Pannes électriques, incendies, sabotages :

RISQUES

L'Assemblée nationale a démarré mercredi l'examen du projet de loi résilience qui doit imposer à de nombreux secteurs économiques « vitaux » de mieux anticiper les risques extrêmes.

Une semaine après la panne géante espagnole, la vulnérabilité des entreprises refait surface.

Matthieu Quiret

Transports à l'arrêt, paiements numériques et télécommunications en panne, stockages alimentaires périmés, eau potable coupée dans certaines villes. La panne électrique espagnole, il y a une grosse semaine, a montré à quel point les entreprises étaient vulnérables.

La catastrophe n'a pas duré assez longtemps pour virer au drame, mais la piqûre de rappel est sévère. « *La crise espagnole est salutaire pour que les entreprises réalisent à quel point les risques se multiplient au-delà des cyberattaques* », pointe Philippe Latombe, député Modem de la 1re circonscription de Vendée. Mercredi, la commission spéciale qu'il préside a abordé le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité.

Ce nouveau texte, déjà voté en mars au Sénat, est la transcription française de trois directives européennes (REC, Dora et NIS 2) qui ont été rapprochées dans un seul projet de loi tant les sujets d'anticipation des risques sont proches. C'est une marche supplémentaire pour les entreprises.

Depuis 2006, environ 300 opérateurs d'importance vitale (OIV) dans une douzaine de secteurs doivent avoir un plan de protection des 1.500 sites sensibles (usines, locaux d'une administration, centres de données, etc.) qu'ils gèrent. La nouvelle réglementation va d'abord ajouter à cette liste plusieurs secteurs d'activité, comme les gestionnaires de réseaux de chaleur, la filière hydrogène ou les stations d'épuration.

Elle fait aussi évoluer la doctrine d'une logique de protection des sites à celle d'une stratégie de résilience à un événement extrême. « *Les menaces sont devenues tellement nombreuses et les attaques informatiques tellement régulières que la question n'est pas de préserver les sites mais de maintenir les services vitaux, au maximum* », explique Olivier Cadic, le sénateur centriste des Français de l'étranger qui préside la commission spéciale de la Chambre haute. « *Auparavant, on demandait à un hôpital de déployer des pare-feu autour de son informatique. Maintenant, on va exiger qu'il réapprenne à travailler avec du papier et un crayon* », illustre encore Philippe Latombe.

Enfin, le texte introduit des sanctions si l'entreprise ne se prépare pas correctement, avec des montants allant jusqu'à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial, puis 5.000 euros par jour de non-conformité. Un dispositif censé se substituer au régime de sanction pénal jusqu'ici en vigueur et jamais appliqué.

Un bâton qui n'effraie pas les grandes entreprises et leurs responsables des risques, représentés à l'Association pour le management des risques et des assurances de l'entreprise (Amrae). « *Le texte devrait faire l'objet d'un consensus,* anticipe Philippe Cotelle, coprésident de la commission cyber de l'Amrae, et risk manager d'Airbus Defence & Space. *En Europe, on a besoin de se réveiller et de réaliser que les entreprises sont menacées.* »

Le risque pandémie décline doucement

Tous les experts ont encore en tête quelques exemples spectaculaires de grosses failles chez les opérateurs sensibles. En 2018, plusieurs gares parisiennes avaient été paralysées, en plein départs de vacances, à cause de l'incendie d'un poste d'alimentation électrique. L'été dernier, juste avant les Jeux Olympiques de Paris, plusieurs petits sabotages attribués à des groupuscules d'extrême gauche avaient suffi à stopper la circulation des TGV. Autre cas d'école régulièrement cité, la ferme de données d'OVH à Strasbourg partie en fumée… avec les données sensibles de bien des entreprises.

A l'étranger, on garde à l'esprit les mégafeux de Californie, les inondations de Valence, en Espagne, ou encore les sectionnements de câbles sous-marins en Baltique.

Pour Clotilde Marchetti, qui pilote l'offre risques extrêmes au cabinet de conseil Grant Thornton France, il faut de tels événements pour que les entreprises mettent le sujet en haut de la liste des priorités. Au lendemain de la panne espagnole, elle expliquait « aux Echos » : « *Je pense que le sujet panne électrique va remonter dans le Top 5 des risques majeurs dans toutes les cartographies des risques. Comme la pandémie, qui était devenue un non-sujet depuis la grippe aviaire en 2009, est remontée tout de suite après le Covid puis est en train de redécliner tout doucement.* »

Le texte, dont le vote définitif n'est pas attendu avant la fin de l'année, devrait donner un coup de fouet dans la culture du risque des entreprises. D'autant que « *80 % des problèmes sont généralement des erreurs d'origine humaine* », rappelle Olivier Cadic. Il cite le cas récent d'une grande organisation qui s'est fait hacker à cause d'un responsable du réseau informatique, qui a laissé son mot de passe fuiter. Une erreur de débutant qui a paralysé le système pendant quinze jours. Pour les parlementaires, les industriels de l'armement sont les plus mûrs sur le sujet, tant ils sont la cible de menaces (espionnage, sabotages) et par la nature sensible de leurs activités. Mais même ce secteur doit progresser. « *EDF anticipe bien les risques environnementaux, comme la nécessité de stopper des centrales en cas de chaleur extrême et de manque d'eau, car c'est le cœur de leur activité. Mais le site de Safran de Montluçon, qui équipe les drones, est-il bien préparé aux feux de forêt ?* » interroge le député Philippe Latombe.

> « En Europe, on a besoin de se réveiller et de réaliser que les entreprises sont menacées. »
>
> **PHILIPPE COTELLE**
> Risk manager d'Airbus Defence & Space

Pour les entreprises, ces nouvelles obligations risquent d'apparaître comme des énièmes contraintes. C'est pourquoi la ministre chargée du Numérique, Clara Chappaz, s'est opposée à la tentative de certains parlementaires d'étendre les obligations des entreprises à leurs fournisseurs.

Anticipant la critique, le sénateur Olivier Cadic balaie aussi d'emblée le sujet des surcoûts induits pour les entreprises : « *Il est sans commune mesure avec les dégâts subis lors d'une attaque.* » A l'Amrae, Michel Josset, par ailleurs directeur assurance-prévention de l'équipementier Forvia, rappelle que les équipes risques du CAC 40 se limitent à une poignée de salariés. Il y a un donc un surcoût humain à prévoir. Quant à l'équation financière, elle est complexe. Entre le coût d'assurance, celui des risques non assurables, celui des investissements de protection et de résilience, les entreprises naviguent sur une ligne de crête, appuie Michel Josset. ■

L'incendie, le 7 avril, d'un centre de tri des déchets à Paris. *Photo Florian Poitout/ABACA*

Pourquoi les distributeurs français sont des « cibles intéressantes » pour les cybercriminels

Les enseignes françaises de la grande distribution sont des cibles de choix pour les cybercriminels. Avec une hausse mondiale de 33 % des attaques en 2024 dans ce secteur, les vols de données clients et les rançongiciels se multiplient.

Julia Lemarchand

C'est une cyberattaque particulièrement virulente. L'offensive à laquelle doit faire face depuis le week-end de Pâques le secteur britannique de la distribution s'éternise. Elle aurait déjà privé Marks & Spencer de 30 millions de livres sterling de revenus. Une telle situation pourrait-elle se produire de ce côté-ci de la Manche ? « *Des attaques de grande ampleur se sont déjà produites dans ce secteur en France et se reproduiront dans le futur* », prévient Yoann Kassianides, délégué général de l'Alliance pour la confiance numérique. Ce syndicat professionnel représente les entreprises du secteur de la cybersécurité, un marché de près de 19 milliards d'euros de chiffre d'affaires et en forte croissance (+10 % chaque année).

Dans son dernier rapport, publié la semaine dernière, la Commission nationale de l'informatique et des libertés (CNIL) signale un doublement des cyberattaques de grande ampleur, soit une quarantaine de violations de données personnelles touchant, à chaque fois, plus d'un million de personnes. « *Tous les secteurs d'activité sont touchés* », souligne la CNIL, qui cite parmi les victimes Auchan, Boulanger, Cultura et Truffaut, aux côtés de France Travail, Free, ou encore la plateforme de streaming Molotov. Ni la CNIL, ni l'Agence nationale de la sécurité des systèmes d'information (Anssi) ne souhaitent indiquer si le secteur de la grande distribution est plus ciblé que d'autres.

Trois grands types d'attaques

Le dernier bilan du cabinet Check Point Research montre que les acteurs du retail, avec 1.415 attaques par semaine en 2024 dans le monde, sont loin d'être les premières cibles des cybercriminels. L'enseignement et la recherche, les administrations et le secteur de la santé, cibles favorites, sont deux fois plus touchés. Reste que les opérations affectant le commerce ont bondi de 33 % l'an dernier (à relativiser toutefois au regard de la hausse moyenne à 44 %, tous secteurs confondus).

« *Toutes les semaines, nous faisons face à des attaques,* nous confie sous couvert d'anonymat un patron de la grande distribution, *avec plusieurs centaines de magasins.* » Un classique, rappelle-t-il, c'est le vol des identifiants et mots de passe liés aux cartes de fidélité, dont « *les cagnottes sont vidées en quelques secondes* ».

Les cyberattaques de grande ampleur ont doublé. *Photo iStock*

Un responsable informatique d'une autre enseigne de la distribution spécialisée témoigne également : « *Nous repérons, tous les jours, des activités malveillantes. Et une fois par mois, en moyenne, nous traitons une attaque sérieuse.* »

Au total, ce sont 700 événements que son équipe de 20 personnes gère chaque année, avec des pics pendant les périodes de vacances, comme Pâques ou les ponts de mai.

Trois grands types d'attaques reviennent régulièrement : des vols de données clients (comme pour les cartes de fidélité) ; des « coups de bluff » de criminels qui font du chantage avec des fausses bases de données qu'ils menacent, par exemple, de vendre ou de rendre publiques contre de l'argent ; et enfin les rançongiciels, utilisés dans les dernières attaques outre-Manche, qui consistent à prendre en otage une partie du système d'information (le système d'encaissement, le site ecommerce…).

Dans ce dernier scénario, « *les attaquants utilisent des outils d'ingénierie sociale, autrement dit toutes les informations que laissent les clients ou les salariés en source ouverte (mails, réseaux sociaux, achats en ligne…). Grâce à cela, ils s'introduisent dans les systèmes avant de remonter jusqu'aux administrateurs. Ils exfiltrent les bases de données, puis effacent leurs traces avant d'attaquer et demander de l'argent* », explique Yoann Kassianides, qui estime que M&S devait avoir des systèmes infectés depuis déjà six à neuf mois.

Des surfaces d'attaques importantes

Selon les experts, les enseignes de commerce sont « intéressantes » pour les cybercriminels à plusieurs titres : en plus de brasser d'importants flux financiers, ces organisations sont très ouvertes, avec d'importantes bases de données clients. Elles disposent également de systèmes d'information nombreux et interconnectés avec des milliers de fournisseurs et de partenaires qui, eux, ne sont pas toujours aussi bien protégés que ces gros acteurs. « *Les distributeurs ont des surfaces d'attaque très larges* », résume Yann Bonnet, directeur général délégué du Campus Cyber, qui fait part d'une hausse d'attaques passant justement par les chaînes d'approvisionnement et les PME. Sans compter une démocratisation des moyens d'attaque depuis deux, trois ans : ce qu'on appelle le « ransomware as a service » (RAAS). « *Ce sont des experts qui donnent les moyens à d'autres d'opérer sous franchise. Les criminels mutualisent les moyens, ce qui élargit le scope des cibles* », explique Yoann Kassianides.

Les solutions existent pour se prémunir des attaques : former les salariés, cartographier les zones de risque, mettre en place des systèmes de chiffrement, faire travailler des hackers éthiques pour challenger les systèmes, ou encore simuler des crises.

> Les opérations affectant le commerce ont bondi de 33 % l'an dernier.

C'est ce que prépare l'Anssi : un exercice de crise cyber de grande ampleur baptisé « REMPAR25 » qui se déroulera le 18 septembre 2025, partout en France. « *A ce stade, nous dénombrons plus de 600 entités (publiques et privées) inscrites afin d'entraîner différents métiers et compétences au sein de leur organisation (dirigeants, métiers du numérique, du juridique, des RH et de la communication)* », fait savoir aux « Echos » l'agence, qui a réalisé un premier exercice en 2022 mais dans un format plus réduit. Il est fort à parier que des distributeurs se sont portés volontaires. Les structures intéressées, peu importe leur taille ou leur secteur d'activité, ont jusqu'au 10 mai pour se manifester. ■

les entreprises vont devoir prévoir le pire

Une menace pas si fantôme

LE REGARD DU JOUR **ÉCONOMIQUE** *de* **David Barroux**

Les militaires nous ont appris que si nous voulions la paix, nous devions nous préparer à la guerre. Les directions des risques se doivent de préparer les entreprises à éviter les séismes économiques en anticipant le pire. Et leur fonction est de plus en plus centrale et vitale, tant la liste des catastrophes qui menacent les entreprises ne cesse de s'allonger. Car au-delà des traditionnels incendies, coupures d'eau, d'électricité ou de services de télécommunications, ce sont désormais les attaques physiques mais surtout cyber qui peuvent annihiler toute activité économique.

La menace étant croissante et protéiforme, les directions doivent déjà apprendre à hiérarchiser les risques. Il y a ceux contre lesquels on ne peut pas grand-chose. On ne pourra jamais se protéger totalement contre un feu, un cyclone ou la défaillance d'un acteur de l'énergie ou des télécoms.

On peut certes multiplier les groupes électrogènes, investir dans un système de communication de secours par satellites ou multiplier les murs pare-feu, mais les dépenses devant être consenties sont si élevées que toutes les entreprises ne peuvent pas investir dans de tels dispositifs. Il faut donc être prêt à investir de façon raisonnable pour limiter les conséquences des catastrophes contre lesquelles on ne peut guère se prémunir et qui sont de nature à provoquer des pertes peut-être importantes, mais limitées dans le temps. Car il y a des catastrophes dont on peut se relever et celles qui vous tuent. Et il faut avoir conscience que dans notre monde numérique, les menaces les plus lourdes sont immatérielles. Se faire siphonner toute sa trésorerie, pirater ses brevets ou sa propriété intellectuelle, perdre l'accès à ses bases de données… voilà bien le cœur de la nouvelle cartographie des risques. On peut mettre sur pied un plan de continuation et redémarrer après un tremblement de terre. On ne pourra pas se relever si on a perdu toute sa mémoire numérique. On peut bien sûr investir dans la cybersécurité et dupliquer ses bases de données dans le cloud, mais l'essentiel n'est pas de voter des lois pour pousser les entreprises à prendre plus au sérieux cette menace. Ce sont les géants du cloud et du numérique qu'il faut mieux encadrer et réguler tant ils sont devenus vitaux. ■

« Il faut de véritables exercices de crise dans les entreprises »

FRANCK GALLAND
Fondateur de d'Environmental Emergency & Security Services

Pourquoi renforcer la réglementation ?

La première chose importante, c'est que ce texte permet une harmonisation à l'échelle européenne. Dans un contexte de guerre hybride depuis le conflit en Ukraine, les infrastructures critiques des pays membres font l'objet de ciblages délibérés. En Allemagne, la Deutsche Bahn a été touchée en 2022. Même chose en Pologne ou dans les pays Baltes, des infrastructures critiques ont connu des actions délibérées de sabotages physiques. Il y a également, au sein des entreprises, une psychose cyber justifiée, mais il ne faut pas oublier que dans les infrastructures, la défaillance technique et le risque incendie restent les menaces prioritaires.

L'extension de la vigilance à des secteurs comme l'assainissement n'est-elle pas exagérée ?

On a aujourd'hui d'énormes stations d'assainissement qui couvrent plus de 500.000 habitants, essentielles pour protéger la ressource en eau, et qui concentrent aujourd'hui beaucoup de risques, notamment autour du biogaz. De ce point de vue, il n'était pas normal que l'assainissement n'ait pas été désigné secteur d'activité d'importance vitale par le passé, il n'y avait que l'eau potable. Même chose, par exemple, pour le chauffage urbain ou les data centers qui sont critiques pour l'économie.

Quelle leçon tirer de la panne espagnole ?

Tout le monde l'a oublié mais, le 19 décembre 1978, la défaillance d'un câble très haute tension de 400.000 volts, dans l'est de la France, avait provoqué un black-out sur la région francilienne. Des problèmes peuvent également arriver sur des postes de transformation, dont certains alimentent directement en 63.000 volts des usines critiques pour l'eau potable. La crise espagnole souligne les risques croissants liés aux interdépendances. Ils sont de trois natures : électriques, télécoms mais aussi liés aux automatismes. Aujourd'hui, on a des usines modernes entièrement automatisées, ce qui empêche une reprise en mode manuel comme auparavant. Il faut vraiment anticiper tout problème sur les automates, et faire monter en compétence une profession devenue stratégique pour les installations critiques : celle d'automaticien.

Que doivent faire les entreprises face à ces risques ?

En matière de prévention des incidents, il s'agit de connaître ses vulnérabilités, en termes d'interdépendance amont notamment. C'est également avoir une culture de la gestion de crise que nous n'avions que de manière perfectible dans les secteurs d'activité d'importance vitale. Culture de la crise qui oblige à avoir une organisation de réponse à incident, une salle de crise, une capacité de traçabilité sous forme de main courante… C'est très important, le nouveau texte impose d'avertir l'Etat des difficultés vécues, comme c'était déjà le cas pour le risque cyber dans la réglementation NIS (sur la sécurité des réseaux et de l'information).

Ces plans de résilience ne sont-ils pas très théoriques ?

A entraînement difficile, guerre facile. Les comex des grandes entreprises pratiquent bien et depuis longtemps des exercices de crise sur des situations diverses et variées : attaque terroriste, prise d'otage, etc. C'est très bien. Mais aujourd'hui, dans le cadre de ce nouveau texte, il faudra plus de mises en condition opérationnelle, de véritables exercices de crises d'exploitation qui répondent aux ruptures de continuité de service à la suite d'un événement climatique extrême, à un problème d'alimentation électrique, à des incidents techniques, etc. Ceci en mettant les équipes à rude épreuve sur le terrain, en testant leur cohésion face aux situations rencontrées, en créant une bonne interface avec les services de l'Etat et avec les primo-intervenants que sont les sapeurs-pompiers, les forces de police et de gendarmerie. Mon cabinet organise ce type de test tous les deux mois pour Veolia, ou pour des régies publiques de l'eau.

Dans les grands contrats de délégation de services publics, les autorités organisatrices exigent d'ailleurs de plus en plus la tenue d'exercices, avec des élus locaux qui ont besoin d'être rassurés sur les capacités de résilience de leurs délégataires. La semaine dernière, nous avons ainsi organisé pour l'exploitant de fermes éoliennes Virya Energy la simulation d'un feu sur une turbine et l'évacuation par les pompiers spécialisés d'un collaborateur coincé en haut d'un mât. On a joué les choses en vrai et cela rassure tout le monde.

L'Etat aura-t-il vraiment les moyens de vérifier la pertinence de tous ces plans de résilience ?

C'est le sujet, oui. La réglementation introduit un système de sanctions. Pour cela, il faut un corps de contrôle, notamment pour s'assurer qu'à la suite des incidents remontés, les mesures correctives ont été apportées. Ce corps de contrôle, ça peut être typiquement ce qui se fait avec les DREAL *[services environnement des préfectures, NDLR]* au niveau de sites classés. Mais il peut également s'inscrire dans une logique de partenariats public-privé, permettant à des cabinets externes de procéder aux audits. C'est ce que nous faisons déjà auprès d'opérateurs critiques du Luxembourg. La France a de ce point de vue de nombreux intervenants possibles qui font déjà du contrôle-incendie comme Socotec, Apave, etc.

— *Propos recueillis par* ***M. Q.***

« Il y a au sein des entreprises une psychose du risque cyber justifiée mais il ne faut pas oublier que dans les infrastructures, la défaillance technique et le risque incendie restent les menaces prioritaires. »