MINISTÈRE
DES ARMÉES
Liberté
Égalité
Fraternité

Service du commissariat des armées

CONCOURS EXTERNE SUR ÉPREUVES
DE RECRUTEMENT D'ÉLÈVES COMMISSAIRES DES ARMÉES EN 2023

RÉDACTION
D'UNE NOTE DE SYNTHÈSE

durée : 4 heures – coefficient 7

Le défi de la mise en œuvre d'une politique publique d'accompagnement de la société française vers la cyber résilience

Vous êtes chargé de mission au sein du cabinet du ministre délégué chargé de la transition numérique et des télécommunications. En vue de l'audition du ministre délégué à l'Assemblée Nationale, le chef de cabinet vous demande de produire une synthèse des actions de l'Etat engagées afin de renforcer la cyber résilience de la Nation.

Sachant que la digitalisation de la société pose de nombreuses questions de sécurité auxquelles les députés sont naturellement vigilants, vous vous attacherez à démontrer que, si cette transition numérique est inéluctable et source de gains d'efficacité, la question connexe de la cyber-résilience est centrale.
Cette note devra rappeler tout d'abord les menaces puis les actions entreprises pour y remédier et formuler des propositions pour renforcer la cyber résilience de la société française dans ses composantes à la fois privée et publique.

Pour cela vous utiliserez les documents du dossier mis à votre disposition ainsi que vos connaissances personnelles sur le sujet.

Vous inscrirez à la fin de votre composition le nombre de mots qui la composent, soit un total de 900 mots (plus ou moins 10%).

SOMMAIRE

Les Echos

De la cyber-sécurité à la cyber-résilience

Dans un environnement de plus en plus incertain, garantir la continuité du business exige d'adopter des approches plus proactives et mieux intégrées. En appliquant les dernières normes et les meilleures pratiques, pour assurer une protection des systèmes « by design » et garantir la confiance des organisations dans le numérique, la cyber-résilience devient fondamentale.

Yves Reding, 14/03/2018

L'année 2017, charnière dans la transformation numérique des entreprises, a vu les systèmes informatiques et les professionnels de la cyber-sécurité mis à rude épreuve. En effet ces derniers mois, des attaques DDoS massives et plusieurs épidémies de ransomware sont venues perturber les activités d'organisations internationales. Beaucoup ont subi des prises d'otage ou ont été paralysées par des attaques malveillantes. Des processus électoraux au sein de pays démocratiques ont même été perturbés par des cyber-activistes aux intentions douteuses.

2017 a été marquée par une nouvelle ère numérique. La multiplication des attaques a mis en évidence les fragilités de nos organisations et les failles de nos sociétés de plus en plus digitales. On a découvert par la même occasion les limites d'une approche traditionnelle en cyber-sécurité, qui vise essentiellement à protéger les systèmes. La cyber-sécurité est dépassée, car trop restrictive ; il faut une approche globale totalement intégrée impliquant à la fois les individus, les processus et la technologie : la cyber-résilience.

Opter pour une approche active

La gestion des données sensibles requiert une approche plus holistique de la sécurité digitale, mieux intégrée aux enjeux organisationnels et business. Dans le contexte actuel, il faut changer de paradigme. La question n'est plus de savoir si l'on va être attaqué, mais bien quand ! À partir de là, nous devons pouvoir mieux nous préparer à absorber le choc, réagir à toute éventualité et rebondir.

Chacun évolue dans un environnement, le cyberespace, incertain, instable, potentiellement hostile. À la manière d'un kayakiste qui descend un torrent et doit jouer avec le courant, éviter les rochers, l'organisation au coeur du cyberespace doit gagner en agilité et en flexibilité. Il faut pouvoir évoluer en tenant compte des éléments présents dans son environnement.

Face à l'éventualité d'un incident de sécurité ou de continuité, il faut opter pour une approche proactive, dynamique, composer en permanence avec les éléments, anticiper et contourner les obstacles, surfer, accélérer, rester la tête hors de l'eau.

Pour certains, moins bien préparés, l'objectif premier sera de survivre. Pour les plus résilients, il s'agira au contraire de rebondir, d'avancer et de profiter de la vitesse du torrent.

Identifier, protéger, détecter, répondre, récupérer : les cinq piliers de la cyber-résilience

La cyber-résilience constitue une approche globale qui intègre cyber-sécurité, continuité d'activité, gestion de crise, stratégie de réponse et organisation de la résilience. En permanence, il faut pouvoir identifier, protéger, détecter, répondre à l'incident et récupérer les systèmes pour garantir la continuité de l'activité et rebondir. C'est l'approche suggérée par la directive NIS, qui vise à sécuriser les réseaux et les systèmes d'information contre tout risque et incident au niveau des infrastructures critiques européennes.

Finalement, la cyber-sécurité n'est qu'un sous-ensemble de la cyber-résilience. On parle de développer pour chaque activité dépendante du numérique un système immunitaire performant. Pour qu'il soit efficient, il faut que les différentes composantes de l'organisation interagissent de manière coordonnée, selon une approche systémique.

Mettre en œuvre une approche par les normes

Pour inviter les acteurs à mieux évoluer et se protéger dans cet univers incertain, les organisations internationales et autorités publiques prônent le développement et le respect de normes toujours plus poussées - ISO 27001 (gestion de la sécurité de l'information), 20000 (gestion des services informatiques), 27018 (protection des données à caractère personnel) ou 22301 (gestion de la continuité d'activité). Ainsi, la nouvelle norme française d'Hébergeur de Santé à caractère personnel qui sera d'application en 2018 exigera les normes ISO 27001, 20000 et 27018.

De même, pour construire le marché unique digital européen, l'Union européenne se dote de nouveaux outils, comme une agence de la cyber-sécurité (rôle confié à l'ENISA) ou encore la directive NIS.

Pour les opérateurs de service numérique, il est fondamental de développer une proposition de valeur de bout en bout dans le domaine de la gestion des données sensibles. Cela permet de garantir la continuité, la sécurité, la protection des activités des clients face à l'ensemble des risques. En apportant toutes les garanties de confiance, les opérateurs de service numérique créent de la valeur dans ce monde digital de plus en plus incontournable, mais également de plus en plus complexe et incertain.

Élaborer une approche « cyber-résilience » intégrée à grande échelle

Choisir une approche intégrée suivant une stratégie d'amélioration continue garantit la protection des clients face aux risques de plus en plus menaçants. Faire évoluer son Security Operation Center (SOC) en intégrant des solutions d'investigations sécurité est également fondamental. Grâce à des algorithmes sophistiqués, celles-ci conduisent à une détection prédictive des menaces au départ de l'analyse des comportements déviants au sein des systèmes d'information. En sus, elles constituent un composant clé dans l'investigation et la remédiation. Autre vecteur de succès, l'intégration d'équipes de conseil et d'équipes opérationnelles renforce considérablement les centres de compétences « cyber-résilience ».

On ne peut plus séparer les enjeux business des problématiques de continuité, de sécurité et de résilience. Les divers éléments entrant en ligne de compte pour garantir le fonctionnement du business doivent être totalement intégrés, comme les cinq doigts d'une même main. Il nous faut mettre en oeuvre des approches de cyber-résilience « by design » renforcées et de bout en bout. La résilience de toute activité, et donc de l'économie digitale, se joue de plus en plus à l'échelle européenne. Seul, dans son pays, on ne peut pas y arriver. Nous devons favoriser l'émergence

de mécanismes de lutte plus efficients à l'échelle du marché numérique unique, notamment en matière de gestion de l'information la plus sensible.

LEMONDE INFORMATIQUE

Certification SecNumCloud, des aides financières pour les start-ups et PME de la cybersécurité

Dominique Filippone , publié le 22 Décembre 2022

Pour accompagner les start-ups et petites et moyennes entreprises de la cybersécurité dans l'obtention d'une qualification SecNumCloud, des aides pouvant atteindre 180 000€ sont proposées. Un guichet unique en ligne est ouvert jusqu'au 19 juillet 2023 mais pourra être fermé avant en cas d'épuisement des moyens affectés au dispositif.

Les prestataires d'audit de la sécurité des systèmes d'information et d'accompagnement et de conseil en sécurité délivreront les modules du dispositif d'accompagnement SecNumCloud. (crédit : akitada31/Pixabay)

Bruno Le Maire, ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique, l'avait annoncé lors de l'inauguration du datacenter SGB5 d'OVH à Strasbourg en septembre dernier. Le dispositif d'accompagnement des petits éditeurs de la cybersécurité pour obtenir la qualification SecNumCloud est désormais sorti de terre. Le gouvernement a créé cet outil pour aider financièrement les start-ups et les PME françaises proposant une offre SaaS ou PaaS en cybersécurité dans cette démarche. Il « s'adresse en priorité à des PME souhaitant commercialiser une offre qualifiée SecNumCloud sous 2 ans, qui ciblent un marché dont les clients ont besoin de recourir à des offres qualifiées, et dont les statuts et les modalités de contrôle ne sont pas manifestement incompatibles avec le référentiel SecNumCloud », précise un document présentant le guichet d'accès à ce dispositif.

Les aides sont organisées en 4 formules : audit inital (évaluation et mesure du niveau cyber), transformation (intégration d'actions cyber dans le fonctionnement technique et orgaisationnel de l'entreprise), conformité (audit de qualification à blanc en application avec les pratiques de l'ANSSI) et aide à la qualification (démarche, respect et application des règles du référentiel de l'ANSSI et visa de sécurité de l'agence). « Les modules d'accompagnement seront délivrés par des prestataires d'audit de la sécurité des systèmes d'information (PASSI) ou des prestataires d'accompagnement et de conseil en sécurité (PACS) lorsque le référentiel sera en vigueur, sous supervision de l'ANSSI », indique le document.

Une part d'autofinancement nécessaire

Les montants pour des modules audit initial, formule conformité et qualification SecNumCloud pourront atteindre 40 000 €, tandis que celui relatif à la formule transformation s'élèvera au maximum à 60 000 €. « Il est attendu que les entreprises candidates apportent une part d'autofinancement en complément du financement public, s'agissant d'une part de leurs coûts internes pour participer aux modules et, d'autre part, du financement de l'audit de qualification », précise le gouvernement.

L'obtention de ces aides nécessite le dépot d'un dossier via un guichet unique accessible sur le site de Bpifrance entre le 20 décembre 2022 et le 19 juillet 2023. Toutefois, ce délai pourrait être raccourci « en cas d'épuisement des moyens financiers affectés à ce dispositif ». Concernant les conditions d'élligibilité, il est notamment précisé que « le capital social et les droits de vote dans la société de l'entité candidate ne doivent pas être, directement ou indirectement, individuellement détenus à plus de 24% et collectivement détenus à plus de 39% par des entités tierces possédant leur siège statutaire, administration centrale ou principal établissement au sein d'un État non-membre de l'Union européenne ».

A S S E M B L É E N A T IO N A L E

Commission de la défense nationale et des forces armées
Audition, à huis clos, de M. Stéphane Bouillon, Secrétaire général de la défense et de la sécurité nationale.
Mercredi 13 juillet 2022

M. le président Thomas Gassilloud. Monsieur le secrétaire général […] vous êtes responsable de la politique de cybersécurité des systèmes d'information classifiés interministériels et de la lutte contre les ingérences numériques étrangères. Pour ces missions, vous disposez de l'agence nationale de sécurité des systèmes d'information (ANSSI),
[…]
Ces derniers mois, vous avez beaucoup travaillé sur une stratégie nationale de résilience visant à tirer les enseignements de la crise sanitaire et à renforcer notre capacité collective à réagir après un choc, de quelque nature qu'il soit : attaque cyber, choc sanitaire, choc énergétique, choc climatique…

Notre défense est efficace si elle est globale. C'est pourquoi, au-delà de l'effort militaire, nous sommes sensibles au fait que l'ensemble du Gouvernement et même l'ensemble des acteurs de la nation soient impliqués dans la défense nationale.
M. Stéphane Bouillon, secrétaire général de la défense et de la sécurité nationale.

[…] Le SGDSN se penche […] sur les nouvelles formes de conflictualité, dites menaces hybrides, et sur le concept « comment gagner la guerre sans avoir à combattre », théorisé par le chef d'état-major des forces armées russes, le général Guerassimov, qui reprenait la théorie ancienne de Sun Tzu (même si celui-ci ignorait les attaques cyber).

Les attaques cyber sont les plus connues puisqu'elles nous touchent tous : citoyens, petites entreprises, entreprises moyennes, grands groupes sont victimes des rançongiciels via le chiffrage des données et des escroqueries. Nous assistons à l'explosion du nombre d'attaques et d'extractions de fichiers, d'espionnage, d'attaques en sabotage par des États et des proxies d'État. En 2021, l'ANSSI a constaté 1 082 intrusions avérées, soit une augmentation de 37 % par rapport à 2020. Et encore, en 2020, en raison du Covid et du recours accru à des moyens numériques, cela avait-il déjà beaucoup augmenté par rapport à l'année précédente. Nous avons en mémoire des affaires célèbres, comme le blocage des systèmes informatiques des hôpitaux, le blocage des services publics et des collectivités locales, l'impossibilité d'émettre ou d'imprimer des journaux pour les grands médias, l'interruption de l'activité des entreprises et des transports. Les smartphones sont de plus en plus touchés. On se souvient de l'affaire Pegasus. Sur les messageries chiffrées comme Telegram ou Whatsapp, il devient alors facile de s'emparer des données d'un smartphone piégé, y compris celles en mémoire et dans le Cloud qui transiteraient sur le smartphone en question. Certains groupes et certains États sont capables d'utiliser ces vulnérabilités contre les uns et les autres. D'ailleurs, avant la campagne pour l'élection présidentielle, nous avions réuni les représentants de tous vos partis pour les mettre en garde sur ces menaces.

[…] Lors de la préparation du service de lutte contre les ingérences numériques d'origine étrangère Viginum, nous avions rencontré les présidents de commissions et les chefs des principaux partis politiques. Il ne s'agissait nullement de s'intéresser à la vie politique française, mais d'observer les attaques numériques de l'étranger ou de proxies de l'étranger visant à porter atteinte à l'ordre public, à la sincérité des élections ou à la stabilité de la société. Après l'attentat contre Samuel Paty, nous

avons subi des attaques venant d'un État étranger, qui ont eu pour objectif de déstabiliser la population et de permettre au dirigeant de ce pays de réassoir son autorité sur sa communauté. Lors des élections, nous avons été attentifs à des attaques de l'ultra-droite américaine visant à mettre en cause la sincérité de nos scrutins et de notre système électoral. Nous subissons aussi de fortes attaques de la Russie contre la présence française en Afrique.

D'autres attaques peuvent viser les entreprises. Danone avait fait l'objet d'attaques fortes sur les médias et plateformes en ligne, fomentées par un pays étranger à l'aide de concurrents, qui avaient nui à son chiffre d'affaires et à sa capacité à réagir.
[…]
Le troisième type de menace hybride est les attaques par détournement du droit, ou « Law Fare », à l'encontre de nos entreprises. Il s'agit de l'application par un État étranger de sa loi dans notre pays. Les Américains sont experts en ce domaine […] La présence d'un composant américain, ne serait-ce qu'une puce, dans le produit d'un État étranger, ouvre le droit aux Américains de demander des explications sur la manière dont il est produit, même si cela relève du secret professionnel, voire de poursuivre l'entreprise et ses dirigeants. En outre, le *Cloud Act* permet aux services de renseignement américains de plonger dans les *Clouds* fournis par des entreprises installées aux États-Unis, les cloud pouvant être n'importe où dans le monde, pour y rechercher des informations sans que personne n'en soit informé et sans autorisation. Le *Defence Act* permet de bloquer des exportations contraires aux intérêts des États-Unis. Les Chinois sont en train de copier ces lois presque mot pour mot. Tout cela complexifie une partie de nos exportations.

[…]
Face aux nouvelles formes de conflictualité, l'ANSSI, qui dispose de 176 millions d'euros au titre du plan de relance, a aidé 600 entités. Des projets de loi viseront à renforcer ses prérogatives pour obliger les plateformes à signaler à leurs clients les vulnérabilités et les attaques. Si, à partir de 130 km/h, la direction de la voiture que je viens d'acheter se met à faseiller, le constructeur a l'obligation de me prévenir. Mais si j'utilise un système informatique vulnérable, exposé à une prise de contrôle extérieur ou au sabotage, l'entreprise n'a pas obligation de me le dire.

Nous allons multiplier le nombre de centres agréés pour aider les entreprises et les particuliers à faire face aux attaques. Nous avons déjà développé des centres dans les régions. Nous allons accroître le contrôle sur les opérateurs d'importance vitale (OIV) et les opérateurs de services essentiels (OSE) afin de les obliger à réaliser les investissements nécessaires pour protéger leur sécurité informatique et à renforcer leur sécurité en tant qu'établissements recevant du public. Cela implique une progression des moyens de l'ANSSI, si vous en décidez ainsi lors de l'examen du prochain projet de loi de finances.

[…] Pendant la guerre en Ukraine, on s'attendait à de nombreuses cyberattaques de la part de la Russie, mais nous en avons eu très peu à ce jour. La seule attaque notable était dirigée contre un satellite de VIASAT, géré par Eutelsat, qui permettait aux forces ukrainiennes de communiquer entre elles et qui arrosait l'Europe de l'Ouest. Il a été atteint, probablement par les Russes, en grillant tous les modems. Chez nous, cela a touché des relais de secours du 15, du 18. En Allemagne, une bonne partie des éoliennes se sont arrêtées.

[…] Des cyberattaques par la criminalité organisée touchent de très grosses entreprises. Ce fut le cas d'un gros armateur qui a son siège sur la Côte d'Azur. Les rançons sont très fortes, mais on se protège.

Certains groupes de criminalité organisée commencent à s'intéresser davantage à des entreprises moins protégées, comme des PME et des TPE. Nous avons observé un petit creux après le début de la guerre en Ukraine. Ils se sont employés à se frapper de chaque côté de la frontière, donc un peu moins sur nous. Moins d'hôpitaux ont été visés, parce que les cybercriminels se sont rendu compte que les hôpitaux n'ont ni le droit ni la capacité de payer.

Des menaces importantes continuent de peser sur les grandes infrastructures étatiques, administratives. Il s'agit souvent d'attaques d'État à État, visant à nuire et à placer des chevaux de Troie. La plus grosse difficulté dans ce domaine, c'est l'installation, dans les grands services publics ou ailleurs, de dispositifs que personne ne décèle et, le jour venu, on appuie sur un bouton et tout s'arrête. C'est un point sur lequel nous essayons vivement de réagir.

[…]
L'ANSSI avec le MEFSIN travaillent à mettre en place des « Clouds de confiance », c'est-à-dire des Clouds qualifiés et répondant à des critères de sécurité et de protection détaillés dans un référentiel produit par l'ANSSI (SecNumCloud). Nous négocions et travaillons avec de gros opérateurs comme Microsoft et avec des entreprises françaises afin qu'ils mettent en place des offres « hybrides » qualifiées par l'ANSSI et supportant certains outils développés par des acteurs étrangers sans permettre aux pays d'origine d'avoir accès à des données sensibles (pour la sécurité économique, pour la protection des données à caractère personnel, etc.). Nous progressons avec certains, prenons du retard avec d'autres. Pour les Jeux olympiques de 2024, une négociation est en cours avec Alibaba, fournisseur officiel de Cloud pour les Jeux olympiques. Nous avons imposé d'avoir un Cloud souverain en France, qui nous permettra d'héberger et donc protéger en France toutes les données sensibles.

[…]
Nous sommes inquiets de l'évolution vers des cyberattaques diffuses et simultanées. Grâce à ses moyens renforcés, l'ANSSI, serait certes capable de faire face à quelques attaques simultanées menées par quatre ou cinq grandes unités identifiées, mais après, ce serait beaucoup plus complexe. Nous prévoyons de travailler plus efficacement avec des sociétés privées comme Orange, Thales, Atos ou Sopra Steria, qui proposent des services qualifiés et donc vérifiés par l'ANSSI sur différents segments. En fonction de leur expertise, elles peuvent agir au profit de différentes entreprises et les soutenir sur les questions de cybersécurité et cyberdéfense. Nous mettons en place avec les conseils régionaux des accords visant à créer des centres de réponse aux attaques dans chacune des régions, afin de développer un dispositif de cybersécurité au profit des PME, TPE, des entreprises locales et petites entreprises.

L'USINENOUVELLE

21 Novembre 2022 \ 08h00

Comment 750 PME et ETI vont pouvoir bénéficier d'un accompagnement en cybersécurité en 2023

Lors de la semaine européenne de la cybersécurité, qui s'est déroulée du 15 au 17 novembre à Rennes, le ministre délégué à la Transition numérique, Jean-Noël Barrot, a annoncé le lancement d'un nouveau volet du plan cybersécurité pour 2023. Doté de 30 millions, il comprend l'activation d'un «bouclier cyber» à destination de 750 PME et ETI.

Le gouvernement prévoit pour 2023 une nouvelle enveloppe de 30 millions d'euros pour financer un nouvel ensemble de mesures de cybersécurité. Elles viseront les PME-ETI, les acteurs publics et les particuliers.

La France continue de déployer sa stratégie nationale en cybersécurité. Dans le cadre de ce plan, annoncé en février 2021 par Emmanuel Macron, un nouveau volet doté de 30 millions d'euros va être lancé en 2023, a annoncé mercredi 16 novembre le ministre délégué à la Transition numérique, Jean-Noël Barrot, lors de sa venue à la semaine européenne de la cybersécurité, à Rennes.

Ce nouveau volet comprend un ensemble de mesures spécifiquement dédiées aux PME et ETI, les plus visées en matière d'attaques aux rançongiciels d'après l'Anssi. Pour élever leur niveau en cybersécurité, le gouvernement prévoit trois actions: une campagne de communication pour promouvoir le site cybermalveillance.gouv.fr, dispositif national d'assistance aux victimes de cyberattaques qui souffre d'un déficit de notoriété; la création d'un service en ligne d'autodiagnostic gratuit pour permettre à chaque entreprise de mieux connaître son niveau en cybersécurité et les premières mesures à enclencher; et enfin le lancement d'un «bouclier cyber» qui ciblera 750 PME et ETI.

Viser les secteurs de la directive européenne NIS2

«Nous avons budgété un accompagnement pour 750 entreprises qui vont, elles, s'engager dans un investissement plus pérenne, explique une source à Bercy. *L'Etat veut amorcer mais il n'a pas vocation à sécuriser les entreprises.»* Les 750 PME et ETI vont être sélectionnées sur la base d'un appel à manifestation d'intérêt, avec remise d'un dossier présentant un projet de sécurisation que l'Etat aidera donc à financer mais sur lequel elles devront aussi engager un financement propre. Bercy précise vouloir cibler des entreprises relevant des secteurs critiques listés par la nouvelle directive européenne NIS2, pour lesquels elle va ouvrir de nouvelles obligations en matière de cybersécurité.

Ce «bouclier cyber», qui reprend le modèle des parcours de sécurisation des collectivités territoriales et institutions de service public (comme les hôpitaux), mis en place par l'Agence nationale de la sécurité des systèmes d'information (Anssi), comprend trois phases que sont l'audit, l'accompagnement et la mise en oeuvre de solutions. Il sera opéré par les services de Bercy et l'Anssi.

Filtre anti-arnaque et cyber-score sur le web

La sécurisation des PME et ETI est d'autant plus importante qu'avec la progression du niveau de sécurité des grands groupes, elles sont devenues une cible privilégiée des attaques et un potentiel maillon faible pour toute la chaîne de valeur. L'Anssi alertait ainsi dès juin 2021 sur la multiplication des attaques via la chaîne logistique.

Toujours dans l'optique d'élever le niveau de sécurité à tous les étages, la nouvelle enveloppe de 30 millions d'euros va également financer des actions à destination du grand public et des acteurs publics (collectivités territoriales et hôpitaux principalement). Pour ces derniers, les parcours de sécurisation de l'Anssi vont être renforcés pour 125 institutions, parmi les 950 qui en ont déjà bénéficié, et 50 nouveaux parcours vont être lancés pour atteindre l'objectif de 1 000 institutions accompagnées d'ici à la fin 2023. Une plateforme de services mutualisés (accessible sur abonnement) va également être lancée en 2023 par l'Etat pour permettre à toutes les collectivités, y compris les plus petites, de bénéficier de trois outils sécurisés: un nom de domaine, une messagerie et des solutions d'hébergement (pour les services en ligne des mairies par exemple).

Dernière strate: les particuliers. Pour eux, le gouvernement prévoit la mise en œuvre, d'ici à l'été 2024, d'un filtre anti-arnaque visant à avertir les internautes (web et mobile) quand ils atterrissent sur un site jugé malveillant. D'ici fin 2023, un cyber-score, basé sur le même modèle que le Nutri-score dans l'alimentation, doit également s'afficher sur tous les sites Internet et réseaux sociaux pour indiquer son niveau de protection par rapport aux données transmises par l'internaute. De quoi tenter de prévenir une cybermenace jugée maximale pour les jeux Olympiques de Paris 2024.

Les Echos

L'hôpital de Versailles victime d'une cyberattaque

Publié le 5 déc. 2022

Après le centre hospitalier de Corbeil-Essonnes en août dernier, l'établissement hospitalier de Versailles est à son tour sous le coup d'une cyberattaque qui perturbe fortement son activité depuis dimanche. Le système informatique a été coupé et l'entrée des malades, réduite.

La panne dure depuis maintenant deux jours. L'établissement hospitalier de Versailles, dans les Yvelines, est victime d'une cyberattaque depuis la soirée de samedi, qui perturbe le travail des soignants et l'accueil des malades. Ce lundi matin, le centre était encore sous le coup de cette cyberattaque. En août dernier, l'hôpital de Corbeil-Essonnes avait déjà pâti d'une telle attaque.

Face à cette tentative de piratage, le centre hospitalier André-Mignot a coupé son système informatique et réduit l'entrée des malades, selon la direction. Il a également déclenché son plan blanc et partiellement déprogrammé les activités du bloc opératoire. L'établissement « met tout en oeuvre » pour maintenir les soins ambulatoires et de consultation, a expliqué la direction.

La cyberattaque vise la totalité de l'établissement, dont l'hôpital André-Mignot, la maison de retraite Despagne et l'hôpital Richaud de Versailles, situé à quelques kilomètres. Du personnel supplémentaire a été mobilisé en renfort pour assurer les soins en réanimation et soin continu, et du matériel a été apporté, selon le ministre de la Santé, François Braun, qui s'est exprimé dimanche soir après une visite dans l'établissement qui emploie environ 3.000 soignants et accueille 700 patients en temps normal. Pour l'heure, l'origine de l'attaque n'a pas été dévoilée.

Transfert des patients critiques

« Les médecins doivent faire toutes leurs prescriptions de médicaments manuellement », ont expliqué des aides-soignantes à l'AFP. Les machines de soins fonctionnent mais pas leur mise en réseau. « Il faut une personne devant chaque chambre pour surveiller les écrans », a expliqué le ministre.

L'hôpital s'est mis en mode « protection des données », a-t-il précisé. Le Samu, pour sa part pas atteint par la cyberattaque, s'est placé en renfort en cas de besoin. Plusieurs patients, ceux dont les cas sont les plus lourds, ont par ailleurs été transférés.

Le ministre délégué à la Transition numérique, Jean-Noël Barrot, a conseillé aux habitants de contacter le 15 plutôt que de se rendre aux urgences du centre hospitalier, dont « l'accueil est extrêmement limité ».

Attaques à répétition

Le parquet de Paris vient d'ouvrir une enquête préliminaire et une plainte a été déposée par l'hôpital. Les investigations ont été confiées au Centre de lutte contre les criminalités numériques de la gendarmerie, qui mènera l'enquête, et à la Sous-direction de la lutte contre la cybercriminalité de la police judiciaire.

Le centre André-Mignot de Versailles a déjà été la cible d'attaques ces derniers mois, qui ont été déjouées, d'après François Braun. « Le système de santé subit des attaques quotidiennes », a-t-il indiqué, assurant que « l'immense majorité de ces attaques sont stoppées ». Le 22 août, le centre hospitalier de Corbeil-Essonnes avait vu son fonctionnement fortement perturbé par une cyberattaque importante qui avait désorganisé son activité durant plusieurs semaines.

E-administration et transition numérique de l'Etat

L'e-administration et la transition numérique en quelques points clés

L'administration électronique ou e-administration a été définie dès 2003, dans un rapport de l'OCDE, comme « l'utilisation des techniques de l'information et de la communication (TIC), et en particulier d'Internet, dans le but d'améliorer la gestion des affaires publiques » (*L'administration électronique : un impératif*). Actuellement, c'est le terme de transition ou de transformation numérique de l'Etat qui semble s'imposer.

Vecteur d'amélioration de la relation administration/citoyen, le numérique permet de proposer une offre plus performante de services aux usagers et d'accroître la transparence administrative. Il est également au coeur de la problématique de modernisation de l'Etat, car il se présente comme un outil d'amélioration de ses procédures et de son fonctionnement (décloisonnement, agilité), ainsi que d'optimisation de ses coûts. La numérisation de l'administration, enfin, pose un certain nombre de questions juridiques complexes et son développement n'est pas spécifique à la sphère française, ni ne se réduit au périmètre de l'Etat. Ses enjeux tant territoriaux qu'européens, notamment, sont importants.

Les premiers services télématiques voient le jour à la fin des années 1980 grâce au Minitel et les administrations participent au développement d'Internet dès la seconde moitié des années 1990. Mais ce n'est qu'à partir de 1997 que l'administration électronique émerge progressivement en tant que politique publique à part entière et que s'élabore une stratégie globale, nourrie par plusieurs rapports et qui se concrétisera dans un ensemble de programmes : Programme d'action gouvernemental pour la société de l'information (PAGSI) en 1998, Projet ADELE (Administration électronique) pour la période 2004-2007. Plus récemment, la transition numérique est devenue un axe central de la politique de réforme de l'Etat, que ce soit avec la Révision générale des politiques publiques (RGPP), la Modernisation de l'action publique (MAP) et le programme Action publique 2022. Outre la question de la numérisation des services publics, celle du pilotage et de la transformation du système d'information de l'Etat et celle de « l'Etat plateforme » s'imposent comme des enjeux clé.

En matière de services aux usagers, on peut distinguer deux grandes étapes dans l'utilisation des TIC: la première consiste à mettre des informations à disposition des citoyens afin de simplifier leurs démarches administratives ; la seconde, qui va plus loin, permet aux usagers de réaliser directement leurs démarches en ligne. On parle alors de téléservices. Se posent néanmoins, dans le développement de ces services numériques, la question de leur accessibilité (couverture Internet des zones rurales, déploiement du haut et du très haut débit, publics en situation de fragilité…), ainsi que des contraintes juridiques fortes en matière de protection des données personnelles et des libertés individuelles. Ces enjeux juridiques prennent une acuité particulière depuis que le droit européen a consacré un principe de réutilisation des données publiques et que l'Open data, qui apparaît comme emblématique d'une

troisième étape – le passage d'une logique de mise à disposition de services publics à une logique de participation, voire de co-création où l'usager devient pleinement partie prenante, grâce, notamment, aux technologies du Web 2.0 – est l'une des priorités de la politique de transition numérique.

Enfin, le développement du numérique dans l'administration s'inscrit dans une perspective de maîtrise des dépenses publiques (une procédure électronique ayant un coût de traitement estimé cent fois plus faible que celui d'une procédure papier) et peut favoriser l'émergence d'un nouveau mode de management (moins autoritaire, plus horizontal), alors que la « politique de la donnée » doit générer une meilleure circulation et valorisation de l'information propice au décloisonnement et gage d'efficience. Mais cette transformation implique une adaptation des agents et des processus et nécessite des investissements financiers préalables (accessibilité et ergonomie des outils, interopérabilité des systèmes d'information, harmonisation du traitement des données, respect de leur sécurité et de leur confidentialité…) avant de devenir source d'économies.

LE FIGARO

Cyberattaques : 62% des Français n'ont jamais reçu une formation à la sécurité informatique

Par Klara Durand
Le 25/10/2022

Selon une étude dans plusieurs pays par Ipsos et l'entreprise Terranova Security, la France est en retard et manque encore d'une « cyber culture » pour se prémunir des attaques informatiques.

« *76% des salariés de France, du Royaume-Uni, du Canada, d'Australie et des États-Unis, déclarent avoir été personnellement visés par une cyberattaque ou connaître quelqu'un qui l'a été* », révèle une nouvelle étude, publiée ce mardi 25 octobre, conduite par l'entreprise de sondages française Ipsos et le fournisseur de formations informatiques, Terranova Security.

L'enquête a été menée à l'été 2022 auprès de 4000 individus âgés de 18 à 75 ans. «*L'objectif était de mesurer le niveau de sensibilisation des répondants aux enjeux de cybersécurité* », explique Anselme Laubier, Directeur d'études chez Ipsos.

La France en retard sur les formations

La France affiche un certain retard. Selon l'étude, « *62% des Français n'ont jamais reçu une formation à la cybersécurité* », contre 47% en moyenne pour l'ensemble des pays interrogés. Seuls 25% des salariés français ont reçu une formation qui était obligatoire. Une différence qui peut s'expliquer par la part du télétravail. Cette pratique demeure moindre dans le pays, avec 44% des salariés français qui disent télétravailler contre 54% pour l'ensemble des cinq pays interrogés.

Par ailleurs, la France « *peine encore à considérer l'investissement dans la cybersécurité comme une épargne plutôt que comme un coût* », souligne Jean-Jacques Ibrahim, Responsable de la sécurité des systèmes informatiques (RSSI) pour l'entreprise Lutessa. D'autant que le Sénat a autorisé les assurances à indemniser les victimes de cyberançons (ou *ransomware* en anglais), en adoptant le 12 octobre dernier la disposition prévue à l'article 4 du projet de loi d'orientation et de programmation du ministère de l'Intérieur (LOPMI). Le texte prévoit qu'une organisation victime pourra, si elle a souscrit une assurance, se faire rembourser la rançon à la condition qu'elle dépose plainte à la police. Une protection nécessaire mais qui peut « *retarder la prise de conscience des entreprises sur le besoin de formations en matière de cybersécurité*», s'interroge Terranova Security.

Développer une culture de la cybersécurité

Or, pour remédier à ces failles, il est nécessaire de « *développer une culture de la cybersécurité à l'échelle globale* », estime Jean-Jacques Ibrahim. En effet, l'enquête souligne un paradoxe : dans les cinq pays, 78% des salariés se disent inquiets par cette menace tout en considérant que c'est au département informatique de leur entreprise de garantir cette sécurité.

Afin d'opérer un changement de mentalité, Ipsos et Terra Nova proposent dans leur étude des pistes de réflexions. Notamment, développer de bonnes pratiques le plus tôt possible. Elle prend pour exemple l'usage d'un mot de passe différent pour chaque compte, ce que seulement 50% des salariés font au travail, indique l'enquête.

De bonnes pratiques qui doivent s'accompagner « *d'un tronc commun de sensibilisation dans les entreprises* », déclare Jean-Jacques Ibrahim et d'une « *généralisation de la communication*» sur les bons réflexes à avoir. Un enjeu qui demeure « *majeur* », conclut le RSSI. En 2021, l'autorité nationale en matière de sécurité et de défense des systèmes d'information (ANSSI) relevait 1082 intrusions avérées dans des systèmes d'information. Une hausse de 37% par rapport à 2020.

Le Monde

« La cyberdéfense de la France a besoin de moyens humains et technologiques »

Le 19 Décembre 2022

Le chercheur Alexandre Papaemmanuel et le sénateur (LR) Cédric Perrin appellent, dans une tribune au « Monde », à accorder les financements nécessaires au commandement de la cyberdéfense pour lui permettre de remplir ses missions.

Le 24 février, quelques heures avant le début de l'invasion russe en Ukraine, une cyberattaque a paralysé un fournisseur américain de communications par satellite utilisé par l'armée ukrainienne. D'aucuns ont alors prédit le début d'une vague d'attaques visant à démanteler des secteurs-clés de l'Ukraine. Mais la cyberblitzkrieg n'a pas eu lieu. La ligne de défense ukrainienne, disposant de ressources humaines compétentes, d'outils performants et s'appuyant sur des partenariats solides, avec des pays tiers comme avec le secteur privé, a réussi à stopper les cyberattaques russes.

Ce combat héroïque des Ukrainiens nous oblige à porter un regard sur l'évolution de la conflictualité numérique. En effet, l'association entre la préparation, la force morale et la combinaison du numérique et du cinétique ont pris à rebours les nombreux analystes qui prédisaient une défaite rapide de l'Ukraine. Autant de pistes devant guider la France dans les prochains débats autour de la future loi de programmation militaire (LPM) 2024-2030 et, en particulier, sur l'effort budgétaire à fournir au profit d'un commandement de la cyberdéfense (Comcyber), acteur de la résilience nationale.

Depuis dix ans, la France a intégré la cybersécurité dans le concept de sécurité nationale. Cette ambition est devenue récemment un objectif stratégique pour disposer d'*« une résilience cyber de premier rang ».* Des défis de taille en découlent pour nos militaires en termes de fidélisation de ressources humaines, d'intégration des effets cyber aux opérations et de gestion des partenariats publics et privés.

Comcyber est un employeur attractif, malgré un marché du travail où la ressource est rare, donc précieuse. Si le défi réside dans la fidélisation d'une ressource convoitée par le privé, qui offre des niveaux de rémunération plus attractifs, les armées doivent monter en puissance afin de faire face à une menace chaque jour grandissante. La prochaine LPM doit confirmer l'objectif stratégique de résilience par une augmentation des ressources humaines du Comcyber. Cette masse est indispensable pour disposer d'une capacité à se défendre et à agir sur les champs hybrides.

Le Comcyber – émanation des armées et non cyberarmée – doit répondre aux besoins opérationnels pour conduire des opérations militaires, y compris de haute intensité, dans tous les champs. Ainsi le concept de multimilieux (terre, mer, air auxquels on peut ajouter l'espace exo-atmosphérique et le cyber) et de multichamps (informationnel et électromagnétique) pose le Comcyber comme un acteur aux carrefours de l'action opérationnelle aussi bien dans la conception, la planification et la conduite des opérations militaires de cyberdéfense. La LPM devra donc offrir une panoplie de capacités techniques spécifiques en complément des capacités des armées.

Outil de diplomatie militaire

La mise en réseau du monde induit qu'une attaque cyber sur l'Ukraine se propage viralement à l'ensemble du globe. Détecter en amont les signaux faibles permet d'anticiper le blizzard de cyberattaques accompagnant une infiltration d'un centre hospitalier ou d'un réseau électrique. Dans une logique de réassurance, les armées doivent plus que jamais se déployer à proximité de nos alliés et partenaires pour découvrir l'infiltration de p irates informatiques dans leurs systèmes. Le hunt forward – la « chasse cyber aux avant-postes » – invite à parcourir en profondeur les réseaux informatiques des pays partenaires à la recherche de signes de pénétration. Le Comcyber peut ainsi contribuer à la diplomatie française tout en étendant la protection de nos systèmes numériques.

La LPM devra renforcer les capacités d'animation des politiques nationale et internationale de cyberdéfense, notamment dans l'élaboration et la mise en oeuvre des plans de coopération. Cet outil de diplomatie militaire numérique placera la France au rang des partenaires lucides à haute valeur ajoutée. Le retour d'expérience de la guerre qui se joue actuellement aux frontières de l'Europe souligne l'importance d'une défense nationale et européenne numérique. Si le cyber n'est pas une arme suffisante pour gagner la guerre, elle constitue en revanche une capacité indispensable pour conserver l'initiative et l'avance sur l'ennemi. La devise du Comcyber est « Per Aether Pugnamus » : « à travers l'éther, nous menons le combat ». Bien qu'immatériel, ce combat a besoin de moyens humains et technologiques pour faire face : la prochaine LPM devra en être l'incarnation.

Alexandre Papaemmanuel est spécialiste des questions numérique et cyber, enseignant à Sciences Po Paris et administrateur du fond Defense Angels.

Cédric Perrin est sénateur (LR) du Territoire de Belfort et vicepresident de la Commission des affaires étrangères, de la défense et des forces armées.

ANSSI | Agence nationale de la sécurité des systèmes d'information

Document 9 : 1/1

ACTUALITÉS

CYBERSÉCURITÉ : PROTÉGER LES SERVICES PUBLICS ET LES COLLECTIVITÉS TERRITORIALES AVEC FRANCE RELANCE

Dans le cadre du plan France Relance, l'ANSSI bénéficie d'une enveloppe de 136 millions d'euros pour renforcer la cybersécurité de l'État et des territoires sur la période 2021-2022. L'objectif est d'élever durablement le niveau de cybersécurité de l'État, des collectivités, des établissements de santé et des organisations au service des citoyens, tout en développant le tissu industriel français de cybersécurité.

LES OFFRES DE SERVICE

L'ANSSI propose aux acteurs publics volontaires plusieurs offres de service :

- un dispositif de sécurisation visant à cofinancer des **projets** et des **Parcours de cybersécurité** de systèmes d'information existants ;
- un accompagnement financier et méthodologique à la création de **centres régionaux de réponse à des incidents cyber** (CSIRT).

La démarche de l'ANSSI est d'élever significativement et durablement le niveau de cybersécurité des bénéficiaires en leur donnant l'impulsion financière nécessaire en vue d'un investissement durable.

LES BENEFICIAIRES

Le budget de 136 millions d'euros sera réparti au profit de différentes priorités :

- 60 M€ au profit des collectivités territoriales, via des parcours de cybersécurité, le co-financement de projets et le soutien à la création des CSIRT régionaux ;
- 25 M€ au profit du secteur de la santé pour la sécurisation des établissements de santé, du ministère et des organismes qui en dépendent
- 30 M€ au profit des ministères et organismes qui en dépendent, hors secteur de la santé, notamment via le co-financement de projets de sécurisation des réseaux de l'État ;
- 21M€ pour le développement et le déploiement mutualisé des capacités nationales de cybersécurité.

Le volet cybersécurité de France Relance se fonde sur l'implication et le volontariat de ses bénéficiaires, et leur capacité à poursuivre les actions dans la durée. Il donne accès à chaque acteur à un accompagnement adapté à son niveau de maturité.

« *Il est plus que jamais urgent d'agir concrètement et collectivement en matière de sécurité numérique. Le plan France Relance est une belle opportunité pour changer la donne, pour donner une impulsion nouvelle là où c'est nécessaire, pour protéger durablement et au juste niveau ce qui doit l'être. L'État, les collectivités territoriales, les établissements de santé, les organismes au service des citoyens sont autant d'acteurs qui pourront en bénéficier avec l'aide de l'ANSSI* » explique Guillaume Poupard, directeur général de l'ANSSI.

CANDIDATURE

Découvrez les offres et les modalités pour en bénéficier sur la rubrique France Relance.

Tout savoir sur le volet cybersécurité de France Relance

Bpifrance et Cybermalveillance.gouv.fr se mobilisent pour accompagner les entreprises face au risque croissant de cyberattaques et publient un guide dédié aux PME et TPE

20 mai 2021

Bpifrance partenaire des entreprises et Cybermalveillance.gouv.fr, groupement d'intérêt public qui assiste les victimes de cyberattaques ont uni leurs efforts afin d'élaborer un guide pratique adapté aux entrepreneurs afin de leur donner les clefs pour se prémunir du risque de cyberattaques et les aider à savoir y faire face.

LA CYBERSECURITE, UN ENJEU MAJEUR POUR LES ENTREPRISES

Les entreprises françaises font face à une recrudescence majeure de cyberattaques qui frappent aussi bien les grands groupes que les TPE. En 2020, ce sont plus de 10 000 entreprises qui sont venues chercher de l'assistance suite à une cyberattaque sur la plateforme Cybermalveillance.gouv.fr. Lorsqu'elles sont insuffisamment préparées, les PME sont particulièrement vulnérables et les conséquences sont souvent dramatiques. Le retard dans la mise à niveau des équipements informatiques, le recours massif au télétravail et la numérisation croissante ont contribué à augmenter leur exposition au risque cyber.

Les entreprises font face aux attaques de réseaux de cybercriminels et mafieux de plus en plus structurés dont les motivations sont diverses, allant de l'appât du gain aux revendications idéologiques. Pour les victimes, les cyberattaques se soldent très souvent par une demande de rançon, un vol de données sensibles ou encore une indisponibilité des équipements. La reprise d'activité, lorsqu'elle est possible, est souvent longue à mettre entre œuvre, coûteuse et très éprouvante pour les dirigeants et leurs collaborateurs.

UN GUIDE PRATIQUE ADAPTE AUX ENTREPRISES

Il existe pourtant des mesures simples et peu onéreuses qui permettent de se prémunir efficacement d'une grande partie du risque cyber. À cet effet, Cybermalveillance.gouv.fr et Bpifrance publient ce guide de sensibilisation qui regroupe l'essentiel des bonnes pratiques de cybersécurité à destination des dirigeants et de leurs collaborateurs. À partir de ses conseils simples, il permet de développer une véritable culture de la cyber hygiène au sein d'une entreprise et de mettre en place des mesures visant à renforcer la cyber résilience de l'organisation en cas d'attaque. La prise en considération du risque par la direction et la sensibilisation des collaborateurs sont des composantes tout aussi essentielles à mettre en oeuvre que les mesures techniques.

Dans ce guide pratique et pédagogique figurent les recommandations concrètes d'experts en cybersécurité, des témoignages d'entrepreneurs et des récits de victimes de cyberattaques, une présentation détaillée des principales attaques et de leurs caractéristiques, ainsi qu'un plan d'action à activer en cas de cyberattaque décrivant les étapes importantes pour reprendre l'activité.

Pour **Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr**, « L'actualité démontre quotidiennement que les entreprises, quelle qu'en soit la taille ou le secteur d'activité, sont victimes d'une cybermalveillance qui ne cesse de s'intensifier de pair avec le développement des usages numériques. Elles doivent donc prendre conscience du risque et se préparer à l'affronter. Ce guide qui vient compléter l'offre d'assistance de Cybermalveillance.gouv.fr a pour objet de les y aider. »

Pour **Pascal Lagarde,** Directeur exécutif en charge de l'International, de la Stratégie, des Études et du Développement de Bpifrance, « Jusqu'alors les entreprises restaient vulnérables face à des cybercriminels très bien préparés et organisés, notamment les PME qui disposent de moyens limités pour faire face à ces attaques. Nous sommes à leurs côtés pour les accompagner au travers d'outils simples et faciles d'accès qui leur permettront de s'armer et de renforcer leur niveau de maturité en cybersécurité. »

UNE PALETTE D'OUTILS COMPLEMENTAIRES POUR RENFORCER LA CYBERSECURITE DES ENTREPRISES ET LES ACCOMPAGNER DANS LE PASSAGE A L'ACTION

- Bpifrance met à disposition des dirigeants un outil d'autodiagnostic en ligne pour leur permettre d'évaluer le niveau de maturité de leur entreprise pour leur cybersécurité. Simple et pédagogique, il leur permet en 15 minutes, à travers une quarantaine de questions, d'établir un diagnostic de leur entreprise et d'accéder à de nombreuses ressources en ligne. Il est accessible gratuitement après inscription sur https://Mon.Bpifrance.fr. L'accès se fait ensuite via Mon Bpifrance ou sur https://diagcybersecurite. bpifrance.fr.

- Bpifrance organise une série de webinaires sur le thème de la cybersécurité : « Cyberattaques : Anticiper et déjouer les ruses », « Réagir face à une cyberattaques ». À la lumière des conseils d'experts en cybersécurité et de témoignages de dirigeants d'entreprises victimes de cyberattaques, ces séances permettent d'appréhender les enjeux cyber dans un cadre interactif. Cette plateforme propose également d'autres contenus en lien avec la cybersécurité (modules de e-learning et digital guide par exemple) accessibles gratuitement à l'adresse suivante : https://www.bpifranceuniversite. fr/formations/transformation-digitale/e-parcours-cybersecurite.

- Cybermalveillance.gouv.fr propose gratuitement sur son site de nombreux contenus d'actualité et de prévention pour permettre aux différents publics de comprendre la réalité de la cybermalveillance ainsi que les mesures à appliquer pour s'en prémunir. Les victimes peuvent également réaliser sur la plateforme un diagnostic en ligne de leur situation, obtenir les conseils et orientations nécessaires pour y faire face et au besoin être mis en relation avec des prestataires spécialisés en mesure de leur apporter l'assistance nécessaire. Services disponibles sur : https://www.cybermalveillance.gouv.fr/

- En partenariat avec l'AFNOR et les organisations professionnelles, Cybermalveillance.gouv.fr a développé le label ExpertCyber qui certifie et reconnaît les compétences des professionnels en sécurité numérique dans l'accompagnement de leurs clients pour la sécurisation de leurs systèmes d'information ainsi que la remédiation de leurs incidents de sécurité. Pour en savoir plus, rendez-vous sur https://www.cybermalveillance.gouv.fr/tous-nos-contenus/labelexpertcyber/ decouvrir-le-label-expertcyber.

À propos de Bpifrance

Bpifrance finance les entreprises – à chaque étape de leur développement – en crédit, en garantie et en fonds propres. Bpifrance les accompagne dans leurs projets d'innovation et à l'international. Bpifrance assure aussi, désormais leur activité export à travers une large gamme de produits. Conseil, université, mise en réseau et programme d'accélération à destination des startups, des PME et des ETI font également partie de l'offre proposée aux entrepreneurs. Grâce à Bpifrance et ses 50 implantations régionales, les entrepreneurs bénéficient d'un interlocuteur proche, unique et efficace pour les accompagner à faire face à leurs défis.

À propos de la Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes d'actes de cybermalveillance, de sensibilisation aux risques numériques et d'observation de la menace sur le territoire français. Ses publics sont les particuliers, les entreprises (hors OIV et OSE), les associations et les collectivités territoriales. Le dispositif est piloté par le Groupement d'intérêt public (GIP) ACYMA, composé d'une cinquantaine de membres issus du secteur public, du privé et du domaine associatif, qui contribuent à sa mission d'intérêt général. Cybermalveillance.gouv.fr référence sur sa plateforme des professionnels en sécurité numérique, répartis sur tout le territoire français, pour venir en aide aux victimes

E-administration : du PAGSI au programme Action publique 2022

Le 4 octobre 2021

La transformation numérique de l'État est continue depuis plus de 20 ans. Grâce à l'évolution des technologies, de nombreux services dématérialisés ont été créés (téléservices, simulateurs, etc.). Aujourd'hui, le numérique est devenu le premier canal d'accès aux services publics.

Le programme Action publique 2022, lancé par le gouvernement fin 2017, constitue une nouvelle étape de la transformation numérique des administrations. Les 250 démarches les plus courantes doivent être dématérialisées d'ici mai 2022. Une administration plus proactive (échanges de données entre administrations, information des citoyens ...), l'ouverture des données publiques et les projets d'intelligence artificielle sont encouragés afin d'offrir de nouveaux services.

Une e-administration en constant développement depuis 20 ans

La période 1998-2007

Depuis 1998, les pouvoirs publics ont élaboré plusieurs programmes ou plans en vue de développer l'administration électronique. Ce mouvement débute avec le programme d'action gouvernemental pour la société de l'information (PAGSI). Il débouche notamment sur l'adoption par les ministères de programmes pluriannuels de modernisation (PPM) et sur la création en 2000 du portail de l'administration, Service-public.fr.

La politique poursuivie vise à faire de l'État un acteur exemplaire et un accélérateur, plus transparent et plus efficace, en facilitant la diffusion en ligne des informations publiques essentielles et en généralisant les téléprocédures. Il s'agit de mettre en place "une administration à accès pluriel" pour les usagers (guichets physiques, courriers, services en ligne ou téléphonie). Ce mouvement de modernisation se poursuit avec le plan ADministration ÉLEctronique (ADELE) sur la période 2004-2007. La finalité de ce plan, doté d'un budget de 1,8 milliard d'euros, est de faire de l'administration électronique un levier de la modernisation de l'État.

Le plan prévoit 140 mesures (https://www.fonctionpublique.gouv.fr/files/files/IMG/pdf/projet_ADELE.pdf) afin que l'ensemble des démarches administratives puissent être accomplies à distance par téléphone ou par internet à l'horizon 2006. L'agence pour le développement de l'administration électronique (ADAE), créée en 2003 auprès du Premier ministre, assure la mise en oeuvre du plan.

La période 2008-2018

En 2008, le plan "France numérique 2012" prend le relais d'ADELE. Il a notamment pour but d'accroître l'accessibilité des sites Internet publics, de développer le paiement en ligne, d'améliorer l'interopérabilité entre administrations et d'ouvrir les données publiques (open data). Selon un bilan présenté en novembre 2011 par le gouvernement, le plan "France numérique 2012" a permis la dématérialisation de 76% des procédures les plus attendues par les usagers. Un référentiel général d'interopérabilité (RGI) est publié en 2009 et valorise les standards ouverts. Quant à la politique d'ouverture des données, elle se concrétise par la création fin 2011 de la plateforme de données publiques, data.gouv.fr (https://www.data.gouv.fr/fr/) , développée par la mission Etalab. Cette structure, placée sous l'autorité du Premier ministre, est également née en 2011.

En 2012, le Secrétariat général à la modernisation de l'action publique (SGMAP) est institué.

Il est chargé de mettre en oeuvre la politique de modernisation de l'État, notamment en matière numérique. Des comités interministériels de la modernisation de l'action publique (CIMAP) décident des actions à engager, conformément au "choc de simplification" annoncé par le président de la République en mars 2013.

Une nouvelle stratégie technologique de l'État est mise en place via le réseau interministériel de l'État (RIE) et le projet dit de "l'État plateforme". Un décret du 1er août 2014 place les différents systèmes d'information (SI) ministériels sous la gouvernance du Premier ministre en créant un système d'information unifié de l'État (socle matériel et logiciel commun).

La même année, le gouvernement présente un projet pour faire du numérique l'instrument de la transformation de l'État. 40 nouvelles mesures de simplification des démarches administratives pour les particuliers sont annoncées (https://www.gouvernement.fr/conseildes- ministres/2014-11-05/la-simplification-pour-les-particuliers) . La majorité correspond à la création par les ministères de nouveaux services numériques (par exemple simulateur pour estimer ses droits aux prestations sociales). Un administrateur général des données (https://www.legifrance.gouv.fr/eli/decret/2014/9/16/PRMX1421510D/jo/texte) est nommé pour animer et impulser la politique d'open data au sein des administrations de l'État.

Fin 2015, les usagers se voient proposer un nouveau service numérique : celui de saisir par voie électronique (SVE) - dans les mêmes conditions qu'une saisine postale – les administrations d'État pour près de neuf démarches administratives sur dix. Cette saisine peut être effectuée par le biais d'une téléprocédure, d'un formulaire de contact ou par courriel.

En 2016, France Connect (https://franceconnect.gouv.fr/) est déployé. Cet outil permet d'utiliser un compte, un identifiant et un mot de passe uniques pour tous les services publics en ligne (impôts, caisse d'allocations familiales, mairie, etc.). La refonte du site Servicepublic. fr (https://www.service-public.fr/) a également lieu. 2016 est aussi marquée par la publication de la loi pour une République numérique, dite loi "Lemaire". Elle impose notamment aux administrations d'ouvrir leurs données publiques par défaut, y compris leurs algorithmes, de plus en plus fréquents dans les décisions administratives (par exemple pour le calcul de l'impôt). La loi crée, en outre, un service public de la donnée.

En 2017, le plan "Préfectures nouvelle génération" (PPNG) est mis en oeuvre. Les procédures de délivrance des titres (demande de permis de conduire ou de carte grise, pré-demande de passeport ou carte d'identité) sont dématérialisées. La réforme repose sur l'Agence nationale des titres sécurisés (ANTS) et les nouveaux centres d'expertise et de ressources des titres (CERT) répartis sur tout le territoire. La mise en place de la téléprocédure pour obtenir sa carte grise a cependant rencontré de nombreuses difficultés qui ont provoqué d'importants retards dans la délivrance des titres.

Pour concevoir des services publics innovants dans des délais courts, des "startups d'État" au sein du SGMAP se multiplient, des "entrepreneurs d'intérêt général" (EIG) (https://entrepreneur-interet-general.etalab.gouv.fr/index.html) sont recrutés pour dix mois dans les administrations. Des hackathons sur deux jours regroupant des développeurs, chefs de projets, etc., des administrations de l'État sont aussi organisés.

D'après l'indice relatif à l'économie et à la société numériques (DESI, pour Digital Economy and Society Index) (http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52349) publié par la Commission européenne en mai 2018, la France était à la 13e place européenne en matière de services publics numériques. Elle disposait d'une note moyenne en ce qui concerne l'étendue des services en ligne (87

contre 84 pour la moyenne européenne). En revanche, elle était en avance en matière de données ouvertes (4e place en Europe).

La transformation numérique de l'Etat dans le cadre d'Action publique 2022

Le programme Action publique 2022, programme de réforme de l'État lancé par le gouvernement en octobre 2017, reprend pour priorité la transformation numérique des administrations. Ce programme est piloté par la direction interministérielle du numérique (https://www.numerique.gouv.fr/dinum/) (DINUM), service du Premier ministre, et par la direction interministérielle de la transformation publique (https://www.modernisation.gouv.fr/qui-sommes-nous) (DITP), rattachée au ministère de la transformation et de la fonction publiques.

Améliorer la qualité des services publics par l'innovation numérique

La transformation numérique est l'un des cinq chantiers transverses d'Action publique 2022. Six comités interministériels de la transformation publique (CITP), qui se sont tenus depuis février 2018, en ont détaillé le programme. Le gouvernement entend tirer parti de la révolution numérique (intelligence artificielle - IA-, open data, etc.) pour offrir des services innovants, tout en réduisant les coûts.

Parmi les diverses réformes mises en oeuvre figurent :

- de nouveaux services en ligne (création d'un code du travail numérique (https://code.travail.gouv.fr/) ...)
- un guichet unique internet des formalités pour les entreprises (https://www.guichetentreprises.fr/fr/) , confié à l'Institut national de la propriété intellectuelle (INPI) ;
- "France Expérimentation" (https://www.modernisation.gouv.fr/transformer-lactionpublique/france-experimentation-entreprises) , un dispositif facilitant la mise en œuvre du droit à l'expérimentation pour les entreprises porteuses de projets innovants ;
- la mise en place d'un bouton "je donne mon avis" à la fin des démarches administratives en ligne ;
- un observatoire de la qualité des démarches en ligne (https://observatoire.numerique.gouv.fr/) créé en juin 2019, qui permet de suivre l'avancée et la qualité de la dématérialisation, selon huit critères de qualité ;
- le lancement en janvier 2021 du programme Services publics + (https://www.modernisation.gouv.fr/ameliorer-lexperience-usagers/services-publics) pour améliorer l'efficacité des services publics en continu ;
- des plans de transformation numérique dans chaque ministère ;
- un laboratoire pour l'intelligence artificielle (Lab IA) interministériel (https://www.etalab.gouv.fr/datasciences-et-intelligence-artificielle) pour accompagner les administrations dans le déploiement de leurs projets d'IA et anticiper les effets de l'IA sur les métiers et la relation aux usagers.

D'autres mesures sont encore annoncées comme :

- la simplification d'ici janvier 2022 de dix démarches emblématiques (dématérialisationde la demande de permis de construire...) et des 100 formulaires les plus utilisés par lesusagers ;

- la dématérialisation d'ici mai 2022 des 250 démarches administratives les plus utilisées par les Français. L'objectif initial fixé par le gouvernement en 2017 de 100% des démarches dématérialisées à l'horizon 2022 a été recentré en 2019 sur ces 250 démarches ;
- un partage des données des usagers entre administrations par défaut (selon le principe "dites-le-nous une fois ") ;
- l'accélération du chantier FranceConnect avec pour objectif 30 millions d'utilisateurs fin 2022 (contre 500 000 début 2017 et 20 millions en 2021) ;
- la simplification de la demande de subvention des associations, en allant vers le modèle d'un guichet unique ;
- l'accélération de la numérisation des processus internes à l'administration, avec l'objectif d'une administration "zéro papier" (https://www.modernisation.gouv.fr/outilset-formations/objectif-0-papier-un-guide-pour-simplifier-et-dematerialiser-vos-processus) afin de simplifier et fluidifier le travail et les circuits de décision ;
- une administration proactive et plus proche, qui anticipe les besoins des usagers afin de lutter contre les non-recours et simplifier l'accès aux démarches ;
- une politique des données publiques plus ambitieuse. La politique de la donnée devient une priorité stratégique de l'État (circulaire du Premier ministre du 27 avril 2021 (https://www.legifrance.gouv.fr/download/pdf/circ?id=45162) qui fait suite au rapport Bothorel remis en décembre 2020). Chaque ministère doit élaborer une feuille de route et désigner un administrateur des données, des algorithmes et des codes sources. Un plan d'actions dédié à l'animation et à la promotion interministérielle du logiciel libre et des communs va être lancé. 15 feuilles de route ministérielles des données, algorithmes et codes sources ont été rendues publiques (https://www.transformation.gouv.fr/laministre/actualite/le-gouvernement-poursuit-son-engagement-pour-une-politiqueambitieuse) le 27 septembre 2021 ;
- une nouvelle stratégie Cloud de l'État afin notamment que les données des usagers soient sécurisées et protégées ;
- un chantier de prospective sur le futur du numérique public à l'horizon 2030.

Les mesures d'accompagnement des agents prévues

Pour mettre en oeuvre la transformation des services publics, le gouvernement a prévu d'accompagner les agents publics.

De nombreux outils sont proposés par la DITP. Ainsi, démarches-simplifiées.fr (https://www.demarches-simplifiees.fr/administration) , offre aux administrations et agents qui ont besoin de dématérialiser des démarches des usagers un générateur de formulaires et une plateforme d'instruction de dossiers.

Un futur "sac à dos numérique de l'agent public" est en cours de conception. Il doit permettre aux agents de l'État de travailler à distance plus facilement et de façon plus sécurisée (visioconférence, messagerie instantanée...). La crise du Covid-19 a déjà fortement accéléré le télétravail. Pour assurer la continuité de l'administration numérique, l'État a dû équiper rapidement ses agents. Au 1er mars 2020, avant le premier confinement, seulement 22% d'entre eux disposait d'un ordinateur portable. Au 1er juillet 2021, ce pourcentage atteint 85%. Fin 2021, tous les personnels dont les fonctions sont télétravaillables devraient être équipés.

L'État souhaite également attirer les talents du numérique. Plusieurs plans ont été lancés. Le dernier date de mai 2021. Il vise à renforcer l'attractivité, la formation et les parcours de carrière dans la filière du numérique publique.

Les investissements dédiés

Outre les outils, des moyens financiers accompagnent la transformation des administrations.

Un fonds pour la transformation de l'action publique (https://www.modernisation.gouv.fr/transformer-laction-publique/fonds-pour-latransformation-publique) , au titre du Grand plan d'investissement 2018-2022, a ainsi été créé. Il est doté de 700 millions d'euros sur cinq ans pour accompagner les administrations centrales et déconcentrées dans leurs projets de transformation et de simplification.

Plus récemment, dans le cadre du plan de relance, une enveloppe d'un milliard d'euros est consacrée à la transformation numérique de l'État. Dans le plan, un fonds d'innovation et de transformation numérique (FITN) est doté de 292 millions d'euros. Un guichet unique (https://france-relance.transformation.gouv.fr/) permettant aux administrations de déposer leurs projets a été mis en place.

Cybersécurité, résilience et souveraineté dans les collectivités territoriales

Frédéric Pointu – Cyril Bras

Auditeur de la 3e session nationale « Cybersécurité et souveraineté numérique » de l'IHEDN. Responsable « Sécurité des systèmes d'information en collectivité territoriale ».

Auditeur de la 2e session nationale « Cybersécurité et souveraineté numérique » de l'IHEDN. Directeur « Cybersécurité » de Whaller et vice-président de l'Institut national pour la cybersécurité et la résilience dans les territoires (INCR).

Relativement épargnées il y a encore quelques années, les collectivités territoriales sont depuis 2020 [1] fortement impactées par l'augmentation mondiale du nombre de cyberattaques. Ainsi, la fréquence et les conséquences des attaques sur ces types de cibles sont maintenant en forte augmentation : elles peuvent se traduire par un « simple » défacement [2] de site *Internet* ou générer une incapacité à assurer les missions de service public qui sont de la compétence des collectivités, et cette tendance devrait vraisemblablement aller en s'amplifiant au cours des années à venir.

Pourquoi cette situation ?

Une prolifération de la menace cyber

Le nombre de cyberattaques mondiales, tous type et nationalité de cibles confondus, a augmenté au cours des cinq dernières années de manière importante [3]. Il est donc mécaniquement normal que le nombre de collectivités touchées augmente. La relative médiatisation de ces attaques les rend également plus visibles, notamment du grand public. Par ailleurs, en quelques années, les objectifs et la nature même des attaquants ont évolué. Ces derniers ont vraisemblablement progressé vers la professionnalisation de leurs activités et se sont orientés vers la rentabilité. Ainsi, il est maintenant quasiment systématique de voir une attaque associée à une demande de rançon et un chantage à la divulgation.

(1) « Cybermoi/s 2020 : un mois pour se protéger du chantage numérique », ANSSI, 1er octobre 2020 (www.ssi.gouv.fr/).

(2) Défacement : lorsque des pirates informatiques remplacent une page *Internet* légitime par une autre réalisée par leurs soins et pouvant porter des messages de revendications.

(3) Valéry Rieß-Marchive : « *Ransomware* : la transparence toujours relative des collectivités territoriales », *LeMagIT*, 29 septembre 2022 (www.lemagit.fr/).

Une prise de conscience progressive des enjeux de la sécurité numérique au sein des collectivités

Du fait de cette évolution récente du nombre d'attaques et des objectifs des pirates, les collectivités sont probablement majoritairement encore peu conscientes de l'ampleur réelle de la menace et de ce fait peu sensibles au sujet. Malheureusement, la cybersécurité reste trop souvent perçue comme exclusivement technique et ainsi logiquement traitée par la seule Direction des systèmes d'information (DSI). Au sein de cette dernière, ce sujet reste secondaire face aux contraintes de production et également perçu en premier lieu comme un centre de coût. Une autre illustration de l'immaturité dans l'appropriation du caractère stratégique de la cybersécurité, se retrouve dans le positionnement du responsable de la sécurité des systèmes d'information (RSSI) au sein de l'organigramme des collectivités, qui reste encore fréquemment rattaché à la DSI. *A contrario*, une évolution se fait jour dans les secteurs qui ont perçu ces enjeux et qui décident alors de rattacher directement le poste au comité de direction ou de créer un poste de directeur de la sécurité des systèmes d'information.

Peut-être faudrait-il encadrer par voie réglementaire le rôle de RSSI dans les collectivités territoriales sur un modèle équivalent à celui des délégués à la protection des données (DPD, *DPO : Data Protection Officer*) voulu par le règlement général pour la protection des données (RGPD).

Le manque de ressources financières et la rigidité administrative freinent le recrutement d'experts compétents

Outre la question de la bonne évaluation de la menace, les aspects financiers liés à la cybersécurité sont un frein à une généralisation de sa prise en compte au bon niveau au sein des collectivités territoriales. Ainsi, les communes, les groupements de communes et les syndicats représentent un peu plus de 45 000 collectivités en France en 2021 [4]. Parmi ces dernières, seuls les établissements les plus importants ont la capacité financière de recruter et d'embaucher le personnel spécialisé indispensable à un niveau de protection suffisant. Les plus petites structures ne comptent souvent qu'un, voire aucun informaticien. Il n'est pas rare que le secrétaire de mairie fasse office d'informaticien. Cette situation est si banale que le Groupement d'intérêt public, Action contre la cybermalveillance (GIP ACYMA) [5], a produit une série de *spots* de sensibilisation dans lesquels le jardinier, le neveu ou une voyante sont appelés par le maire d'une commune fictive pour traiter un problème de cybersécurité [6]. Comment ces personnes pourraient-elles réagir face à une demande de rançon qui apparaît à l'écran et qui vient d'effacer

[4] « Les collectivités locales en chiffres 2021 » (www.collectivites-locales.gouv.fr/).

[5] « Assistance et prévention du risque numérique au service des publics » (https://cybermalveillance.gouv.fr).

[6] *Kit* de communication de la campagne « Face aux risques cyber, faites confiance à un véritable expert », 17 novembre 2021 (www.cybermalveillance.gouv.fr/t).

l'ensemble de la mémoire numérique de la commune ? Pourtant, pour beaucoup, voire la plupart des petites collectivités, le recrutement d'un expert est tout simplement illusoire compte tenu des tensions qui existent sur le marché.

La situation n'est pas forcément plus favorable pour les collectivités plus importantes qui, quand elles disposent d'un RSSI, auront des difficultés à le conserver compte tenu de l'absence de perspectives de carrière proposées, mais aussi d'une rémunération largement inférieure à celles du secteur privé [7].

Un autre frein à l'intégration rapide de compétences cyber dans la fonction publique peut être associé au mode de gestion intrinsèque des ressources humaines et à une vision en retard des évolutions du domaine numérique. Les procédures de recrutement et la rémunération associée, liées à une grille qui prend essentiellement en compte le diplôme et le nombre d'années d'expérience dans la fonction publique, découragent nombre de candidats. Les référentiels métiers du Centre national de la fonction publique territoriale (CNFPT), qui définissent le cadre d'emploi dans la fonction publique territoriale, devraient évoluer en s'appuyant par exemple sur le panorama des métiers de la SSI proposé par l'ANSSI [8].

Une piste peut être de favoriser la formation de nouveaux profils capables de travailler en cybersécurité dans les territoires [9] : former de futurs professionnels compétents, conscients des besoins et si possible motivés par l'intérêt général tout en améliorant l'emploi local. Une autre piste à considérer repose sur la mutualisation de la compétence SSI entre différentes collectivités.

Ces premiers constats pourraient à eux seuls expliquer le résultat suivant : en 2022, en France, les collectivités territoriales sont en moyenne mal protégées, avec des variations extrêmes entre celles qui peuvent se protéger et celles qui n'en ont pas les moyens. Cependant, outre ces causes internes, il existe des causes externes.

Une responsabilité des éditeurs de logiciels à destination des collectivités

Les domaines d'intervention des collectivités sont très vastes, mais restent propres à ces dernières. Pour poursuivre leur transformation numérique, elles doivent donc disposer de logiciels spécialisés. Ce contexte numérique particulier est aussi à l'origine de failles de sécurité. En effet, si certains éditeurs jouent le rôle de réels partenaires et participent à la montée en maturité des collectivités en matière de sécurité numérique, d'autres se montrent pour le moins négligents en la matière. Or, certains éditeurs sont devenus inévitables, car ils sont parvenus à acquérir une

[7] Véronique Loquet : « Enquête exclusive sur la rémunération des fonctions RSSI », *CESIN*, 7 octobre 2021 (www.cesin.fr/).
[8] « Panorama des métiers de la cybersécurité », ANSSI (www.ssi.gouv.fr/).
[9] « L'Institut national pour la cybersécurité des territoires et le Groupe AEN ont conclu un accord de partenariat visant à la mise en place du Bachelor "Cybersécurité des territoires" », *IN-CRT*, 15 avril 2021 (www.groupe-aen.info/).

position dominante sur le marché de niche que représentent les logiciels équipant les collectivités. Malheureusement, ces éditeurs ne prennent pas toujours correctement en compte la cybersécurité dans leurs produits. Il est fréquent de rencontrer des développements bâclés, négligeant l'emploi de protocoles élémentaires de sécurité et la mise en œuvre de bonnes pratiques conformes à l'état de l'art [10]. Certaines entreprises font par ailleurs abstraction de l'obligation de conseil dévolue aux professionnels. Ces dernières devraient donc être des actrices et partenaires de confiance pour la transformation numérique des collectivités. Comme évoqué *supra*, cette situation trouve une part d'explication dans le manque de compétence cyber des collectivités. En effet, pour bon nombre d'entre elles, les seules exigences déterminantes lors d'appels d'offres, concernent le coût des solutions. Les critères concernant des exigences de cybersécurité sont souvent secondaires et ne conduisant pas à écarter les solutions non conformes à l'état de l'art.

Du point de vue des éditeurs, se conformer aux règles d'hygiène numérique n'est pas une priorité, car cela engendre un surcoût de production pour des solutions qui sont de toute façon acquises en l'état.

Une solution possible serait de sensibiliser et de peser sur ces éditeurs et constructeurs pour les inciter ou les contraindre à prendre en compte la sécurité de l'information, afin de transformer un point faible actuel, qui emprisonne les collectivités dans les solutions mal sécurisées d'éditeurs non conscients du problème ou simplement cyniques, en un point fort qui favorisera la création de solutions sécurisées utilisées par tous. Les dispositions de la seconde version de la directive européenne *NIS* (*Network and Information Security*) pourraient aller dans ce sens.

Il serait également possible de systématiser la mise en commun des initiatives locales, financées par des fonds publics. Certaines collectivités ont ainsi fait le choix de partager le code des applications développées pour leur besoin. Par ailleurs, un groupe de collectivités a choisi de réaliser un *bug bounty* [11] sur une liste d'applications et de partager les retours avec les éditeurs à des fins d'amélioration, mais également avec d'autres collectivités à des fins de partage du niveau de sécurité de ces applications. Pour reprendre l'adage cité par le directeur de l'ANSSI, M. Guillaume Poupard, « Tout seul on va plus vite, à plusieurs on va plus loin [12]. » Les collectivités ont actuellement besoin d'aller loin et de construire du pérenne, plus que de vitesse.

---

[10] Par exemple, l'emploi du protocole sécurisé « https », qui permet de protéger l'intégrité et la confidentialité des données échangées sur *Internet*, n'est pas présent dans tous les produits. On rencontre également des logiciels dans lesquels le stockage des mots de passe est réalisé *via* un algorithme de chiffrement réversible alors que la situation précise ne l'exige pas et que les bonnes pratiques exigent, elles, l'emploi d'un *hash*. Enfin, de nombreuses solutions sont incompatibles avec l'utilisation de *proxy-web* qui sont, eux, systématiquement présents en environnement professionnel.

[11] Récompense proposée par une organisation pour la découverte de failles informatiques.

[12] Discours d'ouverture de G. Poupard lors du FIC 2022 (Forum international de la cybersécurité).

Le paiement de la rançon est souvent le premier réflexe, ou perçu comme l'unique porte de sortie

Un dernier élément peut expliquer les attaques de plus en plus nombreuses ciblant les collectivités : certaines paient [13]. Même s'il faut espérer que cela soit de moins en moins le cas, les récentes évolutions réglementaires risquent d'envoyer un mauvais message aux attaquants [14]. En effet, autoriser les assurances à prendre en charge le versement d'une rançon n'est pas de nature à inverser la tendance. Cependant, pour que le risque soit couvert, il est évident que les exigences des assureurs en matière d'hygiène numérique vont être fortes. Pour les entités qui ne seront pas couvertes, la tentation sera toujours présente. Une attaque qui réussit, et se traduit par une fuite des données des usagers ou rend indisponible le service public, impacte très négativement l'image et peut nuire à la capacité d'action publique de la collectivité. De surcroît, ces dernières sont parfois mal préparées à l'après-crise, notamment concernant la récupération des données *via* leurs sauvegardes. L'espoir, pour ne pas dire le rêve, de retrouver rapidement un système d'information pleinement opérationnel en payant une rançon est dans ces conditions très fort et emporte parfois la décision [15]. Ainsi, l'orientation vers le gain financier des pirates associé à des cibles qui paient, crée une incitation à attaquer ces structures.

Conséquences des attaques ou pourquoi il faut améliorer la protection des collectivités

Le risque de paralysie et de désorganisation de territoires entiers

Ce sont les collectivités territoriales qui, sur l'ensemble du territoire, assurent grâce à leurs services la vie en société des Français. Ainsi, sous le coup d'une attaque cyber d'ampleur et coordonnée, il serait *a priori* difficile voire impossible d'assurer des services qui semblent élémentaires, comme de gérer la circulation dans les centres urbains ou à l'échelle d'une région, de ramasser les ordures, de traiter les eaux usées, d'accueillir les enfants dans les établissements scolaires, de gérer les cimetières, de déneiger et de saler, de gérer les aides sociales, etc.

Outre ces missions « historiques », les collectivités sont de plus en plus coporteuses d'une véritable transformation numérique de la société. Un nombre croissant de services informatiques sont créés à destination des usagers. Cela, d'une part, augmente la surface d'attaque, car ces services ont vocation à être accessibles depuis *Internet*, donc potentiellement depuis le monde entier. De plus,

[13] Julie Jeunemaître : « Dans l'Oise, les cyberattaques se multiplient dans les collectivités locales : "on a dû payer 10 000 euros de rançon" », *France 3*, 18 janvier 2021 (https://france3-regions.francetvinfo.fr/).

[14] Gabriel Thierry : « Cybersécurité : les collectivités peuvent-elles payer les rançons ? », *La Gazette*, 26 septembre 2022 (www.lagazettedescommunes.com/).

[15] Lucas Boncourt : « La spirale infernale des rançongiciels décryptée par l'ANSSI », *Localtis*, 12 février 2021 (www.banquedesterritoires.fr/).

l'importance de ces systèmes va croissant au point de pouvoir créer de fortes désorganisations en cas d'indisponibilité ou de rupture d'intégrité pour les usagers. Il suffit d'imaginer un service de prise de rendez-vous pour le dépôt des demandes de passeport dont les données se trouveraient compromises avant les vacances d'été.

Sécurité et souveraineté des données personnelles des citoyens et usagers

Cette évolution numérique amène les collectivités à concentrer dans leurs systèmes d'information (SI) un nombre toujours plus important de données personnelles des usagers. Certaines sont même qualifiées de sensibles par la Commission nationale de l'informatique et des libertés (Cnil). Or, les récipiendaires de ces données, *a fortiori* en tant que représentants la puissance publique, doivent en garantir la confidentialité. En effet, le cadre réglementaire européen créé par le RGPD et auparavant déjà par la Loi informatique et libertés de 1978, oblige les collectivités, en tant que dépositaires de données personnelles confiées par les usagers, à mettre en œuvre des moyens de plus en plus nombreux et complexes pour assurer la protection contre les accès illégitimes, la modification ou la disparition de ces informations sous peine de sanctions financières et publicitaires.

Pour autant, cette exigence de sécurisation des données ne va, à ce jour, pas de pair avec une garantie de souveraineté sur ces mêmes données. En effet, certaines grandes entreprises numériques étrangères, et notamment américaines, offrent des solutions performantes et sécurisées, mais largement centrées sur le *cloud*. Leur poids économique est tel que la généralisation des solutions de *cloud* qu'ils proposent semble inéluctable. Mais la soumission de ces acteurs à la législation américaine extraterritoriale pose question en termes de souveraineté nationale sur les données des citoyens et résidents français.

De plus, le Code des marchés publics, auquel sont soumises les collectivités, ne place pas la souveraineté au rang des exigences. Il faut également souligner la faible sensibilité de certains décideurs aux problématiques de souveraineté, voire un certain aveuglement quant à l'exploitation susceptible d'être faite de ces informations et donc leur valeur réelle. Ainsi peut-on se poser la question d'une certaine opposition entre une responsabilité de protection des données personnelles confiées au sens de la souveraineté, et une responsabilité de protection contre des attaques ciblant ces données. L'opposition entre ces deux responsabilités peut interroger, tant il semblerait naturel de s'orienter vers des solutions européennes plus sensibles aux contraintes du RGPD et donc à même d'en garantir le respect [16].

Nos concitoyens sont, du reste, de plus en plus exigeants concernant la protection des données. Il est donc essentiel que le recours à des solutions de confiance devienne la norme. De plus en plus de solutions européennes et notamment françaises apparaissent qui permettent de satisfaire la quasi-totalité des

[16] Ali Laïdi : *Le Droit, nouvelle arme de guerre économique* ; Actes Sud, 2019.

besoins techniques en matière de cybersécurité. Les offres de *firewall*, *bastions*, *proxy*, sondes de détection, et beaucoup d'autres sont réelles et matures.

De plus, l'ANSSI a récemment actualisé une qualification permettant de garantir une informatique en nuage de confiance, *SecNumCloud* [17]. Les solutions ainsi qualifiées se doivent de respecter des exigences de cybersécurité, mais aussi d'étanchéité face à des lois extraterritoriales hors UE.

Dès lors, les collectivités, en dépensant de l'argent public, ne devraient-elles pas jouer un rôle de tremplin pour ces entreprises françaises et européennes ? Tout en bénéficiant de leur haut niveau de compétence et de la souplesse liée à la proximité géographique et au partage de la langue, les collectivités pourraient accompagner leur progression par retour d'expérience en leur offrant des débouchés.

Au vu des éléments précédemment cités, il serait tentant de conclure à un cercle vicieux : une surface d'attaque qui augmente sans cesse, une valeur des services et de leurs données qui augmente également, des moyens humains et financiers qui restent insuffisants, le tout associé à des éditeurs de logiciels qui ne sont pas systématiquement aidants, dans un contexte de prise de conscience très limitée des enjeux par les décideurs. Ces faits ne peuvent effectivement que caractériser un risque qui s'envole en attendant un sursaut de prise de conscience.

Les collectivités territoriales n'ont pas d'autre choix que de progresser rapidement en matière de cybersécurité tant elles sont devenues une cible de choix pour les pirates numériques avides de gain. De nombreux freins ne favorisent pas la rapidité d'une évolution positive, mais globalement le niveau de sensibilisation augmente lentement dans l'ensemble de l'écosystème. Il faut ici louer les initiatives de l'ANSSI [18] qui, en complément des initiatives de sensibilisation et de son activité de qualification de solutions de cybersécurité, pilote un plan de relance cybersécurité destiné aux collectivités permettant de trouver une réponse à la problématique financière et facilitant nombre de démarches. ◆

[17] « L'ANSSI actualise le référentiel *SecNumCloud* », ANSSI (www.ssi.gouv.fr/).

[18] « Cybersécurité : protéger les services publics et les collectivités territoriales avec France Relance », ANSSI (www.ssi.gouv.fr/).

Mots-clés : ANSSI, territoire, RGPD, résilience.

Lefebvre Dalloz
ACTIVER LA CONNAISSANCE

Cyber Resilience Act : quels changements pour la cybersécurité en Europe ?

Publié le 06/01/2023 - Mise à jour le 05/01/2023

Présentée par la Commission européenne le 15 septembre 2022, la proposition de règlement européen sur la cyber-résilience, connue sous le nom de « Cyber Resilience Act », vise à renforcer la cybersécurité des produits comportant des éléments numériques. Pour cela, elle établit un cadre européen commun en matière de cybersécurité et prévoit d'imposer de nouvelles obligations aux fabricants d'objets connectés.

La création d'un cadre européen pour la cybersécurité des produits comportant des éléments numériques

Le Cyber Resilience Act prévoit d'instaurer un cadre réglementaire commun aux États membres afin de lutter contre la multiplication des cyberattaques dont font l'objet les appareils connectés et de responsabiliser les acteurs économiques sur la cybersécurité des produits qu'ils proposent sur le marché européen.

Cette nouvelle réglementation européenne viserait l'ensemble des produits comportant des éléments numériques, qu'il s'agisse de dispositifs matériels (smartphones, jouets, ordinateurs, etc.) ou de logiciels (antivirus, systèmes d'exploitation, etc.). Elle ne concernerait toutefois pas certains produits connectés qui sont déjà encadrés par des législations spécifiques, comme c'est le cas des appareils utilisés dans les secteurs de l'aéronautique ou de la médecine.

Ce cadre européen serait en outre renforcé pour certains produits jouant un rôle central dans la sécurité des réseaux ou présentant des failles de sécurité touchant un grand nombre d'utilisateurs, comme les systèmes d'exploitation, les hyperviseurs, les antivirus, les gestionnaires de mots de passe, ou les objets connectés destinés au secteur industriel. Selon la proposition de règlement, ces produits « critiques » seraient soumis à des obligations supplémentaires.

Les nouvelles obligations imposées par le Cyber Resilience Act aux fabricants de produits connectés

Le Cyber Resilience Act prévoit deux obligations principales pour les fabricants et les éditeurs de produits connectés, qui devront prendre en compte la sécurité de l'appareil dès sa conception, et s'assurer de livrer des produits ne comportant aucune faille de sécurité connue.

La proposition de règlement sur la cyber-résilience ajoute également d'autres mesures afin de renforcer l'information des utilisateurs et d'assurer la sécurité des objets tout au long de leur cycle de vie. Elle prévoit ainsi d'imposer aux fabricants de fournir une documentation claire sur la sécurité des produits comportant des éléments numériques, et d'assurer la diffusion des correctifs de sécurité et des mises à jour pendant au moins cinq ans après la sortie du produit.

Les fabricants des produits connectés les plus critiques seront de plus tenus de signaler à l'Agence de l'Union européenne pour la cybersécurité (ENISA) les nouvelles vulnérabilités découvertes au sein des produits, dans un délai de 24 heures.

Afin d'assurer l'application du Cyber Resilience Act, les États membres devront désigner une autorité nationale de surveillance. En cas de non-respect des nouvelles règles de cybersécurité, les entreprises s'exposeront à des amendes pouvant s'élever à 15 millions d'euros ou 2,5 % de leur chiffre d'affaires mondial. En outre, si un produit est jugé non conforme au Cyber Resilience Act, il pourra faire l'objet de restrictions de commercialisation au sein du marché européen, voire d'une interdiction de vente.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité
Vie publique
Au cœur du débat public

Cybersécurité : quelles réponses face aux menaces nouvelles ?

Devant la multiplication des attaques menées à partir d'internet, les États se sont progressivement dotés de nouveaux moyens technologiques et institutionnels pour se protéger contre cette nouvelle menace. C'est l'ensemble de ces moyens que l'on désigne par le terme de "cybersécurité".

Par La Rédaction

Dernière modification : 13 mai 2022

Temps de lecture 12 minutes

Le préfixe cyber (du grec kuberneïn, diriger) renvoie aux ordinateurs et à internet. La cybersécurité porte à la fois sur la cyberattaque et sur la cyberdéfense(nouvelle fenêtre), c'est-à-dire l'usage de moyens informatiques pour mener ou riposter à une agression. On peut distinguer deux types d'attaques :

- l'infiltration de réseaux de communications à des fins d'espionnage, d'altération de données ou de prise de contrôle ;

- les campagnes d'influence sur internet, visant à orienter l'opinion publique.

Qu'est-ce que la cybersécurité ?

Le cyberespace, champ de bataille planétaire

Le "cyberespace" est l'espace de communication ouvert par l'interconnexion de tous les ordinateurs via internet. Il comprend des zones publiques (blog) et privées (messagerie, intranet d'une entreprise...). C'est l'espace sur lequel s'exerce la cybermenace. La particularité du cyberespace est d'abolir les distances et les frontières nationales. Par son caractère planétaire, la cybermenace bouleverse donc les repères traditionnels de la sécurité.

Les acteurs de la cybersécurité

La cybersécurité implique des acteurs de statut et de taille très diverses. Parmi eux, on trouve :

- les États et leurs forces armées ;

- les acteurs économiques (de la PME à la multinationale).

La particularité du cyberespace est de brouiller les critères traditionnels de la puissance. Ainsi, les géants du numérique ont souvent des capacités d'action comparables à celles des États. De même, un individu isolé peut à lui seul mettre en danger les systèmes informatiques d'une grande entreprise ou d'un État.

Les intérêts en jeu

Les motivations à l'origine de ces cyberattaques sont principalement de nature économique et politique.

Intérêts économiques :

- vol d'argent à un particulier ou à une entreprise (via de faux e-mails incitant à fournir ses identifiants bancaires par exemple) ;

- campagne de dénigrement d'une entreprise visant à capter sa clientèle ;

- espionnage industriel, etc.

Intérêts politiques :

- campagne d'influence visant à orienter le résultat d'un vote ;

- espionnage politique et militaire ;

- prise de contrôle des outils de communication à distance, etc.

Le cas du cyberterrorisme

Des groupes terroristes ont pu investir le cyberespace pour mener leur combat. Ils y ont vu un moyen de rééquilibrer le rapport de force à leur avantage, l'internet permettant de mener des offensives d'envergure avec des moyens limités. Ainsi, ils ont pu récolter des fonds, recruter des combattants ou encore pirater des sites internet à des fins de propagande grâce à l'outil numérique.

Mais les autorités craignent aujourd'hui des attaques de plus grande envergure, comme la prise de contrôle d'infrastructures stratégiques. En février 2017, le Conseil de sécurité des Nations unies a adopté une résolution incitant les États à se préparer pour intervenir efficacement en cas d'attaque contre les infrastructures essentielles(nouvelle fenêtre).

Quelles réponses contre la cybermenace ?

La surveillance d'internet

Pour surveiller les cybercommunications et lutter contre la cybercriminalité, les États se sont dotés de dispositifs de surveillance dédiés à internet. Des organes

inter-étatiques de surveillance existent, comme le réseau Échelon. Géré conjointement par les États-Unis, le Canada, l'Australie, le Royaume-Uni et la Nouvelle-Zélande, Échelon est le plus gros réseau de surveillance des télécommunications et cybercommunications au monde. Toutefois, de tels outils sont à double tranchant puisqu'ils peuvent servir à des fins d'espionnage (économique, militaire) ou de contrôle des populations.

La collaboration avec les géants du Net

Pour exercer leur autorité sur le cyberespace, les États doivent compter sur la coopération des géants du Net. En plus d'avoir des moyens techniques et financiers supérieurs à de nombreux États, ces derniers ont le pouvoir de dissimuler ou au contraire de rendre publiques les informations qui circulent via leurs services.

Une difficile réponse internationale

Face au caractère international de la cybermenace, les États ont tôt pressenti la nécessité d'une réponse internationale commune. Mais celle-ci se heurte à la lenteur des procédures de coopération nationale, ainsi qu'à la réticence des États à partager certaines informations. Les carences de la coopération internationale en matière de cybersécurité sont ainsi apparues au grand jour avec les attentats terroristes qui ont frappé l'Europe ces dernières années. En réponse à ces attaques, les différents gouvernements se sont engagés à plus de coopération.

Vers un droit international de la cybersécurité ?

Malgré les appels répétés de nombreux responsables politiques, il n'existe toujours pas de droit international contraignant en matière de cybersécurité. En effet, il existe des divergences de fond quant à la manière dont les États envisagent leur cybersécurité.

L'exception européenne

En 2001, le Conseil de l'Europe est à l'origine du premier traité de coopération internationale sur la cybersécurité. Connu sous le nom de Convention de Budapest(nouvelle fenêtre), ce traité a été signé par les États membres du Conseil de l'Europe, même si tous ne l'ont pas ratifié par la suite.

Au sein d'Europol, l'Union européenne (UE) a inauguré, en 2013, le Centre européen de lutte contre la cybercriminalité, visant à faciliter la coopération entre États européens dans la lutte contre le cybercrime.

En septembre 2017, la Commission européenne a proposé le "paquet cybersécurité" qui comprend un ensemble de mesures dont l'introduction d'une certification de cybersécurité à l'échelle de l'UE. Puis, en juin 2019, le règlement de l'UE sur la cybersécurité est entré en vigueur. Il a, à la fois, permis d'introduire un schéma de certification au niveau de l'UE tout en renforçant le nouveau mandat de l'Agence de l'UE pour la cybersécurité. Par ailleurs, en décembre 2020, la Commission européenne et le Service européen pour l'action extérieure ont présenté une

nouvelle stratégie de cybersécurité de l'UE(nouvelle fenêtre) avec, pour objectif, de renforcer la résilience de l'Europe face aux cybermenaces. Ayant adopté, en mars 2021, les conclusions de cette stratégie de cybersécurité, le Conseil a rappelé également que la cybersécurité reste essentielle à l'édification d'une Europe numérique. C'est aussi pourquoi l'UE étudie encore deux propositions législatives concernant les risques actuels et futurs (en ligne et hors ligne) par le biais notamment d'une directive destinée à mieux protéger les réseaux et les systèmes d'information.

Le cas français

La France fait de la cybersécurité sa priorité depuis les années 2000. Le retour de la menace terroriste en 2015 l'a poussée à intensifier ses efforts en la matière. La Stratégie nationale pour la sécurité du numérique a fixé cinq objectifs :

- garantir la souveraineté nationale ;

- répondre aux actes de cybermalveillance ;

- informer le grand public ;

- faire de la sécurité numérique un avantage concurrentiel pour les entreprises ;

- renforcer la voix de la France à l'international.

La surveillance de l'internet

La lutte contre la cybercriminalité passe d'abord par la surveillance d'internet. Le décret n%C2%B0 2015-125(nouvelle fenêtre) permet le blocage administratif des sites pédopornographiques et faisant l'apologie du terrorisme. En 2015 est votée la loi "Renseignement", qui renforce les moyens d'action des services de renseignement dans la sphère numérique. À la suite des attentats de Paris en 2015, le gouvernement a également lancé l'opération "Stop Djihadisme(nouvelle fenêtre)" afin de contrecarrer les campagnes de propagande jihadiste sur les réseaux sociaux.

La cybersécurité dans le droit français

En France, la cybercriminalité est prise en compte dans le droit depuis la loi informatique et libertés(nouvelle fenêtre) (1978) qui réglemente la liberté de ficher les personnes humaines. Aujourd'hui, les pratiques numériques sont encadrées par un dispositif juridique prévoyant des peines allant jusqu'à cinq ans d'emprisonnement et 75 000 euros d'amende pour les attaques informatiques. La loi prévoit en outre une aggravation des peines dans le cas de cyberattaques visant directement l'État.

Traquer les cybercriminels

La police et la gendarmerie disposent de divers organes dédiés à la répression de la cybercriminalité(nouvelle fenêtre). Parmi eux :

- l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) au sein de la Police judiciaire ;

- le Centre de lutte contre les criminalités numériques (C3N) au sein de la Gendarmerie nationale ;

- la Brigade d'enquête sur les fraudes liées aux technologies de l'information (BEFTI) au sein de la préfecture de police de Paris.

Défendre les usagers

L'Agence nationale de la sécurité des systèmes d'information (Anssi)(nouvelle fenêtre) a été créée en 2009 pour défendre et protéger les systèmes d'information et les usagers du numérique contre les cyberattaques. Ses missions sont les suivantes :

- surveiller les réseaux afin de détecter les attaques et permettre de réagir au plus vite ;

- développer des produits et services de cybersécurité à destination des usagers ;

- apporter son expertise et son assistance aux administrations et aux entreprises ;

- sensibiliser le public sur les cybermenaces.

Le Gouvernement a lancé en 2017 un dispositif national d'assistance aux victimes d'actes de cybermalveillance. Incubé par l'Anssi et copiloté avec le ministère de l'intérieur, la plateforme cybermalveillance.gouv.fr(nouvelle fenêtre) permet de mettre en relation des victimes de cyberattaques - particuliers, entreprises ou collectivités territoriales - et des prestataires de services susceptibles de les aider dans leurs démarches. Refondue début 2020, la plateforme a vu une hausse de +155% de sa fréquentation.

Pandémie de Covid-19 et cybersécurité

Lors des premières semaines du confinement du printemps 2020, les visites du site cybermalveillance.gouv.fr ont augmenté de près de 600%. Les recherches d'assistance à propos d'attaques par hameçonnage liées à la crise sanitaire ont crû de 400%. En entraînant une augmentation des usages numériques, l'épidémie de Covid-19 a aussi entraîné une augmentation de la cybercriminalité.

Par ailleurs, le développement du e-commerce depuis quelques années et le recours massif au télétravail durant la crise sanitaire (8 millions de salariés au printemps 2020) ont renforcé les risques de cyberattaques contre les entreprises. Les services informatiques doivent désormais mettre en place des stratégies zero trust(nouvelle fenêtre) : aucun utilisateur sur un réseau n'est totalement digne de confiance.

Le site de la CNIL met à la disposition des usagers des outils et des guides(nouvelle fenêtre) afin de renforcer leur cybersécurité.

La loi du 3 mars 2022 modifie le code de la consommation pour imposer des

obligations nouvelles en matière de cybersécurité aux grandes plateformes numériques. Ces opérateurs devront informer les internautes par un "cyberscore" de la sécurité de leur site ainsi que de la sécurisation et de la localisation des données qu'ils hébergent.

La cyberdéfense

La Revue stratégique de défense et de sécurité nationale de 2017 identifie un renforcement des menaces dans le cyberespace où "certaines attaques, en raison de leur ampleur et de leur gravité, pourraient relever de la qualification d'agression armée". L'actualisation stratégique de 2021(nouvelle fenêtre) ajoute que le "cyber et l'espace constituent désormais des champs assumés de rivalité stratégique permanente, voire de conflictualité" et sont "de nouveaux domaines d'expression de la puissance".

Créé en 2017 et dépendant du ministère des armées, le Commandement de la cyberdéfense (Comcyber) a la responsabilité de la cyberdéfense militaire qui recouvre l'ensemble des actions défensives et offensives conduites dans le cyberespace. Le Comcyber est constitué de 3 400 cyber-combattants. La loi de programmation militaire (LPM) 2019-2025(nouvelle fenêtre), qui consacre 1,6 milliard d'euros à la cyberdéfense, portera le nombre de ces combattants à 4 000 d'ici à 2025.

Le 18 janvier 2018, la ministre des armées a présenté la doctrine de lutte informatique offensive (LIO)(nouvelle fenêtre) qui complète la lutte informatique défensive (LID). La ministre a ainsi officialisé le volet offensif de la doctrine cybermilitaire française. La LIO et la LID renforcent la posture permanente de cyberdéfense (PPC) créée par la LPM 2019-2025. La PCC permet de protéger en permanence tous les réseaux militaires et de réagir à toute attaque contre les intérêts de la défense de la France.

Livre blanc de la cyberdéfense, la Revue stratégique de cyberdéfense(nouvelle fenêtre) a été publiée en février 2018 par le Secrétariat général de la défense nationale (SGDN).

La nouveauté, selon la ministre des armées, c'est "de considérer le cyberespace comme un champ de bataille à part entière, de reconnaître que le cyber [est] une arme, avec un potentiel qui peut être bien plus nuisible et dangereux qu'un missile" (discours sur la cybersécurité et la cyberdéfense, Lille, 8 septembre 2021).

Council of the EU

PRESS
FR

COMMUNIQUÉ DE PRESSE
219/21
22/03/2021

Cybersécurité: le Conseil adopte des conclusions sur la stratégie de cybersécurité de l'UE

Le Conseil a adopté ce jour des conclusions sur la stratégie de cybersécurité de l'UE pour la décennie numérique. Cette stratégie a été présentée par la Commission et le haut représentant de l'Union en décembre 2020. Elle expose le cadre de l'action de l'UE visant à protéger les citoyens et les entreprises de l'UE des cybermenaces, à promouvoir des systèmes d'information sûrs et à protéger un cyberespace mondial, ouvert, libre et sûr.

Dans ces conclusions, le Conseil fait observer que la cybersécurité est essentielle à l'édification d'une Europe résiliente, verte et numérique. Il y fixe l'objectif clé consistant à parvenir à une autonomie stratégique tout en préservant une économie ouverte. Il s'agit notamment d'accroître la capacité à opérer des choix autonomes dans le domaine de la cybersécurité afin de renforcer le leadership numérique et les capacités stratégiques de l'UE.

Dans ses conclusions, le Conseil met en évidence un certain nombre de domaines d'action pour les années à venir, y compris:

- les plans relatifs à la création d'un **réseau de centres des opérations de sécurité** dans toute l'UE afin de surveiller et d'anticiper les signes d'attaques sur les réseaux
- la mise en place d'une **unité conjointe de cybersécurité**, qui permettrait de définir des orientations claires concernant le cadre européen de gestion des crises en matière de cybersécurité
- la ferme volonté qui est la sienne d'appliquer les mesures de la **boîte à outils de l'UE relative à la 5G**, d'en achever rapidement la mise en œuvre et de poursuivre les efforts visant à garantir la sécurité des réseaux 5G et le développement de futures générations de réseaux
- la nécessité d'un effort conjoint pour accélérer l'**adoption des normes clés de sécurité internet**, étant donné qu'elles contribuent de manière déterminante à relever le niveau global de sécurité et d'ouverture de l'internet mondial, tout en renforçant la compétitivité de l'industrie de l'UE
- la nécessité de soutenir le développement du **chiffrement fort**, qui est un moyen de protéger les droits fondamentaux et la sécurité numérique, tout en veillant à ce que les autorités répressives et judiciaires puissent exercer leurs pouvoirs tant en ligne que hors ligne
- le renforcement de l'efficacité de la **boîte à outils cyberdiplomatique**, une attention particulière étant accordée à la nécessité de prévenir et de contrer les cyberattaques ayant des effets systémiques susceptibles d'affecter les chaînes d'approvisionnement, les infrastructures critiques et les services essentiels, ainsi que les institutions et processus démocratiques, et de compromettre la sécurité économique
- la proposition relative à la mise en place éventuelle d'un **groupe de travail en matière de cyber-renseignement**, qui vienne renforcer la capacité spécifique de l'INTCEN dans ce domaine
- l'importance qu'il y a à **renforcer la coopération** avec les organisations internationales et les pays partenaires afin de faire progresser la compréhension commune du paysage des cybermenaces
- la proposition visant à élaborer un **programme de renforcement des cybercapacités externes de l'UE** afin d'accroître la cyber-résilience et les cybercapacités dans le monde entier

Afin d'assurer l'élaboration, la mise en œuvre et le suivi des propositions présentées dans le cadre de la stratégie de cybersécurité, le Conseil encourage la Commission et le haut représentant à établir un plan de mise en œuvre détaillé. En outre, le Conseil suivra les progrès accomplis dans la mise en œuvre des conclusions au moyen d'un plan d'action qui sera régulièrement examiné et mis à jour.

Press office - General Secretariat of the Council
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press

Revue stratégique de cyberdéfense

12 février 2018

Extrait

SGDSN

[difficulté majeure. Les informations relatives aux incidents sont peu ou pas partagées[60], il n'y a pas de lieu de centralisation d'une telle information et aucune réflexion n'a encore été menée quant à sa structuration. Par ailleurs, cette absence de statistiques empêche de modéliser l'offre (bien qu'en France, la plateforme gouvernementale cybermalveillance.gouv.fr commence à le faire et qu'à l'international d'autres initiatives aient été lancées). La constitution d'une base de données européenne répertoriant la majorité des incidents cyber serait à ce titre une avancée. Les données pourraient être agrégées afin d'analyser les tendances en matière de menaces, d'identifier des besoins en termes de sécurité pour les produits et services présents sur le marché, et de fournir des informations chiffrées sur les coûts. La mise en place actuelle de mécanismes d'obligation pour la notification d'incidents au sein de l'Union européenne (à travers notamment le GDPR, la directive NIS et le paquet télécom) pourra utilement contribuer à l'établissement d'un état des lieux du risque numérique.

Une dernière difficulté tient à la question de la valorisation des biens intangibles qui constituent 85 % de la valeur des entreprises aujourd'hui. Un actif informationnel tel qu'entendu dans une économie numérique est un incorporel qui n'est pas qualifié sur le plan juridique, ni quantifié sur le plan comptable. Il n'est donc pas un actif assurable. L'assurabilité de l'actif intangible représente un enjeu essentiel pour la valorisation de l'entreprise dans une économie numérique.

La mise en place d'une politique de management des risques cyber, intégrée au management des risques de l'entreprise, constitue un autre enjeu clé. Les sociétés cotées ont obligation depuis 2011 d'adopter des pratiques de management des risques, s'appuyant sur des outils de cartographie, un comité de gouvernance et des audits. Ces bonnes pratiques doivent être développées dans toutes les entreprises, tout en tenant compte de leur niveau de maturité et de leur taille, car elles permettent de sensibiliser les instances dirigeantes et constituent un pré-requis à la souscription raisonnée d'une offre d'assurance cyber.]

3.4. Les enjeux humains

Le niveau de cybersécurité de notre société est directement lié aux comportements de l'ensemble des Français - particuliers, entreprises et administrations - et par conséquent à leur degré de compréhension et de maîtrise des enjeux de cybersécurité. Les services de l'État, les entreprises et les individus sont en effet de plus en plus connectés par des technologies offrant de nouveaux modes de travail, d'interaction et de transaction. Sous la pression de la mobilité, de l'utilisation massive des données ou encore de l'Internet des objets, le numérique se diffuse toujours plus rapidement et profondément. Si la diffusion de la culture de la sécurité numérique ne suit pas, alors les conditions d'une utilisation sereine et confiante de l'Internet comme des objets connectés ne pourront être réunies. C'est une

[60] Selon des estimations de l'OCDE, entre 60 et 89% des incidents ne seraient pas reportés.

approche pédagogique, positive et ancrée dans la réalité des différents publics de la culture de la sécurité numérique que la présente revue propose, afin d'en renforcer l'impact et d'éveiller au maximum l'intérêt de chacun aux enjeux du numérique. Il faut donner des clés aux entreprises, aux administrations et aux citoyens afin qu'ils deviennent acteurs de la sécurité du numérique, dans leurs vies personnelle et professionnelle.

C'est pourquoi, la cybersécurité doit être intégrée, de l'école élémentaire au lycée, au parcours de formation des élèves. Des approches ludiques doivent, parallèlement, en être proposées tout au long de la vie, adaptées aux différents degrés de familiarité qu'ont les Français avec les systèmes d'information et de communication et à leur usage des objets connectés du quotidien. Une plus forte diffusion de la culture de la sécurité numérique dans les entreprises et dans les administrations publiques apparait aussi souhaitable, tandis que des réponses doivent être apportées aux besoins de recrutement de spécialistes de la cybersécurité chez ces dernières. Notre pays ne peut en outre se contenter de former des spécialistes de la cybersécurité et de la cyberdéfense, il doit également se donner les moyens de les conserver et d'attirer les talents étrangers.

3.4.1. Eduquer dès le plus jeune âge aux enjeux de la cybersécurité

L'éducation dès le plus jeune âge à la cybersécurité doit constituer une priorité. Les enfants et les adolescents ont une pratique quotidienne, et précoce par rapport aux générations qui les ont précédés, des objets connectés, d'Internet et des réseaux sociaux. Selon une étude IPSOS « Junior Connect » datant de 2015, l'âge moyen du premier téléphone portable est de 9 ans et celui du premier *smartphone* de 12 ans. Les jeunes de 13 à 19 ans se connectent en moyenne 13h30 par semaine et 78 % d'entre eux sont inscrits sur les réseaux sociaux[61]. Or, nombre de ces jeunes ne maîtrisent pas les dangers liés à la communication d'informations personnelles, à la connexion avec des inconnus ou à la publication de photos privées[62].

Il appartient à l'école de la République d'éduquer les élèves à la cybersécurité. Cela doit passer par une première sensibilisation au numérique dès les années de maternelle et par une éducation au numérique incluant la maîtrise des exigences en matière de cybersécurité à l'école élémentaire, au collège et dans tous les cursus du lycée. L'éducation au numérique dès le plus jeune âge est structurante pour les comportements futurs. L'ouverture précoce aux grands concepts de la science des techniques informatiques donnera des clés aux élèves pour comprendre le monde qui les entoure et leur permettra plus tard de devenir acteurs de ce monde et non de simples consommateurs du numérique. Il s'agit d'apprendre aux élèves à utiliser le numérique dans tous les domaines de la vie, de leur permettre d'acquérir une culture numérique, de l'initiation au code à la compréhension de la logique des *computers*

[61] Au regard des tendances observées sur les dernières années, on peut estimer que ces chiffres sont, si ce n'est en augmentation, du moins stables depuis 2015.

[62] Selon la même étude IPSOS « Junior Connect », 57 % des 11-12 ans ont un profil FACEBOOK malgré l'interdiction de s'y connecter avant l'âge de 13 ans, 43 % ont déjà ajouté des inconnus à leur liste d'amis et 12 % envoyé des photos ou des vidéos à des inconnus.

sciences, en passant par l'acquisition de compétences en traitement de données et l'aptitude à adopter des comportements respectueux des règles de sécurité.

À l'école élémentaire, il est important de montrer les liens qui unissent les concepts de l'informatique et ceux qui sont enseignés dans les autres disciplines, puis ceux qui les unissent aux objets familiers du quotidien[63].

Au collège, l'enseignement des mathématiques et de la technologie, qui intègre l'apprentissage des algorithmes et de la programmation informatique, doit constituer le principal vecteur de transmission des règles de la cybersécurité.

Bien évidemment, l'apprentissage des règles de la cybersécurité ne doit pas s'arrêter aux portes des lycées, au risque de voir les futurs jeunes adultes rapidement dépassés par des enjeux qui ne manqueront pas de se renouveler extrêmement rapidement. C'est pourquoi il apparaît essentiel que des formations de sensibilisation aux enjeux de la cybersécurité soient intégrées dans les parcours des lycéens généraux, technologiques et professionnels, de la classe de seconde à la classe de terminale.

Les parcours de formation initiale et continue des enseignants, notamment de mathématiques et de technologie, devront intégrer cette exigence nouvelle d'une transmission aux élèves des règles de la cybersécurité. Des MOOC[64] dédiés aux enseignants en formation initiale et en formation continue pourraient être conçus par le ministère de l'éducation nationale avec le soutien de l'ANSSI. De nouvelles ressources pédagogiques dédiées à la sensibilisation des élèves aux règles de la sécurité informatique devront être régulièrement mises à disposition des enseignants[65].

L'efficacité de la sensibilisation des plus jeunes aux enjeux de la cybersécurité pourra être renforcée par des actions ludiques. Certains programmes ont d'ores-et-déjà démontré leur efficacité dans le domaine de la diffusion de la culture numérique. Le *Permis Internet* proposé aux enfants, programme national de prévention développé par la Gendarmerie nationale, la Police nationale, la Préfecture de Police et l'association *AXA Prévention*, permet ainsi de sensibiliser des enfants de CM2 et leurs parents à un usage d'Internet vigilant, sûr et responsable[66]. Le dispositif *Ecole Internet*, développé par l'association *Ville Internet* et qui promeut les usages d'Internet pour les élèves des écoles maternelles et élémentaires francophones en labellisant les écoles participantes, en valorisant leurs actions et en incitant

---

[63] L'apprentissage des règles d'utilisation d'Internet doit notamment constituer une priorité. Les élèves doivent connaître les principes de responsabilité civique et légale de l'internaute, les règles du téléchargement, apprendre à s'informer sur Internet mais aussi à maîtriser les réseaux sociaux et à protéger leur vie privée sur la toile.

[64] MOOC (*Massive Open On Line Course*) : formation en ligne ouverte à tous.

[65] Le portail du ministère de l'éducation nationale *Eduscol* propose déjà de premières ressources pédagogiques pour sensibiliser à l'informatique les élèves de primaire et de secondaire. La direction du numérique pour l'éducation de ce ministère gère par ailleurs une banque nationale de mutualisation de ressources appelée *Edu'base*.

[66] https://www.permisinternet.fr/.

à des échanges d'expériences, constitue également une initiative intéressante. En s'inspirant de ce dispositif, on pourrait par exemple imaginer des démarches de mise en valeur, voire de labellisation, des établissements d'enseignement les plus engagés en faveur de la cybersécurité.

La présente revue recommande la mise en place rapide d'un groupe de travail, sous le pilotage du ministère de l'éducation nationale, chargé de définir les actions à mener, et le cas échéant, les modifications à apporter aux programmes pour que tous les élèves sortent du système éducatif avec un niveau élevé de maîtrise des enjeux de la cybersécurité.

3.4.2. Sensibiliser le grand public par des actions pédagogiques

Si la sensibilisation du public scolaire aux enjeux de la cybersécurité est indispensable, une sensibilisation du grand public doit parallèlement être conduite.

Les initiatives d'ores-et-déjà existantes dans la diffusion de la culture du numérique constituent de premières bases sur lesquelles s'appuyer. On pense notamment au programme de service civique « les D-CoDeUrs », lancé en 2016, qui implique des volontaires engagés pour l'inclusion numérique, en ciblant prioritairement trois publics : les populations peu connectées (à qui sont proposées des ateliers dans des lieux de médiation numérique de proximité), les publics scolaires et périscolaires et des seniors (à travers des actions mises en place au sein de maisons de retraite ou de clubs du troisième âge). On pense également au collectif *EDUCNUM*, initié par la CNIL en mai 2013 et constitué de soixante structures[67], pour porter et soutenir des actions visant à promouvoir une véritable « culture citoyenne du numérique », notamment à travers l'initiation et la promotion d'actions de sensibilisation et de formations de tous les publics, notamment les plus jeunes, à un usage responsable et éclairé des technologies numériques. La plateforme cybermalveillance.gouv.fr assume quant à elle un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française.

Mais il paraît essentiel d'aller plus loin en amplifiant les actions en cours, en communiquant de façon plus efficace et plus stratégique, et en développant des actions de sensibilisation spécifiquement dédiées aux enjeux de la cybersécurité.

La présente revue recommande ainsi que soit créée une application ludique, disponible sur *smartphone*, permettant aux Français de tester leur niveau de connaissances dans le domaine de la sécurité numérique et leur proposant, quel que soit leur niveau initial de maîtrise, de nombreux défis. La réalisation de cette application pourrait être prise en charge par l'ANSSI (qui propose déjà, avec le MOOC *SecNumacadémie*, un programme en ligne de sensibilisation à la sécurité du numérique qui s'adresse à tous[68]). L'agence pourrait notamment s'inspirer, pour concevoir cette application pédagogique sur la sécurité numérique, du projet de

[67] Entreprises, organismes, associations issues du monde de l'éducation, de la recherche, de l'économie numérique, de la société civile, de fondations d'entreprises et d'autres institutions.

[68] https://www.ssi.gouv.fr/particulier/formations/secnumacademie/.

plateforme en ligne d'évaluation et de certification des compétences numériques PIX, actuellement développé par les ministères de l'éducation nationale et de l'enseignement supérieur[69].

Une piste de recherche originale et innovante serait, par ailleurs, d'étudier l'apport des *nudges* pour le développement de l'autonomie des citoyens en matière de cybersécurité. Ces approches incitatives, fondées sur les sciences du comportement, ont connu une reconnaissance retentissante avec l'attribution du Prix Nobel d'économie 2017 à Richard THALER, l'un des pères de la « *nudge economy* ». Les *nudges* sont mis en œuvre dans l'accompagnement des politiques publiques aux Etats-Unis et au Royaume-Uni. En France, un chef de projet *nudge* a été recruté au SGMAP et pourrait être sollicité par l'ANSSI pour réfléchir à la mise en place de *nudges* pour inciter à un comportement plus responsable des utilisateurs face aux menaces cyber.

3.4.3. Diffuser la culture de la sécurité numérique au sein des entreprises et des administrations publiques

La diffusion de la culture de la sécurité numérique doit également être renforcée au sein des entreprises et des administrations publiques.

L'ANSSI publie à cette fin des guides comme le « Guide des bonnes pratiques de l'informatique », qui présente douze recommandations issues de l'analyse d'attaques réussies à l'adresse des TPE et des PME[70], ou le guide sur « La cybersécurité des systèmes industriels », qui propose, en l'illustrant par des situations réelles, aux acteurs concernés une méthodologie simple et adaptée pour sécuriser leurs systèmes industriels. L'agence publie également un référentiel d'exigences applicables aux prestataires de services d'informatique en nuage (*SecNumCloud*), élaboré en concertation avec les acteurs du marché. Parallèlement, les initiatives visant à promouvoir la cybersécurité au sein des entreprises sont nombreuses, de l'organisation en octobre 2017 par l'ENISA (agence européenne chargée de la sécurité des réseaux et de l'information) du « Mois européen de la cybersécurité »[71] aux actions conduites par le CIGREF[72] et le *Cercle européen de la sécurité et des systèmes d'information*, en passant par le *Forum International de la Cybersécurité* (FIC)[73] ou l'*European cyberWeek*[74]. Ces

---

[69] https://pix.beta.gouv.fr.

La plateforme PIX est un référentiel de compétences numériques en ligne pour une certification numérique tout au long de la vie. Son objectif est d'accompagner l'élévation du niveau général de connaissances et de compétences numériques.

[70] http://www.ssi.gouv.fr/publication/lanssi-et-la-cgpme-publient-le-guide-des-bonnes-pratiques-de-informatique/.

[71] https://www.ssi.gouv.fr/agence/cybersecurite/mois-de-la-cybersecurite-2017.

[72] Association dont la mission est de développer la capacité des grandes entreprises à intégrer et maîtriser le numérique.

[73] https://www.forum-fic.com. Le FIC est l'un des événements de référence en matière de cybersécurité et de confiance numérique, réunissant l'ensemble des acteurs en France et en Europe.

initiatives, à l'efficacité réelle, doivent être encore amplifiées, leur coordination renforcée et leur diffusion élargie au plus grand nombre d' acteurs économiques. Enfin, le ministère chargé de l'industrie va contribuer à cet effort, notamment en intégrant une dimension cybersécurité à son programme de soutien à la transformation numérique des entreprises.

Au sein des administrations publiques, centrales, territoriales et déconcentrées, la culture de la sécurité numérique doit être diffusée auprès de tous les agents, quel que soit leur niveau de responsabilité ou leur secteur de spécialisation. La maîtrise de la culture de la sécurité numérique doit être érigée en priorité des programmes de formation initiale et de formation continue. Le développement de modules de formation initiale et continue dans les écoles de la fonction publique nationale et territoriale et le développement des formations cyber à l'Institut des hautes études de défense nationale (IHEDN) et à l'Institut nationale des hautes études de sécurité et de justice (INHESJ) apparaissent ainsi indispensables. L'encadrement doit se saisir des problématiques de sécurité numérique, qui ne peuvent relever de la seule responsabilité des personnels et des directions chargés de la sécurité informatique. L'intégration de celle-ci dans la définition des missions des cadres de la fonction publique devrait être envisagée.

3.4.4. Développer l'offre de formation professionnelle aux enjeux de la cybersécurité

Le niveau d'ambition de la France dans les domaines de la cyberdéfense et de la cybersécurité est aujourd'hui contraint par ses capacités en matière de ressources humaines, notamment s'agissant des ingénieurs spécialisés en informatique et en télécommunications (réseaux informatiques, sécurité, informatique, crypto-analyse, etc.). La construction d'une culture nationale du numérique solide passe par la formation des experts de demain.

Des démarches associatives et syndicales existent pour promouvoir les métiers du numérique et faire tomber les réflexes d'autocensure de certains publics au regard de ces métiers. Le *Syntec Numérique* (syndicat professionnel des entreprises de services du numérique, des éditeurs de logiciels et des sociétés de conseil en technologies) s'est ainsi engagé dans de nombreuses actions pour renforcer l'attractivité des formations dans le numérique, comme le programme JEM'NUM (« Journée des entreprises et des métiers du numérique ») ou l'association *Pascaline* pour inciter les jeunes à aller vers les écoles d'ingénieurs (*cf.* encadré ci-après). Des associations comme *Femmes du Numérique* ou *Informatique au féminin* sensibilisent, quant à elles, les jeunes afin de combattre les préjugés sur les femmes qui exercent dans l'informatique.

[74]https://european-cyber-week.eu/fr/accueil/.