aider à protéger contre les modifications ou suppressions malveillantes.

Durant le mois d'avril de cette année, un individu a tenté de saboter une borne technique située sur la voie publique. Cette borne contient, entre autres, les câbles de connexion entre le site principal et le site de secours. Cet élément a été physiquement sécurisé depuis, mais l'incident a permis de mettre en évidence deux défauts de l'infrastructure :

- l'unicité du lien entre les sites et sa criticité,
- l'impossibilité de disposer d'une connexion internet sur le site de secours en cas de défaillance de ce lien.

Question A2.7
Préconiser une solution permettant de résoudre les deux défauts constatés précédemment (lien inter-site unique et absence de connexion internet). Justifier la réponse.

Réponse :
Pour augmenter la résilience face à une défaillance unique du lien entre les sites ou à l'absence de connexion internet au site de secours, il est recommandé de mettre en place une architecture de réseau redondante. Cela peut inclure l'installation de liaisons internet multiples auprès de fournisseurs différents et l'usage de technologies diverses (fibre optique, SDSL, liaison radio) pour assurer une continuité de service même en cas de panne d'une des connexions. L'utilisation d'un système de basculement automatique (failover) et de répartition de charge (load balancing) entre les connexions peut garantir une haute disponibilité des services en ligne et une reprise rapide après incident. 2ème connexion à un FAI.

1.2.3 Mission A3 Amélioration de la disponibilité des liaisons externes

Cette mission se concentre sur un autre point sensible du réseau. Tout le trafic des connexions FAI (fournisseurs d'accès à internet) emprunte le routeur pare-feu FW-SEC. Une défaillance matérielle ou une attaque ciblée sur celui-ci rendrait indisponible l'ensemble des connectivités externes. Un projet de mise en uvre d'une haute disponibilité des pare-feux est à l'étude. M. Alatur, le collaborateur chargé de sa mise en uvre, est peu au fait des questions de sécurité et vous demande de l'aider dans sa tâche.

M. Alatur s'interroge sur le fait que les pare-feux soient une contre-mesure pleinement efficace contre le déni de service distribué (DDoS), dont il maîtrise peu les problématiques.

Question A3.1

- Rappeler l'objectif et le principe de fonctionnement d'une attaque par déni de service distribué.
- Argumenter sur la capacité des pare-feux à résister à une attaque de type DDoS.

Réponse :

- a) L'objectif d'une attaque DDoS est de surcharger les ressources d'un système (comme un serveur web) pour en empêcher l'accès légitime. Elle est réalisée en inondant la cible de trafic internet excessif depuis de nombreux systèmes compromis sur le réseau.
- b) Bien que les pare-feux puissent filtrer certains types de trafic malveillant et limiter l'exposition à des attaques DDoS, ils ne sont pas infaillibles. Les pare-feux traditionnels peuvent être submergés par le volume de trafic généré par une attaque DDoS volumétrique. Des solutions spécifiques de mitigation des DDoS, qui peuvent analyser et filtrer le trafic à une échelle beaucoup plus grande, sont souvent nécessaires pour protéger efficacement contre ces attaques.

Quoi qu'il en soit, le projet de haute disponibilité des pare-feux sera mis en uvre, car la tolérance de panne s'avère obligatoire. M. Alatur souhaiterait cependant savoir comment réagirait cette partie de l'infrastructure en cas d'attaque, il vous demande donc d'effectuer un test réel en réalisant une simulation d'attaque complète et concrète.

Question A3.2
Proposer une procédure de test permettant de vérifier la résilience de la grappe de haute disponibilité des pare-feux face à une attaque de type DDoS.

Réponse :
Bien que les pare-feux soient conçus pour filtrer le trafic non autorisé, leur efficacité contre les attaques DDoS peut être limitée, surtout si l'attaque est volumétrique et dépasse la capacité de bande passante du système. Pour tester la résilience des pare-feux en haute disponibilité, une simulation d'attaque DDoS contrôlée peut être réalisée. Cette procédure implique :

- La préparation d'un environnement de test qui imite l'infrastructure de production sans impacter les opérations réelles.
- L'utilisation d'outils de génération de trafic pour simuler une attaque DDoS en termes de volume et de type de trafic (par exemple, UDP, SYN flood, etc.).
- La surveillance des pare-feux pour évaluer leur capacité à gérer l'augmentation du trafic, à maintenir la disponibilité des services et à basculer entre les unités en mode actif/passif si nécessaire.
- L'analyse des résultats pour identifier les éventuelles vulnérabilités ou points de défaillance et ajuster la configuration ou la capacité des pare-feux en conséquence.