Veille technologique

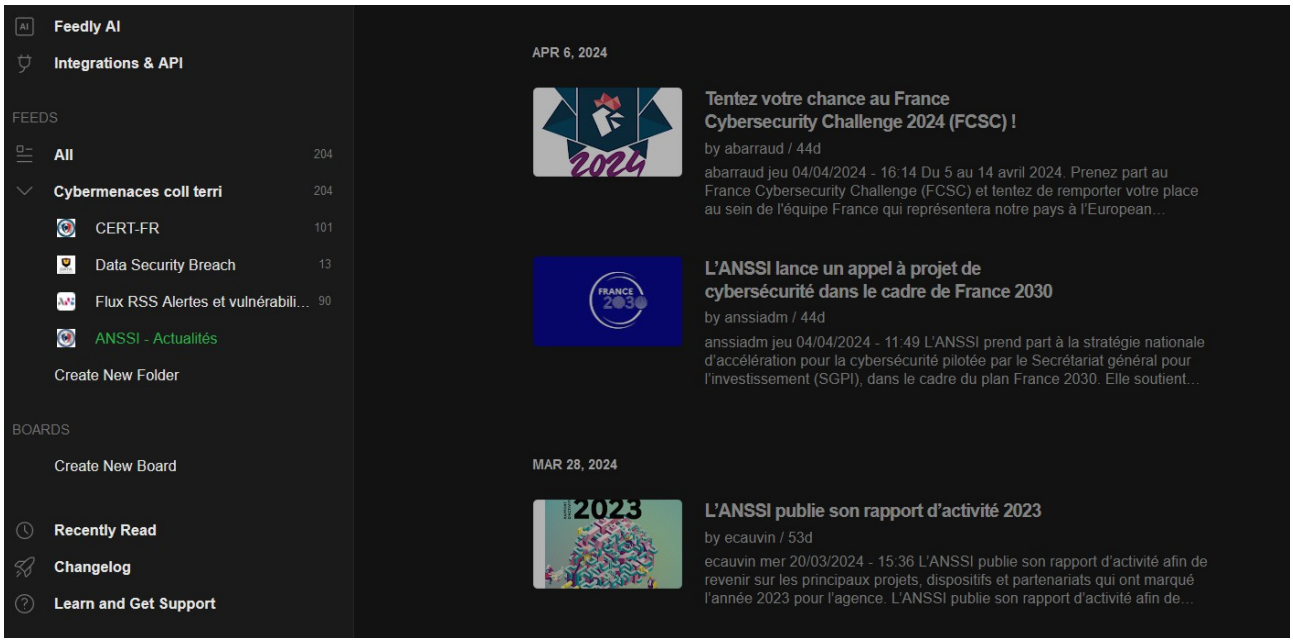
SOMMAIRE

1. Contexte

Dans le cadre de mon alternance à la société Berger-Levrault, je me suis intéressée à la cybersécurité des collectivités territoriales. En effet, je suis en constante relation avec des acteurs de mairies, EPIC... et la question de la cybersécurité se pose ; j'ai eu quelques clients qui m'ont raconté avoir subi une attaque informatique de type rançongiciel dans leur établissement.
Il m'arrive, dans le cadre de mes dépannages, de rappeler aux clients des stratégies de sécurité concernant les mots de passe, les mises à jour, et plus rarement concernant des mails véreux.

Je pense qu'il serait utile, en tant que technicienne support de renseigner nos clients à propos de menaces récurrentes pesant sur eux et sur les dispositifs de sécurité existants.

Pour effectuer cette veille technologique, je m'appuie sur un outil qui réunit tous les potentiels articles concernant mon thème : Feedly



Je n'ai pas trouvé de sites dédiés aux cybermenaces sur les collectivités territoriales. J'ai donc fait des recherches et ai regroupé des flux RSS de sites dans lesquels des articles concernant ce thème sont présents.

2. Menaces pesant sur les collectivités territoriales

Différentes menaces informatiques pèsent sur les collectivités et un article de l'ANSSI publié en avril résume celles qui sont les plus fréquentes.

En 2023, les trois premières cyberattaques subies par les collectivités sont par hameçonnage, rançongiciel et piratage de compte.

https://www.vie-publique.fr/en-bref/291598-cyberattaques-de-fortes-menaces-sur-les-collectivites-territoriales

Selon cet article, entre janvier 2022 et juin 2023, l'Agence de sécurité des systèmes d'information (Anssi) a enregistré et traité 187 cyberattaques visant les collectivités territoriales.
Il est évoqué la faiblesse de leur sécurité informatique qui fait d'eux des cibles de choix. De plus, la grande majorité des attaques ont eu pour but de chiffrer et/ou compromettre des données ce qui a eu pour conséquence sur les collectivités l'impossibilité d'assurer certaines de leurs missions.

3. Dispositifs pour améliorer la cybersécurité des collectivités territoriales

Cette veille technologique a mis la lumière sur des dispositifs pouvant être demandés ou mis en place pour les collectivités territoriale afin de renforcer la sécurité de leur système d'information.

- ***Kit d'exercice pour les collectivités territoriales :***

Ce kit propose 2 types d'exercices :

- **exercice sur table** : exercice de réflexion autour de scénarios de gestion de crise cyber. ***But*** : discuter des bonne pratiques, voir quels processus mettre en œuvre dans différentes situations

- **simulation de crise** : exercice de simulation de crise pour voir quelles sont les réactions et capacités d'organisation et de réponses des différents acteurs. ***But*** : tester une organisation de gestion de crise, des mesures stratégiques et la gestion du stress face à ce genre de situation.

→ sensibiliser et entraîner, éprouver son dispositif de crise et rendre compte des efforts produits (au niveau IT mais aussi autres acteurs)

https://cyber.gouv.fr/le-kit-dexercice-pour-les-collectivites-territoriales

- ***Projet de cybersécurité de l'ANSSI***

Participation possible des collectivités territoriales au **projet de cybersécurité lancé par l'ANSSI** pour renforcer sécurité informatique et être soutenu dans le cadre du plan France 2030

Publié le 04 Avril 2024 • Mis à jour le 04 Avril 2024

L'ANSSI prend part à la stratégie nationale d'accélération pour la cybersécurité pilotée par le Secrétariat général pour l'investissement (SGPI), dans le cadre du plan France 2030. Elle soutient notamment des projets de renforcement de la sécurité numérique portés par des collectivités territoriales et des opérateurs publics de services numériques (OPSN).

Les projets éligibles sont de quatre types différents :

- Des projets innovants ;
- Des projets d'initiative locale ;
- Des projets de déploiement « avancé » ;
- Des projets de déploiement « fondation ».

https://cyber.gouv.fr/actualites/lanssi-lance-un-appel-projet-de-cybersecurite-dans-le-cadre-de-france-2030

- *Dispositifs d'accompagnement des collectivité avec le projet France Relance (qq retours positifs et toujours d'actualité)*

Dispositifs d'accompagnement nationaux

Dans sa mission de prévention, l'ANSSI intervient auprès des fournisseurs de produits et services pour favoriser le développement de solutions adaptées aux besoins de sécurité et contribuant efficacement à la protection des systèmes d'information et des données contre les menaces actuelles. La politique industrielle de l'ANSSI suit avant tout un objectif de sécurité nationale.

Publié le 02 Février 2023 • Mis à jour le 02 Mai 2024

Accompagner les offreurs

L'ANSSI s'appuie fortement sur le tissu industriel et ses solutions cyber identifiées comme pertinentes afin de **renforcer la cybersécurité des acteurs publics sur l'ensemble du territoire**, en finançant l'achat de prestations et produits de sécurité. L'objectif du **plan de relance** lancé par le gouvernement est de renforcer la sécurité des administrations, des collectivités, des établissements de santé et des organismes publics tout en dynamisant l'écosystème industriel français.

Dans ce cadre, le gouvernement a alloué 1,7 Mds€ d'investissements à la transformation numérique de l'État et des territoires. **Le « volet cybersécurité », piloté par l'ANSSI, était initialement doté de 136 millions d'euros sur la période 2021-2022. Il a été réabondé de 40 M€ début 2022, pour ainsi atteindre 176 M€.**

Le plan de relance est un ensemble de quatre grands chantiers :

- **Parcours de cybersécurité** (100 M€) : financement de produits et prestations de cybersécurité au profit du secteur public, et prioritairement des collectivités territoriales et établissements de santé.
- **Produits et services mutualisés de cybersécurité** (32 M€) : développement de la capacité nationale de cybersécurité, au travers de la sécurisation des réseaux de l'État et du déploiement mutualisé de nouveaux services et produits pour les agents de l'État.
- **Appels à projet** (27 M€) : soutien financier à des projets de cybersécurité pour les collectivités territoriales, via un dispositif d'acquisition de produits et de licences mutualisés, sous la forme d'appels à projets s'adressant aux structures mutualisantes en charge de l'accompagnement à la transformation numérique des collectivités qui en sont membres.
- **CSIRT régionaux et sectoriels** (17 M€) : soutien à la création d'un réseau de centres de réponse à incident régionaux et sectoriels (CSIRT), notamment dans les secteurs critiques (dont le maritime, l'aérien, le social et la santé) et auprès des acteurs essentiels du tissu socio-économique territorial.

Le bilan global de ce plan est extrêmement positif : il a permis une augmentation concrète du niveau de cybersécurité des bénéficiaires et un large déploiement de solutions de cybersécurité principalement européennes. La mobilisation de l'écosystème des prestataires et éditeurs de solutions pour répondre aux besoins des utilisateurs, exprimés au travers des dispositifs proposés, a notamment permis cette réussite.

https://cyber.gouv.fr/dispositifs-daccompagnement-nationaux

○ *Les délégués de l'ANSSI*

Une documentation mise à jour ayant pour but que les collectivités territoriales aient des interlocuteurs plus proches (délégués régionaux). Ces délégués peuvent sensibiliser et diriger les acteurs vers de bonnes pratiques informatiques.

Action territoriale

La numérisation de la société s'accélère : la part du numérique dans les services, les produits et les métiers ne cesse de croître, s'accompagnant d'une multiplication des attaques informatiques de tous types.

< Notre écosystème

Action territoriale

Le Campus Cyber

Publié le 12 Juillet 2022 • Mis à jour le 25 Mars 2024

Les délégués de l'ANSSI dans les territoires

Parce qu'ils sont des acteurs de premier plan de cette transformation numérique, les territoires sont aussi de plus en plus vulnérables à la menace cyber. En synergie avec les structures et les autorités régionales existantes, l'ANSSI développe depuis plusieurs années des dispositifs visant à soutenir le tissu économique et les institutions à l'échelle régionale face à cette menace.

Les délégués de l'ANSSI en régions

En tant qu'autorité nationale en matière de cybersécurité, l'ANSSI s'est dotée en décembre 2015 d'un dispositif d'action visant à soutenir les acteurs à l'échelle régionale. Une large part des missions assurées par l'ANSSI nécessite en effet de pouvoir agir au plus près de ses interlocuteurs, répartis sur l'ensemble du territoire, en particuliers les acteurs économiques et les collectivités territoriales.

https://cyber.gouv.fr/action-territoriale