Concours de recrutement des conseillers session 2022 spécialité technique domaine système d'information

Copie numéro 312

À l'attention de Madame la directrice générale des services commune IX

Le 22 septembre 2022

Objet : on note relative aux cyberattaques

Réf. : revoir liste de documents joints

Madame la directrice générale des services,

Le système d'information (SI) de la mairie est sujet à des attaques de diffusion de courriels frauduleux, cela dure déjà depuis quelques jours et commence à prendre de l'ampleur. Grâce à ces attaques nous devons réagir au plus vite avant que notre SI ne soit compromis. aussi comme vous l'avez demandé, vous trouverez dans cette note les mesures nécessaires à l'endiguement des attaques en cours et un plan d'action à mettre en œuvre pour renforcer et sécuriser notre SI contre des futures attaques potentielles.

Dans ce premier temps vous aurez un état des lieux relatifs aux protections actuelles de notre parc informatique ainsi que les mesures applicables de suite pour arrêter cette campagne. Dans un 2nd temps vous trouverez des propositions à mettre en œuvre pour renforcer et sécuriser notre SI.

après avoir consulté notre inventaire (voir document 1) t, vous pouvez remarquer l'obsolescence de notre parc informatique (obsolète à 50 %) R mais malgré cela, tous les postes ont un système d'exploitation (OS) Windows 10 version entreprise installé dans une version assez à jour. de plus un antivirus (Norton antivirus) R installer et le pare-feu Windows activer sur chaque poste. Également, R le

nécessaire a été fait pour que les utilisateurs ne puissent pas infecter les ordinateurs en bloquant les ports USB de la machine. R pour pouvoir consultez des documents externes provenant d'une clé USB il a été demandé aux utilisateurs d'analyser le support sur une des 2 stations blanches installées (PC isolé du réseau local et connecté directement à internet pour les mises à jour de l'antivirus). Toutes ces mesures constituent le minimum requis dans la sécurité informatique mais ne suffisent pas à freiner les attaques. pour se faire, je vous propose que nous mettions en application immédiate les mesures suivantes :

- Lancer une analyse antivirale sur tous les PC du parc ;
- Effectuer des mises à jour de sécurité des machines ;
- Il a changé les mots de passe de tous les collaborateurs y compris les administrateurs. Une politique de mot de passe sera appliquée comprenant la complexité du mot de passe (8 caractères minimum, minuscule, majuscule hé caractère spéciaux obligatoire) hé ainsi qu'un changement obligatoire tous les 45 jours.
- Désinstallation des logiciels superflus et mises à jour des logiciels obsolètes ;
- Interdiction des clés USB non chiffrées, qui implique un achat immédiat de clé chiffrée.
- Enfin, sensibiliser les collaborateurs au cyber risque et attaques en leur diffusant dans un premier temps les documents joints 2 et 6 puis fais des sessions de sensibilisation.

Ces actions, qui se base sur les documents de 6 ainsi que mon expérience, pour freiner l'infection si nous en sommes victime. Malheureusement elles n'auront d'effet que sur un court terme. Elles ne seront efficaces sur le long terme que si nous souhaitons nous investir davantage.

Comme évoqué précédemment, notre parc informatique est obsolète et doit faire l'objet de nombreuses évolutions tant sur le plan de l'infrastructure que sur le plan stratégique, plan qui compte dans la plupart des autres collectivités émis de côté car les collectivités ne se sentent pas touchées. Le manque de sensibilisation des élus à la cybersécurité et sur les impacts directs et indirects on est la cause. Cette sensibilisation fait partie des propositions qui permettra de mener à bien les actions ci-dessous :

Le SI doit faire l'objet d'un audit afin de nous remonter nos faiblesses, il aura pour objectif de :

- Évaluer les systèmes et processus en place qui sécurise nos données
- Déterminer les risques qui pèsent sur les outils informationnels. Aider à identifier les méthodes permettront de minimiser ces risques
- Assurer que les processus de gestion de l'information sont conformes aux lois, politique et norme spécifique au SI
- Déterminer les inefficacités des I et de la gestion associée. Cet audit servira de base de travail pour établir une feuille de route.
- Revoir l'architecture informatique qui est actuellement en niveau plat donc potentiellement moi sécurisé. Pour une sécurité optimale il est recommandé de segmenter le réseau et d'appliquer la ségrégation des flux. pour cela il faudrait mettre en place 2 niveaux de pare-feu et dédié à VLAN par type de serveur et mettre les serveurs critiques en DMZ. Également tous les serveurs devront être virtualiser afin d'en faciliter et sécuriser l'administration
- Installer des solutions de sauvegarde de type veean backup Sans sécurisés en cas de PCA (plan de reprise d’activité)

- Renouveler le parc des PC en mettant en place une stratégie bondissement qui revient à remplacer le parc tous les 3 ans en général.
- Embaucher un responsable de la sécurité des systèmes d'information (RSSI) qui sera en charge de mettre en œuvre tous les processus de sécurité et d'en être le garant
- Embaucher un administrateur système et réseau en plus du poste de technicien. Il aura la charge du bon fonctionnement et du suivi du SI

Enfin sensibiliser nos élus afin qu'ils prennent conscience des impacts de la cybercriminalité et des retombées de ces dernières.

Des solutions existent pour régler nos problèmes et vous avez pu, en lisant cette note, on appréhendait quelques-unes. Il s'agit d'un sujet sensible auquel nous sommes exposés mais dont nous n'avons pas forcément conscience. Il ne tient qu'à vous de faire changer la vision de nos élus et nos utilisateurs afin que ces problèmes soient maîtrisables.