EXAMEN PROFESSIONNEL D'INGÉNIEUR TERRITORIAL
SESSION 2018

SPÉCIALITÉ « INFORMATIQUE ET SYSTÈMES D'INFORMATION »
OPTION « SYSTÈMES D'INFORMATION ET DE COMMUNICATION »

ÉPREUVE DE PROJET

NOTE OBTENUE : 15.88 / 20

Métropole d'INGECO
Direction des Systèmes d'Information
Et des Services Numériques

Le 14 juin 2018

SERVICE MUTUALISÉ SIG
ÉTUDE : SIG ET PRÉVENTION DU RISQUE INONDATION

À l'attention de Monsieur le Président

QUESTION 1 : ENJEUX ET OBJECTIFS DE LA CYBERSÉCURITÉ ET ANALYSE DES RISQUES ET DES PRINCIPALES DIFFICULTÉS DANS LE CONTEXTE DE LA COLLECIVITÉ :

À l'ère du numérique, la collectivité doit faire preuve d'une forte adaptabilité pour se protéger contre les menaces informatiques et répondre aux obligations légales. La cybersécurité est de plus en plus dans les orientations stratégiques des systèmes d'information (SI).
Dans une première partir, je présenterai les enjeux et les objectifs de la cybersécurité pour analyser ensuite les risques et les difficultés dans la collectivité.

I- Enjeux et objectifs de la cybersécurité :

1- Les obligations légales en matière de sécurité du SI :

En premier, le service public a une obligation de continuité de service. Une attaque contre le SI peut suspendre éventuellement les services et avoir des répercussions graves pour les usagers comme nuire à l'image de la métropole.
Un système d'information a pour vocation le traitement, la circulation, le stockage, l'archivage, la communication de l'information sur les niveaux matériels, logiciels donnés, procédures et humains. En ce sens, la cybersécurité protège le SI contre les risques potentiels.
Pour ce faire, le législateur a réglementé avec le référentiel général de sécurité, la commission nationale informatique et liberté et créé des instances comme l'Agence Nationale de la Sécurité des Systèmes d'Informations pour informer et émettre des recommandations. Quant à la CNIL, elle oblige au préalable de déclarer les traitements et des contrôles sur site vérifient l'application des mesures de sécurité.
Les enjeux sont multiples puisqu'il s'agit de protéger les données et les ressources contre une action malveillante. Toute perte ou divulgation d'informations est un préjudice grave contre la collectivité et contre un tiers, par exemple pour le respecte de la vie privée et des données personnelles. Le Règlement Général de Protection des Données poursuit cette responsabilisation des collectivités.
En outre, une indisponibilité de service entraine des coûts considérables pour la collectivité et la destruction d'un service ou de données n'est pas envisageable. Les enjeux sont donc juridiques, financiers, et en terme d'image pour la collectivité.

2- Les trois domaines principaux de la sécurité du SI :

La disponibilité, l'intégrité et la confidentialité sont les objectifs majeurs de toute politique de sécurité. Nous pouvons ajouter l'authentification et la traçabilité.

La direction informatique doit mettre en œuvre des solutions pour atteindre ces objectifs qui sont même une mission prioritaire par rapport à l'offre de services. En plus, elle assure la protection des données personnelles. Ce sont les missions particulières du Responsable Sécurité des Systèmes d'Informations (RSSI) et du Délégué à la Protection des Données (DPD).

II- Analyse des risques et des difficultés dans la collectivité :

1- Inventaire des menaces

Pour les applications web, l'injection SQL, le vol de session ou de cookie, le cross site scripting et le deny of service (appel d'un service de manière intempestive) sont les dangers principaux.
Pour les postes de travail, les virus, spyware, cheval de Troie, etc… sont des menaces classiques et le rançongiciel, plus récent, est cité actuellement dans la presse informatique.
Pour la messagerie, le spam et le phishing, pour les terminaux mobiles, la perte et le piratage visuel.
Pour le facteur humain, il importe de se prémunir contre des intentions malveillantes et de la négligence et pour des menaces plus classiques sur site avec clé USB et autorun.

2- Les difficultés pour la mise en œuvre de la sécurité :

Les technologies de l'information sont en perpétuelles mutation et le RSSI doit réaliser une veille technologique continuelle sur les nouvelles menaces. En plus, la multiplication des postes de travail ou outils de travail rendent difficile la mise à jour des systèmes d'exploitation, des anti-virus etc… Les budgets et les ressources diminuent et pour autant, mes usages augmentent (BYOD, terminaux mobiles, etc…)
Le RSSI est en charge de mettre en cohérence les systèmes d'information avec les évolutions technologiques, les menaces et les besoins.

QUESTION 2 : ENJEUX ET OBJECTIFS DE LA CYBERSÉCURITÉ ET ANALYSE DES RISQUES ET DES PRINCIPALES DIFFICULTÉS DANS LE CONTEXTE DE LA COLLECIVITÉ :

a) Délégué à la Protection des Données :

« Vous serez en charge de mettre en œuvre la conformité au règlement européen sur la protection des données s'agissant de l'ensemble des traitements mis en œuvre par notre collectivité.
Chef d'orchestre entre les services métiers et la direction des systèmes d'information, vous dépendrez directement de la Direction Générale des Services pour un pilotage transversal.
Vous aurez la responsabilité, à tout moment et par défaut, d'assurer que les traitements sont en conformité avec le RGPD. Pour ce faire, vous tiendrez le registre des données à jour, vous participerez à la conception des nouvelles applications (Privacy By Design) pour la gestion des sonnées etc…
Vos tâches et missions précises :
- Réaliser l'inventaire des traitements
- Evaluer ses pratiques et mettre en place des procédures
- Identifier les risques
- Établir une politique de protection des données personnelles
- Sensibiliser les opérationnels et la direction. »

Les services métiers, l'autorité de contrôle, les agents de la DSI et les citadins sont susceptibles de solliciter le DPD.

b) Sur fond d'appauvrissement des ressources (financières et humaines) et devant la transversalité de la démarche et la richesse technologique, la mutualisation pour les fonctions de DPD et RSSI des collectivités de la métropole est souhaitable. Dans le cas du DPD, la règlementation oblige à la présence d'un DPD dans une collectivité comme responsable ; il sera donc judicieux de solliciter la cellule juridique de la métropole pour proposer la forme à retenir (revoir la convention de mutualisation en ajoutant un paragraphe sur le DPD de la métropole et des communes). Il s'agit en effet d'une autorité prévue dans les textes de lois.

Dans le cas du RSSI, l'enjeu est d'appliquer la même politique de sécurité des systèmes d'information dans les communes comme dans la métropole. Il s'agit de réaliser des économies d'échelle, d'avoir une ressource à temps plein pour suivre les recommandations, les menaces et les mesures correctives. La seule obligation légale est l'homologation du SI par l'ANSSI par exemple. Le RSSI n'est pas une autorité administrative mais un expert en la matière de sécurité. Il pourra donc piloter la politique de sécurité des systèmes d'information dans chacune des collectivités.

c) Il s'agit d'une collaboration entre un mission administrative (DPD) et une mission techniques (RSSI). L'espace de travail privilégié sera lors de la conception de nouvelles applications (Privacy By Design) où le DPD ciblera les données utiles et le RSSI appréciera le traitement des données. Ils définiront ou superviseront ensemble le processus métier.

QUESTION 3 : LES BONNES PRATIQUES D'USAGES EN MATIÈRE DE SÉCURISATION DU RÉSEAU INFORMATIQUES :

La sécurité du réseau informatique est primordiale dans la Politique de Sécurité des Systèmes d'Information puisqu'elle protège contre l'intrusion dans le système d'un agent étranger. Il s'agit notamment de protéger les espaces et les zones. Je présenterai dans un premier temps les bonnes pratiques générales pour cibler, ensuite, les propositions sur l'infrastructure technique.

I- Recommandations générales de la sécurité du SI

Il est nécessaire de sensibiliser les utilisateurs avec des formations et par la mise en place d'une charte informatique avec force contraignante.
Ensuite, il faut veiller à l'habilitation des utilisateurs en s'assurant que les agents ayant terminé leur mission soient exclus. L'authentification des utilisateurs est nécessaire sur le poste de travail, sur les serveurs, et sur les terminaux personnels et privés (mot de passe obligatoire pour la messagerie professionnelle, sur le smartphone personnel). En plus, la politique de mot de passe doit suivre les recommandations de la CNIL et il sera demandé régulièrement de changer de mot de passe.
Le poste de travail doit être protégé ave la mise à jour régulière du système d'exploitation et des anti-virus. L'usage de clé USB et de supports de stockage amovibles sera limité (suppression de l'autorun).
Les terminaux mobiles seront chiffrés et une synchronisation régulière du poste sera effectuée pour la sauvegarde des données (cas des ordinateurs portables nomades).
La maintenance applicative sera encadrée et suivie d'une main courante. Des clauses de confidentialité seront citées dans le contrat de service et des bases de données avec des informations fictives ou anonymisées seront uniquement communiquées.
Nous veillerons à journaliser les accès pour suivre et porter un diagnostic rapide en cas d'incident.
Les applications web seront vérifiées et auditées au niveau du code source (login et mot de passe dans l'url à supprimer), et le protocole https sera rendu obligatoire aussi bien en intranet qu'en extranet. Le protocole TLS remplacera le protocole SSL.
Les développements seront encadrés par des clauses, et en plus nous exigerons que les prestataires extérieurs soient certifiés ISO 27001.
Les technologies de cryptographie seront encouragées avec des certificats pour les signatures et cochets, l'authentification etc…

L'ensemble de ces recommandations générales est essentiel à protéger de toute intrusion dans le SI mais le réseau à proprement a des solutions techniques précises pour se prémunir des risques.

II- Sécuriser son réseau informatique : infrastructure technique

Il est important de cloisonner son réseau entre ces différentes zones. Entre le LAN et la DMZ, un firewall segmentera l'intranet et entre la DMZ et le WAN, un firewall isolera de l'internet. Cette architecture réseau permet de concentrer les applications, les données, et les serveurs sensibles dans le réseau interne qui théoriquement n'est en aucun cas accessible de l'extérieur.
Il faut s'assurer de la sécurité d'accès wi-fi en séparant les usages. Le réseau wi-fi doit être limité à un périmètre donné du système d'information.

L'utilisation de protocoles sécurisés (https, smtps, Imops, Pop3s) est préconisée voire à rendre obligatoire en cas d'extranet. Il est recommandé de mettre en place une passerelle d'accès sécurisé à internet, comprenant un firewall et un serveur mandataire (proxy) embarquant différents mécanismes de sécurité.
Les infrastructures des services visibles depuis l'internet doivent être physiquement cloisonnées des infrastructures du système d'information. L'utilisation d'un VPN et/ou Reverse Proxy est obligatoire compte tenu de l'importance de la collectivité.
Les partenaires accéderont au réseau interne après identification de l'adresse IP pour éviter tout risque d'intrusion sut le réseau. Les locaux et les accès aux salles serveurs seront protégés avec des alarmes et une entreprise de gardiennage. Quant aux serveurs, les habilitations seront réduites aux agents ayant une mission ou un rôle.
La norme ISO 27001, les produits ou services qualifiés par l'ANSSI seront privilégiés dans nos projets.

QUESTION 4 : NOTE À L'ATTENTION DU DIRECTEUR POUR PROPOSER UNE DÉMARCHE GLOBALE D'AMÉLIORATION DE LA CYBERSÉCURITÉ

Le directeur des systèmes d'information et des services numériques demande la mise en place d'une démarche globale d'amélioration de la sécurité du SI. En s'appuyant sur le référentiel général de sécurité et les recommandations de l'ANSSI, je présente dans une première partie les grandes étapes de la demande globale de sécurité pour engager dans un second temps l'ensemble des acteurs dans le PSSI.

I- Scénario de mise en œuvre d'une démarche d'amélioration de la sécurité du SI :

Une démarche globale et transversale sera privilégiée pour inclure les éléments responsables de la sécurité.
Ainsi, pour s'organiser, nous désignerons les différents acteurs décisionnels de la sécurité.
Ensuite, nous organiserons des réunions régulières de management de la sécurité du SI. Cette PSSI sera conduite par le RSSI. Un état des lieux sur les points forts et les points faibles en matière de sécurité du SI sera effectué. Ce diagnostic permettra d'établir un fil conducteur.
Une nouvelle analyse des risques sera effectuée. Éventuellement, il sera opportun de recourir à un audit auprès d'un prestataire extérieur qualifié par l'ANSSI. La méthode d'expression du besoin et d'identification des objectifs de sécurité sera utilement mise en œuvre (méthode EBIOS).
Ce système d'information sera corrigé et adapté au nouveau besoin. Une homologation ensuite viendra confirmer la qualité des travaux effectués.

Ensuite, nous procéderons au suivi opérationnel avec l'analyse des journaux d'événements, les incidents rencontrés et les résultats des audits. Une chaîne d'alerte sera mise en place en cas d'incidents ou d'intrusion dans le SI pour avertir les personnes responsables et mettre en place une solution de défense. Les mesures correctives seront effectuées. La gestion des accès et des habilitations des utilisateurs sera améliorée.
Dans le cadre d'un plan d'amélioration continu, nous profiterons de cette transformation pour obtenir la norme ISO 27001 auprès d'un organisme de certification. En décrit en outre les exigences pour la mise en place d'un système de management de la sécurité de l'information. Nous l'exigerons à présent auprès de nos prestataires.

II- Démarche participative et sensibilisation des utilisateurs :

La charte informatique sera adaptée aux nouveaux enjeux avec des exigences supplémentaires pour les utilisateurs en matière de sécurité. On veillera à sa signature pour chacun des agents informés alors des risques qu'il peut entrainer pour l'administration.
Dans un but de créer un engagement dans le changement des conduites, nous organiserons des formations sur la sécurité pour une sensibilisation à la sécurité. Nous fonderons notre action sur une démarche participative pour avoir des informations approfondies sur les problématiques rencontrées dans l'usage de l'outil informatique.
Il appartiendra au RSSI et au DPD de communiquer sur ces thématiques. L'enjeu culturel est primordial pour diminuer la résistance au changement. Nous rappellerons notamment les obligations de confidentialité (devoir de discrétion, de réserve) auxquelles sont tenus les agents.

Le télétravail, les terminaux mobiles, la multiplication des outils professionnels et les mobilités complexifient grandement le travail du RSSI. Il sera judicieux qu'à l'ère numérique, les utilisateurs soient responsabilisés dans leur usage de l'outil informatique.