Séminaire EIFR du 5 juillet 2019

Cybersécurité, quelles protections pour les établissements financiers ?

I Laurent Gerardin, Responsable de la division Coordination Sectorielle, ANSSI

Dans un contexte où le coût des cyberattaques s'envole, où les vols de données peuvent s'effectuer à grande échelle (la société américaine Equifax s'est fait subtiliser les données de 143 millions d'Américains ; l'incident lui a coûté 1,4 milliard de dollars en tout), et où l'on a affaire à des groupes criminels structurés et opérant avec un risque faible, le secteur financier est particulièrement visé et sensible : les banques sont hautement solvables ; elles sont avancées dans la digitalisation et offrent par conséquent une grande surface d'attaque ; le niveau de sécurité est disparate ; plusieurs types d'attaques s'y manifestent. Parmi elles, celles dont la porte d'entrée sont les sociétés de services informatiques travaillant pour les banques.

D'importantes cyberattaques sont passées par le réseau SWIFT avec des virements frauduleux qui n'ont pas pu être stoppés à temps.

L'Agence nationale de la sécurité des systèmes informatiques (Anssi), placée sous l'autorité du Premier ministre et rattachée au Secrétariat général de la Défense et de la Sécurité nationale, a été créée en 2009. Ses trois missions centrales : défense (mission essentielle), prévention et protection, formation et sensibilisation. L'Anssi délivre par ailleurs des visas de sécurité, sortes de labels, aux fournisseurs de services.

Le cadre réglementaire est celui de la Loi de programmation militaire (LPM) et la directive européenne Network and Information System Security (NIS) adoptée en 2016. Les objectifs de ce texte : parvenir à un niveau commun de sécurité ; renforcer les capacités nationales (en 2017 par exemple, tous les pays n'étaient pas dotés d'une agence comme l'Anssi) ; assurer une certaine coopération entre les Etats membres ; construire un cadre pour renforcer la sécurité des fournisseurs de services numériques (entreprises de type Gafa).

Amelie Champsaur, Avocat Associé, Cleary Gottlieb Steen & Hamilton

Il n'y a pas de cadre réglementaire unifié dans le domaine de la cybersécurité, d'où de nombreuses occasions de conflits de lois. En France cohabitent des textes d'application générale (deuxième directive sur les services de paiement, directive Network Information System Security, règlement général sur la protection des données, règlement sur les abus de marché pour les entreprises cotées...) et des règles bancaires, notamment en ce qui concerne le risque de rupture de l'activité, cela sous le contrôle de la Banque centrale européenne pour les très grandes banques et de l'Autorité de contrôle prudentiel et de résolution pour les banques de moindre importance.

En matière d'abus de marché par exemple, le droit européen oblige à déclarer dès que possible toute information privilégiée, une cyberattaque par exemple. Or, au moment du déclenchement de l'attaque, l'émetteur de peut pas connaître précisément les impacts de cet événement.

On trouve la même difficulté dans le domaine de la protection des données personnelles, où le règlement européen fait obligation aux entreprises de notifier à la Commission nationale de l'informatique et des libertés toute violation de données dans les soixante-douze heures et, dans certains cas graves, d'en avertir les personnes concernées. Cela justifie la nécessité d'avoir établi des procédures internes précises.

La deuxième directive sur les services de paiement consacre quant à elle l'avènement de l'open banking et de la mise à disposition de données bancaires à de nouveaux prestataires de services (agrégateurs...) qui sont souvent des entreprises disposant de moyens financiers et humains limités.

Aux Etats-Unis, il n'existe pas non plus de cadre juridique unifié au plan fédéral. Il y a des initiatives, notamment de la part de la Security and Exchange Commission, de la Federal Trade Commission et des Etats de l'Union. La Californie, de son côté, pourrait se doter d'un dispositif légal inspiré du règlement européen sur la protection des données.

Samuel Janin, CIO Advisory Services, Mazars

Les infrastructures sont particulièrement développées et complexes dans le secteur financier, qui est par ailleurs désormais ouvert, avec l'open banking, les banques en ligne, les fintechs et les API qui permettent aux systèmes de communiquer entre eux.

Les grands principes en matière de protection des infrastructures informatiques ne varient pas avec le temps : assurer la continuité des services, détecter et surveiller, assurer la sécurité du périmètre, cloisonner (les systèmes, les données, les métiers...), défendre en profondeur (gestion des vulnérabilités), gérer les identités et les accès. Mais il convient de s'adapter aux évolutions techniques, par exemple en ayant recours à l'intelligence artificielle pour la détection des attaques, et essayer d'appliquer les bonnes pratiques suivantes : établir une carte des risques, rationaliser les systèmes d'information et les services, sensibiliser les personnes, avoir une connaissance fine des modes de défaillance, s'entraîner à la gestion de crise et au contingentement.

Dans ce contexte, le secteur financier bénéficie de points forts, sa longue pratique des risques et du contrôle interne notamment, mais a aussi des talons d'Achille, par exemple le fait de déléguer des choix importants aux directeurs des services informatiques. A noter, la publication par la Banque centrale européenne en mai 2018 d'un cadre européen de test de la résilience des systèmes aux cyberattaques nommé Threat intelligence-based ethical red teaming ou Tiber-EU, cadre qui doit être adapté par les Etats membres.

En synthèse, une cybersécurité réussie : intégrer le risque cyber dans le dispositif général de gestion des risques ; encourager la coopération sectorielle afin d'échanger les modèles de risques, les incidents et les modes de défaillance connus ; former régulièrement les équipes à la gestion de crise et à l'hygiène informatique ; avoir un système d'information maîtrisé et des ressources permettant de connaître finement les modes de défaillance complexes.

Romain Eliot, Responsable des relations institutionnelles risques IT et cybersécurité, Credit Agricole SA

Le risque cyber se matérialise : 72 millions de dollars détournés aux dépens de la Banque du Bangladesh en 2016, 500 millions de comptes Yahoo piratés la même année, ou encore en 2017, les systèmes d'information de Merck, Fedex ou Saint-Gobain sont restés indisponibles pendant plus d'une semaine.

Pour que le risque se matérialise, il faut une motivation (gain en argent ou en données), des moyens et des attaquants (on a désormais affaire à des groupes mafieux ou étatiques puissants et organisés – plusieurs milliers de personnes en Chine), et des vulnérabilités ou des défaillances humaines ou techniques.

Les modes d'attaques se sont sophistiqués et multipliés : attaque frontale (en surchargeant un serveur jusqu'à le rendre inopérant par exemple), ciblée sur une personne (phishing, spear phishing), indirecte (virus, cheval de Troie, point d'eau). Dans les deux derniers cas, l'attaquant profite d'une connexion d'un poste de travail à internet pour franchir la protection périmétrique de l'entreprise.

Un scenario particulièrement redouté est celui de la menace persistante avancée (advanced persistent threat) où l'attaquant parvient à demeurer inaperçue pendant une longue période. La réponse consiste à protéger (les systèmes, le périmètre...), à détecter, à réagir puis à reconstruire. La détection et la réaction sont placées sous la responsabilité d'équipes spécialisées : les centres opérationnels de sécurité (security operation centers ou SOC) spécialisés dans la sécurité, et les Computer emergency response teams (CERT), chargées de la gestion de crise, laquelle doit être très transversale.

Compte tenu du caractère létal de certaines cyberattaques, la cyber-résilience (capacité de reconstruire ses systèmes et d'utiliser ses données) n'est plus une option, mais une nécessité.

Gilles Mawas, Risk expert, BNP Paribas Securities Services

Les risques opérationnels sont les risques non financiers (fraude, procédures défaillantes, cyberattaques...) que les autorités de contrôle du secteur bancaire invitent à gérer depuis les accords de Bâle II. La gestion de ces risques vise à limiter les pertes, à minimiser le risque de non-conformité (amendes...) ou encore à économiser des fonds propres réglementaires (à BNP P SS, les risques opérationnels mobilisent 40 % des fonds propres réglementaires ; dans la banque en général, 10 %).

Dans la perception des banques, le cyber risque est redouté pour ses impacts directs : perte d'actifs des clients ou de la banque (titres, cash...), perte de données relatives aux clients, interruption des opérations (avec notamment un risque d'illiquidité).

Le risque opérationnel est perçu comme de plus en plus élevé par tous les acteurs économiques : les clients, les salariés, les dirigeants, les autorités de contrôle (elles exigent pour l'instant que les banques se dotent de dispositifs ad hoc, mais on se dirige probablement vers une obligation de gestion des risques en direct), la presse et les réseaux sociaux.

La cyber sécurité motive des investissements très importants de la part des banques. Pourtant, pour l'instant, les pertes cumulées dues à des cyberattaques sont très faibles si on les compare aux pertes

enregistrées pour des raison de non-conformité ou de mauvais produits (subprimes) ou à celles résultant de la défaillance de procédures.

La cyber sécurité ne relève pas de la compétence exclusive des informaticiens. Elle doit associer les dirigeants, les spécialistes du risque, les ressources humaines et les clients et constituer un dispositif évolutif.

Nicolas Bonnefous, COO/CTO & cofondateur, VAADATA

Dans le secteur de la finance, le contexte est marqué par la montée en puissance de l'opérabilité, la multiplication des acteurs du paiement, le rôle grandissant des interfaces de programmation applicatives (API en anglais), de l'instantanéité, ou encore un rythme soutenu d'opérations de fusion-acquisition. L'exposition au cyber risque est donc croissante.

Il est essentiel d'appréhender la cyber sécurité dès la conception (des systèmes, des produits, des applications...). Cette démarche garantit des économies de coûts significatives et se révèle plus efficace. Il convient de lutter dès l'origine des projets (Privacy by design) contre la complexité, qui est l'ennemi de la sécurité.

Dejan Draguljevic, SVP- Business & Corporate Development, Pradeo

Les écrans mobiles (téléphones portables, tablettes) servent de plus en plus d'interfaces aux services bancaires. Or ils échappent en grande partie aux efforts déployés pour lutter contre les cyberattaques, les investissements en matière de sécurité se concentrant essentiellement sur les systèmes dans l'entreprise.

Une étude réalisée par Pradeo montre qu'en majorité, les applications courantes, qui manipulent le plus souvent des données sensibles, exfiltrent ces données et/ou sont vulnérables aux attaques.

D'après une enquête d'Opinionway pour le compte de Pradeo, les possesseurs de téléphone mobile ou de tablette disent, à 33 %, qu'il leur est arrivé d'y enregistrer des identifiants ou des mots de passe personnels, à 26 % d'avoir enregistré des copies de documents d'identité. Quelque 22 % ont enregistré des informations relatives à leurs comptes bancaires et 16 % des identifiants ou mots de passe professionnels. Les taux sont dans tous les cas supérieurs quand il s'agit d'appareils (téléphones, tablettes) professionnels.

Slides des intervenants :

- Slides Laurent Gerardin - ANSSI : http://www.eifr.eu/event/file/download/545/laurent-gerardin-pdf
- Slides Amelie Champsaur - Cleary Gottlieb Steen & Hamilton : http://www.eifr.eu/event/file/download/546/amelie-champsaur-pdf
- Slides Samuel Janin – Mazars : http://www.eifr.eu/event/file/download/547/samuel-janin-pdf
- Slides Romain Eliot - Credit Agricole SA : http://www.eifr.eu/event/file/download/548/romain-eliot-pdf

- Slides Gilles Mawas - BNP Paribas Securities Services : http://www.eifr.eu/event/file/download/549/gilles-mawas-pdf
- Slides Nicolas Bonnefous - VAADATA : http://www.eifr.eu/event/file/download/550/nicolas-bonnefous-pdf
- Slides Dejan Draguljevic - Pradeo : http://www.eifr.eu/event/file/download/551/dujan-draguljevic-pdf