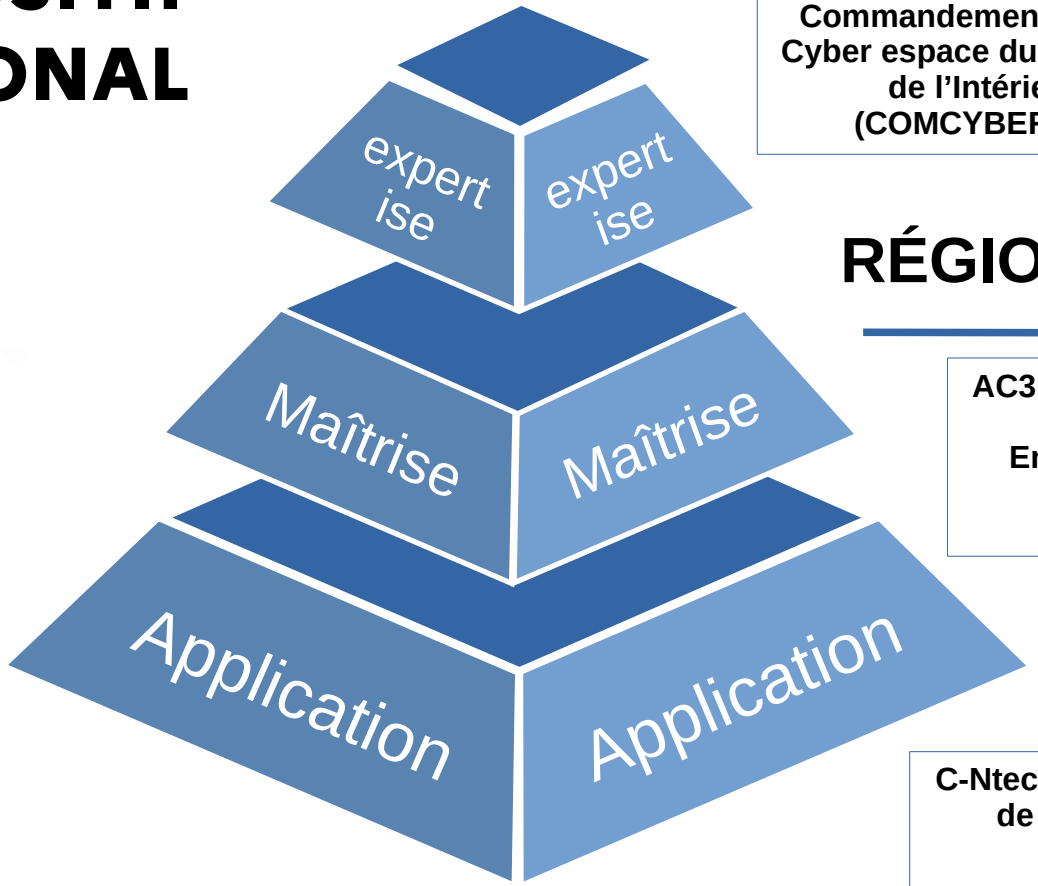
UNE CYBER ATTAQUE, ÇA N'ARRIVE PAS QU'AUX AUTRES...

DISPOSITIF NATIONAL



NATIONAL

Commandement dans le Cyber espace du Ministère de l'Intérieur (COMCYBER_MI)

Unité Nationale Cyber (UNC)

Centre de lutte Contre la Criminalité Numérique (C3N)

RÉGIONAL / DÉPARTEMENTAL

AC3N – Conseiller cyber – Section Appui Judiciaire
Bureau Appui Numérique
Enquêteurs Nouvelles Technologies (NTECH) / Section Opérationnelle de Lutte contre les Cybermenaces (SOLC)

LOCAL

C-Ntech / Introduction aux Cyber Menaces – Brigades de recherches – Communautés de Brigades – Brigades Territoriales

EN RGNA

- 1 officier conseiller cyber zonal
- 1 section cyber de 30 réservistes citoyens
- 1 AC3N, 4 Sections de Recherches
- 1 officier conseiller cyber et 1 sous-officier expert cyber dans chaque département
- 34 NTECH et 873 C-NTECH

RÉPARTIS DANS LES 12 DÉPARTEMENTS

L'OFFRE DE SERVICE GENDARMERIE

1 AVANT LA CRISE

Sensibilisation, prévention, PCA/PRA

2 PENDANT LA CRISE

Le dépôt de plainte, « 17 » en cas d'urgence

3 APRÈS LA CRISE

Temps de l'enquête et de l'accompagnement

REMÉDIATION

LE PRÉ-DIAGNOSTIC CYBER

Evaluation maturité Cyber

Opérations de sensibilisation

Pré-diagnostic élémentaire

Accompagnement en cas d'attaque

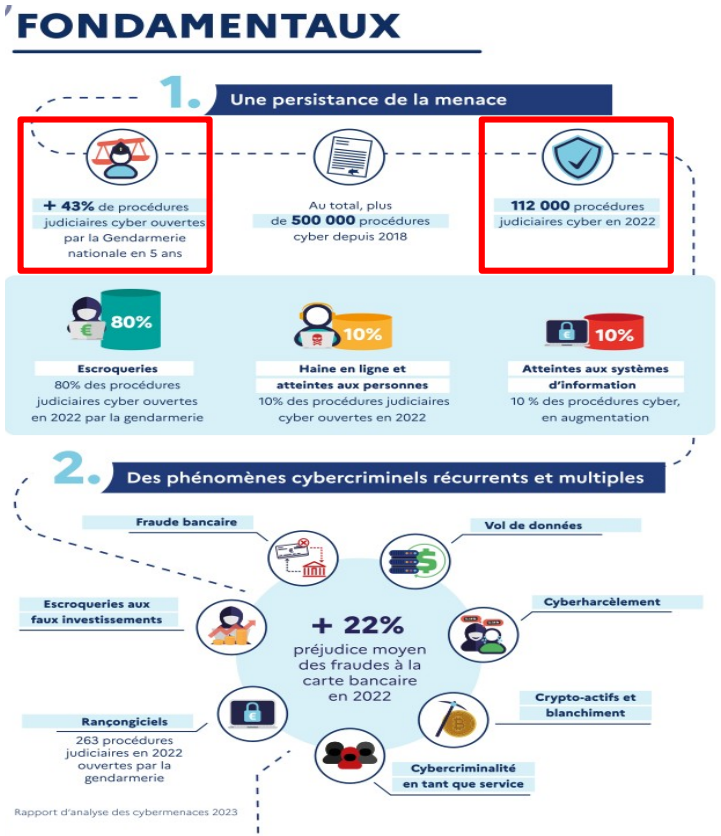
#PrésentsPourLesÉlus

LE PRÉ-DIAGNOSTIC CYBER

di@G@Nal

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

LE PRÉ-DIAGNOSTIC CYBER



JOP 2024
ÉLECTIONS

Finalité lucrative

Campagne de déstabilisation

Opérations d’espionnage

ETAT DE LA MENACE

Déni de Service Distribué (DDOS)

Le DDOS, ou « Déni de Service Distribué », est une attaque informatique visant à saturer un site web ou un service avec des requêtes illégitimes.

Attaque simple et rapide à mettre en oeuvre

METEO FRANCE
À VOS CÔTÉS, DANS UN CLIMAT QUI CHANGE

Avril 2023

LA POSTE

Février 2024

CRÉDIT AGRICOLE

Février 2024

Réseau Interministériel de l'État
Système d'information et de communication de l'État

Mars 2024

CENTRE HOSPITALIER UNIVERSITAIRE DE NANTES

Janvier 2024

COÛT MOYEN D'1 MN D'INDISPONIBILITÉ DU SERVICE : ENV 3000€

+11 % en 2023

LIENS UTILES

LES ESSENTIELS

DÉNIS DE SERVICE DISTRIBUÉS (DDOS *)

1/ CONSTRUIRE ET PROTÉGER

→ **Acquérir et mettre en œuvre un service de protection anti-DDoS dédié à cette seule fonction** :

> auprès de votre hébergeur en cas d'hébergement externe, celui-ci pouvant déjà intégrer une prestation anti-DDoS, en fonction de l'offre d'hébergement souscrite ;

> et/ou auprès d'un fournisseur d'accès à Internet (trou noir, dépollution des flux **) ;

> et/ou auprès d'un fournisseur de service professionnel (déroutement, dépollution des flux **).

Dans tous les cas, sa mise en œuvre nécessite une prise en main préalable, un paramétrage adapté au trafic de l'entité et aux applications exposées et des tests réguliers de la solution pour s'assurer de son bon fonctionnement et de l'absence d'effet de bord.

→ **Protéger son site Web avec un CDN (*Content Delivery Network*) pour la répartition de charge.** Les CDN permettent la répartition de ressources sur un grand nombre de serveurs, ce qui peut contribuer à améliorer la résistance aux attaques DDoS. **Une attention doit être portée au fait qu'une partie de ces ressources peut être hébergée à l'étranger (impact potentiel en confidentialité).**

→ **Configurer les pare-feux en coupure d'Internet** :

> activer uniquement un filtrage au niveau réseau et transport (niveaux 3 et 4 du modèle OSI) et désactiver les fonctions de filtrage applicatif (niveaux 5 et plus) ;

> réduire les flux UDP entrants au strict nécessaire.

→ **Restreindre au strict besoin opérationnel les services exposés à Internet.**

→ **Concevoir les services exposés à Internet de façon à ce qu'une attaque DDoS sur un service n'ait pas d'impact sur la disponibilité des autres services** (chaînes d'accès Internet distinctes, segmentation des plans d'adressage réseau, hébergeurs distincts, etc.).

→ **Concevoir les architectures de telle sorte qu'un service exposé à Internet qui subit une attaque DDoS puisse continuer à être administré malgré cette attaque** (réseau d'administration physiquement dédié, cloisonnement réseau des flux de supervision, etc.).

(*) L'acronyme anglais DDoS pour *Distributed Denial of Service* est le plus couramment utilisé.

(**) Par exemple, la dépollution des flux peut faire intervenir des critères de géolocalisation, de conformité protocolaire, d'inspection de paquets et de volumétrie par protocole susceptible d'être utilisé dans les DDoS (ex. : DNS en UDP, NTP, CHARGEN).

V1.1 (12/23)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

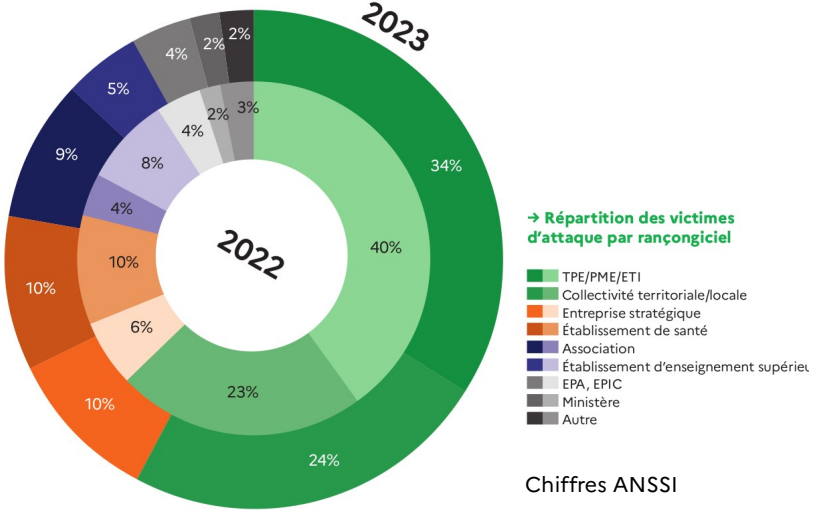
https://cyber.gouv.fr/sites/default/files/document/anssi_essentiels_denis-de-service-distribues_v1.1.pdf

ETAT DE LA MENACE

Rançongiciels (Ransomwares)

Décembre 2023

Octobre 2023



Chiffres ANSSI

2023 : +30 % de faits de rançongiciels portés à la connaissance de l'ANSSI par rapport à 2022

ETAT DE LA MENACE

Fraude au faux conseiller bancaire

L’attaquant contacte la victime par téléphone

Se fait passer pour un conseiller pour lui soutirer des fonds

Attaquant

Gain financier

Fraude au faux conseiller bancaire

ACTES PRÉPARATOIRES

RÉCUPÉRATION DE DONNÉES

- **Leak sur le dark web**

ANONYMAT

- **Modification de voix**
- **Usurper un num tph (spoofing)**

SCRIPT DE COMMUNICATION

Notamment sur l’urgence à agir

Fraude au faux conseiller bancaire

Comment s’en prémunir ?

- ***Votre banque ne vous demandera jamais de réaliser des opérations bancaires via les outils d’authentification mis à votre disposition sur votre application bancaire.***

- ***Ne communiquez jamais vos codes de confirmation.***

- ***Si vous avez un doute, raccrochez et contactez immédiatement votre banque pour vérifier que vous avez le bon interlocuteur.***

- ***Si vous avez été victime de ce type de fraude, modifiez vos codes d’accès à votre espace bancaire, contactez votre banque et déposez plainte sans délai dans une brigade de gendarmerie ou un commissariat de police.***

PLATEFORME PERCEV@L

LES SIGNALEMENTS

En 2022

304 923

signalements enregistrés au total

Une moyenne de

835

signalements par jour

La plateforme avait enregistré au total **324 594** signalements sur l'ensemble de l'année 2021.

LES PRÉJUDICES

En 2022

161 350 088 €

(Contre **140 109 653 €** en 2021)

Hausse du préjudice total

+ 15 %

Le montant moyen s'est élevé à **529 €** en 2022

+22 % de hausse du préjudice moyen en 2022

MINISTÈRE
DE L'INTÉRIEUR
ET DES OUTRE-MER
Liberté
Égalité
Fraternité

POURQUOI DÉPOSER PLAINTE ?

VICTIME D'UNE CYBERATTAQUE

CONTACTER LE 17 OU LA BNUM SUR Ma Sécurité
Site internet

Le dépôt de plainte permet **L'INTERVENTION D'UN BINÔME ENQUÊTEUR / TECHNICIEN** capable de conseiller sur les investigations numériques et les choix stratégiques à mener.
Des **EXPERTS DE LA GESTION DE CRISE DE LA GENDARMERIE** peuvent prendre en charge les interactions avec le cyberdéliquant.

Alerter au plus tôt c'est **PRÉSERVER LES PREUVES NUMÉRIQUES** pour identifier l'attaquant et bénéficier de conseils pour faire cesser l'attaque.
Anticiper le dépôt de plainte permet de faire gagner du temps.

La **TRANSPARENCE** implique la **CONFIANCE**.
L'intervention de la GN peut **RASSURER** l'éco-système de l'entreprise sur la gestion de l'incident.

L'intervention de la gendarmerie n'a **AUCUN IMPACT** sur la reprise d'activité. Les experts de la gendarmerie reccueillent les éléments de preuves en étroite collaboration avec les équipes opérationnelles.

La victime concerve à tout instant la maîtrise de sa communication de crise.

Seul face à la crise ?
Une plainte, est-ce utile pour sortir de la crise ?
Perdre du temps précieux dans la crise
Risquer d'entâcher la confiance
Ralentir les actions de remédiation visant la reprise d'activité
Préserver l'image de l'entreprise

POUR AGIR ENSEMBLE
DÉPASSEZ VOS CRAINTES

Être reconnu en tant que victime
Agir en citoyen
Lutter contre la cyber-criminalité
S'entourer d'un allié dans la crise
Se protéger de futures attaques
Faire valoir ses droits

Victime mais pas coupable !
Le dépôt de plainte permet d'obtenir **RÉPARATION DU PRÉJUDICE.**

Le dépôt de plainte est le seul moyen **D'INFORMER** les forces de sécurité intérieur des menaces qui pèsent sur les citoyens.
Signaler c'est **PROTÉGER ET PARTICIPER À L'EFFORT COLLECTIF.**

Le dépôt de plainte permet de **RECUEILLIR DES ÉLÉMENTS DE PREUVES NUMÉRIQUES** qui permettent d'investiguer et peser sur les organisations cybercriminelles.

La gendarmerie vous **ACCOMPAGNE DANS LA GESTION DE LA CRISE**, grâce à des équipes projetables aux compétences intégrées, dédiées à l'identification des cybercriminelles.

Le dépôt de plainte permet de bénéficier de **L'EXPERTISE DE LA GENDARMERIE** dans la protection de l'entreprise.
La gendarmerie peut détenir des éléments permettant à l'entreprise de récupérer ses données en cas d'attaque par rançongiciel.

L'ASSURANCE CYBER permet à l'entreprise de limiter les conséquences économiques d'une cyberattaque.
La LOPMI (Art.5) soumet l'indemnisation des préjudices d'une cyberattaque au **DÉPÔT DE PLAINTE DE L'ENTREPRISE.**

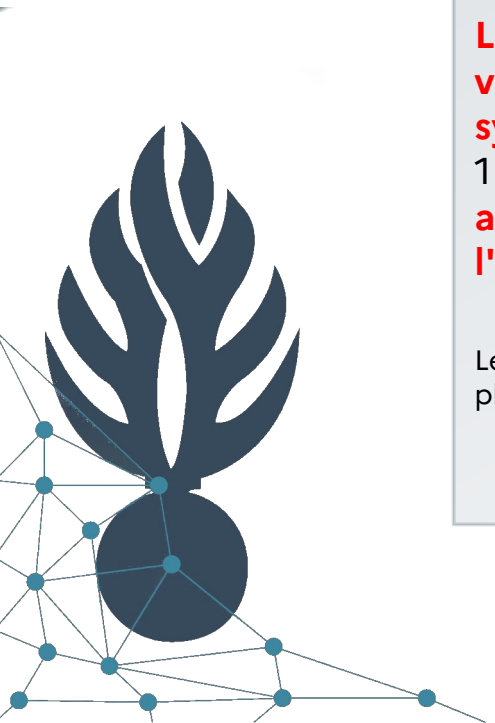
Gendarmerie nationale

LE DÉPÔT DE PLAINTE

Nécessité d'une plainte pour le remboursement par une assurance
Article L12-10-1
Version en vigueur depuis le 24 avril 2023
Création LOI n°2023-22 du 24 janvier 2023 - art. 5 (V)

Le versement d'une somme en application de la clause d'un contrat d'assurance visant à indemniser un assuré des pertes et dommages causés par une atteinte à un système de traitement automatisé de données mentionnée aux articles 323-1 à 323-3-1 du code pénal **est subordonné au dépôt d'une plainte de la victime auprès des autorités compétentes au plus tard soixante-douze heures après la connaissance de l'atteinte par la victime.**

Le présent article s'applique uniquement aux personnes morales et aux personnes physiques dans le cadre de leur activité professionnelle.



Gendarmerie nationale

LE DÉPÔT DE PLAINTE

Lors d'une attaque, le déclenchement de la phase judiciaire est une priorité.

Il se matérialise par le dépôt de plainte qui permet d'enclencher l'action de la gendarmerie et par la suite de la justice. Au-delà de contribuer à faire cesser l'infraction, la gendarmerie est en effet en mesure du vous appuyer tout au long de la crise :

- Négociations
- Investigations
- Traçage de la rançon

LE DÉPÔT DE PLAINTE

Action à effectuer par la victime

En cas de comportement inhabituel de votre ordinateur vous pouvez soupçonner une intrusion (activité importante, connexions inhabituelles, fichiers créés ou modifiés sans votre intervention…).

Il faut déconnecter la machine du réseau mais la maintenir sous tension et ne pas la redémarrer.

Action à effectuer par le technicien informatique

Pour un serveur local :
→ Copie d'écran
→ Effectuer une image du disque dur

Pour un serveur dédié – Site internet :
→ Demander les copies des logs auprès de l'hébergeur
→ Relever l'URL du site
→ Relever le nom de l'hébergeur du site
→ Relever l'adresse IP de l'attaquant
→ Relever le nom de l'équipe ou de l'attaquant

Le dépôt de plainte

Vous devrez déposer plainte auprès de la brigade de Gendarmerie ou du service de Police territorialement compétent.

LES PREUVES PÉNALES NUMÉRIQUES

Bonnes pratiques

- Mail:données techniques => code source / traçabilité au sein de l'entreprise
- Fichier : prouver sa valeur => emplacement du fichier, description, hash
- Adresse IP : dynamiques ? => attribution horodatée des IP/ports
- Le Graal ?

=> Accès aux données en lecture seule (intégrité)
=> Copie bit à bit du support avec hash (disque, partition, ...)

Cybersécurité : protéger votre propriété intellectuelle

Propriété intellectuelle : de quoi s'agit-il ?

- Propriété littéraire et artistique
  * droit d'auteur

Le droit d'auteur s'acquiert sans formalités

- Propriété industrielle
  * création techniques
  * créations ornementales
  * signes distinctifs

Les droits de propriété industrielle s'acquièrent par des formalités administratives, parfois par l'usage.

Quelles sont les atteintes à la propriété intellectuelle ?

- La contrefaçon

- La captation/vol de brevet

- L’espionnage industriel

Pratiques préventives

- protocoles de sécurité

- discrétion

- préparation de ses déplacements / salons /conférences…

- identifier, cartographier et hiérarchiser les zones de l'entreprise en fonction des risques et vulnérabilités et maintenir des contrôles d'accès limités.

- protection (brevets à l'INPI).

- rédaction des clauses de non-concurrence / clauses de confidentialité / accords de non-divulgation.

- mise en place d'une veille pour détecter et se prémunir des contrefaçons / surveiller vos concurrents.

LES BONNES PRATIQUES

- Mises à jour
- Mots de passe
- Les accès
- Les sauvegardes
- MFA (dont contre appel)

LES BONNES PRATIQUES

Mots de passe

Mot de passe : 12 caractère au minimum (minuscules, majuscules, chiffres et caractères spéciaux)

Ne jamais communiquer son mot de passe. Aucune organisation ou personne de confiance ne demandera sa communication.

COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE EN 2023 ?

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
5	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
6	Immédiat	Immédiat	Immédiat	Immédiat	Immédiat
7	Immédiat	Immédiat	1 seconde	2 secondes	4 secondes
8	Immédiat	Immédiat	28 secondes	2 minutes	5 minutes
9	Immédiat	3 secondes	24 minutes	2 heures	6 heures
10	Immédiat	1 minute	21 heures	5 jours	2 semaines
11	Immédiat	32 minutes	1 mois	10 mois	3 ans
12	1 seconde	14 heures	6 ans	53 ans	226 ans
13	5 secondes	2 semaines	332 années	3 000 années	15 000 ans
14	52 secondes	1 an	17 000 ans	202 000 ans	1 million d'années
15	9 minutes	27 ans	898 000 ans	12 millions d'années	77 millions d'années
16	1 heure	713 ans	46 millions d'années	779 millions d'années	5 milliards d'années
17	14 heures	18 000 ans	2 milliards d'années	48 milliards d'années	380 milliards d'années
18	6 jours	481 000 ans	126 milliards d'années	1 trillion d'années	26 trillions d'années

Infographie FRANCENUM.GOUV.FR

Source : Hive Systems

LES BONNES PRATIQUES

Sauvegardes

Contrôler et tester ses sauvegardes !

Règle des 3-2-1

- Créer 3 copies des données (1 copie principale et 2 sauvegardes)
- Stocker les copies sur au minimum 2 types de support (disque local, partage réseau / NAS, lecteur de bandes etc ...
- Stocker une des copies **hors site** (exemple : cloud)

LES BONNES PRATIQUES

Charte informatique

La charte d'utilisation des moyens informatiques a pour finalité de contribuer à la préservation de la sécurité du système d'information de l'entité concernée.

Elle permet d'informer les utilisateurs sur :

- les usages permis des moyens informatiques mis à disposition
- les règles de sécurité en vigueur
- les mesures de contrôle prises par l'employeur
- et les sanctions encourues par l'utilisateur

A RETENIR

2 Principes :

Prise de conscience => une attaque : PAS « SI » MAIS « QUAND »

L'attaquant est déjà dans votre SI

3 phases :

- Avant la crise
- Pendant la crise
- Après la crise

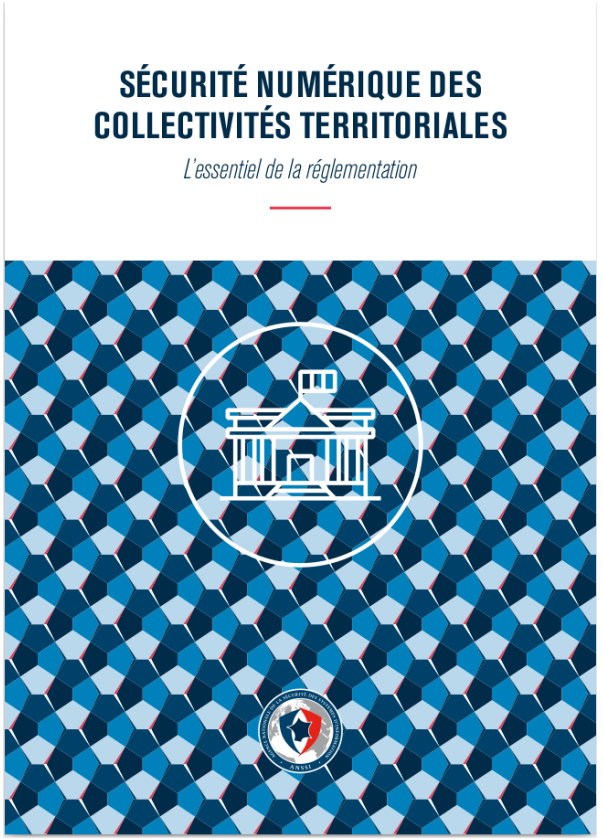
3 domaines d'action :

- Organisationnel
- Humain
- Technique

LIENS UTILES

- https://www.ssi.gouv.fr/
- https://www.cybermalveillance.gouv.fr/
- https://www.masecurite.interieur.gouv.fr/fr
- https://www.signal-spam.fr
- https://www.inpi.fr/comprendre-la-propriete-intellectuelle/les-enjeux-de-la-propriete-intellectuelle
- https://europa.eu/youreurope/business/running-business/intellectual-property/infringement/index_fr.htm
- https://signal.conso.gouv.fr/
- cyber-vigilance-nouvelleaquitaine@gendarmerie.interieur.gouv.fr

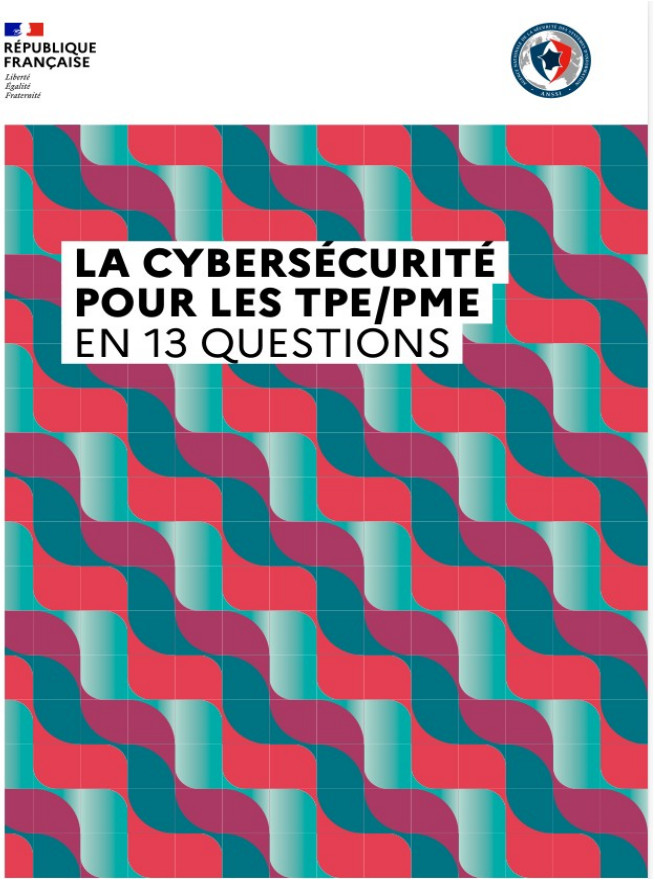
LIENS UTILES



https://www.ssi.gouv.fr/administration/guide/securite-numerique-des-collectivites-territoriales-lessentiel-de-la-reglementation/

https://www.amf.asso.fr/documents-cybersecurite-toutes-les-communes-intercommunalites-sont-concernees/40406

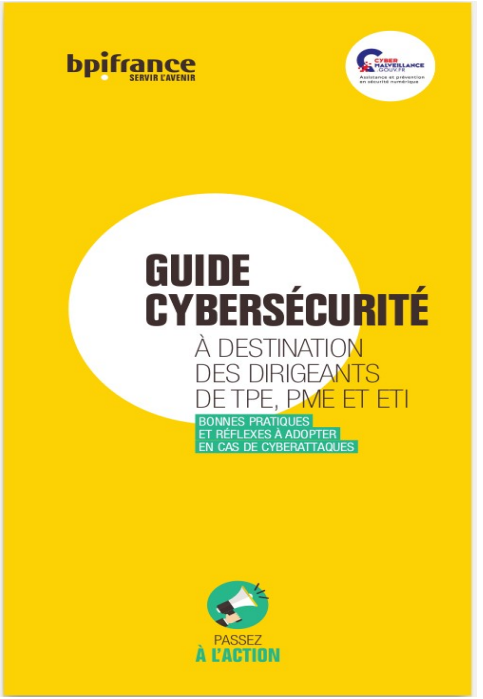
LIENS UTILES



https://www.ssi.gouv.fr/guide/la-cybersecurite-pour-les-tpepme-en-treize-questions/

LIENS UTILES

https://www.economie.gouv.fr/files/files/PDF/2017/bro-memento-cybersecurite-createur_0.pdf



https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/cybermalveillancegouvfr-bpifrance-guide-pme-tpe

QUESTION ?