Retranscription à l'identique de la copie remise par la/le candidat·e

MEILLEURE COPIE

Examen professionnel 1er alinéa par promotion interne
INGÉNIEUR·E TERRITORIAL·E
Session 2022
Spécialité *Informatique et systèmes d'information*
Option *Réseaux et télécommunication*
ÉPREUVE DE PROJET OU ÉTUDE

QUESTION 2 :

a) : La commune d'Ingéville disposant d'une station d'épuration, suivant l'article L.2224-7 du Code Général des Collectivités Territoriales (CGCT), a une compétence obligatoire en matière de distribution d'eau potable, et l'article L.2224-8 du CGCT apporte une compétence obligatoire en matière d'assainissement.

Une cyberattaque pourrait entraîner l'arrêt du traitement des eaux usées, ainsi que l'arrêt de la distribution d'eau potable pour l'ensemble des habitants d'Ingéville.

De plus, une cyber attaque pourrait entraîner le vol des données d'état-civil, des données électorales, des données personnelles des agents, des données des différents services (urbanisme, régie scolaire, centre d'action sociale (CCAS)).

b) : Les conséquences pour de tels piratages sont importantes. Tout d'abord une impossibilité de disposer un réseau d'eau potable fonctionnel. En même temps, le système d'assainissement étant à l'arrêt, les évacuations et les traitements des eaux usées ne fonctionneraient plus.

Ensuite, concernant les autres services, des données personnelles peuvent être dérobées, entraînant des risques d'usurpation d'identité.

c) : Afin de réduire au maximum les risques évoqués précédemment, il est nécessaire de s'assurer que le système informatique dispose de :

- toutes les mises à jour poste de travail, serveurs, éléments actifs
- des mots de passe solides, c'est à dire respectant des conditions tel que majuscule, minuscule, chiffre, lettre, caractère alpha numérique, ainsi qu'une double authentification
- le système informatique doit disposer de sauvegarde hors ligne, permettant une restauration assurée
- la commune doit aussi sensibiliser les agents au risque de cyber sécurité.

QUESTION 3 :

Les réseaux informatiques de la commune apparaisse être tous « joignable », c'est à dire qu'il n'existe pas de segmentation de réseau.

Je préconise une segmentation par VLAN, étant supporté par les équipements réseau.
À la une des schémas, je recommande 12 VLANS :

- VLAN 100 : téléphonie IP
- VLAN 101 : réseau mairie annexe
- VLAN 102 : réseau mairie
- VLAN 103 : réseau CCAS
- VLAN 104 : réseau WIFI
- VLAN 105 : réseau des serveurs réseaux tiers
- VLAN 106 : salle machine
- VLAN 107 : serveurs de messagerie + FTP + relay
- VLAN 108 : réseau des caméras
- VLAN 109 : réseau des équipements de voirie
- VLAN 110 : station d'épuration
- VLAN 111 : écoles primaires.

Afin de garantir une sécurité accrue, et minimiser les accès extérieurs, je mets en place des liaisons pour l'ensemble des sites en fibre optique dédiée. Cela permet de centraliser toutes les connexions vers internet par un firewall, et apporter une sécurisation sur les sites n'en disposant pas.

Un firewall puissant ainsi qu'une connexion haut débit fibre permettront de contrôler simplement tous les échanges d'information du réseau global de la commune.

Le nouveau schéma d'architecture général est en annexe 1.

QUESTION 4 :

a) :

Les actions à mener en priorité sont :

- isoler les sauvegardes et vérifier leur bon état
- prévenir la hiérarchie et l'ensemble du personnel
- déposer plainte dans un commissariat de police
- déclarer l'incident à la CNIL et à l'ANSSI
- déployer le plan de reprise d'activité
- faire un inventaire global des postes et serveurs touchés
- restaurer les serveurs et les postes infectés.

b) :

Il est primordiale d'organiser un comité de pilotage (COPIL), comprenant des élus, des chefs de services directement impliqués et la direction des systèmes d'information.

Leur mission consistera alors à gérer cette crise en prenant très rapidement des décisions.

Le SI, en diagnostiquant le réseau remontera immédiatement les informations au COPIL. En fonction des résultats des actions seront à mener immédiatement.

Le plan du schéma directeur des actions à mener est mis en annexe 2.

QUESTION 1 :

Commune d'Ingéville le 16/06/2022
Direction des systèmes d'information

À l'attention du Directeur
des systèmes d'information

OBJET : constat et enjeux des cyberattaques pour Ingéville

La commune d'Ingéville dispose de 1000 terminaux, et le système d'information s'est construit au fur et à mesure des créations de poste et des besoins.

À la vue exponentielle des attaques en France et à l'étranger il est important de remettre la question de la sécurité informatique des réseaux à la une des enjeux suite à une cyber-attaque.

Dans une première partie, nous définirons et nous établirons un constat des cyber attaques, pour ensuite, en deuxième partie aborder les enjeux et les solutions.

Ⅰ) Les cyber attaques :

a) : Les cyber attaque peuvent survenir à tout moment. Une attaque depuis un poste informatique externe, une pièce jointe d'un virus, une clé USB laissée volontairement sur un bureau. Il s'agit avant tout d'un logiciel qui s'installe sur un poste informatique (PC ou serveur) et qui crypte l'entièreté des données.
Un message apparaît alors, et demande de payer une rançon contre la clé de décryptage.

Ce type de cyber attaque est d'autant plus violente qu'elle se déploit au travers des lecteurs réseaux des postes exposés, et agit comme une toile d'araignée.

B) : En France et dans le monde, on ne cesse de découvrir des sites touchés par des cyber attaques. De la petite collectivité, à la grande entreprise, en passant par des hôpitaux, des sites sensibles, personnes n'est à l'abris car le risque est dans la majorité des cas lié à l'utilisateur.

Les autorités (ANSSI, CNIL) incitent fortement à prendre toutes les mesures adaptées afin de limiter les cyber-attaques. Le risque zéro n'existant pas, il est important de tout mettre en œuvre pour limiter les dégâts en cas de problème.

Ⅱ) : Les enjeux pour Ingéville :

a) :

Une commune comme Ingéville qui dispose de plus de 1000 terminaux, des écoles, une mairie annexe, un CCAS, et un site très sensible comme celui de la station d'épuration, ne peut se permettre d'avoir un système informatique inadapté au cyber attaque.

Entre le vol de données du personnel (logiciel RH), du vol de données des entreprises (comptabilité, service achats), du vol de données des citoyens (état-civil, école), les enjeux

sont cruciaux et entraînerait des conséquences néfastes : très souvent par de l'usurpation d'identité.

Mais malgré tout le plus grave est la paralysie du système de distribution d'eau et de l'assainissement, qui amènerait 100 000 habitants privés d'eau potable.
L'impact serait d'une violence tel qu'un plan de crise devrait être immédiatement déployé afin de distribuer de l'eau potable à tous les habitants. L'image de la commune serait alors dégradé.

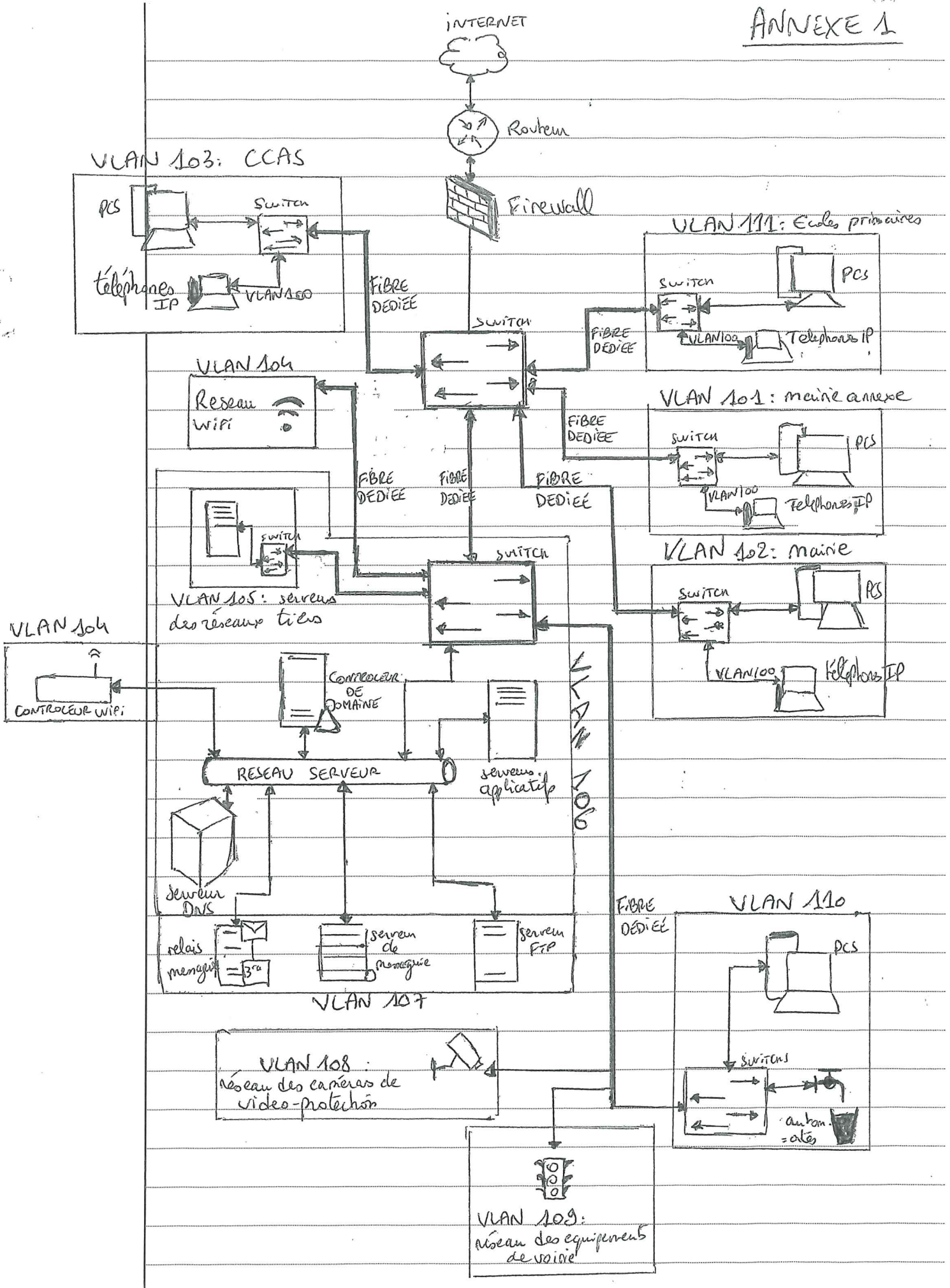
B) :

Afin de minimiser les risques, voici les grandes lignes des actions à mener, afin de réduire au maximum les risques et les enjeux pour Ingéville.

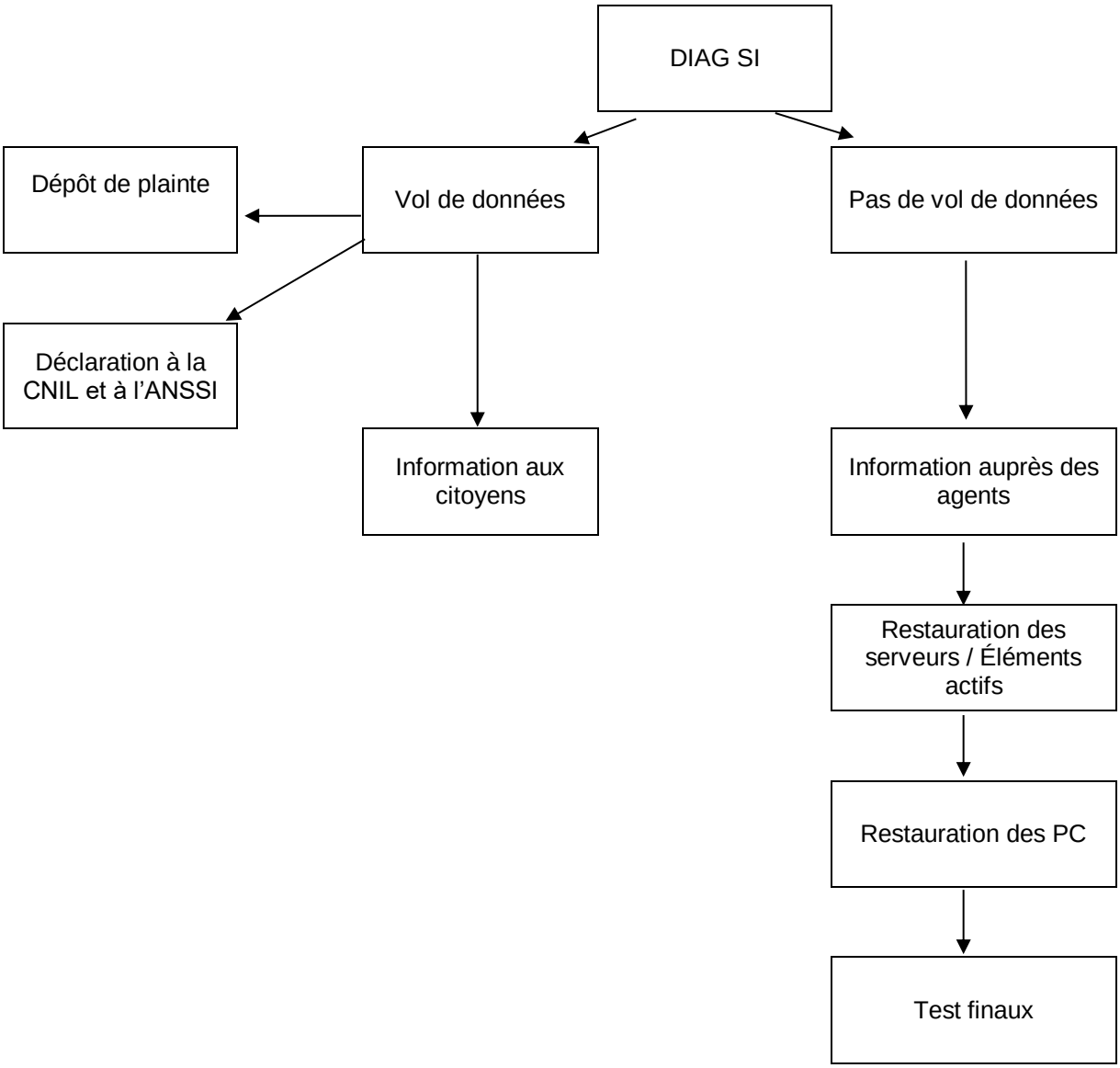
- formation des agents par de la sensibilisation
- sécuriser les réseaux en appliquant le principe de la segmentation, afin de limiter le déploiement d'une cyber attaque
- s'assurer d'une mise hors ligne des sauvegardes tout le temps où les sauvegardes ne fonctionnent pas
- établir un plan de reprise d'activité, afin de savoir exactement comme réagir et éviter la panique
- s'assurer du bon fonctionnement de la veille technologique
- s'assurer que toutes les applications et systèmes d'information soient à jour.

Les cyber attaques sont incontrôlables, elle fonctionne comme un virus et il faut vivre avec car il est impossible de l'éradiquer.
Il nous faut alors tout mettre en œuvre pour limiter au maximum le risque, et essayer de ramener à zéro les conséquences d'une telle attaque.

ANNEXE 1


INTERNET
Routeur
Firewall
VLAN 103: CCAS
PCS
SWITCH
Téléphones IP
VLAN100
FIBRE DEDIEE
SWITCH
VLAN 111: Ecoles primaires
SWITCH
PCS
VLAN100
Telephones IP
FIBRE DEDIEE
VLAN 104
Reseau WiFi
FIBRE DEDIEE
FIBRE DEDIEE
FIBRE DEDIEE
VLAN 101: mairie annexe
SWITCH
PCS
VLAN100
Telephones IP
SWITCH
VLAN 105: serveurs des réseaux tiers
SWITCH
VLAN 102: mairie
SWITCH
PCS
VLAN100
Téléphones IP
VLAN 104
CONTROLEUR WIFI
CONTROLEUR DE DOMAINE
VLAN 106
RESEAU SERVEUR
serveurs applicatifs
serveur DNS
relais messagerie
serveur de messagerie
serveur FTP
VLAN 107
FIBRE DEDIEE
VLAN 110
PCS
SWITCHS
VLAN 108: réseau des caméras de vidéo-protection
VLAN 109: réseau des equipements de voirie

ANNEXE 2


DIAG SI
Dépôt de plainte
Vol de données
Pas de vol de données
Déclaration à la CNIL et à l'ANSSI
Information aux citoyens
Information auprès des agents
Restauration des serveurs / Éléments actifs
Restauration des PC
Test finaux