**CONCOURS EXTERNE / INTERNE D'INGÉNIEUR EN CHEF TERRITORIAL**

**SESSION 2025**

**Note de synthèse et de propositions visant à faire l'analyse du dossier remis au candidat portant sur un sujet technique**

**Option : Systèmes d'information et de communication**

# EPREUVES N° 5 & 10

**Durée : 5 h**
**Coefficient : 5**

**Sujet : La directive européenne NIS2 au service d'une collectivité plus résiliente**

Au vu de l'évolution préoccupante du paysage des cybermenaces et de leurs répercussions potentielles sur le fonctionnement des services publics, la Directrice Générale des Services de la métropole de Soigny, 420 000 habitants, souhaite disposer d'une analyse approfondie permettant de mieux comprendre les enjeux liés à la cybersécurité dans le cadre du renforcement des obligations réglementaires européennes.

En effet, dans un contexte où les collectivités territoriales, et en particulier les métropoles telles que celle de Soigny (420 000 habitants), deviennent des cibles régulières d'attaques informatiques, il apparaît indispensable d'appréhender les risques opérationnels encourus et les dispositifs existants pour y faire face. L'attaque par déni de service (DDOS) survenue en décembre 2023 à l'encontre de la collectivité a, par ailleurs, accentué la sensibilité de plusieurs élus à ces sujets, d'autant que de nombreuses collectivités échangent régulièrement sur les impacts réels subis lors de cyberattaques.

Dans ce contexte, la Directrice Générale des Services souhaite être éclairée sur le cadre stratégique et opérationnel qu'introduit la directive européenne NIS2 (« Network and Information Security »). En effet, après avoir participé à une journée d'actualité sur le sujet, elle estime ce référentiel de la cybersecurité « incontournable » pour les entités publiques, qui doit être non seulement compris dans ses dimensions réglementaires, mais également en tant que levier potentiel d'amélioration de la résilience du système d'information de la collectivité.

En qualité de Directeur des Systèmes d'Information, il vous est demandé de produire une note en vous basant sur l'analyse du dossier documentaire joint permettant à la Direction Générale des Services d'arbitrer les priorités d'action à engager en matière de cybersécurité, dans une perspective de mise en conformité, mais aussi de création de valeur.

**Dans une première partie,** vous rédigerez une synthèse qui justifie la mise en application du règlement NIS2 et les grandes lignes de cette directive.

**Dans une deuxième partie**, vous décrirez les apports possibles de la mise en œuvre de NIS2 pour en faire un levier au bénéfice de la collectivité au-delà du simple respect réglementaire. En proposant des ambitions concrètement envisageables, vous vous attacherez à présenter une orientation stratégique qui identifie les leviers, les actions prioritaires et les ressources internes ou externes à mobiliser.

**Barème de notation :**

Synthèse : 10 points
Propositions : 10 points

**DOCUMENTS JOINTS**


| | | |
|---|---|---|
| **Document n° 1** | La Tribune : Cybersécurité : NIS2, une transposition essentielle pour notre souveraineté numérique (17/10/24) | **Page 3** |
| **Document n° 2** | Solution Numérique 17/10/24 : L'importance de la directive NIS2 pour la cybersécurité et la conformité des entreprises | **Page 6** |
| **Document n° 3** | Usine-Digitale - 02/01/25 : Plusieurs collectivités françaises visées par une cyberattaque pro-russe | **Page 8** |
| **Document n° 4** | LinkedIn - 16/12/2024 – 2025 : année européenne de la cybersécurité par Gaël Le Roux | **Page 9** |
| **Document n° 5** | Solutions num&cyber - 12/09/24 : To do list de rentrée d'un RSSI : quelques mesures pour faire évoluer sa stratégie de cyber défense | **Page 11** |
| **Document n° 6** | Cyberattaque Ville et agglomération de Saint-Nazaire – France TV Region 19/04/2024 | **Page 12** |
| **Document n° 7** | 7- Panorama Cybermenace_ANSSI_2024 – Extrait p4-5 et 10-11 | **Page 15** |
| **Document n° 8** | Directive NIS 2 : les pouvoirs publics prônent de retenir le seuil des 30 000 habitants pour les collectivités 11/03/2024 | **Page 19** |
| **Document n° 9** | Cyberattaque sur les serveurs de Val-de-Reuil, 05/09/2024 | **Page 21** |
| **Document n° 10** | Synthèse 2024 de la menace des collectivités territoriales – ANSSI | **Page 23** |
| **Document n° 11** | Sénat - Commission résilience - Essentiel sur NIS2<br>Extrait : introduction + 1 A et B | **Page 29** |
| **Document n° 12** | Thématiques de contrôles prioritaires CNIL en 2025 | **Page 33** |
| **Document n° 13** | Premier bilan pour les CSIRT territoriaux | **Page 35** |
| | | **TOTAL de 35 pages** |


**NOTA :**

- 2 points seront retirés au total de la note sur 20 si la copie contient plus de 10 fautes d'orthographe ou de syntaxe.
- **Les candidats ne doivent porter aucun signe distinctif sur les copies** : pas de signature ou nom, grade, même fictifs.
- Les épreuves sont d'une durée limitée. Aucun brouillon ne sera accepté, la gestion du temps faisant partie intégrante des épreuves.
- Lorsque les renvois et annotations en bas d'une page ou à la fin d'un document ne sont pas joints au sujet, c'est qu'ils ne sont pas indispensables.

Document 1 : **Cybersécurité : NIS2, une transposition essentielle pour notre souveraineté numérique**
**La Tribune – 17/10/24 - p**ar Jean-Noël de Galzain, président d'Hexatrust

**OPINION. La transposition de la directive de cybersécurité NIS 2 dans le droit national, qui débute à peine et en retard, doit devenir un moment de réflexion collective sur l'ambition française en termes de protection numérique et de souveraineté. Les acteurs de la cybersécurité sont prêts à accompagner le gouvernement et les parlementaires pour assurer la mise en œuvre de ce texte crucial pour notre industrie, pour la résilience de notre économie, et pour le maintien du leadership européen de la France en matière de numérique.**

C'est à deux jours de la date limite de transposition de la directive NIS 2 en droit Français (le 17 octobre) que le Gouvernement français a finalement présenté, mardi 15 octobre, le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité. Une présentation à saluer, dans un contexte où les chantiers sont nombreux, et qui doit permettre de remettre au cœur des agendas politiques et médiatiques la transformation que cette directive impose, vers un nouvel âge numérique industriel et plus résilient.

Si notre actualité politique récente explique le retard pris dans le processus de transposition législatif (de nombreux pays comme la Belgique, la Croatie, le Luxembourg ou la Hongrie ont déjà agi), la volonté de transposer au plus vite ne doit pas nous conduire à revoir nos objectifs à la baisse. Il est nécessaire d'aborder ce dernier avec ambition et vision pour répondre au triple enjeu caché à l'intérieur de ce texte : celui de la cyber-résilience de nos infrastructures, de la compétitivité de notre économie et du rayonnement de la France au niveau européen.

### a) NIS 2 : Un texte fondamental pour notre cyber-résilience

Chaque année, le coût des cyberattaques croit de 10%, le nombre d'organisations touchées augmente de 70%, et certaines entreprises disparaissent faute de prévention. Il est urgent d'endiguer cette menace cyber pour préserver nos services publics, nos hôpitaux, nos PME et ETI toujours plus numériques.

Avec plus de 15 000 entités publiques et privées directement concernées en France, sans compter les milliers de sous-traitants, NIS 2 est appelée à avoir un impact majeur pour lutter contre cette menace. Elle va transformer les pratiques de cybersécurité autour d'un nouveau standard de fait, et au-delà, faire évoluer la gouvernance des organisations de l'UE qui deviendront responsables de leurs usages numériques et de leur fiabilité.

Comment ? En élevant drastiquement le niveau de sensibilisation et d'équipement en solutions cyber des organisations, des chaînes d'approvisionnement, avec la nécessité de notifier un incident majeur lorsqu'il survient. Certes, ces nouvelles obligations vont nécessiter des investissements initiaux qui peuvent inquiéter les entités concernées. Mais ceux-ci sont à mettre en perspective avec les coûts et les pertes que représentent pour elles l'explosion de la menace et des cyber-attaques. Investir aujourd'hui dans la cyber-protection des organisations est indispensable pour s'assurer de la résilience et donc de la compétitivité future de notre économie.

### b) NIS 2 : Une opportunité unique pour l'industrie française de cyber

En cyber aussi, l'organisation des JO 2024 a été un moment de fierté collective. Elle a montré la capacité de la France à mobiliser ses entreprises et ses talents avec les acteurs étatiques pour

répondre en filière aux enjeux de cybersécurité quand les échéances l'exigent. Poursuivant cette dynamique, l'entrée en vigueur de NIS 2 représente une opportunité unique pour l'industrie française de la cybersécurité de grandir autour d'une cause durable : celle de la résilience des entreprises et des utilisateurs de numérique.

En effet NIS2 va logiquement générer un investissement durable des organisations dans leur cybersécurité, et la filière française de cyber composée de grands groupes et de start-ups innovantes de croissance, est déterminée à accompagner en partenaire notre économie et l'économie européenne.

Une telle approche serait gagnant-gagnant pour tous. Pour nos entreprises nationales, avec un accompagnement dans leur montée en compétence cyber via des solutions locales, compétitives et performantes. Et pour notre filière industrielle une occasion unique sur laquelle capitaliser pour atteindre une taille critique et se développer.

Rares sont les législations capables de transformer un secteur tout entier, dans un domaine aussi prometteur, créateur d'emplois qualifiés, générateur de compétitivité, et de croissance pour la France et l'export. A l'heure où la FrenchTech et la souveraineté industrielle sont au cœur des missions gouvernementales, la cyber est probablement l'un des secteurs où le potentiel pour faire émerger des ETI est le plus important, agissant à la croisée de l'IA de confiance et du cloud souverain.

Un texte ambitieux permettra ainsi d'accompagner notre industrie émergeante, et la positionnera comme un acteur majeur de la transposition de la directive à travers toute l'Europe.

### c) NIS 2, un passage obligé pour continuer à jouer les premiers rôles européens sur le numérique

La France a été un moteur historique pour construire autour de RGPD et NIS, un espace numérique plus résilient en Europe, plus fiable et plus durable sur le continent. Ce travail de longue haleine commencé avec NIS1, il y a 10 ans, pour les 200 opérateurs d'importance vitale, devient avec NIS2 en 2024, un standard de la résilience pour tous, avec un marché européen de 150 000 entités concernées, qui doivent se mettre en conformité.

Sous l'impulsion de l'écosystème et de la Stratégie Nationale de Cybersécurité, notre pays a vu émerger en parallèle une génération de startups qui incarnent cette évolution majeure avec des solutions adaptées aux besoins des utilisateurs, portées par les acteurs du service informatique. Sous l'impulsion de ce double effort, la France qui ambitionne un leadership européen dans le Numérique et l'IA doit réussir ce rendez-vous de la transformation numérique européenne qu'est NIS2 si elle souhaite préserver cette place.

Transposer ce texte en prenant le temps du débat parlementaire pour impulser une véritable politique pour le numérique et la cybersécurité à l'échelle nationale, c'est envoyer à nos partenaires européens le message que nous souhaitons conserver ce leadership et porter l'idée d'un numérique responsable pour tous. C'est également envoyer à tous les usagers connectés, c'est-à-dire nous tous, le message que la France est prête à relever le défi de la résilience et de l'avenir.

### d) La cybersécurité ne peut pas attendre, et la France doit avancer

Le 17 octobre, c'est aujourd'hui et la cybermenace est au rendez-vous. La France doit organiser son bouclier et renforcer sa cyber-résilience quoiqu'il arrive. L'étape de la transposition de la directive NIS 2 est un moment clé dans notre histoire, un véritable moment de réflexion collective sur l'ambition française en termes de protection numérique et de souveraineté.

Dans ce contexte, les acteurs industriels, la filière des Solutions Numériques de confiance, l'État représenté par l'ANSSI et Cybermalveillance, les écosystèmes regroupés dans les Campus Cyber à Paris et dans toutes les régions, ainsi que les groupements professionnels et associatifs sont préparés et mobilisés en Equipe de France de la cybersécurité. Celle-ci est prête à accompagner aujourd'hui le Gouvernement et le Parlement dans le nécessaire travail de transposition ; et demain à être le partenaire des entreprises françaises pour assurer la mise en œuvre de ce texte crucial. Il en va de l'avenir de notre industrie, de la résilience de notre économie, et du maintien du leadership européen de la France en matière de numérique.

*Document 2 :* **L'importance de la directive NIS2 pour la cybersécurité et la conformité des entreprises**
**Solutions Numériques&Cybersécurité - 17 octobre 2024**
*Par Marc Lenoble, Key Account Manager, Public Sector chez Synology*

Cette directive se distingue par son champ d'application large et son accent sur la protection des infrastructures critiques. De nombreuses normes ont été adoptées comme le RGPD qui protègent les données personnelles mais ne priorisent pas la résilience opérationnelle des secteurs critiques. NIS2 complète les normes industrielles existantes qui se concentrent uniquement sur la sécurité de l'information pour des industries ou types de données spécifiques. Avec une gamme plus large de secteurs et en mettant en place un cadre de cybersécurité uniforme à travers l'UE, NIS2 comble les lacunes en imposant des normes qui assurent à la fois la protection des données et la résilience face aux menaces cybernétiques.

## La nouvelle directive couvre plus d'entités qu'auparavant

NIS2 s'applique désormais à plus de 100 000 entités, élargissant la Directive NIS originale en couvrant plus de secteurs et en introduisant deux catégories d'organisations : les Entités Essentielles, qui incluent des secteurs critiques comme l'énergie, la santé et les infrastructures numériques, et les Entités Importantes, couvrant des industries comme la production alimentaire, les services postaux et la gestion des déchets. Ces entités doivent adhérer à des mesures de cybersécurité plus strictes, améliorant la résilience et les capacités de réponse à travers l'UE. La nouvelle directive assure une protection plus complète des industries clés et renforce la coordination et la supervision des efforts de cybersécurité.

De plus, si l'entreprise est basée en dehors de l'UE mais offre des services critiques au sein de l'UE, la Directive NIS2 s'applique également, car elle étend son champ d'application pour couvrir les entités non-UE qui fournissent des services essentiels ou importants au sein de l'UE. Cela signifie que les entreprises devront se conformer aux mesures de cybersécurité plus strictes suggérées par les nouvelles directives pour assurer la sécurité et la résilience des services fournis sur le marché de l'UE. La première chose que les entreprises doivent vérifier est si elles opèrent dans les régions couvertes par la nouvelle directive.

## Les différences entre une directive et un règlement

En plus de NIS2, il en existe d'autres comme le RGPD, le NIST CSF, l'ISO27001, mais quelles sont les distinctions entre les directives, les règlements ou les cadres ? Dans l'Union Européenne, les directives sont des actes juridiques, comme NIS2, qui doivent être transposés en droit national par chaque État membre, permettant des interprétations spécifiques à chaque pays. Les règlements, comme le RGPD, sont contraignants dans tous les États membres sans nécessiter de transposition, assurant une application uniforme. Enfin, les cadres comme le NIST CSF, l'ISO 27001, SOC 2 et PCI DSS sont des meilleures pratiques largement adoptées mais non contraignantes légalement. Dans ce contexte, NIS2, en tant que directive, complète ces cadres en établissant des normes de cybersécurité plus strictes et transposables à travers l'UE.

## Comment les organisations peuvent-elles se préparer à NIS2 ?

NIS2 met l'accent sur des approches proactives de la cybersécurité, ce qui rend essentiel pour les organisations de traiter les incidents après leur survenue, mais aussi de prévenir et d'atténuer les

risques à l'avance. Elle est construite autour de quatre piliers clés : la responsabilité des entreprises, la gestion des risques, les obligations de reporting et la continuité des activités.

### *Les dirigeants doivent désormais jouer un rôle plus actif et informé*

La responsabilité des entreprises est un aspect fondamental de la cybersécurité sous NIS2. La cybersécurité est la responsabilité des départements informatiques mais aussi une priorité stratégique au niveau du conseil d'administration. Les dirigeants et les cadres doivent assumer directement la responsabilité de la posture de cybersécurité de l'organisation au lieu de déléguer cette responsabilité uniquement à l'équipe informatique.

### *Des pratiques de gestion des risques plus robustes pour minimiser les cybermenaces*

Maintenant que les dirigeants deviennent plus vigilants, il est également important de diriger les organisations pour atténuer les risques potentiels. Une gestion efficace des risques implique l'intégration de protocoles robustes de réponse aux incidents, la sécurisation de la chaîne d'approvisionnement et la protection du réseau et des données par des mesures comme le chiffrement. Un Software Bill of Materials (SBOM) peut aider les organisations à obtenir une visibilité sur les vulnérabilités des logiciels tiers. De plus, l'adoption d'un modèle de sécurité Zero-Trust renforce les défenses en vérifiant chaque utilisateur et chaque appareil avant de leur accorder l'accès au réseau.

### *Assurer la continuité des Activités et les plans de récupération après sinistre en cas de grand incident*

La NIS2 met fortement l'accent sur la planification de la continuité des activités et de la récupération après sinistre (BCDR), soulignant la nécessité de systèmes de sauvegarde robustes et de stratégies pour garantir que même en cas de cyberattaque, les opérations peuvent reprendre rapidement et les perturbations sont minimisées. Des solutions de sauvegarde fiables existent, qui protègent non seulement les charges de travail physiques et virtuelles mais assurent également la récupérabilité rapidement et sont cruciales pour maintenir la résilience dans le paysage actuel des menaces.

### *Mettre en place des processus pour un reporting rapide des Incidents*

La NIS2 met l'accent sur le reporting rapide des incidents, exigeant des organisations de notifier les autorités peu après la détection d'attaques significatives. Un reporting rapide aide à minimiser l'impact plus large des attaques, assurant une réponse coordonnée et une récupération plus rapide. Ce délai strict encourage les organisations à avoir des processus établis pour identifier, documenter et signaler les incidents de manière efficace.

La Directive NIS2 renforce les mesures de cybersécurité à travers les secteurs critiques et importants en imposant des délais de reporting plus stricts, des processus de gestion des risques améliorés et des sanctions plus sévères pour non-conformité. Cependant, malgré le fait que NIS2 soit transposée en lois locales d'ici octobre 2024, il reste encore 1 à 2 ans pour se préparer pleinement. Les organisations sont fortement encouragées à prendre des mesures immédiates en établissant une force opérationnelle dédiée pour adopter les lois dérivées de NIS2 et en révisant leurs infrastructures de cybersécurité et de protection des données.

Document 3 : **Plusieurs collectivités françaises visées par une cyberattaque pro-russe**
Usine Digitale – 02/01/25 par Yoann Bourgin

Ces attaques par déni de service (DDoS) ont rendu inaccessibles plusieurs sites internet de collectivités territoriales, dont les villes de Marseille, Bordeaux et Nantes. Le parquet de Paris a ouvert une enquête pour entrave à un système de traitement automatisé de données en bande organisée.

Plusieurs sites internet de villes et de départements français ont été ciblés par des attaques par déni de service (DDoS) les 31 décembre 2024 et 1er janvier 2025. Cette méthode d'attaque consiste à submerger les serveurs informatiques de requêtes automatiques jusqu'à les rendre indisponibles.

### a) Plus d'une dizaine de grandes villes françaises ciblées

La première salve de cyberattaques a eu lieu le 31 décembre au matin, contre les sites internet des villes d'Angers, Bordeaux, Le Havre, Marseille, Nantes, Nice, Nîmes, Pau, Poitiers et Tarbes. Certains départements de l'Hexagone ont également été ciblés (Haute-Garonne, Landes) ainsi que deux territoires d'outre-mer, la Nouvelle-Calédonie et la Polynésie française. Ces sites renvoyaient alors vers une page d'erreur 503 de serveur indisponible ou d'erreur d'accès en HTTPS.

Le lendemain, le portail de la ville de Montpellier a été rendu hors-service, tout comme les départements de l'Aude et de l'Eure, la région Centre Val-de-Loire et la Chambre de commerce et d'industrie des Hauts-de-France. Le site du ministère de la Justice était également inaccessible, de même que celui du fournisseur d'électricité Enercoop. Les portails ont désormais été rétablis.

### b) Une opération justifiée par l'aide militaire de la France à l'Ukraine

Le parquet de Paris a ouvert une enquête pour “entrave à un système de traitement automatisé des données (STAD) en bande organisée” et a confié les investigations à la DGSI. Certaines municipalités, comme Marseille ou Nice, ont également indiqué qu'elles allaient porter plainte de leur côté.

Dans plusieurs messages postés sur son compte X (ex-Twitter), le groupe de hackers pro-russes NoName057(16) a revendiqué la quasi-totalité des cyberattaques. *“L'Ukraine a reçu 150 millions d'euros du Danemark, de la France et de la Lituanie pour soutenir l'industrie de défense*, écrivent les cybercriminels. *(…) Nous avons décidé de “féliciter” la France russophobe”*. Le groupe affirme avoir rendu hors-service d'autres sites, comme celui d'AXA, de l'Arcep ou de la Préfecture de police.

## Conséquences limitées

Bien que ce type d'attaques puisse paraître impressionnant au regard des entités visées, les dégâts restent généralement limités et disparaissent en quelques heures. Repéré pour la première fois en 2022, NoName057(16) est spécialisé dans les attaques par déni de service. Le groupe est notamment à l'origine d'attaques DDoS contre le Parlement européen, l'Assemblée nationale, le Sénat et la RATP.

**Document 4 : 2025 : année européenne de la cybersécurité**
Linkedin – 16/12/24
Gaël Le Roux - EU law & policy / Affaires européennes

La nouvelle Commission européenne, qui a pris ses fonctions en cette fin d'année, compte parmi ses membres une commissaire en charge du numérique dont le portefeuille couvre la **Souveraineté technologique, la sécurité et la démocratie.** Loin d'être anecdotique, l'association de ces trois thématiques confiées à la Finlandaise Henna Virkunnen, témoigne d'une prise de conscience par l'Union européenne du lien consubstantiel entre le développement technologique, les intérêts stratégiques et la défense d'un modèle de société.

Alors que convergent une série d'obligations réglementaires en matière de cybersécurité (DORA, NIS2, CRA…), 2025 s'annonce donc plus que jamais (pour ceux qui en doutaient) comme l'année européenne de la cybersécurité !

Un défi de plus à surmonter pour des entreprises déjà confrontées à de nombreuses difficultés certes. Mais, si elle est souvent perçue comme une contrainte, la cybersécurité peut tout autant s'avérer être un facteur de compétitivité. En effet, c'est un moyen de renforcer la confiance de ses clients et partenaires, d'optimiser la numérisation de son activité, de mieux valoriser ses actifs matériels et immatériels, d'accéder à des financements ou encore de s'ouvrir certains marchés... Ainsi, une stratégie cyber bien élaborée et efficacement implémentée n'est plus un poste de coûts, mais devient un levier de croissance à exploiter.

Mais par où commencer? Quelles priorités retenir? Quels moyens envisager? Quelles expertises et compétences mobiliser? Pour répondre à ces interrogations légitimes, une compréhension globale du cadre réglementaire cyber est nécessaire.

- Pourquoi autant de nouvelles règles d'un coup ? Dans un contexte d'augmentation du nombre, de l'ampleur, de la sophistication, de la fréquence et de l'impact des attaques, un arsenal réglementaire complet a dû être élaboré. Ces règles visent à embarquer une **masse critique d'acteurs** dont l'action coordonnée à l'échelle européenne permettra de rehausser le niveau global de cybersécurité de notre économie et de notre société. Le message est clair: puisque personne n'est immunisé contre le risque, chacun à la responsabilité de l'anticiper, le limiter et le gérer dans la mesure de ses capacités.
- Quels sont les points communs entre ces règles ? Qu'ils s'agisse de DORA, de NIS2 ou du CRA, elles postulent toutes un changement de paradigme qui consiste à ne plus considérer que les acteurs de l'économie et de la société ont un droit à la sécurité, mais bien **une obligation de sécuriser**. En choisissant cette approche, l'Union européenne confie à certains acteurs clés une mission d'intérêt général dont l'exécution est assurée au niveau de chaque entité susceptible d'être visée ou de chaque produit avant sa mise sur le marché. Néanmoins cette action déconcentrée est coordonnée par un cadre juridique harmonisé permettant de favoriser la transparence et de faire émerger une méthodologie commune.
- Comment ces règles sont elles conçues et que vont elles concrètement impliquer? Ces textes partent du constat que la sanction d'une violation de la sécurité *ex post* n'est pas aussi efficace que l'obligation de la prévention du risque *ex ante*. Cela implique pour l'entreprise de **gérer le risque cyber de manière proactive** dans son organisation et/ou sa production et d'être en mesure de le prouver. Cette logique de conformité implique la mise en place de mesures qui doivent être organisées, répertoriées et auditées par des

acteurs identifiés comme responsables, car capables, de sécuriser l'économie et la société à leur échelle.

- Comment doit on les appliquer? Il convient en priorité pour une entreprise d'identifier quel(s) cadre(s) réglementaire(s) s'applique(nt), dans quels délais, avec quels spécificités, et impliquant quelles actions clés. Il faut ensuite s'approprier les **méthodes de la compliance** à mi-chemin entre le contrôle juridique et la gestion de projets. Il faut enfin mobiliser des moyens techniques, opérationnels et juridiques et les intégrer dans une stratégie de cybersécurité globale et déclinable à l'échelle de l'entité et/ou des produits qu'elle met sur le marché.
- Qui doit on mobiliser? La **cybersécurité est un sujet stratégique** qui doit être piloté au niveau de la direction et impliquer tous les postes d'encadrement clés. C'est aussi un sujet global qui doit prendre en compte l'ensemble des parties prenantes d'une entreprise à commencer par ses salariés mais aussi par ses fournisseurs, ses clients et ses sous-traitants. La cybersécurité enfin un sujet pluridisciplinaire qui nécessité de rassembler les experts de différents métiers: RSSI, RH, responsable qualité, responsable supply chain, responsable juridique et conformité...

L'Union européenne a tracé le chemin que les entreprises européennes doivent désormais emprunter. De la multinationale à la PME en passant par les entités publiques, chacun a désormais un rôle à jouer dans ce processus qui prendra plusieurs mois, voire années. Le défi est grand mais l'enjeu à la clé l'est tout autant: Il en va de notre prospérité et de notre souveraineté.

**Document 5 : To do list de rentrée d'un RSSI : quelques mesures pour faire évoluer sa stratégie de cyber défense**
**Solutions Numériques&Cybersécurité – 12 septembre 2024 -** Par Romain VERGNIOL

Faire le point chaque année sur sa stratégie de cybersécurité est désormais un impératif stratégique pour l'ensemble des organisations. En effet, pour se protéger de menaces toujours plus complexes, les entreprises de toutes tailles se doivent de mettre en œuvre des dispositifs efficaces qui leur permettront de limiter leur exposition aux cyber risques. Dans ce contexte, la rentrée est un bon moment pour prendre le temps nécessaire afin d'analyser l'existant et de définir les évolutions à venir pour renforcer sa gouvernance cyber (moyens nécessaires, actions à mettre en place…).

- ***Se baser sur une analyse du risque objective***

En ce sens, il faut prendre en considération toutes les composantes propres à l'organisation, existantes à l'instant T, et y intégrer les éventuels nouveaux périmètres et opérations qui ont pu faire évoluer le schéma existant (rachats d'entreprises, nouvelles organisations, déménagements…). Le contexte externe doit également être évalué : évolution de la menace cyber, des règlementations et des évènements géopolitiques. Il est alors possible d'avoir une cartographie concrète et actualisée des nouveaux risques et d'identifier les plus sensibles. Pour mener à bien cette tâche, les RSSI peuvent s'appuyer sur des schémas éprouvés à l'image de la méthode EBIOS Risk Manager de l'ANSSI qui permet d'apprécier les risques et d'identifier les mesures de sécurité à mettre en œuvre pour les maitriser. On notera enfin qu'il est important de prendre en considération la dimension sectorielle et contextuelle propre à chaque entreprise pour être parfaitement exhaustif.

- ***Intégrer la composante humaine***

À l'occasion du mois de la cyber en octobre, il est opportun de prendre le temps de sensibiliser tous les collaborateurs aux sujets de la cybersécurité afin qu'ils puissent intégrer les bons réflexes et les bonnes pratiques à adopter dans des situations diverses : ne pas cliquer sur certains liens, être vigilants dans différents cas d'usage… Des campagnes de sensibilisation dans plusieurs formats peuvent ainsi être proposées et adaptées au profil des équipes. Cette étape de sensibilisation est un maillon central d'une bonne gouvernance cyber.

Toujours au niveau des équipes, la rentrée est le bon moment pour évaluer et budgéter précisément les nouvelles ressources dont aura besoin l'entreprise sur les prochains mois : embauche de nouveaux talents, recherche de support en externe sur certains profils… Ces demandes doivent s'appuyer sur l'analyse de risque préalablement réalisée.

- ***Tester la résilience de son infrastructure et de son SI***

Enfin, une autre mesure, à prendre en compte, consiste à faire le point sur son Plan de Continuité d'Activité (PCA) et de le tester via des exercices pour s'assurer que les services et activités critiques pourront toujours être opérationnels en cas de crise. Il est donc vital de s'assurer que ce point soit maitrisé et que les équipes en charge de le gérer soient formées et rompues à l'exercice.

Ces trois points structurants sont donc les actions fondamentales à adopter pour faire évoluer son dispositif et s'assurer que son organisation puisse s'appuyer sur une gouvernance cyber actualisée et adaptée à son organisation.

**Document 6 : Cyberattaque à Saint-Nazaire : "on est passés au papier, à la gomme et au crayon"**

19/04/2024 - Écrit par Olivier Quentin – France3 Région

**Un tiers des 450 serveurs de la ville et de l'agglomération de Saint-Nazaire a été crypté par le virus.**

Dans la nuit du 9 au 10 avril, les services de la Ville et de l'Agglomération de Saint-Nazaire ont été la cible d'une cyberattaque. "Il faudra deux ans pour s'en remettre" dit Le maire, David Samzun qui faisait le point ce vendredi sur les conséquences de ce qui est officiellement une demande de rançon via un cryptovirus.

Le maire de Saint-Nazaire s'est voulu très transparent sur l'ampleur et les conséquences de la cyberattaque dont a été victime sa ville et l'agglomération qu'il préside : "C'est une cyberattaque, ce n'est pas un incident cyber" a commencé par préciser Didier Delaunois, directeur des systèmes d'information de la ville, présent lors de la conférence de presse, aux côtés du maire et président de l'agglomération, David Samzun.

Pour réactiver ces systèmes, il était indiqué qu'il fallait payer une rançon et, pour cela, cliquer sur un lien.

"Nous nous sommes interdits de le faire, ne sachant pas ce que ça allait déclencher derrière, déclare David Samzun. Et je préfère financer de la solidarité que de payer une rançon."

Depuis, tous les ordinateurs des deux collectivités sont à l'arrêt et il n'est, pour le moment, pas question de les rallumer.

"On est passés au papier, à la gomme et au crayon", constate le maire de cette ville de la côte Atlantique qui compte, avec l'agglomération, plus de 127 000 habitants... et 2 000 agents, plus ou moins impactés.

## Le standard sur un téléphone portable

Le standard est hors service, les appels qui y arrivent sont désormais déroutés sur un 06 où un agent prend en note la demande et va la transmettre physiquement au service concerné. On imagine difficilement la galère que vivent les personnels qui doivent tout prendre en note.

"Nous créons un tas de sable" constate David Samzun pour imager ce qui se passe. Car toutes ces prises de note devront être, plus tard, saisies sur les ordinateurs de la ville. Mais quand ?

## Deux ans pour retrouver un service de niveau

Lors d'une telle attaque, il faut, expliquent les spécialistes, deux heures pour comprendre ce qui se passe, deux semaines pour analyser comment cela s'est passé et par où les pirates se sont introduits dans le système et, enfin, deux ans pour trouver un niveau de service informatique équivalent à celui qui a été détruit.

Multipliant les métaphores pour bien faire comprendre dans quelles difficultés se trouvent les services, David Samzun, a comparé ce qui s'est passé à une tour d'une vingtaine d'étages qui a été détruite et qu'il faut entièrement reconstruire. Un travail qui est déjà enclenché.

Pour exemple, la prise de rendez-vous pour l'État Civil est à nouveau possible, le service de la restauration scolaire est rétabli, tout comme celui de la collecte des déchets ou des inscriptions sur les listes électorales. Ce qui, à la veille du scrutin européen, à son importance.

Hommage a été rendu à cette occasion aux personnels de la Ville et de l'Agglomération pour leur professionnalisme dans la gestion de cette crise. "Les paies seront versées" a rassuré le maire. Même si certaines lignes manqueront. Notamment celles des heures supplémentaires et on peut penser qu'il y en aura.

Un appel a été lancé à plusieurs reprises à la population et aux partenaires de la collectivité pour qu'ils fassent preuve de patience et de compréhension dans cette période dont on ne sait combien de temps elle durera exactement.

Le service urbanisme est encore dans le noir ainsi que celui des factures d'eau ou de la réservation pour les centres de loisir.

## Une plainte déposée

Très vite après la détection de l'attaque, il a été fait appel à l'Agence Nationale de la Sécurité des Systèmes d'Information de l'État, l'autorité nationale en matière de cybersécurité et de cyberdéfense, qui connait les systèmes de Saint-Nazaire pour avoir déjà été sollicitée préventivement. Son expertise ne sera pas de trop.

À combien va s'élever la note de cette attaque ? Impossible de le dire. Une plainte a été déposée auprès du parquet de Paris spécialisé dans ce type de délinquance.

Parallèlement à la remise en route des services, une crainte demeure : le virus a-t-il amené avec lui un "cheval de Troie", autre programme informatique malveillant qui attend, tapi dans l'ombre des serveurs, de se déclencher ? Une fuite de données est-elle possible ?

"Nous devons prendre toutes les précautions, répond Didier Delaunois, le directeur des systèmes d'information de la ville. On n'a pas détecté de volumes de données qui seraient sortis".Ce à quoi David Samzun ajoute "peut-être que dans une heure, deux heures, on sera amenés à dire le contraire."

"Toute attaque a aussi pour objet de subtiliser des données", confirme Didier Delaunois.

Il est vivement demandé à tous les usagers des services de la ville et de l'agglomération, population ou entreprises, de changer leurs codes d'accès.

"Prenez-soin de blinder vos mots de passe" insiste David Samzun, dont le conseil dépasse le simple champ des démarches administratives.

## D'où vient l'attaque ?

Pas de réponse précise à cette question, mais un contexte international. La Russie n'est pas nommée, mais son ombre plane. "Il y a une volonté de déstabiliser les collectivités à la veille des JO" remarque le maire de la ville.

Chaque jour, la collectivité nazairienne est la cible de 150 à 200 cyberattaques, peut-être plus, selon le directeur des systèmes d'information. "Ce sont des attaques qui sont automatisées, explique-t-il. Quand une faille est identifiée, le pirate prend la main."

## De nombreuses attaques

Un système bien rodé qui fait appel à plusieurs niveaux de compétences avec, pour chacun, un domaine d'intervention. Il y a celui qui conçoit l'attaque, celui qui la met en œuvre et celui qui gère la demande de rançon. Une mécanique bien huilée qui fait de plus en plus de victimes dans les grosses institutions.

France Travail en a été victime récemment. La ville d'Angers également en 2021 ainsi qu'une clinique de cette ville.

"Nous étions avertis qu'il y avait une recrudescence de ces attaques, reconnait Didier Delaunois. Des attaques comme celle d'Angers donne lieu à des retours d'expérience."

Celle de Saint-Nazaire générera son lot de conclusions et de précautions à prendre, d'outils à activer, de process à suivre. « C'est une nouvelle guerre » conclut le maire de Saint-Nazaire.

**Document 7 : Panorama Cybermenace – ANSSI 2024 – Extrait p4-5 et 10-11**



# INTRODUCTION

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) est l'autorité nationale en matière de cybersécurité.

Le *Panorama de la cybermenace* est un document publié annuellement, couvrant une période allant du 1er janvier au 31 décembre de l'année précédente, dans lequel l'ANSSI revient sur les grandes tendances de la menace informatique ainsi que sur les éléments et incidents marquants dont elle a eu connaissance sur cette période.

Principalement destiné à la sphère institutionnelle et aux bénéficiaires de l'Agence, le *Panorama de la cybermenace* s'adresse également à la communauté française de la cybersécurité au sens large ainsi qu'aux partenaires internationaux de l'ANSSI.

Écrit du point de vue de l'ANSSI, il ne constitue pas une revue exhaustive de l'actualité de la cybersécurité française en 2024. Au-delà de son objectif de sensibilisation à la menace pesant sur la sécurité des systèmes d'information, le *Panorama* illustre également l'importance de l'application des mesures de sécurité.

Dans la continuité des années précédentes, l'ANSSI estime aujourd'hui que les attaquants liés à l'écosystème cybercriminel ou réputés liés à la Chine et la Russie constituent les trois principales menaces tant pour les systèmes d'information (SI) les plus critiques que pour l'écosystème national de manière systémique.

L'année 2024 a été marquée par l'organisation des Jeux Olympiques et Paralympiques de Paris (JOP 2024), dont l'exposition médiatique et la surface d'attaque ont constitué des opportunités majeures pour les attaquants. Dans ce cadre, l'ANSSI a observé des attaques à des fins d'extorsion et d'espionnage stratégique, et une majorité d'attaques à but de déstabilisation menées par des groupes *hacktivistes* sans qu'aucune de ces attaques ne porte atteinte au déroulement de l'événement.

L'année a également été marquée par le nombre et l'impact des vulnérabilités affectant les équipements de sécurité situés en bordure de SI : plus de la moitié des opérations de cyberdéfense de l'ANSSI, constituant son plus haut niveau d'engagement en réponse à incident, ont ainsi eu pour origine l'exploitation de vulnérabilités sur ces équipements.

Du point de vue des moyens mis en œuvre par les attaquants, l'ANSSI a constaté la poursuite des attaques visant la chaîne d'approvisionnement pour atteindre des cibles finales d'intérêt. Ces attaques, qui sont en constante expansion depuis la fin des années 2010, illustrent combien la maîtrise du SI, de ses interconnexions et de ses dépendances est un enjeu majeur pour les organisations.

En parallèle, l'utilisation des réseaux d'anonymisation par les attaquants se poursuit. Ces réseaux de machines compromises communiquant entre elles permettent à un attaquant de dissimuler ses actions et rendre difficile leur imputation, à toutes les étapes de l'attaque informatique. Ils constituent des infrastructures qui se développent, se complexifient et dont les utilisateurs ne sont pas toujours clairement identifiables. L'essor des entreprises privées de lutte informatique offensive (LIOP) se poursuit quant à lui avec la mise à disposition à un éventail relativement large de clients, de capacités qui étaient jusqu'alors l'apanage des États les plus avancés en matière cyber.

Les attaques par rançongiciel ont largement mobilisé les équipes de l'ANSSI en 2024 avec un nombre d'incidents comparable à l'année passée. Les attaques à but d'espionnage ont quant à elles été caractérisées par le ciblage soutenu d'équipements et d'infrastructures de télécommunications.

Enfin, en plus des attaques à but d'espionnage et d'extorsion, qui restent les plus importantes en termes d'investissement des équipes de l'ANSSI, 2024 a marqué une hausse des attaques à finalité de déstabilisation, notamment opérées par des groupes *hacktivistes*.

**Que faire en cas de compromission ?**

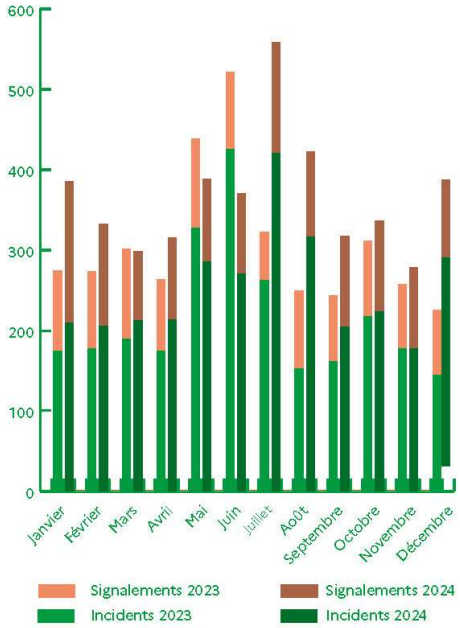
En cas de compromission ou de suspicion de compromission, le CERT-FR vous invite à prendre connaissance de cette page : *https://www.cert.ssi.gouv.fr/les-bons-reflexes-en-cas-dintrusion-sur-un-systeme-dinformation/*

Le CERT-FR est joignable :
- Par téléphone :
→ depuis la France métropolitaine au 3218 (service gratuit + prix d'un appel) ou 09 70 83 32 18
→ depuis certaines collectivités territoriales situées en outre-mer ou depuis l'étranger au +33 9 70 83 32 18
- Par courriel :
→ à l'adresse *cert-fr@ssi.gouv.fr*

## Comparatif du nombre d'incidents et signalements 2023/2024

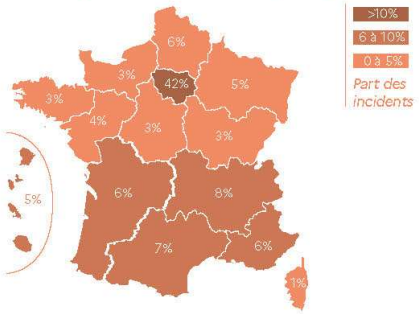
Au cours de l'année 2024, l'ANSSI a traité – avec un degré d'engagement variable – 4386 événements de sécurité[1], soit une augmentation de 15% par rapport à l'année 2023.

Ainsi, 3004 signalements[2] et 1361 incidents[3] ont été portés à la connaissance de l'ANSSI. Cette augmentation peut trouver une explication dans le contexte des JOP 2024, qui s'illustre par une hausse des signalements et des incidents à partir du mois de mai – date de l'arrivée de la flamme olympique en France – jusqu'à la cérémonie de clôture des Jeux Paralympiques en septembre, avec un pic de signalements atteint au mois de juillet.




## Répartition par région des incidents traités par l'ANSSI

Une observation de la répartition par région des incidents traités par l'ANSSI au cours de l'année montre que la menace affecte tous les territoires mais reste proportionnelle à l'activité économique et aux usages numériques de chaque région.




*Seuls les incidents ayant affecté des bénéficiaires qui sont présents uniquement dans ces territoires sont comptabilisés. À noter qu'un certain nombre de bénéficiaires de l'Agence ont leur siège social en région parisienne.*

## Capacités de détection de l'ANSSI

L'ANSSI opère un service de supervision au profit des ministères comprenant à la fois des moyens de détection réseau et système. En 2024, l'ANSSI a adressé 162 signalements aux institutions étatiques bénéficiant de ses services de détection. Ces signalements ont couvert majoritairement les domaines suivants[4] :

- Communications suspectes vers des infrastructures d'attaque, détectées à la fois en temps réel et à travers des recherches d'antécédents dans les journaux collectés ;
- Actions d'administration suspectes ou utilisation d'outils légitimes connus comme étant régulièrement détournés par des attaquants ;
- Exploitation ou tentative d'exploitation de vulnérabilités ;
- Campagnes d'hameçonnage ciblant certains ministères.

1 Événements portés à la connaissance de l'ANSSI et qui ont donné lieu à un traitement par les équipes opérationnelles.

2 Les signalements regroupent tous les comportements anormaux ou inattendus pouvant avoir un caractère malveillant ou ouvrir la voie à des usages néfastes à l'encontre d'un SI.

3 Un incident est un événement de sécurité où l'ANSSI est en mesure de confirmer qu'un acteur malveillant a conduit des actions avec succès sur le SI de la victime.

4 Les ministères disposant d'un service de détection traitent en complément les alertes de leurs systèmes d'information.

# B
# FAIBLESSES TECHNIQUES

Si l'actualité et les grands événements offrent aux attaquants des moments propices pour agir, les faiblesses techniques exposées par les SI leur fournissent quant à elles des opportunités constantes. Comme les années précédentes, l'ANSSI observe ainsi que des attaquants aux compétences variables sont en mesure d'exploiter les vulnérabilités de SI dont le niveau de sécurité est insuffisant. Le durcissement des SI et leur maintien en condition de sécurité permettent de réduire la surface d'attaque et les opportunités de latéralisation suivant le principe de défense en profondeur[5].

## 1/ RAPPEL DU TRIPTYQUE DES BONNES PRATIQUES DE SÉCURITÉ DES SYSTÈMES D'INFORMATION (SSI)

L'ANSSI rappelle que les bonnes pratiques pour protéger les SI et les maintenir en condition de sécurité se déclinent au travers des actions suivantes :

1. La sécurisation constitue la première ligne de défense. Elle vise à prévenir les attaques en réduisant l'exposition du SI et les possibilités de latéralisation, notamment au travers d'actions de durcissement, et à contraindre un attaquant à faire usage de techniques ou d'outils susceptibles de générer des événements journalisés ;
2. La supervision permet de détecter une activité malveillante au travers de l'analyse des journaux système, applicatifs ou réseau et de lever les alertes le plus tôt possible dans la progression d'un attaquant ;
3. La réponse à incident intervient en dernier lieu et comprend la gestion de crise, les investigations numériques et la remédiation. L'ANSSI a publié en 2024 trois guides dédiés aux volets stratégique, organisationnel et technique de la remédiation [07].

Les coûts de sécurisation du SI et de mise en place d'une supervision, qui permettent de limiter significativement le risque de survenue d'un incident de sécurité et de limiter sa gravité et son impact, sont souvent largement inférieurs à ceux de la remédiation.

## 2/ DURCISSEMENT DU SYSTÈME D'INFORMATION

L'ANSSI constate qu'un nombre important de ses bénéficiaires a recours à des produits ou services de détection d'incidents de sécurité. Toutefois, ces dispositifs n'atteignent leur plein potentiel que lorsque le SI a fait l'objet d'une sécurisation, avec en particulier l'application de mesures de défense en profondeur. D'une part, ces mesures permettent de ralentir la progression de l'attaquant et de réagir avant qu'il n'ait obtenu des privilèges élevés sur le SI, facilitant donc son éviction. D'autre part, elles rendent les tentatives de latéralisation plus complexes, générant ainsi de meilleures opportunités de détection. Enfin, elles permettent de limiter drastiquement les conséquences de la compromission du poste utilisateur, qui est par nature un élément très exposé du SI.

Selon ce principe, la priorité doit donc être donnée à la sécurisation de l'actif le plus critique du SI : l'annuaire d'authentification (ou le tenant dans le cas de l'utilisation de services nuagiques), le plus souvent un annuaire *Active Directory*[6].

S'il est essentiel, le durcissement de l'annuaire *Active Directory* ne permet pas de se prémunir de l'ensemble des attaques. Des incidents aboutissant au déploiement d'un rançongiciel ont notamment pu être observés dans les cas suivants :

- L'exploitation de la vulnérabilité *Zerologon* sur les contrôleurs de domaine *Active Directory* dont la version n'est pas à jour, permettant la compromission de l'ensemble du SI [08] ;
- L'absence de gestion du mot de passe du compte administrateur local des serveurs et postes de travail Windows, permettant également une latéralisation. Certaines solutions (comme le service LAPS de Microsoft) permettent de se prémunir de ce risque ;
- Le détournement de l'usage légitime d'applicatifs métier ou de gestion de parc mal configurés ou vulnérables (outils de sauvegarde, de déploiement de mises à jour ou de prise en main à distance,

5 Ces mesures peuvent inclure le durcissement des configurations, la mise en place de bonnes pratiques d'administration ou encore la mise en place de segmentation réseau.

6 L'annuaire *Active Directory*, centre névralgique de la sécurité des systèmes d'information Microsoft, est un élément critique permettant la gestion centralisée de comptes, de ressources et de permissions. L'obtention de privilèges élevés sur cet annuaire entraîne une prise de contrôle instantanée et complète de toutes les ressources ainsi administrées.

consoles antivirales ou EDR, etc.), permettant de compromettre une proportion significative d'un SI.

Le premier exemple illustre la nécessité de maintien en condition de sécurité des éléments critiques du SI. L'ANSSI constate qu'une part importante de ses bénéficiaires ayant un SI en environnement Microsoft dispose de serveurs et de postes de travail dans une version obsolète ou prochainement en fin de support :

- 82% des postes de travail[7] des organismes utilisateurs du service ADS de l'Agence utilisent le système d'exploitation Windows 10, dont la fin de support est prévue le 14 octobre 2025 (hors version LTSC et support étendu). L'ANSSI recommande d'initier les travaux de migration vers Windows 11 au plus tôt.
- 36% des serveurs Windows des organismes utilisateurs du service ADS se trouvent dans une version obsolète (Windows Server 2012R2 ou inférieur). L'ANSSI recommande de mettre à jour vers la version la plus récente du système d'exploitation afin de bénéficier de la plus grande période de support possible.

Parmi les mesures de défense en profondeur, la segmentation réseau interne est un moyen efficace pour réduire les possibilités de latéralisation de l'attaquant et faciliter la détection d'actions malveillantes. Elle peut notamment être mise en œuvre par l'utilisation de mécanismes réseau tel que le VLAN privé[8], associé à des règles de filtrage.

Les moyens d'authentification constituent également un élément central de la sécurisation du SI. L'ANSSI constate que certains moyens d'authentification comme le TOTP[9] ou l'utilisation d'une application tierce sont désormais contournés par les attaquants au moyen de nouvelles techniques (voir par exemple [09]). Il convient de préférer une authentification forte utilisant l'emploi de certificats ou de clés de sécurité.

Enfin, l'ANSSI rappelle l'importance de disposer de sauvegardes, y compris hors ligne. ←

**Mauvaises pratiques systémiques de configuration des annuaires *Active Directory***

Les mauvaises pratiques de configuration des annuaires *Active Directory* décrites ci-dessous sont un point commun à de nombreux SI ayant été victimes d'attaques informatiques, en particulier de chiffrement par un rançongiciel. En effet, des outils largement disponibles permettent de faciliter leur exploitation.

- **Comptes privilégiés ayant l'attribut ServicePrincipalName (SPN) positionné :** L'attribut SPN permet d'associer des noms de service Kerberos[10] à des comptes *Active Directory*. Lorsqu'un compte possède un nom de service Kerberos, n'importe quel utilisateur authentifié peut demander un ticket Kerberos pour ce service, et ainsi réaliser une attaque par force brute pour obtenir le mot de passe du compte (attaque couramment appelée *Kerberoasting*). Compte tenu de ces risques, l'attribut SPN ne devrait être positionné que sur des comptes de service non privilégiés.
- **Comptes à hauts privilèges dont le mot de passe est inchangé depuis plus de 3 ans :** Les mots de passe des comptes à hauts privilèges doivent être changés à une fréquence régulière de maximum 3 ans pour que ces secrets soient connus uniquement par les administrateurs actuels. L'ANSSI constate régulièrement des mots de passe de comptes à hauts privilèges inchangés depuis 15, 20 voire 25 ans et dont la complexité ne répond pas aux exigences actuelles.
- **Permissions d'enrôlement sur les modèles ou conteneurs de certificats :** Ce type de vulnérabilité est lié à une mauvaise configuration de l'infrastructure de gestion de clé Microsoft AD-CS permettant de générer des certificats de sécurité. Ainsi, un demandeur peut générer un certificat valable pour l'authentification Windows pour n'importe quel compte de l'annuaire, y compris les comptes à hauts privilèges.
- **Permissions dangereuses :** Les permissions d'un compte non privilégié vers des membres de groupes privilégiés, vers les contrôleurs de domaine, vers la racine des *naming contexts* ou vers les objets de GPO s'appliquant aux membres des groupes privilégiés permettent à un attaquant qui compromettrait ce compte de prendre le contrôle d'un élément critique de l'annuaire, et ainsi compromettre l'ensemble du SI.

L'ensemble de ces vulnérabilités est vérifié par le service ADS (*https://club.ssi.gouv.fr*) proposé par l'ANSSI à ses bénéficiaires [10]. 🐞

7 Disposant d'un support Microsoft.

8 *Private VLAN* ou PVLAN, technique de segmentation réseau qui permet de limiter les communications entre équipements reliés à un même commutateur.

9 TOTP: «*Time-based One-time Password*», mot de passe à usage unique basé sur le temps.

10 Kerberos est un protocole d'authentification reposant sur l'utilisation de tickets pour accéder à des services, couramment utilisé en environnement Microsoft.

Document 8 : Directive NIS 2 : les pouvoirs publics prônent de retenir le seuil des 30 000 habitants pour les collectivités
La Gazette – 11/03/24 – Publié par Gabriel Thierry

Le texte européen consacré à la cybersécurité laisse le choix aux Etats-membres d'inclure leurs collectivités dans le champ d'application. Les pouvoirs publics veulent faire classer les collectivités de plus de 30 000 habitants dans la catégorie des entités "essentielles".

On commence à y voir plus clair sur la façon dont les collectivités vont être impactées par l'arrivée de la directive européenne NIS 2 (Network and information security). Ce texte, adopté à la fin de l'année 2022, doit être transposé dans le droit français d'ici octobre 2024.
Mais pour les collectivités, il y a un grand flou qui tarde à se dissiper, celui du périmètre exact d'application de la directive. Le texte européen laisse en effet aux Etats-membres le choix d'inclure ou non les administrations publiques dans le champ d'application.

Certes, l'Anssi, le cyber-pompier de l'Etat, avait déjà expliqué qu'elle allait se saisir de la transposition pour demander l'intégration des collectivités dans le champ d'application. Mais sans donner vraiment plus de précisions, à part pour indiquer que les petites communes, telles celles de 500 habitants par exemple, ne seraient pas concernées par ce texte qui va entraîner toute une série d'obligations en matière de sécurité informatique.

Lors d'une audition à l'Assemblée nationale, Stéphane Bouillon, le patron du SGDSN, la tutelle de l'Anssi, vient toutefois d'en dire enfin un peu plus. Répondant à une question de la députée (Renaissance) de Seine-et-Marne Patricia Lemoine sur les partenariats de ce service du Premier ministre avec les collectivités, le préfet a indiqué qu'il était envisagé de considérer comme "entités essentielles" les régions, les départements, les communes et les intercommunalités de plus de 30 000 habitants.

## 2) Seuil attendu

La directive NIS2, qui a pour objectif d'harmoniser les règles en matière de sécurité informatique, distingue en effet deux types d'acteurs régulés aux obligations différentes, les entités essentielles et celles dites importantes. Ce seuil des 30 000 habitants, synonyme le plus souvent d'une direction des systèmes d'information déjà conséquente, est anticipé par une partie de la communauté numérique dans les collectivités. Il correspond en effet à celui de la création d'une communauté d'agglomération quand celle-ci comprend le chef-lieu du département.

Si le préfet Stéphane Bouillon n'a pas précisé les raisons du choix de ce seuil, il s'est toutefois attardé sur les attentes en matière de sécurité informatique des pouvoirs publics pour les collectivités de taille inférieure. Ces derniers ne vont pas leur demander "des choses impossibles". Mais elles ne devraient pas échapper toutefois à de nouvelles obligations, en étant classées "entités importantes".

"On leur demandera simplement de veiller à des actions d'hygiène informatique", a rassuré Stéphane Bouillon. Comme par exemple changer régulièrement de mots de passe, s'assurer de la certification et de la vérification des logiciels achetés, et avoir à disposition "des sauvegardes en nombre suffisant et débranchées des réseaux informatiques". Reste désormais à voir si les parlementaires suivront les pouvoirs publics pour ce seuil des 30 000 habitants.

La transposition – le projet de loi n'a pas encore été déposé – devant être votée au Parlement, ce sont in fine les députés et les sénateurs qui devraient trancher sur ce point. Dans un communiqué, Intercommunalités de France, France Urbaine et Les Interconnectés, des associations de collectivités, ont déjà appelé à la prudence, en plaidant pour "une transposition intelligente de la directive". "Le nombre d'habitants ne peut être le seul critère d'obligations imposées", ajoutent-elles.

Document 9 : Cyberattaque sur les serveurs de Val-de-Reuil : la Ville prend des mesures pour assurer la continuité du service public

05/09/2024 par Coline Lefèvre – Actualités du site https://www.valdereuil.fr

Depuis plusieurs jours, des incidents inhabituels ont été constatés sur le réseau informatique interne de la collectivité. Des investigations menées par les services de la Ville, soutenus dans leurs recherches par l'Agence Nationale de la Sécurité des Systèmes d'Information, ont permis d'en déterminer la cause. Elles font apparaitre qu'une cyberattaque d'origine inconnue a pris pour cible les serveurs de la Mairie.

Jusqu'à preuve du contraire et en l'état actuel des analyses, aucune fuite de données personnelles ou à caractère confidentiel n'a été décelée. Néanmoins et en vertu du principe de précaution, la Ville appliquera strictement les recommandations émises par les autorités.

À partir d'aujourd'hui et pour une durée pouvant aller de 24 à 48 heures, les lignes téléphoniques et Internet des services de la Ville sont donc suspendues. Avec l'appui de la direction régionale d'Orange, que la municipalité souhaite ici remercier, les accueils téléphoniques de la Mairie, du CCAS, de la Police municipale, du service des sports, de la résidence Espages et de la crèche des Noés restent accessibles et leurs numéros d'appel inchangés.

Le système de vidéoprotection, indépendant du réseau informatique municipal, reste opérationnel.

Les écoles, centres de loisirs, crèches familiale et du Pivollet ainsi que le Théâtre de l'Arsenal, dont les serveurs sont hébergés auprès d'un prestataire extérieur, ne sont également pas concernés.

En revanche, pour les démarches et les renseignements qui relèveraient d'autres services, il vous est recommandé d'utiliser le formulaire de contact mis en place par la Ville depuis son site Internet (https://www.valdereuil.fr/services-municipaux/demarches-en-ligne/nouscontacter) ou d'utiliser les adresses de messagerie rappelées ci-dessous :

- enfancejeunesse@valdereuil.fr
- dirfin@valdereuil.fr
- drh@valdereuil.fr
- etat-civil@valdereuil.fr
- comptoirdesassociations@valdereuil.fr
- environnement@valdereuil.fr
- urbanisme@valdereuil.fr
- mairie@valdereuil.fr

Par ailleurs, un accueil physique continuera à être assuré dans chacun des bâtiments municipaux selon les horaires habituels d'ouverture au public. Ces mesures visent à maintenir la continuité du service public municipal. Elles ont également pour but de limiter les éventuelles conséquences de cette attaque sur le fonctionnement régulier de la collectivité.Les élus et les agents de la Ville sont pleinement mobilisés pour assurer un retour à la normale dans les meilleurs délais. Nous vous remercions pour votre compréhension.

# 1 INTRODUCTION

Les collectivités territoriales sont des personnes morales de droit public exerçant, sur un territoire défini, des compétences qui lui sont déléguées par l'État. En France, ces collectivités revêtent plusieurs formes : les communes, plus petit échelon des collectivités territoriales, les Établissements Publics de Coopération Intercommunale (EPCI), les départements et les régions. La France dispose également de collectivités à statut particulier, regroupant parfois les compétences des départements et des régions (collectivités territoriales de Martinique, de Guyane, département de Mayotte), ou les compétences d'une commune et d'un département (Ville de Paris, Métropole de Lyon), ou bien encore en Outre-mer des collectivités disposant de compétences spécifiques (Polynésie française, Nouvelle-Calédonie, *etc*.).

Les collectivités territoriales gèrent de nombreux services selon leurs compétences, en matière administrative et régalienne (état civil), éducative (gestion des écoles, collèges et lycées), sociales (prestations sociales, centres sociaux), médicales (EHPAD), d'urbanisme, de gestion des ressources en énergie et en eau (approvisionnement et traitement), *etc*. Ces compétences sont exercées soit directement par les collectivités, soit en mutualisation par le biais de régies intercollectivités. Maillons essentiels de la relation entre l'État et les citoyens, les collectivités territoriales sont de fait dépositaires d'un très grand nombre de données personnelles de leurs administrés.

**Les conséquences d'attaques informatiques peuvent donc être majeures à l'échelle d'une collectivité, et affecter de multiples champs de compétences et de nombreux citoyens.**

# 2 BILAN DES INCIDENTS PORTÉS À LA CONNAISSANCE DE L'ANSSI EN 2024

De janvier à décembre 2024, l'ANSSI a traité **218 incidents cyber** affectant les collectivités territoriales, soit une **moyenne de 18 incidents par mois**. Le périmètre étudié prend en compte les communes, les établissements publics de coopération intercommunales (EPCI) [1] , les dé- partements, les régions, les collectivités territoriales uniques et collectivités d'outre-mer. **Ces incidents représentent 14% de l'ensemble des incidents traités par l'ANSSI sur la période**.

Au cours de l'année 2024, la majorité des évènements de cybersécurité touchant les collectivités territoriales portés à la connaissance de l'ANSSI concerne des communes et/ou des EPCI à fiscalité propre. Néanmoins, la prépondérance des communes et EPCI à fiscalité propre est à mettre en perspective avec leur nombre en France : il existe près de 35 000 communes, 1250 EPCI à fiscalité propre et près de 9000 EPCI sans fiscalité propre en 2023 sur l'ensemble du territoire national.

Au cours de la période étudiée, l'ANSSI a traité **44 incidents affectant des départements** et **29 incidents affectant des régions**. Ces chiffres se révèlent élevés en comparaison du nombre de départements (101) et de régions (18) sur le territoire français et pourraient indiquer un ciblage

1. Les EPCI sont des structures administratives françaises regroupant plusieurs communes afin d'exercer certaines de leurs compétences en commun. Il existe deux catégories d'EPCI : les EPCI à fiscalité propre (communauté de communes, communauté d'agglomérations, communauté urbaine et métropole) et les EPCI sans fiscalité propre (syndicats intercommunaux et syndicats mixtes).

plus important de ces structures et/ou un signalement d'incidents auprès de l'ANSSI effectué de façon plus systématique par ce type de collectivités territoriales. Enfin, l'ANSSI a traité 2 évènements de cybersécurité ciblant des EPCI sans fiscalité propre.

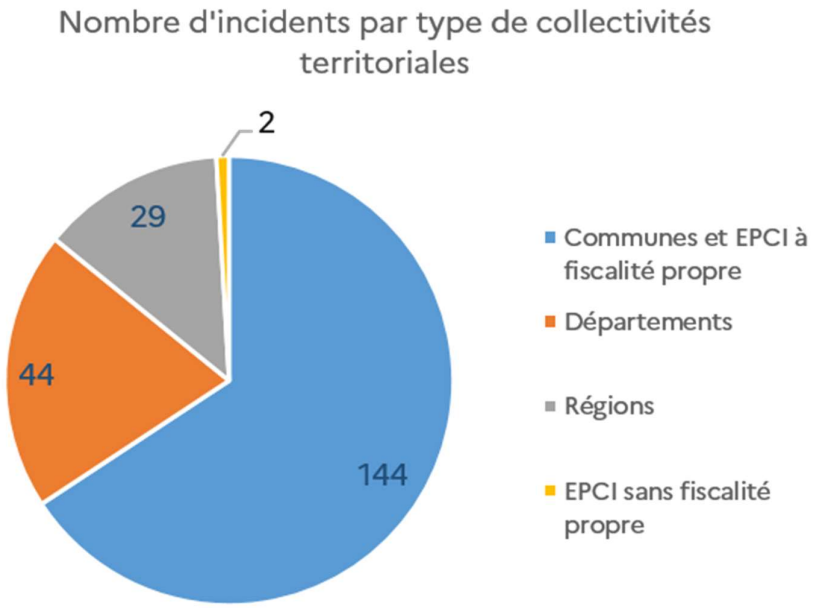



FIGURE 1 – Répartition des incidents portés à la connaissance de l'ANSSI en 2024

# 3 ATTAQUES À BUT LUCRATIF

**Les attaques à but lucratif représentent la principale menace cyber pour les collectivités territoriales.** Quelle que soit leur taille, elles sont ciblées de façon opportuniste par l'ensemble des acteurs de l'écosystème cybercriminel.

**Les collectivités territoriales sont en effet des cibles de choix pour ces acteurs** : souvent peu ou mal sécurisées, gestionnaires de systèmes d'information nombreux et disparates, elles peuvent éprouver des difficultés à maîtriser la cartographie de leurs réseaux et à les garder dans de bonnes conditions de sécurité.

## 3.1 Attaques au moyen de rançongiciels

Ainsi, de nombreuses municipalités en France et dans l'ensemble du monde sont victimes d'attaques menées par des groupes cybercriminels au moyen de rançongiciels. Ces attaques représentent une part importante de l'engagement opérationnel de l'ANSSI, tant au sein de l'Hexagone que dans les collectivités d'Outre-mer.

Au cours de la période étudiée, les collectivités territoriales se sont révélées être des cibles privilégiées de la **menace cybercriminelle**. Ainsi, parmi les incidents ayant affecté les collectivités portés à la connaissance de l'ANSSI, on retrouve majoritairement des **compromissions de comptes de messagerie** (66, soit 30% des événements signalés) puis les **attaques en déni de service distribué** (DDoS) (58).

L'ANSSI a également traité divers incidents relatifs à des **intrusions sur les systèmes d'information** (hors attaques par rançongiciel) allant de la **connexion illégitime réussie** jusqu'au **dépôt de code malveillant** sur le réseau de la victime. De nombreuses collec- tivités territoriales ont été victimes d'une intrusion sur leur système d'information via **l'exploitation de vulnérabilités** [a][1].

**25 incidents touchant des collectivités territoriales liés à des compromissions et chiffrements par rançongiciel** ont été rapportés à l'ANSSI au cours de l'année 2024, soit 11% des incidents en lien avec ce secteur. La majorité des victimes de rançongiciel sont des **communes** et **EPCI à fiscalité propre**. Sur la période étudiée, 21 de ces 25 incidents ont engendré des effets importants sur le fonctionnement des collectivités territoriales ci- blées. Les souches de rançongiciel les plus signalées à l'ANSSI sont **LOCKBIT** (5), suivie de **RAMSOMHUB** (3), **BABUK** (2) et **8BASE** (2). Des **exfiltrations de données** à caractère technique, personnelle ou administrative ont été identifiées au cours de **12 incidents**.

*a*. Majoritairement des vulnérabilités affectant des équipements de bordure (CVE-2023-46805, CVE- 2024-21887, CVE-2024-21893, CVE-2024-3400 et CVE-2024-47575).

**De plus, en raison d'interconnexions ou de regroupement de systèmes d'information entre collectivités, les compromissions observées peuvent également avoir des effets de bord sur d'autres collectivités territoriales.**

Le CERT-Bund, dans son rapport annuel pour 2024, mentionne ainsi la compromission par rançongiciel d'un fournisseur de services informatiques dédié aux collectivités territoriales allemandes en octobre 2023. Cette compromission a touché en même temps un nombre impor- tant de collectivités, le prestataire gérant les services informatiques de 72 collectivités et 20 000 postes de travail. Les conséquences de cette attaque, revendiquée par le groupe cybercriminel Akira, ont pesé sur 1,7 millions d'habitants concernés par les interruptions de service des col- lectivités clientes de ce fournisseur.

La gestion de l'incident a, selon le CERT-Bund, impliqué de nombreux acteurs et **la restauration complète des services des collectivités n'était pas complète plusieurs mois après l'attaque** [2].

En avril 2024, l'ANSSI est alertée de la **compromission** et du **chiffrement** d'une commune par le biais du rançongiciel LOCKBIT 3.0. En raison de l'ampleur de la compromission, la commune a été contrainte d'**isoler** son système d'information d'internet et de **couper l'ensemble des interconnexions** avec d'autres communes. Le système d'information du bénéficiaire **hébergeant** ceux d'autres organisations, la coupure des accès a rendu les services de ces dernières **indisponibles**. La réouverture des flux a été permise **progressivement** dans les semaines suivant l'incident.

**L'arrêt des services des collectivités en cas d'attaque, notamment par rançongiciel, revêt une gravité particulière et renforce la pression sur ces entités.**

À la suite de la compromission du parc informatique d'une entité, de multiples services pu-

blics (aides sociales, état civil, urbanisme, administration des cimetières, gestion de l'eau et des déchets, *etc*.) et services internes à la collectivité (téléphonie, messagerie, finances, ressources humaines, *etc*.) ne sont plus opérationnels. Ces difficultés obligent souvent la collectivité affectée à basculer vers un mode de fonctionnement dégradé, voire manuel, affectant son activité opérationnelle et ses missions de service public auprès des usagers. Ce fonctionnement dégradé est observé également, avec une ampleur moindre, lors d'incidents sans impact majeur. En effet, les mesures d'endiguement mises en place pour remédier aux incidents affectent également la qualité de service des collectivités.

Lors d'incidents présentant une criticité importante, **plusieurs mois sont souvent nécessaires avant le retour à un fonctionnement en mode nominal**. Cette situation est causée par le délai important nécessaire à la reconstruction et au durcissement du système d'information ainsi qu'à la remontée progressive des différentes applications métiers de la collectivité.

Ainsi, certaines attaques peuvent non seulement avoir des conséquences sur la continuité des services publics, mais également entraîner des pertes financières importantes pour une collectivité. La compromission du site de vente de billets de transports urbains de l'État de l'Uttar Pradesh en Inde en 2023, a entraîné une interruption de vente de plus de dix jours et une perte significative de revenus pour la collectivité [3].

Au cours de l'année 2024, 33 incidents affectant des collectivités territoriales ont eu une **criticité élevée**, soit 15% du nombre total d'incidents sur le périmètre étudié. Ces incidents sont majoritairement constitués d'attaques par rançongiciel et/ou d'actions illégitimes menant à des exfiltrations de données.

En avril 2024, l'ANSSI est informée de la **compromission** et du **chiffrement** de plusieurs serveurs du système d'information d'une commune de taille importante par le biais du **rançongiciel BABUK**. Contrainte de déconnecter son système d'information d'Internet, la commune a subi la **mise à l'arrêt de l'ensemble de ses services publics et internes**. Ceux-ci ont pu être redémarrés petit à petit dans les semaines suivant l'incident.

En novembre 2024, un **conseil départemental** signale à l'ANSSI la compromission de son environnement ***Active Directory*** et une **exfiltration de données**. L'ensemble du système d'information a été isolé d'internet, provoquant de **forts impacts métiers**, notamment du fait de la perte d'accès à la messagerie.

Dans de nombreux cas, la présence d'un **plan de reprise d'activité** (PRA) recensant et priorisant les différentes applications ainsi que la disponibilité de **sauvegardes saines et déconnectées du réseau** permettent d'améliorer significativement le temps nécessaire aux actions de remédiation.

## 3.2 Exfiltration et vente de données et d'accès

Les **données administratives, financières et personnelles des administrés** détenues au sein des collectivités sont nombreuses et présentent un intérêt pour les attaquants, qui peuvent accentuer le **chantage à la publication** de ces données lors de leurs attaques.

Ainsi, en 2024 de nombreuses collectivités territoriales ont fait l'objet de vente d'accès à leurs systèmes d'information ou à leurs données par des acteurs cybercriminels sur des forums du *darknet*. Ces ventes peuvent découler d'attaques par rançongiciel précédées d'une exfiltration

massive de données (comme cela aurait été le cas pour la municipalité de Dubaï en juin 2024, victime du groupe cybercriminel Daixin) [4], ou bien de l'utilisation d'*infostealers*[2]. L'origine des données mises en vente reste parfois inconnue.

Ces cas mettent en évidence des **atteintes importantes à la vie privée** (accès à des registres d'état civil et de gestion de biens et propriétés, accès aux modules de facturation des collectivités etc.) des administrés et des agents des collectivités concernées.

Les cas d'exfiltration et de publication de données constituent enfin un véritable enjeu pour les collectivités territoriales sur les plans **juridiques** et **réputationnels**.

> En janvier 2024, l'ANSSI est informée qu'une commune est affectée par une **fuite de données**. L'ensemble de l'**annuaire** de la commune a été exfiltré et partagé sur plusieurs forums cybercriminels, exposant des **données personnelles des employés de la ville**.

## 3.3 Autres types d'attaques à but lucratif

Les collectivités sont également la cible d'autres types d'attaques à but lucratif menées par des cybercriminels : arnaques dites « au président », hameçonnage à des fins de collecte de données personnelles (ensuite revendues sur des forums cybercriminels), spam *etc*. Ainsi, en 2023, une grande collectivité territoriale française a fait l'objet d'une compromission de ses comptes de messageries : les attaquants ont pu récupérer les identifiants d'un agent de cette collectivité, puis de là ont pu mener des campagnes d'hameçonnage envers les autres agents et les parte- naires de cette collectivité. Suite à la compromission des comptes de messagerie, des données potentiellement sensibles ont probablement été exfiltrées.

Les compromissions de messagerie ainsi que les attaques par point d'eau (ajout de liens illégitimes sur un site web en vue de compromettre de nouvelles cibles), constituent un vecteur de compromission plus large qu'il peut être possible d'éviter par la mise en œuvre de mesures de **sécurisation** et de **durcissement** ainsi que par des mesures de **sensibilisation** auprès des utilisateurs.

# 4 ATTAQUES À BUT DE DÉSTABILISATION

Les attaques à but de déstabilisation revêtent deux grandes réalités : d'une part des attaques menées par des groupes plus ou moins informels d'activistes aux motivations politiques, d'autre part des attaques menées par des groupes affiliés à des États ayant des objectifs de sabotage. Si les collectivités françaises sont aujourd'hui davantage ciblées par des groupes dits « hackti- vistes », d'autres collectivités dans le monde ont pu être ciblées par des attaques destructrices, notamment conduites par des attaquants réputés étatiques.

2. Les *infostealers* sont des programmes malveillants ayant pour fonction d'exfiltrer des identifiants de connexion, des informations bancaires ou d'autres types de données personnelles. Les *infostealers* sont souvent opérés par des acteurs malveillants spécialisés, qui revendent ensuite ces données à d'autres acteurs cybercriminels. Les attaques menées au moyen d'*infostealers* ont fortement progressé depuis quelques années.

## 4.1 Hacktivisme

Les attaques à but de déstabilisation sont fortement dépendantes du contexte national et international, notamment géopolitique. Ainsi depuis 2022, les collectivités territoriales françaises ont été régulièrement ciblées dans les contextes successifs de l'invasion de l'Ukraine par la Rus- sie et du soutien apporté à l'Ukraine par la France, du conflit au Proche-Orient depuis le 7 oc- tobre 2023, mais également de l'organisation des Jeux Olympiques et Paralympiques en France à l'été 2024.

Le soutien apporté par la France à l'Ukraine depuis le début de l'invasion de l'Ukraine par la Russie en février 2022 a entraîné des vagues régulières d'**attaques par déni de service distribué** (DDoS) contre des entités de toute nature, notamment des sites Internet de collectivités territoriales françaises. Ces attaques sont menées par des groupes hacktivistes pro-russes en représailles au positionnement de la France. Les collectivités semblent ciblées essentiellement parce qu'elles représentent l'administration française.

La vague d'attaques du 31 décembre 2024, revendiquée par le groupe hacktiviste pro-russe NoName057(16) et ayant touché (sans conséquences majeures) de nombreuses collectivités françaises (villes, départements et régions) ainsi que de nombreuses administrations, est un exemple de ces actions. Des attaques similaires ont eu lieu dans de nombreux pays européens.

Le contexte du conflit au Proche-Orient a également été exploité par des groupes hacktivistes pro-palestiniens pour mener des attaques contre des collectivités. Si la majorité des collecti- vités sont victimes de DDoS, certaines (notamment en Israël) ont également subi des attaques entraînant des exfiltrations et publications de données ou des défigurations de leurs sites Web.

La période des Jeux Olympiques et Paralympiques de Paris 2024 a été particulièrement propice à ce type d'attaques par DDoS contre des entités de toute nature, parmi lesquelles de nombreuses collectivités territoriales.

Depuis une dizaine d'années les collectivités ont subi des vagues d'attaques par des groupes d'hacktivistes cherchant une visibilité au moyen de **défiguration de sites Internet**. Exploitant des failles de sécurité dans les sites Internet de nombreuses communes, ces attaquants modifient le contenu des pages affichées et y inscrivent des revendications politiques ou religieuses, souvent liées au contexte géopolitique. Ces défigurations touchent des collectivités territoriales dans le monde entier. Ainsi, plusieurs dizaines de sites Internet de mairies françaises ont fait l'objet de défigurations portant des messages pro-russes en mai 2023 [5].

**Si ces attaques ne sont pas d'une grande sophistication, elles portent atteinte à l'image de ces collectivités et peuvent susciter la crainte chez leurs administrés.**

## 4.2 Sabotage par des acteurs réputés étatiques

Dans le cadre de tensions géopolitiques ou de conflits, certaines collectivités territoriales sont également ciblées par des attaques ayant pour but de **saboter des infrastructures**. Les infrastructures liées à l'approvisionnement en eau et en énergie, souvent opérées ou sous la responsabilité des collectivités, sont des cibles récurrentes de ce type d'attaque.

Ainsi, un groupe d'attaquants réputé lié à l'Iran et soutenant les revendications palestiniennes (Cyber Av3ngers) aurait compromis en novembre 2023 une infrastructure municipale de gestion de l'eau en Pennsylvanie (États-Unis). Les attaquants auraient pris le contrôle de la station mais sans réussir à y créer de dommages, au travers de la compromission d'un logiciel métier édité par une société israélienne, probablement la cible initiale des attaquants, ceux-ci ayant des liens

présumés avec l'Iran[6]. Toujours aux États-Unis, la CISA et le FBI ont publié en août 2024 un avis de sécurité mentionnant, entre autres secteurs, le ciblage de collectivités territoriales états- uniennes par le MOA Pioneer Kitten, utiliser pour mener des attaques par rançongiciel. Le FBI considère que ce MOA est aligné avec les intérêts stratégiques iraniens [7].

Dans le cadre de l'invasion russe de l'Ukraine, des entités du secteur de l'énergie gérées par des municipalités en Ukraine ont été ciblées par le biais de MOA liés aux intérêts russes. Ces at- taques visent des protocoles couramment utilisés dans des infrastructures critiques et s'ajoutent aux destructions physiques dues au conflit.

Selon les données portées à la connaissance de l'ANSSI, les collectivités territoriales françaises n'ont pas fait l'objet d'attaques par sabotage dans une période récente. Cependant, dans **le contexte d'une hausse de la menace à but de déstabilisation liée au conflit en Ukraine et de l'organisation des Jeux Olympiques et Paralympiques de Paris 2024**, plusieurs infrastruc- tures d'envergure locale, notamment liées à la gestion de l'eau ont pu faire l'objet de campagnes de reconnaissance par des acteurs offensifs durant l'année 2024 [8].

# 5 ATTAQUES À BUT D'ESPIONNAGE

Les collectivités territoriales ne sont pas réputées être les premières cibles des attaques à fina- lité d'espionnage menées par des attaquants liés à des États. Cependant, comme toutes entités renfermant des données, elles peuvent faire l'objet de telles compromissions. **Les collectivités peuvent gérer des données sensibles dont l'exfiltration peut être jugée intéressante pour des groupes opérant pour le compte d'États**.

Le ciblage de collectivités territoriales par des acteurs liés à des États a pu être révélé par l'ana- lyse de campagnes de hameçonnage ciblé : en mars 2024, une campagne associée au MOA Mud- dywater, réputé lié aux intérêts stratégiques iraniens, aurait utilisé des envois de **mails d'hame- çonnage** invitant à télécharger une application malveillante prétendant répondre à des besoins spécifiques de collectivités israéliennes [9]. De même, des mails d'hameçonnage reprenant des thématiques liées aux collectivités territoriales ont été retrouvés lors d'une campagne associée au MOA réputé lié aux intérêts russes APT 28, ciblant l'Argentine en mars 2024 [10].

Les collectivités peuvent également, à leur insu, participer à la **construction d'infrastructure d'attaques** pour des modes opératoires d'attaque : ces groupes, procédant avec un haut niveau de sophistication, cherchent en effet à compromettre des équipements informatiques légitimes afin de les enrôler dans des réseaux servant à anonymiser leur navigation, pour ensuite mener des compromissions à but d'espionnage sur leurs cibles finales. Les collectivités territoriales, par la taille de leurs réseaux informatiques et la multitude d'équipements, parfois mal sécurisés, qu'elles doivent gérer, sont fréquemment victimes de ces compromissions.

**La sécurisation de ces équipements périphériques (routeurs notamment) est importante pour lutter contre la prolifération de ces réseaux d'anonymisation utilisés par de nombreux groupes d'attaquants pratiquant des compromissions à but d'espionnage**.

Document 11 : Sénat - Commission résilience - Essentiel sur NIS2
Extrait : introduction et chapiter 1A et 1B

Commission spéciale
RÉSILIENCE
CYBERSÉCURITÉ

SÉNAT

…le projet de loi relatif à résilience des infrastructures critiques et au renforcement de la cybersécurité

# LA FRANCE TRANSPOSE 3 DIRECTIVES EUROPÉENNES POUR RENFORCER LA RÉSILIENCE ET LA CYBERSÉCURITÉ

a) Rapport n° 393 (2024-2025) de MM. Michel CANÉVET, Patrick CHAIZE et Hugues SAURY au nom de la commission spéciale présidée par M. Olivier CADIC.

**Les attaques par rançongiciel ont augmenté de 30 % entre 2022 et 2023**. **La cybermenace n'épargne plus aucun secteur de la vie économique et sociale** : 34 % de ces attaques visaient des TPE/PME, 24 % des collectivités territoriales, 10 % des entreprises stratégique, 10 % des établissements de santé et 9 % des établissements d'enseignement supérieur.

Ce phénomène a conduit l'Union européenne à adopter, en 2022, **trois directives**, pour lesquelles **le projet de loi relatif à résilience des infrastructures critiques et au renforcement de la cybersécurité prévoit la transposition** :

- la directive sur la **résilience des entités critiques** (REC) acte le **passage d'une logique de protection à une approche axée sur la résilience vis-à-vis des risques de toute nature** dont la transposition actualise le dispositif français de sécurité des activités d'importance vitale (SAIV) ;

- la directive *Network and Information Security* (NIS 2), visant à **assurer un niveau élevé de cybersécurité dans l'ensemble de l'Union**, va porter les 6 secteurs essentiels actuels à 18 secteur critiques et élargir le périmètre de régulation à 15 000 entités essentielles et importantes et près de 1 500 collectivités territoriales ;

- la directive *Digital Operational Resilence Act* (DORA) relative à la **résilience opérationnelle numérique du secteur financier, bancaire et assurantiel**.

***

*La commission spéciale a adopté, le 4 mars 2024, le projet de loi relatif à résilience des infrastructures critiques et au renforcement de la cybersécurité. Le texte issu des débats de commission est enrichi de 61 amendements dont 53 de ses rapporteurs.*

# 1. TROIS DIRECTIVES EUROPÉENNES POUR RENFORCER LA RÉSILIENCE DES ENTITÉS CRITIQUES ET LA

## A. REC : LE PASSAGE D'UNE LOGIQUE DE PROTECTION À UNE APPROCHE DE RÉSILIENCE

**Le titre I du projet de loi vise à transposer la directive (UE) 2022/2557 du parlement européen et du conseil du 14 décembre 2022 sur la résilience des entités critiques, dite « REC », en modifiant le code de la défense**.

La directive REC, qui a été négociée sous présidence française de l'Union européenne, s'inspire en grande partie du dispositif français existant. Sa transposition en droit national consiste donc essentiellement en une actualisation du dispositif de sécurité des activités d'importance vitale (SAIV) en place depuis 2006.

Ce texte a pour ambition de fournir à l'ensemble des opérateurs du marché intérieur des standards de sécurité équivalents tout en offrant des règles de concurrence plus équitables.

Le Gouvernement a ainsi fait le choix de s'appuyer sur ce dispositif, en reprenant par exemple la terminologie existante, plutôt que de créer un dispositif ex nihilo. Cette décision semble opportune, le dispositif de SAIV étant désormais bien connu et maîtrisé par les opérateurs concernés. Par ailleurs, le nombre d'opérateurs d'importance vitale (OIV), qui est d'environ 300, ainsi que le nombre de points d'importance vitale, de l'ordre de 1 500, ne devraient pas évoluer de manière significative.

Toutefois, cette transposition marque un changement important de philosophie : elle acte **le passage d'une logique de protection des infrastructures d'importance vitale à une approche axée sur la résilience**.

**Les obligations inscrites dans le projet de loi sont conformes à la directive**

► Le champ d'application de la directive comprend 11 secteurs, contre 2 seulement antérieurement – énergie et transport – dans la directive de 2008. Concrètement, pour la France, la transposition de la directive REC se traduira par un élargissement du champ d'application du dispositif national actuel à plusieurs sous-secteurs, notamment les réseaux de chaleur et de froid, l'hydrogène et l'assainissement ;

► Le texte prévoit la réalisation d'un « plan de résilience opérateur », qui reprendra en partie le contenu des documents existants.

► Il impose également une obligation de notification des incidents et prévoit que les opérateurs désignés comme entités critiques d'importance européenne particulière, c'est-à-dire exerçant la même activité ou une activité similaire dans au moins six États membres, pourront faire l'objet d'une mission de conseil organisée par la Commission européenne ;

► Un mécanisme de sanction administrative pouvant être prononcée par une commission des sanctions créée à cet effet est prévu en cas de manquement. Ce dernier point posant la question des plafonds de sanction – 2 % du chiffre d'affaires ou 10 millions d'euros – inscrits qui, dans le projet de loi, sont plus élevés que dans d'autres États membres.

## B. NIS 2 : UN CHANGEMENT DE PARADIGME POUR LES ENTITÉS ASSUJETTIES ET POUR L'AUTORITÉ NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

### b) Le titre II du projet de loi transpose la directive (UE) 2022/2555 du Parlement Européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, dite « NIS2 ».

Ce texte conduit à un changement majeur de paradigme : il s'agit non plus seulement, comme avec la directive NIS 1, de sécuriser des infrastructures critiques (environ 500), mais aussi d'assurer la résilience quelque 15 000 entités « essentielles » ou « importantes », en tant

qu'organisations, et de l'ensemble de leurs systèmes d'information dans la lutte contre les cyberattaques (cf. encadré ci-dessous).

**Principaux types de cyberattaques contre lesquelles entend lutter la directive NIS 2**

► Les attaques par rançongiciel, qui consistent à exiger une rançon pour rendre des données ou ne pas les publier ;

► Les attaques par hameçonnage, qui visent les systèmes bancaires en ligne et les données financières des clients ;

► Les attaques sur Internet, exploitant les vulnérabilités des applications ;

► Les attaques de la chaîne d'approvisionnement, qui compromettent la sécurité d'une entité en exploitant les vulnérabilités des produits, services et systèmes de tiers (par exemple, un fournisseur de logiciels) ;

► Les attaques par déni de service distribué (DDoS), qui perturbent les transactions de grande valeur et le traitement des données ;

► Les attaques à caractère social, exploitant les vulnérabilités humaines.

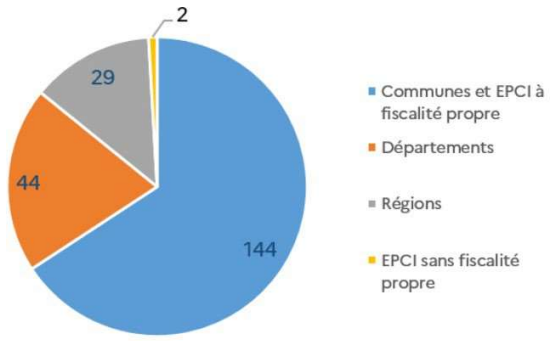
En outre, sur le constat étayé de l'augmentation des menaces cyber sur les collectivités territoriales (cf. grapique ci-dessous), le Gouvernement propose d'inclure dans la transposition près de 1 500 collectivités territoriales, groupements de collectivités et organismes placés sous leur tutelle, dont l'ensemble des régions et des départements, près de 1 000 communautés de communes et de 300 communes de plus de 30 000 habitants.

### c) Pour la commission spéciale, le choix d'inclure un grand nombre de collectivités territoriales et les établissements d'enseignement supérieur est ambitieux mais nécessaire.

**Nombre d'incidents cyber par type de collectivité en 2024**

En 2024, l'ANSSI a traité 218 incidents cyber affectant les collectivités territoriales, soit une moyenne de 18 incidents par mois, dont 44 incidents affectant des départements et 29 incidents affectant des régions. Ces chiffres se révèlent élevés en comparaison du nombre de départements (101) et de régions (18).

*Source : ANSSI – synthèse de la menace sur les collectivités territoriales en 2024*




### d) Les cyberattaques ont un coût très élevé, estimé en 2022 par le cabinet d'études économiques Asterès à 2 milliards d'euros.

Dans le secteur privé, une enquête menée en juin 2024 par l'ANSSI auprès des membres du CLUSIF, une association de professionnels de la cybersécurité, révèle qu'une cyberattaque coûte en moyenne 466 000 euros pour les TPE/PME, 13 millions d'euros pour les ETI et 135 millions d'euros pour les grandes entreprises.

Ce coût représente en moyenne 5 à 10 % du chiffre d'affaires de l'organisation, quels que soient sa taille ou son secteur d'activité, réparti entre les pertes d'exploitation (50 %), le coût des prestations externes d'accompagnement (20 %), le coût de remise en état et d'investissement dans le système d'information (20 %) et le coût réputationnel (10 %).

Dans la sphère publique, les établissements hospitaliers évoqués supra ont supporté des dégâts particulièrement importants : les coûts directs ont ainsi été estimés à 2,36 millions d'euros pour le Centre hospitalier Dax-Côte d'Argent (février 2021) et à plus de 5,5 millions d'euros pour le Centre hospitalier Sud-Francilien déjà cité.

Les collectivités territoriales et les intercommunalités ont également été lourdement affectées, avec des coûts directs estimés à 900 000 euros pour la Métropole Aix-Marseille-Provence (mars 2020) et à plus de 1,5 million d'euros pour la ville de Bondy (novembre 2020).

A ces coûts directs s'ajoutent des coûts indirects, liés aux activités non réalisées ou à la perte de confiances des usagers, mais leur chiffrage est complexe, tout particulièrement dans le cas des missions de service public.

# L'adoption de la directive NIS 2 constitue une réponse à l'augmentation de la cybercriminalité

La directive NIS 2 distingue **deux catégories d'entités régulées : les entités « essentielles » et les entités « importantes »** du point de vue de la sécurité des systèmes d'information. Cette catégorisation s'établit selon leur degré de criticité, leur taille et leur chiffre d'affaires (pour les entreprises).

Deux caractéristiques qui conduisent à qualifier une **entité d'essentielle** :

- son appartenance à un secteur d'activité « hautement critique » ;
- le dépassement de certains seuils d'effectifs ou d'activité, à savoir le fait d'employer 250 personnes ou d'avoir un chiffre d'affaires annuel excédant 50 millions d'euros et un bilan annuel de plus de 43 millions d'euros.

Au total, selon l'ANSSI, quelque 2 000 entreprises privées devraient ainsi être considérées comme des entités « essentielles »

S'agissant des entités importantes, le texte prévoit que sont désignées comme telles les entreprises appartenant à un des secteurs d'activité « hautement critiques » ou « critiques » qui ne sont pas des entités « essentielles » et qui emploient au moins 50 personnes ou dont le chiffre d'affaires et le total du bilan annuel excèdent chacun 10 millions d'euros.

Le tableau ci-dessous présente la classification des critères applicables aux entreprises selon qu'elles seront assujetties à l'une ou l'autre catégorie.

### e) Seuils de classification des entités essentielles et importantes

| Nombre d'employés | Chiffre d'affaires (millions d'euros) | Bilan annuel (millions d'euros) | Secteur d'activité hautement critique | Secteur d'activité critique |
|---|---|---|---|---|
| **Supérieur à 250** | Supérieur à 50 | Supérieur à 43 | Entités essentielles | Entités importantes |
| **Entre 50 et 250** | Compris entre 10 et 50 | Compris entre 10 et 43 | Entités importantes | Entités importantes |
| **Inférieur à 50** | Inférieur à 10 | Inférieur à 10 | Non concernées | Non concernées |

La commission spéciale a néanmoins observé qu'une certaine incompréhension demeurait quant aux différences d'approche de la définition des seuils entre la directive (qui procède par exclusion) et le projet de loi qui définit positivement les critères d'assujettissement. **Un effort de pédagogie et de communication important devra être consacré à ce volet de l'application de la loi car dans en pratiques, les entités devront elles-mêmes identifier la catégorie dont elles relèvent.**

Environ un quart des contrôles de la CNIL s'inscrit dans le cadre de thématiques prioritaires annuelles qu'elle définit. En 2025, elle se concentrera sur les données collectées via les applications mobiles, la cybersécurité des collectivités territoriales ainsi que les traitements de données par l'administration pénitentiaire.

La CNIL conduit des centaines de contrôles par an (321 en 2024) qui font suite à des plaintes, de précédentes mesures correctrices, des signalements de violations de données ou sont en lien avec l'actualité.

En 2025, la CNIL se concentrera sur les données collectées par le biais des applications mobiles, la cybersécurité des collectivités territoriales ainsi que les traitements de données par l'administration pénitentiaire.

## 3) Les thématiques de contrôles prioritaires en 2025

### Collecte de données par le biais des applications mobiles

Les Français téléchargent désormais une trentaine d'applications mobiles par an. Elles sont devenues le premier usage numérique au quotidien et sont ainsi une source de traitement massif de données personnelles (bancaires, de géolocalisation, publicitaires, etc.).

Dans le prolongement de la publication de sa recommandation sur les applications mobiles en octobre dernier et comme elle l'avait annoncé, la CNIL mènera cette année une série de contrôle des différents acteurs de l'écosystème, en particulier des éditeurs d'applications et des fournisseurs de kits de développement logiciel (SDK).

Les vérifications porteront essentiellement sur les questions abordées dans la recommandation, notamment le paramétrage des SDK ainsi que les accès aux données du téléphone via la gestion des permissions (ou « autorisations).

Ces contrôles concerneront aussi bien les acteurs privés que publics, notamment au regard de la multiplication des services publics proposant une application mobile pour des tâches administratives du quotidien.

### Cybersécurité des collectivités territoriales

La cybersécurité fait partie des axes majeurs du plan stratégique 2025-2028 de la CNIL. Ces dernières années ont en effet été marquées par de nombreuses cyberattaques impliquant une grande partie de la population. La CNIL a ainsi reçu 5 629 notifications de violation en 2024, soit 20 % de plus qu'en 2023. Face aux risques de vol de données personnelles, notamment bancaires ou de santé, la cybersécurité est un réel enjeu de société.

Parmi les acteurs concernés, les collectivités territoriales sont particulièrement vulnérables. Or, ces dernières traitent un grand nombre de données, pour certaines sensibles (gestion de l'état civil des usagers, versement de prestations sociales, données financières, ou encore services en ligne de paiement de contravention).

La CNIL a donc décidé de contrôler les mesures mises en œuvre par les collectivités territoriales afin de protéger les données des usagers. En parallèle de ces contrôles, la CNIL va continuer à renforcer son action en vue de sensibiliser et d'accompagner les collectivités territoriales en matière de cybersécurité.

Par cette double action, la CNIL souhaite aussi préparer l'entrée en application de la directive NIS2, en cours de transposition, qui prévoit une montée en compétences et des exigences nouvelles pour les collectivités territoriales en matière de sécurité informatique

### Données traitées par l'administration pénitentiaire

D'après le ministère de la Justice, 77 800 personnes sont aujourd'hui en détention en France. L'ensemble des informations relatives aux personnes faisant l'objet d'une mesure restrictive ou privative de liberté sont répertoriées au sein du traitement informatisé de « Gestion nationale des personnes écrouées pour le suivi individualisé et la sécurité » (« GENESIS »). Il contient notamment des informations particulièrement sensibles liées à la gestion de la vie en détention et la réinsertion de ces personnes.

Par ailleurs, les établissements pénitentiaires doivent veiller de manière accrue à la sécurisation de leurs installations informatiques et des moyens de communication qui y sont déployés.

Lors de ses investigations, la CNIL vérifiera ainsi les conditions de traitement des données des personnes incarcérées ainsi que l'ensemble des mesures de sécurité mises en place par les établissements.

### Droit à l'effacement

Dans le cadre de la quatrième action du cadre d'application coordonné, La CNIL et ses homologues européens vont procéder à des vérifications sur les conditions de mise en œuvre du droit à l'effacement. Cette action vise à harmoniser l'application effective du RGPD et la coordination entre les autorités de contrôle.

Document 13 : Bilan pour les CSIRT territoriaux
Actu ZDNet - Forum InCyber - 02/04/25 Par Gabriel Thierry

Les quinze centres de réponse à incidents cyber territoriaux sont désormais tous en activité. Voici ce qu'ils remontent du terrain.

Quatre ans après le lancement de ce projet en 2021 dans le cadre du plan de relance, avec un financement par l'Etat des trois premières années d'activité, les quinze centres cyber d'assistance installés dans les régions françaises - seule la région Auvergne-Rhône-Alpes n'a pas incubé de structure - sont tous opérationnels.

Pour certains, comme la Normandie, depuis plus de deux ans, quand pour d'autres, comme La Réunion, depuis seulement quelques mois.

Selon les chiffres présentés hier en marge du forum InCyber à Lille, les CSIRT territoriaux ont traité en 2024 1387 événements de sécurité, soit :

- 658 incidents - une action d'un acteur malveillant
- 729 signalements - un comportement anormal ou inattendu pouvant avoir des conséquences néfastes

Enfin, les quinze structures ont accompagné 136 organisations victime d'un rançongiciel, ces programmes malveillants qui chiffrent ou exfiltrent des données.

## • 700 actions de prévention

Dans le détail :

- Les signalements les plus observés étaient d'abord relatifs au hameçonnage et à des techniques d'ingénierie sociale.
- Venaient ensuite les vulnérabilités non corrigées.
- Et enfin les déni de service.

De même, ce top 3, pour les incidents de sécurité, renvoyait à des attaques par rançongiciel, la compromission d'un compte aux accès non privilégiés et enfin au typosquattage ou usurpation d'identité.

Sur le terrain de la prévention, les CSIRT ont conduit près de 700 actions. Il s'agit de conférences, de webinaires, ou d'un accompagnement pour réaliser un diagnostic "Mon Aide Cyber" - 189 en tout. Les centres de réponse à incident ont également lancé une campagne de détection de vulnérabilités au profit des collectivités locales françaises. Le centre cyber des Hauts de France a de son côté mis en place un exercice de gestion de crise en amont des Jeux olympiques de Paris. Son homologue du Grand Est a déployé un service gratuit de scan de vulnérabilité.

## • Rôle à jouer avec NIS 2

Autant d'actions qui font désormais de ces structures "un maillon essentiel du dispositif national de réponse aux incidents de sécurité", plaident-elles. Ce sont, insistent-elles, des acteurs de proximité qui assurent "le dernier kilomètre" du dispositif national de réponse aux incidents de sécurité.

Le groupement d'intérêt public Cybermalveillance vient d'annoncer à ce sujet que les CSIRT territoriaux seront associés au "17Cyber", un guichet d'assistance unique. Les victimes professionnelles pourront avoir, si besoin, une mise en relation pour une remédiation technique activée par le centre cyber local.

Ces structures, dont le modèle économique est encore à stabiliser, auront enfin "un rôle à jouer dans l'accompagnement des futures entités régulées" par la transposition de la directive européenne NIS 2. Et ce notamment "dans le rappel dans leurs obligations de notification en cas d'incident" mais aussi "dans l'accompagnement dans la montée en maturité de ces acteurs".