Faire face à la menace du risque cyber

Tout le monde est concerné par le risque Cyber : particuliers, collectivités locales, établissements de santé, administration, petites et grandes entreprises. Chaque jour, les exemples d'attaques sont nombreux, qu'il s'agisse des médias ou de l'entourage proche.

FLORENCE PICARD,

Actuaire certifié de l'Institut des actuaires Membre du Directoire de la Fondation du Risque

Quelles sont les menaces ?

Les menaces résultent de la conjonction de stratégies malveillantes des attaquants et de failles de protection des victimes (humaines ou techniques).

Elles ont des objectifs variés. Menées par des « entreprises » du crime motivées par l'argent, elles agissent souvent par rançonnage. Elles peuvent aussi servir des intérêts privés, ou agir pour des Etats, notamment par espionnage industriel, ou simplement pour nuire : porter atteinte à l'image ou saboter des outils de production ou de service.

Nous nous limiterons ici au domaine économique, sachant que la défense nationale joue un rôle clé dans la guerre cyber.

Car il s'agit d'une forme de guerre, silencieuse, atypique, qui concerne chaque acteur de l'économie et ne relève que partiellement de la Défense Nationale car il s'agit d'actes qui, pris individuellement, ont une motivation lucrative, mais qui servent au final des opérations de déstabilisation géopolitique.

Contrairement aux risques habituellement assurés (risque automobile, incendie, perte d'exploitation, catastrophes naturelles, etc..), il n'y a rien de naturel dans cette menace qui utilise la technologie au service de stratégies d'attaques criminelles.

Il s'agit d'une véritable économie souterraine composée d'entreprises structurées, employant des ingénieurs compétents (et cupides), « travaillant » en direct mais aussi via des « affiliés » autorisés à utiliser leurs logiciels moyennant une rétrocession sur les gains, et souvent, le respect de certaines règles de comportement (sorte de « code d'honneur »), pour ne pas gâcher le marché en attaquant des cibles populaires. Ils sont d'ailleurs parfois débordés par ces affiliés moins intelligents dans leur cupidité, comme en atteste les attaques contre les hôpitaux, tel que celui de Corbeil Essonne.

Les ingénieurs de cyber sécurité des entreprises déploient des moyens de plus en plus importants pour sécuriser les systèmes informatiques (SI) et faire barrage aux attaquants. L'Intelligence Artificielle commence à les aider dans la détection et la prévention des attaques.

Mais souvent, les intrusions dans les systèmes d'information s'effectuent via des messages piégés (phishing) et ce sont les victimes elles-mêmes qui ouvrent la porte aux hackers (en cliquant sur un lien frauduleux par exemple).

Quels sont les risques pour une entreprise ?

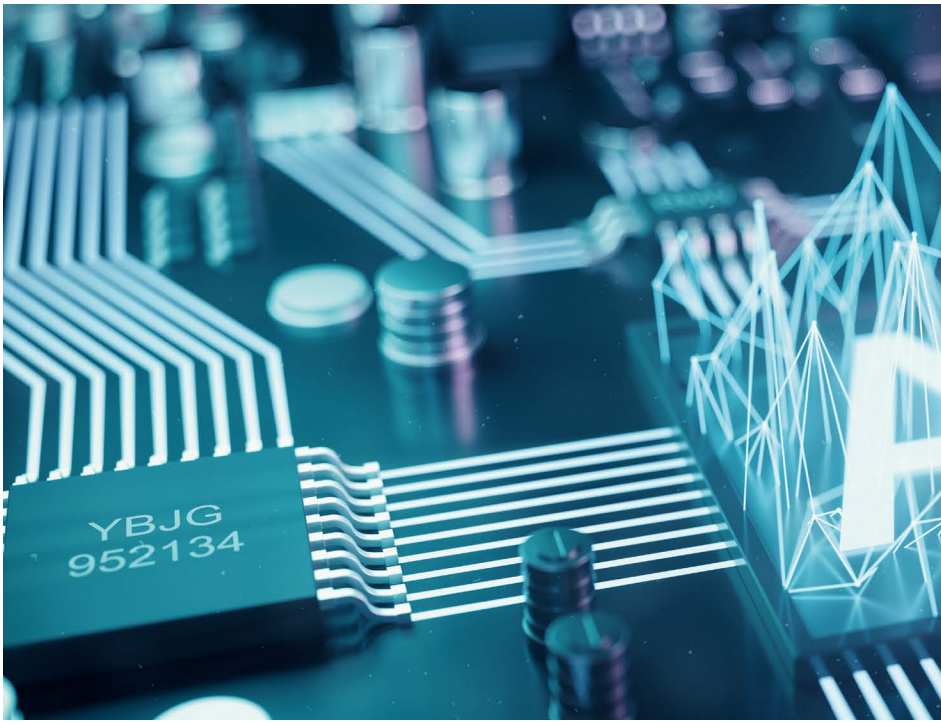
Une entreprise peut être spécifiquement visée par une attaque, mais elle peut aussi être victime du caractère viral de certaines attaques, par exemple via un prestataire lui-même infecté. Ce caractère systémique peut provoquer une diffusion de nombreux sinistres, dans tous les pays à la fois, affectant des entreprises de tous secteurs d'activité et de toutes tailles (exemple des rançongiciels WannaCry et Petya en 2017).

Les types d'attaques sont assez nombreux : parmi les plus fréquentes citons le « deni de service » et le « vol de données » avec demande de rançons pour les restituer.

Une attaque par deni de service rend le service inaccessible par saturation de demandes ; c'est un type d'attaque très efficace quand l'entreprise a pris des engagements de rendre un service dans un délai donné (c'était le cas pour TV5 Monde en 2015).

Le vol de données avec cryptage les rend inutilisables et payer la rançon pour les récupérer n'est pas une solution recommandée car non seulement les hackers ne rendent pas toujours les données non cryptées, mais surtout, cela alimente les industries criminelles du dark web qui ont pris une importance considérable : drogues et armes à feu, payables en Bitcoin, plateforme de financement participatif pour organiser toutes sortes de crimes, notamment les trafics d'armes et de stupéfiants, voire même des assassinats.

Pour l'entreprise, c'est l'arrêt de tout ou partie du SI et de l'activité de l'entreprise qui constituent le risque principal de la menace : perte d'exploitation, de production, de commercialisation, de clientèle, surcoût pour pallier partiellement l'arrêt du SI par l'embauche de temporaires. Le délai de récupération d'un fonctionnement normal est souvent très long : plusieurs mois. C'est aussi le cas pour les villes : Angers en 2021, Atlanta en 2018 en sont des exemples. Plus d'un an après, Angers en subissait encore les conséquences, notamment



pour la réservation de places en crèches encore à l'arrêt, malgré près d'un milliard d'euros dépensés. Selon l'ANSII, Agence nationale de la sécurité des systèmes d'information, il faut environ deux ans à une ville attaquée pour se remettre sur pied.

Pour les petites entreprises, mal protégées, et mal préparées, le risque cyber peut être vital. Malheureusement, faute d'une obligation de déclaration des attaques, il n'existe pas de statistiques fiables.

Comment répondre à ces menaces : cyber sécurité et formation du personnel

Pendant quelques temps, la cyber sécurité a espéré pouvoir assurer à elle seule la protection des systèmes d'information (SI), le SI étant vu comme un château fort qu'il faudrait rendre imprenable.

Il est ensuite apparu évident que, au-delà de l'informatique, c'est l'ensemble du personnel de l'entreprise qui était concerné pour éviter que les collaborateurs contribuent aux attaques par manque de vigilance. Des formations, suivies de training réguliers, sont maintenant une pratique courante dans les grandes entreprises pour le respect des « gestes barrière Cyber ». Elles

ne garantissent pas l'absence d'erreur humaine, mais de gros progrès ont été réalisés. Au-delà de l'entreprise, c'est même chaque citoyen qui est concerné, car les bots (robots), qui lancent des attaques Ddos (deni de service), sont parfois dormants dans des machines appartenant à des particuliers.

Malheureusement la situation est différente pour les petites PME et TPE, qui disposent rarement d'un directeur informatique, encore moins d'un spécialiste de la sécurité et qui n'ont pas toujours connaissance des outils très pratiques et efficace mis à leur disposition par le GIP ACYMA.

Vivre avec la menace

Il faut se rendre à l'évidence : nous devons apprendre à vivre avec cette menace, comme c'est le cas avec la Covid ou avec les nouveaux risques climat ou géopolitique.

L'idée n'est plus seulement de se protéger de la menace, mais d'apprendre à agir de la façon la plus appropriée si elle se réalise, afin de minimiser l'impact d'une attaque réussie : prendre les bonnes décisions dans les premières minutes du sinistre, chacun sachant exactement ce qu'il a à faire, cela se prépare dans un bon plan de crise, alliant technique informatique et organisation des activités. Restaurer au plus vite un SI endommagé, mettre en place les solutions alternatives de fonctionnement prévues dans le cadre du plan de crise, se protéger par des process d'organisation du travail conçus « by design » pour que l'activité soit moins dépendante du SI, il s'agit bien de ne pas s'épuiser en cherchant à tout éviter, mais parallèlement à l'éducation de toute la population et aux mesures de prévention qui sont essentielles, de travailler en amont d'une éventuelle attaque pour accélérer la capacité à restaurer le SI et les données au plus vite, car c'est le temps d'arrêt d'activité qui coûte cher. Pour cela il faut identifier les activités dont la mise à l'arrêt est le plus dommageable, pour prévoir des solutions de contournement avec des fonctionnements en mode dégradé.

Ainsi, le risque cyber confère une importance capitale à la prise en compte des risques opérationnels et à leur analyse fine, activité par activité, et avec leurs interactions.

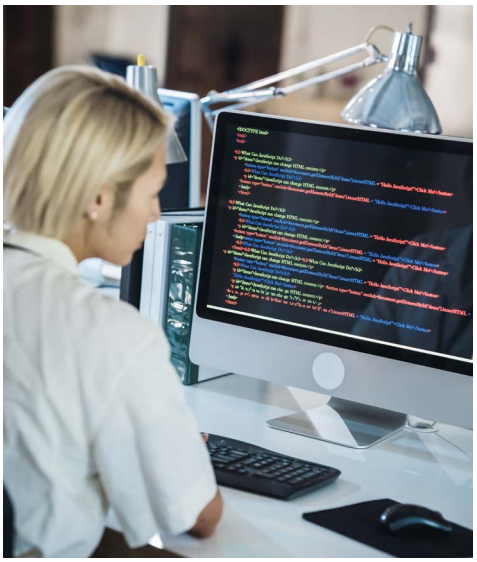
Le législateur a pris des mesures pour garantir que les grandes entreprises du système financier prennent tous les moyens nécessaires et allouent les budgets adéquats. La responsabilité des dirigeants est engagée, notamment au travers de la loi NIS2.

Un plus large ensemble d'entreprises sera bientôt concerné par la loi Dora.

Mais quand l'attaque est là, que le SI a été infecté ou piraté, il est important, pour la valeur économique et la pérennité de l'entreprise, de disposer de l'indemnisation d'un contrat d'assurance et de l'assistance technique souvent proposée avec ces contrats.

A cet égard, après avoir accompagné le marché et essuyé des pertes, en l'absence de données pour évaluer le risque, les assureurs et les réassureurs sont devenus prudents car il y va de leur solvabilité : ils ne peuvent pas supporter les risques systémiques qui relèvent de la solidarité nationale.

Ils sont d'autant plus handicapés pour assurer ce risque que, outre l'absence



de données, la réglementation n'est pas adaptée : à l'inverse des captives que peuvent créer les entreprises, les assureurs n'ont pas le droit de mutualiser le risque dans le temps, ce qui leur permettrait de lisser sur plusieurs années les pics des grands sinistres.

Si l'on veut que les assureurs puissent jouer leur rôle, il est indispensable que la réglementation les autorisent à constituer des provisions pour égalisation.

Bien connaître les impacts économiques de la menace pour protéger efficacement le tissu des entreprises

Tout l'effort actuel des pouvoirs publics (1 milliard affecté au plan de cyber sécurité en 2021) porte sur la prévention et la sécurité informatique, mais pas sur la protection financière ni la connaissance de la dimension économique du risque, pourtant non maîtrisable par la technologie, à court-moyen terme.

Le Campus Cyber initié par le Président de la République, inauguré en février 2022, est le lieu totem de la cybersécurité. De gros moyens financiers y sont consacrés et nul doute que des solutions techniques vont émerger, notamment par un dialogue à établir entre ingénieurs de sécurité et spécialistes de l'Intelligence artificielle.

La dimension technologique est certes essentielle mais l'écosystème cyber doit non seulement bénéficier de la prévention et la remédiation technique, mais aussi de la protection et la remédiation financière, comme pour tous les risques car, malgré les meilleurs efforts de prévention, il n'existe pas de risque zéro.

Le choix a été fait de protéger les grands groupes et de leur permettre de s'organiser pour disposer des provisions nécessaires en cas de sinistre.

Mais c'est tout le tissu industriel qui devrait l'être. Or rien n'est fait à ce niveau. La mort de petites entreprises emportées par une attaque et la perte des emplois concernés n'est pas une sanction méritée. Il faut pouvoir permettre aux petites entreprises de disposer, à un prix abordable, d'une couverture financière à la hauteur des dommages.

Bien connaître ce risque nouveau, très particulier, est une nécessité pour que les assureurs puissent organiser des mutualisations et intervenir massivement sur la partie aléatoire. Le risque systémique et les évènements exceptionnels mériteraient de bénéficier par ailleurs d'un système de solidarité inspiré du régime des catastrophes naturelles.

Connaître le risque nécessite la collecte et le partage des données de façon sécurisée afin d'avoir une observation holistique de la menace et que chaque assureur mène sa politique de souscription en connaissance de cause, comme c'est le cas par exemple s'agissant de la mortalité.

Or pour le moment, rien n'est fait pour l'Observatoire de la menace. Prévu dans les statuts du GIP ACYMA comme l'une de ses 3 missions, il ne fait plus partie du programme de travail de ce Groupement d'intérêt public.

Un effort national pour la création d'un observatoire du risque est pourtant indispensable pour permettre d'évaluer et d'organiser la solidarité financière par la mutualisation.

Car faire face à la menace, c'est observer et mesurer ces dommages et leur contexte de survenance, pour bien connaître le risque et préserver le tissu économique de ses impacts à la fois techniques et financiers. ■