Les collectivités face aux cyberattaques

Depuis quelques mois, régulièrement, l'actualité fait état d'attaques informatiques contre des établissements publics ou des collectivités. Selon une recension (non exhaustive puisque plusieurs attaques sont demeurées non revendiquées par les pirates, ni signalées par les victimes) du site Numerama, au moins 19 collectivités auraient été victimes de cyberattaques en 2022.

Ces attaques peuvent paralyser les victimes pendant des jours – et, naturellement, un hôpital paralysé pendant des jours, cela peut avoir des conséquences dramatiques ! Mais aussi elles coûtent très cher. On a estimé, par exemple, que le retour à la normale de l'hôpital de Corbeil avait coûté 2 millions d'euros.

Mais, si les pirates obtiennent rarement gain de cause (les administrations ne paient pas les rançons demandées), pourquoi s'obstinent-ils dans ces attaques ? Principalement parce que ces dernières leur permettent de mettre la main sur des milliers, parfois des millions de données personnalisées, parfois très sensibles (comme les données médicales), qui peuvent se revendre très cher.

En un mot comme en cent, la guerre informatique ne fait que commencer et les collectivités – de toute taille, car les pirates s'en prennent désormais aussi bien aux petites communes qu'aux métropoles – auraient tout intérêt à se saisir du sujet sous peine de voir les services publics ravagés, les contribuables ruinés et les données personnelles des citoyens livrées en pâture à toutes sortes d'individus plus ou moins malfaisants ou de sociétés peu scrupuleuses…

Les cyberattaques contre les collectivités locales en 2022

Régions :

- **La Normandie** le 8 décembre,
- **La Guadeloupe** le 21 novembre,
- **Le Centre Val de Loire** le 17 novembre,

Départements :

- **Les Alpes Maritimes** le 9 novembre,
- **La Seine-et-Marne** le 6 novembre,
- **La Seine-Maritime** le 10 octobre,
- **La Collectivité européenne d'Alsace** le 28 septembre,
- **L'Indre-et-Loire** le 11 juillet,
- **L'Ardèche** le 6 avril,
- **Le Centre Interdépartemental de Gestion Grande Couronne** (administration conjointe à plusieurs départements d'Île-de-France) le 28 janvier.

Communes de plus de 5 000 habitants :

- **Brunoy** le 29 octobre,
- **Frontignan** le 26 octobre,
- **Chaville** le 15 octobre,
- **Maison-Alfort** le 27 septembre,
- **Caen** le 26 septembre,
- **Les Mureaux** le 24 septembre,
- **Faulquemont** le 10 juin,
- **Guingamp** en juin,
- **Redon** le 25 mai,
- **Saumur** le 23 mars,
- **Aix-les-Bains** le 22 mars,
- **Communauté de communes de Montesquieu** le 13 mars,
- **Sens** le 5 mars,
- **Communauté de communes Rives de Moselle** le 4 mars,
- **Saint-Cloud** le 21 janvier,
- **Communauté de communes Cœur de Maurienne Arvan** le 15 janvier.

Liste (non exhaustive) établie par le site Numerama

Stéphane Bouché

“Les collectivités sont mal préparées aux cyberattaques !”

Journal des Communes : Pensez-vous que les collectivités territoriales françaises soient bien préparées aux risques de cyberattaque ?
Stéphane Bouché : Malheureusement, les collectivités territoriales sont mal préparées face aux cyberattaques. En effet, ce sont souvent des structures avec des SI hétérogènes (plusieurs noms de domaines, des outils de mobilité mal contrôlés, cas des communautés de communes), réparties sur des territoires vastes, avec des usagers, parfois en télétravail, diversement sensibilisés aux menaces informatiques et aux usages digitaux. Le plan France Relance et la multiplication des attaques médiatisées, ces 3 dernières années, ont généré un regain de sensibilisation à la cybersécurité et parfois des plans d'action, pour les établissements les plus importants. Mais est-ce le cas des plus petites collectivités ?


DR

Stéphane Bouché est le président de Secuserve, société française de cybersécurité.

JDC : Quels sont les types d'attaques les plus fréquents contre les établissements publics ou les collectivités ?
SB : La messagerie est clairement la porte d'entrée principale et initiale (90 %) des malwares et des opérations de phishing. Les cryptolockers (chiffrement des données) avec demande de rançons sont l'attaque la plus lucrative et la plus visible médiatiquement. Toutefois, il ne faut pas négliger les vols d'information par usurpation d'identité via des messages SMS ou courriels. Ces attaques sont souvent destinées à prendre le contrôle des boîtes aux lettres des utilisateurs pour mener ensuite soit des campagnes de SPAM (ce qui nuit à la réputation et délivrabilité des domaines utilisés), soit des *« arnaques au Président »* (détournement de fonds).

JDC : Secuserve travaille dans différents domaines de la sécurité informatique, de la messagerie au stockage. Quels vous semblent les domaines de plus grande vulnérabilité ?
SB : Les attaques évoluent en permanence. Ces derniers mois, nous avons constaté une recrudescence du VISHING (phishing par appel téléphonique), SMISHING (par SMS) et SPEAR PHISHING (introduction dans le SI, par des opérations d'ingénierie sociale unitaires et discrètes). Une fois que l'organisation a mis en place une solution efficace et administrable de sécurité pour sa messagerie (e-securemail par exemple), la

Pixabay

plus grande vulnérabilité reste l'utilisateur final. En effet, il faut trouver le juste équilibre entre sécurité et liberté, et surtout sensibiliser les utilisateurs pour qu'ils deviennent acteurs de la politique de cybersécurité (par des systèmes de rétroaction par exemple).

> **« La plus grande vulnérabilité des systèmes d'information reste l'utilisateur final. »**

JDC : La plupart des grandes sociétés de cybersécurité sont étrangères, ce qui n'est pas votre cas. Y a-t-il une spécificité française en ce domaine ?
SB : La France est le 4e pays en matière d'exposition aux attaques de cybersécurité, et nous disposons d'acteurs EXPERTS en cybersécurité et de groupements spécialisés qui n'ont pas à rougir devant les acteurs anglo-saxons. C'est le cas de SECUSERVE, qui opère depuis 20 ans dans le domaine de la sécurité de la messagerie. Les acteurs français sont plus réactifs, abordent les attaques en langue française avec plus de justesse et d'efficacité. Ils sont également capables de prendre des engagements de résultats supérieurs, tout en respectant les lois françaises et européennes (hébergement des données en France, RGPD, etc.). *A contrario,* les SLA (Service Level Agreement : niveau de service garanti) des acteurs étrangers (Microsoft par exemple) ne portent que sur les SPAM en langue anglaise, sans parler de la pertinence du support des acteurs trop généralistes !

JDC : Quels conseils donneriez-vous à un maire ou président d'exécutif local désireux de se pencher sur la cybersécurité ?
SB : Un maire devra faire réaliser un rapide audit, de mettre en place un firewall pour son réseau, puis de sécuriser sa messagerie, et enfin de s'assurer que des sauvegardes des données et systèmes essentiels sont effectives et déconnectées du réseau. Il faut en parallèle sensibiliser les utilisateurs avec des kits de communication simples (ceux de l'ANSSI sont prêts à l'emploi) : gestion des mots de passe, sécurité des appareils mobiles, usages pro-perso, ne pas cliquer en cas de doute, etc.… Les RSSI (Responsable de la Sécurité des Systèmes d'Information) en temps partagé peuvent être une solution efficace pour les plus petites structures.

Propos recueillis par
Guillaume de Thieulloy

22 propositions pour renforcer la cybersécurité

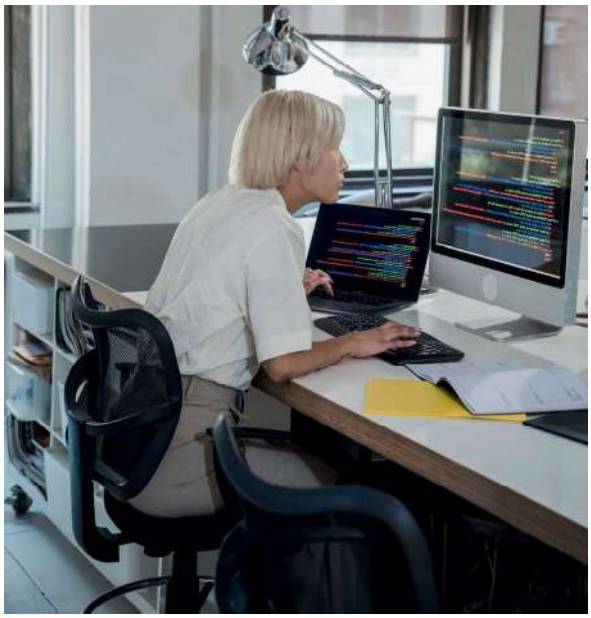
Le rapport de la délégation sénatoriale aux entreprises, présenté par Rémy Cardon (sénateur de la Somme) et Sébastien Meurant (sénateur du Val d'Oise), sur la cybersécurité, présentait 22 propositions pour améliorer la situation.

Proposition n° 1 : Promouvoir davantage le dispositif cybermalveillance.gouv.fr auprès des entreprises et dédier un service d'urgence aux entreprises ; des étudiants disposant des compétences numériques adéquates pourraient y effectuer leur service civique.

Proposition n° 2 : Ouvrir un guichet de recueil anonymisé des cyberattaques frappant les entreprises, afin de disposer de statistiques fiables.

Proposition n° 3 : Décliner des équipes de réponse aux incidents informatiques (CSIRT, Computer Security Incident Response Team) dans les Régions et inclure la cybersécurité dans les schémas régionaux de développement économique, d'internationalisation et d'innovation (SRDEII) afin de sensibiliser les collectivités locales.

Proposition n° 4 : Adapter le droit de la commande publique pour favoriser l'écosystème de la cybersécurité en :
- Pérennisant les dispositions du décret du 24 décembre 2018 au profit des collectivités locales permettant l'achat sans mise en concurrence de « services innovants » ;
- Permettant l'accès à l'offre de cybersécurité en dehors des plateformes de grossistes ;
- Étudiant la possibilité que les opérateurs de réseaux puissent privilégier un achat européen ou national de solutions de cybersécurité.



Proposition n° 5 : Élaborer des plans nationaux de prévention des cyberrisques, afin de coordonner la réponse des pouvoirs publics et des acteurs privés en cas d'attaque numérique systémique affectant une part significative des entreprises quelle que soit leur taille. Des exercices de simulation devraient être régulièrement organisés.

Proposition n° 6 : Renforcer la réponse pénale à la cybercriminalité :
- Développer la formation initiale et continue des magistrats en matière de cybercriminalité ;
- Augmenter les effectifs spécialisés en cybersécurité des forces de sécurité ;
- Doter les forces de cybersécurité de moyens financiers adéquats ;
- Étudier la faisabilité de la création d'un Parquet national de lutte contre le cybercrime ;
- Créer, à chaque degré de juridiction, une chambre spécialisée dans la lutte contre la cybercriminalité.

Proposition n° 7 : Adapter les procédures pénales à la cybercriminalité et renforcer la coopération des institutions judiciaires avec l'ANSSI au-delà de la lutte contre le terrorisme.

Proposition n° 8 : Accélérer les négociations européennes sur le projet de règlement sur la preuve électronique (« e-evidence ») et reprendre les négociations entre l'Union européenne et les États-Unis, afin d'approfondir la coopération internationale concernant la cybercriminalité.

Proposition n° 9 : Prévoir que les salariés doivent se voir proposer une sensibilisation à la cybersécurité, dans le cadre de la formation professionnelle au numérique.

Proposition n° 10 : Déployer une campagne massive de promotion des métiers de la cybersécurité, cofinancée par l'État et les acteurs privés du secteur.

Proposition n° 11 : Réserver à terme l'éligibilité à un remboursement par les assurances aux entreprises ayant eu recours aux services des prestataires labellisés Expert Cyber.

Proposition n° 12 : Interdire l'assurabilité tant des rançongiciels que des sanctions administratives en cas en cas de violation de la réglementation sur la protection des données à caractère personnel, par un amendement à la convention de Budapest du Conseil de l'Europe, par un règlement européen, et par une disposition législative expresse dans le code des assurances.

Proposition n° 13 : Afin de renforcer la conception sécurisée (security by design) :
- étudier l'extension aux entreprises de la « garantie logicielle » concernant les mises à jour de sécurité ;
- organiser, avec le support de l'ANSSI, un « hackathon de la cybersécurité » des entreprises, lors de la Journée mondiale de la cybersécurité, le 30 novembre.

Proposition n°14 : Construire un référentiel accessible aux TPE et PME pour renforcer la certification en matière de cybersécurité.

Proposition n°15 : Sensibiliser les PME sur la responsabilité personnelle des dirigeants en cas de cyberattaque de la chaîne d'approvisionnement dont ils sont partie prenante.

Proposition n°16 : Affermir le marché de l'assurance en matière de cybersécurité par :
- Une meilleure compréhension du risque, en ayant la connaissance la plus exhaustive possible des sinistres ;
- L'utilisation de logiciels et d'experts en cybersécurité certifiés, afin de promouvoir le label ExpertCyber ;
- La création d'une agence de cybernotation européenne, utilisant les référentiels de l'Agence européenne chargée de la sécurité des réseaux et de l'information –ENISA-, ou française, utilisant ceux de l'ANSSI.

Proposition n° 17 : Faciliter la mutualisation des responsables de la sécurité des services informatiques (RSSI) pour les PME, par exemple par la constitution de groupements d'employeurs, ayant un statut de tiers de confiance.

Proposition n° 18 : Développer l'offre d'un « package » simplifié de solutions de cybersécurité aux TPE et PME.

Proposition n° 19 : Accorder aux TPE et PME, dont le champ de l'activité principale n'est pas le numérique, la protection de l'article L.212-1 du Code de la consommation sur les clauses abusives pour les contrats conclus en matière de cybersécurité.

La cybersécurité en chiffres

- Au niveau mondial, la cybercriminalité a coûté **6 000 milliards de dollars** en 2021 (deux fois plus qu'en 2015).
- Si le cyberrisque était un pays, il représenterait la **3e économie mondiale.**
- **43 % des PME françaises** ont constaté un incident de cybersécurité en 2020.
- **16 % des cyberattaques** lancées contre des PME françaises en 2020 menaçaient la survie de la victime.
- Le site gouvernemental cybermalveillance.gouv.fr a connu **une hausse de sa fréquentation de 155 %** en 2020.
- Entre 2020 et 2021, les attaques au rançongiciel ont été **multipliées par 4.**
- Le marché français de la cybersécurité représente un chiffre d'affaires annuel de **13 milliards d'euros.**
- **67 000 personnes** travaillent dans le secteur de la cybersécurité en France.
- En 2023, le marché mondial de la cybersécurité devrait représenter un chiffre d'affaires de l'ordre de **150 milliards de dollars.**
- Le marché mondial du cloud représentait **63 milliards d'euros** en 2021 et il devrait atteindre **560 milliards** d'ici 2030.

Source : Rapport sénatorial sur la cybersécurité des entreprises

Proposition n° 20 : Étudier la faisabilité d'une solution de démarrage rapide configurant l'usage du cloud aux prescriptions de cybersécurité définies par l'ANSSI et d'une approche commune franco-allemande en faveur d'une meilleure prise en considération des PME dans la stratégie commune européenne de cybersécurité dans le cloud, définie par l'ENISA.

Proposition n° 21 : Mettre en place un crédit d'impôt à destination des chefs d'entreprise et des salariés des PME, prenant en charge une partie des dépenses d'équipement et de formation à la cybersécurité.

Proposition n° 22 : Instaurer un cyberscore des plateformes numériques destinées au grand public, afin de sensibiliser les citoyens à la cybersécurité.

Source : Délégation aux entreprises

5 Clés pour une sensibilisation à la cybersécurité réussie

L'Association des Maires de France et Cybermalveillance.gouv.fr ont mis au point un guide pour sensibiliser les agents des collectivités aux risques cyber. Ce guide repose notamment sur 5 clés présentées ci-dessous.

1

- **Prendre conscience** du risque cyber
- **Comprendre les impacts** d'une cyberattaque
- **Reconnaître** les usages à risque

2

- **Adopter** les bons réflexes
- **Atteindre** ses publics

5

- **Confronter les retours** d'expérience
- **Mesurer le taux d'engagement** à la campagne de sensibilisation

3

- **Renforcer ses messages** avec les bons contenus
- **Élaborer un plan d'action** et un calendrier

4

- **Répéter** pour garantir la mémorisation du message
- **Personnaliser** la communication