MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

ANNALES DU CONCOURS

Accès à l'emploi de contrôleur spécialisé de la DGSE

Épreuve d'admissibilité :
cas pratique

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Session 2021

MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

1ère épreuve d'admissibilité

Cas pratique

Epreuve de cas pratique avec une mise en situation à partir d'un dossier à caractère technique remis au candidat pouvant comporter des graphiques ainsi que des données chiffrées.
Le dossier doit relever d'une problématique relative aux politiques publiques et comporter plusieurs questions précédées d'une présentation détaillée destinée à mettre le candidat en situation de travail.
Pour cette épreuve, le dossier documentaire ne peut excéder vingt pages.

RÉPUBLIQUE FRANÇAISE
DGSE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE

Durée : 3 heures - coefficient 3

CONCOURS EXTERNE
POUR L'ACCÈS À L'EMPLOI DE CONTRÔLEUR
SPÉCIALISÉ DE CLASSE NORMALE

SESSION 2021

<u>1ère épreuve d'admissibilité</u> :

Épreuve de cas pratique

Épreuve avec mise en situation à partir d'un dossier à caractère technique remis au candidat pouvant comporter des graphiques ainsi que des données chiffrées.
Le dossier doit relever d'une problématique relative aux politiques publiques et comporter plusieurs questions précédées d'une présentation détaillée destinée à mettre le candidat en situation de travail.
Pour cette épreuve, le dossier documentaire ne peut excéder vingt pages.

Durée : 3 heures ; coefficient 3

Contrôleur spécialisé, vous êtes détaché à la Mairie de Paris en tant que conseiller technique.

A la suite de cyberattaques subies par les hôpitaux franciliens en 2020, la mairie souhaiterait faire l'inventaire des menaces répertoriées ainsi que des risques encourus en cas de compromission. Pour cela, vous avez été mandaté pour rédiger une note abordant les trois problématiques suivantes :

- Quels sont les principaux enjeux de la commune face à la menace cyber ?
- Quelles sont les différentes menaces recensées qui pourraient affecter la commune ?
- Quelles seraient les préconisations à adresser aux agents et prestataires de la Mairie ?

Sommaire du dossier documentaire :

Document 1 : Bâtir et promouvoir une souveraineté numérique nationale et européenne
N°4299 – enregistré à la Présidence de l'Assemblée nationale le 29 juin 2021

Document 2 : Pouvons-nous éviter un Pearl Harbor numérique ?
MISC, N°114 – Mars/Avril 2021

Document 3 : Cybersécurité : Toutes les communes et intercommunalités sont concernées
AMF (Association des Maires de France), novembre 2020

Document 1 : Assemblée Nationale – Bâtir et promouvoir une souveraineté numérique nationale et européenne

Source : N°4299 – enregistré à la Présidence de l'Assemblée nationale le 29 juin 2021

INTRODUCTION

La crise sanitaire que nous avons vécue a fait la démonstration de la formidable dépendance de la France et de l'Europe vis-à-vis des solutions et matériels numériques non européens. Les outils utilisés afin de poursuivre une activité à distance ont été, dans leur grande majorité, américains. Au même moment, nombre de problématiques numériques ont refait surface, de la protection des données de santé aux enjeux de cyber-sécurité, face aux attaques informatiques qui ont notamment touché des collectivités territoriales et des structures de soins. Dans ce contexte compliqué, la question de la souveraineté numérique est réapparue avec force. La France et l'Europe doivent en faire la priorité de leurs politiques pour répondre à la demande de protection des citoyens, de compétitivité des entreprises, et, enfin, à une double exigence d'efficacité et de transparence des institutions publiques.

Dans ce contexte, le groupe MODEM a demandé et obtenu la création d'une mission d'information pour s'attacher aux conditions et moyens pour « Bâtir et promouvoir une souveraineté numérique nationale et européenne. »

La mission d'information, qui a tenu quatre-vingt-trois auditions, pendant plus d'une centaine d'heures, a ordonné celles-ci selon plusieurs thématiques, dans l'intention de faire suivre chaque constat de propositions opérationnelles :

– la base industrielle – industrie électronique et industrie du numérique, infrastructures – dont l'appréciation objective de la situation permet de mesurer la dépendance qu'il convient de réduire et le réalisme des objectifs à atteindre ;

– la compétitivité des entreprises, différentes autant par leur spécialisation que par leur taille, mais qui, toutes, évoluent dans un monde où la concurrence globale amplifie l'impact de leurs atouts comme de leurs handicaps ;

– la capacité des acteurs publics à piloter aussi bien les politiques de numérisation des administrations – leurs procédures, les relations avec leurs agents, leurs usagers et leurs fournisseurs – que les politiques de soutien à l'écosystème et aux filières d'avenir ;

– la compréhension des enjeux de la cybersécurité et de la mobilisation qu'ils requièrent de la part de tous, ce qui va bien au-delà des seules missions régaliennes ;

– l'impératif de la formation, dans toutes ses dimensions : de l'école à l'université, de la culture générale du numérique à la recherche de pointe, de l'utilisation des outils du quotidien à la maîtrise des algorithmes ;

– le rôle de l'Europe comme puissance normative, scientifique et économique, sans perdre de vue la dimension géopolitique qui interroge la possibilité d'un modèle numérique européen.

Votre rapporteur a tenu à hiérarchiser, selon l'urgence d'agir, les propositions découlant du constat sans fard auquel il s'est astreint, ce qui l'a conduit à définir quatre axes de propositions :

– premier axe : garantir la résilience de nos infrastructures ;

– deuxième axe : faire confiance à nos entreprises technologiques ;

– troisième axe : mettre la souveraineté numérique au cœur de l'action publique ;

– quatrième axe : mettre le citoyen au cœur des politiques numériques.

Votre rapporteur tient à remercier le président Jean-Luc Warsmann pour sa présidence attentive, l'ensemble de ses collègues qui ont participé aux travaux de la mission et toutes les personnes qui ont accepté d'être auditionnées pour leur approche, leur compréhension de la souveraineté numérique nationale et européenne, et pour la volonté d'action persévérante qu'ils ont tous appelée de leurs vœux, action dont dépend la faculté pour la France et ses partenaires européens de tenir leur rang – un rang à la mesure de leurs capacités – dans le monde et à l'âge numériques.

30 PROPOSITIONS CLÉS

AXE 1 : GARANTIR LA RÉSILIENCE DE NOS INFRASTRUCTURES

Ambition n° 1 : Garantir la sécurité de nos réseaux

Proposition n° 2 : Renforcer les contrôles mis en œuvre par l'Autorité de régulation des communications électroniques, des postes et de la distribution de la presse (ARCEP) sur la qualité du déploiement des réseaux fixes (page 42).

Proposition n° 3 : Maintenir une exigence maximale de sécurité vis-à-vis des déploiements 5G (page 43).

Ambition n° 2 : Faire face l'accroissement réel de la menace cyber

Proposition n° 1 : Créer un « comité numérique de crise » réunissant les opérateurs, les grands acteurs du numérique et les pouvoirs publics en cas de difficulté majeure sur les réseaux numériques (page 40).

Proposition n° 19 **:** Former les citoyens aux gestes-barrières face au risque cyber (page 66).

Proposition n° 40 : Accélérer la mise à niveau des équipements numériques des collectivités territoriales et des structures de soins pour garantir leur résilience (page 120).

Ambition n° 3 : **Assumer le coût de notre souveraineté numérique**

Proposition n° 34 : Augmenter les moyens financiers et les effectifs de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) pour répondre à la croissance de la menace cyber (page 109).

Proposition n° 35 : Consentir un engagement financier inédit à destination des acteurs de la protection numérique au sens large, c'est-à-dire la plateforme Pharos, le groupement d'intérêt public Action contre la Cybermalveillance (ACYMA) et le parquet national cyber (page 109).

Proposition n° 39 : Veiller à ce que la trajectoire définie au sein de la loi de programmation militaire pluriannuelle soit en adéquation avec l'état de la menace et le niveau d'ambition porté par la France dans ce domaine (page 119).

Proposition n° 41 : Appliquer une doctrine de l'autonomie technologique maximale en matière de renseignement et de cyberdéfense en faisant du recours à des technologies extra-européennes une exception devant être motivée (page 122).

AXE 2 : FAIRE CONFIANCE A NOS ENTREPRISES TECHNOLOGIQUES

Ambition n° 4 : **Faire de nos entreprises technologiques une priorité nationale**

Proposition n° 26 : Privilégier, en matière de commande publique, le recours aux solutions d'acteurs technologiques français ou européens (page 98).

Proposition n° 27 : Exiger de l'Union des groupements d'achats publics (UGAP) des délais raisonnables dans le traitement des demandes de référencement des acteurs de l'offre numérique française (page 98).

Proposition n° 31 : Renforcer le soutien public à destination de la French Tech, pour encourager ses membres à « chasser en meute » (page 100).

Ambition n° 5 : Accélérer les projets européens de « reconquête » numérique.

Proposition n° 57 : Garantir au sein de Gaia-X une gouvernance et une conduite de projets conformes aux ambitions exprimées par ses membres fondateurs afin d'éviter que cette initiative ne devienne un instrument au service de la croissance d'acteurs déjà dominants (page 160).

Proposition n° 58 : Accélérer le déploiement d'une constellation européenne de satellites en orbite basse (page 162).

Proposition n° 60 : Renforcer les moyens mis en œuvre dans le cadre des projets importants d'intérêt européen commun (PIEEC) et adopter à chaque reprise des calendriers ambitieux de déploiement (page 164).

AXE 3 : METTRE LA SOUVERAINETÉ NUMÉRIQUE AU CŒUR DE L'ACTION PUBLIQUE

Ambition n° 6 : Faire de l'État le moteur d'une politique de souveraineté numérique assumée.

– Défendre cette ambition au plus haut niveau de l'État

Proposition n° 45 : Créer un ministère du numérique, doté d'une administration et de moyens propres, et chargé de porter les politiques numériques aux niveaux national, européen et international (page 133).

Proposition n° 46 : Mettre en place un briefing hebdomadaire du Président de la République sur les questions technologiques en s'inspirant du modèle américain (page 133).

Proposition n° 65 : Mettre le numérique au cœur de la présidence française de l'Union européenne au premier semestre de l'année 2022 (page 178).

– Faire évoluer rapidement les pratiques de l'administration

Proposition n° 13 : Favoriser la circulation des compétences numériques au sein du secteur public (page 62).

Proposition n° 52 : Imposer au sein de l'administration le recours systématique à des solutions numériques françaises lorsque leur niveau de performance est satisfaisant pour les usages concernés (page 138).

Proposition n° 53 : Imposer au sein de l'administration le recours systématique au logiciel libre en faisant de l'utilisation de solutions propriétaires une exception (page 138).

AXE 4 : METTRE LE CITOYEN AU CŒUR DES POLITIQUES NUMÉRIQUES

Ambition n° 7 : Simplifier la vie des citoyens grâce au numérique.

Proposition n° 10 : Accélérer le déploiement de l'identité numérique en France (page 59).

Proposition n° 17 : Développer une culture de la transparence vis-à-vis des données utilisées par la puissance publique dans le cadre de ses interactions avec les citoyens (page 65).

Proposition n° 50 : Créer un portail public rassemblant l'ensemble des offres numériques françaises disponibles (page 135).

Proposition n° 15 : Créer un guichet numérique unique d'accès de chaque citoyen à l'ensemble des services publics, lui permettant aussi d'être informé en temps réel de l'utilisation de ses données par l'administration (page 63).

Proposition n° 16 : Créer un numéro d'identification unique afin de mettre fin aux difficultés que rencontrent les administrations pour identifier les administrés et partager leurs informations de façon efficace (page 65).

Ambition n° 8 *:* Se donner les moyens de protéger leurs données personnelles

Proposition n° 5 : Renforcer les effectifs de la commission nationale de l'informatique et des libertés (CNIL) dans le cadre du projet de loi de finances pour 2022 (page 47).

Proposition n° 6 : Simplifier le processus de sanction mise en œuvre par la commission nationale de l'informatique et des libertés (CNIL) au sein des dossiers de moyenne et de faible intensité afin de renforcer sa capacité à prononcer les « mesures correctrices » prévues par le RGPD (page 47).

Proposition n° 7 : Intégrer de façon systématique au sein des arbitrages techniques des projets numériques les enjeux ayant trait à la souveraineté numérique, en particulier concernant la protection des données personnelles et la localisation des données en Europe (page 50).

Document 2 : Pouvons-nous éviter un Pearl Harbor numérique ?
Source : MISC, N°114 – Mars/Avril 2021

OÙ EN EST-ON DU PEARL HARBOR NUMÉRIQUE ?

David SORIA – dsoria@astar.org (@Sibwara)
Spécialiste Sécurité de l'Information chez Astar – dsoria@astar.org (@Sibwara)

Emblème du marketing par la peur pour les uns, cygne noir pour les autres, cette appellation désigne l'éventualité d'une attaque informatique éclair contre un pays et qui serait paralysante pour son économie. Le terme fait couler de l'encre depuis au moins 20 ans [1] et nourrit moult fantasmes. Mais sont-ce des fantasmes ? D'aucuns diraient que si en 20 ans il ne s'est rien passé, c'est probablement qu'il y a eu un alarmisme exagéré.

mots-clés : *PROSPECTIVE / CYBERCRIMINALITÉ*

1. ONT-ILS CRIÉ AU LOUP ?

En réalité, le premier Pearl Harbor numérique est déjà derrière nous.

Certains l'attribuent à **[Stuxnet]**, ce « virus » très perfectionné qui s'est attaqué aux centrales nucléaires iraniennes entre 2008 et 2010. Le modus operandi était suffisamment discret pour pouvoir rester en place plusieurs années sans être détecté. L'administration Obama estimait que cette « cyber-arme » avait retardé d'au moins deux ans les progrès de l'Iran vers un nucléaire militaire.

Pour autant, on ne peut pas exactement parler de « paralysie » et encore moins « d'attaque éclair ».

Plus consensuellement, l'attaque **[WannaCry]** de 2017 est considérée comme le premier vrai Pearl Harbor. Elle a notamment paralysé l'informatique du service de santé britannique, obligeant de nombreux hôpitaux à décaler des opérations et occasionnant des pertes définitives de données.

Notons que plusieurs choses se sont correctement passées.

Les spécialistes ont commencé à avertir du risque d'un tel scénario 17 ans avant WannaCry, à une époque où l'informatique s'engouffrait dans de plus en plus de secteurs.

Des entreprises, positionnées sur les moyens pour s'en prémunir, ont émergé environ 15 ans avant WannaCry.

L'État a commencé à se préparer sérieusement à peu près au même moment (plan **[Piranet]**).

Les médias ont relayé les avertissements des experts environ 10 ans avant WannaCry.

En quelque sorte, il y avait de quoi voir venir.

Face à ce risque, seulement quelques entreprises s'étaient correctement préparées. Des entreprises pensaient être prêtes **[TV5]**. Beaucoup d'entreprises attendaient que ça arrive aux autres pour s'en occuper.

Il ne s'agit pas pour autant de leur jeter la pierre. En effet, dans une gestion rationnelle du risque, si vous me dites qu'un Pearl Harbor se produit tous les 10 ans et que, quand il advient, je perds 10 millions d'euros, je peux lisser le risque en considérant que je subis 1 million de dégâts par an. Toute solution qu'on me propose pour traiter ce risque, et qui coûte moins d'un million par an, est donc intéressante à implémenter.

Mais tant que le premier Pearl Harbor ne s'est pas produit, j'ignore s'il va advenir tous les 10 ans, tous les 20 ans ou tous les 50 ans et combien ça va me coûter. C'est ce que l'on nomme un **[cygne noir]**.

2. À QUOI RESSEMBLE LE MONDE APRÈS PEARL HARBOR ?

Le premier changement significatif est que la plupart des entreprises évaluent désormais leur sécurité (au travers d'audits, d'outils, de personnels dédiés, etc.).

La première mauvaise nouvelle est que les recommandations émises par ces évaluations ne sont majoritairement pas appliquées (et parfois pas applicables). Les sociétés amenées à auditer la sécurité d'un client plusieurs années consécutives peuvent témoigner d'un certain « air de famille » entre les rapports produits.

La faute à des technologies historiques difficiles à remplacer (adhérence logicielle), à l'instabilité des correctifs (il faut d'abord les tester sur un échantillon pour mesurer les effets de bord) et quelques autres facteurs.

Face à ces obstacles, nombre d'entreprises emploient la stratégie du *best effort* : s'occuper uniquement des « blockbusters » qui font l'actualité (Bluekeep, Zerologon...). Bien que peu glorieuse, cette approche donne des résultats significatifs. En effet, dans l'écosystème actuel, corriger 1% des vulnérabilités peut prémunir de 99% des attaques (qui sont automatisées et peu complexes).

Mais 1% des vulnérabilités c'est déjà beaucoup de travail et le 1% des attaques restantes c'est encore un beau volume.

Un autre changement majeur est l'évolution du marketing en cybersécurité de même, d'ailleurs, que le terme cybersécurité. Il y a 15 ans les éditeurs essayaient de vous convaincre qu'avec leur antivirus vous ne risquiez rien. Aujourd'hui, ils essayent de vous convaincre qu'avec leur SIEM vous ne risquez rien (ou avec leur VPN si vous êtes un particulier).

De ce fait, de plus en plus d'entreprises possèdent désormais des capacités de détection, ce qui est positif, mais y investissent exagérément leur budget et leur temps. Or ce sujet n'est qu'une strate de protection (palliative qui plus est) parmi d'autres aussi importantes.

Prenons le cas d'un e-mail contenant une pièce jointe malveillante :

- Il va d'abord rencontrer l'antispam. Parfois, il passera à travers.
- Il arrive sur le poste de l'utilisateur et rencontre l'antivirus. Parfois, il passera à travers.
- Il est maintenant en face de la vigilance de l'utilisateur (le fameux facteur humain). Parfois, il passera à travers.
- Il s'exécute maintenant sur le poste. « Parfois », il profitera d'un manque de mises à jour ou d'un utilisateur ayant des droits d'administrateur, ou bien il utilisera une 0day, et il prendra le contrôle de la machine.
- Il cherche désormais à se répandre dans le réseau. Parfois, la segmentation et l'étanchéité ne seront pas correctement configurées (ou bien il profitera d'une 0day sur un pare-feu ou un commutateur) et il pourra affecter des actifs plus sensibles que celui duquel il part.
- Pendant qu'il fait son œuvre, les sondes et le SIEM mettront un certain temps à le détecter et les analystes mettront aussi un certain temps à confirmer l'attaque. Dans le meilleur des cas, ça prendra quelques minutes, si l'on n'a vraiment rien, ça prendra des mois. Plus il a de temps devant lui, plus le maliciel peut faire de dégâts.
- Une fois qu'il a été détecté et éradiqué, il faut réparer ses dégâts. Si le système de sauvegarde est complet et agile, la restauration ne prendra que quelques heures. Si la sauvegarde n'a pas été bien pensée, ce sera plus douloureux (serveur de sauvegarde lui-même chiffré par un rançongiciel, dossiers locaux non sauvegardés, etc.).

Le principe de la défense en profondeur c'est qu'il est très peu probable que tout se passe mal en même temps. Donc, si l'on a investi raisonnablement dans chaque strate de sécurité, on a de bonnes chances de contrer le maliciel.

En revanche, si l'on a succombé aux sirènes du SIEM et mis tous ses moyens en priorité dessus, on risque de se retrouver avec un tas de cendres à la place du SI et de dire *« oui, mais je sais exactement d'où c'est arrivé, comment c'est arrivé et jusqu'où c'est arrivé »*...

Notons que cette vision globale, des strates de défense en profondeur, est aussi l'occasion de dépasser l'éternel poncif « la plus grosse faille c'est le facteur humain ». Premièrement, toutes les failles sont

humaines (les programmes sont codés par des humains). Deuxièmement, la vigilance des utilisateurs est une strate comme les autres, il n'y a pas de raison de l'accuser de tous les maux quand il y a eu un problème, car ce n'est pas la seule à avoir failli.

Un troisième changement est l'explosion de l'*Infrastructure as a Service* (IaaS) : AWS, Azure et autres qui promettent de vous soulager des tâches de MCO/MCS réseau et système pour ne vous concentrer que sur les applications.

Dans les faits, personne ne migre complètement en *cloud* et donc tout le monde se retrouve à gérer une infrastructure hybride avec plus de couches d'abstraction qu'avant : au lieu d'installer une appli dans une VM, je vais déployer une image Docker avec Kubernetes, installé via Ansible, déployé via Terraform qui est lui-même installé sur une VM.

Qui dit nouvelles couches, dit nouveaux outils et sujets à maîtriser : scanners d'images Docker (qui souvent loupent les paquets en *standalone*), permissions des containers (souvent lancés en root et sans segmentation inter-container), etc.

Le mille-feuille numérique a gagné quelques étages et le nombre d'angles morts a augmenté.

Peut-être n'est-ce que le prix à payer d'un temps de transition vers une informatique unifiée et scalable, peuplée de DevOps. Mais quelques éléments font douter que cette transition soit pour demain.

Premièrement, le Cloud mutualisé s'accouple mal avec la souveraineté des données. Tant qu'aucun vrai modèle Zero Knowledge n'existe **[ZK]**, vous êtes condamnés à devoir accorder une confiance quasi aveugle au fournisseur, quant au fait qu'il n'ira pas fouiller dans vos données.

Deuxièmement, les solutions IaaS ressemblent de plus en plus à des SPOF (*Single Point Of Failure*). Si demain AWS tombe ou se fait hacker, pas mal d'entreprises se retrouveront à l'âge de pierre. Il est vrai qu'Amazon est certainement plus compétent en sécurité que n'importe quelle autre entreprise, dans la mesure où c'est leur cœur de métier de ne pas se faire hacker. Mais ils sont devenus une cible tellement attrayante que ça arrivera forcément un jour.

Les acteurs, qui s'engouffrent actuellement dans le concept à la mode du Zero Trust, où « aucune brique n'accorde une confiance aveugle à une autre », proposent souvent des architectures en cloud mutualisé... pour lesquelles, justement, il faut accorder une confiance aveugle au fournisseur.

Dernier changement que nous mentionnerons : l'aspect légal, normatif et réglementaire a également suivi le pas. Le RGPD a été mis en place. Les grands industriels sont plus regardants avec leurs sous-traitants. L'État produit des référentiels pour le privé et du service pour les acteurs essentiels.

Ceci a aussi produit un nouveau type d'humour avec les prestations du type « Mettez-vous en conformité avec le RGPD ».

Sans avoir à les auditer, je peux vous donner le nombre d'entreprises conformes au RGPD : 0.

Pour l'être il faudrait, a minima, pouvoir répondre à ces trois problématiques :

- Pour une donnée, lister tous les endroits où elle se trouve.
- Pour une donnée, lister toutes les personnes qui y accèdent.
- Pour une personne, lister toutes les données auxquelles elle accède.

Cela semble être le b.a.-ba et pourtant, aujourd'hui, on est à des lieux de pouvoir y répondre avec l'outillage existant (ceux qui ont déjà fait de l'audit de permissions en milieu Windows le savent) dans des frais raisonnables. Les objectifs sont pertinents, mais les ruptures technologiques qui permettraient de les atteindre se font attendre.

Est-ce à dire que rien ne s'est amélioré ? Les anciens problèmes existent toujours... mais en moins grand nombre... mais de nouveaux sont apparus. Toujours est-il que suffisamment d'éléments existent pour que le *nicolasruffisme* (« la sécurité est un échec ») ait de nombreux adeptes.

3. LE PROCHAIN PEARL HARBOR

Ce qui a permis à WannaCry d'advenir n'a donc pas disparu. Quand le prochain événement de ce type se produira-t-il ? En toute vraisemblance, la fréquence va augmenter (donc un prochain avant 2030).

D'une part, l'informatique continue de gérer de plus en plus d'aspects de notre vie (villes connectées, santé, prises de décisions...).

D'autre part, on découvre de nouvelles vulnérabilités plus vite qu'on ne les corrige.

Ce qui nous amène au point principal de cet article : contrairement à ce que le grand public semble croire, l'absence actuelle de catastrophe numérique tient moins au bon niveau de sécurité de nos infrastructures qu'à une question d'alignement des planètes.

Il y a des acteurs qui ont les compétences, les moyens et l'occasion pour en provoquer une, mais pas l'intention (les États-Unis par exemple).

Il y a des acteurs qui ont les moyens, l'occasion et la volonté d'en provoquer une, mais pas les compétences (certaines organisations terroristes par exemple).

Il y a des acteurs qui ont les compétences, les moyens et la volonté d'en provoquer une, mais pas l'occasion (des hacktivistes par exemple).

Dès demain, on pourrait imaginer que les États-Unis bloquent tous les postes Windows de la Chine pour faire pression dans un conflit diplomatique (évidemment c'est le genre de moyen de pression qu'on n'utilise qu'une seule fois puisqu'après ça Microsoft n'est plus près de vendre des machines en Chine).

Dès demain, on pourrait imaginer qu'une organisation terroriste recrute un type calé en informatique industrielle, qui dérègle une centrale nucléaire, qui ouvre un barrage ou qui, par exemple, pousse quelques satellites à se rentrer dedans, jusqu'à provoquer une réaction en chaîne qui annihile tout ce qui orbite autour de la Terre (*cf.* Gravity).

Dès demain, on pourrait imaginer un groupe d'hacktivistes qui arrive à se faire embaucher dans une banque « systémique » et qui profite de cet accès privilégié aux réseaux sensibles pour provoquer une crise financière mondiale (*cf.* Mr ROBOT).

Si rien d'important n'a craqué jusqu'ici, c'est en bonne partie, car ceux qui pourraient mettre à genoux les éléments cruciaux ne sont pas ceux motivés pour le faire.

Symétriquement, certains éléments cruciaux sont peu protégés, en bonne partie, car personne ne les a encore attaqués. *Je ne donnerai pas d'exemple ici afin de ne pas inspirer quelque mauvais bougre.*

Or, comme les connaissances se propagent de plus en plus vite, il n'est pas raisonnable de parier sur l'immuabilité de cette situation.

Voilà pour la fréquence. Qu'en est-il de la sévérité ?

Vu que tout est de plus en plus interconnecté, ne risque-t-on pas de passer d'événements de type « Pearl Harbor » à une sorte d'« Armageddon numérique » : une attaque paralysant le monde entier ?

La réponse est incertaine (décidément). Les interconnexions de plus en plus nombreuses, et l'immixtion de l'informatique dans toujours plus de domaines, étendent le nombre de portes d'entrée et l'étendue de ce qui sera affecté.

Mais d'un autre côté, l'hétérogénéité des technologies, et la complexification du monde numérique, multiplient les compétences que devrait avoir un adversaire pour avoir un impact généralisé. Le CV qu'il faudrait pour tout faire tomber, de la banque à la ville connectée, provoquerait des afflux sanguins titanesques chez nos recruteurs LinkedIn. Le résultat est donc que les attaques d'envergure mobilisent de plus en plus des équipes plutôt que des loups solitaires.

Même si un retour complet à l'âge de pierre semble donc improbable, il n'en demeure pas moins que l'on peut mettre un pays à genoux en ne ciblant qu'un seul élément de son infrastructure. Imaginez Paris, un seul jour, sans électricité ou sans métro ou avec des feux rouges désynchronisés ou, pire, avec des caisses qui refusent les transactions tant que le client n'a pas dit bonjour... ce serait l'anomie.

Or chacun de ces points névralgiques est à la fois assez gros pour ne pas être exempt de vulnérabilités et assez homogène pour qu'un seul homme ait les compétences nécessaires à le saborder.

4. FACE À CELA QUE FAIRE ?

Miser uniquement sur la robustesse (entendez : empêcher les adversaires de pénétrer nos réseaux) est actuellement illusoire pour les raisons que nous avons développées. Il faut privilégier la résilience (être capable de récupérer rapidement).

Toute entreprise mature possède un Plan de Continuité d'Activité (PCA) et un Plan de Reprise d'Activité (PRA) qui sont des protocoles à dérouler pour supporter un sinistre informatique puis retourner à une situation nominale.

L'avantage d'un PCA/PRA est que la démarche pour le mettre en œuvre nécessite de passer par des étapes comme la cartographie des actifs (et de leur criticité), des menaces, des risques, etc. Autant de choses qui sont utiles pour bien d'autres champs de la sécurité (préventifs et palliatifs).

Si vous n'avez pas de PCA/PRA, mettez-en un en place. Si vous en avez un, testez-le de temps en temps et évitez qu'il ne s'appuie sur des ressources potentiellement indisponibles si l'événement est national, voire mondial (produits d'importation, lignes téléphoniques, etc.).

Comment faire maintenant pour diminuer la survenance des Pearl Harbor numériques ? Demander aux utilisateurs de changer leur mot de passe tous les 6 mois ne vous sauvera pas (passer de Yolo2k18! à Yolo2k19! ou de Welcome03 à Welcome04 n'est pas « game changing »). La problématique ne se résume pas à quelques rustines piochées dans la rubrique informatique de la matinale de votre radio préférée, il s'agit plutôt de voir comment se dépatouiller avec un colosse aux pieds d'argile.

C'est une vaste question qui n'a pas encore de réponse consensuelle parmi les experts. Nous nous contenterons de cinq pistes de réflexion.

4.1 Renoncer à avoir des chaussettes connectées

On entend partout parler de « l'explosion de l'IoT », mais il semble qu'il y ait une part d'astroturfing **[2]** là-dedans. La plupart des gens conçoivent, heureusement, qu'« innovation » n'est pas exactement le bon terme pour qualifier une bouilloire connectée.

Bien que ce discours puisse paraître trop « boomer », anti innovation et autres, limiter ce qui est connecté limitera ce qui sera affecté en cas d'attaque grave. Donc il serait sage de ne pas absolument tout connecter juste, car « on peut le faire ».

De plus, l'IoT peut ressembler à une régression lorsqu'il s'applique à certains sujets. Prenons une serrure connectée. Qu'est-ce qui arrive le plus souvent : perdre des clés physiques ou se retrouver à cours de batterie sur votre portable (qui sert de clé) ? Quiconque sait crocheter une serrure physique devra quand même y passer un certain temps quand il sera en face de la vôtre. Mais quiconque sait pirater une serrure connectée donnée pourra automatiser l'attaque et revendre un outil permettant de l'ouvrir instantanément.

L'actualité a montré un exemple saisissant de cette limite du raisonnable avec des portes connectées inutilisables lors d'une panne AWS **[Panne]**.

4.2 Mettre un peu de « biodiversité » dans le numérique

Lorsqu'un acteur a le monopole d'un segment technologique, chaque fois qu'une vulnérabilité critique affecte son produit, c'est le monde entier qui est sur la sellette.

Si chaque pays essayait de développer au moins un acteur dans chaque grand domaine (matériel, système, réseau, hébergement), cela diminuerait la possibilité, pour une seule vulnérabilité, d'avoir un impact planétaire.

L'idée n'est pas tellement d'aboutir à ce que chaque entreprise d'un pays utilise l'OS souverain, le constructeur de PC souverain, l'hébergeur souverain, etc. Ni même de pousser les entreprises à complexifier leur SI avec de multiples constructeurs. Mais qu'au moins on évite qu'il n'y ait qu'un seul constructeur sur étagère. Ces positions de quasi-monopole sont délétères pour la sécurité (avec des entreprises qui émettent des standards non sécurisés, non documentés et que, parfois, elles ne suivent pas elles-mêmes).

De cette manière, connaître sur le bout des doigts le fonctionnement d'un routeur Pisco ou d'un OS Doors, et y trouver une vulnérabilité, ne serait plus suffisant pour attaquer 99,99 % des entreprises.

4.3 Réinvestir du budget en cartographie informatique

On ne maîtrise pas ce qu'on ne connaît pas. Une entreprise qui n'a pas de moyen d'inventaire performant s'expose à des attaques depuis cet angle mort **[Shadow IT]**.

La plupart des entreprises ont souvent des moyens minimaux en termes de cartographie. La vraie difficulté pour un outil d'inventaire est triple :

- qu'il soit unique et centralisé ;
- qu'il soit à jour ;
- qu'il soit exhaustif.

Or il semble que ce soit une sorte de triangle d'incompatibilité. Mettez en place un outil assez riche pour que toutes les infos, utiles au service achat comme au service réseau, s'y trouvent et probablement que ce sera un enfer à maintenir à jour. Faites un outil qui se met à jour semi-automatiquement et vous aurez des données incomplètes, etc.

Mais il faut essayer quand même.

L'idée générale serait qu'en quelques minutes (deux ou trois requêtes sur l'outil) vous puissiez sortir une liste lorsque quelqu'un vous demande :

- Est-ce que des machines chez nous utilisent le programme X ?
- Quels sont les utilisateurs de l'application Y ?
- Est-ce qu'on a des routeurs Z dans notre parc et où sont-ils ?

4.4 Sécuriser « by design »

Arrêter l'hémorragie en limitant la commercialisation d'outils informatiques dont la sécurité n'a pas été auditée, tout comme on ne commercialise pas de voiture qui n'a pas passé les contrôles de sécurité.

Au moins pour les produits et logiciels payants, ce devrait être incontournable. Aujourd'hui, on paye parfois des fortunes pour des outils qui, indirectement, nous font perdre d'autres fortunes, car ils sont truffés de vulnérabilités.

Sans parler des cordonniers mal chaussés que sont les produits de sécurité (antivirus et autres) : quand ils sont eux-mêmes des sources de vulnérabilités **[F5]** alors qu'ils sont censés nous en prémunir...

Cette idée peut paraître rebutante, car elle semble aller à l'encontre de certains aspects positifs, comme les logiciels gratuits ou le fait que n'importe qui puisse créer une application depuis sa chambre, avec trois bouts de ficelle, et toucher des millions d'individus.

Mais gardons à l'esprit qu'il faudra déjà de nombreuses années pour éliminer les vulnérabilités dans nos réseaux, or, si on en rajoute chaque année plus qu'on en corrige...

4.5 Rendre la sécurité « simple »

Favoriser des architectures informatiques où les opérations importantes sont simples.

Combien de vulnérabilités existent dans nos réseaux, car « l'application du patch a été testée sur

60 machines, mais ça a fait bugger 15 d'entre elles, du coup on attend pour l'appliquer aux 2000 postes du parc », ou encore « on ne met pas à jour l'Active Directory, car l'application X ne marche qu'avec la version 2003 et le fournisseur n'a pas produit de version plus récente ».

Alors, oui, c'est mal fait et les fournisseurs pourraient quand même se débrouiller pour que leurs produits puissent être utilisés dans la durée sans créer plus de problèmes qu'ils n'en solutionnent. Mais un peu d'autocritique ne fait pas de mal non plus. « Dieu se rit de ceux qui déplorent les conséquences dont ils chérissent les causes », ou comme le disait Coluche « quand on pense qu'il suffirait que les gens n'achètent pas pour que ça ne se vende pas ».

Cela fait 10 ans que le problème de « l'adhérence logicielle » est clairement identifié et subi par toutes les entreprises. Peut-être faudrait-il penser à arrêter d'acheter des produits qui ne sont pas maintenables, même s'ils sont dans le Gartner. Peut-être faudrait-il que tous les cahiers des charges incluent des exigences sur le maintien en conditions de sécurité (MCS).

Ces dernières années, les paradigmes se multiplient et certains proposent des améliorations sensibles de ce point de vue.

Les applications web (internes ou en SaaS) permettent de n'avoir qu'une seule machine à mettre à jour, plutôt que de passer sur chaque poste. Les infrastructures avec clients légers mutualisent aussi l'effort de patch.

Enfin, garder en tête que la solution à un problème n'est pas toujours de rajouter un outil. À force d'empiler les couches d'outillage, on perd en productivité, en visibilité et en maintenabilité.

Les SI profiteraient d'avoir des campagnes, une fois tous les 3 ans par exemple, où l'on ne fasse aucun nouvel achat et où, à la place, on fasse la chasse à tout ce qui est inutile, superflu ou qui produit plus de problèmes qu'il n'en résout. En quelque sorte : « dégagez les oreilles et la nuque » afin d'éclaircir la visibilité sur le SI, de récupérer du budget pour des choses plus utiles, etc.

« La perfection est atteinte, non pas lorsqu'il n'y a plus rien à ajouter, mais lorsqu'il n'y a plus rien à retirer. » (Saint-Exupéry)

CONCLUSION

Toute prospective est par essence périlleuse. Peut-être ai-je raison. Ou peut-être qu'en 2030 la blockchain et l'ordinateur quantique nous auront sauvés de tous ces périls. La vérité est probablement entre ces deux extrêmes... (en fait non, j'ai juste raison, mais c'est pas classe comme conclusion). ■

RÉFÉRENCES

[1] https://bdc.aege.fr/public/L_ennemi_a_l_ere_numerique.pdf

[Stuxnet] https://fr.wikipedia.org/wiki/Stuxnet

[Wannacry] https://www.lemonde.fr/pixels/article/2017/05/13/ce-que-l-on-sait-du-logiciel-de-racket-qui-a-paralyse-les-hopitaux-britanniques-et-touche-des-dizaines-de-pays_5127351_4408996.html

[Piranet] https://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/

[TV5] https://www.20minutes.fr/medias/1582579-20150409-piratage-tv5monde-chaine-repris-diffusion-jeudi-fin-journee-plainte-deposee

[cygne noir] https://fr.wikipedia.org/wiki/Th%C3%A9orie_du_cygne_noir

[ZK] https://security.stackexchange.com/questions/238441/solution-to-the-browser-crypto-chicken-and-egg-problem?noredirect=1&lq=1

[Panne] https://www.01net.com/actualites/un-probleme-technique-d-amazon-web-services-fait-tomber-de-nombreux-sites-americains-2010637.html

[2] https://fr.wikipedia.org/wiki/Astroturfing

[Shadow IT] https://fr.wikipedia.org/wiki/Shadow_IT

[F5] https://www.cert.ssi.gouv.fr/alerte/CERTFR-2020-ALE-015/

La synthèse des recommandations

Les différentes recommandations recensées dans ce document sont reprises en synthèse ci-dessous et réparties en quatre grands thèmes : gouvernance, moyens, résilience et relations avec des tiers.

GOUVERNANCE

Recommandations	
1	Prévoir un dispositif financier d'accompagnement pour une gouvernance partagée entre les communes et les intercommunalités.
2	Promouvoir la mutualisation, afin que les plus petites communes puissent s'appuyer sur l'expertise et les moyens financiers des structures plus importantes. Des économies substantielles pourront être réalisées grâce à l'émergence de groupements d'achats.
6	Inciter les communes et les intercommunalités à entreprendre une réflexion sur le développement et le renforcement de la sécurité numérique.
7	Mutualiser les services de sécurité numérique à travers le mécanisme de « service commun » entre les intercommunalités et leurs communes membres ou le recours à un syndicat mixte « numérique » déjà existant entre plusieurs collectivités.
8	Motiver les décideurs à prendre les mesures de gouvernance.
9	Transmettre la prise de conscience du risque numérique et porter cette responsabilité au plus haut niveau de l'organisation.
10	Organiser une gouvernance adaptée au contexte local, par exemple un comité simple composé d'élus et de techniciens, voire des formes d'organisation plus élaborées (comité technique, commission, élu référent).
11	Porter la démarche au plus haut niveau de la commune ou de l'intercommunalité et en assurer le pilotage sur le long terme.

MOYENS

Recommandations	
3	À l'inverse des pratiques majoritaires actuelles, il serait préférable d'évaluer d'abord les exigences en matière de sécurité numérique pour pouvoir ensuite dimensionner le budget à allouer.
4	Opérer les choix stratégiques et budgétaires issus des réflexions associant les élus et les techniciens.
5	Insister auprès du préfet pour obtenir des financements dédiés.
12	Miser sur l'humain et accompagner les communes et les intercommunalités à sensibiliser leurs agents aux bonnes pratiques.
13	Prioriser un accompagnement des agents qui produisent, traitent et exploitent des données sensibles. Un bon moyen d'acculturer les personnels peut être de s'appuyer sur le règlement général de la protection des données (RGPD) et les nouvelles pratiques induites.
14	S'appuyer sur le guide « Maîtrise du risque numérique – L'atout confiance » sur le site de l'ANSSI afin d'évaluer, organiser, bâtir et piloter un socle complet de sécurité.
19	Un travail préalable de cartographie des données et des flux, de classification des données et d'analyse des risques devra avoir été réalisé en amont de la souscription d'une offre d'informatique en nuage (cloud).
20	Ne souscrire, si possible, qu'à des offres d'informatique en nuage auprès de prestataires de confiance et notamment ceux disposant d'un Visa de sécurité de l'ANSSI . Dans le cadre de cette démarche, l'ANSSI a élaboré le référentiel SecNumCloud en vue de permettre la qualification de prestataires de services d'informatique en nuage. Sont concernés les prestataires d'informatique en nuage offrant des services de type SaaS (Software as a service), PaaS (Platform as a service) et IaaS (Infrastructure as a service).

RÉSILIENCE

Recommandations	
21	Rédiger le volet numérique du plan de crise de la commune ou de l'intercommunalité en s'appuyant sur les dispositifs existants (exemple : plan communal de sauvegarde (PCS)). L'intégrer au plan communal de sauvegarde de la commune et/ou à un Centre de ressources numériques territorial (CRNT).
22	Élaborer des éléments de langage liés à des scénarios de cyberattaque avant que la crise ne survienne. Intégrer ces éléments de langage au plan de communication de crise.
23	Faire un exercice de gestion de crise avec un scénario de cyberattaque.
24	Développer un scénario de cyberattaque dans le plan de continuité d'activité (PCA)/ plan de reprise d'activité (PRA) de la collectivité (privilégier le scénario d'attaque par rançongiciel *).
25	Maintenir le PCA/PRA à un niveau opérationnel via l'organisation régulière d'exercices.
26	Mettre en place, former et animer un réseau de référents locaux en matière de sécurité numérique.
27	Fournir son plan de crise à ses fournisseurs afin qu'ils l'appliquent (chaîne de réponse).
28	Désigner un responsable qui sera chargé de diffuser les informations tant en interne qu'à l'extérieur de la collectivité.
29	Tenir « une main courante » durant la crise afin de faciliter la formalisation du retour d'expérience.
30	Accompagner les agents en cas de cyberattaque pour améliorer la résilience collective.

RELATIONS AVEC DES TIERS

Recommandations	
15	Formaliser les exigences de sécurité puis vérifier l'adéquation des mesures proposées par les prestataires notamment à travers un « plan d'assurance sécurité » (cf. guide de l'ANSSI « Maîtriser les risques de l'infogérance »).
16	Inclure systématiquement un chapitre contractuel sur la sécurité numérique pour les prestations, qu'elles soient ou non informatiques.
17	Inclure dans les cahiers des charges des conventions de délégation de service public, des clauses explicites et express préci-sant la répartition des responsabilités et des obligations entre le délégant et le délégataire.
18	Inclure systématiquement la clause de réversibilité dans les documents contractuels liant la commune ou l'intercommuna-lité au prestataire/partenaire privé. Faire préciser aux prestataires les moyens qu'ils mettront en œuvre pour assurer cette réversibilité.

1. Quels sont les menaces et les points de vulnérabilité dans les communes et les intercommunalités ?

Les communes et les intercommunalités, quelle que soit leur taille, peuvent être la cible d'attaques informatiques. Ces cyberattaques peuvent être d'origine externe (site internet, téléphone mobile, cybercriminels…) ou interne (élus, agents, prestataires, clés USB, mots de passe faibles…) et utiliser des vulnérabilités techniques, juridiques, organisationnelles ou humaines.

1. Les menaces : tendance et typologie des incidents numériques

Le panorama qui suit n'est pas une représentation ex-haustive de la réalité des évènements cyber affectant les communes et les intercommunalités. Ce tableau est dressé sur la base des faits portés à la connais-sance de l'ANSSI. Ainsi, la vision qui en résulte n'en est que partielle et repose sur le besoin d'aide expri-mé par les bénéficiaires et leur volonté de signaler ces évènements à l'ANSSI.

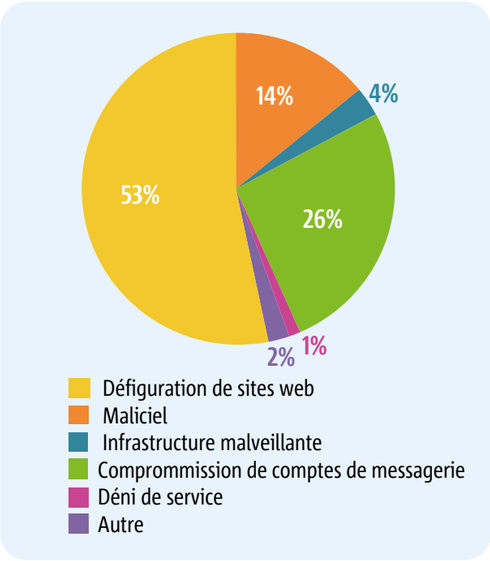
Le périmètre retenu pour cette étude comprend tous les incidents de sécurité d'origine cyber affectant les communes, les communautés de communes, d'ag-glomération, urbaines ainsi que les métropoles fran-çaises traités par l'ANSSI tout au long de l'année 2019.

Les incidents correspondent aux signalements rele-vant d'une compromission* avérée de l'entité victime ou d'une attaque réussie. Dans le cas de compromis-sions dont la gravité et l'impact requièrent un enga-gement renforcé de l'agence, les incidents peuvent alors évoluer en incident majeur voire en opération de cyberdéfense.

A - Panorama de la situation cyber

Au cours de l'année 2019, l'ANSSI a recensé et traité 92 incidents de sécurité d'origine cyber af-fectant les communes et les intercommunalités, soit près de 25% des incidents totaux traités par l'agence sur cette période. Cette proportion consé-quente reste toutefois à nuancer au regard de la gravité relative des compromissions détectées sur le système d'information des entités concernées. Ces dernières n'ont pas fait l'objet en 2019, ni même les années précédentes, d'incident majeur ou d'opération de cyberdéfense.

Comme représenté ci-après, on dénombre trois grandes catégories de compromission affectant les systèmes d'information des collectivités, objet de cette étude :



Si les deux premières catégories, malgré leur nombre, relèvent de compromissions d'impact et de gravité mineures, la troisième, quant à elle, couve une réalité non négligeable et aux impacts forts pour ces entités. En effet, sur 12 cas de com-promission de système d'information avec dépôt de code malveillant, 9 d'entre eux sont relatifs à des rançongiciels* paralysant tout ou partie du parc informatique infecté.

Du fait d'une maturité à la sécurité numérique encore à développer, les communes et intercom-munalités sont des cibles accessibles aux yeux d'acteurs malveillants pour qui l'attaque par ran-çongiciel est devenue une source de revenu effi-cace. Cette tendance s'inscrit dans une tendance globale qui a vu le nombre d'attaques par rançon-giciel augmenter de manière drastique au cours de l'année 2019.

Panorama détaillé : la défiguration* de sites internet

La majorité (88%) des défigurations de sites Inter-net de communes et intercommunalités françaises est portée à la connaissance de l'ANSSI via le site ZONE-H qui recense et archive les défigurations de pages web en tout genre depuis 2002. À no-ter que les auteurs de défigurations sont parfois eux-mêmes susceptibles d'y soumettre ce qu'ils voient comme leurs « exploits ». Pour le restant, les signalements proviennent de particuliers, de partenaires nationaux mais rarement des victimes elles-mêmes concernées.

Lorsqu'une défiguration est portée à la connais-sance de l'ANSSI, cette dernière constate la véra-cité des faits et, le cas échéant, transmet le signa-lement à l'entité concernée pour prise d'action. Dans la majeure partie des cas, l'incident est clos dans les jours qui suivent. Ainsi, le vecteur initial de compromission n'est généralement pas connu de l'ANSSI.

Panorama détaillé : la compromission de comptes de messagerie

Sur les 24 cas de compromission de comptes de messagerie signalés à l'ANSSI, 17 proviennent d'une même intercommunalité. L'actualité de cette dernière, quasi exhaustivement portée à la connaissance de l'agence, est loin d'être un lieu d'exception cyber et permet donc, par extension, d'entrevoir les problématiques opérationnelles rencontrées par les autres entités du périmètre. Les incidents ne sont, en effet, pas systématique-ment détectés ni remontés à l'ANSSI.

La prise de conscience récente des enjeux liés à l'hygiène informatique et le développement nou-veau de la culture de la sécurité numérique des personnels des communes et des intercommuna-lités laissent encore ces dernières être des cibles privilégiées et faciles d'accès pour la distribution d'hameçonnage à des fins cybercriminelles. À titre d'exemple, il est courant que des couples d'identi-fiants et mots de passe de comptes de messagerie des personnels des communes et intercommunali-tés se retrouvent dans des divulgations, facilitant ainsi leur compromission ultérieure.

Panorama détaillé : la compromission avec attaque de maliciels*

C'est sans nul doute la catégorie d'incidents dans laquelle se situent les attaques ayant eu l'impact le plus marquant pour le périmètre étudié. Outre les cas de dépôt opportuniste de codes malveillants, notamment à des fins de cryptominage*, neuf cas sur douze ont trait à une attaque par rançongiciel. Si, pour l'une de ces attaques seulement, le péri-mètre de compromission s'est restreint à un seul poste utilisateur, les autres ont affecté fortement le fonctionnement du système d'information infec-té allant, parfois, jusqu'à sa nécessaire reconstruc-tion complète. L'impact opérationnel et le coût as-socié de ces attaques sont autant d'arguments qui doivent amener les communes et les intercommu-nalités à se saisir du sujet et renforcer leur sécurité informatique.

Fait intéressant, sur ces huit incidents notables, quatre ont été portés à la connaissance de l'ANSSI par voie de presse. Une fois le contact pris, une assistance a donc pu leur être proposée.

Panorama détaillé : autres types d'incidents

D'autres incidents mineurs, de par leur nombre et leur gravité, ont affecté des communes françaises. On dénombre, ainsi, un cas d'attaque par déni de service* et plusieurs cas de compromission de ser-veurs pour héberger des activités malveillantes comme des pages d'hameçonnage*.

B - Exemples d'incidents notables

Exemple 1 : site internet d'une commune aspiré par un nom de domaine en .tk

En août 2017, le responsable de la sécurité infor-matique d'une mairie informe l'ANSSI d'un inci-dent concernant le site Internet de sa commune. En effet, le contenu du site Internet a été aspiré et publié sous un autre nom de domaine en .tk. Ce faisant, les attaquants auraient modifié les pages du site cloné et ajouté du contenu porno-graphique. De plus, des résultats de recherche liés au site Internet de cette commune pointent vers le site malveillant.

Face à cette situation préoccupante, le responsable contacte l'hébergeur du site et obtient le déréfé-rencement du site malveillant en 24 heures par les moteurs de recherche. Il porte également plainte auprès des services de police. La réaction prompte du responsable aura permis de faire cesser cette atteinte à l'image dans de brefs délais.

Exemple 2 : présence d'un mineur de cryptomonnaie sur le site internet d'une commune

En janvier 2018, un agent de l'ANSSI effectue un signalement avisant de la présence d'un crypto-mineur* sur une page du site Internet d'une com-mune. Ce signalement provient du résultat d'un moteur de recherche spécialisé (publicwww) qui indexe le code source des sites Internet. Bien que ce cryptomineur soit disponible en source libre et que son utilisation puisse être légitime, il peut être surprenant d'en faire la découverte sur un site « institutionnel ». L'ANSSI transmet ce signalement à la commune qui fait le nécessaire pour le supprimer.

Exemple 3 : une attaque par rançongiciel sur le site d'une commune

En juillet 2019, une commune fait part à l'ANSSI de la compromission de son système d'information par un rançongiciel. Les fonctions critiques de la mairie ne sont plus fonctionnelles durant l'incident. Il apparaît que les sauvegardes sont compromises et que leur réinstallation réactive un processus

de chiffrement des données les rendant inexploi-tables. Cet incident nécessitera une réinstallation complète des machines virtuelles de la commune.

Après analyse, il semble que le système d'informa-tion était fragilisé par une politique de mots de passe faibles et une prolifération de comptes avec des privilèges administrateurs non connus des ser-vices de la mairie, ce qui a facilité l'attaque via un des comptes administrateur.

Lien vers le guide *Attaques par rançongiciels, tous concernés :* https://www.ssi.gouv.fr/guide/attaques-par-rancongiciels-tous-concernes-comment-les-anticiper-et-reagir-en-cas-dincident/

Exemple 4 : typosquattage de noms de domaine d'une métropole

En novembre 2019, les services informatiques d'une métropole informent l'ANSSI de la réservation de plusieurs noms de domaine usurpant son identité. Après des investigations, il s'avère qu'une entre-prise étrangère a réservé ces noms de domaine, sans les rendre actifs, prétextant une utilisation professionnelle. L'ANSSI émet des recommanda-tions à l'attention de la métropole suggérant un rapprochement avec l'AFNIC (organisme qui gère les noms de domaine). Une surveillance accrue des noms de domaine similaire est également conseillée.

En effet, la réservation de noms de domaine proches sémantiquement du nom officiel d'une organi-sation (typosquattage) peut entraîner différents risques pour cette dernière. Ces noms peuvent être utilisés pour envoyer des courriels d'hameçonnage. Profitant de la confiance que peuvent suggérer ces adresses, la propagation de maliciels ou la récupé-ration de données d'identification ou de données personnelles peuvent s'en trouver facilitées, autant envers les agents de la métropole qu'envers les ci-toyens.

Exemple 5 : exploitation d'une vulnérabilité informa-tique rendue publique

En décembre 2019, un avis de vulnérabilité (exécu-tion de codes arbitraires à distance) concernant les applicatifs CITRIX a été publié par l'éditeur. En janvier 2020, une métropole et un département font part à l'ANSSI de la compromission d'équipe-ment CITRIX de leurs systèmes d'information res-pectifs.

Concernant plus particulièrement la métropole, qui n'avait pas appliqué la solution de contournement proposée par l'éditeur, il a été constaté des modi-fications dans les tâches planifiées sur son serveur CITRIX ainsi que des connexions sortantes vers un serveur en Russie.

Suite à des échanges avec l'ANSSI, la métropole a pris diverses mesures de remédiation, en appliquant notamment le correctif proposé fin janvier par l'édi-teur et en changeant les identifiants du serveur.

Exemple 6 : compromission par un cheval de Troie (type de logiciel malveillant)

En février 2020, une communauté d'agglomération fait part de la compromission d'un poste de travail par le cheval de Troie EMOTET suite à l'ouverture d'une pièce jointe au contenu malveillant.

La communauté d'agglomération a notamment constaté des modifications de fichiers PDF et JSE sur un serveur distant. Deux postes de travail au-raient également été compromis par l'ouverture de ces fichiers modifiés par l'attaquant.

Le cheval de Troie EMOTET, initialement utilisé pour dérober des identifiants bancaires, sert éga-lement aujourd'hui de première étape d'infection pour nombre de maliciels, parmi lesquels des ran-çongiciels.

2. Les points de vigilance

Les sites Internet ne doivent pas être l'unique point d'attention, les vulnérabilités sont multiples. Une attention particulière doit notamment être portée sur le wifi public, les capteurs, l'hébergement des données... *(cf. - Quelques bonnes pratiques pour pré-venir le risque de malveillance numérique - page 24)*

Sites Internet

- Les sites Internet des collectivités devraient disposer d'une gestion des mots de passe conforme aux bonnes pratiques (mots de passe de qualité).
- Le socle technique *(système d'exploitation)* des serveurs sur lesquels reposent les sites internet devraient être régulièrement mis à jour.
- Les logiciels de gestion de contenu *(CMS)* sur lesquels reposent les sites internet devraient être régulièrement mis à jour.

Wifi

- Les mots de passe wifi devraient être régulièrement changés.
- Le cloisonnement entre utilisateurs visiteurs et internes devrait toujours être mis en place.
- Les connexions devraient être opérées via un portail captif*.

Capteurs

- Les données de capteurs devraient être envoyées dans une offre d'information « nuagique » euro-péenne.

Cloud

- Les modalités de réversibilité *(récupération des données)* devraient être définies avant la signa-ture du contrat.

Mobiles

- Les équipements mobiles *(tablettes ou ordiphones)* devraient disposer d'un antivirus, si possible administré pour vérifier ses mises à jour.
- Les équipements mobiles devraient être administrés afin de disposer d'un verrouillage/effacement automatique en cas de vol.

Messageries

- Les messageries devraient systématiquement utiliser les versions chiffrées des protocoles d'en-voi et de réception.
- Les comptes de messagerie et les adresses de courrier éléctronique des élus et agents quittant la collectivité devraient être supprimés sans délai après leur départ.

Serveurs et postes de travail

- Les sauvegardes et les mises à jours applicatives sont indispensables.

FOCUS

Usages personnels et professionnels

Les usages et les mesures de sécurité sont différents sur les équipements de communi-cation (ordinateur, ordiphone, etc.) person-nels et professionnels. Très répandues, les pratiques qui mélangent les deux sphères posent des problèmes en matière de sécurité des données : vol ou perte des appareils, in-trusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur.

Dans ce contexte, il est recommandé de séparer les usages personnels des usages professionnels, à savoir :

- **ne pas faire pas suivre les messages élec-troniques professionnels sur des services de messagerie utilisés à des fins personnelles ;**
- **ne pas héberger de données profession-nelles sur les équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne ;**
- **de la même façon, éviter de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de la commune ou de l'intercommunalité.**

Si ces bonnes pratiques ne sont pas appli-quées, il y a le risque que des personnes mal-veillantes volent des informations sensibles de la commune ou de l'intercommunalité, après avoir réussi à prendre le contrôle de la machine personnelle.

https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf

MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Copie ayant obtenu la meilleure note

Cas pratique

L'administration n'a volontairement pas corrigé les imperfections de fond et de forme dans les copies communiquées ci-après.

RÉPUBLIQUE FRANÇAISE
DIRECTION GÉNÉRALE DE LA SÉCURITÉ EXTÉRIEURE
DGSE

Année : 2021

Concours : Externe Contrôleur Spécialisé de classe normale

Épreuve : Cas pratique

Consignes :

- *Ne pas signer la composition et ne pas y apporter de signe distinctif*
- *Numéroter chaque page; placer l'ensemble dans l'ordre et le bon sens*
- *N'effectuer aucun collage ou découpage de sujets ou de feuilles*
- *Ne joindre aucun brouillon*

Une commune connectée et à la pointe de la technologie n'est pas à l'abris de cyberattaques. En effet suite aux attaques informatiques rencontrées par les hôpitaux franciliens en 2020, la mairie de Paris souhaite répondre aux interrogations portées sur les menaces et les risques en cas de compromission.

Les principaux enjeux de la commune face à la menace cyber :
L'idéal serait que chaques communes soit totalement numériques, qu'elles puissent offrir leurs services et poursuivre leurs activités à distance tout en garantissant un environnement sécurisé et d'actualité à l'ensemble de ses utilisateurs. Au jour d'aujourd'hui les avancées technologiques ne permettent pas encore de garantir une sécurité optimale du parc informatique mais nous pouvons identifier les principaux enjeux de la cyber-sécurité.
Un des facteurs principaux est la dépendance de l'Europe aux outils informatiques américains. Bien que des politiques de sécurité soit mise en place par les entités américaines, la France et l'Europe n'est pas maître de la garantie de la protection des données. Ainsi, afin de garantir la souveraineté numérique nationale et européenne, la France et l'Europe doivent faire de la ~~base industrielle, la compétitivité des entreprises~~, garantie de résilience de nos infrastructures, de la confiance aux entreprises nationales technologiques, de la souveraineté numérique au coeur de l'action publique et de la place du citoyen au coeur des politiques numériques, une priorité.
En garantissant la sécurité de nos réseaux et en renforçant les contrôles de l'ARCEP cela permettra de maintenir une exigeance maximale de sécurité, de faire face à l'accroissement de la menace cyber et

ainsi de justifier et d'assumer le coût financiers de notre souveraineté numérique.
En mettant en place un environnement sécurisé nous pouvons ainsi encourager nos entreprises technologiques à se développer, les soutenir et ainsi encourager les projets européens de "reconquête" numérique.
Ceci avec le soutient de l'Etat sera aussi bénéfique pour les ~~cy~~ citoyens que les services administratifs qui pourront continuer à proposer leurs services en ligne en toute sécurité.

Les menaces recensées qui peuvent affecter la commune :
Il est plus simple de justifier une telle exigence de niveau de sécurité en effectuant un inventaire des menaces répertoriées.
Trois grands groupes de menace se distinguent :

- La défiguration de site-web, ~~bien que~~ malgré leur nombres, leur degré d'impact et de gravité reste mineure. Nous rencontrons des exemples tels que des contenus de site internet dupliqué ou avec du contenu inapproprié. ~~Bien que déplacé~~, le contenu du site web peut être restauré et publié sur un nom de domaine approprié.
- La compromission de comptes de messagerie laissant place au hameçonnage à des fins cybercriminelles.
- La compromission avec attaque de maliciels, l'impact opérationnel et le coût associé à ces attaques sont bien trop importante pour ne pas inciter les communes à renforcer leur sécurité informatique. Sachant que les rançongiciels paralysent tout ou une partie du parc informatique, obligeant la réinstallation complète du système.

Beaucoup d'autres menaces sont recensées mais restent pour l'heure moins répandues, tel que le typosquattage, déni de service, compromission par un cheval de Troie, exploitation d'une vulnérabilité informatique rendue publique.

Afin de pallier à ces menaces, quelques préconisations sont adressées aux agents et prestataires de la Mairie.
Les préconisations contre les cyberattaques :

- Un point primordial, la différence entre l'usage à des fins personnelles et à des fins professionnelles. Il est importants de limiter voire d'interdire l'utilisation des appareils par les collaborateurs pour un usage personnel (héberger des données professionnelles sur du matériel personnel, faire suivre des messages electroniques professionnels vers une messagerie

personnelle.

- les sites internet doivent disposer d'une gestion de mot de passe de qualités
- les systèmes d'exploitation et les logiciels de gestion de contenu doivent être régulièrement mis à jour.
- Un plan de continuité d'Activité (PCA) et un Plan de Reprise d'Activité (PRA) doivent impérativement être mis en place et être un priorité (éviter qu'ils s'appuient sur des ressources potentiellement indisponibles en cas d'attaques.
- Développer une cartographie informatique (outil d'inventaire performant) unique et centralisé, constemment mis à jour et exhaustif.
- Favoriser une architecture informatique simple pour la maintenance.
- limiter les outils informatiques dont la sécurité n'a pas été audité
- Les sauvegardes et les mises à jours applicatives des serveurs et des postes de travail sont indispensables.
- les messageries devraient systématiquement être chiffrées.
- les équipements mobiles devraient disposer d'un antivirus, verifier les mises à jours et disposer d'un système de verouillage en cas de vol.
- les réseaux wifi devraient être opérées via des portails captifs.

Nombre d'autre préconisations qui pourront être mis em place uniquement si nous faisons de la cybersécurité une priorité d'un point de vue de développement informatique, ~~de discussion~~ d'être au coeur des discussions politiques et du plan de financement de l'Etat.