# Cybersécurité : "Un filtre anti-arnaques doit être déployé d'ici aux JO 2024", selon le ministre Jean-Noël Barrot

*Loin de s’arrêter, les cyberattaques tendent à se multiplier avec l’essor du numérique. Après avoir exposé à Maddyness sa vision de l’intelligence artificielle, le ministre chargé de la Transition numérique, Jean-Noël Barrot, expose cette fois-ci les mesures mises en place par le gouvernement pour renforcer la cybersécurité des collectivités, des entreprises et des citoyens.*

Temps de lecture : minute

*9 février 2023*

Mairies de Caen et de Chaville, départements de Seine-Maritime, de Seine-et-Marne et des Alpes-Maritimes, ou encore régions de Guadeloupe et de Normandie… Toutes ces collectivités ont été victimes d’une cyberattaque l’an passé. Et des cybercriminels s’en sont même pris à des hôpitaux, comme ceux de Versailles et de Corbeil-Essonnes.

Piratage de comptes, hameçonnage, rançongiciels, les actes de cybermalveillance prennent diverses formes et affectent tous les acteurs de la société. Les “simples” internautes sont régulièrement la cible d’arnaqueurs en ligne. Et plus d’une entreprise sur deux déclare avoir subi entre une et trois cyberattaques en 2021, selon la 7e édition du baromètre du Cesin. Les chiffres pour 2022 ne sont pas encore connus, mais risquent encore de refléter une cybermalveillance omniprésente.

Le coût d’une cyberattaque atteint souvent plusieurs millions d’euros. Pour renforcer la cybersécurité en France, le gouvernement a annoncé

mobiliser un milliard d’euros début 2021, dont 720 millions de financements publics. Plusieurs mesures concrètes ont depuis vu le jour. Jean-Noël Barrot, le ministre délégué chargé de la Transition numérique et des Télécommunications, revient sur les dispositifs déployés par le gouvernement et ceux qu’il compte mettre en place cette année et d’ici l’été 2024.

## Les cyberattaques se sont multipliées en 2022, affectant notamment des collectivités et des hôpitaux. Quelles mesures avez-vous prises pour arrêter ou tout au moins limiter ces attaques et leurs conséquences?

Jean-Noël Barrot : Dès 2021, dans le cadre du plan de relance du gouvernement, des parcours de cybersécurité ont été lancés pour 950 collectivités, hôpitaux et établissements publics et consulaires. Ils passent par une phase d’audit, suivie d’une phase d’équipement en solutions de protection et de formation des collaborateurs. Sur ces 950 établissements et collectivités ciblés, presque l’intégralité ont déjà initié un parcours de cybersécurité, mais tous ne les ont pas encore terminés.

Fin août 2022, nous avons décidé avec François Braun, ministre de la Santé, d’étendre ces parcours, qui ciblaient déjà 150 hôpitaux, à 150 nouveaux hôpitaux, et de renouveler l’enveloppe de 20 millions d’euros qui leur était consacrée.

## Ces parcours de cybersécurité portent-ils déjà leurs fruits?

J-N.B : La mairie de Caen, qui avait mis en oeuvre les préconisations du parcours de cybersécurité et s’était dotée d’un EDR (Endpoint detection

and response, ndlr), soit un antivirus synchronisé sur l'ensemble des systèmes et postes informatiques, a beaucoup mieux résisté que les autres collectivités à la cyberattaque dont elle a été victime. Et elle en a limité les conséquences.

## Que prévoit le gouvernement pour les plus petites communes, dotées de moins de moyens?

J-N.B : Pour les plus petites collectivités, nous travaillons avec l'Anssi (Agence nationale de la sécurité des systèmes d'information, ndlr) à la mise à disposition d'un service sur abonnement de noms de domaine et de messageries sécurisées nativement, de manière à ce qu'elles puissent bénéficier facilement de solutions en matière de cybersécurité. Ce système sur abonnement sera complété à terme par un hébergement sécurisé des services en ligne gérés par les collectivités.

## Et pour les entreprises, fréquemment victimes de cyberattaques?

J-N.B : Pour les entreprises de taille modeste, nous allons lancer une campagne de communication massive avec Cybermalveillance (dispositif national d'assistance aux victimes de cybermalveillance qui a fêté ses cinq ans en décembre, ndlr).

Nous allons en outre développer, sous l'égide de l'Anssi, un outil d'auto-diagnostic gratuit pour toutes les entreprises. Et nous prévoyons en plus un accompagnement, à l'image des parcours de cybersécurité mis à disposition des collectivités. Il s'adressera à 750 entreprises prioritaires, suffisamment grandes pour qu'une attaque les visant perturbe leur chaîne de valeur (donneurs d'ordres, fournisseurs…) et pour lesquelles le RSSI (responsable de la sécurité des systèmes d'information, ndlr) ou

l’équipe dédiée à la cybersécurité a besoin de moyens renforcés.

## Au-delà des entreprises et collectivités, de nouvelles mesures ciblant les citoyens et les internautes vont-elles voir le jour en 2023?

J-N.B : Notre priorité, c’est de mieux protéger nos concitoyens dans l’espace numérique, face à la menace croissante des cyberattaques. Pour nos compatriotes, les deux mesures les plus significatives sur lesquelles nous travaillons actuellement sont le filtre anti-arnaques et le cyberscore. Le filtre anti-arnaques sera un filtre simple, gratuit, mais facultatif pour les internautes, qui avertira préventivement si vous êtes en train de vous diriger vers un site malveillant. Notre objectif est d’avoir une version bêta pour la Coupe du monde de rugby en 2023, qui sera enrichie dans les mois qui suivront pour être généralisée à l’été 2024, au moment des Jeux Olympiques.

Ce filtre pourrait s’appuyer sur les navigateurs et fournisseurs d’accès à Internet. Nous espérons ainsi contrer les arnaques, comme celles qui visent à collecter des informations personnelles via des campagnes de phishing (sites qui imitent un autre site, comme celui des impôts ou de la Caf, ndlr).

Le cyberscore doit permettre quant à lui d’informer ou d’alerter les internautes du degré de sécurité d’un site sur lequel ils s'apprêtent à laisser des données d’identité ou de paiement. À la manière du Nutri-score, qui permet à chacun d'identifier les caractéristiques nutritives des produits dans un supermarché, le cyberscore sera un outil pour jauger les sites internet et créer un cercle vertueux : les sites avec un cyberscore élevé montreront l’exemple et inciteront les autres à relever leur niveau de sécurité.

Le déploiement du cyberscore est prévu cette année. Tous les sites n’en seront pas pourvus. Il sera réservé à ceux les plus visités sur Internet.

## Où en est l’Europe dans la protection des consommateurs et des mineurs sur Internet et les réseaux sociaux?

J-N.B : Lors de mon déplacement aux Etats-Unis (début janvier, ndlr) puis au Forum de Davos, j’ai pu constater que le monde entier regardait avec attention la mise en oeuvre en Europe des règlements DMA (Digital Markets Act, ndlr) et DSA (Digital Services Act, ndlr), le premier introduisant des principes de concurrence saine et équitable sur les marchés numériques, le second élevant le niveau de responsabilité des réseaux sociaux et plateformes de marché. Ces initiatives européennes se situent plutôt à l’avant-garde de ce qui se fait en matière de régulation des géants du numériques. Nous sommes en train de préparer le projet de loi qui adaptera le droit français à ces règlements, pour qu’ils s’appliquent rapidement en France.

Des discussions sont par ailleurs en cours avec des réseaux sociaux pour vérifier et contrôler l’âge sur Internet, dans l’optique de mieux protéger les mineurs. Le président de la République, Emmanuel Macron, a déjà lancé un Laboratoire pour la protection de l’enfance en ligne le 10 novembre, auquel participe par exemple l’application TikTok.

---

Article écrit par Louis Carle et Thomas Chenel