TRIP printemps 2021

11 & 12 mai

Cybersécurité: de la menace à l'action territoriale

Table ronde 2

Table ronde 2

Cybersécurité : de la menace à l'action territoriale

- **Julie DULAC**, Directrice administrative et financière - Seine-et-Marne Numérique
- **Denis VERMOT**, Directeur des systèmes d'information communs et **Mathieu SOUCHARD**, RSSI - La Rochelle ville et CA
- **Éric HAZANE**, Chargé de mission stratégie des territoires - ANSSI
- **Philippe STEUER**, RSSI - Bordeaux Métropole, et membre du Club des RSSI des collectivités
- **Cyril BRAS**, Vice-président - IN.CRT (Institut national pour la cybersécurité et la résilience des territoires)

Animation : **Luc DERRIANO**, Chargé de mission - Avicca

✧✧✧✧✧

Luc DERRIANO, Chargé de mission - Avicca

Cette table ronde est organisée en trois temps avec tout d'abord les témoignages de collectivités victimes qui vont montrer l'état de la menace. Dans un deuxième temps, des responsables de sécurité des systèmes d'information (RSSI) territoriaux expliqueront comment s'organiser pour se préparer ensemble à mieux réagir, car il n'y a pas que des problèmes, il y a aussi des solutions. À l'issue de chaque exposé, nous aurons la possibilité de prendre des questions via la plateforme Slido.

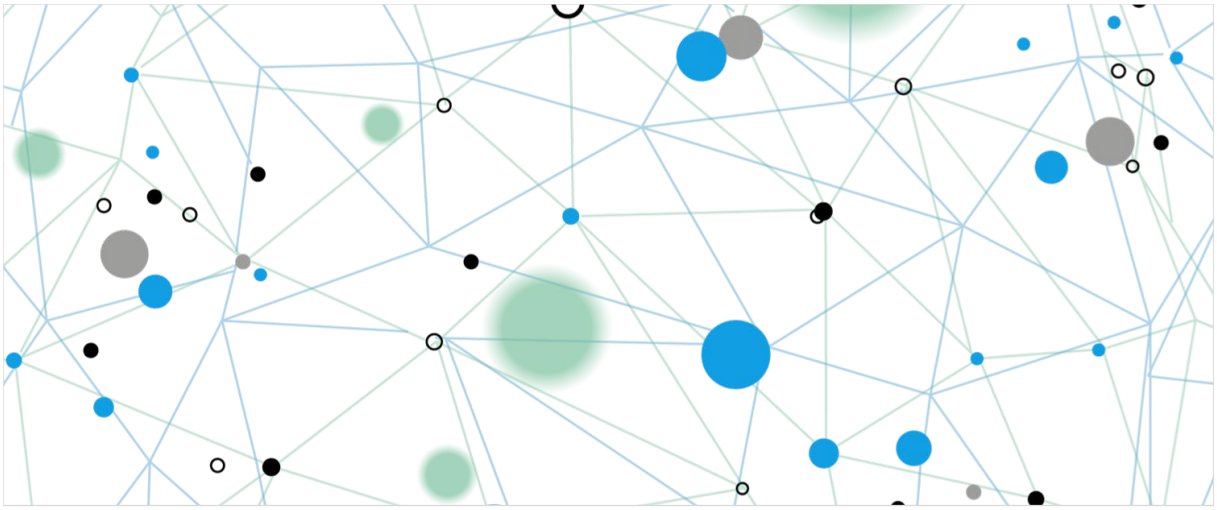
Tout d'abord, merci à celles et ceux qui ont répondu à notre invitation et qui ont eu l'accord de leurs supérieurs pour échanger avec nous ce matin. Preuve que les temps ont changé, nous n'en sommes plus à cacher que les systèmes d'information sont tous vulnérables. L'obligation d'informer est aussi passée par là avec le RGPD notamment. La crainte de l'atteinte à l'image pour la collectivité semble presque dépassée. Les élus, comme le maire d'Angers dont le discours tourne en boucle sur les réseaux sociaux depuis quelques temps, montrent désormais qu'ils maîtrisent leur communication en temps de crise cyber.

Nous accueillerons successivement Julie Dulac, directrice administrative et financière du syndicat mixte Seine-et-Marne Numérique ; Denis Vermot, directeur des systèmes d'information communs et Mathieu Souchard, RSSI, de la vile et de la communauté d'agglomération de La Rochelle ; Éric Hazane, chargé de mission stratégie des territoires de l'ANSSI ; Philippe Steuer, RSSI de Bordeaux Métropole et membre fondateur du Club des RSSI des collectivités ; Cyril Bras, vice-président de l'IN.CRT (Institut national pour la cybersécurité et la résilience des territoires).

Les piratages, cela n'arrive pas qu'aux autres. La progression des cyberattaques est de 400% et le top cinq des menaces est quasi identique pour les particuliers et les professionnels, dont les collectivités, comme le confirme le rapport d'activité 2020 de Cybermalveillance.gouv.fr publié le 15 avril dernier. Rançongiciel, piratage informatique de compte, virus et hameçonnage : c'est le quinté gagnant - ou plutôt perdant. En cette période de crise sanitaire, les hôpitaux ne sont d'ailleurs pas épargnés : des dizaines d'entre eux ont subi des cryptolockages, de Villefranche-sur-Saône à Marseille, en passant par Dax Montpellier, Rouen, Narbonne, Toulon, Issoudun, mais aussi des villes (Évreux, Bayonne, Angers, Houilles…). Quelle que soit leur taille et leur notoriété, les collectivités représentent des cibles comme les autres pour les cybercriminels. Une quarantaine de collectivités publiques sont attaquées par semaine, selon Guillaume Poupard, directeur général de l'ANSSI. Parmi ces collectivités, Seine-et-Marne Numérique.

Julie Dulac, après avoir brièvement présenté la collectivité dont vous êtes la directrice administrative et financière et, à ce titre, en charge de la gestion du système d'information, racontez-nous comment vous avez subi votre première attaque cyber. C'est à un retour de week-end que tout a basculé pour vous en février dernier…

Julie DULAC, Directrice administrative et financière - Seine-et-Marne Numérique



SEINE-ET-MARNE
NUMÉRIQUE

TRIP Avicca

Table ronde - Cybersécurité 12 mai 2021

Un SI pour qui, pour quoi ?

Une « petite » équipe de 15 personnes

Une activité d'aménagement numérique sur 50% du territoire d'Ile-de-France :

- **RIP 1G FttO et THD Radio**
- **RIP 2G FttE/FttH affermo-concessif**
- **Exploitation parc PRM MeD en régie**

Le SI en bref

Fonction SI portée par la DAF :

- **Une assistante pour traitement des tâches courantes**
- **Une directrice pour pilotage et supervision**

Une architecture repensée en 2018 :

- **Serveur en propre hébergé en salle SI du département - baie dédiée sans adhérence**
- **Lien FON entre le syndicat et le site d'hébergement**
- **Téléphonie en IP Centrex**
- **Accès Internet FTTO**

Une infogérance via marché de service

www.seine-et-marne-numerique.fr 1

En effet ; nous avons été cyberattaqués au retour d'un week-end. Il faut savoir que le syndicat mixte Seine-et-Marne Numérique est une petite équipe de 15 personnes, dont l'objet est l'aménagement numérique avec un RIP 1G, un RIP 2G et des PRM-MeD en régie. De fait, la fonction SI est portée par la direction ressources, c'est-à-dire la direction administrative et financière. Nous avons une assistante pour le traitement des taches courantes, et moi-même j'essaye de faire le pilotage et la supervision.

En 2018, nous avons remis en ordre l'architecture SI qui avait besoin d'un sérieux toilettage. Nous avons des serveurs en propre hébergés grâce à un partenariat avec le département, un lien fibre noire entre le syndicat et ce site d'hébergement, une téléphonie en voix sur IP et un accès Internet en fibre.

La structure étant assez petite, nous avons externalisé l'infogérance avec un marché de services car nous ne pouvions pas nous permettre de prendre un agent à temps complet.

Des mesures de sécurité préexistantes et en place

- **Anti-virus sur chaque poste de travail (SOPHOS)**
- **Pare-feu entre la téléphonie fixe et l'accès internet**
- **Politique de blocage de l'accès à certains sites internet**
- **Mots de passe utilisateurs à 8 caractères + caractères spéciaux**
- **Processus de renouvellement automatique des mots de passe utilisateurs**
- **Confidentialité des mots de passe administrateurs**
- **Logiciel anti-spam (MIB)**
- **Sauvegarde avec réplication (VEEAM Backup)**
- **Réplication des serveurs centraux sur le site du syndicat via la solution VMware**
- **Accès VPN sécurisé avec mot de passe individuel**

Parallèlement, nous étions déjà informés des mesures de sécurité et avions essayé de mettre en place le maximum de sécurité - en tout cas ce dont nous pensions pouvoir nous prémunir - avec des éléments assez classiques : des antivirus pour chacun des postes de travail ; des pare-feu entre la téléphonie fixe (voix sur IP) et l'accès Internet ; une politique de blocage de l'accès aux sites Internet non recommandés ; une sensibilisation des utilisateurs à avoir des mots de passe comptant plus de 8 caractères et des caractères spéciaux ; une scission entre l'utilisation des mots de passe administrateur et les autres mots de passe ; un logiciel antispam (Mailinblack) ; une sauvegarde par la VEEAM Backup de tout le réseau ; une réplication…. Enfin, crise sanitaire oblige, il y avait beaucoup de télétravail et nous avions donc sécurisé tous les accès VPN par des mots de passe individuels.

Prise de poste le lundi 8 février 2021 matin : les agents constatent l'impossibilité d'accéder aux fichiers et dossiers enregistrés sur les serveurs. L'ensemble est crypté par une extension « .e344p8xk »

Classeur1.xlsx.e344p8xk	06/02/2021 20:22	Fichier E344P8XK	12 Ko
signature_élec_SMN77_JDC.jpg.e344p8xk	06/02/2021 20:22	Fichier E344P8XK	28 Ko
SMN petit.png.e344p8xk	06/02/2021 20:22	Fichier E344P8XK	26 Ko

9h48 : ouverture d'un ticket auprès du support technique informatique de l'infogérant

10h00 à 13h00 : prise de main à distance sur postes et serveurs. Les documents impactés se trouvent sur la machine VM-DATA-01 cryptée depuis samedi soir à 20h22

Autre constat : la sauvegarde n'est plus fonctionnelle depuis le 23/01

13h00 à 15h00 : plan d'action - vérification des LOG sur le Firewall - coupure de tous les serveurs « utilisateurs » - création d'un réseau isolé BAC A SABLE pour identifier la source du cryptolocker. En parallèle, restauration de la VM-DATA-01 à partir de la dernière sauvegarde du 23/01/21.

Mais tout ceci ne nous a pas protégés d'une cyberattaque.

Un lundi matin, le 8 février, les agents essaient de se connecter : impossible ! Il s'avère que tous les fichiers enregistrés sur le serveur ont une extension bizarre.

Nous l'avons signalé à l'infogérant en ouvrant un ticket, ils ont pris la main à distance… Et ils nous ont dit que nous étions cyberattaqués et que cela avait l'air de remonter au samedi précédent, à 20h22.

Autre mauvaise nouvelle, la sauvegarde n'était plus fonctionnelle depuis le 23 janvier, et les données étaient perdues entre le 23 janvier et le 8 février.

L'infogérant a enclenché un plan d'action et a essayé d'attraper le cryptolocker avec une machine virtuelle dite « bac à sable » pour l'attirer. Malheureusement cela n'a pas suffi. La machine virtuelle de base, celle qui avait été la plus attaquée, étant trop petite, elle a dû être écrasée pour pouvoir être reconstruite.

09/02/2021 : restauration de la VM terminée à 100%. Pas de nouveau cryptage
mise en place d'une supervision renforcée de la solution Veeam Backup

10/02/2021 : l'infrastructure est de nouveau opérationnelle

11/02/2021 : divers problèmes sont constatés notamment par les utilisateurs en accès VPN

12/02/2021 : finalisation de la reconstruction de la VM-DATA-01

12/02/2021 : l'infrastructure est opérationnelle

En sus, déclaration à l'assureur et rejet car pas d'assurance cybersécurité spécifique, déclaration à la CNIL, plainte au commissariat (classement sans suite depuis lors)

Informations aux agents tout au long du process

Il a quand même fallu une semaine avant que l'interface soit opérationnelle. L'infogérant a réussi à restaurer la *virtual machine* (VM), il n'y avait pas de cryptage, l'infrastructure était opérationnelle et le 12 février nous avons pu retravailler.

Nous avons fait une déclaration à l'assureur qui l'a rejetée parce que nous n'avions pas d'assurance cybersécurité spécifique. Nous avons fait une déclaration à la CNIL et porté plainte au commissariat qui ne comprenait pas du tout ce que nous essayions de dire ! Pour finir ; la plainte a été classée car le tiers n'a pas été identifié.

Parallèlement, nous avons bien sûr informé les agents tout au long du processus.

1 - Mesures immédiates

- **Modification de toutes les extensions VPN (suppression du .local / accès VPN unifiés avec le compte Active Directory)**
- **Modification de tous les mots de passe d'accès VPN**
- **Accès direct des agents comptables en télétravail au logiciel Finances**
- **Doublement des emails de supervision de sauvegarde à deux agents de la DAF**
- **Audit de l'ensemble des anti-virus**
- **Sensibilisation des agents aux gestes à respecter (mise en ligne documentation ANSSI, comment bâtir un mot de passe complexe, etc.)**

2 - Mesures en cours

- **Suppression de la possibilité pour chaque agent d'être administrateur de son poste (même en raison du logiciel téléphonie fixe ou métier)**
- **Renforcement de l'anti-virus**
- **Étude sur le choix d'une sauvegarde des données sur bande (règle du 3-2-1)**
- **Souscription d'une assurance cybersécurité**

www.seine-et-marne-numerique.fr 5

Cette expérience nous a incité à essayer de muscler tout de suite nos défenses. Nous avons changé toutes les extensions VPN et tous les mots de passe, sachant que le cryptolocker était parvenu assez haut dans le système puisque, *a priori*, il avait réussi à prendre la main en qualité d'administrateur…

Nous avons souhaité scinder l'accès en télétravail des agents des finances, car le logiciel des finances entraîne des complexités en télétravail.

La sauvegarde a été rétablie et nous avons doublé les mails de supervision, c'est-à-dire que nous recevons aussi en interne, au syndicat, les mails de supervision de la sauvegarde.

Nous avons également réalisé un audit de l'ensemble des antivirus et puis nous avons sensibilisé les agents aux gestes à respecter en les informant de la documentation de l'ANSSI et en les invitant à bâtir des mots de passe complexes. Tout au long du processus, nous avons essayé de communiquer le plus souvent possible avec eux pour les sensibiliser et éviter d'être de nouveau cyberattaqués.

Parmi les mesures en cours de réflexion, nous pensons supprimer la qualité d'administrateur pour tous les agents. Certains d'entre eux ont cette qualité à cause de logiciels métiers et nous estimons que cela représente une porte ouverte vers des risques futurs.

Nous envisageons également le renforcement de l'antivirus et étudions comment mettre en place la règle du 3-2-1 avec un retour à une sauvegarde sur bande (disposer de trois copies des

données au moins ; stocker ces copies sur deux supports différents ; conserver une copie de la sauvegarde hors site).

Enfin, nous devons souscrire une assurance cybersécurité qui pourrait être un complément en cas de nouvelle attaque.

Minimes en termes de perturbations du travail

Les données sensibles (ex. : RH) cryptées n'ont pas été communiquées à l'extérieur. Les effets ont donc été limités.

Mais, double sauvegarde inopérante depuis le 23/01/2021 et perte de l'ensemble des documents produits ou modifiés sur le réseau jusqu'au 06/02/2021.

Inventaire de ces documents finalisé = perte de l'ensemble des courriers entrants/sortants, bons de commande émis, mises à jour de tableaux de suivi (conventions, marchés publics, suivi financier, indicateurs), permissions de voirie, ordres de service et procès-verbaux, des calendriers et ordres du jour et certains archivages.

Le cryptolocker n'ayant pu être trouvé, le risque d'une nouvelle cyberattaque demeure réel.

En termes d'impacts, nous avons eu la confirmation que les données, notamment RH, n'avaient pas été communiquées à l'extérieur, l'impact est donc limité. Cependant, comme la sauvegarde a été inopérante, nous avons tout perdu entre le 23 janvier et le 8 février… Il a fallu tout reconstruire et vérifier, mais on ne se rend compte qu'au fur et à mesure de ce que l'on a perdu. Le cryptolocker n'ayant pas été trouvé ; nous savons que nous vivons avec une épée de Damoclès au-dessus de la tête, avec une cyberattaque qui pourrait à nouveau se produire. La cyberattaque a eu lieu le 6 février mais en fait, il y avait auparavant un agent dormant qui a étudié notre système avant de se déclencher le jour J.

- **Établir une revue de sécurité du SI régulière (check list)**
- **Prévoir deux à trois sauvegardes des données**
- **Vérifier les modes de fonctionnement des sauvegardes**
- **Vérifier que les VM sont suffisamment dimensionnées pour permettre qu'en cas d'attaque, il n'y ait pas besoin de les « écraser » pour rendre le service à nouveau opérationnel**
- **Recourir à une assurance cybersécurité**
- **Sensibiliser les agents à la sécurité informatique en continu**

Quels enseignements en tirons-nous ? Il faut vraiment établir une revue de sécurité régulière du SI et prévoir également une sauvegarde des données, mais pas uniquement sur la VEEAM Backup.

Il faut vérifier le bon fonctionnement des sauvegardes et veiller à avoir des VM suffisamment dimensionnées.

Nous allons recourir à une assurance cybersécurité. Et enfin, nous continuons à sensibiliser les agents, mais avec le télétravail, nous avons moins de pratiques communes et cela représente un challenge important.

Voilà pour notre cyberattaque du 6 février qui, nous l'espérons, ne se reproduira pas !

Luc DERRIANO

Merci pour ce témoignage. Où en êtes-vous concernant l'assurance que vous envisagez de souscrire et qu'en attendez-vous ?

Julie DULAC

Du fait que nous passons en groupement de commandes avec le centre de gestion de la grande couronne, les délais de procédure sont assez longs… Nous en attendons, d'une part, un audit de sécurité puisque l'assureur viendra auditer le SI pour repérer ses failles éventuelles et, d'autre part, une réparation. En l'occurrence, les dégâts ont été assez limités, cependant, si nous avions subi des pertes, nous aurions pu être indemnisés par l'assurance.

SEINE-ET-MARNE NUMÉRIQUE

Merci de votre attention

Contact : Julie DULAC
Directrice administrative et financière
julie.dulac@seineetmarnenumerique.fr
01 64 10 66 13

www.seine-et-marne-numerique.fr 8

Luc DERRIANO

Merci pour ce témoignage. Où en êtes-vous concernant l'assurance que vous envisagez de souscrire et qu'en attendez-vous ?

Julie DULAC

Du fait que nous passons en groupement de commandes avec le centre de gestion de la grande couronne, les délais de procédure sont assez longs… Nous en attendons, d'une part, un audit de sécurité puisque l'assureur viendra auditer le SI pour repérer ses failles éventuelles et, d'autre part, une réparation. En l'occurrence, les dégâts ont été assez limités, cependant, si nous avions subi des pertes, nous aurions pu être indemnisés par l'assurance.

Luc DERRIANO

Merci. On sait que plus de 1 400 collectivités publiques ont été récemment attaquées. Parmi celles-ci, la ville et la communauté d'agglomération de La Rochelle et nous accueillons maintenant Denis Vermot, directeur des systèmes d'information communs, et Mathieu Souchard, RSSI. Pour Seine-et-Marne Numérique, c'est au retour d'un week-end que l'attaque a été découverte, pour vous, c'est carrément pendant la trêve des confiseurs, entre Noël et le Nouvel An ! Mais d'abord, expliquez-nous ce qu'est la direction des systèmes d'information communs…

Denis VERMOT, Directeur des systèmes d'information communs et Mathieu SOUCHARD, RSSI - La Rochelle ville et CA

Denis VERMOT

Introduction

Contexte : la Communauté d'agglomération et la Ville de La Rochelle ont mutualisé leurs directions des systèmes d'information le 1er janvier 2019.

Périmètre de la Direction des Systèmes d'Information Communs


3 000 postes de travail


400 serveurs


200 applications métiers

Les missions du Responsable de la Sécurité des Systèmes d'Information

- ✓ Créer et mettre en application la Politique de Sécurité des Systèmes d'Information
- ✓ Accompagner les métiers dans la formalisation des besoins de sécurité
- ✓ Former et sensibiliser les utilisateurs
- ✓ Homologuer les téléservices et les applications sensibles
- ✓ Contrôler le niveau de sécurité avec des tests d'intrusion

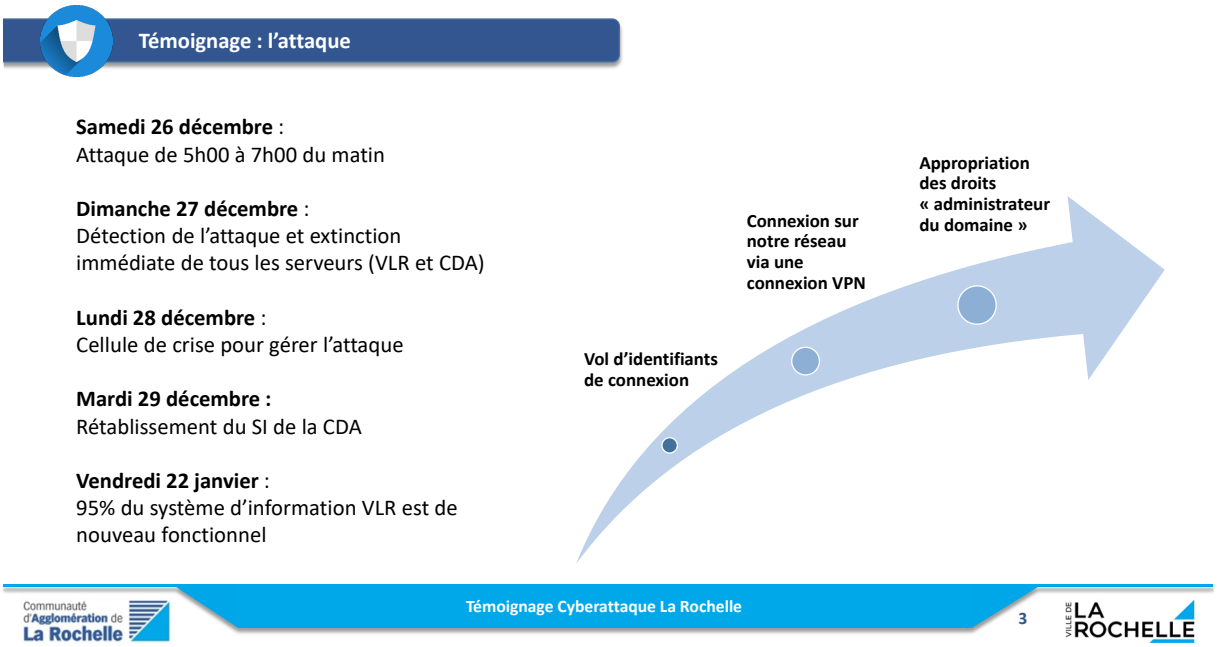
Témoignage Cyberattaque La Rochelle 2

La communauté d'agglomération de la Rochelle, c'est 177 000 habitants et plus de 3 000 agents. Les systèmes d'information ont été mutualisés le 1er janvier 2019 et le périmètre commun concerne environ 3 000 postes de travail, 400 serveurs et plus de 200 applications métiers.

Lorsque nous avons réalisé cette mutualisation, j'ai souhaité qu'un poste de RSSI soit créé. En effet, il existait un mi-temps à la ville mais pas à la CA, il fallait donc créer un poste de RSSI pour les deux collectivités. Ses missions principales sont de mettre en application la politique de sécurité des systèmes d'information, d'accompagner les métiers et les services dans la formalisation de leurs besoins de sécurité, de former et sensibiliser les utilisateurs, d'homologuer les téléservices et les applications sensibles, et enfin de contrôler le niveau de sécurité avec des tests d'intrusion.

Nous avions déjà mis en place les outils et les structures, avec une PSSI (politique de sécurité du système d'information) et une charte qui est en cours de rédaction. Nous pensions être suffisamment armés et sécurisés pour ne pas être attaqués. Mais il y a eu une attaque le week-end du 26 décembre. Mathieu Souchard va vous expliquer en détail ce qui s'est passé.

Mathieu SOUCHARD



La plupart des cyberattaques de cryptolockers (ou rançongiciels en français) se produisent le week-end parce que c'est le moment où il y a le moins de personnes dans les DSI pour intervenir. Nous n'avons pas échappé à la règle et avons subi cette attaque le samedi 26 décembre entre 5h et 7h du matin, c'est-à-dire que les attaquants ont pu rester deux heures sur le réseau et crypter plusieurs de nos serveurs, pour demander finalement une rançon.

Il y avait eu deux premières alertes le samedi mais nous n'avions pas détecté l'attaque. En revanche, elle a été détectée dès le dimanche après-midi par le DGS parce qu'il y avait des extensions de fichiers un peu particulières sur le serveur, exactement comme pour le syndicat mixte de Seine-et-Marne. Dès la détection de l'attaque, nous avons coupé tous les serveurs (il y a deux SI différents, celui de la ville de La Rochelle d'un côté et de la CDA de l'autre) parce que nous ne savions pas quelle était son ampleur, et nous avons également coupé la connexion Internet pour éviter de se faire réattaquer par la suite.

Dès le lundi matin, nous avons monté une cellule de crise avec la direction générale, le service juridique, la DSIC et les élus afin de définir un plan d'actions.

Dans notre cas, il a été utile d'avoir deux SI cloisonnés : celui de la CDA n'ayant pas été touché du tout, nous avons pu redémarrer la messagerie, ce qui nous a permis de communiquer et de rétablir le SI de la ville assez rapidement. Finalement, moins de quatre semaines après l'attaque, 95 % du SI de la ville de La Rochelle avait été rétabli.

Comment s'est déroulée l'attaque ? Les attaquants ont d'abord volé des identifiants de connexion (nous soupçonnons qu'ils ont pu le faire en attaquant le pare-feu grâce à une faille assez importante). Ils se sont alors connectés via le VPN, malgré des comptes et mots de passe uniques par agent (comptes nominatifs avec mots de passe complexes, mais il s'avère que ce

n'était pas suffisant en termes de sécurité VPN). Ensuite, ils se sont approprié les droits « administrateur de domaine » et, à partir de là, ils ont pu faire ce qu'ils voulaient sur le réseau.

Une attaque par rançongiciel pour une collectivité a un impact énorme sur ces valeurs essentielles :

- **Perte de la qualité du service public** :
  - L'ensemble des services était à l'arrêt ou en mode dégradé
- **Perte financière** :
  - Stationnement : en cette période, environ 6 000 euros / jour (rétablissement au bout de 4 jours)
- **Perte d'image** :
  - L'incident a été médiatisé à l'échelle nationale
- **Vol potentiel de données**

Quels ont été les impacts sur l'ensemble de la collectivité ? Le plus important est la perte de la qualité du service public. On sait maintenant que les systèmes d'information et les outils numériques sont indispensables dans beaucoup de métiers : les 250 applications métiers étaient toutes à l'arrêt et le service était dégradé. Par exemple, il n'était plus possible de payer les agents ni les fournisseurs externes, il y avait des soucis au niveau du stationnement pour lever les barrières et les descendre, au niveau de l'état civil, etc. Tous les services fonctionnaient en mode dégradé, avec un retour au papier, ce qui représentait un impact énorme pour la collectivité.

Il y a aussi eu une perte financière. Par exemple, en cette période, le stationnement représente une recette de 6 000 euros par jour. Au sein de la cellule de crise, le DGS a tout de suite priorisé les services à rétablir le plus rapidement possible ; le stationnement en faisait partie, tout comme les RH, le logiciel des cimetières, l'état civil, etc.

L'impact se mesure également en termes de perte d'image et perte de confiance de la part des usagers. Lorsqu'une collectivité subit une cyberattaque, il y a toujours un doute concernant le vol de données personnelles.

Enfin, cet événement a été médiatisé à l'échelle nationale. Il est très important de gérer les médias lors d'une cyberattaque : certains médias nous ont contactés et nous leur avons répondu ; d'autres ont tenté de le faire mais, pris par le temps, nous n'avons pas pu répondre à tous ; et enfin, certains ne nous ont pas contactés mais ont quand même sorti des articles… Cette période a été assez compliquée à gérer vis-à-vis des médias.

Dernier impact, comme les attaquants sont restés deux heures sur le réseau, nous considérons que nous avons pu subir un vol de données mais, pour l'instant, aucune donnée n'a été rendue publique.

Témoignage : le plan d'actions

Suite à la cyberattaque, le plan de rétablissement s'est décomposé en trois phases :

1. **Investigation**
   - L'objectif est d'identifier les vulnérabilités exploitées par l'attaquant et de faire un état des lieux des ressources impactées. L'investigation a été menée par Orange Cyber Défense qui nous a accompagnés pendant 4 semaines. Le coût financier a été de 45 000 €.

2. **Restauration**
   - L'objectif est de rétablir les équipements informatiques permettant le bon fonctionnement de la collectivité (53/160 serveurs ont été restaurés et 42/900 ordinateurs ont été formatés)

3. **Sécurisation**
   - L'objectif est de sécuriser les vulnérabilités identifiées dans la phase d'investigation

Communauté d'Agglomération de La Rochelle — Témoignage Cyberattaque La Rochelle — 5 — Ville de La Rochelle

Pour gérer les suites de cette cyberattaque, nous avons défini un plan d'actions en trois grandes parties.

La première était une phase d'investigation dont l'objectif était tout d'abord de savoir quel périmètre avait été touché, quels serveurs impactés, quels services, et si la sauvegarde avait été touchée. L'état des lieux a été mené avec l'aide d'Orange Cyberdéfense : un tiers des serveurs avaient été cryptés, 42 postes touchés, mais par chance, la sauvegarde n'avait pas été impactée.

L'objectif était ensuite de savoir comment nous avions été attaqués et d'éviter que cela se reproduise. Orange Cyberdéfense nous a fourni des logiciels pour récupérer les logs ainsi que la traçabilité des serveurs, ce qui a permis, petit à petit, de déterminer le point d'entrée des attaquants et de comprendre quels serveurs avaient été le plus touchés. Le coût financier pour Orange Cyberdéfense qui nous a accompagné pendant quatre semaines s'est élevé à 45 000 €, c'est-à-dire un budget conséquent, mais indispensable au vu de l'aide apportée.

La deuxième phase est celle de la restauration. Certains services ou directions devaient être rétablis très rapidement. 53 serveurs sur les 160 de la ville ont été rétablis, et 42 postes informatiques.

La troisième phase est la sécurisation : nous souhaitons à tout prix éviter que l'événement se reproduise et la phase d'investigation nous a permis de déterminer les nouveaux points à sécuriser.

Témoignage : durcissement de la sécurité

Quelques exemples de mesures de sécurité suite à la cyberattaque :

- ❑ Modification de tous les mots de passe (utilisateur, administrateur, équipements de sécurité…)
- ❑ Sécurisation du VPN (double authentification via certificat)
- ❑ Durcissement des équipements de sécurité
- ❑ Mise en place d'une sauvegarde déconnectée
- ❑ Création d'un Plan de Reprise d'Activité
- ❑ Veille quotidienne sur les failles de sécurité

J'ai évité de lister tous les points de sécurité mis en place, mais voici une sélection de certains d'entre eux que je tenais à présenter :

Modification de tous les mots de passe (utilisateurs, administrateurs, équipements de sécurité).

Sécurisation renforcée du VPN avec une double authentification, c'est-à-dire que nous installons un certificat sur le poste, ce certificat faisant office de connexion (il n'est pas possible de se connecter de n'importe quel poste). Dans un second temps, nous envisagerons peut-être une double authentification via SMS ou mail.

Amélioration des équipements de sécurité.

Mise en place d'une sauvegarde déconnectée : c'est un peu le retour aux bandes évoquées précédemment, c'est-à-dire que la sauvegarde serait déconnectée du réseau et donc inaccessible en cas de cyberattaque.

Nous allons mettre en place un plan de reprise d'activité (PRA) afin de pouvoir ordonnancer toutes les actions à mettre en place en cas de nouvelle cyberattaque.

Enfin, nous assurerons une veille quotidienne encore plus approfondie sur les failles de sécurité.

Denis VERMOT

Nous avons eu la chance de pouvoir rétablir le système d'information de la ville de la Rochelle en quatre semaines.

On peut souligner la forte mobilisation de la DSIC qui a travaillé en osmose avec tous les services (études, géomatique, infrastructures…). Ces derniers se sont tous portés volontaires pour travailler sur des périmètres qui n'étaient pas forcément les leurs. Il y a eu un vrai soutien entre les équipes et un nombre important d'heures de travail.

Le soutien de la hiérarchie a été très important. La DGS et les élus n'ont pas cherché à nous mettre la pression en exigeant que tout soit rétabli tout de suite. Ils ont constaté les dégâts en disant qu'il fallait que cela fonctionne de manière nominale, pas de manière dégradée. Cette bienveillance est à souligner car elle nous a permis de travailler en toute tranquillité.

Surtout, il y a eu une prise de conscience. Nous avions des projets en matière de sécurité depuis quelques mois, voire quelques années, et cet épisode a permis de les lancer immédiatement et de les mettre en œuvre, du fait de la sensibilisation accélérée de tous les agents et de toutes les strates de la collectivité en matière de sécurité.

La volonté de départ avec la mutualisation qui a été réalisée il y a deux ans, presque trois, était de faire converger les systèmes d'information des deux collectivités, mais nous avons compris qu'il fallait rester prudent : il est possible d'avoir deux systèmes d'information différents qui sont capables de dialoguer, mais nous n'avons pas besoin d'avoir un système d'information unique. En revanche, il faut veiller à avoir un niveau de sécurité identique sur les deux systèmes d'information et penser au cloisonnement de certains périmètres qui ne sont pas mutualisables, parce que certaines applications ou systèmes sont dédiés à une collectivité ou à l'autre.

En conclusion, on peut dire que nous ne nous en sommes pas si mal sortis, 4 semaines après la cyberattaque !

Contacts

Denis Vermot
Directeur des Systèmes d'Information Communs

Denis.vermot@agglo-larochelle.fr

Mathieu Souchard
Responsable de la Sécurité des Systèmes d'Information

Mathieu.souchard@agglo-larochelle.fr
05 46 37 73 29

Luc DERRIANO

Merci pour ce retour d'expérience très précis. Vous avez évoqué un accompagnement par un prestataire qui vous connaissait déjà. C'est peut-être un sujet d'attention, pensez-vous que cela a pu faciliter le traitement de l'incident ?

Denis VERMOT

Nous connaissions Orange Cyberdéfense mais pas en tant que prestataire. En revanche, Orange était un des prestataires de nos marchés de téléphonie. Au moment de l'attaque, le responsable de l'unité infrastructures réseaux et télécoms, Jean-Philippe Robillard, a contacté en urgence plusieurs organismes pour travailler sur le problème. Certains ont répondu qu'ils n'en étaient pas capables et d'autres n'ont pas répondu. Seul Orange Cyberdéfense a répondu qu'il était capable de tout prendre en charge et a pu travailler immédiatement dessus.

Certes, cela a coûté 45 000 € mais la dépense n'a pas été inutile compte tenu de l'ampleur de l'attaque (un tiers des serveurs infectés, sachant que nous avons dû traiter tous les postes même s'il n'y en avait que 42 d'infectés). Avec Orange Cyberdéfense, la situation a pu être rétablie en quatre semaines.

Luc DERRIANO

Avez-vous une évaluation du coût financier de l'attaque ? (question de Pascal Bourdillon de Berry Numérique). Des communes de l'agglomération de la Rochelle ont-elles été impactées ? (question d'Olivier Devillers, journaliste pour la Banque des Territoires notamment)

Denis VERMOT

Les communes de la communauté d'agglomération ne sont pas sur notre système d'information, elles ont des systèmes d'information indépendants pour l'instant et l'attaque n'a concerné que la ville de La Rochelle.

Mathieu SOUCHARD

En matière financière, le coût total de l'attaque n'a pas encore été évalué. C'est une étude un peu longue à réaliser car le coût doit être établi sur chaque service indépendamment.

Luc DERRIANO

Merci. Le 18 février dernier, le président de la République a annoncé un plan doté d'un milliard d'euros pour lutter contre les menaces cyber. Après ces retours d'expérience de collectivités sur des cyberattaques, Éric Hazane, chargé de mission stratégie des territoires de l'ANSSI, va exposer l'état de cette menace, qualitativement et quantitativement, pour les collectivités, et les nouveaux moyens de l'ANSSI pour accompagner les structures publiques. Il y a notamment des délégués présents dans chaque région, le dispositif d'accompagnement des victimes Cybermalveillance.gouv.fr, divers guides réalisés par l'AMF ou la Banque des Territoires, mais aussi des appels à projets pour déployer les CSIRT (*Computer security incident response team*), ces centres d'alerte et de réaction aux attaques sur tout le territoire, et encore d'autres dispositifs de financements pour aider au diagnostic…

Éric HAZANE, Chargé de mission stratégie des territoires - ANSSI

Je remercie l'Avicca pour son invitation à participer à cette table ronde, je salue votre travail et votre engagement sur les questions du numérique et de sécurité du numérique. Je tiens aussi à remercier tout particulièrement Seine-et-Marne Numérique et la Rochelle pour leurs témoignages car peu de victimes acceptent de témoigner publiquement, mais quelques collectivités ont décidé de prendre le taureau par les cornes et de communiquer. Elles ont subi une cyberattaque, en dépit de leur préparation et d'un bon niveau de maturité sur le sujet pour certaines. Finalement, à quelque chose malheur est bon et ce partage d'expérience est très positif.

Je faisais le constat, en écoutant ces témoignages, que les sauvegardes n'avaient pas été touchées. Ce n'est pas toujours le cas pour certaines collectivités où les attaquants ont recherché tout particulièrement les systèmes de sauvegarde ou l'*Active Directory* quand il existe, avant de déclencher l'attaque. Vous avez sans doute évité la catastrophe, car quand les sauvegardes sont touchées, il est difficile de redémarrer. Ce qui se pratique beaucoup également, aujourd'hui, c'est la fuite de données partielle à des fins de chantage sur le *Dark*

Web… Je serais intéressé par un retour sur le coût final de l'attaque car le chiffrage est toujours compliqué à établir, entre les coûts directs (perte de recettes de parking, par exemple) et le coût indirect (la perte en ligne des services, le service qui n'est pas rendu au public, l'indisponibilité du système d'information, la perte en termes d'image, etc. sont difficiles à calculer).

Les collectivités font partie de la transformation numérique, elles la vivent et parfois la subissent avec les questions de réglementation, notamment au travers de la dématérialisation. Il s'agit d'un mouvement d'ampleur.

Qui dit transformation numérique dit grande dépendance aux systèmes d'information et au numérique et, on le voit aujourd'hui, beaucoup de vulnérabilités exploitées par des groupes d'attaquants, de la cybercriminalité mais pas uniquement, qui s'en donnent à cœur joie.

Heureusement, même si le panorama est assez sombre dans l'ensemble, il y a des réponses des services de l'État, notamment l'ANSSI, l'Agence nationale de sécurité des systèmes d'information, autorité nationale en matière de cybersécurité et de cyberdéfense, avec 550 agents répartis pour le moment sur deux sites à Paris. L'ANSSI dispose également d'une implantation de délégués en région.

Dans les mois qui viennent deux nouvelles implantations sont prévues, l'une au Campus Cyber dans le quartier de La Défense à Paris, et l'autre du côté de Rennes, où nous allons ouvrir une antenne qui comprendra à terme près de 200 agents.

Les missions de l'Agence se composent de deux volets. D'une part, celui de la protection des systèmes d'information en faisant de la prévention, en proposant des missions de sensibilisation, des guides, etc. ; et, d'autre part, celui de la défense, l'intervention, la réaction aux attaques. Nous sommes en capacité d'intervenir de manière indirecte car nous avons participé au développement d'un écosystème français de la cybersécurité et nous disposons aujourd'hui d'un certain nombre de prestataires qui peuvent intervenir sur différents champs de compétences. Le nombre d'attaques augmentant, l'ANSSSI n'est pas en mesure de répondre à toutes les demandes, et Cybermalveillance.gouv.fr est aussi là pour répondre aux particuliers et aux petites entreprises.

La stratégie des dernières années a été de déployer une famille de prestataires qualifiés en mesure d'intervenir dans différents champs (audit, détection et/ou réponse aux incidents, etc.) en coordination régulière avec l'ANSSI en fonction de la gravité de la cyberattaque. Quand une collectivité de taille importante est touchée, nous sommes évidemment informés et suivons attentivement toutes les opérations qui y ont trait. Il arrive que, sur des affaires beaucoup plus importantes, nous devions intervenir plus directement (par exemple, Aix-Marseille-Provence qui a été touchée très sérieusement en 2020).

En termes quantitatifs, nous observons une tendance très sensible à l'augmentation des attaques ces dernières années. Le graphique que je vous présente ne reprend « que » les chiffres de l'ANSSI, c'est-à-dire une petite portion de visibilité de ce qui se passe réellement dans le cyberespace et de ce qui touche vraiment nos différentes entités, publiques comme privées. Sur la seule typologie des rançongiciels, le nombre de victimes touchées a été multiplié par quatre entre 2019 et 2020 (passant de 54 à 192 cas). Il s'agit donc d'une tendance lourde, sachant que les chiffres du premier trimestre 2021 ne font que confirmer cette tendance à

l'augmentation très importante des rançongiciels, qui touchent de nombreux secteurs d'activité et notamment les collectivités territoriales de manière assez forte.

Les collectivités territoriales sont de plus en plus exposées, elles représentent un attrait pour la cybercriminalité. Certains attaquants considèrent qu'elles sont relativement simples à attaquer et que, pour pouvoir rétablir leur système d'information et rendre ce service public aux citoyens, elles paieront sans doute une rançon - ce qui est loin d'être vrai heureusement de toute façon.

Si les collectivités ne sont pas une nouvelle cible pour les criminels, l'évolution se produit dans la typologie des attaques. En un an, nous avons observé une baisse concernant les défigurations de site Internet qui touchaient traditionnellement beaucoup les communes et les collectivités depuis de nombreuses années. Une défiguration de site Internet, c'est gênant notamment en termes d'image, mais finalement cela ne provoque pas forcément beaucoup de dégâts sur le système d'information. En parallèle, nous avons constaté une augmentation assez sensible des compromissions de comptes de messagerie et un doublement des attaques par maliciels et par rançongiciels.

Cela signifie que les attaquants ne se contentent plus simplement de porter des messages « d'hacktivisme » ou autres, mais cherchent vraiment à pénétrer les systèmes d'information, à en prendre le contrôle, à les cryptolocker et à obtenir le maximum d'effets en exploitant souvent des vulnérabilités assez simples, malheureusement.

À travers cette évolution, les collectivités apparaissent donc comme diversement protégées et d'une maturité très hétérogène. On voit que certaines sont ciblées par des attaques d'opportunité, mais on voit également une forme d'ingénierie, une recherche de chemin d'attaque et surtout de déclenchement de cette attaque à un moment opportun (pendant le week-end ou les fêtes de fin d'année…). Il n'y a pas de hasard à ce type d'attaques qui vont spécifiquement toucher des collectivités de taille importante, voire très importante.

Nous proposons un certain nombre de réponses opérationnelles avec des délégués en région. C'est la division de la coordination territoriale à laquelle je suis rattaché qui porte le sujet de la réponse territoriale de l'ANSSI depuis plusieurs années. N'hésitez pas à contacter vos délégués en région, il est toujours utile d'avoir ce point de contact en cas de besoin, mais aussi en amont pour faire connaissance, échanger et connaître l'offre proposée par l'ANSSI en région. Les délégués ne travaillent pas seuls mais avec les autres services de l'État qui vont chercher à apporter une protection sur le plan numérique mais également économique, et ils disposent également d'un réseau extrêmement important et puissant, apte à démultiplier les effets recherchés.

Note : le lien vers la page internet consacrée :
https://www.ssi.gouv.fr/agence/cybersecurite/action-territoriale/

Le site de l'ANSSI contient de nombreuses informations actualisées constamment, des guides, des ressources, un MOOC (formation gratuite en ligne), ainsi que le catalogue des visas de sécurité, c'est-à-dire une offre de produits et de services de confiance, certifiés ou qualifiés par l'ANSSI. Si vous recherchez un produit de sécurité vraiment robuste et qui apporte toutes les garanties, ou un prestataire en matière d'audit, de réponse aux incidents, de détection, etc., allez sur le site de l'ANSSI et téléchargez le catalogue des visas de sécurité, vous devriez trouver une réponse à vos questions.

Cybermalveillance.gouv.fr est un dispositif précieux. C'est un peu le chaînon manquant avec le haut du spectre des attaques et la réponse de l'ANSSI qui s'occupe en priorité de l'administration, de l'État, des opérateurs régulés ou critiques (opérateurs d'importance vitale ou de services essentiels : OIV et OSE), des grandes collectivités… Cybermalveillance a vocation à répondre aux citoyens de manière très large, mais également aux très petites et moyennes entreprises et à un certain nombre de collectivités petites et moyennes, en proposant notamment des guides et des fiches pratiques, ainsi qu'un « parcours victime ». En cas d'incident, c'est le bon point de démarrage pour rechercher de l'information et se faire assister si nécessaire.

Cybermalveillance propose également depuis cette année un label « experts cyber » qui permet de disposer d'un certain nombre de prestataires ayant un bon niveau de qualification. Ils sont labellisés pour pouvoir intervenir auprès des victimes en cas d'attaque importante et remédier à cet incident.

Il existe des guides spécifiques destinés aux collectivités. Un guide ANSSI consacré à l'essentiel de la réglementation s'appliquant à une collectivité. L'idée était de concentrer en un seul document la somme de tous les documents réglementaires et législatifs qui peuvent s'appliquer à une collectivité (guide « Sécurité numérique des collectivités territoriales ») : RGS, RGPD, etc.

La Banque des Territoires / groupe CDC, a sorti un « Guide pratique pour une collectivité et un territoire numérique de confiance », complété de quatre vidéos de sensibilisation très pédagogiques.

Enfin, l'ANSSI a contribué au guide de l'AMF intitulé « Cybersécurité : toutes les communes et intercommunalités sont concernées ». Réalisé avec des élus et des praticiens des collectivités, ce guide très pratique propose une trentaine de recommandations concrètes qui peuvent s'appliquer à toutes les collectivités, y compris les plus importantes.

Pour conclure, je souhaite passer trois messages. Premièrement, informez-vous, restez vraiment connectés, faites de la veille et formez-vous également, je pense notamment à tous les cadres territoriaux, aux élus. Beaucoup de formations sont aujourd'hui disponibles, il est sans doute possible de trouver un format adapté à vos attentes.

Identifiez deuxièmement vos points de contact en région, notamment les délégués de l'ANSSI bien sûr.

Enfin, troisièmement, exercez-vous pour anticiper les crises. Vous trouverez ci-après un lien vers le guide de l'ANSSI qui a été rendu public l'année dernière sur ce sujet. Organisez des exercices de gestion de crise, impliquez vos élus ou votre hiérarchie. Ce type d'exercice peut durer deux jours et même plus, mais peut aussi être très court. N'hésitez pas à réfléchir à cette possibilité car il sera toujours utile de s'être un peu entrainé, d'avoir pu se préparer, d'avoir identifié des lacunes sans doute majeures, et ça vous fera gagner un temps certain. Il faut vous y préparer parce que tout système d'information est potentiellement à risque aujourd'hui.

Luc DERRIANO

Pourquoi l'ANSSI ne détermine-t-elle pas un seuil minimal de dispositif de sécurité dont devraient obligatoirement disposer les collectivités territoriales ? Quelle est la présence d'antennes de

l'ANSSI dans les territoires ultramarins et notamment sur l'ile de La Réunion ? (questions de la région La Réunion).

Éric HAZANE

Je suis le point de contact chargé de l'outre-mer à L'ANSSI. La stratégie des territoires, ce sont les territoires au sens large.

Concernant la détermination d'un seuil minimal de dispositif de sécurité, la question pourrait se poser un jour, on pourrait rechercher un dispositif adapté aux collectivités, de type opérateur critique. Mais, il existe un principe constitutionnel de libre administration des collectivités et nous sommes donc très prudents sur la façon d'aborder le sujet. La philosophie de l'ANSSI est plutôt de chercher à fonctionner en mode co-construction ou incitation qu'en mode obligation.

Le plan France relance est également là pour permettre d'élever le niveau général de maturité, notamment des collectivités. Sur les 136 millions d'euros du volet cyber du plan de relance, une soixantaine de millions sont consacrés aux collectivités, notamment à travers ce que l'on appelle des parcours de sécurisation permettant de poser un diagnostic, donner un niveau de maturité *a priori* et proposer en sortie un plan d'actions (techniques, organisationnelles…) pour augmenter ce niveau de maturité. Nous sommes heureux de contribuer ainsi et de permettre aux collectivités de mieux se protéger pour résister aux cyberattaques.

Luc DERRIANO

Merci beaucoup. Nous avons la chance d'avoir aussi Amandine Del-Amo, chargée de mission à Cybermalveillance.gouv.fr, qui pourra répondre à une question relative au partage entre les actions de l'ANSSI et celle de Cybermalveillance.

Amandine DEL-AMO, Chargée de mission partenariats - Cybermalveillance.gouv.fr

Cybermalveillance a été créé pour apporter une solution aux victimes d'actes de cybermalveillance : pour les plus petites entreprises, les collectivités et les particuliers. Cela a été l'essence même de ce dispositif né il y a un peu plus de 3 ans maintenant. Sa mission principale est d'assister les victimes qui pourront suivre pas-à-pas sur la plateforme un parcours pour établir un pré-diagnostic de ce qui leur arrive, recevoir des conseils précis pour savoir comment y faire face. Elles seront également redirigées vers des organismes existants qui sont compétents et spécialisés (sites de signalement, sites de cyberharcèlement ou autres…). Nous allons jusqu'à la mise en relation avec des prestataires informatiques locaux qui pourront dépanner, venir en aide physiquement auprès des petites collectivités, petites entreprises ou particuliers.

Notre deuxième mission est la sensibilisation. Pour ce faire, nous créons des contenus. Nous avons notamment conçu un kit de sensibilisation pour faire comprendre les risques numériques et partager les bonnes pratiques. Ce kit est enrichi régulièrement. En fin d'année dernière, nous avons également réalisé des vidéos dédiées aux collectivités (avec la Banque des Territoires, qui est membre de Cybermalveillance.gouv.fr), pour les élus sur ce sujet de la cybersécurité.

Notre troisième mission est l'observation de la menace. Nous avons la chance d'occuper un poste stratégique puisque les prestataires sur le terrain nous remontent des informations, et les victimes nous font part de ce qui leur arrive à travers les parcours. Nous avons donc la chance de

disposer de nombreuses données et de pouvoir en dégager des tendances. N'hésitez pas à consulter notre rapport d'activité sorti il y a quelques semaines et disponible sur notre site. Parmi les tendances qui ont pu être dégagées, à ce jour un peu plus de 265 000 victimes sont venues sur la plateforme depuis son lancement. Nous nous sommes aperçus que l'immense majorité de ces attaques auraient pu être évitées si les utilisateurs avaient été sensibilisés… Nous avons donc tous un très grand rôle à jouer pour être acteur de cette sensibilisation.

Cybermalveillance.gouv.fr est encore peu connue des collectivités et je suis ravie de l'arrivée de l'Avicca en 2021 au sein la plateforme pour la faire connaître auprès des collectivités. Nous pouvons vraiment vous aider en matière de sensibilisation et de prévention des agents, et bien sûr en cas d'attaque éventuellement, en vous mettant en relation avec des prestataires de confiance, notamment les prestataires « labellisés » dont a parlé Éric Hazane de l'ANSSI. Ce nouveau label né en 2020 permet d'identifier les prestataires ayant une compétence plus forte en cybersécurité et ainsi de faire appel à des professionnels de confiance. Cela permet de savoir vers qui se tourner en cas d'attaque, ou même de les rencontrer en amont pour anticiper ce qu'il convient de faire en cas d'attaque.

Pour terminer, grâce aux membres liés aux collectivités (CoTer Numérique, Déclic, l'ANSSI, l'Avicca et la Banque des Territoires), nous avons lancé l'année dernière un programme de sensibilisation des élus en trois volets. Le premier visait à sensibiliser les élus avec une approche assez pragmatique de leurs problématiques notamment via des questions de maires sur la cybersécurité : « pourquoi serais-je attaqué ? »…

Le deuxième volet comportait des témoignages de collectivités ayant été attaquées. Ces témoignages étant anonymisés, j'ai été ravie d'entendre aujourd'hui des collectivités parler à visage découvert, c'est important pour faire avancer les choses. Le troisième volet sortira d'ici la fin du mois de mai, il présentera des témoignages de collectivités ayant mis en place des actions de sensibilisation. Chacun à notre niveau, nous pouvons tous faire des choses, même avec peu de moyens financiers ou humains, ne serait-ce qu'en faisant de l'affichage, par exemple.

Luc DERRIANO

Merci beaucoup pour cette prise de parole au pied levé ! L'Avicca a rejoint la plateforme Cybermalveillance.gouv.fr au 1er janvier 2021. Nous y travaillons au sein d'un groupe qui rassemble aussi les associations de collectivités Déclic et CoTer Numérique sur la préparation de la troisième phase de sensibilisation en direction des élus. Nous avons déjà commencé à identifier quelques collectivités qui ont accepté de témoigner.

Mais il n'y a pas que l'État qui peut apporter des solutions de partage de documents et d'expertise, les collectivités se saisissent également de ces enjeux. La cybersécurité pour certaines d'entre elles s'inscrit dans la transformation numérique des territoires, comme à Bordeaux Métropole. Philippe Steuer, RSSI à Bordeaux Métropole, vous allez nous parler de votre rôle et de ce qui vous a conduit à devenir membre fondateur du Club des RSSI des collectivités.

Philippe STEUER, RSSI - Bordeaux Métropole, et membre du Club des RSSI des collectivités

Merci à l'Avicca pour son invitation et à l'ANSSI pour son soutien régulier. Et merci aux intervenants pour leurs retours d'expérience et la transparence de leurs propos, cela nous permet d'améliorer ainsi nos défenses respectives. Il est clair que nous sommes tous soumis à la

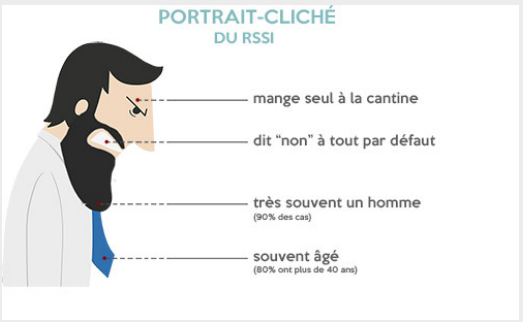
même menace et que nous devons être vigilants face à ses attaques. C'est aussi l'objectif du Club des RSSI que je vais vous présenter.

BORDEAUX MÉTROPOLE

La Sécurité des Systèmes d'Information à Bordeaux Métropole

Colloque TRIP - 12 mai 2021

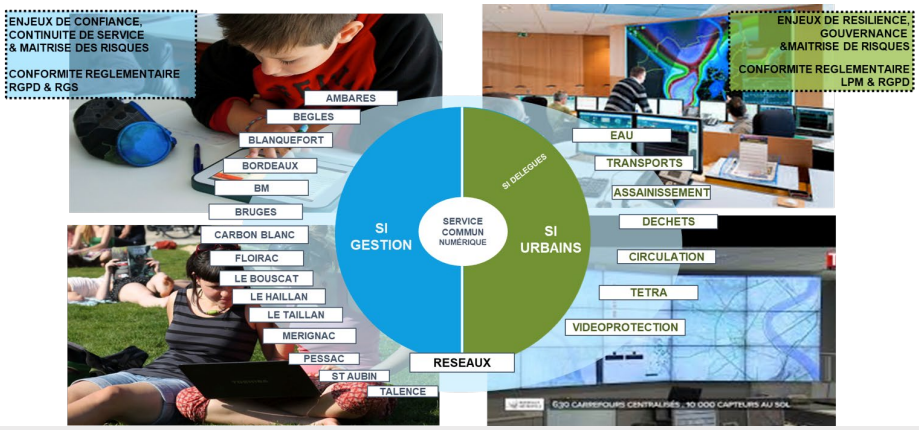
Cybersécurité : de la menace à l'action territoriale



Si vous ne connaissez pas votre RSSI, ce petit portrait-robot vous permettra de le reconnaître !

LE PLAN DE TRANSFORMATION NUMÉRIQUE AU SERVICE DE LA SÉCURITÉ

NOTRE PÉRIMÈTRE DE RESPONSABILITÉ ACTUEL

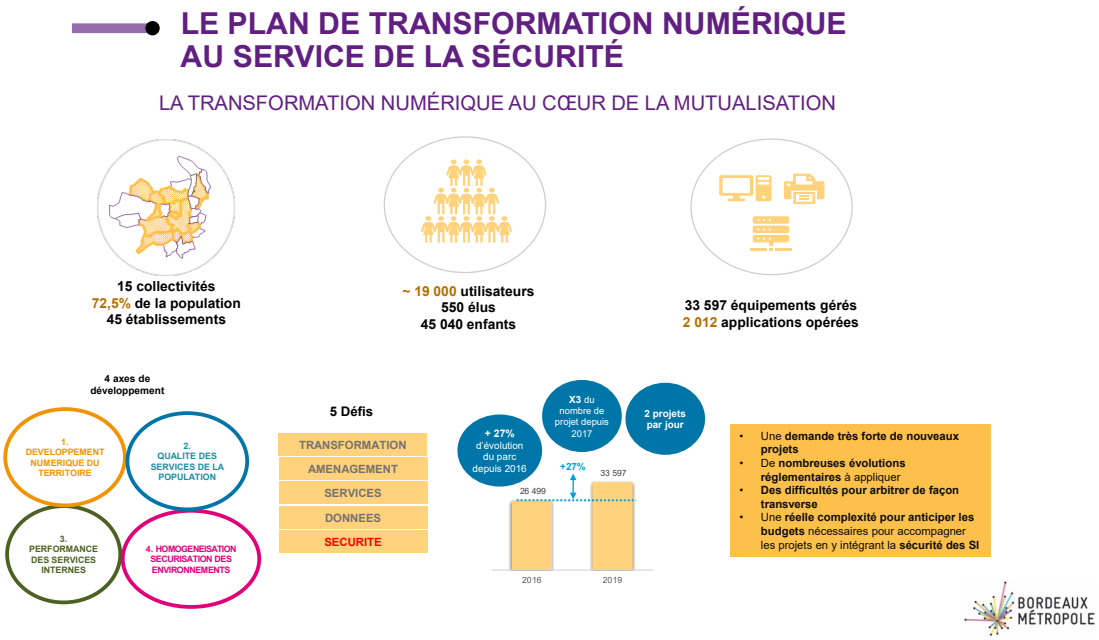


La protection des données et la disponibilité de nos systèmes numériques deviennent stratégiques pour la conduite de nos activités de service public, la confiance numérique des citoyens, ainsi que le respect de la vie privée des usagers et des agents.

BORDEAUX MÉTROPOLE

En tant que RSSI, les actions que je mène au quotidien sont de différentes natures et couvrent des aspects réglementaires : elles portent sur le référentiel général de sécurité, le RGPD pour les données à caractère personnel, la mise en place de la sécurité le plus en amont dans les projets, la mise en place de référentiels comme la politique générale de sécurité des systèmes d'information (PSSI), mais également sur la sensibilisation.

Je commencerai par présenter Bordeaux Métropole vu de son SI pour vous montrer la complexité de celui-ci ou plutôt de ceux-ci, car il y en a deux : un système d'information de gestion et un système urbain, plutôt industriel, avec une couverture géographique de 15 communes sur les 28 que compte Bordeaux Métropole et avec une palette extrêmement ~~et~~ large d'applications informatiques. Il existe en effet de nombreux métiers dans les communes, ce qui implique une grande hétérogénéité des applications et un effort constant de convergence.



Quelques chiffres pour expliquer qui nous sommes. La métropolisation est un vaste programme de transformation qu'il a fallu construire et conduire depuis 2016 pour mutualiser 9, puis 14, puis 15 systèmes d'information totalement hétérogènes, tout en s'adaptant à chaque nouveau cycle d'intégration. Les communes que nous avons intégrées avaient leur système d'information et leurs applications, et il fallait mettre en place un accompagnement au changement.

C'était l'opportunité de faire plus ensemble et de faire converger nos solutions historiques vers des applications plus récentes, mais cela représentait aussi un risque face à l'hétérogénéité des niveaux de sécurité des différentes communes et la complexité de ces SI à gérer. Je rappelle que de nombreuses attaques se font par le maillon le plus faible. Les grandes entités qui ont été attaquées l'ont été par des tiers beaucoup moins sécurisés qui constituent de fait une « porte ouverte ».

Le Club des RSSI est né il y a 15 mois lors du Forum international de cybersécurité (FIC) de Lille en 2020. Cette structure va nous permettre collectivement de prendre un peu de la hauteur et d'avoir une vision globale de la menace et de la cybersécurité dans les collectivités territoriales.

Depuis deux ans, on constate une évolution exponentielle de la menace et des attaques, avec des cas concrets donc vous avez quelques exemples (cf. diapo). L'ANSSI, dans ses différents guides sur l'état de la menace, donne un coefficient multiplicateur par quatre pour les attaques

de type cryptolocker. Par ailleurs, de plus en plus d'élus parlent de l'impact de l'informatique sur leur quotidien et surtout du fait que nous sommes tous complètement dépendants de l'outil numérique aujourd'hui. « *Comment assurer nos missions de services publics sans informatique* » est la question de beaucoup d'élus.

Le Club des RSSI tient à jour une carte des collectivités qui ont été attaquées (cf. diapo, ici une carte qui date de quelques mois).

Pourquoi répondre aux recommandations cyberdéfense ?

REVUE STRATÉGIQUE DE CYBERDÉFENSE FÉVRIER 2018

« Améliorer la cyberprotection des collectivités territoriales »

Soutenir la création, par les collectivités territoriales elles-mêmes, d'un réseau de correspondants en cybersécurité.

Améliorer l'intégration des besoins et des contraintes spécifiques aux collectivités territoriales dans les référentiels de l'ANSSI et dans ses catalogues de produits et services qualifiés.

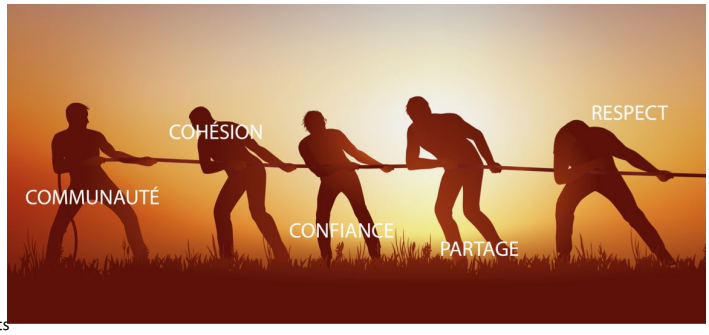
Le Club des RSSI a également été créé pour répondre à la revue stratégique de cyberdéfense de février 2018 (livre blanc sur la cyberdéfense), afin de soutenir la création, par les collectivités territoriales elles-mêmes, d'un réseau de correspondants en cybersécurité d'une part et, d'autre part, pour améliorer l'intégration des besoins et les liens avec l'ANSSI. La volonté est de travailler ensemble, plutôt que chacun dans son coin, pour assurer la cyberprotection des collectivités territoriales, et l'idée était de fédérer la communauté de RSSI.

Qui sommes-nous ?

- C'est l'histoire d'une bande de jeunes RSSI…
  - ✓ Grégory BOUET, Toulouse Métropole, Ville de Toulouse et CCAS
  - ✓ Cyril BRAS, Grenoble-Alpes Métropole, Ville de Grenoble et CCAS
  - ✓ Florian DUMAS, Département de l'Isère
  - ✓ Nicolas LEMAYRIE, Région Occitanie
  - ✓ Jean-Thomas POLETTI, Collectivité de Corse
  - ✓ Philippe STEUER, Bordeaux Métropole
- A vocation nationale, associant les collectivités métropolitaines ainsi que celles des territoires ultramarins
- Avec le soutien de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) dans la mise en œuvre de ce regroupement national des RSSI des collectivités territoriales, initié lors du Forum International de la Cybersécurité (FIC) 2020

Un groupe de RSSI - jeunes et moins jeunes ! - qui a décidé lors du FIC 2020 de travailler ensemble pour expérimenter ce qu'il était possible de faire. Nous avons reçu dès le début le soutien de l'ANSSI qui nous a aidés à mettre en place une interaction plus forte entre nous et l'agence, et en fournissant des moyens, en l'occurrence informatiques. C'est un club à vocation nationale, associant toutes les collectivités métropolitaines, ainsi que celles des territoires ultramarins.

Quels objectifs ?



- Encourager la mutualisation de ressources des CT, à l'échelle d'un ou plusieurs territoires
- Favoriser la communication en matière de sécurité numérique entre les membres, en créant un cercle de confiance et d'échanges
- Favoriser le développement d'une offre de produits et de services adaptée aux besoins spécifiques des CT
- Favoriser l'acculturation à la SSI au sein des différentes CT, organisation de sensibilisation, formation de référent à la cybersécurité…
- Faciliter la communication entre les membres et l'ANSSI, grâce à une organisation connue de tous, en utilisant des moyens et des canaux de communication adaptés

L'objectif principal du Club des RSSI est de permettre aux différents membres d'échanger des informations et de partager des documents ou des ressources, dans un cadre de confiance - c'est très important -, au sein d'une communauté de RSSI, et en relation avec l'ANSSI notamment.

L'objectif est aussi de créer une communauté d'entraide entre ses membres qui offre un cadre de mutualisation des travaux réalisés, des bonnes pratiques que nous avons dégagées des retours d'expérience, et des interactions avec les acteurs de la cybersécurité de manière générale.

C'est également un espace pour mener des actions de groupe vers les éditeurs de solutions. Dans les métropoles et collectivités, nous utilisons tous les mêmes applications (gestion des cimetières, des médiathèques, etc.). Nous menons ainsi des demandes auprès des éditeurs pour pouvoir faire monter le niveau de sécurité, le nôtre mais également celui des fournisseurs.

Il y a également un principe de soutien des membres disposant de ressources importantes vers des structures plus contraintes, afin de regrouper toutes les collectivités, les petites comme les grandes.

Nous avons mis en place une gouvernance avec une réunion mensuelle et la participation de quatre membres de l'ANSSI. Nous proposons des orientations sur des thèmes à traiter. L'année dernière, par exemple, alors que nous étions en plein confinement, nous avons édité un document pour préparer la sortie du confinement d'un point de vue informatique : nous avions ouvert de nombreux systèmes d'information et donné des équipements à nos utilisateurs mais tout n'était pas obligatoirement maîtrisé car la priorité était d'assurer la continuité du service public. Ce guide allait jusqu'à se poser la question de ce qu'il faudrait faire en cas de reconfinement.

Comment s'inscrire dans cette démarche ?

- Note de cadrage
- Charte
- Engagement de confidentialité
- Fiche de renseignements individuels
- Fiche de poste ou lettre de mission SSI

PRINCIPE DE COOPTATION

ADHÉSION GRATUITE ET OUVERTE

- Conseils régionaux
- Conseils départementaux
- Métropoles
- Communautés d'agglomération
- Communauté de communes
- Communauté urbaines
- Communes
- Autres formes de collectivités territoriales
- Syndicats mixtes
- SDIS
- Administrations centrales de l'État

Entre 2020 et 2021, nous étions dans une première phase de démarche progressive. Aujourd'hui, nous sommes dans la phase de déploiement pour le club que nous ouvrons plus largement : l'encadré sur la droite de la diapositive présente une liste non exhaustive des types de structures concernées. Nous avons établi une charte qui décrit les droits et devoirs des membres, et nous avons décidé de limiter l'accès du club aux profils RSSI ou aux personnes ayant des missions de RSSI. Aujourd'hui, nous sommes déjà plus de 100, et pour faciliter les travaux d'intégration des nouveaux membres nous avons mis en place des points de contacts territoriaux.

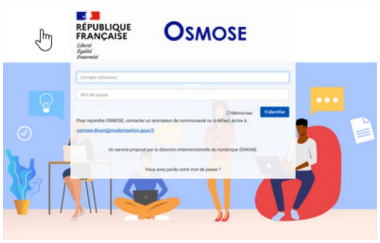
Et quels sont nos outils ?

COLLABORATION + COMMUNICATION + PROTECTION

OSMOSE, plateforme des communautés professionnelles de l'État ≈ 101 inscrits
Espace collaboratif dédié à la communauté Club RSSI administré par le délégué ANSSI, **Rémy DAUDIGNY**

RDSSI, groupe de discussion de RSSI ≈ 120 inscrits
Administré par le RSSI du département de l'Isère, Florian DUMAS

MISP, plateforme d'échange d'IOC ≈ 114 inscrits
Administrée par le RSSI de Grenoble-Alpes Métropole, Cyril BRAS



Nous disposons de trois types d'outils de travail. Le premier est une plateforme d'échanges (Osmose) qui nous a été fournie par l'ANSSI qui compte actuellement plus de 100 inscrits. Sur cet espace collaboratif, nous échangeons des bonnes pratiques, nous travaillons sur des documents communs, etc.

Le deuxième outil est une liste de diffusion appelée RDSSI (plus de 120 inscrits) qui permet d'échanger des informations. Cette liste a potentiellement vocation à disparaître, mais la décision n'est pas encore prise.

Troisièmement, une plateforme qui nous a été fournie par le RSSI de Grenoble pour échanger des indices de compromission en cas d'attaque. Cela nous permet d'anticiper et de fermer le système d'information pour se protéger de menaces qui ont déjà atteint d'autres collectivités territoriales. À ce jour, cette plateforme regroupe 114 personnes.

Hauts de France Grand Est Ile de France Bourgogne Franche Comté	Delphine RIDER – rider@sdis77.fr Eric HAZANE – eric.hazane@ssi.gouv.fr
Bretagne Normandie Centre Val de Loire Pays de Loire	Bruno CAUDAL – bruno.caudal@mairie-vannes.fr pays-de-la-loire@ssi.gouv.fr
Nouvelle Aquitaine Auvergne Rhône Alpes	Philippe STEUER – p.steuer@bordeaux-metropole.fr auvergne-rhone-alpes@ssi.gouv.fr
Occitanie Provence alpes Côte d'Azur	Gregory BOUET – gregory.bouet@toulouse-metropole.fr occitanie@ssi.gouv.fr
Outre-Mer	Nicolas LEYMARIE – nicolas.leymarie@laregion.fr Eric HAZANE – eric.hazane@ssi.gouv.fr

Nous avons également anticipé le fait que ce Club des RSSI devienne assez important en divisant le territoire national en cinq zones, afin d'avoir une gestion facilitée.

Luc DERRIANO

Merci pour cette présentation. Vous avez évoqué le FIC (Forum international de la Cybersécurité à Lille), en quoi est-ce un lieu important pour les RSSI ?

Philippe STEUER

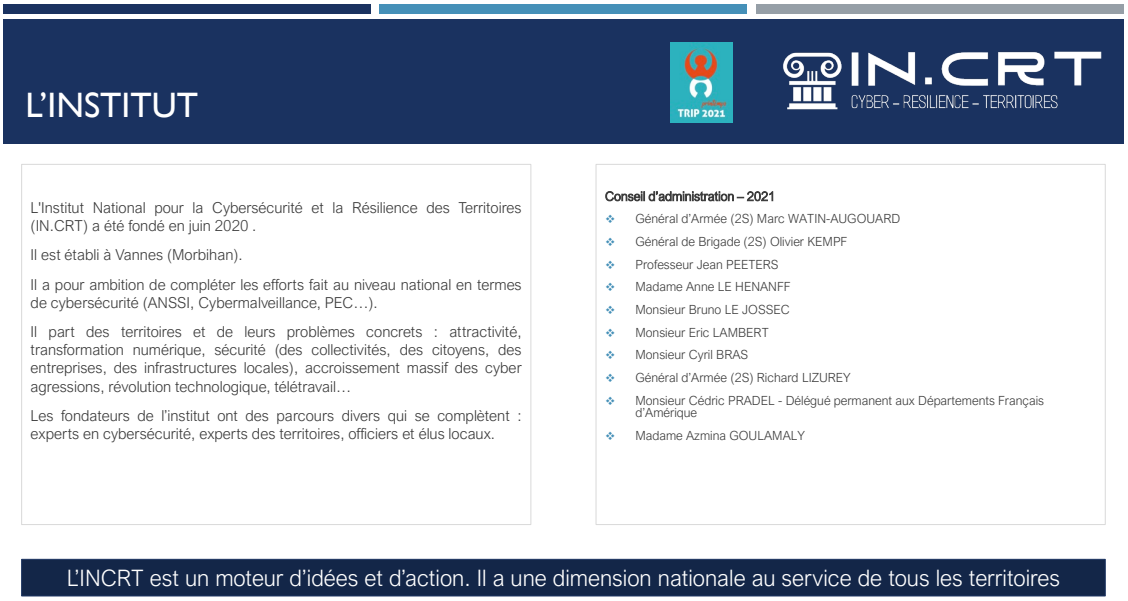
Il existe deux événements en France, l'un au nord (le FIC) et l'autre au sud (les Assises de la cybersécurité). Le FIC est devenu un événement européen extrêmement important pour les RSSI qui peuvent en quelques jours participer à des tables rondes et à des ateliers, et échanger entre pairs. La logique d'échange est primordiale pour notre défense cyber car il faut savoir qu'en face, les groupes de pirates s'organisent (Crime As A Service). Enfin, ces événements permettent de faire une veille technologique mondiale (en quelques jours, sur 20 000 m², on peut découvrir les dernières versions des logiciels de sécurité, etc.). C'est donc en parfaite adéquation avec le Club des RSSI qui prône l'échange, l'entraide et la confiance au quotidien. Cela nous permet également de voir les autorités, les services de renseignement, la cyberdéfense (militaire) sur un même lieu… C'est l'endroit où il faut être quand on fait de la cybersécurité !

Luc DERRIANO

C'est d'ailleurs aussi autour du FIC qu'est né l'IN.CRT (Institut national pour la cybersécurité et la résilience des territoires) dont va nous parler Cyril Bras, vice-président de l'IN.CRT, pour expliquer en quoi consiste cet institut installé en région qui cible plus spécifiquement des collectivités territoriales de taille intermédiaire, et qui veille à la formation et à la mutualisation des RSSI. Pourriez-vous brosser le portrait type de ce Monsieur cybersécurité ?

Cyril BRAS, Vice-président - IN.CRT (Institut national pour la cybersécurité et la résilience des territoires)

Le club des RSSI, auquel je participe aussi activement, est une transition parfaite pour présenter l'IN.CRT.



L'IN.CRT a été créé à l'initiative du même créateur que le FIC, à savoir le Général Marc Watin-Augouard à Lille. Il regroupe un certain nombre d'experts, que ce soit en cybersécurité ou en territoires, des officiers, des élus… J'ai rejoint cet institut en novembre 2020 afin d'y apporter la vision de terrain du RSSI de collectivité que je suis pour la métropole de Grenoble. Il vise à compléter tout ce qui est fait par l'écosystème de la cybersécurité (Cybermalveillance.gouv.fr, ANSSI…) grâce à l'expertise de ses membres.

Pour beaucoup de collectivités malheureusement, la découverte du sujet cybersécurité se fait encore dans la douleur, comme l'ont montré les témoignages précédents que je tiens également à remercier - le retour d'expérience est une démarche forcément profitable à tout le monde, qui fait avancer la cause et favorise la prise de conscience.

C'est aussi ce que prône l'IN.CRT : nous voulons aider cette prise de conscience sur les enjeux de la cybersécurité et les impacts d'une cyberattaque sur une collectivité. Cela passe nécessairement par un apport d'information mais aussi par des solutions concrètes. Le Club des RSSI est une forme d'action que soutient l'IN.CRT, mais nous avons aussi d'autres idées pour agir, d'autres chantiers à venir.

L'objectif est de rendre la cybersécurité accessible à tous. Plus une collectivité est grande, plus elle a de moyens, un service informatique, un RSSI, etc. Inversement, plus on descend dans de petites collectivités, moins le sujet cybersécurité est traité, parce qu'il n'est pas accessible. Une des volontés de l'institut est vraiment d'apporter cette aide et un moyen de monter en compétence pour les EPCI et les communes, ainsi que pour tous les acteurs du territoire. On ne peut pas parler de cybersécurité sans inclure tout le monde, à tous les échelons d'un territoire.

L'institut a vocation à agir au niveau national mais également ultramarin, avec un représentant permanent dans les territoires d'outre-mer, toujours avec cette volonté de considérer que la cybersécurité des collectivités concerne tout le monde. Les cyberattaques, on le voit, se produisent un jour à la Rochelle, le lendemain à Annecy, etc., il s'agit d'un problème vraiment global.

L'institut propose un accompagnement par le biais notamment de la mutualisation de ressources et de compétences. Puisque les petites collectivités n'ont pas la capacité d'avoir un RSSI dédié, on peut imaginer le mutualiser.

Les collectivités devant aussi se soumettre à des obligations légales, l'institut propose de leur apporter une connaissance de ces obligations et comment y répondre.

Cela passe par la création d'emplois au niveau territorial sur le domaine de la cybersécurité. L'institut proposera à partir de la rentrée prochaine une formation visant à créer des RSSI de collectivités pour en faire des acteurs à part entière, accessibles à de petites entités.

La transformation numérique est évidemment en cours dans l'ensemble des collectivités. La capacité à mettre de la cybersécurité et de la résilience va de pair avec cette transformation numérique parce qu'elle permet de garantir la confiance dans l'usage des moyens que l'on veut mettre à disposition.

L'institut envisage de créer un événement annuel qui s'appellera Cyberterritoires. Cet événement aura lieu cette année le 7 octobre à Vannes et il s'adressera avant tout aux élus et aux décideurs mais aussi aux RSSI. L'idée est d'avoir un événement spécifique lié à la cybersécurité, pour l'ensemble de ses acteurs.

- L'institut dispose d'un collège RSSI qui apporte la vision terrain des enjeux de cybersécurité
- Il en ressort notamment la nécessité de :
  - Faire évoluer la perception du rôle et de la fonction de RSSI au sein des collectivités territoriales
  - Lui permettre d'apporter son expertise auprès des élus et des dirigeants
  - D'être un acteur incontournable de la transformation numérique
- Pourquoi ?

En tant que vice-président de l'institut, je suis en charge du collège RSSI. On ne peut pas traiter la cybersécurité si on n'a pas la vision de terrain de ses enjeux. Malheureusement le RSSI n'est pas encore bien connu ou perçu.

Nous devons montrer que le RSSI peut apporter son expertise sur ce sujet complexe auprès des élus et des dirigeants, et ainsi devenir un acteur incontournable de la transformation numérique. En effet, comme le maire d'Angers a pu le dire, « *on a peut-être voulu faire trop de numérique et pas assez de sécurité* », alors que la cybersécurité est un élément incontournable de la transformation numérique.

En effet, on se rend compte que la sécurité informatique est bien souvent perçue comme purement technique et relevant de la DSI. La cybersécurité englobe évidemment la sécurité informatique. Pour l'illustrer, ce schéma présente les trois couches cyber. La première est la couche physique (ordinateurs, box ADSL, câbles, etc.), la deuxième est la couche logique (système d'exploitation, navigateur internet, logiciel de messagerie…). Ces deux couches, c'est la sécurité informatique qui les couvre.

Il existe une troisième couche qui est la couche sémantique, ce que nous, humains, nous comprenons. Aujourd'hui, nous constatons que les cyberattaques se produisent sur ces trois couches. Par conséquent, si l'on se contente de faire de la sécurité informatique, on ne traitera qu'une partie du problème. Il est essentiel de prendre conscience que la cybersécurité dépasse le cadre purement technique et qu'elle vise à protéger l'ensemble du patrimoine informationnel d'une entité.

- Le RSSI est encore perçu comme « *Monsieur NON* »
- Le RSSI doit être un « Monsieur non, MAIS »
  - Trouver la solution adéquate entre le risque et l'usage
  - Faire en sorte que la cybersécurité soit un gage de confiance dans l'usage du numérique

Le RSSI est encore trop souvent perçu comme « Monsieur NON » ; il est vrai que pendant longtemps cela a été sa posture, mais cette posture doit évoluer. Le RSSI doit être un « Monsieur NON MAIS » ; il y a des choses qu'on ne peut pas laisser faire sans courir à la catastrophe, mais il existe des solutions pour permettre le meilleur compromis entre la sécurité et l'usage attendu.

La cybersécurité doit être perçue comme un gage de confiance et non comme un frein à la transformation numérique. C'est un des enjeux que porte l'institut.

- En 2021, un RSSI est un manager pas simplement un technicien !
- Ce fait est plus évident sur sa déclinaison anglaise CISO - Chief Information Security Officer
  - Il fait partie de la C-Suite dans laquelle on retrouve les principaux décideurs d'une structure

En 2021, un RSSI est avant tout un manager et pas simplement un technicien. C'est un expert en cybersécurité, mais ce n'est pas « le gars qui branche des câbles dans une armoire pour faire en sorte que ça marche » !

Il me semble que la déclinaison du terme RSSI en anglais (CISO pour *Chief informations security officer*) permet de mieux percevoir cette transformation. En anglais, tous les directeurs d'une structure font partie de la « *C-Suite* » et le CISO en fait naturellement partie. Il s'agit clairement d'une évolution nécessaire dans la compréhension du métier de RSSI au niveau des collectivités. Cette personne ne doit plus être perçue comme un simple technicien. Le RSSI doit évidemment être capable de comprendre techniquement le sujet pour pouvoir faire des arbitrages pertinents ou aider à faire des choix, mais il doit aussi être un bon communicant parce que le sujet est complexe. Il faut parvenir à le vulgariser, à le faire mieux comprendre par la direction générale ou les élus. Enfin, c'est un métier où il faut savoir se remettre en question en permanence. La SSI évolue ; il y a encore deux ou trois ans, le sujet de la cybersécurité n'existait quasiment pas pour les collectivités, mais l'actualité a rendu ce sujet essentiel.

- Il doit :
  - Être bon techniquement pour faire des choix pertinents
  - Être un bon communiquant pour aider les dirigeants et élus à mieux comprendre les enjeux de cybersécurité
  - Savoir se remettre en question car le domaine de la SSI est en constante mutation
- Panorama des métiers SSI de l'ANSSI
  - Apparition de la fonction de directeur cybersécurité

L'évolution du métier de RSSI est donc indispensable et, sur ce point, je tiens à saluer le travail réalisé par l'ANSSI avec le panorama des fonctions SSI qui dresse la liste de ces métiers, dont celui de RSSI, en détaillant ses attributions et ses missions en 2021, mais qui montre aussi l'apparition de nouveaux métiers, comme la fonction de directeur de cybersécurité qui, à mon avis, devrait apparaître dans les collectivités de grande taille. À Grenoble, par exemple, nous avons des systèmes d'information qui sont vraiment très étendus, qui concernent un nombre important d'agents et qui nécessitent d'avoir les moyens de réaliser cette mission correctement.

- La cybersécurité ne doit plus être perçue comme un frein au développement du numérique mais plutôt comme une condition nécessaire, un gage de confiance.
- Rendre la cybersécurité accessible y compris aux collectivités de tailles plus modestes.

En conclusion, la cybersécurité ne doit plus être perçue comme un frein, mais elle ne doit pas non plus être une option. Il faut qu'elle soit une condition nécessaire à la mise en œuvre de la transformation numérique. Grâce à cela, on garantit une confiance dans l'usage des moyens numériques mis à disposition.

Enfin, l'institut vise à rendre la cybersécurité accessible à tout le monde, en tout cas à toutes les petites collectivités qui ne pourraient pas se le permettre en l'état actuel des choses.

Luc DERRIANO

Merci. D'ailleurs, c'est dans le cadre des territoires intelligents où il faut de la confiance pour que se développent les nouveaux usages et services que l'Avicca s'est saisie de cette question de la cybersécurité.

Nous avons parlé aujourd'hui des atteintes du SI, mais on aurait pu parler du piratage de panneaux d'information à Rousies (dans le Nord, ce 1er mai), des feux de circulation à La Roche-sur-Yon (en mai 2019), ou de l'arrosage automatique à Carquet (dans le Lot)… Ou, plus grave, des ordinateurs d'une usine d'approvisionnement en eau potable en Floride (en février dernier) ou enfin d'un oléoduc aux États-Unis, il y a quelques jours.

La FNCCR prépare justement une étude sur le sujet de la cybersécurité dans les smart territoires. Le chef du département numérique de la FNCCR, Jean-Luc Sallaberry, va nous parler de cette étude qui devrait être rendue publique courant juin.

Jean-Luc SALLABERRY, Chef du département numérique - FNCCR

Merci de me permettre de faire le *pitch* d'une étude qui a été lancée il y a maintenant quelques mois et qui devrait se terminer dans un mois et demi environ. Elle va permettre de balayer un peu tous les sujets évoqués durant cette table ronde : les pratiques et les attaques qui ont été perçues, l'analyse du comportement des collectivités territoriales dans la protection (ou pas), et puis une vision plus globale ou plus nationale de cette approche, de manière à modéliser la maturité des collectivités territoriales en matière de cyberdéfense. L'étude va aborder à la fois la partie juridique et législative de l'environnement cybersécurité qui est assez riche et divers mais pas forcément homogène. Nous verrons s'il y a lieu de prévoir des modifications législatives en la matière.

À travers une enquête auprès des collectivités (plus de 250 ont répondu à un questionnaire et à des auditions), nous avons un retour assez précis sur leurs forces et faiblesses, selon les strates, petites, moyennes ou grandes collectivités territoriales. Nous avons aussi mené des auditions de différents acteurs, notamment l'IN.CRT et l'ANSSI, mais aussi les Archives nationales ou la CNIL, c'est-à-dire des acteurs nationaux qui travaillent sur la sécurisation et la protection des données. Il est important de voir, dans le cycle de la donnée, quelle est l'approche la plus pertinente à construire en matière de cybersécurité.

Comme c'est une étude sur la cybersécurité dans les smart territoires ainsi que dans les smart services, l'enjeu est également de prévoir dans toutes les innovations de services au public ou de services territoriaux, les technologies qui vont être utilisées par les services publics territoriaux, comment cette cybersécurité va pouvoir s'incruster dans ces nouveaux systèmes. Quand on évoque les smart grid, les réseaux de transport, la gestion des données territoriales ou le Cloud, il faut avoir une vision globale et sécurisée des données. Certaines collectivités ont d'ailleurs évoqué l'importance de la notion de confiance de la part des citoyens envers leurs collectivités territoriales et envers les élus et agents publics qui travaillent dans ces services. Cette confiance ne peut exister que si, véritablement, on a le sentiment que tout est sous contrôle. Or, on constate quand même au quotidien que ce n'est pas toujours le cas.

Cette étude arrive à point nommé pour accompagner les collectivités territoriales dans le développement de la cybersécurité et dans la hiérarchisation des investissements dans les systèmes d'information. En effet, les collectivités ont des obligations dans quasiment tous les domaines, mais on voit bien que, si un domaine est capital voire vital en matière

d'investissement numérique, c'est bien celui de la cybersécurité. Les préconisations de l'étude l'évoqueront, mais on peut probablement déjà anticiper le fait qu'il est nécessaire de rendre prioritaires les investissements territoriaux en matière de cybersécurité. Voilà un aperçu du rapport qui sera probablement publié fin juin.

Luc DERRIANO

Y aura-t-il des éléments sur la cybersécurité des capteurs et des smart grid des territoires intelligents ? Les feux de circulation, l'arrosage automatique, les réseaux d'ordinateurs pour les régies de l'eau, par exemple…

Jean-Luc SALLABERRY

On ne va pas entrer dans le détail du code des objets ou des systèmes. Mais sur un certain nombre de nouvelles technologies, de nouvelles approches de réseaux télécoms et de services smart, nous allons essayer d'identifier comment sécuriser et rendre plus matures ces systèmes en matière de cybersécurité. Tout n'est pas vital au même niveau : un réseau d'arrosage automatique n'est pas aussi vital qu'un hôpital régional. Il faut distinguer les différents systèmes d'information, mais cela fait aussi partie du métier du RSSI d'accompagner en interne la priorisation de la sécurisation des systèmes.

Luc DERRIANO

Rendez-vous en juin pour les éléments chiffrés de cette étude. Denis Vermot nous indique que des tests d'intrusion sont réalisés à la CA de La Rochelle.

Denis VERMOT

Nous faisons depuis trois ans des tests d'intrusion : tests d'intrusion interne la première année ; tests d'intrusion externe la deuxième année. Pour la cyberattaque qui nous a concernés, Microsoft a signalé qu'il y avait une faille de sécurité sur le pare-feu que nous utilisions. Nous l'avons mis à jour fin octobre-début novembre, et nous avons réalisé le test d'intrusion externe début décembre. Celui-ci a été concluant puisque nous étions totalement sécurisés, mais malheureusement les cyberattaqueurs avait réussi à utiliser la faille de sécurité pour voler nos comptes et profils d'utilisateur début octobre.

Il est important d'essayer de faire des tests d'intrusion systématiques au moins une fois par an avec un prestataire, parce que les choses bougent très vite… On peut ainsi détecter des outils qui ne sont plus utilisés mais qui restent sur les systèmes informations et qui ne sont plus sécurisés ni mis à jour, et qui deviennent des failles de sécurité.

Luc DERRIANO

Merci à l'ensemble des intervenants d'avoir posé plusieurs jalons importants pour agir ensemble.

Nous avons essayé de parler des attaques mais aussi de la défense. Retenons que le RSSI n'est pas ce « Monsieur NON », plutôt ce « Monsieur NON MAIS »… Et qu'il vaut mieux anticiper, s'organiser, s'outiller avant les attaques. Sur le site de l'Avicca, vous trouverez les guides ou rapports évoqués (ANSSI, AMF, Banque des Territoires) et qui ont déjà été présentés à l'occasion de nos ateliers sur le sujet de la cybersécurité. D'autres ressources seront ajoutées au fil de l'eau dans notre boîte à outils (sites internet incontournables, etc.).

L'Avicca va lancer un groupe de travail sur ce sujet, Seine-et-Marne Numérique a déjà répondu présent pour y participer. Nous espérons qu'il sera rejoint par d'autres de nos membres et que nous pourrons adresser les sujets de montée en compétence sur la sécurité des systèmes d'information de manière générale, et plus spécifiquement sur l'Internet des objets qui concerne les territoires intelligents.

D'autres projets de partenariat sont d'ailleurs à l'étude sur ce sujet.