CONCOURS INTERNE DE COLONEL DE SAPEURS-POMPIERS PROFESSIONNELS

SESSION 2025

Note d'analyse et de propositions à partir d'un dossier portant sur l'Union Européenne
et permettant de mettre en évidence une problématique
et éventuellement proposer des solutions possibles

EPREUVE n°5

Durée : 4 h
Coefficient 2.

SUJET : Votre directeur départemental reconnait être peu averti des enjeux de cybersécurité et vous demande une note stratégique portant sur les enjeux de la cybersécurité au niveau européen.

DOCUMENTS JOINTS

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.

Déclaration commune du commissaire au marché intérieur, Thierry Breton, et du secrétaire à la sécurité intérieure des États-Unis, Alejandro Mayorkas

Washington, DC, le 30 janvier 2024

À l'occasion du premier anniversaire de leur déclaration commune de 2023, Thierry **Breton**, commissaire européen au marché intérieur, et Alejandro N. Mayorkas, secrétaire à la sécurité intérieure des États-Unis, ont publié, dans les termes suivants, une déclaration commune actualisée sur la coopération entre les États-Unis et l'Union européenne dans le domaine de la cyberrésilience:

«Nous nous félicitons vivement de la coopération étroite entre l'Union européenne et les États-Unis pour protéger nos citoyens, nos infrastructures critiques et nos entreprises contre les activités préjudiciables dans le cyberespace. Dans un paysage géopolitique et technologique marqué par la prolifération de nouvelles menaces et d'acteurs malveillants, il est primordial que nous continuions à coopérer et à unir nos forces pour promouvoir les valeurs et les objectifs communs qui sont les nôtres dans le cyberespace.

Nous célébrons le partenariat large et efficace qui existe entre la direction générale des réseaux de communication, du contenu et des technologies (DG CONNECT) de la Commission européenne et le ministère de la sécurité intérieure (DHS) des États-Unis, tel qu'il ressort des axes de travail communs mis en place à la suite de notre précédente déclaration commune. Au cours de l'année écoulée, ces axes de travail ont fait l'objet d'une coopération solide, ciblée et stratégique. Parmi les résultats notables obtenus, on peut citer: l'engagement de comparer nos exigences en matière de notification des incidents de cybersécurité et, dans la mesure du possible, d'harmoniser leur mise en œuvre; l'intensification de la coopération de nos agences de cybersécurité respectives à la suite de la signature des arrangements de travail entre l'Agence de l'Union européenne pour la cybersécurité (ENISA) et la Cybersecurity and Infrastructure Security Agency (CISA, agence de cybersécurité et de sécurité des infrastructures); la création d'un groupe de travail transatlantique composé d'experts en matière de sécurité des codes sources ouverts; le lancement de la bourse UE-États-Unis dans le domaine de la cybersécurité; d'autres échanges entre experts sur des sujets liés à la politique en matière de cybersécurité, tels que les partenariats public-privé et la gestion des vulnérabilités.

Compte tenu des fruits qu'elle a portés, nous avons décidé cette semaine de poursuivre notre coopération afin de promouvoir des objectifs communs concernant un cyberespace sûr, alors que nous sommes confrontés à un paysage des menaces en constante évolution. En particulier, nous nous sommes engagés à:

- *Travailler ensemble pour harmoniser, dans toute la mesure du possible, les exigences et les lignes directrices que nous publions pour faire progresser la cybersécurité et réduire la charge réglementaire qui pèse sur les entreprises.*
  - *Il s'agit notamment de publier un produit commun comparant nos cadres de notification des incidents de cybersécurité pour les infrastructures critiques, y compris les champs d'information et le calendrier des notifications, afin de recenser les domaines dans lesquels ils sont alignés et ceux dans lesquels il existe des divergences.*
- *Assumer notre responsabilité commune concernant l'adoption sûre et sécurisée de l'intelligence artificielle, compte tenu du potentiel considérable de cette technologie en pleine évolution.*
  - *Il s'agit notamment de créer un axe de travail en matière de cybersécurité consacré à l'intégration sécurisée de l'intelligence artificielle dans les infrastructures critiques, à l'appréciation de la situation concernant la cybersécurité des modèles et des applications d'IA et à la collaboration concernant nos approches de la cybersécurité de l'IA dans l'ensemble de nos missions communes.*
- *Collaborer au niveau bilatéral et avec des services partenaires afin de mieux préparer les réponses que nous apportons collectivement aux incidents de cybersécurité, y compris lorsqu'un soutien rapide et efficace à des pays partageant les mêmes valeurs est justifié.*

- *Il s'agit notamment de faciliter l'examen commun de scénarios afin d'analyser les mécanismes de réaction aux crises liées au cyberespace.*

- *Faire progresser conjointement la cybersécurité des logiciels et du matériel dans des domaines critiques en matière de cybersécurité afin de préparer au mieux l'administration publique, les entreprises et les infrastructures critiques à l'évolution des menaces à l'avenir.*
  - *Il s'agit notamment de mettre en place ou de formaliser des échanges réguliers sur la sécurité des codes sources ouverts, la nomenclature des logiciels (SBOM) et la sécurisation des cadres logiciels dès leur conception, y compris en vue de leur alignement sur les efforts déployés dans le cadre du règlement de l'UE sur la cyberrésilience et d'une coopération internationale plus large.*
  - *Il s'agit également d'approfondir les échanges sur les aspects liés à la cybersécurité des technologies émergentes et de rupture, y compris sur des sujets tels que la cryptographie post-quantique.*
- *Continuer à intensifier les échanges de personnel et de talents afin de renforcer les efforts actuellement déployés et de mieux soutenir les axes de travail actuels et futurs.*
  - *Il s'agit notamment de poursuivre le programme 2024 de bourses UE-États-Unis dans le domaine de la cybersécurité, qui mettra en contact des fonctionnaires européens et américains chargés de la cybersécurité pour débattre au niveau opérationnel de questions transatlantiques liées à la politique en matière de cybersécurité. Forts du succès de cette bourse, nous sommes convenus de la nécessité d'un futur programme d'échanges dans le cadre duquel un expert sera détaché par chaque partie pour se joindre aux équipes de l'autre.*

*Ces engagements et les résultats qui y sont associés reflètent l'ambition exprimée dans la déclaration commune de la présidente **von der Leyen** et du président Biden en mars 2022, qui appelait à une coopération plus approfondie et à des échanges d'informations plus structurés en matière de cybersécurité sur les menaces, ainsi que dans la déclaration commune publiée à l'issue du sommet UE-États-Unis d'octobre 2023, qui invitait à une coopération permettant de créer un cyberespace plus sûr et de protéger les consommateurs et les entreprises. Les résultats attendus devraient être communiqués lors du 10^{e} dialogue UE-États-Unis sur le cyberespace, qui se tiendra dans le courant de l'année à Washington D.C.»*

STATEMENT/24/576

La Commission se félicite de l'accord politique obtenu sur le règlement relatif à la cyberrésilience

Brussels, le 1er décembre 2023

La Commission se félicite de l'accord politique auquel le Parlement européen et le Conseil sont parvenus la nuit dernière concernant le règlement sur la cyberrésilience, proposé par la Commission en septembre 2022.

Le règlement sur la cyberrésilience est le premier acte législatif de ce type au monde. Il permettra d'améliorer le niveau de cybersécurité des produits numériques dans l'intérêt des consommateurs et des entreprises dans l'ensemble de l'UE, en imposant des exigences obligatoires proportionnées en matière de cybersécurité pour tous les produits matériels et logiciels, qu'il s'agisse de moniteurs pour bébés, de montres intelligentes et de jeux informatiques ou de pare-feu et de routeurs. Les exigences en matière de sécurité varieront en fonction du niveau de risque que présenteront les produits. Moins de 10 % des produits feront l'objet d'une évaluation par un tiers.

Grâce à ce nouveau règlement, tous les produits devront satisfaire à des exigences en matière de cybersécurité avant d'être mis sur le marché de l'UE. Il s'agit là d'une étape cruciale dans la lutte contre la menace croissante que représentent les cybercriminels et autres acteurs malveillants.

Une fois le règlement sur la cyberrésilience en place, les fabricants de matériel et de logiciels devront mettre en œuvre des mesures de cybersécurité dès la conception et le développement du produit et tout au long de son cycle de vie, c'est-à-dire après sa mise sur le marché. Les produits logiciels et matériels devront porter le marquage CE indiquant qu'ils sont conformes aux exigences du règlement et qu'ils peuvent donc être vendus dans l'UE.

Le règlement introduira également une obligation légale pour les fabricants de fournir aux consommateurs des mises à jour de sécurité en temps utile pendant plusieurs années après l'achat. Cette période devra rendre compte de la durée d'utilisation prévue des produits.

Grâce à ces mesures, le nouveau règlement permettra aux utilisateurs de faire des choix plus éclairés et plus sûrs, étant donné que les fabricants seront tenus d'assurer une plus grande transparence et d'assumer une plus grande responsabilité quant à la sécurité de leurs produits.

Prochaines étapes

L'accord obtenu doit être à présent approuvé de manière formelle par le Parlement européen et le Conseil. Une fois adopté, le règlement sur la cyberrésilience entrera en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel*.

À compter de son entrée en vigueur, les fabricants, importateurs et distributeurs de produits matériels et logiciels disposeront de 36 mois pour s'adapter aux nouvelles exigences, à l'exception de l'obligation de signalement des incidents et des vulnérabilités imposée aux fabricants pour laquelle un délai de grâce plus limité, de 21 mois, est prévu.

Contexte

La cybersécurité est l'une des principales priorités de la Commission européenne. Nous devons prendre des mesures fortes pour sécuriser nos produits numériques, tant logiciels que matériels.

Le règlement sur la cyberrésilience s'appuie sur la stratégie de cybersécurité de l'UE de 2020 et sur la stratégie de l'UE pour l'union de la sécurité de 2020, et a été annoncé dans le discours sur l'état de l'Union européenne de 2021 dans le cadre du plan visant à bâtir une Europe adaptée à l'ère du numérique. Il complétera la législation existante, en particulier le cadre SRI2, adopté en 2022.

Au cours de l'année écoulée, le nombre d'attaques visant la chaîne d'approvisionnement des logiciels a triplé et, chaque jour, des petites entreprises et des établissements critiques tels que les hôpitaux sont la cible des cybercriminels. Toutes les onze secondes, une organisation est victime d'une attaque par rançongiciel, ce qui représente un coût estimé à 20 milliards d'euros par an. Pendant la seule année 2021, les cybercriminels ont été capables de pirater des appareils pour lancer près de

10 millions d'attaques par déni de service distribué au niveau mondial, rendant des sites web et des services en ligne inaccessibles pour leurs utilisateurs.

IP/23/6168

Quotes:

Les consommateurs doivent se sentir en sécurité avec les produits disponibles sur le marché de l'UE. Le règlement sur la cyberrésilience, sur lequel un accord a été obtenu aujourd'hui, garantira que les produits numériques que nous utilisons à la maison et sur notre lieu de travail respectent des normes strictes en matière de cybersécurité. Ceux qui mettent ces produits sur le marché doivent être tenus pour responsables de leur sûreté.
Věra Jourová, vice-présidente chargée des valeurs et de la transparence - 01/12/2023

La sûreté de tous les produits circulant dans l'UE a toujours été une priorité et une réussite. Le règlement sur la cyberrésilience nous permet de combler une lacune en complétant les règles en matière de sécurité, de sorte que la sécurité dès la conception s'applique à tous les produits qui parviennent aux consommateurs et aux utilisateurs de l'UE. Ces nouvelles règles imposent que tous les produits interconnectés vendus dans l'UE satisfassent à des exigences en matière de cybersécurité, et permettront ainsi de rendre nos entreprises et nos foyers plus sûrs.
Margaritis Schinas, vice-président chargé de la promotion de notre mode de vie européen - 01/12/2023

Je me félicite de l'accord auquel le Parlement européen et le Conseil sont parvenus concernant ce règlement important présenté par mes services. Ce règlement garantit, dans l'UE, la prise en compte de la cybersécurité dès la conception des produits numériques et tout au long de leur cycle de vie. Cette prise en compte de la cybersécurité dès la conception est indispensable pour assurer la sécurité des consommateurs et de la société dans son ensemble.
Thierry Breton, commissaire au marché intérieur - 01/12/2023

DOCUMENT 3

Premier schéma de certification de cybersécurité à l'échelle de l'UE pour rendre l'espace numérique européen plus sûr

La Commission a adopté le tout premier schéma européen de certification de cybersécurité, conformément au règlement de l'UE sur la cybersécurité. Le système propose un ensemble de règles et de procédures à l'échelle de l'Union sur la manière de certifier les produits TIC tout au long de leur cycle de vie et de les rendre ainsi plus fiables pour les utilisateurs.

European Union Agency for Cybersecurity (ENISA)

La certification permet de reconnaître officiellement que les produits TIC peuvent être fiables pour protéger à la fois le matériel et les logiciels que les citoyens utilisent quotidiennement.

Thierry Breton, commissaire au marché intérieur, s'est exprimé en ces termes:

> Dans un paysage très dynamique de menaces en matière de cybersécurité, nous nous efforçons d'accroître notre cyber-résilience collective. Aujourd'hui, nous lançons un nouveau cadre pour garantir la cybersécurité des produits que nous utilisons dans certains des environnements les plus sensibles, tels que les routeurs et les cartes d'identité. Nous voulons que nos citoyens, nos entreprises et le secteur public puissent

faire confiance aux produits dont ils dépendent pour sécuriser leurs réseaux et fournir des services publics sensibles.

Le système volontaire complétera la législation sur la cyberrésilience, qui introduit des exigences contraignantes en matière de cybersécurité pour tous les produits matériels et logiciels dans l'UE. Cette étape majeure contribue à renforcer le leadership numérique de l'Europe à l'échelle mondiale. En outre, le régime stimulera également la mise en œuvre de la directive SRI 2.

Le régime sera publié prochainement au Journal officiel de l'UE et entrera en vigueur 20 jours après sa publication. Parallèlement à la publication du système de certification au Journal officiel, la Commission publiera également le premier programme de travail glissant de l'Union pour la certification européenne de cybersécurité. Le présent document expose une vision stratégique et des réflexions sur les domaines possibles pour les futurs schémas européens de certification de cybersécurité, compte tenu de l'évolution récente de la législation et du marché.

Le système adopté repose sur des projets élaborés par l'Agence de l'Union européenne pour la cybersécurité (ENISA) en étroite coopération avec les experts du secteur et les États membres, à l'issue de discussions techniques et juridiques, ainsi que d'une consultation publique.

MAIRE info

Cybersécurité : la transposition de la directive « NIS 2 » enfin en route

18/10/2024
Cybermalveillance

Le projet de loi de transposition de la directive européenne « NIS 2 » a été présenté en conseil des ministres. 1 489 collectivités territoriales et 992 communautés de communes métropolitaines et d'outre-mer devraient être concernées par ces nouvelles règles de cybersécurité.

Mieux vaut tard que jamais. Le 17 octobre, c'est-à-dire hier, chaque pays de l'Union européenne devait avoir transposé la directive NIS 2 dans sa législation nationale. Retardée par les remous politiques actuels, cette transposition va enfin pouvoir débuter son parcours législatif.

Ainsi, mardi, le ministre de l'Économie, des Finances et de l'Industrie, le ministre de l'Enseignement supérieur et de la Recherche, et la secrétaire d'État chargée de l'Intelligence artificielle et du Numérique, ont présenté un projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Trois transpositions en une

Trois directives européennes adoptées le 14 décembre 2022 vont être transposées via un projet de loi « visant à renforcer les dispositifs nationaux de sécurisation des activités d'importance vitale et de lutte contre les menaces cyber ». Parmi ces directives, l'une concerne les « infrastructures critiques » ; l'autre concerne le secteur économique et enfin l'une concerne les entreprises et les collectivités (NIS 2).

L'exposé des motifs et le projet de loi ont déjà été publiés. Ainsi, le texte rappelle que *« la directive NIS1 avait établi les bases d'une cybersécurité renforcée sur un ensemble de secteurs d'activité sur le territoire de l'Union européenne. Depuis 2016, la menace cyber a fortement évolué, devenant systémique. Alors que les cyber-attaquants se concentraient jusqu'à il y a quelques années sur les acteurs et opérateurs stratégiques, ils ciblent désormais l'ensemble du tissu social et économique.* » On observe d'ailleurs une recrudescence des attaques à l'encontre des collectivités : de la petite commune rurale à la grande métropole.

L'entrée en vigueur de NIS 2 vient donc renforcer le niveau commun de cybersécurité. Concrètement, certaines mesures seront à mettre en place *« pour certaines entités qualifiées comme essentielles ou importantes, en raison des services qu'elles fournissent et de leur taille. »* Ce nouveau règlement *« élargit ainsi considérablement le périmètre des acteurs et secteurs régulés par la directive. En France, cela se traduit par une augmentation estimée du nombre d'entités régulées de 500 à près de 15 000, et une augmentation du nombre de secteurs régulés de 6 à 18. »*

Quid des collectivités ?

La présentation de ce texte intervient quelques jours après la présentation du rapport de la Commission supérieure du numérique et des postes (CSNP) (lire *Maire info* du 4 octobre). Les sénateurs et députés auteurs de ce rapport insistaient sur la nécessité d'adapter les règles pour les collectivités.

Le projet de loi apporte des précisions sur les définitions des entités essentielles et importantes, qui devront selon leur classification répondre à certaines obligations. Le texte confirme que, notamment, les régions, les départements et les communes d'une population supérieure à 30 000 habitants correspondent au spectre des « entités essentielles » (elles

auront davantage d'objectifs à remplir que les entités importantes). Pour les entités importantes, sont notamment concernés *« les communautés de communes et leurs établissements publics administratifs »*. **Enfin il a été confirmé dans ce projet de loi que l'Anssi, ne souhaite pas voir les collectivités être soumises à des sanctions en cas de non-conformité.**

Mais rien n'est fixé. Il est possible que lorsque le projet de loi sera étudié prochainement par les parlementaires, le seuil des 30 000 habitants évolue par exemple.

Besoin d'accompagnement

Du côté des associations d'élus on espère qu'il sera donné aux collectivités concernées les moyens et le temps suffisants pour respecter le futur référentiel de cybersécurité. Le rapport de la CSNP insiste sur *« la nécessité d'un accompagnement spécifique des collectivités locales »*. **La commission recommande d'abord de** *« faire auditer par l'Anssi le degré de maturité des collectivités qui seront soumises à la directive ».* **Elle plaide pour qu'un accompagnement** *« spécifique, technique et financier »* **soit prévu pour les collectivités n'ayant pas les moyens nécessaires :** *« La mobilisation de financements de la stratégie nationale d'accélération cyber vers des outils intégrés conformes aux exigences posées par l'Anssi doit être étudiée ».*

A l'occasion d'une question écrite publiée hier, la sénatrice du Finistère Nadège Havet demande au gouvernement *« de prendre le temps d'envisager un accompagnement spécifique, technique et financier des collectivités territoriales les moins avancées sur la question de lutte contre les cyberattaques et de prévoir un délai de mise en conformité soutenable. »* **Le délai de mise en conformité est pour le moment fixé à trois ans, ce qui paraît court pour certaines collectivités qui partent de loin sur ces problématiques de cybersécurité...**

Reste à savoir quand ce projet de loi va être examiné par le Parlement et comment les principales mesures concernant les collectivités vont évoluer durant la navette parlementaire.

DOCUMENT 5

Cybersécurité : que fait l'Union européenne ? - Touteleurope.eu

Arthur Olivier

Le piratage de comptes en ligne a augmenté de 139 % en France en 2021, selon le groupement d'intérêt public "Action contre la Cybermalveillance", qui rassemble des acteurs privés et publics - Crédits : Anyaberkut / iStock

En septembre 2021, l'Assistance Publique-Hôpitaux de Paris (AP-HP) porte plainte. Le motif ? Le vol des données personnelles d'environ 1,4 million de personnes qui avaient passé un test PCR en Ile-de-France. Cette attaque concernait un service de partage de fichiers, utilisé ponctuellement en 2020

pour transmettre des informations à l'Assurance maladie et aux agences régionales de santé (ARS). Quelques semaines plus tard, un étudiant opposé au pass sanitaire reconnaît être à l'origine du piratage, qui visait selon lui à montrer les failles informatiques des hôpitaux parisiens.

Ce genre d'attaque, qui fait fi des frontières, devrait se multiplier dans les années à venir. C'est pourquoi l'Union européenne cherche à assurer un haut niveau de cybersécurité.

Qu'est-ce que la cybersécurité ?

La cybersécurité consiste à protéger les systèmes informatiques contre les attaques malveillantes ou l'espionnage. Elle englobe toutes les techniques et les outils mis en œuvre pour protéger les infrastructures mais aussi la confidentialité, l'intégrité et la disponibilité des données qui sont stockées ou échangées dans le monde numérique.

Plus largement, selon l'UE, la cybersécurité recouvre "*les activités nécessaires pour protéger les réseaux et les systèmes d'information ainsi que les utilisateurs de ces systèmes et les autres personnes exposées aux cybermenaces*".

Selon une information reprise par le Conseil de l'UE, la valeur du marché européen de la cybersécurité est estimée à plus de 130 milliards d'euros et progresse à un rythme de 17 % par an.

Quelles sont les menaces ?

Les menaces qui peuplent l'espace virtuel sont relativement nouvelles et touchent les citoyens mais aussi les administrations et les entreprises. "*Le cyberespace est devenu un domaine de concurrence stratégique, dans une période de dépendance croissante à l'égard des technologies numériques*", explique

l'UE dans sa "boussole stratégique", un document définissant les grandes orientations européennes en matière de sécurité.

L'Agence de l'Union européenne pour la cybersécurité (ENISA, voir plus bas) identifie 9 menaces principales :

- les **logiciels rançonneurs**, ou "*ransomware*", consistent à attaquer un système informatique et à demander une rançon pour en rétablir le bon fonctionnement,
- les **logiciels malveillants**, afin d'endommager ou d'accéder à un appareil sans autorisation,
- le **minage clandestin**, qui infiltre un ordinateur ou un téléphone afin de produire de la cryptomonnaie à l'insu du propriétaire de l'appareil,
- les attaques par **e-mail**, avec les spams ou l'hameçonnage,
- les menaces sur **les données**, surtout concernant le vol et la divulgation d'informations personnelles,
- les attaques par **déni de service**, qui empêchent les internautes d'accéder à un réseau ou à un système, en bombardant par exemple un serveur web de sollicitations,
- la **désinformation,**
- les **attaques sur la chaîne d'approvisionnement**, c'est-à-dire ciblées sur un fournisseur de logiciels pour infester d'autres entités,
- les incidents qui ne proviennent pas d'intentions malveillantes, liés à l'erreur humaine ou à de mauvaises configurations informatiques.

Si tout internaute peut être la cible de ces menaces, les entreprises sont aussi concernées par des actes de malveillance, et pas seulement les plus grandes d'entre elles.

Selon un Eurobaromètre, 28 % des PME européennes ont connu une cyberattaque en 2021. Un chiffre qui grimpe jusqu'à 41 % en Grèce et 48 % au Portugal. Les petites et moyennes entreprises sont particulièrement touchées par les virus informatiques et les logiciels espions ou malveillants. "*Moins armées que les grandes entreprises face à cette menace, elles constituent des cibles privilégiées pour les acteurs malveillants*", explique la CNIL dans un rapport.

De nombreuses administrations sont également la cible de cyberattaques. La mairie de Saint-Cloud, dans les Hauts-de-Seine, a par exemple subi récemment une paralysie de ses systèmes informatiques, avec une demande de rançon de la part de ces malfaiteurs des temps modernes.

Certaines attaques de grande ampleur peuvent entraîner des conséquences beaucoup plus graves, touchant notamment les infrastructures de base. Mi-avril, l'Ukraine a affirmé avoir déjoué une opération informatique russe visant un fournisseur d'électricité, qui aurait pu plonger dans le noir des "*millions d'Ukrainiens*".

D'où viennent ces menaces ?

De fait, les attaques cyber semblent être l'apanage de certains Etats. Mais les failles de cybersécurité peuvent aussi être exploitées par des individus isolés ou des groupes ne dépendant pas d'un pays en particulier. Des organisations terroristes sont par exemple amenées à utiliser internet pour transférer des fonds, ou à se servir de monnaies virtuelles afin de contourner les circuits bancaires traditionnels.

Dans le cadre de la coopération structurée permanente, une équipe composée d'experts européens aide l'Ukraine à

repousser les cyberattaques provenant de son voisin russe.

Que dit le droit européen en matière de cybersécurité ?

Consciente de ces menaces et de leur nature transnationale, l'Union européenne a mis en place une Agence de l'UE pour la cybersécurité (ENISA). Créée dès 2004 et renforcée en 2019, elle produit des schémas de certification de cybersécurité et coopère avec les Etats membres ainsi qu'avec les organes européens, afin de maintenir et de renforcer la sécurité numérique sur le Vieux Continent. Défini en 2019, ce cadre englobe des exigences techniques, des normes et des procédures.

Un centre européen spécialisé dans la lutte contre la cybercriminalité a par ailleurs été créé au sein d'Europol. Il se concentre sur les crimes perpétrés en ligne, la pédocriminalité et la fraude financière.

Avant le règlement de 2019 redéfinissant l'ENISA, la première initiative européenne en matière de cybersécurité s'était concrétisée par la directive "NIS" (ou SRI, pour "sécurité des réseaux et des systèmes d'information"). Celle-ci a établi des obligations en matière de sécurité pour les opérateurs dans des secteurs stratégiques comme les transports, l'énergie, la santé ou la finance, incluant par exemple une obligation de notifier des incidents à l'autorité nationale compétente lorsqu'ils se produisent.

La Commission européenne a souhaité réviser cette législation, proposant la directive "NIS 2" en décembre 2020. Adoptée en novembre 2022 (les Etats ont doivent la transposer en droit national d'ici l'automne 2024), celle-ci couvre un plus grand

nombre de secteurs, comme les messageries des administrations publiques ou les services de gestion des déchets et des eaux usées. Elle entend aussi rapprocher les exigences de chaque Etat membre en matière de cybersécurité.

La directive vise aussi à renforcer les obligations des entreprises et à introduire des mesures de surveillance plus strictes pour les autorités nationales. Les Etats membres sont par exemple tenus d'inclure les câbles sous-marins, cruciaux pour les liaisons téléphoniques et internet, dans leur stratégie de cybersécurité.

Un réseau européen pour la préparation et la gestion des crises numériques (UE-CyCLONe) a par ailleurs été installé. Son objectif est d'améliorer la coordination lors d'incidents de cybersécurité à grande échelle. La Commission et les Etats membres organisent ainsi chaque année des simulations de cyberattaques à grande échelle afin d'être mieux préparés en cas d'agression réelle. L'édition 2022 s'est tenue les 7 et 8 novembre en Lituanie.

En décembre 2022, le règlement "DORA" (pour "*Digital Operational Resilience Act*", ou "résilience opérationnelle du numérique" en français) a également été adopté. Celui-ci vise à renforcer la sécurité des systèmes numériques du secteur de la finance : banques, compagnies d'assurance, producteurs de cryptomonnaies… Ces acteurs doivent s'assurer de pouvoir résister à des cyberattaques, et mener des tests approfondis pour vérifier s'ils sont bien préparés aux incidents informatiques.

Comment l'Union européenne prévoit-elle d'aller plus loin ?

La cybersécurité concerne également les consommateurs. La

Commission européenne a proposé un “*European Cyber Resilience Act*” (règlement européen sur la cyber-résilience) le 15 septembre 2022. Avec l’objectif de fixer des règles communes en matière de cybersécurité tout au long de la vie des produits vendus, en particulier des objets connectés. L’exécutif a remarqué que de nombreux fabricants ne fournissaient pas de mises à jour permettant de remédier aux vulnérabilités de leurs marchandises, et que les Européens étaient mal informés du niveau de cybersécurité des produits achetés. La nouvelle législation vise notamment à imposer de nouveaux standards minimums de sécurité.

L’UE prévoit également d’installer des “centres opérationnels de sécurité” (SOC), associés à de l’intelligence artificielle et qui pourraient s’apparenter à des “policiers” du monde numérique.

Elle compte par ailleurs mettre en œuvre une “connectivité spatiale sécurisée”. Il s’agit d’une nouvelle constellation de plusieurs centaines de satellites en orbite basse, destinée à améliorer la connectivité et l’accès à internet. Un dispositif visant à assurer la poursuite du service en cas de cyberattaque ou de catastrophe naturelle, pour un coût total estimé à 6 milliards d’euros. Baptisée “IRIS2”, la future constellation doit être opérationnelle d’ici 2027.

Dans le cadre du budget pluriannuel 2021-2027 et de son programme pour une Europe numérique, l’UE compte investir 1,6 milliard d’euros pour la cybersécurité sur cette période. Elle souhaite notamment financer des infrastructures et des outils sur l’ensemble de son territoire.

DOCUMENT 6

Cybersécurité : l'Europe en ordre de marche

Julie Le Bolzer

Face à une menace qui va crescendo, l'Europe réplique. Près de 85 % des dirigeants européens font part d'une augmentation, sur un an, des incidents affectant la cybersécurité de leur organisation. Tel est l'un des enseignements de la dernière édition du panorama des cybermenaces en Europe, réalisé dans treize pays par l'éditeur de solutions de sécurité Cloudflare.

Face à « ce fléau pour les entreprises, comme pour les particuliers », selon Michel Van Den Berghe, le président du Campus Cyber, la réponse de l'Europe s'opère notamment sur le front réglementaire. Aussi bien en durcissant la lutte contre les pratiques anticoncurrentielles (comme en 2023, lorsque la Commission européenne a enjoint des Gafam, désignés comme des « contrôleurs d'accès », à se plier aux exigences du règlement DMA sur les marchés numériques), qu'en demandant aux entreprises de se conformer à de nouvelles règles de protection.

Infrastructures critiques

Et Michel Van Den Berghe de citer le Cybersecurity Act de 2019 et DORA, visant à renforcer la résilience du secteur financier

face au risque cyber, en vigueur à partir de 2025. Ou encore NIS 2, en vigueur à partir du 17 octobre, qui concerne 30.000 entreprises et collectivités en France, « l'un des pays les plus ciblés, notamment via ses infrastructures critiques tels les hôpitaux », dit-il.

« L'Europe se mobilise, tant en termes d'exigences vis-à-vis des entreprises, que de financements », dit-il, en évoquant l'enveloppe de 5 millions d'euros allouée au Campus Cyber pour la création du Cybiah (cybersécurité et intelligence artificielle hub) qui, avec la Région Ile-de-France, propose un accompagnement consacré aux PME et collectivités franciliennes.

210 millions d'euros

Autre illustration des ressources mises sur la table, la Commission européenne a lancé aux prémices de l'été 2024 des appels à propositions en vue d'accroître la protection des installations industrielles et des infrastructures critiques, et de développer des technologies et des centres d'opérations de cybersécurité. Le montant annoncé : 210 millions d'euros, financés dans le cadre du programme « Pour une Europe numérique ».

Malgré ces efforts, la menace s'avère difficile à circonscrire, « notamment du fait de l'explosion des opportunités apparues dans le sillage de l'IA », rappelle Michel Van Den Berghe. Et d'ajouter qu'« à l'heure où les grandes entreprises européennes se révèlent plus résilientes face aux cyber attaques, les malfaiteurs s'en prennent désormais à leurs fournisseurs ».

DOCUMENT 7

L'Europe victime de cyberattaques : ingérence russe ?

Plusieurs entreprises, institutions et organes publiques européens ont été victimes de cyberattaques, menées par le groupe de hackers APT28, lié aux services de renseignement russes.

Ces derniers jours, plusieurs pays européens ont déclaré avoir été la cible de cyberattaques. Berlin, ainsi que la ville de Prague, dénoncent des attaques répétées contre leurs institutions, et accusent le groupe de hackers russes APT28, surnommé les "*fancy bears*", ou "*les ours fantaisistes*".

Des actions géopolitiques, selon l'Union européenne et l'OTAN, qui alertent sur le risque d'une ingérence russe en cette super année électorale. Les deux pays payent probablement leur soutien à l'Ukraine : ce sont du moins les éléments invoqués par les gouvernements concernés pour l'instant.

La Russie, à l'origine des cyberattaques ?

APT 28 n'est pas un nouveau venu dans l'univers de l'hacking. Ses membres, actifs depuis vingt ans, sont vraisemblablement liés aux renseignements militaires russes. Washington a rapidement réagi en attribuant ces attaques à la Russie et en

qualifiant ces "*ours fantaisistes*" d’acteurs "*dangereux au passé lourd de pratiques malveillantes, néfastes, déstabilisantes et perturbatrices*".

La France garde également un mauvais souvenir d’APT 28. Les services leur attribuent notamment les "*Macronleaks" :* diffusion de milliers de documents internes liés à l’entourage du futur président de la République lors de sa première campagne en 2017.

La Russie dément toute responsabilité dans les récentes attaques et dénonce des accusations sans preuve et infondées. Il est en effet difficile d'attribuer une cyberattaque à un pays. Les groupes de hackers sont des officines, soi-disant indépendantes, qui agissent "officiellement" pour leur propre compte. Il est donc rarement possible pour les services de renseignement de dépasser le stade de la supposition.

Une menace difficilement appréhendable

Au-delà de l'annonce de ces cyberattaques fréquentes, nous ne savons jamais véritablement comment sont résolues ces affaires. Sans doute en raison de la nature de l’attaque : une offensive virtuelle de piratage de données, très désincarnée, qui ne mobilise pas véritablement notre empathie.

Notre imaginaire, lui, est par contre bel et bien stimulé. Constitué de scène de films ou de séries, dans lesquels un geek pianote à toute vitesse sur son clavier pour se battre avec des lignes de code et tenter de contrer une menace invisible. Souvent, nous attendons la fin de la séquence et peinons à ressentir une quelconque émotion.

Il y a quelques semaines, des lampadaires de la ville de Leicester en Angleterre sont restés allumés toute la journée,

conséquence d’une cyberattaque ayant complètement déréglé le système. La mairie n’arrivait plus à reprendre la main sur les lumières de la ville. Ce n'est qu'à ce moment-là que les habitants ont véritablement compris l'impact que pourraient avoir ces menaces dans leur vie. Un détail, qui permet de mieux comprendre les risques - parfois pour notre survie. Il est de bon ton de cultiver des zones d’ombres.

DOCUMENT 8

Les régions jouent collectif face à la menace cyber

Frank Niedercorn

Au sein du Campus régional de cybersécurité et de confiance numérique de Nouvelle-Aquitaine (C3NA), trois écrans affichent en temps réel les indicateurs de la menace numérique. Depuis le début de l'année, 222 incidents cyber ont ainsi été traités dans la région (en hausse de 25 % par rapport à 2023) dont 44 sont toujours en cours. Les attaques par rançongiciel concernent 25 % des cas, devant les vols de données (15 %). Près de la moitié des victimes sont les PME, devant les collectivités pour 25 % des cas.

Depuis la fin de l'année dernière, la France dispose ainsi de treize centres de réponse aux incidents cyber ou CSIRT (computer security incident response team). Le rôle de ces vigies de la cyberdélinquance, dont la création a été décidée en 2021, est d'offrir une réponse de premier niveau et de proximité aux incidents pour suppléer les efforts de l'Agence nationale de sécurité des systèmes d'information (Anssi).

Dès la mise sur pied de ce réseau de CSIRT , ses membres ont choisi de jouer collectif. « Au sein de chaque CSIRT, on passe, par exemple, du temps sur le darknet à la recherche de données volées. On appelle évidemment les autres CSIRT dès lors que cela concerne d'autres régions », illustre Bernard Giry,

directeur général adjoint à la transformation numérique de la région Ile-de-France.

La région Rhône-Alpes-Auvergne étant la seule région métropolitaine à n'avoir pas créé de CSIRT, ses homologues transmettent les informations à l'Anssi.

Collaboration d'envergure…

La collaboration ne s'arrête pas là. Ainsi, le Breizh Cyber créé en 2023 a mené une opération d'évaluation des vulnérabilités des collectivités bretonnes en s'appuyant sur le logiciel Onyphe. Sorte de Google de la cybersécurité, celui-ci s'appuie sur les données publiques pour identifier les failles des sites web.

Au printemps, il a répété l'opération à l'échelle nationale. « Nous avons obtenu l'accord de l'éditeur intéressé par cette mise en avant. Quant à nous, cela montrait qu'une entité même jeune pouvait mener une opération d'envergure », explique Guillaume Chéreau, directeur du Breizh Cyber.

25.000

SITEs de collectivités analysEs Avec 186 entités publiques présentant 311 failles critiques

Au printemps 2024, les sites de 25.000 collectivités françaises ont ainsi été analysés. L'opération a permis d'identifier 186 entités publiques présentant 311 failles critiques, notamment sur les logiciels de messagerie ou les systèmes de gestion de parc informatique. « Ce taux de vulnérabilité de 0,73 % constituait plutôt une bonne surprise. En sachant tout de même que Onyphe ne collecte que les vulnérabilités les plus graves », précise Guillaume Chéreau.

Cette démarche collaborative se joue à tous les étages. Ainsi,

en Nouvelle-Aquitaine, le Campus cyber va s'appuyer sur des entreprises privées et seize écoles d'ingénieurs pour tester la résistance aux attaques d'une quinzaine de logiciels métiers de collectivités locales. « Certains logiciels, comme la réservation de salles polyvalente ou de gestion des appels d'urgences dans les Samu ou les Sdis, ont révélé des failles. C'est d'autant plus dangereux qu'ils sont utilisés par 90 % des collectivités », explique Guy Flament, directeur du C3NA.

Ecoles d'ingénieurs et entreprises privées

Pour cette opération d'envergure, qui démarre au mois d'octobre pour deux ans, le campus s'appuie sur Marl Digital Services, une entreprise de services numériques qui se charge du recrutement des élèves ingénieurs qui joueront les hackers de façon éthique. « C'est très motivant pour les élèves ingénieurs qui vont travailler de façon supervisée pour le bien commun, avec des technologies qu'ils ne verront jamais ailleurs », assure Riccardo Montisano, le président de Marl Digital Services qui intervient bénévolement.

Le C3NA demande en effet à chaque entreprise de la filière de participer à l'activité commune « en consacrant 1 % de son temps au fonctionnement du cybercampus », précise Guy Flament.

Des éditeurs de logiciels apportent aussi leur concours. Par exemple, Solidnames, qui édite un logiciel destiné à protéger les marques et qui repère les sites de vente de produits de contrefaçons. Il a donné naissance à Defacement Checker, qui surveille 2.800 sites officiels de la région pour repérer les victimes de « defaçage » (détournement d'un site web par des hackers), comme ce fut récemment le cas de celui de l'office du tourisme des Sables-d'Olonne qui orientait les internautes vers

de faux camping.

« Notre logiciel contenait 90 % des briques permettant de surveiller les sites des collectivités. Il est désormais disponible en open source », explique Anthony Don, directeur associé de Solidnames.

DOCUMENT 9

RÉPUBLIQUE FRANÇAISE
Liberté Égalité Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

CHIFFRES CLÉS

3ÈME ÉDITION DU BAROMÈTRE DE LA MATURITÉ CYBER DES COLLECTIVITÉS :

la frontière s'accentue entre les petites collectivités et celles de plus de 1 000 habitants

44% +6pts
s'estiment
faiblement exposées
aux risques
et 47% pour les - de 1 000 hab

53% +6pts
déclarent bénéficier d'un
bon niveau de protection

14%
se sentent
bien préparées

et pourtant

1 / 10
déclare avoir
déjà été victime
d'une ou plusieurs cyberattaque
au cours des 12 derniers mois

Principales conséquences

Interruption d'activité et de services
37%

Destruction ou vol de données
24%

mais

45%
n'en connaissent pas
la cause

77%
indiquent dépenser
moins de 2 000 €
pour leur cybersécurité
et 87% des - de 1 000 hab

Principaux freins : le manque...

de **connaissances** **47%**

de **budget** **36%**

de **compétences** **36%**

62%
appellent à une
sensibilisation accrue
des élus et agents

*Étude 2024 conduite par OpinionWay pour Cybermalveillance.gouv.fr du 26 août au 4 octobre en ligne (CAWI) auprès d'un échantillon de 1710 élus de collectivités / agents communaux en charge de l'informatique et de la sécurité des communes de moins de 25 000 habitants en France métropolitaine et dans les départements et régions d 'Outre-Mer.

DOCUMENT 10

Qui coûte plus cher, la réglementation ou les cyberattaques ?

Paul Loubière

« Le coût de la réglementation est en train de devenir plus élevé que celui des cyberattaques ! » L'attaque de Guillaume Collard, président de BPR Security, est directe. Dans sa ligne de mire, la directive européenne NIS-2. Le but de ce nouveau texte ? Obliger les entreprises qui travaillent pour des secteurs essentiels à se protéger des cyberattaques. Théoriquement, la directive devrait entrer en vigueur le 1er octobre. Selon l'Anssi, l'organisme français chargé de la cybersécurité, *« elle vise à protéger les acteurs économiques majeurs de l'UE en élargissant le champ des entités et secteurs concernés avec des exigences renforcées. Elle prévoit un socle de mesures juridiques, techniques et organisationnelles que les futures entités régulées devront mettre en œuvre en fonction du risque existant. »*

Schématiquement, la directive distingue les EE (entités essentielles) et les EI (entités importantes), l'attribution de l'une ou de l'autre est faite selon la criticité des activités, la taille et le chiffre

d'affaires. Le nombre d'entités concernées en France n'est pas encore connu avec précision. L'Anssi annonce prudemment *« plus de 10 000 entités sur 18 secteurs d'activité »*. Les professionnels du secteur misent plutôt sur 30 000. D'autres réglementations vont progressivement entrer en vigueur, comme DORA pour le secteur financier.

Inquiétude des entreprises

Malgré les efforts de communication de l'Etat et de l'Anssi, les entreprises restent inquiètes et ignorent jusqu'à quel point elles sont concernées. *« On peut se demander à quel point la réglementation n'est pas plus dangereuse et plus coûteuse que la malveillance »*, lâche Guillaume Collard. Un avis partagé par de nombreux professionnels du secteur : en mars dernier, Helmut Reisinger, directeur général pour l'Europe de Palo Alto Networks, ironisait en qualifiant l'Europe de *« Silicon Valley de la réglementation »*.

Pourtant, même aux Etats-Unis, les mentalités évoluent et les professionnels ne sont pas forcément hostiles à toute réglementation. Pour Joey Levy, directeur général de Sophos, elle est un peu comme le frein sur une voiture : *« C'est parce que vous voulez aller de plus en plus vite que vous avez besoin d'un frein. La réglementation est ce qui permet d'aller plus loin et plus vite. »* Toujours est-il que NIS-2 ne se contente plus de vœux pieux : *« en face de chaque réglementation*, souligne Guillaume Collard, *il y a une sanction. Les autorités se sont rendu compte que dans NIS-1,*

faute de sanction, personne ne faisait rien. »

Un coût insupportable pour l'économie française

Une situation insupportable pour la Commission européenne. Rien qu'en France, la cybercriminalité représente 129 milliards de dollars, soit près de 5 % du PIB, selon Statista Technology Market Insights. A l'échelle mondiale, le cyber crime coûte plus de 5 000 milliards. Ces considérations ont amené la Commission à prendre une décision de sécurité pour des motifs avant tout économiques. *« NIS-2 n'est pas un sujet tech*, poursuit Guillaume Collard, *c'est un sujet économique. La directive a été écrite en ce sens, pour protéger l'économie européenne. C'est pour sauver l'économie que la sanction ne portera pas sur les finances de l'entreprise mais sur les dirigeants. En cas de manquement, ce n'est pas l'entreprise qui paye, c'est le PDG qui risque sa tête. »* De fait, la grande nouveauté consiste à impliquer directement les dirigeants.

La conformité n'est pas un gage de cyberprotection

Les cabinets d'avocats et les cabinets de conseils sont en ordre de marche. En cas d'attaque, les entreprises concernées devront démontrer qu'elles ont respecté l'obligation de moyens. *« C'est le paradoxe de cette loi*, reprend Guillaume Collard. *Les entreprises vont davantage chercher à se mettre en conformité qu'a se mettre en sécurité. La conformité n'est pas un gage de sécurité et, inversement, une cyberprotection, aussi bonne soit-elle, n'entraîne pas automatiquement la conformité. »* La multiplication des cabinets de conseil autoproclamés spécialistes en cybersécurité et

NIS-2 conduit parfois à des excès : *« certains n'hésitent pas à faire croire à des PME qu'elles sont concernées alors que ce n'est pas le cas »*, confie un professionnel.

La directive n'est pas encore transcrite en droit français

« Il ne faut pas croire pour autant que ce soit une manne, corrige Elisabeth Marrache avocate associée chez Addleshaw Goddard. *La transposition de NIS-2 en droit français n'a pas encore été faite. Un projet de loi a été déposé en avril mais il n'a pas été discuté. Ce sera au nouveau gouvernement de le traiter. Je ne pense pas qu'il y aura tout d'un coup une ruée vers les cabinets d'avocats. Les entreprises sont plus mûres aujourd'hui que lors de l'adoption du RGPD. Nous sommes davantage dans un travail d'accompagnement continu car il y a toujours de nouvelles réglementations et de nouvelles transpositions. Nous effectuons un travail de veille permanente. »* Quant aux sanctions brandies pour faire peur aux dirigeants, si elles sont bien réelles, Vincent Strubel, directeur général de l'Anssi, a rappelé qu'aucune ne serait appliquée durant les trois premières années suivant le lancement de la directive NIS-2, *« afin de donner aux entités dites essentielles et importantes le temps nécessaire pour se mettre en conformité avec les nouvelles exigences de cybersécurité et de cyber-résilience. »* Un répit pour les entreprises.

DOCUMENT 11

CYBIAH, la cybersécurité abordable pour les PME et les collectivités d'Ile-de-France - Touteleurope.eu

Juliette Verdes

Porté par le Campus Cyber, le programme CYBIAH (Cybersécurité et Intelligence Artificielle Hub) donne les moyens aux petites entreprises et aux collectivités locales de se protéger des cyberattaques. Il est soutenu par la Région Ile-de-France et l'Union européenne.

Le programme CYBIAH réunit un consortium d'acteurs privés et publics, notamment des établissements de l'enseignement

supérieur - Crédits : CYBIAH

“Rançongiciels”, phishing, espionnage… : les cybercriminels disposent de nombreux moyens pour déstabiliser les entreprises et paralyser les administrations, parfois pendant de longues semaines. Dans un rapport annuel en 2022, l’Agence nationale de la sécurité des systèmes d’information (Anssi) constatait que les petites entreprises étaient une cible privilégiée. Si les plus grandes sociétés ont investi ces dernières années pour se prémunir contre la cybermalveillance, seule une TPE/PME sur trois est correctement protégée.

Le projet CYBIAH est né de ce constat : celui de la difficulté pour ces petites structures d’accéder à une offre de services cyber, et de la nécessité de prévenir ces attaques en leur proposant des solutions concrètes.

“*Les PME, c’est un énorme sujet : elles constituent plus de 90 % de notre tissu économique. Si l’on compte les TPE, ce sont 4 millions de structures au total qui sont concernées*”, explique Yann Bonnet, directeur général délégué du Campus Cyber. “*CYBIAH vise à les aider à mieux comprendre les problématiques de type cyber, et à trouver des solutions qui leur sont adaptées*”, poursuit ce spécialiste des questions numériques.

L’Union européenne finance ce projet à hauteur de 5 millions d’euros, dont 2 millions dans le cadre du Fonds européen de développement régional (FEDER) géré par la Région Île-de-France.

Un accompagnement personnalisé

CYBIAH réunit un consortium d’acteurs privés et publics de la cybersécurité et du numérique. Il est coordonné par le Campus

Cyber à Paris, qui assure la gestion stratégique et opérationnelle du programme. Les experts issus de cet écosystème proposent un accompagnement personnalisé aux structures franciliennes qui sont éligibles : les petites collectivités territoriales, et les entreprises comptant entre 10 et 250 employés dont le chiffre d'affaires annuel est inférieur à 50 millions d'euros.

Le parcours CYBIAH est composé de plusieurs étapes. Des actions de sensibilisation aux risques cyber sont d'abord menées auprès des entreprises et des administrations. Après avoir évalué leur "maturité" cyber puis réalisé un diagnostic des besoins, les experts de CYBIAH leur proposent un plan d'action. Le programme joue ainsi le rôle de tiers de confiance en les mettant en relation avec des partenaires adaptés.

"*Grâce aux fonds alloués par la Commission européenne et la Région, nous proposons un plan d'action sans reste à charge. Sans l'aide de l'Ile-de-France et de l'Europe, ces PME n'auraient pas eu les moyens de se protéger*", souligne Yann Bonnet. "*Nous orientions les entreprises vers des possibilités de financements qui leur permettent d'acheter des solutions, comme le dispositif "chèque cyber" proposé par la Région Ile-de-France par exemple*".

Le profil des structures accompagnées est très divers. De nombreux secteurs sont concernés : la santé, l'agroalimentaire, les nouvelles technologies, l'informatique quantique… et même la pâtisserie.

Un pôle européen de référence

CYBIAH a été sélectionné comme pôle européen d'innovation numérique par la Commission européenne. Dans le cadre du

programme Digital Europe, ces “*European Digital Innovation Hubs*” (EDIH) sont désignés et coordonnées par l’exécutif européen. Ils aident les entreprises et les organisations du secteur public à relever les défis numériques et à devenir plus compétitives. On en compte actuellement 151 présents dans tous les Etats membres de l’UE, en Islande, au Liechtenstein et en Norvège.

Une reconnaissance pour CYBIAH qui apporte de la visibilité et des opportunités de collaboration à l’échelle européenne : des “EDIH corridors” ont été mis en place, permettant aux experts du programme d’échanger des informations et des bonnes pratiques avec leurs homologues européens. “*L’idée est de bénéficier de l’effet de réseau européen pour gagner en intelligence collective*”, précise Yann Bonnet.

Le projet a donc vocation à se développer à travers l’Europe, mais aussi en France. Le modèle de CYBIAH pourrait être répliqué à l’avenir dans d’autres régions dotées d’un campus cyber ou d’un pôle technologique. Des initiatives qui devraient stimuler l’emploi, dans un secteur en pleine expansion mais qui peine encore à recruter : environ 15 000 postes restent à pourvoir en France à l’heure actuelle.

Le programme vous intéresse mais vous n’êtes pas en Ile-de-France ?

CYBIAH propose également des services de conseil en cybersécurité pour les structures localisées hors d’Ile-de-France. Un reste à charge est à prévoir en revanche pour les services fournis. Si vous souhaitez bénéficier d’aides, il faudra pour cela vous rapprocher des gestionnaires de fonds européens dans votre région pour déterminer les sources de financement disponibles en matière de cybersécurité.

DOCUMENT 12

Les pompiers des Pyrénées-Atlantiques victimes d'une cyberattaque

sudouest.fr

Le service départemental d'incendie et de secours des Pyrénées-Atlantiques (Sdis 64), basé à Pau, est la cible d'une cyberattaque depuis jeudi 12 octobre. L'accueil des appels d'urgence au 18 n'est pas affecté, assure la préfecture

« Le service départemental d'incendie et de secours des Pyrénées-Atlantiques (Sdis 64) connaît depuis ce jeudi 12 octobre au matin une cyberattaque affectant ses infrastructures informatiques et bureautiques. »

La panne informatique, rendant le réseau administratif inopérant, aurait débuté tôt le matin, jeudi.

Dans un communiqué envoyé le soir même, la préfecture des Pyrénées-Atlantiques explique que « des mesures ont immédiatement été prises afin d'assurer la continuité des activités du Sdis 64 et permettent de maintenir la réponse opérationnelle à son niveau attendu ».

Elle précise que la réception d'appels d'urgence par le 18 « n'a pas été impactée par cette attaque et reste pleinement fonctionnelle ».

Une attaque comparable avait ciblé les pompiers de Dordogne (Sdis 24) en novembre 2019, ou encore de Lot-et-Garonne (Sdis 47) en mars 2021. A Agen, plus d’une centaine de postes informatiques, soit la moitié du parc, avaient été durablement affectés.