Cybersécurité et télétravail

Cyril Bras

Vice-président IN.CRT

RSSI Grenoble-Alpes Métropole

IN.CRT
CYBER – RESILIENCE – TERRITOIRES

Sommaire

1. Qu’est-ce que la cybersécurité ?
2. Evolution de la menace
3. 2020, les collectivités dans le viseur
4. Crise sanitaire facteur aggravant ?
5. Quelles solutions ?

Cybersécurité,
la Gironde
contre attaque !

Cybersécurité et télétravail

QU’EST-CE QUE LA CYBERSÉCURITÉ ?

Qu’est-ce que la cybersécurité ?

L’ANSSI l’entend comme l’« *état recherché pour un système d’information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l’intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu’ils rendent accessibles* ».

Source : Rapport d’information sur la Cyberdéfense Juillet 2018 p.14

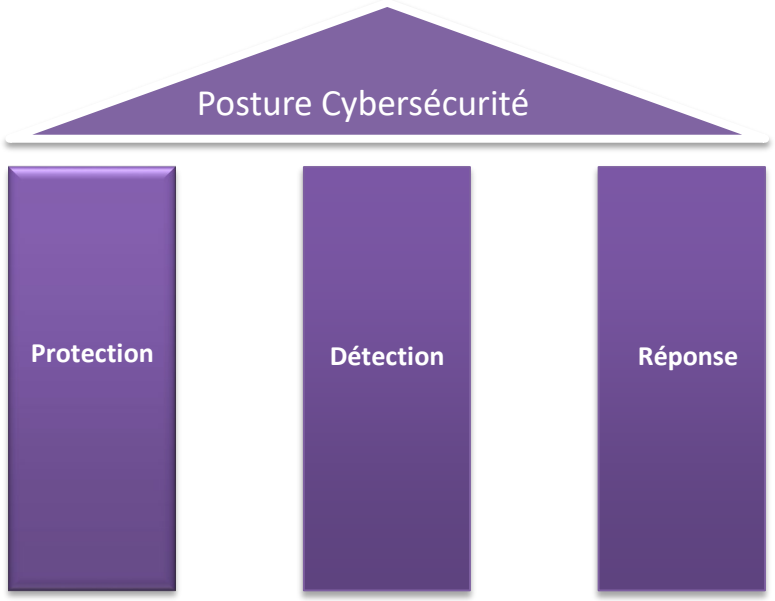
Cybersécurité
la Gironde
contre attaque !

Qu’est-ce que la cybersécurité ?

- Sécurité informatique ⊆ Cybersécurité
- 3 couches :
  - Physique (ordinateurs, équipements réseaux…)
  - Logique (système d’exploitation, suite bureautique…)
  - Sémantique (ce que comprend notre cerveau)

Cybersécurité,
la Gironde
contre attaque !

Qu’est-ce que la cybersécurité ?



- L’acquisition de solutions technique n’est plus suffisante
- Les attaques se produisent aussi sur la couche sémantique
- Comment intégrer l’humain dans la stratégie de défense ?

- Source : Cybersecurity – Attack and Defense Strategies, Yuri Diogenes & Erdal Ozkaya, 2nd Edition Packt>

Cybersécurité et télétravail

EVOLUTION DE LA MENACE

Evolution de la menace

- 2003, 2009 Toulouse : Contrefaçon de site officiel
- 2005 Clichy Sous Bois : publication d'une fausse information (démission du maire)
- 2009 Longjumeau : prise de contrôle d'ordinateurs municipaux
- 2010 Gaillac & Croisilles: Dénaturation de site web
- 2011 Reims : pénétration directe via un flux RSS

Source: Rémy Février, « Toujours plus cyber-menacées : les collectivités territoriales »,*Sécurité globale* 2015/3 (N° 3-4), p. 9-93.

ⓘ

Une sous estimation du risque pendant des années

Peu d'attaques documentées

Evolution de la menace

- 24 mars 2018 :
  - attaque par ransomware de la ville d'Atlanta
  - 51 000 $ demandés,
  - système d'information de la ville inopérant plus qu'une semaine
- 12 avril 2018 : la ville a dépensé 2,7 millions de $ en contrats de prestation de sécurité informatique après l'incident
- La plateforme de paiement de la rançon a été désactivée après le délais laissé
- Management focalisé sur les aspects smartcity
- Au final le coût estimé de cette attaque est de 16 millions de $

Source : The Atlanta Journal-Constitution, *CONFIDENTIAL REPORT: Atlanta's cyber attack could cost taxpayers $17 million* 1er août 2018

ⓘ
2018
De gros incidents commencent à se produire aux USA contre des collectivités

Evolution de la menace

La Croix Valmer

- 31 juillet 2018 : Cryptovirus paralyse l'ensemble du SI de la ville (comptabilité, RH…) pendant une semaine.
- La mairie refuse de payer la rançon.
- Plusieurs semaines de travail détruites
- 2 mois pour rétablir complètement le SI

ⓘ
2018
Mais aussi en France

Source : https://www.20minutes.fr/high-tech/2315667-20180731-var-mairie-croix-valmer-refuse-payer-rancon-apres-piratage-systeme-informatique

Cybersécurité,
la Gironde
contre attaque !

Evolution de la menace

- Renforcement de la sécurité des principaux acteurs
- Les attaquants se déportent vers des cibles moins exposées
- De nombreuses campagnes d'hameçonnage visent les collectivités territoriales en 2018

Source : Rapport annuel 2018 ANSSI, avril 2019

Cybersécurité,
la Gironde
contre attaque !

Evolution de la menace

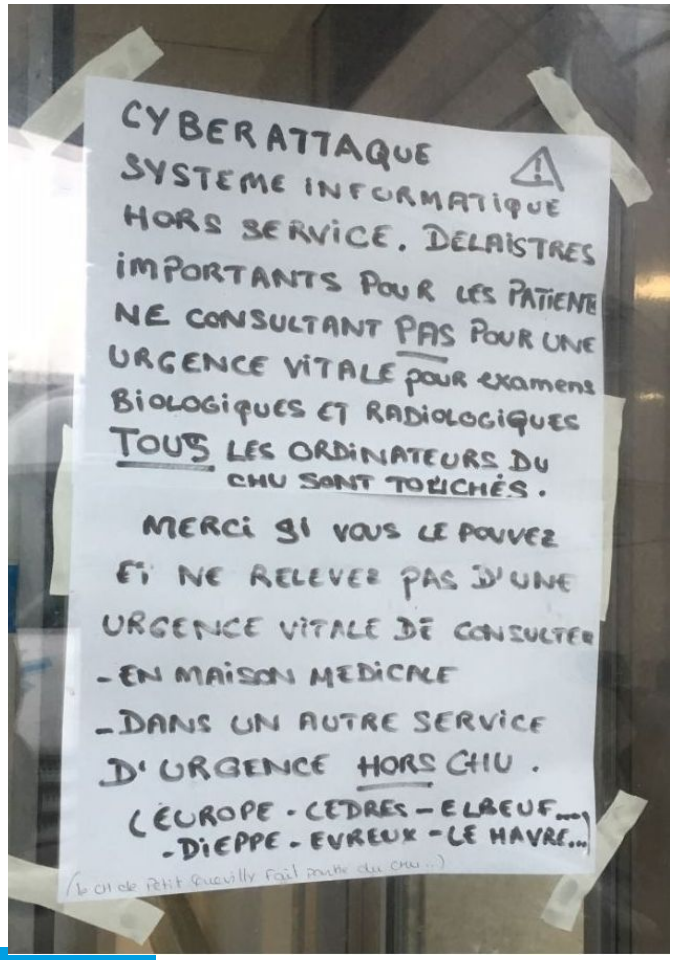
- 13 mai 2019

Intrusion sur le système de contrôle de l'éclairage public et les feux de circulation.

Cybersécurité,
la Gironde
contre attaque !

Evolution de la menace

- 15 novembre 2019
  - Rançongiciel Clop déployé sur tout le SI de l'hôpital par le groupe criminel TA505
  - L'attaque a en réalité débuté le 16 octobre par une campagne d'hameçonnage



Cybersécurité,
la Gironde
contre attaque !

Evolution de la menace

	Top Threats 2019-2020	Assessed Trends	Change in Ranking
1	Malware	---	---
2	Web-based Attacks	---	↗
3	Phishing	↗	↗
4	Web application attacks	---	↙
5	Spam	↙	↗
6	Denial of service	↙	↙
7	Identity theft	↗	↗
8	Data breaches	---	---
9	Insider threat	↗	---
10	Botnets	↙	↙
11	Physical manipulation, damage, theft and loss	---	↙
12	Information leakage	↗	↙
13	Ransomware	↗	↗
14	Cyberespionage	↙	↗
15	Crytojacking	↙	↙

Legend: Trends: ↙ Declining, --- Stable, ↗ Increasing **Ranking:** ↗ Going up, --- Same, ↙ Going down

- Sur 2019-2020, les 5 premiers types d'attaques concernaient directement l'utilisateur final
- Avec la numérisation de la société, la surface d'attaque s'étend

- Source ENISA Threat Landscape 2019-2020

Cybersécurité,
la Gironde
contre attaque !

Cybersécurité et télétravail

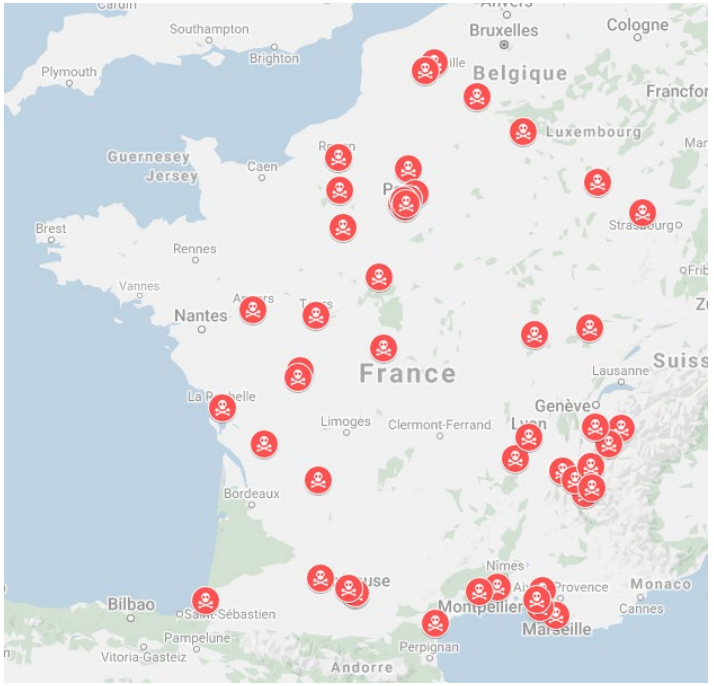
2020
LES COLLECTIVITÉS DANS LE VISEUR

Cybersécurité,
la Gironde
contre attaque !

2020, les collectivités dans le viseur

- Saint-Paul-en-Jarez (42 – Loire – 18-19 janvier 2020)
- Tullins-Fures (38 - Isère – 30-31 janvier 2020)
- Crêts en Belledone (38 – Isère – 11 février 2020)
- Région Grand Est (67 – Bas-Rhin – 13 février 2020)
- Charleville-Mézières / Ardenne Métropole / CCAS (08 – Ardennes – 5 mars 2020)
- Marseille, Métropole Aix-Marseille-Provence, Martigues (13 -Bouches-du-Rhône – 14 mars 2020)
- Hôpitaux de Paris (75 - Paris – 22 mars 2020)
- Département Isère (38 – Isère - Grenoble– 30-31 mars 2020)
- Etablissement public de santé (32 – Gers - Lomagne – 02 avril 2020)
- Métropole de Toulouse, de Besançon, Bayonne…
- La Rochelle, Grand Annecy…
- **Des attaques hebdomadaires…**

ⓘ
2020
Explosion des cyberattaques

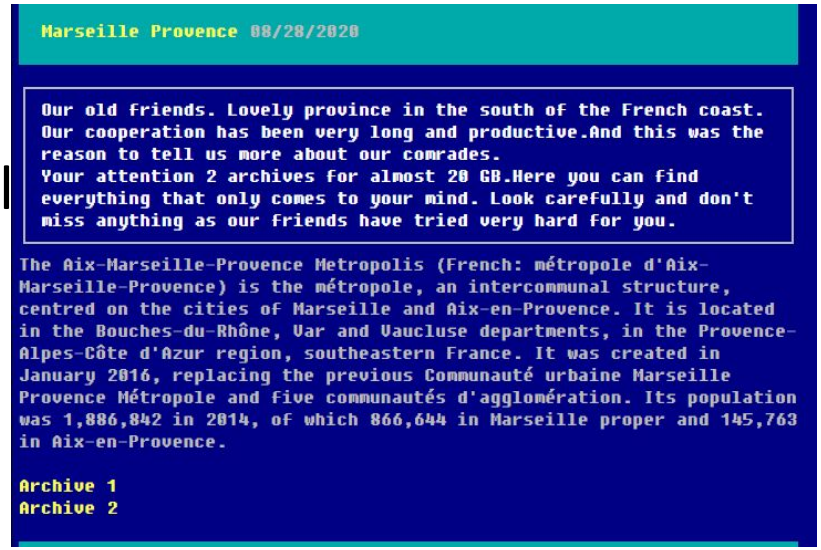


Cybersécurité, la Gironde contre attaque !

2020, les collectivités dans le viseur

Mode opératoire d'une attaque

- *Phase 1* : Campagne d'hameçonnage
- *Phase 2* : Attaque par rançongiciel
  - Attaquants présents pendant plusieurs jours ou semaines, exfiltration de données puis destruction du SI
- *Phase 3* : Chantage sur les données exfiltrées



Cybersécurité,
la Gironde
contre attaque !

2020, les collectivités dans le viseur

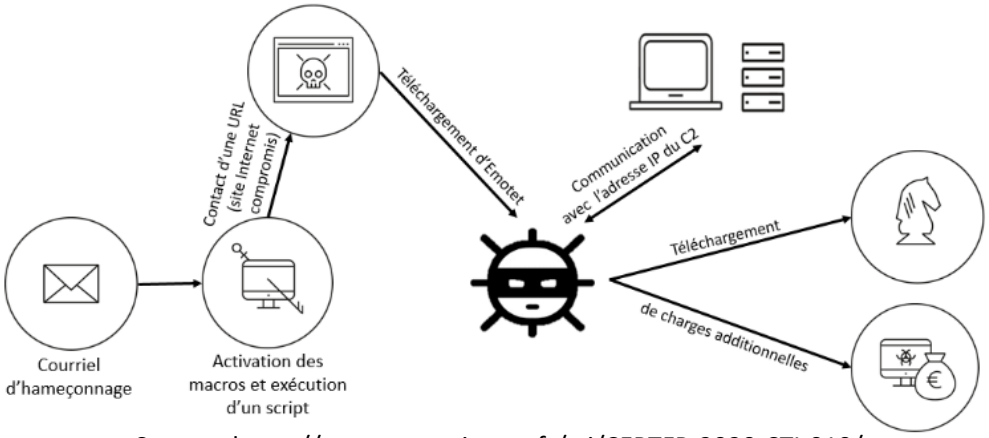
- Aout 2020
  - Exploitation de vulnérabilités sur les VPN Pulse
  - Identifiants disponibles sur des sites de hacking
  - Des collectivités françaises compromises

Source : https://www.zdnet.fr/actualites/la-cnil-pousse-les-entreprises-a-patcher-leurs-vpn-pulse-secure-de-toute-urgence-39908725.htm

Cybersécurité,
la Gironde
contre attaque !

2020, les collectivités dans le viseur

- Aout/septembre 2020 Campagne Emotet
  - Nombreuses collectivités concernées
  - Réception de courriels composés d'échanges légitimes
  - Avec PJ ou URL



Source : https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-010/

Cybersécurité, la Gironde contre attaque !

2020, les collectivités dans le viseur

- Des attaques :
  - opérées par des organisations criminelles
  - revendiquées

Un groupe russe revendique la cyberattaque qui a touché la ville de La Rochelle

Mardi 5 janvier 2021 à 19:42 - Par Audrey Abraham, France Bleu La Rochelle, France Bleu

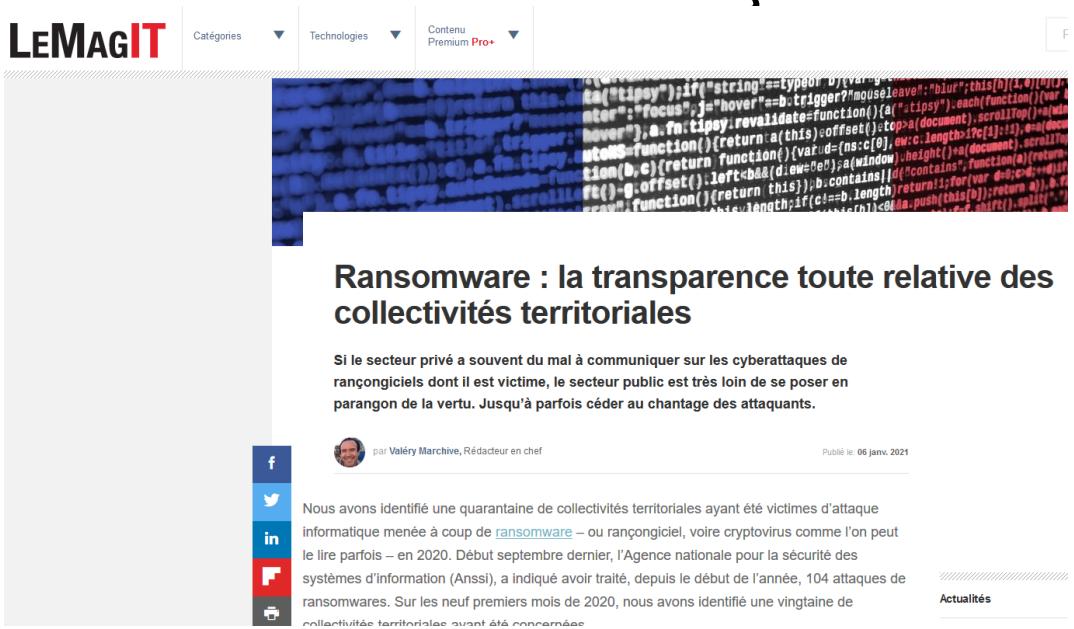
La Rochelle

Le groupe de piratage russophone Netwalker a revendiqué lundi la cyberattaque qui a paralysé la quasi totalité des services en ligne de la ville de La Rochelle la semaine dernière.

Une attaque en ligne a touché les services de la ville de La Rochelle fin décembre. © Radio France - david Morel

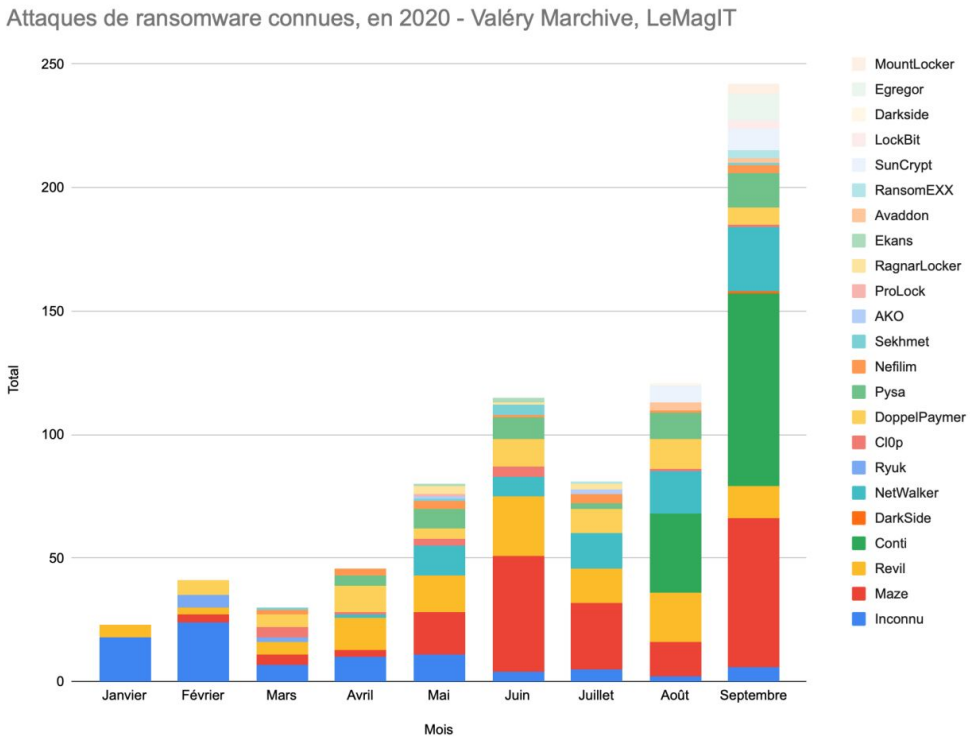
2020, les collectivités dans le viseur

- Face à l'impréparation certaines collectivités payent les demandes de rançon …



Source : https://www.lemagit.fr/actualites/252494433/Ransomware-la-transparence-toute-relative-des-collectivites-territoriales

2020, les collectivités dans le viseur



ⓘ
2020
Autant d'attaque par raçongiciel en septembre que sur le reste de l'année

Cybersécurité,
la Gironde
contre attaque !

Cybersécurité et télétravail

CRISE SANITAIRE FACTEUR AGGRAVANT ?

Cybersécurité,
la Gironde
contre attaque !

Crise sanitaire facteur aggravant ?

- La crise sanitaire liée à la COVID-19 a renforcé l'usage du télétravail dans les collectivités
- La travail à distance affaibli la sécurité globale du système d'information car les agents sont moins bien protégés à leur domicile
- La surface d'attaque se trouve augmentée par un télétravail parfois mis en place en urgence

Cybersécurité,
la Gironde
contre attaque !

Crise sanitaire facteur aggravant ?

- Le domicile, un environnement numérique comportant différentes sources de vulnérabilités

Cybersécurité,
la Gironde
contre attaque !

Crise sanitaire facteur aggravant ?

Coronavirus (COVID-19)

LES PRINCIPAUX RISQUES ET CYBERMENACES LIÉS AU TÉLÉTRAVAIL

L'hameçonnage (*phishing*)

Les rançongiciels (*ransomware*)

Le vol de données

Les faux ordres de virement (FOVI/BEC)

Tous ces conseils en détail sur
www.cybermalveillance.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

Cybersécurité, la Gironde contre attaque !

Crise sanitaire facteur aggravant ?

Au niveau des collectivités territoriales

- Une dépendance à l'informatique toujours forte
- Un budget dédié à la SSI
  - Méconnu
  - Non pérenne d'une année sur l'autre
  - Variable d'ajustement ?

Source : Etude MIPS 2020 :
Collectivités territoriales du Clusif

Cybersécurité,
la Gironde
contre attaque !

Crise sanitaire facteur aggravant ?

- De fortes disparités suivant la taille des collectivités
- Le MCO prime encore sur le MCS
- Le RSSI
  - Fonction dédiée dans 59 % des collectivités (lorsque la fonction existe…) mais difficile à dédier pour 1/3.
  - Un positionnement qui ne permet pas toujours de faire remonter le sujet au niveau décisionnel hors DSI

Source : Etude MIP3 2020 : Collectivités territoriales du Clusif

Cybersécurité, la Gironde contre attaque !

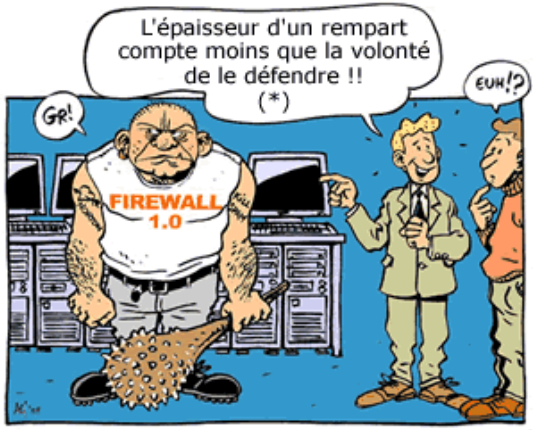
Cybersécurité et télétravail

QUELLES SOLUTIONS ?

Quelles solutions ?

<u>Platon :</u>

Ce ne sont pas les murs qui font la cité mais les hommes.



Le maillon faible de la cybersécurité reste toujours le facteur humain, les performances des meilleurs équipements réseau reposent sur leur bonne configuration et la robustesse des logiciels.

70% des incidents Cybersécurité sont d'origine humaine

Quelles solutions ?

Production de documents par les acteurs institutionnels sur les besoins de cybersécurité des collectivités

- ANSSI : *Sécurité numérique des collectivités territoriales : l'essentiel de la réglementation*
- Cybermalveillance.gouv.fr : *Programme de sensibilisation aux risques numériques dans les collectivités territoriales*
- AMF : *Cybersécurité : toutes les communes et intercommunalités sont concernées*

Quelles solutions ?

- Création d'un réseau de RSSI de collectivités territoriales en lien avec l'ANSSI
  - Réponse à incident
  - Entraide, partage d'informations

Cybersécurité,
la Gironde
contre attaque !

Quelles solutions ?

- Création de l'Institut National pour la Cybersécurité et la Résilience des Territoires
  - Il s'adresse d'abord aux EPCI et Communes et au-delà à tous les acteurs des territoires
  - Il vise à soutenir la constitution, la veille et la diffusion des idées, réflexions et études ayant trait à la cybersécurité et la résilience des territoires

Cybersécurité,
la Gironde
contre attaque !

Cybersécurité et télétravail

CONCLUSION

Conclusion

- La cybersécurité ne doit plus être perçue comme un frein au développement du numérique mais plutôt comme une condition nécessaire, un gage de confiance.

Cybersécurité,
la Gironde
contre attaque !

Merci pour votre attention !

IN.CRT
CYBER – RESILIENCE – TERRITOIRES