INSTITUT Montaigne

institutmontaigne.org
RAP2306-02

RAPPORT - Juin 2023

Cybersécurité
Passons à l'échelle

Historiquement, la cybersécurité a été d'abord une préoccupation des grandes entreprises à portée internationale, inquiètes de la protection de leurs flux de données et de leurs secrets industriels ou commerciaux. Sensibles au contexte mondial dans lequel elles évoluaient, elles ont été les premières à prendre des mesures pour se prémunir contre les cyberattaques. Aussi, les politiques régaliennes de sécurisation cyber se sont-elles essentiellement concentrées sur ces grands acteurs économiques et sur les entités critiques, laissant les plus petites structures - TPE/PME/ETI, collectivités et établissements de santé - très largement démunies et exposées aux dangers.

Deux éléments appellent aujourd'hui une correction rapide de ce désintérêt. Le premier est **l'intensification des menaces dans le cyberespace découlant de la mondialisation de la cybercriminalité.** L'élargissement de la surface d'attaque devient un facteur de déstabilisation économique et sociale potentiellement grave, qu'il s'agisse de bloquer l'activité d'une entreprise, d'un établissement de santé ou d'une collectivité, mettant en péril leur capacités opérationnelles, leur santé financière voire leur survie. Selon les chiffres gouvernementaux**, une PME sur deux fait faillite dans les 18 mois suivant une cyberattaque.** On estime également qu'**1 collectivité sur 10 (majoritairement de moins de 5000 habitants) a déjà été victime d'un rançongiciel.** Le coût, à lui seul, des attaques par rançongiciel subis pour les PME de moins de 50 employés est estimé à plus de 720 M€ par an.

Le second élément invitant à une action rapide est **l'application française de la directive européenne NIS 2 d'ici à septembre 2024**, dont les nouvelles orientations visent à entamer la diffusion de la cybersécurité dans l'ensemble de la chaîne numérique, précisément dans cette logique de sécurisation des maillons faibles. Une amende proportionnelle au chiffre d'affaires sera exigée en cas de non

conformité. Surtout, ce respect de la directive sera une condition d'insertion des petits dans les chaînes de décision ou de valeur des plus grands.

Les entretiens menés pour cette étude révèlent tout à la fois une prise de conscience de la menace cyber de la majorité des acteurs et une forte **volonté de passer à l'action, mais aussi un manque de moyens et d'accompagnement pour franchir le pas.** Peu d'entreprises rendent compte des attaques subies. Une minorité des acteurs locaux (principalement des petites communes et de très petites entreprises) reste néanmoins soit inconsciente des risques, soit rétive à la prise en compte de la menace car ne se sentant pas concernée.

En effet, les entités de taille modérée font rarement de la cybersécurité une priorité, et lorsqu'elles s'y intéressent, le manque de visibilité de ce qu'elles doivent faire, le manque de compétences disponibles, le manque de financement et l'existence d'une multitude de solutions techniques contribuent à les décourager d'agir. Pourtant, la littérature facilement accessible recèle d'excellentes recommandations pour tout responsable cherchant à mieux protéger sa structure. Encore faut-il savoir par où commencer et vers qui se tourner, comment anticiper les risques et comment réagir en cas d'attaque.

Des mesures spécifiques adaptées à ces acteurs doivent donc être proposées.
Côté pouvoirs publics, beaucoup d'excellentes choses existent déjà et les acteurs de l'État sont unanimement reconnus pour leur professionnalisme et leurs compétences. Mais la répartition de leurs prérogatives n'est pas nécessairement maîtrisée et le besoin de moyens additionnels ne croît pas au rythme de la menace. Surtout, la coordination de leurs actions est un impératif aux échelles appropriées des structures à protéger – régions, départements, communes. Et cette coordination doit non seulement s'appliquer à prévenir les cyberattaques, elle doit aussi traiter au mieux leur remédiation et leur répression.

Ainsi, il apparaît nécessaire de **créer les conditions d'un passage à l'échelle pour mobiliser à tous les niveaux et protéger plus exhaustivement le territoire.** Cependant, ce nécessaire passage à l'échelle de la part des acteurs locaux publics et économiques est confronté à deux impératifs contradictoires. Face à l'urgence de la situation, le premier plaide pour des mesures d'obligation afin d'accélérer le pas. Au vu du besoin de pédagogie et d'accompagnement d'acteurs qui se sentent démunis, le second plaide pour une approche moins rigide, centrée sur l'incitation.

Le rapport propose ainsi une **approche incrémentale**.

- Dans un premier temps, il a semblé nécessaire de se concentrer sur ce que les entreprises et collectivités pouvaient faire par elles-mêmes et de les accompagner au plus près dans cette montée en sensibilisation et en protection autonome.

- Dans un deuxième temps, la contrainte réglementaire poussera naturellement ces acteurs à une prise en charge minimale des enjeux de cybersécurité.

- Enfin, une approche plus contraignante pourra être envisagée auprès des plus rétifs afin d'élargir la couverture territoriale et d'assurer un niveau minimum de cybersécurité à l'échelle du pays.

Dans cette démarche de rehaussement collectif du niveau de cybersécurité, l'Institut Montaigne a proposé **une méthode simple et rapidement opérationnelle fondée sur les solutions et acteurs existants.**

À cette fin, à partir du constat partagé, de **nombreux entretiens ont été conduits avec des personnages-clé de l'écosystème français de la cybersécurité.** Pour les compléter, des experts de ce même écosystème et des entreprises adhérentes à l'Institut Montaigne se sont réunis et ont collaboré pour imaginer et consolider les réponses adaptées.

Plus spécifiquement, **une dizaine d'ateliers thématiques ont été conduits** réunissant entreprises, experts et acteurs de terrain, en partenariat avec le Mouvement des entreprises de taille intermédiaire (METI) et la Gendarmerie nationale. Cette approche collaborative a permis un constat partagé de la situation et l'identification des pistes les plus utiles pour mieux sensibiliser responsables et employés des structures visées. Les ateliers se sont appliqués à identifier les types de produits de sécurité numérique les plus adaptés – dans une logique du juste besoin, et les modalités d'accompagnement des bénéficiaires. La question de la maîtrise des risques et du modèle assurantiel possible a été sérieusement examinée, tandis que le sujet des financements et de la nécessaire mutualisation des solutions ont fait l'objet d'une attention particulière. Enfin, les enjeux de simplification du signalement, de remédiation et d'action judiciaire ont été intégrés à la réflexion.

Ces ateliers ont ensuite été complétés par des **études de terrain**, auprès d'entreprises nationales et locales, de collectivités territoriales et d'un Centre Régional de Réponse à Incidents (CSIRT). Ces études ont permis de **tester la validité des recommandations** au plus près des acteurs engagés sur le terrain.

Le coût annuel global de cet effort de passage à l'échelle pour les petites entreprises et collectivités représenterait une centaine de millions d'euros, englobant tant les moyens humains nécessaires que les subventions en faveur d'offres mutualisées et des structures qui les portent.

Axe 1 :

Mobiliser les acteurs locaux en faveur d'un parcours de cybersécurité simple et progressif à même de les protéger et de les préparer aux crises : diagnostic, ambition, précautions, exercices et organisation

RECOMMANDATION 1 : Inciter à recourir à des diagnostics organisationnels et techniques en proposant un référentiel commun comprenant différentes profondeurs de diagnostic

RECOMMANDATION 2 : Fixer une cible de cybersécurité à atteindre pour les structures, en fonction de leur criticité et de leurs moyens, et les inciter à progresser dans la durée en proposant un système de badges les aidant à prioriser leurs arbitrages

RECOMMANDATION 3 : Limiter nativement la présence de vulnérabilités et de failles dans les poduits et équipements numériques disponibles sur le marché européen en exploitant tout le potentiel du règlement européen *Cyber Resilience Act*, et informer les utilisateurs en temps réel en cas de trafic Internet suspect grâce à une "cyber vigie" opérée par les opérateurs de télécommunications

RECOMMANDATION 4 : Exhorter les entreprises et collectivités à considérer le risque cyber comme une préoccupation stratégique encadrant les choix humains, organisationnels, budgétaires et techniques de leur activité

RECOMMANDATION 5 : Organiser une simulation annuelle d'alerte cyber (équivalent de "l'alerte incendie") pour tous les salariés ou agents d'une entreprise ou d'une collectivité, afin de les acculturer à la menace et aux bonnes pratiques numériques

RECOMMANDATION 6 : Instaurer une fonction de conseiller à la sécurité numérique (CSN) auprès de chaque responsable de structure (dirigeant d'entreprise ou élu) pour accompagner celui-ci sur les questions de cybersécurité

Axe 2 :

Coordonner les ressources, les outils et les prérogatives de chaque acteur aux échelles appropriées : nouveaux moyens nationaux et mutualisations locales

RECOMMANDATION 7 : Mutualiser les compétences et les outils chez les acteurs de confiance publics et privés en charge de la cybersécurité afin de permettre une couverture complète du maillage territorial

RECOMMANDATION 8 : Faciliter le signalement des attaques cyber via une "Plateforme de Signalement des faits Cyber", base de données commune aux différents services publics compétents en matière de cybersécurité, permettant un suivi consolidé

RECOMMANDATION 9 : Renforcer les moyens et l'organisation des acteurs de la lutte contre la cybercriminalité dans une logique de proximité, en mettant l'accent sur la prévention et sur la répression

RECOMMANDATION 10 : Pérenniser le financement de l'effort public en faveur d'une sécurité numérique collective par un abondement vertueux des budgets

Cette étude à la fois globale et territoriale a montré l'urgence d'une action coordonnée aux différentes échelles du territoire. L'expérience de terrain invite à un pragmatisme volontaire qui mobilise chaque acteur de la sécurité numérique à son juste niveau.

Au niveau national, l'ANSSI porte l'ambition de la sécurité numérique nationale et promeut les solutions et outils les plus pertinents pour les acteurs concernés. Les services de l'Intérieur portent les enjeux de prévention et d'investigation, couplés avec la Justice pour la partie sanctions.

Au niveau local, les conseils régionaux, les préfectures, la gendarmerie et la police nationales, et autres services de l'État, les chambres consulaires et les collectivités ont tous un rôle à jouer de sensibilisation, de formation, d'anticipation des attaques et de collecte d'informations. Le secteur privé a essentiellement une responsabilité d'accompagnement, d'ingénierie technique et de remédiation en cas de problème.

Les conditions clés pour un passage à l'échelle effectif et réussi reposent essentiellement sur l'articulation des efforts de ces différents acteurs en temps réel et la mobilisation rapide des moyens identifiés.

Côté entreprises et petites collectivités, la priorité est à la compréhension des enjeux, l'acceptation des accompagnements disponibles et la mise en place des outils proposés (diagnostic et mise à niveau personnalisée).

La conviction des professionnels du secteur est qu'il suffit parfois de peu pour améliorer la sécurité des structures, pour autant que celles-ci en comprennent l'utilité et en acceptent les modalités pratiques. Le numérique irriguant désormais tous nos usages, la sécurité doit devenir un réflexe naturel, comme le port de la ceinture de sécurité dans les voitures ou la fermeture de la porte d'entrée de sa maison : un comportement de bon sens que personne ne remet en cause.