Dossier de corrigé : La protection du système d'information de votre mairie

Date :le 2/06/2022

Les agents de la mairie reçoivent de manière récurrente des courriels frauduleux qui, peuvent s'apparenter à des échanges professionnels tant les expéditeurs et les contenus sont en rapport avec leur domaine d'activité.

Le système d'information dans son ensemble se trouve exposé à des actions malveillantes de la part des initiateurs.

Le but recherché est de s'emparer ou de corrompre l'ensemble des données disponibles.

Cette note a pour objectif de décrire l'état de l'art actuel du système d'information, d'évaluer son degré de maturité et de proposer des pistes d'amélioration à court, moyen et long terme afin de garantir une intégrité maximale et le rendre pérenne.

I) Etat des lieux actuel

L'intégrité du système d'exploitation dépend à la fois de la vigilance de chaque agent, mais également d'un environnement technique sain, régulièrement mis à jour dans toutes ses composantes.
C'est la raison pour laquelle l'aspect fonctionnel doit faire l'objet d'un accompagnement et d'un rappel régulier aux règles de bonnes pratiques. Chaque agent est un acteur à part entière de la bonne santé du système d'information.
L'aspect technique vient en complément du fonctionnel en s'assurant qu'il n'existe aucune faille de sécurité identifiée.

I.1) Les postes de travail

I.1.1) Mesures organisationnelles

Les agents sont régulièrement sensibilisés par la diffusion de courriel d'alerte interne sur la conduite à tenir en cas de réception de mel frauduleux qui consiste à ne pas ouvrir les pièces jointes ou cliquer sur les liens proposés.

De même, l'ensemble des agents ont connaissance des bonnes pratiques dans le choix de leurs mots de passe. Il faut à tout prix éviter d'utiliser des mots de passe trop simples en introduisant des majuscules, des nombres et des caractères spéciaux. Il doit être changé tous les trois mois en respectant le degré de complexité.

Il est désormais interdit de connecter tout support externe (clé USB, disque dur externe, chargement de téléphone portable ect …) sans avoir au préalable vérifié à la station blanche disponible à l'accueil qu'aucun virus n'est présent.

I.1.2) Mesures techniques

Les postes de travail sont tous dotés d'un antivirus professionnel (Norton) qui bénéficie de manière régulière des mises à jour de la part de l'éditeur.

Le système d'exploitation Microsoft (Windows 10) nouvellement déployé est lui aussi à jour de tous les correctifs de sécurité (Windows Update).

Le pack Msoffice 2013 installé sur la majorité des ordinateurs est maintenu à jour des failles de sécurité jusqu'en 2023. À ce sujet, il va falloir songer à renouveler ces licences qui expirent l'année prochaine.

Quant au navigateur Web, Firefox a été installé à la place d'Internet Explorer devenu trop vulnérable. Il est lui aussi mis régulièrement à jour et évalué pour garder la pleine compatibilité avec les applications et les services numériques utilisés au quotidien.

II) Infrastructure

II.1) Serveurs

Les serveurs ont été renouvelés en 2016

Il va falloir prévoir leur remplacement dans les deux années qui viennent pour maintenir un niveau de performance et bénéficier de noyaux qui ne présentent pas de failles de sécurité.

Par la même occasion, il faudra étudier la possibilité de rendre résilient le contrôleur de domaine, qui assure les briques de sécurité indispensables comme l'authentification lors de l'ouverture de la session.

Pour suivre l'évolution des besoins, la capacité globale de stockage et la réplication des données fera l'objet d'une attention toute particulière.

La résilience , la sauvegarde régulière des données contribuent à garantir un fonctionnement optimum et offrir la capacité de restaurer les données dans les meilleurs délais d'un système d'information corrompu.

Concernant la virtualisation , il existe une ébauche de cartographie applicative pour savoir quelle machine porte quelle application . Elle nécessite une mise à jour et un travail de consolidation pour être pleinement exploitée.

II) Réseau informatique

II.1) Réseau fixe

Le réseau informatique n'est pas segmenté de manière logique en Vlan. Il va falloir à minima séparer dans deux LAN différents, les clients(poste de travail) et les serveurs pour cloisonner davantage les flux applicatifs.

De même, la création d'un VLAN spécifique pour les postes de téléphonie sur IP, et un second pour l'infrastructure de ToIP va renforcer le niveau de sécurité.

II.2) Réseau Wifi

Le réseau Wifi, nouvellement déployé, offre une couverture tout à fait satisfaisante mais ne présente pas un niveau de sécurité suffisant. Il est trop ouvert et son accès facile.
Les connexions vont devoir très rapidement être journalisées afin de maîtriser l'usage de la liaison mise à disposition par la mairie.
Il en est de même pour les mots de passe qui doivent être complexifiés et changés régulièrement .
Une connexion invité, avec une durée de connexion limitée dans le temps devra être proposée et soumise à la validation d'un administrateur du système.

III) Compétences

Le technicien système qui a déployé l'architecture virtualisée a fait valoir ses droits à la retraite. Le maintien à niveau des compétences apporte la garantie de paramétrer au mieux les différents éléments qui composent le système d'information et ainsi de réduire son degré de vulnérabilité.
La veille technologique, la consultation de forums spécialisés permet également de manière pérenne de garder un niveau de protection élevé et un système d'information intègre.

Commentaire du concepteur : cet aspect du sujet ne fait l'objet d'aucune documentation et doit faire appel au bon sens des candidats. Cependant cette information est évoquée dans le « Document 1 : Éléments de contexte (F. POLLET, 4 juin 2022). 1 page »

IV) Les pistes d'amélioration

IV.1) A moyen terme

Les pistes d'amélioration à moyen terme concernent essentiellement les composants de l'infrastructure.
Cela consiste à gérer les droits d'accès aux différentes ressources du système de manière rigoureuse.
Lors du départ d'un agent ou d'un stagiaire, le profil est à supprimer au plus tôt.
Les mots de passe utilisés par les administrateurs du système doivent être nominatifs et d'une complexité qui respecte les règles définies.
L'investissement de manière substantielle dans la sauvegarde des données et leur réplication est en enjeu majeur pour redémarrer le système d'information après une compromission.
Pour les agents amenés à se déplacer à l'extérieur il est fortement recommandé de chiffrer le contenu des supports amovibles.
Une étude sur le cloisonnement logique du réseau local va permettre de segmenter les flux et éviter la propagation totale d'un virus à l'ensemble des machines, que ce soit les clients ou les serveurs.

IV.2) À long terme

Sur le long terme, il est indispensable de définir une Politique de Sécurité des Systèmes d'Information (PSSI), pour définir la stratégie et les règles à appliquer.

De même, une cartographie précise du système d'information est le gage d'une bonne maîtrise globale et rendra plus facile l'expertise en cas d'attaque.
Pour les applications les plus sensibles, une analyse de risque permettra de prendre les mesures les plus adaptées pour garantir une protection optimale des données.
Un audit de sécurité réalisé par une entreprise spécialisée dressera un état précis des lieux afin d'appliquer les règles de l'art des différentes composantes.
La dernière étape visée est d'obtenir une homologation qui garantira la robustesse et la pérennité de notre système d'information.

V) Conclusion

D'après l'ANSSI, agence nationale de la sécurité informatique, les Cyberattaques vont augmenter de manière exponentielle.
Les scénarios déroulés vont être de plus en plus réalistes, et le panel des attaques de plus en plus diversifié.
La sécurité est l'affaire de tous et commence par une prise de conscience des agents des risques majeurs encourus.
Il faut avant tout protéger la donnée, la dupliquer et ainsi permette la restauration rapide du système d'information.
Les composants sensibles comme le contrôleur de domaine doivent être dupliqués pour apporter un niveau de résilience élevé.
Une bonne segmentation logique du réseau local apporte un niveau de sécurisation supérieur.
Le maintien des compétences des techniciens, les formations régulières permettent de paramétrer au mieux les composants du système et ainsi limiter les failles de sécurité.

Grille de correction-Note- Correcteur : copie n°

Partie	Précisions		Points (+)	Pénalités (-)	Bonus (+)
PARTIE PAR PARTIE					
Introduction	**« bonne » introduction**	// introduction de la note / (~ 10 à 15 lignes) ▪ entrée en matière- reformulation du sujet (1 pt), ▪ annonce de la problématique (1 pt) ▪ + annonce du plan (organisation des parties) (1 pt) Introduction parfaite	**/ 3 pts**		/ 1 pt
	Absence d'introduction *Absence de problématique*			*/ 0.5 pt* */ 0.5 pt*	
Plan	**Plan retenu**	▪ Dvpment organisé en parties & sous-parties (1 pt) ▪ Plan apparent par de saut de ligne (0,5 pt) ▪ Qualité du plan choisi et respect /. à l'intro (1 pt) ▪ Présence de transitions (0,5 pt)	**/ 3 pts**		
	Absence de plan ou plan non justifié ou non respecté			*/ 0.5 pt*	
Conclusion	*Pas de conclusion ou Conclusion inappropriée*	*Relance de la problématique ;* *Eléments nouveaux ou omis dans le développement de la note ;*		*/ 0.5 pt*	
	« bonne » conclusion	Réaffirme ou synthétise les principales idées ; Résumé de ce que l'on doit retenir ; (~ 5 à 10 lignes) Ouverture du sujet Conclusion parfaite	**/ 1,5 pts**		/ 1 pt
Contenu	**Pertinence de la problématique (0,5 pt)** **Plan cohérence (0,5 pt)** **Compréhension du sujet p/ à la question posée (1 pt)** **Répond à la question posée (1 pt)** **Connaissance des textes et leur application (1,5 pt)** **Maîtrise des connaissances requises pour le traitement du sujet (2 pt)** **Idées précises et pertinentes (1 pt)** **Utilisation des documents joints (1pt)** Copie exceptionnelle (qualité d'expression + connaissance + réponse)		**/ 8,5 pts**		/ 1 pt
	Hors sujet *Contresens, non maîtrise des contenus* *Oubli d'informations primordiales*			*/ 1 pt* */ 1 pt* */ 1 pt*	
DE MANIERE GENERALE : LA FORME DE LA COMPOSITION					
Ensemble du corps de la note	**Présentation, écriture : clarté, lecture aisée**		**/ 1 pt**		
	Style (vocabulaire précis, règles de syntaxe, ...)		**/ 1 pt**		
	Esprit d'analyse, capacité à la réflexion, parties équilibrées		**/ 2 pts**		
	Présentation désastreuses (ratures, absence de clarté)			*/ 1 pt*	
	Présence de faute d'orthographe, grammaire (à partir de 5)			*/ 3 pts*	
	Expression familière, défaillante, absence de terme technique			*/ 0.5 pt*	
	Absence d'esprit d'analyse et d'argumentation			*/ 1 pt*	
	Présentation des idées et des connaissances de manière inorganisée			*/ 1 pt*	
	Opinions personnelles affichées et trop affirmatives sans justification			*/ 1 pt*	
	Longueur de la copie			*/ 0.5 pts*	
	Devoir inachevé			*/ 0.5 pts*	
TOTAL GENERAL = /20 *= (points – pénalités + bonus)*			**/20 pts**	**/13,5pts**	**/3 pts**

Appréciation générale justifiant la note et signature du correcteur