Les entreprises face aux cyberattaques

Vers un bouclier européen contre les cyberattaques

Les entreprises face aux cyberattaques

La Commission européenne souhaite renforcer la cybersécurité dans l'UE. Les entreprises sont particulièrement visées par les cyberattaques qui sont capables de menacer leur survie.

L'actualité

Le commissaire européen au Marché intérieur, Thierry Breton, a annoncé mercredi dernier la création d'un « **bouclier cyber européen** ». Cette infrastructure, qui « scannera » le réseau internet en Europe « à l'aide de technologies d'intelligence artificielle », a pour objectif de détecter les cyberattaques en « quelques heures », contre « 190 jours » en moyenne à l'heure actuelle.

Les cyberattaques ont augmenté de 140 % en un an sur le territoire européen, a précisé Thierry Breton. Il souhaite par ailleurs renforcer « la sécurité et la résilience des infrastructures critiques », en priorité dans les secteurs de l'énergie, des transports et du numérique, en mettant en place « des scénarios d'attaque ». Ces mesures seront incluses dans **un nouveau règlement, le Cyber Solidarity Act**, que la Commission européenne, codétentrice du pouvoir exécutif de l'UE avec les États membres, doit présenter mardi prochain.

« Une cyberattaque est une atteinte à des systèmes informatiques réalisée dans un but malveillant », explique sur son site le gouvernement français. Elle peut viser différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, des équipements périphériques tels que les imprimantes ou encore des appareils communicants comme les téléphones mobiles. Les entreprises sont visées pour divers motifs, tels que le vol de données, l'extorsion d'argent, l'espionnage ou encore le sabotage.

Les entreprises ciblées

Depuis ces dernières années, les pirates informatiques ciblent prioritairement les entreprises, plus rentables à attaquer que les particuliers, expliquait un rapport sénatorial de 2021. Les attaques pour voler leurs données ou bloquer leurs systèmes se sont multipliées. Les attaques par rançongiciel, un programme qui chiffre les fichiers pour les rendre inaccessibles jusqu'au paiement d'une rançon, se sont fortement développées.

Les grands groupes ont pris « des mesures de défense », ce qui a eu « comme contrepartie de détourner la cybercriminalité » vers les petites et moyennes entreprises. Ces dernières ont représenté 40 % des attaques par rançongiciels en 2022, devant les collectivités territoriales (23 %) et les établissements publics de santé (10 %), selon l'Anssi, l'autorité nationale en matière de sécurité et de défense des systèmes d'information. « Une entreprise peut fermer après une cyberattaque », rappelait le rapport du Sénat. Les coûts sont multiples : perte d'exploitation liée à l'arrêt des systèmes, frais de gestion de crise et de communication, frais juridiques en cas de vol de données, etc.

La vulnérabilité des salariés

Le budget que les entreprises consacrent à la cybersécurité a plus que quadruplé entre 2019 et 2022, selon le panorama mondial de l'assureur Hiscox. Pour sécuriser leurs systèmes, les entreprises recourent à différents outils et technologies, comme la sauvegarde des données et la cryptographie. La formation des salariés aux risques reste souvent insuffisante. Le phishing, un type d'attaque qui consiste à envoyer, sur une messagerie professionnelle ou privée, un mail contenant un lien piégé, est « le point d'entrée numéro un pour les pirates informatiques (62 %) pour infiltrer avec succès les entreprises », selon Hiscox. Le « shadow IT », c'est-à-dire l'ensemble des outils (mails, réseaux sociaux, etc.) utilisés par les collaborateurs sans avoir été approuvés par le service informatique, constitue également « un terrain propice aux cyberattaques », notait le cabinet d'analyse économique Xerfi dans une note de 2022.

48 % des entreprises interrogées dans le cadre d'une étude ont déclaré avoir été confrontées à au moins une cyberattaque en 2022, selon le rapport [PDF] de Hiscox portant sur les États-Unis et neuf pays européens, dont la France. Les principales attaques étaient l'utilisation abusive des ressources informatiques, par exemple pour voler des données, le détournement de paiement et les rançongiciels. Les deux tiers des entreprises visées par un rançongiciel ont payé la rançon, selon le même rapport.

L'assurance du risque cyber

Les premières offres d'assurance concernant le risque « cyber » sont apparues aux États-Unis dans les années 1990. En 2021, en France, 84 % des grandes entreprises étaient couvertes, mais moins de 0,3 % des PME, selon l'Amrae, une association professionnelle. Dans un rapport de 2022, la direction générale du Trésor, une branche du ministère de l'Économie, recommandait de développer ce marché pour « renforcer la résilience » de l'économie française. Elle estimait le risque cyber « maîtrisable » pour les assureurs, dans la mesure où « 97 % des sinistres » couverts en 2021 ont donné lieu à une indemnisation « inférieure à 3 millions d'euros ». Promulguée en janvier, la **loi Lopmi** prévoit à partir du 24 avril le remboursement par les compagnies d'assurance des rançons pour les entreprises assurées contre ce risque, à condition qu'une plainte soit déposée dans les 72 heures. Début février, le Cesin, une association de professionnels de la sécurité de l'information, notait une « forte hausse des tarifs » des assurances avec « des niveaux d'exigences de la part des assureurs quasiment inatteignables ».

La France et l'UE ont adopté plusieurs textes visant à améliorer la cybersécurité. Les entreprises sont par exemple tenues de protéger les données personnelles qu'elles hébergent sous peine de sanctions. En 2018, la **Cnil**, l'autorité de contrôle en matière de protection des données personnelles, a condamné la société Uber France à une amende de 400 000 euros pour manquement à cette obligation. Adoptée par l'UE en 2016 et transposée en France en 2018, la **directive NIS** a augmenté le niveau de cybersécurité de certaines entités stratégiques, représentant une centaine d'administrations et d'entreprises en France, selon l'Anssi. Avec l'adoption en 2022 de la **directive NIS 2**, les obligations auxquelles elles sont soumises vont être étendues à « des milliers d'entités » en France. La réglementation a pour effet de stimuler le marché de la cybersécurité et de la sécurité numérique, analysait Xerfi dans sa note. En 2022, en France, le chiffre d'affaires de ce secteur s'est élevé à 14,6 milliards d'euros, en hausse de 7 % par rapport à 2021, selon l'Alliance pour la confiance numérique, une organisation professionnelle.

Pour aller plus loin

TEMOIGNAGES

Le site des Digiteurs, un service proposé par la Chambre de commerce et d'industrie d'Île-de-France, présente les huit principales cyberattaques ciblant les entreprises. Chacune est accompagnée du témoignage d'une entreprise victime.

Lire l'article.

DONNEES PERSONNELLES

Si une entreprise ne dispose pas des moyens techniques lui permettant de garantir la sécurité des données personnelles qu'elle héberge, elle doit les anonymiser. Dans un article publié en février sur le site The Conversation, les professeures Nesrine Kaaniche et Maryline Laurent présentent les différentes méthodes d'anonymisation ainsi que leurs limites.

Lire leur analyse.

Source : https://www.brief.eco/