La dynamique du post-marché

Les impacts de la cybersecurite sur les metiers du post marché

L'Association Française des professionnels des Titres (AFTI) et son sous-groupe Sécurité Financière ont organisé, le 14 octobre 2021, une conférence sur le thème de la Cybersécurité, en association avec la Fédération Bancaire Française (FBF). La Cybersécurité est un thème majeur pour nos institutions, que ce soit en préventif ou en curatif.

Introduction

Pierre Jond, *Président*
AFTI – BNP Paribas Securities Services, Paris

Je tiens à remercier tous les participants à cette webconférence, en particulier le cabinet Chappuis Halder & Co, qui nous a beaucoup aidés et a mis à disposition son infrastructure pour l'organiser.

Je souhaite vous partager une anecdote qui me vient à l'esprit à chaque fois que je parle de cybersécurité : il y a une dizaine d'années, je bavardais avec un policier qui s'occupait plus particulièrement de cybercriminalité. Au détour de la conversation, je lui ai expliqué que j'avais un Mac à la maison et qu'il n'était pas nécessaire d'avoir d'antivirus sur un Mac. Ce monsieur m'a regardé avec un tel air de pitié que la première chose que j'ai faite quand je suis rentré à la maison a été de télécharger Norton Antivirus et de l'installer sur tous les ordinateurs de la famille…
Pourquoi une conférence sur la cybersécurité ? Il suffit d'ouvrir n'importe quel journal pour se rendre compte de l'importance vitale de la cybersécurité dans le monde en général, dans la finance en particulier et dans le monde du post marché. L'AFTI dispose d'un sous-groupe sécurité financière comprenant le sujet cybersécurité sur sa feuille de route.

Stéphanie Saint Pé,
Déléguée Générale – AFTI, Paris

Afin de mettre en perspective l'importance de la cybersécurité sur les métiers post marché, nous avons invité d'éminents experts capables de partager des leçons et observations provenant de projets concrets menés avec des institutions financières, mais aussi d'aborder le caractère humain d'une crise cyber, des causes de déclenchement jusqu'aux difficultés humaines dans sa résolution.

Sébastien Meunier, *Directeur Cybersécurité et Technologie – Chappuis Halder & Co, New-York*

Chappuis Halder est un cabinet de conseil en management dédié aux services financiers. Il travaille pour la plupart des institutions financières en France et dans d'autres pays, et couvre toutes leurs problématiques (front, back, comptabilité, y compris la cybersécurité). Les retours d'expérience et les projets menés avec des institutions financières en matière de cybersécurité permettent de distinguer quelques tendances ou leçons qui se répètent, sous l'angle de la gestion des risques, de la gouvernance, des nouvelles technologies et du retour sur investissement.

DE L'UTILITÉ DES MÉTHODES DE GESTION DES RISQUES POUR ÉVITER LES INCIDENTS

Dès lors que vous disposez d'un système d'information et d'une organisation complexe, la question n'est pas de savoir si des incidents de sécurité peuvent arriver, mais quand, et quel sera leur impact. Il s'agit d'essayer de minimiser leur fréquence et leur impact en se protégeant. La cybersécurité, c'est 80 % de gestion des risques et 20 % de technologie, comme le montre la slide ci-dessous. Comme dans une démarche classique de gestion des risques, une fois évalué l'impact d'un incident potentiel et sa probabilité, vous en déduisez le risque inhérent et vous évaluez les contrôles en place pour aboutir au risque résiduel. Vous comparez ce risque résiduel à votre appétit pour le risque : si vous êtes au-dessus, il faut diminuer le risque en appliquant des traitements d'atténuation, de transfert, d'évitement ou d'acceptation. Bien entendu, si vos systèmes sont vulnérables en raison de failles de sécurité, la probabilité d'un incident sera plus importante.

L'utilisation d'une matrice des risques montre qu'il est souvent plus facile de diminuer la

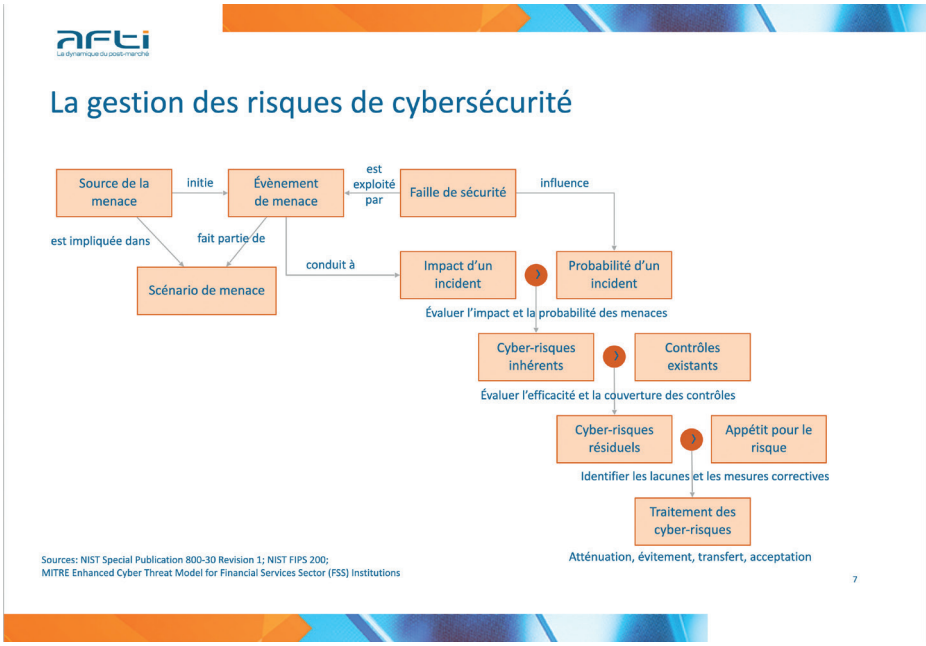
probabilité d'un incident en appliquant des contrôles de sécurité que d'en diminuer l'impact, lié aux données manipulées. Il est parfois possible de réduire l'impact en supprimant les données confidentielles d'un fichier pour n'y laisser que les données indispensables aux métiers au cas où ce fichier se retrouve sur Internet.
Il est aussi possible de quantifier les risques de cybersécurité en utilisant notamment la méthode FAIR (voir slide ci-contre), qui permet de découper les risques par fréquence et intensité pour en déduire de potentielles pertes financières et allouer du capital en face de ces risques.

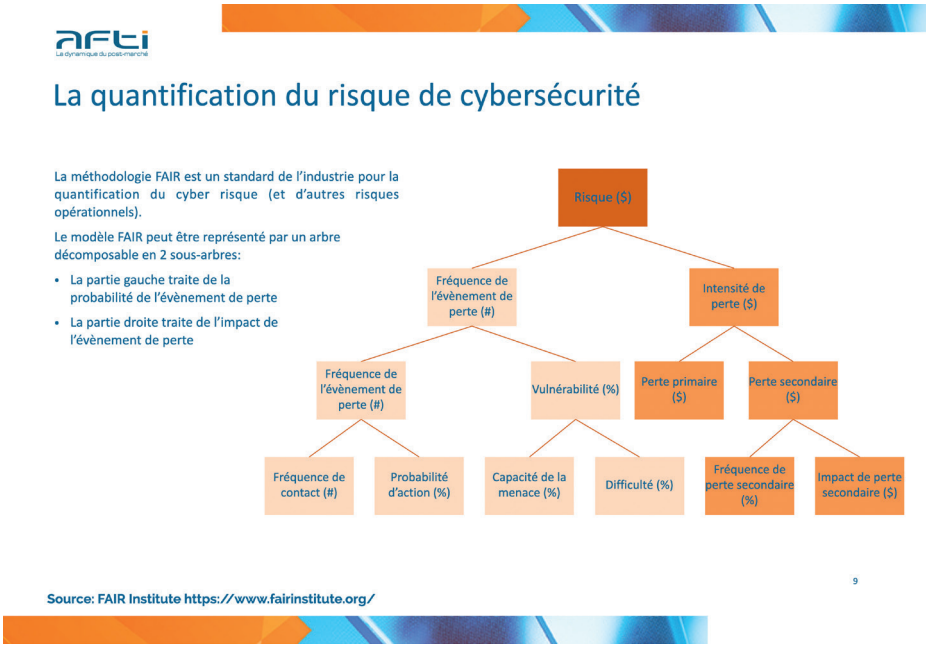
LES PROBLÉMATIQUES DE GOUVERNANCE DE LA CYBERSÉCURITÉ

Les structures souvent complexes des grandes institutions financières soulèvent souvent des problématiques de périmètre : ceux-ci sont amenés à se chevaucher entre la gestion des risques de cybersécurité, des risques technologiques, et des risques liés au traitement des données personnelles. Des querelles de clocher peuvent survenir entre les différents responsables, à la fois en termes de procédure et de prise de décision. Ces questions de périmètre sont résolues avec la mise en place de procédures de décision très claires et des matrices RACI (pour responsible, accountable, consulted et informed).
Le responsable de la sécurité des systèmes d'information (RSSI ; en anglais, Chief information security officer ou CISO) fait face à une réglementation sans cesse évolutive à laquelle il doit se conformer, même s'il ne s'agit que de recommandations. Il doit documenter, justifier en travaillant avec l'équipe de la conformité et consacrer parfois plus de temps à la conformité qu'à la protection de l'organisation. Mon point est qu'il est possible d'être «conforme» tout en ayant des failles de sécurité.

LA CYBERSÉCURITÉ À TRAVERS LES 3 LIGNES DE DÉFENSE

La première ligne – le CISO - assure la protection quotidienne de l'organisation avec ses contrôles, ses propres procédures et indicateurs. La deuxième ligne doit être





capable de « challenger » la première ligne et de l'aider dans la mise en place de méthodologies de gestion des risques ; elle rencontre parfois des difficultés à challenger la première ligne par manque d'expertise et est amenée à recruter des personnes compétentes en cybersécurité. La troisième ligne, l'audit interne, doit également se doter de compétences en cybersécurité afin de pouvoir auditer les deux autres lignes, soit en recrutant des spécialistes en cybersécurité ou, de plus en plus, en formant des auditeurs «système d'information» en cybersécurité. En général, le CISO ou RSSI est souvent une entité indépendante rattachée au directeur général ou directeur des opérations ; il peut aussi être rattaché au département informatique ou au responsable des risques. J'ajouterais ici quelques recommandations : clarifier le rôle de chaque ligne, avoir une gouvernance bien structurée et définir un RACI de haut niveau entre tous les acteurs

Les impacts de la cybersécurité sur les métiers du post marché

ainsi que des RACI détaillés pour tous les processus de cybersécurité transversaux.
Le CISO doit être capable d'avoir une vision des risques par ligne de métier et de parler avec les responsables métiers et les équipes en charge de la continuité de l'activité : à la fin, ce sont bien les métiers qui assument les risques et qui décident s'ils les acceptent ou non.

LES RISQUES LIÉS AUX NOUVELLES TECHNOLOGIES

• **Le Cloud** s'est déployé de plus en plus dans les institutions financières. Il apporte non seulement des bénéfices, mais aussi des risques (concentration des fournisseurs, déploiement incontrôlé ou shadow IT - quand les utilisateurs déploient des solutions sans passer par le département informatique -, localisation des données, verrouillage vendeur, suspension juridique...). Il existe des modèles ou standards internationaux[A1] permettant d'estimer le risque et de déterminer les sujets sur lesquels vous devez travailler.
• **L'intelligence artificielle** se répand également et peut parfois être perçue comme une « boîte noire ». Un des risques les plus médiatisés tient aux biais éthiques : en présence de biais dans les sources de données, les algorithmes produiront des résultats biaisés qui peuvent être utilisés pour des cyberattaques. Si les données sont compromises, l'algorithme est lui-même compromis.
• **La chaîne de blocs** est très à la mode depuis plusieurs années. Cette technologie est souvent présentée comme sécurisée parce qu'elle utilise la cryptographie. Il s'agit d'un mythe. Même si le cœur des blockchains publiques telle que Bitcoin est sécurisé par conception (et non par magie), dès que vous utilisez un logiciel externe pour vous connecter, vous êtes à la merci d'un piratage. Les blockchains privées développées par exemple par des institutions financières présentent encore plus de vulnérabilité que les blockchains ouvertes. Certes, la cryptographie aide à certifier l'intégrité des données. Cela ne signifie pas que les blockchains soient davantage sécurisées que les autres systèmes, comme en témoignent les piratages réguliers dont elles font l'objet. Il faut leur appliquer, comme pour les autres systèmes, une évaluation des risques. Les utilisateurs doivent être formés à la cybersécurité, les clients physiques et logiciels doivent être sécurisés, et les codes des « smart contract » doivent faire l'objet d'une revue poussée.

QUEL EST LE RETOUR SUR INVESTISSEMENT DE LA CYBERSÉCURITÉ POUR LES INSTITUTIONS FINANCIÈRES ?

Nous avons procédé à une étude aux Etats-Unis à partir de différentes sources. Les coûts moyens dépendent de la méthodologie utilisée (qu'inclure dans les coûts ? perte de business, coût postérieur pour remédier à l'incident, etc.). Les coûts moyens s'échelonnent de 600 000 à près de 6 millions de dollars, mais ils peuvent aller bien au-delà : d'une centaine à plusieurs centaines de millions de dollars. Par ailleurs, une nouvelle tendance s'est faite jour : non seulement les régulateurs interrogent les banques sur leurs pratiques de sécurité, mais ils fixent des amendes quand des manquements sont constatés. Si en Europe, seules quelques amendes ont été infligées aux banques pour manquement à la directive RGPD, je ne serais pas étonné que les régulateurs européens commencent à mettre des amendes pour des manquements en cybersécurité.
Afin d'évaluer le coût interne de la cybersécurité, nous avons procédé à la même analyse que pour le coût moyen, à partir de différentes sources : la part moyenne des dépenses par rapport au budget de l'IT oscille entre 7 et 15 %. Il existe d'autres métriques, telles que le coût moyen par employé ou le coût en pourcentage des revenus. Bank of America et JP Morgan dépensent plus de 600 millions de dollars en cybersécurité.
Ces chiffres donnent un ordre de grandeur. C'est ensuite à chaque institution financière de se positionner en fonction de son histoire, de son contexte et de son appétit au risque. Le retour sur investissement de la cybersécurité se mesure à la réduction des risques et à la libération du capital de risque associé.

[A1] *https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/*

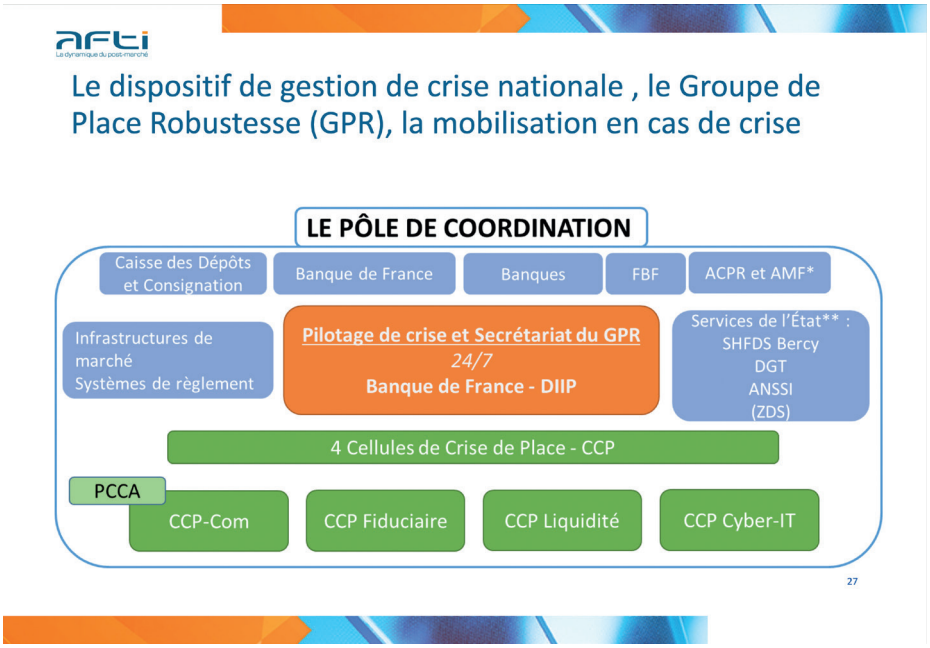
Stephane Schatteman
Responsable du pôle Robustesse et Cyber Résilience au sein du Service Résilience et Études des Infrastructures de Marché. En charge du Groupe de Place Robustesse-Banque de France, Paris

En préambule, imaginez ce qui pourrait arriver de pire dans votre travail (interruptions de services, pertes de savoir, de données, incapacité à agir...), et dites-vous que, parmi tous les facteurs susceptibles d'entraîner ce pire, les facteurs cyber sont les plus puissants et rapides. Ajoutez à cela le développement du télétravail qui a ouvert des portes pour pénétrer dans les systèmes et l'interconnectivité de nos systèmes qui accroît notre vulnérabilité. Comme l'a dit Sébastien Meunier, le risque zéro n'existe pas, même si des moyens considérables sont mis en œuvre (RSSI, CERT ou encore les règles utilisateurs auxquelles nous devons tous adhérer).
Un chiffre délivré par l'ANSSI suffit à comprendre l'ampleur du sujet : de 2019 à 2020, le nombre d'attaques cyber a été multiplié par 4. De plus, les pirates se professionnalisent et prennent leur temps pour imaginer des attaques difficilement détectables. Il est donc primordial de se préparer individuellement et collectivement aux impacts qu'aurait un incident sur les systèmes d'information.
Dans ce but, des initiatives ont été menées au niveau international, avec l'organisation d'un exercice de 3 jours en 2019 par le cyber expert group du G7, qui a créé il y a quelques années le cyber incident response protocol permettant la mobilisation d'une vingtaine d'autorités financières à travers le monde en cas d'incident de cybersécurité transfrontière. Au niveau européen, l'exercice « Unitas » a réuni les acteurs du marché pour réfléchir ensemble aux impacts que pourrait avoir une cyberattaque sur les infrastructures tandis que la Place de Paris dispose, elle, de son dispositif national autour du Groupe de Place Robustesse (GPR).

Les impacts de la cybersécurité sur les métiers du post marché

LE DISPOSITIF DE GESTION DE CRISE NATIONALE

Depuis 2005, le GPR, présidé et piloté par la Banque de France, a pour objectif de contribuer à renforcer et garantir la stabilité financière de la Place de Paris en la rendant plus robuste, plus résiliente, pour lui permettre d'affronter un choc ou une crise opérationnelle majeure dont l'origine serait exogène au système financier, mais qui pourrait entraîner des impacts systémiques. L'origine de ces crises peut être diverse, voire conjuguée (attaque terroriste, catastrophe naturelle, mouvement social majeur, pandémie, défaillance d'un prestataire critique, cyberattaque), avec des effets pluridimensionnels sur l'opérationnel, liés aux ressources humaines et aux sites physiques, sur les systèmes d'information et sur les activités financières critiques (gestion de liquidité, opérations de paiements, refinancement, etc.).
Notre action se déroule en 3 temps : avant la crise, pendant la crise et après la crise.
Avant la crise, l'idée est de faire vivre une structure de coordination de crise en y instaurant un climat de confiance pour être le mieux préparé possible avant la survenue éventuelle de la crise. Pendant la crise, il ne s'agit pas de résoudre la totalité des problèmes, mais d'établir un diagnostic complet de la situation de la Place, diagnostic qui est actualisé régulièrement, et d'identifier des actions collectives possibles, les mettre en œuvre et dégager une position de Place tout en favorisant le dialogue avec les services de l'État. Enfin, le GPR a pour objectif de travailler sur l'après-crise, afin de garder toujours un coup d'avance. Par exemple, lors de la pandémie, nous avons travaillé très en amont de la fin du confinement sur l'après-confinement. Il s'agit, pour nous, de tirer les enseignements de la crise tant au niveau individuel que collectif pour adapter et renforcer le dispositif.
Le slide ci-dessus montre comment le GPR se mobilise en cas de crise.



Notre action s'appuie notamment sur 4 cellules de crise de Place qui réunissent des experts opérationnels capables de traiter des sujets relatifs à leurs domaines.
Pour pouvoir faire fonctionner ce dispositif, nous devons nous entraîner à la fois au niveau individuel et au niveau du Groupe.

LA PRÉPARATION DE LA PLACE VIA SES EXERCICES ANNUELS

Les scénarios utilisés lors des exercices annuels doivent permettre d'activer le pôle de coordination et les 4 cellules de crise de Place. Ils servent à éprouver la capacité de la Place à maintenir ses processus critiques, à renforcer la capacité de coordination du secteur financier et à exercer la communication interne et externe.
Ce cadre général s'appuie sur une stratégie triennale fixant des axes prioritaires. La stratégie 2021-2023 a en particulier pour but de mettre en œuvre une dimension plus cyber et IT de nos exercices, et de renforcer encore leur dimension financière.
Le trigger de crise est choisi parmi les contextes de mobilisation du GPR. En 2012, 2018, 2019 et 2021, le contexte était une cyberattaque, ce qui sera également le cas en 2022 et 2023.

CONCRÈTEMENT, À QUOI SERT UN EXERCICE ?

Au niveau des entités, il s'agit de s'exercer à déclencher les procédures de secours imaginées à froid, afin de s'assurer que tout le monde les comprenne, sache comment elles fonctionnent et qu'elles soient maîtrisées (ce qui peut déboucher sur des questions métiers). Les exercices permettent également d'activer les cellules de crise pour s'assurer que les personnes convoquées sont bien les bonnes, mais aussi pour qu'elles se rencontrent et échangent avant la crise (sinon cela ne fonctionnera pas lors d'une crise réelle). La gestion de crise est un sport d'équipe : il faut savoir où chacun se positionne et ce qu'on attend de lui. L'exercice permet également de faire participer les experts pour alimenter les décideurs et les back-up, car il faut savoir vers qui se tourner en cas d'absence de celui qui sait ! Ces exercices sont enfin un moyen d'élaborer un langage commun en interne, mais aussi de s'entraîner à communiquer vers les clients et contreparties en cas de défaillance.
Au niveau du GPR lui-même, nous devons nous entraîner afin de coordonner l'action des Cellules de Crise de Place, de partager l'information entre acteurs publics et privés, de s'étalonner et de dégager si besoin une position de Place.
Enfin, l'objectif d'un exercice est d'étudier ensemble les pistes de solution posées sur la table et d'utiliser nos outils de gestion de crise en reconstituant un environnement de stress pour les équipes.
Parvenir à ce résultat nécessite une pré-

paration très lourde du scénario, de bien connaître ses cibles et de préparer réellement les joueurs (leur expliquer les règles, les objectifs pour qu'ils s'investissent vraiment) et de contrer les stratégies d'évitement. Le scénario doit rester inconnu et être accepté tel quel par les joueurs.
Malgré tout, il ne faut pas oublier les limites d'un exercice.
Un exercice qui se déroule sans accrocs est un exercice qui a manqué sa cible. Tous les participants, y compris les animateurs, doivent pouvoir en tirer des enseignements.
Un exercice c'est l'occasion, à chaud, puis à froid de :
• Déceler, nos forces, nos faiblesses, nos manques
• Valoriser et partager nos bonnes pratiques
• Consolider notre relationnel
• Faire émerger des pistes de travail, des préconisations.

En bref, de se poser des questions et de construire nos réponses, nos plans d'actions que nous éprouverons… lors de l'exercice suivant. Il faut sans cesse remettre l'ouvrage sur le métier pour vérifier que nous avançons, sans aucun jugement.

RETOUR SUR LES DERNIERS EXERCICES

Le premier exercice G7 lié au Cyber Expert Group a été organisé et joué en France par le GPR avec plus de 1000 participants sur la seule Place de Paris en 2019. Il a marqué un véritable changement de dimension : les exercices qui jusque-là s'intéressaient principalement aux impacts RH ou sur les locaux, ont commencé à toucher les mécanismes financiers. Cette évolution en termes d'impact coïncidait avec la prise d'importance de l'aspect cyber. Ce scénario exceptionnel est devenu la norme pour les exercices suivants : au cours des 3 jours de l'exercice, nous avons dû faire face à une panne de Target 2, deux jours de modules de contingence successifs, des impacts sur T2S, une cyberattaque internationale coordonnée, 3 banques françaises ciblées et impactées en France, en Europe et dans le monde avec leur système d'information en partie détruit, une panique des publics et un emballement médiatique…. Ces trois jours nous ont fait énormément progresser et ont livré des enseignements nombreux. Le premier a été la confirmation de la pertinence du travail sur la sphère financière. Le deuxième a montré l'appétence de la Place pour ce type d'exercice. Enfin, cette préparation nous a été très utile lorsque nous avons dû gérer une crise réelle, la crise COVID.
Il n'y a pas eu d'exercice en 2020 en raison de la pandémie.
Le 15 juin 2021, l'exercice préparatoire de la stratégie 2021-2023 a vu la première participation de la CCP cyber-IT avec davantage de technique et d'aspect cyber. Pour la première fois, nous avons mis au point un double scénario d'attaque (retail et marché-liquidité), qui a touché directement 7 membres du GPR. 800 spécialistes ont été mobilisés dans le domaine du retail, de l'IT, du cyber, de la liquidité, du fiduciaire, des marchés. En tout 300 événements ou injects ont été envoyés et certains établissements ont reçu jusqu'à 90 injects dans la journée, ce qui laisse imaginer le rythme de l'exercice.
Le scénario de l'exercice a démarré de la manière suivante : au matin, les dirigeants de plusieurs groupes bancaires de la Place ont reçu des menaces de hackers leur demandant de régler une rançon en cryptoactifs, sous peine de voir leur réputation et leur SI détruits. Les établissements ont ensuite constaté des anomalies dans leur système et opérations… l'exercice était lancé.
Cet exercice n'appelle pas de conclusion, mais plutôt un programme et une invitation à nous accompagner dans la démarche. 70 % des membres participant ont identifié des axes d'améliorations à leur dispositif de crise interne, alors qu'au niveau du dispositif du GPR, nous avons repéré des axes forts d'amélioration.
C'est ainsi, depuis 16 ans que le GPR existe, chaque exercice apporte un gain, nous sommes davantage préparés même si cette préparation n'est jamais terminée.

Frédéric Rogé
Expert en gestion et négociation de crise – Incertis, Nantes

Il y a encore un an, j'étais le chef de la cellule négociation du GIGN. Aujourd'hui, je viens vous parler des aspects humains de ces crises.

UNE ORGANISATION HUMAINE QUI EN RANÇONNE UNE AUTRE

Les assaillants font partie d'équipes humaines préparées à rançonner d'autres organisations humaines. Que ce soit dans la menace, dans la préparation ou dans la crise, l'humain est prépondérant. Le nombre d'attaques a sensiblement augmenté entre 2019 et 2020. Les prévisions pour les années à venir ne sont pas meilleures car le mode opératoire de ces assaillants est très rentable. En France, environ 15 % des entreprises ont fait l'objet d'une attaque et une part importante d'entre elles a payé la rançon demandée bien que ce ne soit pas la bonne solution. La France fait partie des pays qui ont le plus payé de rançon en Europe. A cette situation vient s'ajouter le fait que les moyens mis en place pour protéger les entreprises n'ont pas évolué aussi vite que les progrès technologiques.
Ces donneurs de rançons poursuivent plusieurs objectifs : l'activisme, notamment dans le milieu bancaire, et l'espionnage industriel et étatique, mais la menace criminelle (l'appât du gain) reste la motivation première aujourd'hui pour 80 % des assaillants, qui ciblent les entités ayant les capacités financières et les stocks de données suffisants. Le journaliste Damien Bancal, via son blog « Zataz », surveille plus de 180 groupes de criminels (dont seuls 4 ou 5 groupes ont pu être démantelés), contre une trentaine il y a quelques années. Ces groupes se sont professionnalisés et passent du temps à se préparer avec une organisation bien structurée, le commanditaire étant différent de celui qui cherche la vulnérabilité et de celui qui gère le malware. Et s'il y a autant de groupes sur le « marché », c'est parce que le rapport gain/risque reste en faveur des attaquants.
Hormis les rançons, la captation des données peut s'avérer une source de revenus très intéressante, soit pour effectuer d'autres chantages ou les revendre. Les criminels n'hésitent plus à s'attaquer à des organisations nouvelles telles que les hôpitaux car les données recueillies sont pérennes et introuvables ailleurs : il est très facile d'usurper l'identité d'une personne dès lors que

vous disposez de son numéro de sécurité sociale, de sa date de naissance et de son adresse, par exemple.

UNE VOLONTÉ D'AFFAIBLIR L'ORGANISATION VISÉE

Le facteur humain est prépondérant (85 % des attaques sont dues à un facteur humain) parce que les assaillants ont bien compris que chaque collaborateur pouvait représenter une porte d'entrée dans un système d'information, que ce soit sous forme de phishing ou de compromission d'un e-mail professionnel… Il est plus simple de passer par une personne que d'entrer dans des systèmes de sécurité efficaces. Et si l'assaillant n'y arrive pas, il essaie avec la personne suivante ! 1 % seulement de personnel défaillant permet aux attaquants de trouver des informations intéressantes et d'avancer dans leur projet.

Véritables stratèges, les hackers utilisent les biais cognitifs associés aux deux modes de pensée décrits par le lauréat du « prix Nobel d'économie », Daniel Kahneman : le système 1 (rapide, instinctif et émotionnel) et le système 2 (plus lent, plus réfléchi et plus logique). Ils exploitent le sentiment de sécurité des utilisateurs du système, qui est trompeur puisque aucun système n'est fiable à 100 %. Le cas de l'ingénieur qui reçoit un message de son prestataire lui demandant de cliquer sur 3 lignes de code afin de vérifier plus rapidement leur efficacité est révélateur : l'assaillant a trouvé en moins de 2 heures suffisamment d'informations sur les réseaux sociaux pour dresser le cadre de travail de l'ingénieur ; il a repéré le nom de son prestataire et s'est adressé à lui au nom du prestataire, dans un esprit de bienveillance. L'ingénieur ne s'est pas senti en danger et il a cliqué sur le lien, ce qui a permis à l'assaillant de prendre le contrôle de son ordinateur et de préparer une attaque par la suite.

Il est heureusement possible d'améliorer les choses à l'aide d'une bonne sensibilisation : dans le cas précédent, il aurait fallu que l'ingénieur active son système 2 et se pose la question de la légitimité du message du prestataire : pourquoi y a-t-il nécessité d'aller vite ? qui demande l'action ? est-ce le bon canal pour transmettre les informations ? les règles de sécurité sont-elles respectées ? L'ingénieur aurait dû téléphoner à l'auteur du message, vérifier son adresse e-mail ou a minima appeler le RSSI pour qu'il s'assure de l'identité de la personne derrière le lien des 3 lignes de code.

Une autre approche repose sur la compromission interne : certains employés peuvent, par mégarde, envoyer des fichiers complets de clients à un de leurs prestataires, ou se filmer dans des vidéos où apparaissent des informations sensibles à l'écran. Un collaborateur peut aussi décider de voler un fichier client pour le vendre à son nouvel employeur. Heureusement, les systèmes d'information peuvent être programmés pour relever des actions ciblées sur des comportements malveillants. Il est aussi possible d'impliquer les collaborateurs et de les sensibiliser pour qu'ils relèvent voire signalent des comportements suspicieux (horaires atypiques, non-respect des règles de sécurité, agissement inhabituel…), susceptibles de déclencher une vérification des informations par les spécialistes du système d'information, ceci afin de réduire le facteur humain dans la compromission.

Enfin, le facteur humain est prépondérant dans la gestion de crise. Comme l'indique Sébastien Meunier, il est fréquent (pour l'instant aux Etats-Unis, mais cela va bientôt arriver en Europe) d'avoir des pénalités lorsque la cybersécurité n'est pas bien architecturée : l'organisation doit être capable de démontrer sa résilience.

Pourquoi ? Comme l'indique Stéphane, il ne s'agit pas, lorsqu'une crise survient, de déployer le plan de continuité d'activité (PCA) : la part d'impondérables ou de problèmes sous-estimés qui surgit rend impossible d'appliquer le PCA dans son ensemble. Si, avant la survenue de la crise, l'organisation ne s'est pas exercée, il sera difficile de mobiliser l'ensemble des parties prenantes. Elle subira un effet de latence qui aura pour conséquence la paralysie complète de l'organisation. Le déni de la crise est naturel, mais il peut être contré au quotidien en travaillant sur des exercices.

LA CRISE CYBER : UN TEST DE RÉSILIENCE

Les groupes de hackers accumulent les procédés de pression. Le chiffrage des données avec demande de rançon est souvent accompagné d'un ultimatum, de la menace d'un arrêt du système de supply chain, d'une campagne de dénigrement de vos produits, du déploiement de campagnes téléphoniques pour diffuser en interne que votre organisation est attaquée, etc.

La survenue d'une crise porte les regards sur votre organisation. Vous serez jugés a posteriori sur la façon dont vous avez géré cette crise et votre système de cybersécurité fera peut-être même l'objet d'un audit.

Ce n'est pas au moment de l'attaque qu'il faut décider s'il faut payer la rançon, la manière de construire la communication, l'analyse de l'impact de l'absence du système d'information pendant plusieurs jours et le choix des priorités pour le reconstruire ou encore, de s'assurer de la conformité des solutions envisagées. Un modèle de gestion des imprévus et de l'incertitude doit être développé. Par exemple, dans une crise cyber, la gestion du temps n'est pas du tout la même que dans une crise classique. Le système de prise de décision dans l'incertitude doit être travaillé, avec un leadership et une communication efficace, pour pouvoir garder le cap. On peut citer en exemple la communauté de communes d'Angers qui a publié un journal de bord hebdomadaire pour montrer ses difficultés en délivrant des éléments factuels à la suite de la cyberattaque dont elle a été victime, journal complété par une vidéo du Maire souhaitant partager son retour d'expérience.

Cette gestion de la communication doit faire la part belle aux collaborateurs. Certains ingénieurs ayant dû faire face à une attaque ont été un peu moins collaboratifs par peur d'être licenciés : c'est aux dirigeants d'aller les rassurer. De même, c'est à l'entreprise de communiquer en interne sur l'impact des vols de données sur les collaborateurs pour éviter des recours collectifs.

Conclusion

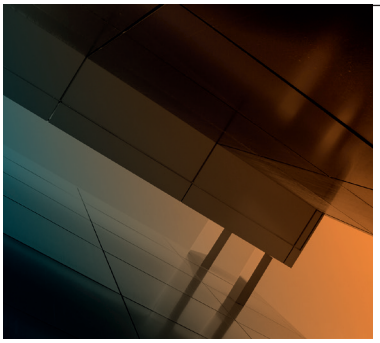
Stéphanie Saint Pé, *Déléguée Générale,* ***AFTI***

Pour conclure, je souhaite vous donner quelques éléments s'appliquant spécifiquement à notre monde financier :

- La blockchain n'est pas aussi sécurisée qu'on ne le croit ;
- Il faut anticiper les crises ;
- Les crises peuvent avoir un impact systémique, d'où la nécessité des travaux de Place collectifs comme ceux menés par la Banque de France ;
- Le risque 0 n'existe pas ;
- Le facteur humain est une faiblesse, mais il peut devenir une aide si les collaborateurs sont correctement sensibilisés ;
- Chacun peut être concerné de manière individuelle par des biais cognitifs exploités par les hackers ;
- L'impondérable imprévu arrive toujours, comme en témoigne l'interruption de connexion subie par Frédéric Roger !

Nous avons désormais une bonne connaissance de cet environnement de cybersécurité qui devrait permettre à chacun, individuellement et au sein de ses structures professionnelles, de se poser les bonnes questions.

Je remercie les intervenants de grande qualité et vous donne rendez-vous pour la prochaine conférence qui aura lieu le 19 novembre et aura pour thème l'impact de la finance durable sur les métiers du post marché, en partenariat avec la FBF et l'AFG.



Spécial Conférence

Périodique édité par l'AFTI • ISSN 2677-4755

Directeur de Publication : Stéphanie Saint Pé
Rédacteur en chef : Stéphanie Saint Pé
Rédaction : Anne Bechet
Réalisation : Café Noir

Les supports de présentation sont disponibles sur www.afti.asso.fr

La dynamique du post-marché

Association Française
des Professionnels des Titres
36, rue Taitbout - 75009 PARIS
Tél. : 0148005201
Fax : 0148005048