# Le risque Cyber dans le domaine bancaire

Nous habitons un monde dans lequel la connexion est devenue reine. Grâce à elle, mais aussi grâce aux terminaux de toutes sortes par lesquels elle s'exprime, nous communiquons à la vitesse de la lumière dans notre univers numérisé. Nos démarches sont simplifiées, notre réactivité est exemplaire. Et nos organisations s'en trouvent grandies, améliorées.

Vincent
MÉRIC de BELLEFON,

Directeur Cybersécurité-Risques IT du Groupe Crédit Agricole et Directeur Général Adjoint CA-GIP (Credit Agricole Group Infradtructure Platform)

## Bien qualifier le risque cyber

Pourtant, car il y a un revers à toute médaille, un risque nouveau est apparu en corollaire de cette évolution bénéfique : **le risque cyber.** Et il ne cesse de croître et de menacer ces mêmes organisations, enrichies par les fonctionnalités nouvelles du digital, mais aussi dépendantes de leur transformation digitale. Bien évidemment, cette menace concerne les banques au même titre que toutes les entreprises. Pour bien la comprendre, encore faut-il bien la qualifier. Elle pose, en effet, trois problèmes importants : **la confidentialité, l'intégrité et la disponibilité.**

Les banques disposent de toutes sortes de données extrêmement précieuses. Elles concernent les clients, les collaborateurs, le marché, les paiements, etc…. Les Cybercriminels chercheront à mettre la main dessus pour les exporter de manière illicite en vue de les revendre ou d'exercer un chantage à la publication (risque de confidentialité). Ils essaieront de les manipuler en vue de fraudes ou de destruction (risque d'intégrité). Ou, enfin, ils tenteront de bloquer les systèmes (risque de disponibilité).

Avant les années 2014-2015 le risque portait essentiellement sur la surface exposée sur Internet (les sites web, les serveurs B2B, etc.). Désormais, la multiplicité des portes d'entrée peut mener l'attaquant au cœur même du réseau de l'entreprise. On peut citer pêle-mêle les PC dont la conception et la surveillance sont inadéquates (ports USB non restreints, anti-virus obsolètes…), l'internet des objets (IOT), les réseaux WiFi mal sécurisés.

## Les fondamentaux de la réponse des établissements financiers

Les établissements financiers sont exposés aux mêmes menaces que tout autre type d'entreprise. Une différence toutefois, et de taille : lorsqu'un de leur client subit une attaque, en particulier une fraude, celle-ci peut avoir des répercussions sur l'établissement lui-même. Il est donc d'autant plus prégnant pour eux d'établir une ligne de défense efficace.

Très tôt, les établissements ont développé des chaines de défenses basées sur quatre principes clefs : **la prévention, la protection, la détection et la réaction.**

La prévention rassemble les actions autour de l'analyse de la menace, de la formation des parties prenantes de

la sécurité du système informatique, de la sensibilisation de l'ensemble du personnel, de la gestion adéquate des droits d'accès aux applications et aux systèmes et de la mise en place d'équipes spécialisées comme le CSIRT ou la Red Team.

La protection est plus une question de matériel. Elle concerne par exemple les équipements de filtrage des flux, dispositifs de blocage des logiciels malveillants, durcissement des configurations logicielles, chiffrement, signature électronique des transactions, etc…

La détection résulte d'un état d'alerte permanent qui permet par exemple, le repérage du déclenchement d'un logiciel suspect dans un poste de travail ou l'activité anormalement élevée d'un serveur , etc…. Elle amène également au repérage des échanges, internes aux réseaux, typiques d'une attaque en cours.

Enfin, la réaction représente le dernier stade, celui de l'urgence. C'est la mise en place d'un dispositif de gestion de crise ou d'équipes fonctionnant, selon l'urgence en mode commando ou au fil de l'eau.

## Les fondamentaux de la réponse du Crédit Agricole

Pour un groupe comme le Crédit Agricole, composé de systèmes d'informations complexes, multiples, eux-mêmes répartis dans les nombreuses structures juridiques constituant un Groupe, il est fondamental d'assurer une homogénéité des pratiques. Cela passe par des corpus de règles et de normes, définies pour chaque domaine de l'informatique (développements, gestion des identités, conception des réseaux, protection des données, etc.).

Par ailleurs, une attention particulière a été portée, et depuis longtemps, à la constitution d'une communauté de professionnels de la cyber sécurité répartie sur tous les aspects : sécurité des applications, sécurité des infrastructures, détection, anticipation, cryptographie. Elle travaille de concert avec les maîtrises d'ouvrage, les products owners et d'autres spécialités telles que la protection des données à caractère personnel et la conformité.

En complément, au niveau de chaque entité, des collaborateurs spécialisés sont dédiés à cette surveillance numérique. De même, à l'échelle du Groupe, une équipe traite le sujet cyber mais aussi celui des risques IT, et coordonne cet effort en lui donnant force et cohérence.

Autre rouage essentiel de cette démarche de sécurité, la sensibilisation et la formation des collaborateurs aux activités hostiles dont ils peuvent être la cible. Une information permanente est organisée

autour de cette thématique dans les newsletters du Groupe. Des actions spécifiques et récurrentes sont mises en place : tests de sensibilité au phishing, campagnes de communication, formation obligatoire annuelle, parcours ludiques et digitaux à l'occasion du cyber mois. Il faut présenter les messages de façon originale, souvent décalée et éviter le côté anxiogène inhérent au propos. Trouver le juste ton est un exercice complexe.

Enfin, des unités dédiées au contrôle évaluent continuellement les systèmes et les pratiques et émettent des recommandations. Ainsi, le CSIRT centralise les demandes d'assistance, traite les alertes, effectue la veille, échange les informations avec d'autres unités équivalentes,..... La Red Team, quant à elle, détecte, prévient et élimine les vulnérabilités en imitant le rôle d'un attaquant et en trouvant les chemins d'intrusion, étape par étape, vers une cible en exploitant les vulnérabilités des ordinateurs et autres composants informatique mais aussi des processus et de l'environnement physique.

S'ajoute à ce travail permanent les travaux de la Direction Risques Groupe et de l'Inspection Générale ainsi que les audits des superviseurs (ACPR, BCE notamment).

## Et les clients dans tout ça ?

Il est inconcevable de laisser le client sur le bord du chemin. Les établissements financiers représentent une véritable chaîne dont le client fait intimement partie. C'est pourquoi les banques sensibilisent en continu leurs clients particuliers et entreprises : sites web de banque en ligne, courriers, fascicules distribués en agence, newsletters, événements spécifiques... Dans le Groupe Crédit Agricole, les rencontres pluriannuelles des Caisses Régionales avec leurs sociétaires, représentent autant occasions de passer les messages de cybersécurité.

D'un point de vue plus technique, les moyens mis à disposition des clients apportent des fonctions de sécurité avancées (validation des ordres, authentification multi-facteurs, plafonnement des transactions ainsi que d'autres moyens internes et confidentiels).

De même, les ordres de paiement sont analysés et les transactions suspectes sont bloquées ou sur-contrôlées.

La menace cyber prend souvent une tournure dramatique pour les entreprises. Les ransomwares peuvent remettre en cause une santé financière considérée comme saine. C'est pourquoi certains établissements financiers proposent des services d'accompagnement à la mise en place de mesures de cyber-protection, ainsi que des offres d'assurances.

Notre monde s'est digitalisé. Le réel et le virtuel se côtoient désormais naturellement. De même, les menaces se sont développées dans ces deux univers. Aujourd'hui, le risque cyber n'est plus nouveau. Nous avons appris à y faire face. L'efficacité de nos réponses respectives dépend de notre organisation collective, mais aussi de notre capacité d'étonnement individuelle.

Nous devons toujours avoir à l'esprit, que **lorsqu'il y a un doute... c'est qu'il n'y a pas de doute.** ■