Cybersécurité des professions financières : les régulateurs demandent des comptes

Nicolas ARPAGIAN,

Vice-President Cybersecurity Strategy & Digital Risks du cabinet HeadMind Partners, Enseignant à l'Ecole Nationale Supérieure de la Police (ENSP) et à Sciences Po Saint Germain.

Auteur de « La Cybersécurité » (PUF) et « Frontières.com » (Editions de l'Observatoire)

Twitter : @cyberguerre

3,15 millions d'euros. C'est l'amende infligée en décembre 2022 à la banque espagnole Abanca par la Banque Centrale Européenne (BCE) suite à la cyberattaque dont l'établissement avait été victime en février 2019. Elle avait conduit à la paralysie de ses distributeurs de billets, à l'incapacité à procéder à des virements et à accéder aux comptes via l'application maison. Ce n'est pas en raison du principe d'être piraté que le banquier espagnol a été sanctionné : mais pour avoir attendu quarante six heures pour avertir le gendarme bancaire européen. Or, depuis 2017, les entités placées sous l'autorité de la BCE doivent informer celle-ci dans les deux heures de la détection d'un incident informatique significatif. Cette réactivité est exigée afin de limiter les effets d'une possible propagation à l'ensemble de la communauté financière. Il existe en effet un véritable risque systémique en raison de l'interconnexion des systèmes d'information, et de la capacité de l'attaquant d'exploiter une faille d'un logiciel qui serait présente au sein de différentes sociétés du même domaine d'activité.

Dans le même esprit, le Conseil de Stabilité Financière (CSF), qui rassemble une trentaine d'autorités financières nationales (banques centrales, ministères des finances…), ainsi que différentes instances internationales chargées d'établir des normes en matière précisément de stabilité financière plaide[1] régulièrement pour le déploiement de modèles d'appréciation du risque cyber qui soient harmonisés au sein des organisations du secteur. L'importance stratégique de la disponibilité et de l'intégrité des systèmes de communication dans le bon fonctionnement des échanges financiers et commerciaux explique la prise en compte grandissante des moyens de détection et de remédiation des cybermenaces dans les processus d'évaluation des acteurs économiques[2]. Au point que l'ensemble des auditeurs (juridiques, comptables…) réclament désormais des éléments de mesure de l'exposition au risque cyber. Qui font désormais partie intégrante des démarches de « due diligence » pour connaître la valeur d'une entreprise. Et cela concerne désormais les structures au sens large. Puisque la BCE estime qu'en 2021 les sommes concernant les prestations externalisées (cloud computing, sous-traitants, consultants…) constituaient presque la moitié (47,4%) des dépenses informatiques des banques européennes. Une tendance cadencée par l'adoption grandissante de services dans le nuage. Ce qui pose la question de la maîtrise en continu de l'environnement technique élargi de l'entreprise. Avec des partenaires ou des fournisseurs qui peuvent être l'objet d'agressions qui conduisent en cascade à la détérioration, voire à l'arrêt des services bancaires. Le Trésor des Etats-Unis[3] a indiqué qu'au cours de l'année 2021 les institutions financières du pays avaient été amenées à payer près de 1,2 milliard de dollars pour faire face à des rançongiciels. Soit le double du montant payé en 2020. Sur la même période, le nombre d'attaques sous la forme de rançongiciels a triplé, représentant quelque 1 500 incidents documentés par l'autorité étatsunienne visant la sphère financière. ■

1/ "Towards a framework for assessing systemic cyber risk"- John Fell, Nander de Vette, Sándor Gardó, Benjamin Klaus & Jonas Wendelborn, *Financial Stability Review*, Novembre 2022.

2/ « Entreprises, mettez de la cybersécurité dans vos comptes », Nicolas Arpagian, *Les Echos*, 29 décembre 2021.

3/ *Financial Trend Analysis*, Financial Crimes Enforcement Network, Novembre 2021.