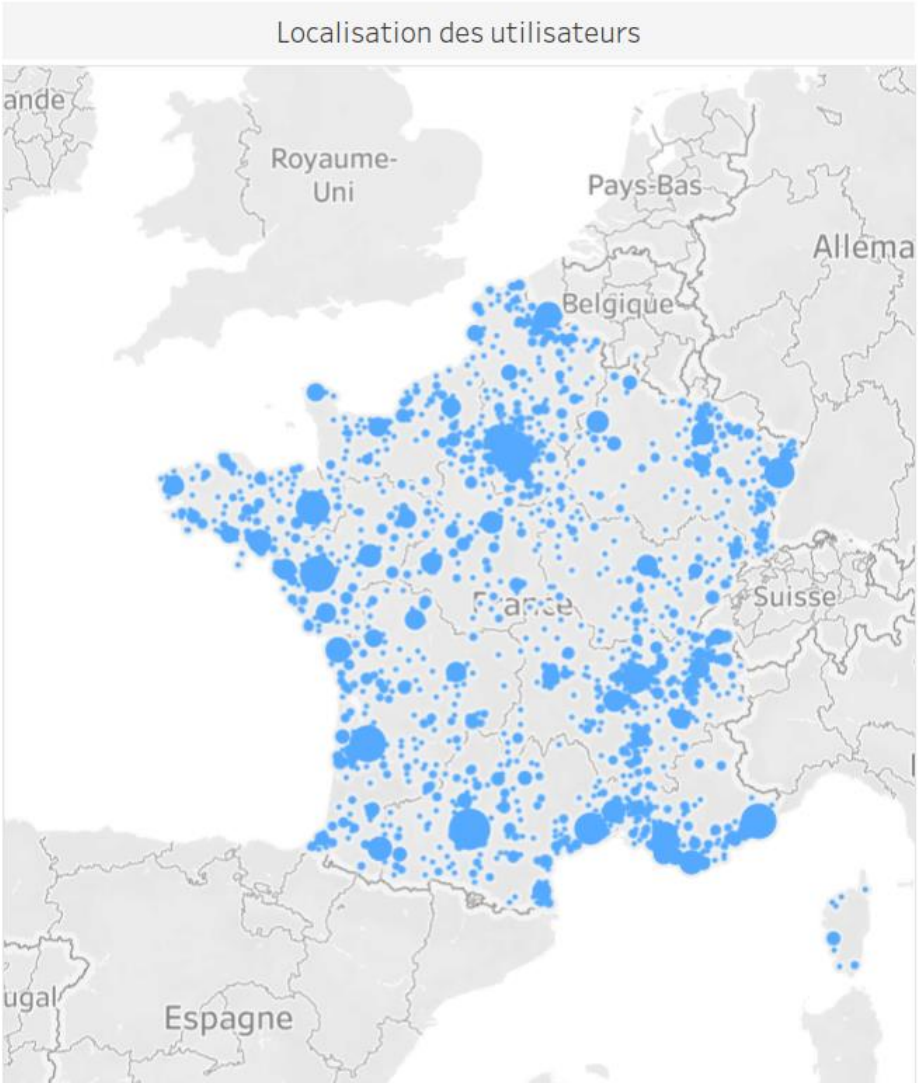
...LA CYBERSÉCURITÉ : ENTREPRISES, COLLECTIVITÉS TERRITORIALES : TOUTES CONCERNÉES !

Le rapport de la délégation sénatoriale aux entreprises établi par Sébastien Meurant et Rémi Cardon a souligné **l'ampleur du risque cyber** pour les entreprises, en particulier les PME, mais aussi pour toutes les organisations territoriales. Ce sujet a été à nouveau largement évoqué lors de la 5ème Journée des entreprises qui s'est déroulée au Sénat le 21 octobre 2021, puis lors de la table-ronde, organisée avec la délégation aux collectivités territoriales le 28 octobre. Suite à ces travaux, il est apparu que **les entités publiques, à savoir les** collectivités territoriales, établissements de santé et établissements publics, **sont également concernées par cette menace qui peut paralyser le fonctionnement du service public**. La réponse appropriée pour réduire cette menace nécessite une synergie des actions publiques et privées.



Source : Cybermalveillance.gouv.fr, 2021

1. UNE PRISE DE CONSCIENCE TARDIVE ET INSUFFISANTE DE L'AMPLEUR DES CYBERMENACES

En 2020, près de 30 % des collectivités territoriales ont été victimes d'une attaque au rançongiciel selon une étude du Clusif[1]. En effet, cette même année a vu le nombre de cyberattaques contre des collectivités territoriales **augmenter de 50 %** par rapport à 2019[2].
En mai 2020, Guillaume Poupard, directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) s'est déclaré « ***inquiet*** »[3] pour la cybersécurité des collectivités territoriales. Pourtant, la cybersécurité était, en 2018, **loin d'être une préoccupation centrale des collectivités territoriales**. Selon un sondage Ifop[4] pour l'Observatoire des Politiques Publiques, en janvier 2020 encore seuls 33 % des fonctionnaires territoriaux interrogés déclaraient que leur organisation avait mis en place un programme de cybersécurité. Le manque de budget et de personnes qualifiées justifie en partie les difficultés des collectivités territoriales en matière de cyberprotection de leurs outils et données numériques.
Les élus locaux prennent désormais, et de manière croissante, la pleine mesure de ce risque. Les associations d'élus accompagnent la prise de conscience des collectivités territoriales, qui demeure inégale sur le territoire. Ainsi, l'Association des maires de France (AMF) a édité en novembre 2020 un **guide** intitulé « *Cybersécurité : toutes les communes et les intercommunalités sont concernées* »,
Faute de temps mais également de compétences et de ressources humaines qualifiées, les petites communes se contentent parfois d'installer ponctuellement un anti-virus, alors que la cybersécurité doit être **mise à jour en permanence**. Or, la pénurie de compétences est telle que l'ANSSI a lancé un « observatoire des métiers de la cybersécurité » afin d'aider les acteurs concernés dans leur politique de recrutement et de formation. Dans ce contexte, la **mutualisation au plus près des collectivités concernées** s'avère être un choix judicieux pour mettre en commun les efforts, affronter les pénuries de professionnels qualifiés et ainsi mettre en place **une protection collective**.

2. LE DISPOSITIF DE CYBERPROTECTION PUBLIQUE

Le bouclier

Il s'articule autour de **l'Agence nationale de la sécurité des systèmes d'information (ANSSI)** et d'un **réseau de CERT (*Computer Emergency Response Team*)**, organismes officiels chargés d'assurer des services de prévention des risques et d'assistance aux traitements d'incidents. Ces CERT sont des centres d'alerte et de réaction aux attaques informatiques, dont les informations sont accessibles à tous. L'objectif du **volet cybersécurité de France Relance**, lancé en septembre 2020 et dont le pilotage a été confié à l'ANSSI, doit renforcer la sécurité des administrations, des collectivités, des établissements de santé et autres organismes publics, tout en dynamisant l'écosystème industriel français.

Doté d'un fonds de **136 millions d'euros**, il comprend :
- **un parcours de cybersécurité** ayant pour objectif de renforcer la sécurité des systèmes d'information des bénéficiaires en proposant un pré-diagnostic et un accompagnement par des prestataires compétents, de la maîtrise d'ouvrage jusqu'à la mise en œuvre ;
- **des appels à projets**, pour certaines collectivités territoriales dont le niveau de cybersécurité est suffisamment mature et le besoin assez clair pour que le projet soit mené hors du cadre des

---

1 *https://clusif.fr/newspaper/le-risque-associe-aux-rancongiciels-demeure-sous-evalue-dans-les-collectivites-territoriales-clusif/*
Le Clusif est l'association de référence de la sécurité du numérique en France.

2 *https://www.lesechos.fr/tech-medias/hightech/flambee-dattaques-informatiques-contre-les-mairies-en-france-1284537*

3 *Face aux membres de la commission de la défense nationale et des forces armées de l'Assemblée nationale : https://www.assemblee-nationale.fr/dyn/15/comptes-rendus/cion_def/l15cion_def1920054_compte-rendu.pdf*

4 *https://2020.forum-fic.com/Data/ElFinder/s23/PDF/20200206-note-cyber-et-territoires.pdf?_t=1581012131*

« Parcours de cybersécurité ». Basés sur le cofinancement et destinés à sécuriser des systèmes d'information existants, ces projets peuvent être des prestations d'audit, d'analyse de risque, d'acquisition et de déploiement de produits... ;

- **le réseau des CSIRT régionaux** (*Computer Security Incident Response Team*), centres de réponse aux incidents cyber au profit des entités implantées sur le territoire régional, devra traiter des demandes d'assistance des acteurs de taille intermédiaire, dont les collectivités territoriales, et les mettre en relation avec des partenaires de proximité : prestataires de réponse à incident et partenaires étatiques.

La prévention et l'assistance aux victimes

Depuis 2017, la plateforme Cybermalveillance.gouv.fr, du GIP ACYMA, dispositif national de **sensibilisation, prévention et assistance** aux victimes d'actes de cybermalveillance pour les particuliers, entreprises et collectivités territoriales, est porté par un **partenariat public-privé**. Outre l'ANSSI et les principaux ministères, cette plateforme rassemble de nombreux acteurs de la société civile comme des associations de consommateurs ou d'aides aux victimes, des représentations professionnelles de type fédération ou syndicat, des assureurs, des opérateurs, des éditeurs de logiciels…
Face à la recrudescence des cyberattaques contre les collectivités territoriales, Cybermalveillance.gouv.fr a créé un groupe de travail dédié à ce public composé de l'ANSSI, l'AVICCA, la Banque des Territoires, le CoTer Numérique et Déclic, et lancé un **programme de sensibilisation** à destination des élus.
Il comporte **trois étapes** :

- Étape une : Menaces et réflexes essentiels pour la sécurité numérique des collectivités
- Étape deux : Vigilance face aux cyberattaques : les collectivités sont toutes concernées !
- Étape trois : Sensibilisation aux risques numériques : les collectivités se mobilisent

Les **ressources documentaires** destinées aux collectivités territoriales sont les suivantes :

- Vidéos de sensibilisation sur les risques numériques
- Campagne de sensibilisation inter-régions sur la cybersécurité
- Supports pour résumer les premiers gestes en cas d'attaque
- I.M.M.U.N.I.T.É.Cyber : questionnaire pour sensibiliser les élus à la cybersécurité

L'enquête et la répression : la CyberGendarmerie et l'autorité judiciaire

Le centre de lutte contre les criminalités numériques (C3N) est chargé d'assurer le pilotage et l'appui spécialisé de l'action de la gendarmerie contre la cybercriminalité et les criminalités numériques, de mener ou coordonner les investigations d'ampleur nationale ayant trait à la cybercriminalité, et de réaliser une surveillance permanente de l'Internet, pour y détecter et collecter les preuves des infractions qui peuvent y être commises. Le réseau d'enquêteurs spécialisés de la Gendarmerie forme une chaîne de 7 000 gendarmes qui seront 10 000 en 2022. Cette montée en puissance s'est traduite par la création le 25 février 2021 **du COMCyberGEND, ou Commandement de la gendarmerie dans le cyberespace.**

Sur le plan judiciaire, le rôle primordial est joué par le **tribunal judiciaire de Paris** qui bénéficie, depuis la loi du 3 juin 2016, d'une compétence nationale en matière d'atteintes aux systèmes de traitement automatisé de données (STAD) et crimes de sabotage informatique. Il existe depuis 2015 une section du parquet de Paris dédiée au traitement de certaines affaires de cybercriminalité, notamment les plus complexes, aux effectifs toutefois modestes. Au-delà, les juridictions interrégionales spécialisées (JIRS) connaissent de plus en plus de contentieux de la cybercriminalité, notamment celle liée à la criminalité organisée.

#CYBERATTAQUE

Délégation aux collectivités TERRITORIALES

Délégation aux ENTREPRISES

QUE FAIRE EN CAS DE CYBERATTAQUE ?

1 **Déconnectez du réseau** tous les ordinateurs infectés, ainsi que les disques externes et autres terminaux reliés.

2 **Contactez des prestataires externes expérimentés en neutralisation des attaques informatiques.** Vous pouvez faire appel à **votre assurance.** L'ANSSI propose également une liste de prestataires habilités.

3 **Portez plainte** auprès de la gendarmerie ou du commissariat de proximité. Vous pouvez aussi adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent. **Des services spécialisés se chargent ensuite de l'enquête.**

4 Si des **données à caractère personnel** ont été dérobées, **avertissez la Cnil** dans les 72h.

5 Si vous êtes un **opérateur d'importance vitale, prévenez l'ANSSI** dans les meilleurs délais.

6 Vous pouvez également **signaler les faits** via la plateforme de signalement **« Pharos »** ou le numéro dédié : 0811 02 02 17.

7 En parallèle, si nécessaire, vous pouvez élaborer un plan de communication pour rassurer vos usagers.

ET APRÈS ?

Consultez le site **CYBERMALVEILLANCE.GOUV.FR**. Il peut **vous mettre en relation avec des prestataires de services informatiques de proximité agréés (cyber-experts) pour remettre votre système en état de fonctionnement et le sécuriser.**
Une fois l'incident terminé, **prenez des précautions** :

- sauvegardes et mises à jour régulières des logiciels
- sécurisation de la borne d'accès internet
- souscription d'un contrat d'assurance spécifique

NOVEMBRE 2021

www.senat.fr