EXAMEN PROFESSIONNEL D'INGÉNIEUR TERRITORIAL 2022

SPÉCIALITÉ « INFORMATIQUE ET SYSTÈMES D'INFORMATION »

OPTION « RÉSEAUX, TELECOM »

ÉPREUVE DE PROJET

NOTE OBTENUE : 15.88 / 20

Ingéville le 16 juin 2022
Direction des Systèmes d'Information

À l'attention de Monsieur le directeur des systèmes d'information

Objet : la menace informatique

La cybersécurité est devenue l'une des missions les plus importantes des directions des systèmes d'information (DSI) des entreprises et des collectivités. La menace, toujours grandissante (virus, ransomware, usurpation), doit être prise avec le grand sérieux au sein des administrations publiques. Un système vérolé représente un coût important aux collectivités et donc aux citoyens. La situation internationale actuelle fait de la France une cible privilégiée notamment des pays de l'Est. L'ANSSI (Agence Nationale de Sécurité des Systèmes d'Information) subventionne, dans le cadre de France Relance, la mise en place de système de cybersécurité au sein des établissements publics car maintenant la question n'est plus « comment va-t-on se faire pirater ? » mais « Quand ? ». Il faut donc chercher à minimiser l'impact d'une cyberattaque. Dans ce contexte et pour éclairer l'exécutif de notre commune, je vais traiter le domaine de la cybercriminalité en répondant aux questions suivantes.

Question n°1 : Constat des cyberattaques et les enjeux pour Ingéville

Ingéville le 16 juin 2022
Direction des Systèmes d'Information

À l'attention de Monsieur le directeur des systèmes d'information

Objet : les cyberattaques
Référence : loi de programmation militaire 2019/2025

Les cyberattaques peuvent prendre plusieurs formes mais le constat reste le même, en cas d'attaque, le système informatique de l'entreprise ou de la collectivité est le plus souvent à l'arrêt, le temps de retirer l'infection et réparer les dommages, si cela est possible. Dans un premier temps, nous dresserons un constat des cyberattaques puis dans un deuxième temps, les enjeux de notre collectivité se de prémunir de cette cybercriminalité.

1- Constat des cyberattaques

Il devient plus facile de nos jours de voler de l'argent derrière un ordinateur que de forcer les portes d'une banque. La cybercriminalité est omniprésente aujourd'hui, avant les hackers s'attaquaient aux grandes entreprises mais maintenant même une petite collectivité peut être touchée. Les cyberattaques les plus connues sont les ransomwares, c'est-à-dire une attaque où l'on récupère, ou l'on crypte les données et pour les récupérer ou décrypter, on paye une rançon très souvent ne bitcoin. Ces attaques font des dégâts importants, perte de fichiers, vol de dossiers à caractère personnel par exemple et arrêt total du système d'information.
Les logiciels espions sont aussi dangereux mais dans une autre forme. Ils permettent de s'introduire dans un système informatique et d'exécuter son piratage des jours, voire des semaines plus tard ; il extirpe des informations importantes pour ensuite les revendre ou demander de l'argent contre restitution.
La cyberattaque passe principalement par une page internet vérolée ou par la messagerie.

2- Enjeux pour Ingéville

Ingéville est une commune de 100 000 habitants et beaucoup d'entre eux utilisent les services de la ville : écoles, périscolaires, restauration scolaire. Nous possédons donc des données personnelles leur appartenant (civilité, nom, adresse, coordonnées bancaires) ; nous nous devons donc de sécuriser ces données. Avec le RGPD (Règlement Général de la Protection des Données), nous sommes obligés d'identifier tous les fichiers à caractère personnel, de les déclarer auprès de la CNIL (Commission Nationale de l'Informatique et des Libertés) et d'en assurer leurs sécurités sur un temps donné.
En tant que commune, nous avons l'obligation de distribuer l'eau potable même si celle-ci est gérée par un prestataire. Il nous faut donc assurer notre sécurité informatique au sein de nos stations d'épuration, qui peuvent elles-aussi être attaquées. Ces compétences dites de secteur vital doivent toujours être sécurisées, cela pourrait entrainer des catastrophes sanitaires importantes.

La commune d'Ingéville se doit de mettre en place des systèmes sécurisés pour contrer, ou tout du moins freiner, la cybercriminalité à laquelle elle peut faire face.

Question n°2

a) Quels systèmes pourraient être la cible de cyberattaque et les risques associés

La donnée personnelle, et surtout sa gestion, sont de la responsabilité de la commune, qu'elle concerne un agent ou un administré. Une fuite d'information, notamment bancaire, peut-être préjudiciable à chacun.
La sécurité des bâtiments, en terme d'accès, d'électricité, de fluide, doit être aussi préservée, notamment dans des lieux recevant du public. Une porte contrôlée par un accès sécurisé et ne s'ouvrant qu'avec un badge, comme dans beaucoup de crèches par exemple, si une cyberattaque bloque l'accès à la porte, il y a un risque pour les usagers.
L'eau potable et surtout sa livraison en qualité fait aussi partie de la responsabilité de la commune, i faut donc se prémunir des éventuelles attaques sur nos stations.
Notre système de téléphone ne doit pas subir d'attaques ; dans tous les bâtiments recevant du public, un téléphone doit être accessible pour prévenir les secours.

b) Conséquences d'un tel piratage pour les administrés d'Ingéville

Les conséquences sont énormes pour les administrés. Tout d'abord, en cas de récupération de leurs données personnelles, les hackers peuvent usurper leur identité et se servir de leurs nos à des fins malsaines. Ils peuvent également récupérer leurs informations bancaires et vider le compte des administrés ou faire des achats avec. En récupérant les données personnelles, les hackers vont connaître leur adresse mail et envoyer ainsi des mails frauduleux en leur nom et permettre une chaîne de mails qui peuvent infecter d'autres personnes.
Il y a bien sûr la conséquence sanitaire, indiquée ci-dessus, en cas de changements de paramétrages dans les stations d'épuration.
Les hackers vendent aussi des renseignements sur Internet ; en récupérant les coordonnées postales d'un administré, sa profession, les cambrioleurs achètent ces données et connaissent le lieu de résidence ainsi que les heures d'absence des habitants de leur domicile.

Moyens pour réduire les risques abordés

Pour protéger les risques potentiels pour un administré en cas de cyberattaque de notre système informatique, nous devons protéger les données les concernant. La CNIL nous oblige à garder les données à caractère personnel que sur un temps donné. Ces données seront donc automatiquement supprimées à la fin de la période. De plus, le temps de la conservation, ces données seront chiffrées et cryptées par nos outils, ce qui en cas de vol ne donnera pas la possibilité aux hackers de les exploiter.
Pour ce qui est du risque sanitaire, il faut protéger notre réseau informatique et séparer par des systèmes de VLAN, le réseau d'assainissement. Ce réseau sera hermétique à notre système de données et transitera dans un réseau protégé et isolé.

Question n°3

Au vu des annexes 1 et 2 du réseau informatique d'Ingéville, le renforcement de la sécurité du réseau doit être fait. Les principaux équipements de sécurité sont déjà présents mais nécessité d'être configuré différemment. Les sites distants accèdent au site de la mairie uniquement par Internet sans contrôle entre les 2, idem pour la mairie annexe. La mise en place de Firewall sur chaque site est essentiel et permettra de monter des liens VPN IPSEC entre les sites, liens sécurisés et chiffrés. Du côté de la mairie, il n'y aura pas d'accès direct entre le Switch et le Routeur, les données sortantes transiteront par le Firewall, idem pour les données entrantes. Il existe plusieurs types de matériels (PCs, Téléphones IP, Caméra, Bornes Wifi, Équipements voiries, automates pour les stations d'épuration), nous créerons des VLANs pour chaque type de matériel. Les Switchs étant compatibles à cette séparation des réseaux. Un VLAN sera également mis en place pour les serveurs. Pour limiter les interactions entre VLANs, nous mettrons en place des ACLs. Nous utiliserons également le Firewall de la mairie pour mettre le serveur relais de messagerie et serveur FTP en DMZ (zone démilitarisée) qui permettront aux usagers utilisant le FTP de ne pas accéder en direct au réseau serveur. Le relais de messagerie en DMZ permettra un premier filtrage des mails grâce à un antispam installé et un antivirus. Cela limitera les mails frauduleux à pénétrer notre réseau.
Les postes sont équipés d'un antivirus, nous installerons un nouveau serveur qui gèrera l'ensemble des antivirus des postes et des serveurs. Ce système antivirus sera muni d'un module EDR (EndPoint Detection and Response) pour être plus efficace en cas de cryptage de données. Ce module permet en cas de plusieurs fichiers cryptés dans un laps de temps court, de bloquer le processus.
Dans le but de sécuriser encore un peu plus le système informatique, nous installerons un serveur de sauvegarde sur le site de la mairie ; celui-ci sera répliquer dans le CLOUD chez un fournisseur de service CLOUD, et en cas d'infection de notre système, nous pourrions repartir sur des données propres de la veille de l'incident.
Nous prévoirons par la suite de raccorder les 2 mairies directement ensemble par de la fibre noire (non opérée) et dupliquerons les éléments serveurs sur la mairie annexe en utilisant la virtualisation pour éviter d'avoir trop d'équipements.

Question n°4

a) Actions à mener en priorité suite à une cyberattaque

La première action à mener est de couper les accès à internet et entre les sites distants. Ensuite, éteindre les serveurs pour éviter que la contamination continue. Les 2 actions peuvent être menées en même temps mais certaines cyberattaques s'arrêtent dès lors qu'elles n'ont plus accès au serveur du hacker. Si le problème vient d'un poste de travail, on l'isole du réseau en le débranchant. On vérifie que l'attaque n'a pas eu lieu sur un autre poste. Ensuite, on redémarre les serveurs, les uns après les autres, en les redémarrant en mode « sans échec » ; on limite l'accès aux comptes administrateurs en se connectant uniquement avec un compte local sur le serveur en ayant bien, au préalable, débranché sa carte réseau ou désactivé s'il s'agit d'un serveur virtuel. Une fois après avoir isolé le réseau du poste et/ou le serveur vérolé, on nettoie le serveur de ce logiciel espion avec des outils adaptés. On peut ensuite analyser d'où est venue l'attaque, par quel biais avec des antivirus de type EDR et, une fois l'installation protégée, on reconnecte tous les équipements, les sites distants et internet. Pour le serveur incriminé, on le restaure avec des sauvegardes saines et avant de la rebrancher sur le réseau, on vérifie que le logiciel espion n'était pas déjà présent et en sommeil.

b) Organisation de crise adaptée

Dans le cas d'une cyberattaque sur notre système d'information, nous devrons définir d'une organisation adaptée à la situation et à l'échelle de la ville.
Après avoir coupé nos systèmes informatiques de l'accès internet, nous appellerons nos sites distants sur des téléphones portables d'agents qui auront été désignés en tant que référent pour leur indiquer l'arrêt des services. Les services accueillant du public devront prévenir les usagers de cet incident.
Les collègues de la DSI analyseront, comme indiquer dans les actions, d'où est venue l'attaque. Toujours par l'intermédiaire des téléphones portables, indépendant de notre réseau informatique, nous préviendrons les organismes de sécurité de notre cyberattaque, notre direction de la communication interviendra pour indiquer un message sur le site internet de la ville ainsi que sur nos réseaux sociaux.
Le directeur des Systèmes d'Information appellera la gendarmerie pour un dépôt de plainte pour que les services de l'État, spécialisés dans la cybercriminalité, puissent étudier notre problématique.
Le directeur des services techniques ainsi que le gestionnaire des stations d'épuration passeront les automates en mode « déconnecté » pour ne pas prendre de risque.