Assurance transport : la menace cyber

LA RÉDACTION | 12/07/2018 à 17h00

Le secteur des transports, particulièrement vulnérable, a pris la mesure d'un risque cyber en pleine croissance. Mais les réponses apportées par l'assurance ne sont pas encore réellement satisfaisantes. Par Anne Kerriou.

« Il y a trois types d'entreprises : celles qui ont été victimes d'une cyberattaque, celles qui le seront, et celles qui le sont sans le savoir. » Ces propos sévères, Bernard Squarcini, ancien directeur de la Direction centrale du renseignement intérieur (DCRI) aujourd'hui dirigeant de Kyrnos Conseil, les a tenus le 21 juin dernier devant des professionnels du transport réunis pour l'assemblée générale de l'organisation professionnelle Union TLF. Exagération ? Pas si sûr. En 2016, à la question « Êtes-vous exposé à un risque cyber dans votre entreprise ? », 60 % des dirigeants répondaient négativement. Deux ans plus tard, 76 % confirment avoir subi un cyberincident.

« On est donc passé d'une menace plus ou moins bien comprise à un danger réel et éprouvé », a rappelé Frédéric Denèfle, directeur du département relations

extérieures du Comité d'études et de services des assureurs maritimes et transports (Cesam), lors des Rendez-vous de l'assurance transports, organisés les 26 et 27 juin à Paris. Tous secteurs confondus, le montant des conséquences financières des cyberattaques explose. « Selon le Center of Strategic and International Studies, un organisme américain, le coût de ces attaques est passé de 400 à 650 milliards de dollars entre 2014 et 2018, soit une augmentation de 26 % », a précisé Frédéric Denèfle.

Un secteur friand de digitalisation

Cette inflation est d'abord le reflet d'une digitalisation croissante et d'une interconnexion accrue des systèmes. Le secteur du transport et de la logistique, en la matière, est particulièrement vulnérable, puisqu'il repose sur une chaîne d'acteurs tenus de partager des informations. « Que ce soit pour le reporting, la localisation, la surveillance ou le suivi des chocs et des anomalies pendant le transport, toutes les prestations de services complémentaires au simple déplacement physique de marchandises sont organisées grâce à des objets connectés et des plateformes de mise en relation », souligne Frédéric Denèfle. Et ce mouvement ne cesse de prendre de l'ampleur, avec « aujourd'hui l'apparition des drones et, demain, des navires sans équipage ».

La douloureuse facture de Petya pour FedEx et Maersk

La cyberattaque mondiale du virus Petya, l'une des plus sévères intervenues de 2017, compte deux grands noms du transport parmi ses principales victimes, FedEx et Maersk. Touchée par le biais de sa filiale TNT Express, FedEx évalue ses pertes à quelque 300 millions de dollars, incluant la baisse des volumes, le déploiement d'un plan d'urgence et la résolution de la crise. « Nous n'avons pas d'assurance cyber ou autre couvrant cette attaque », précisait le géant mondial du transport express de colis au lendemain de l'agression. Le groupe danois Maersk a quant à lui été touché dans trois branches d'activité : le transport maritime, l'exploitation de terminaux portuaires et la logistique. Perte globale : « entre 250 et 300 millions de dollars ». Le groupe précise qu'il a depuis contracté une assurance cyber afin « d'atténuer les effets négatifs d'éventuelles attaques répétées ».

Du petit transporteur routier au groupe mondial, tout le monde est donc concerné par cette menace protéiforme qui peut aller du hameçonnage au sabotage en passant par l'attaque au « rançongiciel » ou l'atteinte à l'image. En 2017, deux grands noms du transport, le danois Maersk et l'américain FedEx, en ont fait la coûteuse expérience. À l'augmentation des cibles potentielles s'ajoute une hausse de la valeur

des données, qui fait grimper le risque à assurer, qu'il soit d'origine criminelle ou pas. « L'évolution de la réglementation sur la protection des données, avec le RGPD en Europe ou le Cloud Act aux États-Unis, fait que toute organisation doit se préoccuper du risque pour se protéger vis-à-vis de l'extérieur, mais aussi organiser la sûreté de son fonctionnement. Un bug, ce n'est pas une action malveillante, mais ça peut aussi avoir des conséquences dramatiques », souligne François Beaume, administrateur de l'Amrae, l'Association pour le management des risques et des assurances de l'entreprise et vice-président du Bureau Véritas.

Des risques difficiles à cerner

La nécessité de prendre en compte la menace cyber fait l'unanimité. Mais les assureurs et leurs clients sont confrontés à une difficulté majeure : identifier les contours de ce risque. Dommages, responsabilité, pertes d'exploitation, voire assurabilité du cyber terrorisme ou des rançons : le spectre est large. D'autre part, « il n'est circonscrit ni à un secteur d'activité, ni à une zone géographique », note Corinne Cipière, CEO France de Allianz Global Corporate & Specialty (AGCS).

Source : *article de l'argus de l'assurance n°7565*