RENCONTRES TERRITORIALES

CYBER SÉCURITÉ

PARTIE 1

Présentation générale

CONTEXTE GÉNÉRAL

- **Hausse exponentielle du risque cyber : transformation numérique, nouveaux enjeux géopolitiques…**

- **Quelques chiffres :**

6 000 milliards de dollars : coût de la cybercriminalité mondiale (2021)

23% des cyberattaques concernent les collectivités territoriales (2022)

- **Une véritable menace pour les institutions publiques et les entreprises (espionnage, sabotage informatique, rançongiciels)**

ÇA LEUR EST ARRIVÉ…

« Dans la nuit du 14 au 15 octobre 2022, les serveurs informatiques de la mairie de Chaville ont été victimes d'une cyberattaque organisée et de grande ampleur. Malgré la réactivité et la mobilisation de la mairie, les services municipaux subissent pour l'instant une forte ***paralysie de leur activité.*** *»* *Site de la commune octobre 2022*	**COMMUNE DE CHAVILLE (20 000 hab)**
VILLE D'ANGERS (151 000 hab)	*« Nous n'avons plus la capacité à pouvoir produire le suivi de nos missions administratives. On ne peut* ***pas délivrer, par exemple, un extrait d'acte de naissance.*** *»* *Christophe Béchu, Maire - 2021*
« La rançon s'élève à 95 000 euros. Le collectif de cybercriminels (…) a décidé de mettre la pression sur l'établissement ***en publiant (des) pièces d'identité ou des attestations médicales*** *des résidents et des documents administratifs. »* *76Actu 25 octobre 2023*	**EHPAD (département de la Manche)**

ÇA LEUR EST ARRIVÉ…

« La Ville de Betton a été victime d'une cyberattaque dans la nuit du 30 au 31 août 2023, à la suite de laquelle environ 2% de nos fichiers ont été exfiltrés et divulgués sur le Dark Net, le 16 septembre dernier. *Une campagne d'information est en cours afin de prévenir les personnes concernées de la* ***diffusion de données sensibles****. »l* *Site de la commune septembre 2023*	**VILLE DE BETTON** **(12 000 hab)**

RÉGION NORMANDIE	*« La cyberattaque qui a touché la Région Normandie en décembre 2022* ***a coûté des centaines de milliers d'euros »*** *Ouest France 10/03/23*

UNE MENACE RÉELLE POUR LES COLLECTIVITÉS

L'ANSSI constate que la menace touche de moins en moins d'opérateurs régulés et se déporte sur des entités moins bien protégées.

- **Les collectivités manquent de moyens**, financiers et humains, pour faire face aux risques numériques
- Elles détiennent des **données sensibles** (données d'identité, sociales, de santé…)
- Elles fournissent les **services numériques** indispensables à leurs habitants.

→ **Elles constituent donc des cibles réelles**

UNE OBLIGATION CROISSANTE

La directive NIS 2 :

- *Network and Information Security, version 2* : vise à **harmoniser et à renforcer la cybersécurité sur le territoire européen**. Publiée au journal officiel de l'UE du 14 décembre 2022, **elle devra être transposée par les Etats-membres d'ici le 18 octobre 2024.**
- En France, de nombreuses entreprises et administrations **seront soumises à cette nouvelle règlementation.**
- Les collectivités, qui étaient exclues du périmètre de la précédente directive, **sont désormais inclues dans NIS 2**, comme les structures privées.
- Pour la 1ère fois, une obligation de **moyen en matière de cybersécurité** sera donc introduite à leur égard

UNE CYBERATTAQUE : QUELS IMPACTS POUR LES COLLECTIVITÉS ?

- **Désorganisation ou arrêt des services**
- **Perte, dégradation, diffusion de données**
- **Coût financier**
- **Risque en termes d'image et de confiance**
- **Conséquences pour les agents**
- **Responsabilité juridique :** https://mairesdefrance.com/cybersecurite-obligations-responsabilites-collectivites-article-2035-0

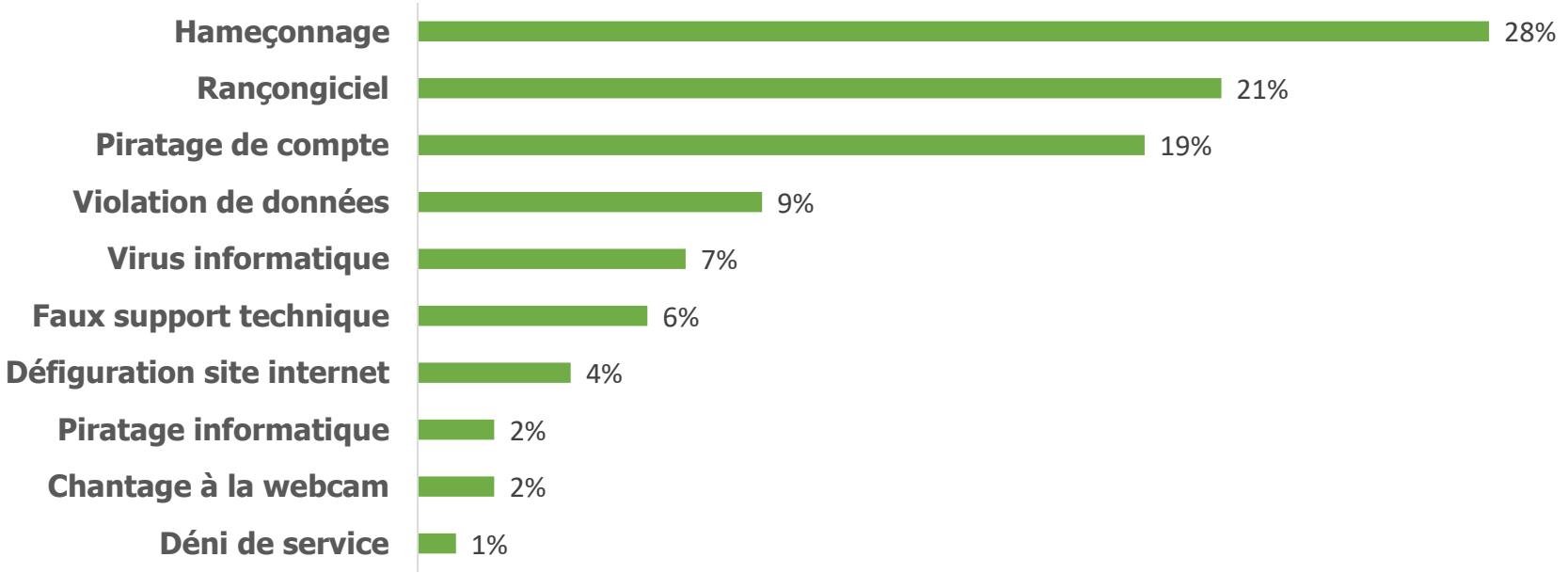
➢ **La responsabilité administrative : la Cnil sanctionne la méconnaissance des dispositions relatives à la loi n° 78-17 du 6/01/1978 relative à l'informatique, aux fichiers et aux libertés et/ou au RGPD**. Les administrés ou entreprises peuvent engager la responsabilité d'une collectivité pour faute lorsque cette dernière a manqué à ses obligations et réclamer l'indemnisation des préjudices subis. La responsabilité de l'administration s'applique pour dommage de travaux publics (par exemple, si une cyberattaque génère le dysfonctionnement d'une installation ou d'un ouvrage public occasionnant des dommages aux usagers).

➢ **Un élu ou un agent public peut voir sa responsabilité civile engagée sur son patrimoine personnel** pour réparer des dommages causés aux tiers, si l'existence d'une faute «détachable du service » est établie. Elle est caractérisée lorsque les faits reprochés révèlent de préoccupations d'ordre privé, procèdent d'un comportement incompatible avec les obligations s'imposant dans l'exercice de fonctions publiques ou relèvent une particulière gravité.

➢ **La responsabilité pénale d'un élu et d'un agent peut résulter de la violation des règles relatives à la protection des données personnelles** (le Code pénal réprime les atteintes les plus graves aux règles du RGPD) ou de la commission de fautes d'imprudence ou de négligence (qui peuvent trouver à s'appliquer juridiquement au cas d'une cyberattaque conduisant à des atteintes aux personnes).

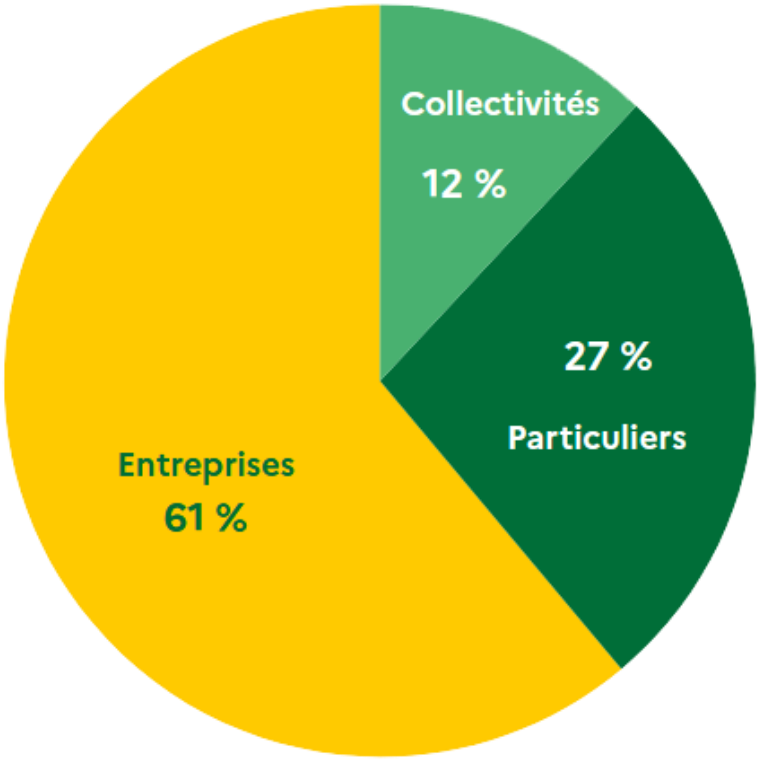
UNE CYBERATTAQUE : COMMENT CELA ARRIVE ?

Principales recherches d'assistance pour les collectivités et administrations :



Source : www.cybermalveillance.gouv.fr - Rapport d'activités 2022

RANÇONGICIELS : PRINCIPALE MENACE POUR LES PROFESSIONNELS



+95% de hausse en 2021 par rapport à 2020

Source : www.cybermalveillance.gouv.fr

POUR VOUS ACCOMPAGNER

L'Agence Nationale de la Sécurité des Systèmes d'information (ANSSI)

Défendre les systèmes d'information critiques de la Nation et structurer au niveau national l'assistance aux victimes de cyberattaques

Agence régionale en Normandie - votre délégué : M. Eric HAZANE

France Relance

Offrir à chaque acteur, **un accompagnement adapté** à son niveau de sécurité informatique

AD Normandie

Accompagner les entreprises et collectivités de taille intermédiaire dans leurs démarches en matière de sécurité numérique (avec NORMANDIE CYBER)

NORMANDIE CYBER
CENTRE DE RÉPONSE AUX INCIDENTS CYBER

0 808 800 001
[service gratuit - prix d'un appel local]
Un service opéré par l'AD Normandie

Cybermalveillance.gouv.fr

Assister les différents acteurs du territoire victimes de cybermalveillance et les informer sur les menaces numériques et les moyens de s'en protéger

QUID DES SYTÈMES DE PROTECTION ?

Les moyens matériels

- **Les incontournables :** nom de domaine, boîte mail sécurisée, anti-virus, antispam, mises à jour régulières, gestionnaire de mots de passe, sauvegarde sécurisée…
- **Les prioritaires :** pare-feu, filtrage URL, VPN, mots de passe complexes, chiffrement de disques durs, sauvegardes externalisées, NAC…
- **Les systèmes plus avancés :** EDR, SOC, sauvegardes immuables …

Mais le plus important reste le **facteur humain** qu'il faut sans cesse renforcer (sensibilisation, formation)

"Une chaîne n'a que la force de son maillon le plus faible"

ET LE CDG14 DANS TOUT ÇA?

- Accompagne les collectivités et établissements publics dans leurs **obligations de conformité RGPD**, depuis 2019, avec 2 DPO.
- **Collecte et partage** de plus en plus de données avec les collectivités (santé, carrière …)
- **S'engage** à aider les collectivités à **renforcer leur sécurité numérique**