INSTITUT MONTAIGNE

Cybermenace : avis de tempête

CLIQUEZ ICI POUR TÉLÉCHARGER LE RAPPORT

Paris, le 21 novembre 2018 - Dans certains États, la part de crimes liés au numérique dépasse désormais celle du crime traditionnel. L'hypothèse d'un "cyber ouragan" ébranlant une multitude d'organisations n'est plus de l'ordre de la seule fiction, et les gouvernements doivent s'y préparer en mobilisant l'ensemble des acteurs privés et publics. Dans ce contexte, l'Institut Montaigne publie un nouveau rapport *Cybermenace : avis de tempête* dans lequel nous proposons une série de recommandations susceptibles de favoriser la coopération et la libération de l'information et, ainsi, l'amélioration de la cyberrésilience de notre pays.

"La cybersécurité est l'affaire de tous. Si les bénéfices apportés par le numérique ne sont plus à prouver, ces derniers ne seront pérennes qu'à la seule condition que les systèmes soient sécurisés et les données, protégées. C'est pourquoi nous en appelons à un changement de paradigme afin que la compétition face au risque cyber laisse place à la collaboration concrète entre les acteurs." **Marwan Lahoud, associé chez Tikehau Capital et président du groupe de travail.**

Les risques inhérents au numérique

Le marché du numérique est dominé par un nombre très limité d'acteurs, qui crée une **dépendance technologique forte** : c'est le cas du marché des systèmes d'exploitation et du marché des microprocesseurs. La fragilité systémique qui en découle est renforcée par l'**interconnexion croissante entre les systèmes**. Les entreprises et les administrations, en se décloisonnant et en s'ouvrant vers l'extérieur, accroissent chaque jour un peu plus leur vulnérabilité. En parallèle, l'**essor des objets connectés** et l'**adoption grandissante du *cloud*** par les entreprises contribuent également à augmenter ce risque. On estime par exemple qu'en 2020, il y aura jusqu'à 212 milliards d'objets connectés à travers le monde, contre 10 milliards en 2017 (Gartner, ABIresearch, Cisco, Idate, IDC). Les solutions apportées se heurtent à une **carence de compétences**, accrue par la **croissance constante des besoins en cybersécurité**, en hausse de 10 % par an en France. Enfin, l'essor de l'intelligence artificielle pose sans aucun doute de nouvelles interrogations, que ce soit dans la nature des cybermenaces ou dans la manière dont nous pourrons, à l'avenir, les combattre.

"***La menace cyber est en constante progression, elle change de forme en continue car les cybercriminels sont très habiles pour utiliser les dernières technologies et la moindre faille présente dans les systèmes. Pour eux, l'absence de frontière dans le cyberespace est un facilitateur et un bon moyen pour se cacher,***" ajoute Gérôme BILLOIS, associé en cybersécurité au cabinet Wavestone, rapporteur général du travail de l'Institut Montaigne.

En dépit des premières inflexions, la sphère publique demeure exposée

Depuis plusieurs années, l'État prend progressivement conscience de la nécessité de considérer le risque cyber à part entière. L'élan national a débuté en 2009, avec la création de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Avec l'entrée en vigueur de la loi de programmation militaire (LPM) en décembre 2013 et l'adoption de la directive *Network and Information Security* (NIS) par l'Union européenne en juillet 2016, 200 structures françaises de toutes tailles ont été identifiées comme "indispensables au bon fonctionnement et à la survie de la Nation". Ce sont les Opérateurs d'Importance Vitale (OIV) et les Opérateurs de Services Essentiels (OSE), qui bénéficient dès lors de dispositifs de protection accrus. Toutefois, **la culture du risque cyber reste faible au sein des ministères, institutions publiques, collectivités territoriales ou forces de l'ordre.**

Les grandes entreprises : une prise de conscience et une préparation au risque cyber inégales

Les grandes entreprises sont globalement les mieux protégées. C'est sous l'effet conjoint des exigences des consommateurs et des diverses règlementations (norme PCI-DSS, RGPD, etc.), que nombre d'entre elles ont été poussées à investir en la matière, tant dans leurs plans d'actions concrets que dans leur communication. **Toutefois, seuls 25 % des groupes du CAC40 abordent la problématique de la cybersécurité au niveau de leurs comités exécutifs et seuls 12,5 % d'entre eux annoncent avoir lancé un programme de cybersécurité** (Wavestone, 2018). Le secteur industriel, quant à lui, présente encore un niveau de protection insuffisant, alors que les activités de ce secteur impliquent une connectivité croissante.

Les TPE/PME/ETI : une situation alarmante

Ces structures **manquent de compétences et de moyens en leur sein pour se préparer et faire face à l'éventualité d'une cyberattaque**. Ce, d'autant plus qu'elles ne sont ni ciblées ni concernées par les différentes mesures initiées par l'État. SystemX évalue à 50 000 le nombre de PME victimes d'une cyberattaque en 2017, avec des dégâts significatifs pour leur trésorerie. Si 100 % des entreprises du CAC40 ont souscrit des assurances cyber, ce taux chute à 30 % pour les ETI et est plus faible encore parmi les TPE et PME. **Ce qui doit être collectivement saisi, TPE/PME/ETI comprises, c'est que n'importe quelle structure peut, aujourd'hui, faire l'objet d'une cyberattaque**. Ainsi, certaines PME sont visées pour la simple raison qu'elles travaillent pour de grandes entreprises : les liens numériques entre entreprises d'une même chaîne d'approvisionnement reflètent **une nouvelle chaîne de risques, dans laquelle l'élément le plus faible peut mettre en danger l'ensemble du groupe**, rendant plus plausible la possibilité d'un "cyber ouragan".

Nos propositions pour une amélioration de la cyberrésilience française

Mobiliser l'ensemble du tissu économique...

… pour les entreprises cotées d'une certaine taille

PROPOSITION 1 - Encourager la rédaction d'un rapport sur les risques cyber à disposition des administrateurs, voire une intégration partielle dans les rapports annuels.

PROPOSITION 2 - Mobiliser les réseaux des métiers du chiffre (experts comptables et commissaires aux comptes) pour réaliser un diagnostic cybersécurité annuel avec un cahier des charges minimum (construit avec les autorités nationales). Il serait communiqué aux dirigeants à titre d'information avec les recommandations de base pour couvrir les risques.

PROPOSITION 3 - Inciter et mobiliser les grands groupes sur leur responsabilité pour augmenter le niveau de cybersécurité de leur chaîne d'approvisionnement et de leurs fournisseurs.

… pour les secteurs critiques

PROPOSITION 4 - Inciter à la création et à la souscription d'offres cybersécurité pour les TPE/PME/ETI, en particulier des offres de connectivité réseau intégrant par défaut des mesures de sécurité de base (nettoyage du trafic), des offres d'applications métier (e.g. ERP) sécurisées par défaut et des offres de cyberassurance, incluant des services en cas d'incidents.

PROPOSITION 5 - Faire évoluer le corpus réglementaire, en particulier les textes liés à la loi de programmation militaire (LPM) 2014-2019, pour y ajouter des exigences précises de cyberrésilience (réalisation annuelle d'un exercice de crise, existence d'un système d'information de crise indépendant du système d'information nominal, introduction de diversité technologique sur les systèmes d'information d'importance vitale, etc.).

Démultiplier les compétences et être solidaire en cas de crise

PROPOSITION 6 - Créer un parcours de formation financé par l'État en contrepartie d'un engagement dans la réserve de cyberdéfense pour un nombre minimum d'années afin de réaliser un appui opérationnel en cas de crise et de maintenir les compétences (entraînement, action de prévention…).

PROPOSITION 7 - Étendre le rôle de la réserve de cyberdéfense à la résolution de crises touchant les acteurs privés et augmenter le nombre et les compétences des réservistes en en faisant la promotion auprès des acteurs du secteur privé et de la recherche académique.

PROPOSITION 8 - Proposer un cadre permettant aux acteurs privés de partager le personnel et leurs compétences avec leurs pairs en cas d'attaque.

PROPOSITION 9 - Renforcer la capacité d'échange opérationnelle de signatures d'attaques et d'informations sur les menaces *a minima* entre les entreprises stratégiques pour la nation, *via* une plateforme sécurisée d'échange opérée soit par l'État, soit par un ou des acteurs français majeurs de la cybersécurité et de confiance (avec une possible segmentation sectorielle).

Pouvoir répondre à des attaques larges et rapides

PROPOSITION 10 - Mobiliser le tissu économique et l'État autour de l'intelligence artificielle pour détecter les attaques et réagir à la bonne vitesse (et sécuriser l'intelligence artificielle pour prévenir les dérives).

PROPOSITION 11 - Définir une doctrine opérationnelle spécifique à l'échelle de l'État pour faire face à une attaque large (actions opérationnelles pour mobiliser les acteurs de l'écosystème cybersécurité dans le tissu économique privé, anticiper des actions pour isoler le pays d'Internet, pour communiquer auprès du grand public en cas de destruction des moyens de communication classiques, etc.).

PROPOSITION 12 - Inciter et donner un cadre aux entreprises sur la mise en place d'une stratégie de défense active mais sans sortir du cadre législatif en vigueur.

PROPOSITION 13 - Imposer un label de cyberrésilience pour les équipements les plus à risque pour pouvoir continuer à agir en cas de crise et préserver les vies humaines. Cela doit s'inscrire dans un mouvement de responsabilisation des éditeurs et des fabricants en imposant des mesures de fonctionnement garanti même en cas de cyberattaque pour les équipements les plus sensibles (médicaux, industrie à risque, véhicule, radio des services de secours…) et ce malgré la compromission des réseaux IT/OT/ IoT.

CLIQUEZ ICI POUR TÉLÉCHARGER LE RAPPORT

Nous vous attendons sur Twitter, Facebook et sur Instagram.
Inscrivez-vous à notre Newsletter.

Contact presse : Claire Lemoine, chargée de communication
01 53 89 05 76 - clemoine@institutmontaigne.org

À propos de l'Institut Montaigne :

Think tank indépendant créé en 2000, l'Institut Montaigne est une plateforme de réflexion, de propositions et d'expérimentations consacrée aux politiques publiques en France et en Europe. Ses travaux sont le fruit d'une méthode d'analyse et de recherche rigoureuse et critique, ouverte sur les comparaisons internationales. L'Institut Montaigne, association à but non lucratif pionnière en France, réunit des chefs d'entreprise, des hauts fonctionnaires, des universitaires et des personnalités issues d'horizons divers. Ses financements sont exclusivement privés, aucune contribution n'excédant 1,5 % d'un budget annuel de 4,5 millions d'euros. À travers ses publications et les événements qu'il organise, l'Institut Montaigne souhaite jouer pleinement son rôle d'acteur du débat démocratique.