La cybersécurité dans le secteur financier

Avec un niveau général de cybermenace qui reste élevé en 2022, le secteur financier fait face à une menace cyber permanente, principalement criminelle et hacktiviste. Face à cette menace, le secteur est globalement sécurisé et se prépare aux scénarios de crises majeures, en étroite collaboration avec la Place financière de Paris et l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Le règlement DORA qui entrera en vigueur en janvier 2025, viendra encore renforcer le secteur en imposant des exigences en matière de résilience.

DIDIER COLLET,

Chef de la Division Coordination Sectorielle de l'ANSSI

Une menace principalement criminelle et hacktiviste

La menace cyber impactant le secteur financier diffère en fonction des acteurs : banques, assurance, infrastructures de marché.

Les banques sont sujettes à une diversité de menaces, principalement motivées par le vol d'argent, de données, ou l'extorsion. Un récent rapport[1] indique ainsi qu'en 2022 des banques de pays d'Afrique de l'Ouest, comme le Sénégal ou la Côte d'Ivoire ont été la cible de campagnes d'hameçonnage ciblées. Les cybercriminels auraient cherché à compromettre les systèmes de paiement des banques, et ils auraient eu accès aux passerelles SWIFT dans certains cas, afin de transférer des sommes d'argent vers des comptes sous leur contrôle. En tant qu'entités centrales du système économique d'un pays, les banques sont également sujettes à la menace hacktiviste. Dans le contexte de l'invasion de l'Ukraine par la Russie, de nombreux groupes hacktivistes sont apparus de part et d'autre. Les types d'actions revendiquées par ces groupes sont principalement des attaques par déni de service distribué (DDoS). Le groupe **IT Army of Ukraine**, composé de volontaires défendant les infrastructures ukrainiennes et ciblant des entités russes, a ainsi revendiqué le 13 mars 2023 sur son canal Telegram le ciblage de la banque russe Rosbank, suivi du ciblage des banques russes UBRiR, Bank Bars et de la Banque de Saint-Pétersbourg.

Les assurances, quant à elles, sont des victimes fréquentes de vol de données, du fait de la nature de leur activité. Ces entreprises exploitent un grand nombre d'informations personnelles de leurs clients. La sensibilité de ces données est une motivation potentielle des cybercriminels qui attaquent les assurances à des fins d'extorsion, mais aussi potentiellement de vol d'identité. En 2022, l'assureur médical privé australien MediBank a été victime d'une attaque informatique ayant résulté en une fuite de données. D'après MediBank, les attaquants auraient eu accès au système d'information de l'entreprise en exploitant le couple identifiant et mot de passe d'un prestataire informatique. Les attaquants ont revendiqué la fuite de données personnelles appartenant aux clients de l'entreprise. MediBank a confirmé que les attaquants avaient accès à l'entièreté des données personnelles et de santé de ses 9,7 millions de clients. L'entreprise a déclaré qu'elle refusait de

1/ Rapport conjoint d'Orange Cybersécurité et de l'éditeur de sécurité Group IB

payer une rançon qui ne garantirait pas que ces données ne soient pas publiées. L'exemple de MediBank rappelle que les prestataires des entreprises peuvent constituer un point de vulnérabilité.

Enfin, les infrastructures de marché sont des entités peu ciblées par des attaques informatiques. Toutefois, ces entités sont fortement exposées au risque d'attaque du fait du caractère informatique des échanges, du grand nombre de participants et de la complexité de leurs interactions. Elles sont généralement prises pour cible par des attaques à des fins de déstabilisation. Fin février 2022, une attaque DDoS revendiquée par l'**IT Army of Ukraine** contre la Bourse de Moscou, a eu pour conséquence de rendre le site internet de l'entité indisponible pendant quelques heures. Les attaques sur des entités reliées aux marchés de capitaux peuvent avoir des effets systémiques du fait de l'interconnexion des acteurs. Début 2023, le groupe de rançongiciel **LockBit** a ciblé une filiale de l'entreprise britannique ION Market, qui fournit des logiciels d'opération financière. L'attaque aurait été circonscrite au SI de la filiale de l'entreprise. Toutefois, d'après l'agence américaine CFTC chargée de la régulation des bourses de commerce, l'interruption d'une partie des activités d'ION Market aurait pu avoir des effets sur l'activité du secteur, et illustre ainsi les conséquences potentielles d'une attaque ciblant la chaîne d'approvisionnement (*supply chain*).

Un secteur interconnecté avec une maturité certaine face à la menace cyber

Le secteur financier français est très interconnecté à l'échelle nationale, mais également internationale, avec des filiales pour les établissements de crédit et avec les infrastructures européennes et mondiales pour les infrastructures de marché. Cette caractéristique constitue, de fait, un risque systémique. L'ANSSI accompagne et coopère de longue date avec les acteurs du secteur financier.

La mobilisation du secteur, face à la menace cyber, a conduit à la création de plusieurs enceintes sectorielles (le Groupe de Place Robustesse de la Banque de France, le Forum des Compétences, le groupe de travail interbancaire du Campus Cyber). L'ANSSI collabore efficacement avec ces différents acteurs, notamment dans le cadre de l'anticipation et de la préparation aux crises cyber.

A ce titre, en septembre 2022, la Banque de France et la place financière de Paris (le Groupe de Place Robustesse) ont organisé un exercice de gestion de crise majeure sur la thématique d'une cyberattaque par *supply chain* sur plusieurs acteurs clefs de la Place avec un volet important sur la communication de crise. Cet exercice, accompagné par l'ANSSI, a permis de plonger le secteur financier et certains services de l'Etat dans une crise majeure entrainant des impacts métiers importants et systémiques.

Cet exercice, dont l'objectif était de travailler sur la coordination au sein du secteur, a permis aux dispositifs de gestion de crise de Place composés de cellules thématiques (Fiduciaire, Communication, Liquidité) ainsi qu'aux autres instances de gestion de crise entre acteurs de déclencher leurs mécanismes de mobilisation et de mettre en œuvre leurs mesures de continuité. L'aspect hors norme des évènements a mené à l'identification de solutions de contournement novatrices et de pistes de travail pour faire face à un scénario catastrophe.

Ces axes de travail permettront au Groupe de Place Robustesse de poursuivre le renforcement de la coopération au sein de la Place financière de Paris pour en accroître sa résilience. Pour les autres acteurs du secteur financier, l'ANSSI propose trois guides sur la gestion de crise, disponibles sur le site de l'Agence. Un premier propose une méthodologie pour organiser un exercice de gestion de crise. Un deuxième s'intéresse à la communication de crise et le troisième est consacré à la gestion de crise d'origine cyber pour disposer des meilleurs pratiques pour faire face au niveau opérationnel et stratégique.

Des exigences de cybersécurité renforcées pour le secteur financier

Au cours des dix dernières années, le contexte réglementaire en matière de cybersécurité s'est étoffé. La France a été l'un des premiers en Europe à se doter d'une doctrine cyber. Ainsi, depuis 2016, l'ANSSI accompagne les opérateurs d'importance vitale pour la Nation, dont ceux du secteur financier, pour le renforcement de la sécurisation de leurs systèmes d'information.

Dans l'intervalle, face à la transformation numérique des sociétés européennes et à l'interconnexion des états-membres, le Parlement européen et le Conseil de l'Union européenne ont adopté, en juillet 2016, la directive « Network and Information Security » (NIS). Transposée au niveau national en 2018, cette directive a eu pour effet d'augmenter le niveau de cybersécurité des acteurs essentiels de dix secteurs d'activité.

La nouvelle directive *Network and Information System Security* (NIS 2) du 14 décembre 2022, qui sera transposée en droit français au deuxième semestre 2024, poursuivra l'effort de sécurisation des entités importantes et essentielles européennes. Ces entités vont de la PME aux entreprises du CAC40, en passant par les administrations publiques et couvrent a minima dix-huit secteurs d'activité.

Concomitamment, à la directive NIS2, le secteur financier s'est doté du règlement européen DORA (*Digital Operational Resilience Act*). Ce règlement, qui entrera en vigueur en janvier 2025 se substituera, pour le secteur financier, à NIS 2, selon le principe *Lex specialis*, et imposera des exigences en matière de résilience. En France, l'ACPR (autorité de contrôle prudentiel) supervisera la bonne application de ce règlement. L'ANSSI continuera sa collaboration avec le secteur financier, tant dans le domaine de la connaissance de la menace, que dans sa sécurisation et la préparation aux situations de crise. ■