ÉTUDE DE DOSSIER

Cadre 2019-01

La multiplication des cyber-attaques ces dernières années a incité les principaux acteurs de l'économie mondiale à adopter une approche de type « cyber-résilience » dans la gestion de la sécurité informatique.

À partir des documents qui vous sont proposés, vous répondrez aux questions suivantes :

1. Définissez le concept de « cyber-résilience ».
2. Comment les entreprises organisent-elles leur « cyber-résilience » ?
3. Les banques centrales ont-elles un rôle à jouer en matière de cyber-résilience ? Si oui, comment ?

Les questions sont indépendantes ; nous vous recommandons toutefois de les traiter dans l'ordre. Il n'est pas nécessaire de recopier l'intitulé des questions.

LISTE DES DOCUMENTS JOINTS

1. **Introductory remarks (B. Coeuré)**
   www.ecb.europa.eu – 19/06/2017 – 3 pages
2. **Que retenir des cyberattaques qui ont frappé l'industrie en 2018 ?** – R. Amalvy
   www.usinenouvelle.com – 14/01/2019 – 2 pages
3. **De la cyber-sécurité à la cyber-résilience** – Y. Reding
   www.lesechos.fr – 14/03/2018 – 2 pages
4. **Face à un cyber ouragan, comment la France peut se preparer** – H. Meddah
   www.usinenouvelle.com – 21/11/2018 – 2 pages
5. **No Target is Too Small : Why SMEs Must be Cyber-Resilient** – M. Wilczek
   www.infosecurity-magazine.com – 24/12/2018 – 2 pages
6. **La cyberguerre est déclarée** – S. Caulier
   www.lemonde.fr – 02/12/2018 – 5 pages
7. **Coup d'envoi du mois européen de la cyber-sécurité** – M. Daoua
   www.actualitesdudroit.fr – 02/10/2018 – 3 pages
8. **Cyberattaques : apprendre à travailler sans ordinateurs** – J. Henno
   www.lesechos.fr – 30/03/2018 – 3 pages
9. **Why is cyber resilience important?**
   www.ecb.europa.eu – 10/04/2018 – 1 page
10. **Cyberguerre : la cyber-résilience n'est pas le vaccin mais un bon contrepoison**
    Y. Chatelain – www.forbes.fr – 05/02/2019 – 3 pages
11. **Les 5 indicateurs d'une cyber-résilience optimale** – S. Terrey
    www.itpro.fr – 01/03/2017 – 2 pages
12. **Succès de l'exercice de crise cyber de la Place financière de Paris**
    www.banque-france.fr – 15/11/2018 – 1 page
13. **Best Cyber Resilience Initiative: Bank of England** – R. King
    www.centralbanking.com – 06/09/2018 – 1 page
14. **Fin du cash : pourquoi les banques centrales travaillent aux monnaies numériques d'État**
    D. Cuny – www.latribune.fr – 19/11/2018 – 3 pages
15. **En quoi la capacité de résistance informatique est-elle importante ?**
    www.ecb.europa.eu – 10/04/2018 – 1 page
16. **La BRI lance une réflexion sur les monnaies numériques émises par les banques centrales**
    www.lefigaro.fr – 12/03/2018 – 1 page

Introductory remarks (B. Coeuré)

Remarks by Benoît Cœuré, Member of the Executive Board of the ECB, at the High-Level Meeting on Cyber Resilience, Frankfurt am Main, 19 June 2017.

Introduction

It is a pleasure to welcome you here today to this strategic high-level meeting on cyber resilience for pan-European financial market infrastructures.

The aim of bringing together high-level representatives from large European market infrastructures, critical service providers and public authorities is threefold:

First we would like to gain a deeper understanding of the cyber threat landscape in Europe.

The European Union Agency for Network and Information Security (ENISA) will make a presentation on the cyber threat landscape and its relevance for the financial sector.

Second, we will share with you the Eurosystem's cyber strategy for financial market infrastructures and also explain ECB Banking Supervision's approach to the issue of bank cyber resilience.

Third, we would like to hear your views on how we can all collaborate in a trusted environment to enhance the cyber resilience of financial market infrastructures.

More specifically, we would like to assess with you how much interest there is in creating a high-level cyber resilience forum for pan-European financial market infrastructures, critical service providers and competent authorities.

Before we start, let me briefly set the scene.

The evolving cyber threat landscape in Europe

Besides the undeniable advantages of information and communication technology, the increase in users and data on digital platforms, in cloud computing and across networks has also created greater opportunities for cybercrime.

There are a variety of agents involved: criminals, hacktivists or nation states.

They may have different motives: financial gain, espionage, disruption and destabilisation.

But what they all have in common is that they are steadily increasing their level of sophistication and exploring ways of attacking.

A sound operational risk management and IT security framework are the first line of defence.

But resilience to cyberattacks means more than that. Unlike critical failures, the likelihood of cyberattacks cannot be mitigated. A paradigm shift is necessary. We have to accept that

cyberattacks are inevitable and that attackers are persistent. Consequently, we have to establish how – in case of persistent attacks – we prioritise our operations and resources, protect our key assets and restore functionalities. Cyber resilience goes beyond technology, it also encompasses governance, company culture and business processes.

Given the extensive interlinkages and interdependencies in the financial system, it is obvious that markets' overall cyber resilience depends not only on the resilience of each individual market actor but also on that of interconnected market infrastructures, participants and service providers.

The Eurosystem cyber strategy for financial market infrastructures

Following the increase in both the frequency and severity of cyberattacks over the last few years, legislators, regulators and standard setters have issued legislation and guidance on cyber security at national and international level and at cross-sectoral as well as sector-specific level.

Let me briefly mention three initiatives.

First, in 2016, the EC adopted the Directive on security of network and information systems (the NIS Directive).

Its aim is to bring the cybersecurity capabilities of operators of essential services to the same level of development in all the EU Member States and to ensure an efficient exchange of information and good cooperation on the topic throughout the EU.

Second, at international level, the G7 countries have drawn up a set of fundamental elements of cybersecurity for the financial sector, as well as three further recommendations on the effectiveness of cybersecurity assessments, third-party risks, and coordination with other critical sectors.

Third, with a key focus on financial stability, the CPMI-IOSCO published a principles-based "Guidance on cyber resilience for financial market infrastructures" in June 2016.

Supplementing the "Principles for Financial Market Infrastructures", it provides additional detail related to the preparations and measures that financial market infrastructures should undertake to enhance their cyber resilience.

In recognition of the escalating cyber threats, the legislative and regulatory guidance and the required paradigm shift, the Eurosystem's overseers have launched a strategy for cyber resilience in relation to financial market infrastructures. This strategy – which will be explained in more detail at agenda item 3 – is built on three pillars.

- The first pillar refers to the cyber resilience of individual financial market infrastructures.
- The second pillar refers to the resilience of the financial sector as a whole.
- The third pillar highlights the importance of establishing a forum which brings together market actors, competent authorities and the cybersecurity service providers.

This brings me to the third and final objective of today's meeting.

Creation of a high-level cyber resilience forum

Tackling cyber risk is not for regulators or market actors in isolation.

Rather it is a collaborative endeavour that must be undertaken together.

Hence, I invite you to seriously consider the creation of a high-level cyber resilience forum for pan-European financial market infrastructures, critical service providers and competent authorities.

I am convinced that there is cross-fertilisation and collective learning to be gained from such collaboration and I am looking forward to a fruitful meeting today.

Que retenir des cyberattaques qui ont frappé l'industrie en 2018 ?

Comme chaque année, l'association Clusif a présenté son panorama de la cybercriminalité. Entre les scandales, les fuites et les cyber piratages, l'année 2018 fut noire pour plusieurs secteurs industriels, comme la santé et le maritime. L'Usine Nouvelle fait le point sur ce qu'il faut en retenir.

2018, année des fuites et des piratages ? Le 10 janvier, le Club de la Sécurité de l'Information français (Clusif), une association centrée sur la cybersécurité, a dévoilé son panorama de la cybercriminalité.

L'année fut noire pour certains, et pas seulement le géant américain Facebook, confronté au scandale Cambridge Analytica (violation de données majeures, collecte sans consentement des données personnelles, Mark Zuckerberg contraint de s'expliquer devant le Sénat...).

Le secteur maritime fragilisé

D'autres, moins chanceux, ont été les victimes d'attaques de hackers. C'est le cas du secteur maritime. Ainsi, trois ports ont été victimes de rançongiciels, heureusement rapidement contenus pour éviter l'impact opérationnel : Long Beach Port en Chine, Barcelone en Espagne, et San Diego aux États-Unis.

Bien qu'on les ait longtemps pensé protégés car isolés au milieu de la mer, les navires sont de plus en plus connectés, et donc de plus en plus vulnérables. Reliés en permanence à internet pour leurs systèmes de cartographie ou de pilotage automatique, voire même pour la gestion des moteurs, les risques peuvent rapidement devenir critiques sans protection adéquate. Mais les choses s'améliorent. En décembre dernier, l'International Association of Classification Societies a publié douze recommandations sur la cybersécurité maritime.

Les secteurs médicaux et aériens pas épargnés

Le secteur médical n'aura pas non plus été épargné par les cyberattaques. Cibler les hôpitaux permet aux pirates de mettre la main sur des données sensibles pouvant donner lieu à des chantages financiers, des usurpations d'identités ou des déstabilisations de personnalités « importantes ». Entre le 25 juin et le 4 juillet, une cyberattaque visant en particulier le Premier ministre de Singapour a permis le vol d'1,5 million de dossiers médicaux, soit 25 % de la population de la cité-État. À l'aide d'un ordinateur infecté par un malware, les hackers ont réussi à accéder aux bases de données médicales, elles-mêmes mal protégées.

Qu'il s'agisse de logiciels malveillants, de hameçonnage (phishing) ou de simples erreurs du personnel, les procédés d'intrusion restent classiques. L'hyper-connexion de plus en plus fréquente des appareils biomédicaux ne devrait rien arranger. Le secteur médical devrait rester « une cible privilégiée pour les cybercriminels », selon Erwan Brouder de BSSI Conseil.

Même son de cloche du côté du secteur aérien, « un écosystème dont tous les acteurs dépendent les uns des autres pour fonctionner », selon Vincent Mignon, du groupe ADP. Pour répondre à des attaques toujours plus nombreuses, « les différentes parties prenantes s'organisent et se structurent pour améliorer la cyber-résilience globale de l'ensemble du secteur », précise-t-il.

Des failles sensibles côté « hardware »

En début d'année dernière, les failles de sécurité Meltdown et Spectre, identifiées sur certains processeurs, se sont vues plus difficiles à gérer que prévu. Des recherches universitaires ont permis de déceler un défaut de conception très profond. Pour Loïc Guézo, de Trend Micro, « seuls des changements d'architecture dans les prochaines versions de microprocesseurs pourraient régler la vulnérabilité qui affectent les processus d'exécution spéculative, les caches internes du CPU et d'autres étapes d'exécution internes ».

Malgré tout, le piégeage « software » sera resté supérieur en 2018, notamment grâce aux pirates de Magecart. « 21 lignes de code changées dans un JavaScript de 2012, et British Airways a vu 77 000 données complètes de paiement fuiter », a ainsi rappelé Loïc Guézo.

La fin des mots de passe ?

La conférence du Clusif a enfin été l'occasion de rappeler l'importance de bien choisir ses mots de passe. Parmi les plus utilisés, on retrouve toujours « 123456 », « password » ou « 000000 ». Pour éviter aux moins inspirés de se faire subtiliser leurs données, de plus en plus de services proposent désormais des modes d'authentification multi-facteurs (MFA), comme la reconnaissance faciale ou digitale et les codes reçus par SMS.

Mais cette dernière méthode atteint ses limites. Les cas de sim swap (un individu va voir votre opérateur en se faisant passer pour vous, demande une nouvelle carte Sim et accède à vos SMS) permettent d'outrepasser cette protection. D'autres techniques de MFA devraient se démocratiser, notamment grâce au Machine learning. Reste à voir si elles feront disparaître le traditionnel mot de passe.

Rémi Amalvy

De la cyber-sécurité à la cyber-résilience

Dans un environnement de plus en plus incertain, garantir la continuité du business exige d'adopter des approches plus proactives et mieux intégrées. En appliquant les dernières normes et les meilleures pratiques, pour assurer une protection des systèmes « by design » et garantir la confiance des organisations dans le numérique, la cyber-résilience devient fondamentale.

L'année 2017, charnière dans la transformation numérique des entreprises, a vu les systèmes informatiques et les professionnels de la cyber-sécurité mis à rude épreuve. En effet ces derniers mois, des attaques DDoS massives et plusieurs épidémies de ransomware sont venues perturber les activités d'organisations internationales. Beaucoup ont subi des prises d'otage ou ont été paralysées par des attaques malveillantes. Des processus électoraux au sein de pays démocratiques ont même été perturbés par des cyber-activistes aux intentions douteuses.

2017 a été marquée par une nouvelle ère numérique. La multiplication des attaques a mis en évidence les fragilités de nos organisations et les failles de nos sociétés de plus en plus digitales. On a découvert par la même occasion les limites d'une approche traditionnelle en cyber-sécurité, qui vise essentiellement à protéger les systèmes. La cyber-sécurité est dépassée, car trop restrictive ; il faut une approche globale totalement intégrée impliquant à la fois les individus, les processus et la technologie : la cyber-résilience.

Opter pour une approche active

La gestion des données sensibles requiert une approche plus holistique de la sécurité digitale, mieux intégrée aux enjeux organisationnels et business. Dans le contexte actuel, il faut changer de paradigme. La question n'est plus de savoir si l'on va être attaqué, mais bien quand ! À partir de là, nous devons pouvoir mieux nous préparer à absorber le choc, réagir à toute éventualité et rebondir.

Chacun évolue dans un environnement, le cyberespace, incertain, instable, potentiellement hostile. À la manière d'un kayakiste qui descend un torrent et doit jouer avec le courant, éviter les rochers, l'organisation au cœur du cyberespace doit gagner en agilité et en flexibilité. Il faut pouvoir évoluer en tenant compte des éléments présents dans son environnement.

Face à l'éventualité d'un incident de sécurité ou de continuité, il faut opter pour une approche proactive, dynamique, composer en permanence avec les éléments, anticiper et contourner les obstacles, surfer, accélérer, rester la tête hors de l'eau.

Pour certains, moins bien préparés, l'objectif premier sera de survivre. Pour les plus résilients, il s'agira au contraire de rebondir, d'avancer et de profiter de la vitesse du torrent.

Identifier, protéger, détecter, répondre, récupérer : les cinq piliers de la cyber-résilience

La cyber-résilience constitue une approche globale qui intègre cyber-sécurité, continuité d'activité, gestion de crise, stratégie de réponse et organisation de la résilience. En permanence, il faut pouvoir identifier, protéger, détecter, répondre à l'incident et récupérer les systèmes pour garantir la continuité de l'activité et rebondir. C'est l'approche suggérée par la directive NIS, qui

vise à sécuriser les réseaux et les systèmes d'information contre tout risque et incident au niveau des infrastructures critiques européennes.

Finalement, la cyber-sécurité n'est qu'un sous-ensemble de la cyber-résilience. On parle de développer pour chaque activité dépendante du numérique un système immunitaire performant. Pour qu'il soit efficient, il faut que les différentes composantes de l'organisation interagissent de manière coordonnée, selon une approche systémique.

Mettre en œuvre une approche par les normes

Pour inviter les acteurs à mieux évoluer et se protéger dans cet univers incertain, les organisations internationales et autorités publiques prônent le développement et le respect de normes toujours plus poussées - ISO 27001 (gestion de la sécurité de l'information), 20000 (gestion des services informatiques), 27018 (protection des données à caractère personnel) ou 22301 (gestion de la continuité d'activité). Ainsi, la nouvelle norme française d'Hébergeur de Santé à caractère personnel qui sera d'application en 2018 exigera les normes ISO 27001, 20000 et 27018.

De même, pour construire le marché unique digital européen, l'Union européenne se dote de nouveaux outils, comme une agence de la cyber-sécurité (rôle confié à l'ENISA) ou encore la directive NIS.

Pour les opérateurs de service numérique, il est fondamental de développer une proposition de valeur de bout en bout dans le domaine de la gestion des données sensibles. Cela permet de garantir la continuité, la sécurité, la protection des activités des clients face à l'ensemble des risques. En apportant toutes les garanties de confiance, les opérateurs de service numérique créent de la valeur dans ce monde digital de plus en plus incontournable, mais également de plus en plus complexe et incertain.

Élaborer une approche « cyber-résilience » intégrée à grande échelle

Choisir une approche intégrée suivant une stratégie d'amélioration continue garantit la protection des clients face aux risques de plus en plus menaçants. Faire évoluer son Security Operation Center (SOC) en intégrant des solutions d'investigations sécurité est également fondamental. Grâce à des algorithmes sophistiqués, celles-ci conduisent à une détection prédictive des menaces au départ de l'analyse des comportements déviants au sein des systèmes d'information. En sus, elles constituent un composant clé dans l'investigation et la remédiation.

Autre vecteur de succès, l'intégration d'équipes de conseil et d'équipes opérationnelles renforce considérablement les centres de compétences « cyber-résilience ».

On ne peut plus séparer les enjeux business des problématiques de continuité, de sécurité et de résilience. Les divers éléments entrant en ligne de compte pour garantir le fonctionnement du business doivent être totalement intégrés, comme les cinq doigts d'une même main. Il nous faut mettre en œuvre des approches de cyber-résilience « by design » renforcées et de bout en bout.

La résilience de toute activité, et donc de l'économie digitale, se joue de plus en plus à l'échelle européenne. Seul, dans son pays, on ne peut pas y arriver. Nous devons favoriser l'émergence de mécanismes de lutte plus efficients à l'échelle du marché numérique unique, notamment en matière de gestion de l'information la plus sensible.

Yves Reding

Face à un cyber ouragan, comment la France peut se préparer

Mieux échanger l'information sur les cyberattaques, protéger les PME, renforcer l'arsenal législatif, développer l'expertise technologique et la formation... Le rapport « Cybermenace : avis de tempête » de l'Institut Montaigne préconise une dizaine de mesures pour renforcer la capacité du pays à faire face à une cyberattaque aussi massive que destructrice.

Trains et avions bloqués, médias incapables d'émettre, des milliers d'entreprises touchées, des millions d'ordinateurs infectés, les services de l'État paralysés en partie... Et si un cyber ouragan s'abattait sur la France, une cyberattaque massive et destructrice capable de mettre à mal les infrastructures critiques et le tissu économique du pays ? L'Institut Montaigne a imaginé un tel scénario catastrophe dans son rapport « *Cybermenace : avis de tempête* » publié mercredi 21 novembre. L'exercice n'est pas si théorique que cela.

« Les attaques de l'été 2017 (WannaCry et Notpetya) ont eu des conséquences graves pour les acteurs touchés. (....) Elles sont notamment la preuve que le risque d'une attaque large touchant l'ensemble du tissu économique est réel », souligne l'étude. Les facteurs aggravants sont connus : interconnexion à outrance des systèmes d'information, recours massif aux technologies de stockage dans le Cloud, développement exponentiel des objets connectés, uniformisation des technologies informatiques...

Développer la cyber-résilience

Pour éviter une telle catastrophe, les auteurs du rapport appellent à développer une cyber résilience, soit la capacité à rapidement endiguer une attaque, en limiter les effets et reprendre l'activité au plus vite. Ils avancent une dizaine de mesures concrètes à prendre pour anticiper un tel cyber ouragan et s'y préparer à la fois au niveau de l'État et des entreprises.

Certaines de ces mesures sont réalisables aisément. Pour mieux connaître leur vulnérabilité, les auteurs incitent les entreprises à réaliser un diagnostic de cybersécurité annuel incluant les recommandations de base pour couvrir les risques révélés. Selon eux, il faut avant tout mieux protéger les PME, considérées comme « *des points d'entrée privilégiés pour les attaquants dans la chaîne d'approvisionnements des grands groupes* ». Cela passe par le développement d'une offre de cybersécurité prête à l'emploi et d'un coût abordable. Le rapport préconise de faire appel à la communauté des experts comptables, les interlocuteurs naturels des chefs d'entreprise en matière de risque pour leur société.

Le rapport propose de renforcer l'arsenal législatif lié à la sécurité informatique. Les auteurs sont favorables à un renforcement de la loi de programmation militaire (LPM) qui impose notamment aux OIV (opérateurs d'importance vitale, ndlr) de relever leur niveau de cybersécurité. Ils voudraient inclure de nouvelles exigences comme la réalisation d'un exercice annuel de crise et la mise en place d'un système d'information de secours indépendant du système d'information nominal qui pourrait être paralysé.

Des recommandations sont également formulées en matière de recherche. Des priorités sont ciblées. « *Il faut accélérer les investissements dans les technologies d'apprentissage automatique associées à la cyber pour être en mesure de répondre à des attaques larges et rapides* ».

Une plateforme d'information sur les cyberattaques

Les rapporteurs conseillent la mise en place de nouveaux outils collectifs pour éviter la propagation d'une cyberattaque. Comme une plateforme de diffusion des signatures d'attaque caractérisant le mode opératoire des attaquants. Cette plateforme d'échanges serait opérée soit par l'État soit par un ou des acteurs majeurs français de la cybersécurité. « *Cette structure pour échanger de l'information constitue un manque flagrant aujourd'hui* », déplore l'étude.

Enfin pas de cybersécurité sans experts ! Or la France souffre d'une pénurie de techniciens et d'ingénieurs en sécurité informatique. L'étude préconise de mettre les bouchées doubles dans le domaine de la formation et souligne la responsabilité de la puissance publique. À l'État de créer un parcours de formation incitatif sachant que le coût des études longues ou de formation de reconversion constituent une barrière financière. Selon les auteurs du rapport, l'ensemble de leurs propositions ne seront réellement efficaces que dans un contexte où les dirigeants politiques et économiques sont hautement sensibilisés aux enjeux de la cybersécurité.

Hassan Meddah

5

No Target is Too Small: Why SMEs Must be Cyber-Resilient

Cyber-attacks have hit, and hurt, companies of all shapes and sizes. The financial costs arise from the attack itself, fixing it, and addressing the reputational impact by re-fostering public trust, along with potential regulatory fines and legal bills.

Even so, many organizations – especially micro and small businesses – are unprepared to defend themselves against the increasing threat of cyber-attacks.

This is concerning for several reasons, and not just because small businesses are the number-one employer in most economies. If a smaller company has to close its doors, even for a relatively short period, the negative impact on the business can be huge, far larger than it might be for a large, well-funded business that has multiple service areas and locations.

This was highlighted in an October 2018 survey, which found that the average amount demanded during a ransomware attack is $1,077 – but the average cost to remediation cost to businesses is $133,000, when downtime, recovery costs and lost business opportunities are factored in. While these costs are troubling enough for enterprise organizations, they could well be unaffordable for many SMEs. Paying the ransom is not an option, as less than 20% of victims who do give in to the extortion demand actually get their data unlocked.

SMEs exposed to attack

The Cyber Security Breaches Survey 2018 commissioned by the UK's Department for Digital, Culture, Media & Sport, found that micro/small businesses are less apt than medium or large businesses to combat cyber-threats. While 79% of the latter have actively looked for information, advice or guidance about cyber security, only 58% of micro or small businesses have done the same. The differences become even more stark with respect to cybersecurity policies (26% vs. 62%) and training (19% vs. 47%). The numbers are clear: SMEs are simply more vulnerable to cybercrime.

Although just over half (55%) of SMEs have carried out health checks, risk assessments or audits to identify cybersecurity risks, a quarter (25%) have not implemented any cybersecurity governance or risk management measures. Also just 12% of micro/small businesses have instituted a formal cybersecurity incident management process.

Fortunately, awareness of this issue is on the rise. The directors or senior management in three-quarters (74%) of micro/small businesses place a high priority on cybersecurity. However, the necessity is obvious in light of the facts. 42% of micro/small businesses identified at least one breach or attack in the last year. In 17% of incidents, these businesses took 24 hours or more to recover from the breach.

The #1 attack trends: ransomware and DDoS

Over the past few years, ransomware and distributed denial of service (DDoS) attacks have become notoriously common and caused countless small business owners to lose sleep – and, sometimes, big money. According to the UK's National Crime Agency's 2017/2018 Cyber-Threat to UK Business Report, both of these threats comprise the top attack trend.

These attacks can be truly damaging, even fatal, to a vulnerable target. If the IT systems of a small e-commerce business are inaccessible or down for many hours or days, the ramifications can be brutal.

In the digital era, business can be brought to a standstill with just a few clicks. POs can no longer be placed or processed, billing can't be done, or the firm's customer database is locked down. Ouch.

Unfortunately, various Cybercrime-as-a-Service platforms on the Darknet sell ransomware toolkits or targeted DDoS attacks for as little as $10, so cybercrime is easier and more accessible than ever. For criminals who know their way around this shady corner of the web, taking advantage of illegal tools and the capabilities of the black market is simple and cheap.

Ignoring or downplaying risk management in the digital world is like playing Russian roulette – the odds are not good, and there is everything to lose. The increased awareness about cyber-threats among SMEs is encouraging, but insufficient to keep the bad guys at bay. SMEs must do more. They need to take tangible action and play catch-up with their big-boy counterparts that take cyber-threats seriously.

However, building in-house expertise can be costly and time-consuming – especially in light of the ever-increasing shortage of cybersecurity professionals. To speed things up and benefit from economies of scale, SMEs should consider engaging a security-specialized consulting firm to help them identify any compromising loopholes.

If it's too expensive or complicated to implement the right tools and to operate them around the clock, a managed service provider can be recruited to run the various security services along the SME's IT value chain.

Since these providers usually have a shared infrastructure spread across hundreds or thousands of clients, their fees are typically less than the costs associated with the do-it-yourself approach.

Avoiding an attack is the top priority, but businesses should consider "what-if" scenarios and institute a corporate cybersecurity incident management process that can assist them during a potential crisis. Whether it's about troubleshooting, restoring IT backups, stakeholder management or customer communication, nothing is more effective than a capable team that knows precisely what to do when an attack strikes, and how to get things back on track across multiple work streams.

No business is too small to be attacked; but equally, with the right approach to security, no business is too small to defend itself.

Marc Wilczek

La cyberguerre est déclarée

Sensibilisés par les cyberattaques WannaCry et NotPetya en 2017, gouvernements et grandes entreprises ont réagi en créant des instances et des plans de cyberdéfense. Mais les PME restent à la traîne.

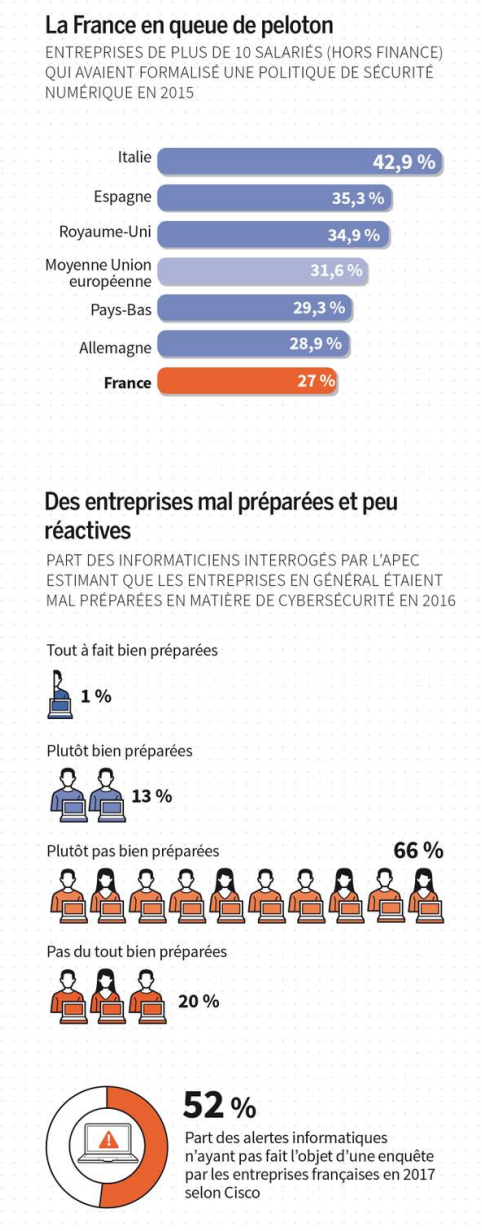
L'ambiance du Forum de gouvernance de l'Internet (FGI) était plutôt solennelle ce 12 novembre. Dans la grande salle de l'Unesco à Paris, en présence du secrétaire général des Nations unies (ONU), Antonio Guterres, le président de la République Emmanuel Macron lançait officiellement l'Appel de Paris.

Déjà signée par une soixantaine d'États et plusieurs centaines d'entreprises privées et d'organisations, cette déclaration appelle tous les acteurs de l'Internet à élaborer et à partager des principes de sécurisation du cyberespace. Le texte prend acte de l'omniprésence du numérique dans nos existences et alerte sur la multiplication et la gravité des menaces : *« Le développement de la cybercriminalité et d'activités malicieuses peut aussi bien mettre en danger nos données privées que certaines infrastructures vitales »*, affirme-t-il.

L'avertissement n'est pas exagéré. L'année 2017 a connu de nombreuses attaques informatiques particulièrement virulentes dont l'objectif n'était pas seulement le vol ou la demande de rançon.

Dans son bilan 2017, l'Agence nationale de la sécurité des systèmes d'information (Anssi) constate l'apparition de deux nouvelles finalités des cyberattaques : la déstabilisation des processus démocratiques, notamment par la perturbation des élections, et la déstabilisation de l'ordre économique ciblant des entreprises précises. L'Anssi constate aussi la prolifération d'outils d'attaques sophistiqués et, plus inquiétant encore, la recrudescence d'attaques aux effets destructeurs. L'agence a traité pas moins de 1 621 événements de sécurité numérique sur 2 435 signalés, dont vingt incidents majeurs, douze opérations de cyberdéfense d'organisations vitales ou sensibles et trois crises publiques.

Le ton a changé. Il est maintenant question de cyberguerre. Les attaques ne proviennent plus seulement d'officines mafieuses qui utilisent le numérique à des fins économiques (rançons, blanchiment, trafics en tout genre). Désormais, elles menacent la démocratie (élections, infox), l'économie (blocage de l'activité) et la vie humaine (énergie, transports, hôpitaux, système de santé). Et nombre d'entre elles sont menées par des groupes souvent aux ordres de leur gouvernement. Soulignons que la Russie n'a pas signé l'Appel de Paris, ni d'ailleurs les États-Unis et la Chine…



(…) Le Comcyber assure la cyberdéfense des armées

Du côté des pouvoirs publics, la riposte s'organise. Le secrétariat général de la défense et de la sécurité nationale (SGDSN) a publié sa « Revue stratégique de cyberdéfense » en mars. « C'est le vrai document fondateur, le premier exercice de synthèse stratégique », souligne Gérôme Billois, associé cybersécurité du cabinet conseil Wavestone.

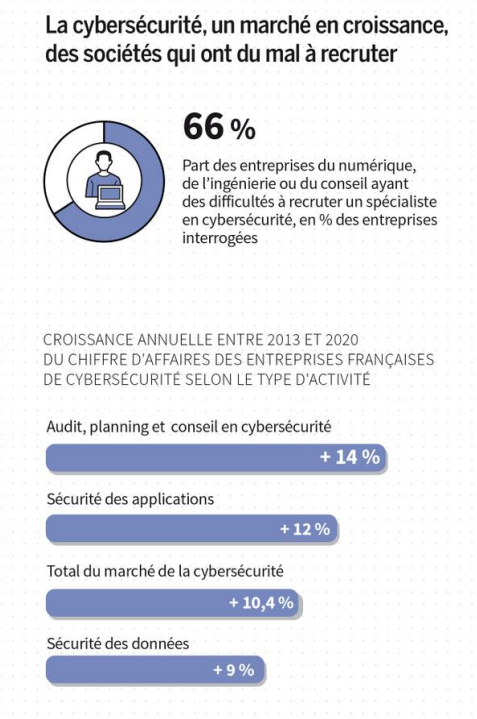
Ce livre blanc fait le bilan des risques et des menaces, il pose les responsabilités des acteurs et notamment de l'État, chargé de la cyberdéfense de la nation et garant de la cybersécurité de la société. « Cette distinction est importante, c'est la caractéristique du modèle français qui sépare l'offensif du défensif ». Dans ce modèle, l'Anssi est chargée de la cyberdéfense de l'État alors que l'offensif relève du monde du renseignement.

Créé en 2017, le commandement de cyberdéfense, alias Comcyber, s'ajoute à ce dispositif et assure la cyberdéfense des armées. Signe de la prise de conscience des enjeux au plus haut niveau de l'État, les membres du Comcyber ont participé pour la première fois au défilé du 14 juillet sur les Champs-Élysées.

Côté entreprises, la situation est beaucoup plus contrastée entre les grands groupes et les TPE-PME. L'édition 2018 du rapport sur les risques mondiaux du World Economic Forum montre que les premiers ont pris la mesure des enjeux. En effet, l'étude place les cyberattaques et la fraude ou le vol de données respectivement au troisième et quatrième rangs des risques probables pour les dix prochaines années, derrière les événements météorologiques extrêmes et les catastrophes naturelles.

Preuve que l'attaque NotPetya a marqué les esprits des grands patrons et leur a fait prendre conscience de la vulnérabilité de leurs systèmes d'information devenus essentiels à leurs activités. Preuve qu'ils se sont également rendus compte des conséquences économiques d'un vol ou d'un détournement de données depuis l'entrée en vigueur, en mai, du Règlement européen sur la protection des données (RGPD), dont les sanctions peuvent atteindre 4 % du chiffre d'affaires mondial de leur entreprise.

« Les dégâts causés par NotPetya, notamment à Saint-Gobain, ont fait progresser le sujet de la cybersécurité dans la tête des dirigeants. La numérisation des entreprises change beaucoup de choses. Il faut dire qu'avec le cloud, les plates-formes installées pour l'essentiel à l'étranger et les logiciels collaboratifs, comme par exemple SharePoint, elles ont quasiment perdu le contrôle de leurs données », affirme Alain Bouillé, président du Club des experts de la sécurité de l'information et du numérique (Cesin). Cette instance, créée il y a six ans, rassemble des responsables de la sécurité des systèmes d'information (RSSI) d'entreprise. Le nombre de ses membres est passé de 30 au départ à 480 aujourd'hui.



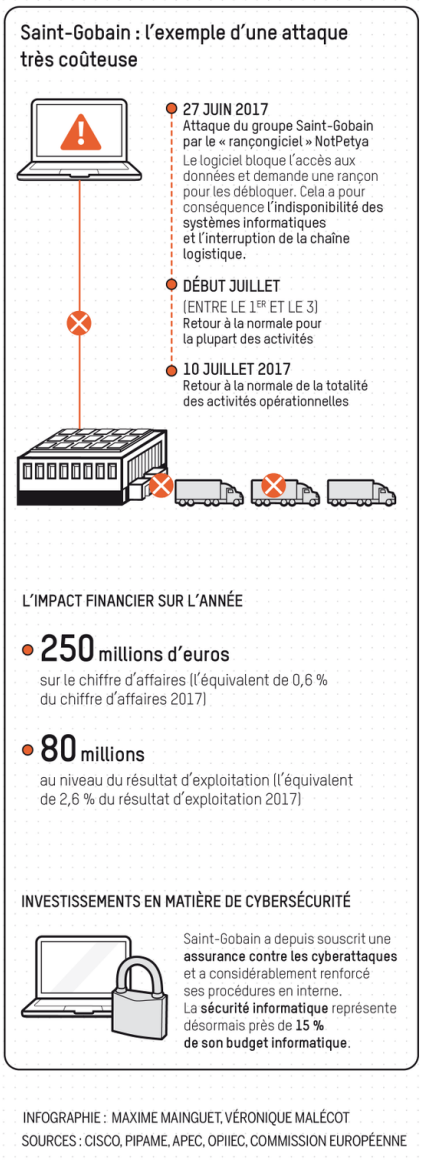
La cybersécurité est rarement une priorité

Les grands groupes ont gagné en maturité. Ils définissent des stratégies de cybersécurité, commandent des audits, recrutent des spécialistes et font tester leur résilience par des équipes spécialisées, les Red Team. Celles-ci identifient les points faibles des systèmes informatiques en tentant de s'y introduire et d'y dérober des codes, des mots de passe ou les logiciels stratégiques… Ce qu'elles réussissent à chaque fois ! Les entreprises connaissent ainsi leurs principales vulnérabilités et peuvent y remédier.

La situation est très différente dans les TPE, les PME et les ETI. La plupart d'entre elles ne prennent conscience des risques que lorsqu'elles subissent une attaque. C'est le cas de Herige, groupe de 2 500 personnes actif dans le négoce, le béton et la menuiserie industrielle. « En 2015, nous avons subi plusieurs attaques de rançongiciels qui ont causé des dégâts heureusement limités. À chaque fois, nous avons pu réinstaller la sauvegarde de la veille et nous n'avons pas perdu de données essentielles », raconte Jean-Michel Soulard, responsable de l'infrastructure informatique du groupe. Ces attaques ont sensibilisé la direction qui a alloué un budget à la mise en œuvre d'une solution de sécurisation des serveurs et des postes de travail.

Les principaux freins dans ces entreprises sont l'absence de personnel spécialisé et spécifique, et le manque de maturité des utilisateurs sur ce sujet. De plus, la cybersécurité est rarement une priorité pour la direction, qui la perçoit comme un coût et une complexité supplémentaire pour les employés.

Pour lever ces obstacles, les éditeurs de solutions de cybersécurité cherchent à automatiser le plus possible la détection d'attaques et leur traitement. Ils recourent pour cela de plus en plus à l'intelligence artificielle. Ils cherchent aussi à s'affranchir du binôme « identifiant + mot de passe » en développant d'autres modes d'authentification, par biométrie par exemple.



Les « voleurs » ont un temps d'avance sur les « gendarmes »

Particularité du monde de la cybersécurité, acteurs publics et privés partagent et échangent beaucoup d'informations. « Personne ne peut lutter seul dans ce domaine. Les entreprises privées ont accès à des informations et des outils que les États ou les organisations publiques n'ont pas. Elles ont aussi intérêt à travailler avec ces États. Nous ne partageons pas tout, nous restons concurrents, mais chacun a des pièces nécessaires au puzzle », explique Tanguy de Coatpont, directeur général de Kaspersky Lab France.

Cette coopération a donné naissance à Cybermalveillance.gouv.fr, site d'assistance aux victimes d'actes malveillants, qui associe plusieurs ministères, des organismes publics et de nombreuses sociétés du secteur. De même, le site Nomoreransom.org regroupe forces de police et sociétés de cybersécurité sous l'égide d'Europol, afin d'aider les victimes de rançongiciels. Grâce à leur coopération, Europol, le FBI américain et la société roumaine de cybersécurité Bitdefender ont pu démanteler AlphaBay et Hansa, deux places de marché du dark web qui vendaient des armes, de la drogue et des cyberattaques prêtes à l'emploi.

Malgré cette coopération active, les « voleurs » gardent un temps d'avance sur les « gendarmes ». Les premiers sont devenus des experts du cyberespace alors que les seconds sont en défense.

« Le "dark web" se banalise. En France, on comptait 10 000 utilisateurs du réseau Tor, favori des cybercriminels, en 2016. Ils sont 100 000 aujourd'hui. Et on y trouve tout ce que l'on veut, un faux passeport, de quoi ouvrir un compte en banque ou lancer une cyberattaque, le tout en quelques minutes », regrette Michel Van Den Berghe, directeur général d'Orange Cyberdefense.

Et d'alerter sur les prochaines menaces : « Les utilisateurs n'ont pas encore mesuré les risques que représentent les objets connectés. Un pirate a mené une cyberattaque contre un casino. Il est entré dans le système informatique par le thermomètre de l'aquarium du hall d'entrée, qui était connecté au système pour afficher la température sur un écran… ».

Sophy Caulier

Coup d'envoi du mois européen de la cyber-sécurité

Mounir Mahjoubi a lancé le 1er octobre dernier le « Cyberoctobre 2018 ». Un mois pour amener particuliers et entreprises à prendre conscience de l'importance des cyber-risques et à s'en prémunir.

Chaque année, a lieu en octobre une campagne de sensibilisation à la sécurité du numérique coordonnée en France par l'Agence nationale de la sécurité des systèmes d'information (l'ANSSI). Lors de son lancement, des experts ont débattus des risques et des enjeux liés à de telles attaques et sur la manière de s'en protéger.

Une recrudescence des pratiques malveillantes sur internet

Dans son propos introductif, Mounir Mahjoubi, secrétaire d'État chargé du numérique, a évoqué des pratiques qui polluent le web, de nature « *à éloigner les personnes du numérique* » alors qu'il faut les y intégrer. Il a également fait le constat d'une augmentation du nombre de ces actions malveillantes, citant :

- les « *fake news* » qui pullulent sur la toile et qui « *nous obligent à être beaucoup plus mobilisés* » ;
- les contenus haineux en ligne : le ministre reconnait un retard de la France vis-à-vis de l'Allemagne. Un rapport de la députée Laetitia Avia, de l'écrivain Karim Amellal et du vice-président du CRIF, Gil Taieb, visant à renforcer la lutte contre le racisme et l'antisémitisme sur internet, a été remis au premier ministre (Avia L., Amellal K. et Taieb G., 21 sept. 2018, Rapport visant à renforcer la lutte contre le racisme et l'antisémitisme sur internet). Il donnera lieu « *soit à une législation nationale, soit à une accélération de l'agenda européen sur ce point* », a annoncé le secrétaire d'État ;
- les atteintes aux données : le ministre a fait le point sur une année 2018 qui a été l'année du RGPD, mais aussi celle de « *deux grandes fuites des données de Facebook* » (faisant allusion à l'affaire de Cambridge Analytica et la fuite de 50 millions de données de cette semaine, v. Actualités de droit, 29 sept. 2018, Piratage, données, manipulation russe : les scandales qui empoisonnent Facebook). Il appelle donc tous les acteurs à rester vigilant sur ces points ;
- les arnaques en ligne : pour Bruno de Laigue, président de l'association des directeurs financiers et de contrôle de gestion (DFCG), « *les cyberattaques sont devenues des sujets prégnants pour l'entreprise : leurs données, leur réputation et leurs finances sont en jeu* ».

« *L'addition et l'accumulation de ces risques* (…) *obligent à faire prendre conscience à chacun de l'impérative nécessité de se protéger* », a encore insisté Mounir Mahjoubi.

Les bonnes pratiques à l'usage des particuliers et des entreprises

Delphine Gény-Stéphann, la secrétaire d'État auprès du ministère de l'Économie et des Finances, est pour sa part revenue sur l'importance pour les particuliers comme les entreprises d'adopter une « *bonne hygiène numérique* ». Ce qui passe, pour Mounir Mahjoubi, par trois gestes essentiels :

- faire des sauvegardes ;
- faire des mises à jour ;
- disposer d'un antivirus.

Une campagne spécifique sera d'ailleurs lancée cette semaine, en partenariat avec les CCI et les experts-comptables, pour sensibiliser les PME-TPE sur ces gestes de base, mais d'une grande importance.

Une autre bonne pratique consiste à porter plainte en ligne, sur un site dédié. Christophe Marais, capitaine de police et expert présent à la conférence, a ainsi mis l'accent « *sur l'importance de déposer plainte le plus rapidement possible. Cela peut déboucher sur une procédure pénale mais surtout, cela permet à la police de cartographier la délinquance numérique* ».

Assurer le risque numérique

Une étude menée en 2018 par la DFCG, avec la société EulerHermes, révèle que 70 % des entreprises sondées ont été victimes d'au moins une tentative de fraude sur internet (v. Fraude et cybercriminalité : les conclusions du baromètre DFCG 2018). Sébastien Hager, responsable souscription assurance fraude chez EulerHermes, a évoqué une « *industrialisation des attaques* », qui se décline en une propagation des attaques dites « *ransomwares* » (logiciel de rançons de type Wannacry qui prend en otage les données des entreprises), d'arnaques aux faux-mails ou de *phishing* (obtenir des renseignements personnels dans le but d'usurper ensuite une identité).

Un chiffre qui met en exergue la nécessité de se prémunir d'une assurance couvrant le risque cyber. Mais pour Gil Delille, expert, directeur des risques du SI Groupe Crédit Agricole SA, si « *l'assurance fait partie du dispositif de protection, mais elle arrive a posteriori. Ce n'est pas l'assurance qui va restaurer les données* ».

Alain Bouillé, président du club des experts de la sécurité de l'information et du numérique (CESIN), préfère parler de « *cyber-résilience* » et souhaite inciter les entreprises à augmenter leur capacité à « *rebondir* » après une attaque, notamment en prévoyant un « *plan B* ».

Le rôle moteur de l'État

La personne publique est elle aussi concernée. Pour Bruno de Laigue, l'État doit être une « *locomotive de l'évangélisation dans la prise de conscience de la cyber-fraude* ».

La secrétaire d'État a annoncé des mesures allant dans ce sens, orchestrées par Bercy. « *Nous avons mis en place avec un certain nombre de sites partenaires* (…), *un outil qui permet sous la forme d'un bandeau de couleur d'indiquer de manière simple et visuelle si le navigateur que vous êtes en train d'utiliser bénéficie bien de la dernière mise à jour* ».

Par ailleurs, la ministre a annoncé que les marchés publics de service informatique « *font l'objet de clauses spécifiques à la cyber-sécurité* ». Un cahier des clauses simplifiées a ainsi été publié à l'attention des acheteurs, afin de définir « *un cadre contractuel minimal* » (Arr. 18 sept. 2018, portant approbation du cahier des clauses simplifiées de cybersécurité, NOR : ECOP1825228A).

La responsabilisation des plateformes en ligne

Les plateformes internet sont bien sûr associées à cet impératif de sécurité. Vincent Courson, expert « trust and safety » chez Google, a ainsi insisté sur l'intérêt pour les opérateurs de sécuriser leur site par protocole « https ». « *Depuis 2015, l'usage de ce protocole est passé en France de 36 % à 86 %* ».

La protection des utilisateurs d'internet est également le souci des navigateurs. Vincent Courson est revenu sur le rôle des notifications lorsqu'une personne tente de se connecter à un site malveillant. Son efficacité passe selon lui par « *un interstitiel avec un aspect visuel interpellant* » la personne.

Sur les sites de commerce en ligne, la sécurité passe par des « *certifications* » qui renseignent les personnes sur la fiabilité du site, explique Fabien Lemarchand, responsable de sécurité des systèmes d'information. En effet, *« avec la certification, on a tous les ans un organe indépendant qui va évaluer le niveau de sécurité de l'entreprise qui propose du paiement en ligne* ».

Une démarche de co-construction

Delphine Gény-Stéphann a insisté dans sa conclusion sur la collaboration entre les entreprises et l'État, pour « *lutter contre la cybercriminalité ».* Il s'agit également d'inclure cet objectif dans « *le plan de numérisation des TPE et PME* ». Et ce d'autant que « *les GAFA unissent leurs efforts en recherche fondamentale en matière des cyber-sécurité parce qu'ils ont conscience qu'elle est l'affaire de tous* », a rappelé Vincent Courson.

Mahfoud Daoua

Cyberattaques : apprendre à travailler sans ordinateurs

Les attaques de l'année 2017 l'ont prouvé : la paralysie totale des systèmes d'information est désormais possible. De plus en plus d'entreprises se dotent d'une cellule de crise chargée de réfléchir à la meilleure façon de travailler en mode dégradé, c'est-à-dire sans écrans.

Les responsables informatiques des grands groupes industriels, de distribution ou de logistique se souviennent encore avec effroi du mardi 27 juin 2017, lorsque la cyberattaque NotPetya a paralysé des centaines de milliers de PC et de serveurs fonctionnant sous Windows. Dans certaines entreprises, tandis que la direction cherchait désespérément à acheter des milliers de PC neufs, les salariés étaient priés de rester chez eux et d'utiliser smartphones, et mails personnels pour répondre aux clients et aux fournisseurs ; les cadres, pour communiquer entre eux, créaient des groupes sur LinkedIn ; dans les entrepôts, on se demandait comment atteindre les plus hautes étagères, accessibles seulement aux robots...

Résultats ? Quelque 220 millions de chiffre d'affaires partis en fumée chez Saint-Gobain, un manque à gagner de 300 millions de dollars (241 millions d'euros) chez FedEx, 135 millions de dollars (109 millions d'euros) de ventes évaporés pour le laboratoire pharmaceutique Merck...

Envisager le pire

« Il y a un avant et un après WannaCry et NotPetya, note Vincent Vallée, président du CCA (Club de la Continuité d'Activité), qui regroupe 150 professionnels de la gestion de crise. Ces deux attaques survenues à quelques semaines d'intervalle ont fait prendre conscience aux chefs d'entreprise que nul n'était à l'abri d'un 'crash' informatique et que ça pouvait coûter cher et mettre l'entreprise en grande difficulté... ».

Tout le monde doit désormais envisager le pire. Certains États planchent même sur la cyber catastrophe ultime : l'arrêt complet d'Internet pendant plusieurs jours. « Il ne faut pas se demander si on va être attaqué, mais quand ! », résume Richard Olszewski, secrétaire général du HCFDC (Haut Comité français pour la défense civile), un think tank spécialisé dans la résilience des organisations.

Certes, voilà plusieurs années que beaucoup d'entreprises -dont tous les OVI, les opérateurs d'importance vitale, jugés indispensables pour la survie de la Nation- ont mis en place des plans de continuité d'activité (PCA), qui doivent leur permettre de continuer à travailler en mode dégradé. « La plupart de ces PCA intégraient la crue d'un cours d'eau, une grève massive ou un incendie, mais ne prenaient pas en compte les cyberattaques », constate Gérôme Billois, expert cybersécurité chez Wavestone, un cabinet de conseil en management, qui a aidé plusieurs sociétés lors de l'attaque NotPetya. Aujourd'hui, de plus en plus de grands noms de la banque ou de l'énergie incluent des scénarios de cyberattaques.

Cyber-résilience

Ces entreprises tentent d'abord de devenir « cyber-résilientes », c'est-à-dire capables d'atténuer les effets d'une cyberattaque sur leurs infrastructures. Elles mettent les sauvegardes « en quarantaine » pour s'assurer que ces dernières n'ont pas été elles-mêmes infectées (« On met en moyenne 270 jours à détecter la présence d'un malware », prévient Philippe Trouchaud, associé chez PwC, spécialiste en cybersécurité). Elles installent des cloisons étanches pour isoler machines et serveurs des réseaux contaminés. Et elles ne mettent pas tous leurs oeufs dans le même cloud : elles font appel à plusieurs prestataires (un pour le réseau social de l'entreprise, un deuxième pour la GRC -gestion de la relation clients- ; un troisième pour la bureautique...). Sans oublier de souscrire une cyberassurance.

Mais même cela ne suffit pas. « L'entreprise est de plus en plus ouverte sur le monde : il est donc impossible d'ériger des murs tout autour. Il faut protéger ce qui a de la valeur et, pour le reste, se mettre en capacité de réagir en cas de crise. Cela passe par la construction d'un plan de réponses aux cyber incidents qui devra être testé et maintenu », conseille Laurent Peliks, associé France chez EY et spécialiste de la cybersécurité.

Apprendre à réagir

Première étape : accepter de regarder le risque en face. Si les dirigeants des grands groupes industriels sont habitués depuis longtemps à simuler des crises, cette culture est moins répandue dans les services et dans les entreprises de taille intermédiaire, sans parler des PME. Or entraîner les individus est encore plus indispensable pour se préparer aux cyberattaques : contrairement aux accidents industriels qui restent cantonnés localement, les virus informatiques peuvent mettre à plat toute l'entreprise. « S'entraîner à une gestion de crise habitue les salariés à réagir : 1) à l'inconnu, 2) dans l'urgence, et 3) ensemble, martèle Olivier Lasmoles, professeur associé de droit à l'École de Management de Normandie et chargé de mission cyberdéfense à l'Institut des hautes études de la défense nationale. Sinon, le jour de la crise, tout le monde partira dans tous les sens comme des canards sans tête ».

Deuxième temps : entraîner quelques managers à imaginer les scénarios les plus fous. « Lorsque j'entraîne des dirigeants, je leur demande de se poser quatre questions : quel est le sujet, quels sont les pièges, qui sont les acteurs, quelles combinaisons de solutions proposez-vous pour vous remettre en dynamique positive ? », relate Patrick Lagadec, directeur de recherche honoraire à Polytechnique et auteur du « Continent des imprévus » (Les Belles Lettres).

Troisième point : cerner les priorités. « Il faut rétablir avant tout des flux d'informations, y compris s'il le faut en recourant aux smartphones personnels des salariés, et les flux de matériaux ; les flux financiers suivront », souligne Olivier Lasmoles. À l'heure de l'intelligence artificielles, les données sont, en effet, tout aussi primordiales que les marchandises.

Enfin, il ne faut pas oublier de communiquer. En interne, d'abord. « Le service client doit être averti que l'entreprise est en mode dégradé afin qu'il puisse délivrer un message cohérent, constructif et protecteur aux clients », insiste Loïc Guézo, administrateur et secrétaire général du Clusif (Club de la sécurité de l'information français). Sinon, une partie de la clientèle pourrait passer définitivement à la concurrence. Et un partage de retour d'expérience avec d'autres dirigeants profite à tout le monde. Pierre Bessé, président de la société de conseil en

assurances Bessé, souhaite même la création d'un cluster d'entreprises sur le thème de la cyber résilience.

Les sept points d'un bon plan B

« Il faut anticiper les problèmes concrets des premières 48 heures », détaille Hervé Schauer, expert en cybersécurité :

- prévoir des plans B détaillés pour chaque activité (dans les aéroports, il existe une procédure alternative pour le contrôle des passagers à l'embarquement, en cas de panne informatique) ;
- configurer une messagerie de secours utilisable par l'encadrement ;
- prévoir la logistique (lits, nourriture...) pour des équipes informatiques qui vont être mobilisées 24H/24 pendant plusieurs jours ;
- s'assurer que ses fournisseurs peuvent travailler en mode dégradé ou possèdent un stock tampon ;
- se demander quelles unités de production peuvent se substituer les unes aux autres ? En France ? Dans le monde ? Comment délocaliser, loger, nourrir le personnel nécessaire ?
- négocier avec son prestataire informatique qu'il puisse fournir plusieurs centaines ou milliers de PC en quelques jours ;
- prévoir que ses cabinets conseils puissent mettre à disposition des experts en informatique, logistique, communication...

Un risque systémique pour les assureurs ?

De plus en plus d'entreprises souscrivent une cyberassurance couvrant, en cas de cyberattaque, les coûts liés à la récupération des données, les pertes d'exploitation, les frais de la reconstitution de leur image auprès des clients... Or cette couverture présente un risque systémique pour les compagnies d'assurances, des dizaines, voire des centaines de leurs clients pouvant être touchés en même temps par un même virus informatique. « Nous sommes sur un risque nouveau dont nous devons accélérer notre connaissance », commente Stéphane Pénet, directeur assurance de dommages et de responsabilités à la FFA (Fédération française de l'assurance).

Jusqu'à présent, les entreprises étaient plutôt réticentes à communiquer sur ce genre d'incidents. Mais la transposition en droit français du RGPD (règlement général sur la protection des données) et de la directive européenne NIS (« Network and Information Security ») devrait amener plus de transparence. « Et comme ces textes s'appliquent à l'ensemble de l'Union européenne, toutes les entreprises de l'Union devront déclarer leurs incidents ; nous espérons à terme les compiler à travers Insurance Europe, la fédération européenne des fédérations des compagnies d'assurances », poursuit Stéphane Pénet.

Jacques Henno

Why is cyber resilience important?

Information technology has become deeply ingrained in our lives. From personal needs – buying a cup of coffee or sharing some family photos – to business tasks – like designing machinery or buying and selling shares – it is hard to imagine life without it. It makes society more connected and our economies richer, but it also comes with new risks.

What if something goes wrong? What if your pictures end up in the wrong hands? What if someone hacks your smartphone to steal money?

Risks like these are just as paramount in the business world, including the financial sector. Cyberattacks can cost companies a fortune. They can bring down the power grid. They can pose a risk to the stability of the financial system. That is why it is so important that companies and organisations are prepared for, and equipped to deal with, such threats.

What does the ECB do to promote cyber resilience?

We take cyber threats very seriously. We continuously work to improve our defences so that we can protect our data and information systems. We develop strategies to deal with crisis situations, should an attack occur. And we work together with the EU national central banks to protect the European System of Central Banks – and its data – as a whole.

But it is not only our own cyber resilience we care about. We promote cyber security more widely, particularly in the financial sector.

For example, we cooperate with other EU institutions, such as the European Parliament, the Council and the Commission, as well as with other international organisations and financial institutions to share information, increase understanding of cyber risks and develop best practices for handling them.

As a regulator for market infrastructure – for example, payment and settlement systems – we set rules and best practices to ensure that individual institutions and providers have a strong level of cyber resilience.

In our role as banking supervisor, we ask the largest euro area banks to report significant cyber incidents as soon as they detect them. This helps us to identify and monitor trends in cyberattacks, which puts us in a position to be able to react more swiftly to a potential crisis caused by a cyberattack. We are also developing specific IT risk management guidelines intended to help banks and financial institutions become stronger and better equipped to face cyber threats.

Whose responsibility is cyber resilience?

The ECB actively collaborates with many partners to increase awareness of cyber risks. However, just as we are all responsible for locking our own doors and windows at home, and if necessary installing security measures, companies, banks and public institutions are ultimately responsible for their own security. They need to make sure their security systems are up to date and keep themselves informed and alert about cyber threats – both for their own sake and for others.

Cyberguerre : la cyber-résilience n'est pas le vaccin mais un bon contrepoison

La cyber-résilience, d'apparence contre-nature, et pourtant…

« La cyber-résilience fait référence à la capacité d'une entité à fournir en permanence le résultat souhaité malgré les cyber-événements indésirables. La cyber-résilience est une perspective en évolution qui est de plus en plus reconnue ». La cyber-résilience se donne pour objectif de permettre à des organisations d'être les plus réactives possible face à une cyber attaque. Cela passe par une approche qui peut apparaître -au niveau des entreprises comme des États- contre nature dans une cyberguerre puisqu'il est alors question -pour les cibles potentielles- de développer et de partager des outils et des informations afin de mutualiser les moyens défense ! L'union fait la force ! Aussi, que les grandes entreprises, les PME, les TPE, et toutes infrastructures critiques nationales en soient prévenues : devant la menace, le proverbe « À la guerre comme à la guerre » a vécu, celui qui prévaut désormais c'est : « À la cyberguerre comme à la cyberguerre ! ».

Le coût d'un arrêt d'activité !

Le 15 janvier 2019, l'AGCS (Allianz Global Corporate & Specialty SE) publiait le « baromètre des risques 2019 d'Allianz ». Comme le pointe cette 8e enquête annuelle sur les principaux risques d'entreprise qui a réuni pas moins de 2 415 experts dans 86 pays, « *la cybersécurité est devenue la première préoccupation des entreprises en France* ». Dans le top dix des préoccupations, les incidents cyber arrivent en première place (41 % des sondés), talonnés par les interruptions d'activités (40 %). Et ce, à l'inverse des entreprises américaines, allemandes et chinoises qui, elles, placent l'interruption d'activité en tête de leurs classements devant la cybersécurité. Si, en France, une baisse de sept points est constatée par rapport au baromètre 2018 pour ce qui est de l'arrêt d'activité, il est à noter, et il n'en demeure pas moins :

1. que cyber-incident et interruption d'activité ont souvent un lien de cause à effet dans des entreprises de plus en plus tributaires du numérique ;
2. que les pourcentages sont aussi proches que conséquents.

Pour Corinne Cipière, CEO d'AGCS, cette inquiétude sur la cybersécurité est liée au fait que *« les entreprises françaises sont de plus en plus préoccupées par la fréquence et la gravité croissante des incidents cyber, les plaçant ainsi pour la première fois en tête du classement des risques en France »*. On peut pour le moins comprendre cette inquiétude au regard des chiffres : *« La délinquance cybernétique aurait coûté 600 milliards de dollars en 2018, contre 445 milliards de dollars en 2014. C'est trois fois plus que la moyenne des pertes économiques liées aux catastrophes naturelles sur dix ans, qui s'élève à 208 milliards de dollars »*.

Pour ce qui est de l'arrêt d'activité, comme je le soulignais, cyber-incident et interruption d'activité sont intimement liés. Ainsi, dans ce rapport, il est également notable que « *l'interruption d'activité et les cyber-incidents arrivent en tête du classement avec 37 % des réponses. Toutefois l'interruption d'activité a reçu plus de réponses en nombre : 1 078 contre 1 052* ».

Devant la montée en puissance des coûts inhérents à ces problématiques, la cyber-résilience que j'ai pu évoquer en introduction apparaît comme un enjeu majeur, en capacité d'infléchir ces

coûts démesurés qui demeurent en forte croissance. Il est indéniable que la poursuite de l'informatisation au travers -entre autres- de la multiplication des objets connectés ne peut, sans les précautions (Privacy by Design…), les mesures (RGPD…) et les approches adéquates (Partenariats servant la cyber-résilience…), qu'ouvrir de nouvelles portes et soutenir cette croissance qu'il appartient à tous et à toutes d'endiguer.

L'exemple d'Orange et Europol…

Pour faire face à ces risques, les entreprises s'organisent et entreprennent des démarches cyber-résilientes. En juillet 2018, à titre d'exemple, et pour illustrer la démarche -même s'il s'agit là d'un rapprochement entre une entreprise de type infrastructure critique et une agence européenne de police criminelle-, Jean-Luc Moliner, Directeur de la Sécurité du Groupe Orange, et Steven Wilson, Directeur du Centre Européen de Lutte contre la Criminalité d'Europol (EC3), ont signé un accord au service de cette cyber-résilience. Ce partenariat porte sur le principe de partage de connaissances sur les cyber-menaces pouvant peser au niveau européen. « *L'accord fixe un cadre à Orange et à Europol afin d'échanger des informations sur l'état de la menace sur les réseaux et les tendances en matière de cybercriminalité. Orange participera au renforcement et à l'enrichissement des données à travers des échanges de savoir-faire technique et le partage d'indicateurs que l'opérateur peut voir passer sur ses réseaux : spams, attaques DDoS, fraude, cyberattaques mobiles ou encore les cyberattaques bancaires par exemple* ».

Cela va dans le sens d'une meilleure connaissance de la typologie de la cybercriminalité… Dans le même temps, la formation à la cyber-résilience devient de plus en plus performante au service des entreprises : par exemple, un accord de partenariat a été signé en octobre 2018 lors de la Cybersecurity-Week Luxembourg entre l'EBRC (European Business Reliance Centre) et le C3 (Cybersecurity Competence Center) -ce rapprochement « *permettra aux entreprises, à partir d'une analyse d'impacts, de définir un scénario de crise sur-mesure et de le tester dans la Room#42 du C3* »- (La Room42 est un simulateur qui offre un ensemble d'outils très complet qui met en situation le management d'une entreprise lors d'une gestion de crise). Naturellement, de nombreuses autres offres de formations existent et sont proposées par des cabinets spécialisés… Si la demande ne manque pas d'être au rendez-vous, c'est que les entreprises ont bien conscience d'être au cœur d'un écosystème où il ne suffit pas, comme nous allons le voir, d'être protégé soi-même pour être à l'abri d'une attaque, et devenir la victime de cyber-dégâts collatéraux…

Altran a ainsi subi le 24 janvier 2019 une attaque au rançongiciel d'importance qu'elle a confirmée par un communiqué de presse « Information sur une cyber attaque » en date du 28 janvier 2019, ce dernier met en avant sa capacité à réagir :

(…) « *Pour protéger nos clients, employés et partenaires, nous avons immédiatement déconnecté notre réseau informatique et toutes nos applications. La sécurité de nos clients et des données est et sera toujours notre priorité absolue. Nous avons mobilisé des experts techniques et d'investigation indépendants mondialement reconnus, et l'enquête que nous avons menée avec eux n'a révélé aucun vol de données ni aucun cas de propagation de l'incident à nos clients. Notre plan de rétablissement se déroule comme prévu et nos équipes techniques sont pleinement mobilisées. Tout au long du processus, Altran a été en contact avec ses clients, les autorités gouvernementales et les régulateurs compétents* ». (…)

Comme l'indique Emmanuel Paquette, journaliste à *L'Express Expansion*, « *l'offensive s'avère si importante qu'Altran a saisi la brigade d'enquêtes sur les fraudes aux technologies de l'information (Befti) et le parquet de Paris. Le cyber-pompier de l'État, l'Anssi, a également été*

sollicité en soutien ». Si la société Altran ne peut être qualifiée « d'opérateur d'importance vitale » (OIV), sa capacité à réagir et à mobiliser les acteurs internes et externes (investigations), le respect des exigences de transparence totale prévues par le Règlement Général sur la Protection des Données (RGPD), ont été des éléments déterminants pour contenir la crise et la régler sans occasionner de potentiels dégâts collatéraux. Rappelons qu'Altran compte en effet parmi ses clients des organisations identifiées par l'État comme ayant des activités indispensables ou dangereuses pour la population telles qu'Orange, EDF, Engie…

Cyber-résilience et principe de réalité…

Si l'approche est raisonnable, « tout n'est pas pour autant pour le mieux dans le meilleur des cyberespaces possibles » ; la cyber-résilience est un incontournable qui doit tenir compte d'un principe de réalité : on ne peut pas dire que les États soient des parangons de vertu en matière de renoncement à des cyber-attaques, qui par ailleurs sont des attaques qui peuvent s'inscrire dans la durée et sont difficilement détectables. Le mot cyber-résilience sonne bien ; cependant, partager certaines informations n'est pas une sinécure, nul n'est à l'abri de l'attaque d'un pays a priori identifié cyber-ami… Pour ceux qui en doutent, il suffit de se rappeler de l'affaire des 35 chefs d'État mis sur écoute en 2013 par les services de renseignement des États-Unis et des conséquences sur la confiance des intéressés envers ce pays ami. C'est ce qui a été rappelé tant aux entreprises qu'aux infrastructures critiques nationales, lors du 11e FIC (Forum International de la Cybersécurité) qui s'est tenu à Lille les 22 et 23 janvier 2019, autour des thématiques RGPD et résilience : au-delà du respect des données privées sur lesquelles l'Europe a souhaité progresser avec le RGPD, Guillaume Poupard, le directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) a rappelé que « *les attaques récentes sont des prépositionnements pour les conflits de demain, avec des groupes très organisés et probablement soutenus par des États. Ils mettent des charges dans les systèmes d'information en prévision d'un conflit. Un peu comme si on mettait de la dynamite sur les piliers des ponts en attendant la guerre* ».

Il ne s'agit pas de baisser les bras, mais d'accepter cet état de fait. La cybercriminalité est protéiforme, elle ne disparaîtra pas, elle peut seulement se combattre de façon plus efficiente. Il s'agit donc d'intégrer que la cyber-résilience est l'affaire de tous et de toutes. C'est notamment celle des TPE/PME -souvent moins armées et plus vulnérables- qui peuvent, sans être la cible finale, constituer des points d'entrée privilégiés vers de grandes entreprises, au même titre que l'est tout salarié peu au fait ou mal informé des principes de précautions les plus élémentaires lorsqu'il est connecté aux réseaux de son entreprise.

Pour conclure

La cyber-résilience est un contrepoison, cela ne sera vraisemblablement jamais un vaccin, à moins naturellement d'un changement généralisé de la nature humaine qui m'apparaît, à l'heure où j'écris, relativement improbable. Mais à la cyberguerre comme à la cyberguerre. Une cyberguerre complexe de type « asymétrique atypique », puisqu'elle oppose les forces cyber-armées d'un État, d'une entreprise… à des combattants matériellement insignifiants (Black Hat Hacker isolé), ou a contrario extrêmement conséquents (autre État, groupe criminel organisé…) qui attaquent sans ultimatum et se servent des points faibles de la cible pour parvenir à leur but souvent politique ou financier.

Yannick Chatelain

Les 5 indicateurs d'une cyber-résilience optimale

Entre augmentation des cyber-attaques et complexité des processus des services IT, quel est le degré acceptable de cyber-résilience et quel est le niveau d'engagement des entreprises françaises ? Investissement, compétences et leadership fort sont les maîtres mots !

La cyber-résilience est définie comme « la synchronisation des capacités de prévention, de détection et de réaction qui permettent de gérer une cyberattaque, d'en atténuer les répercussions et de s'en remettre ». En d'autres mots, l'entreprise peut-elle maintenir le cap lors d'une attaque et prévenir, détecter, contenir les menaces liées aux données, applications et infrastructure ?

Comment maintenir son activité ?

Un haut niveau de cyber-résilience réduit ainsi le nombre d'attaques de données, permet de résoudre rapidement tout incident IT et doit être complété par un plan de réaction aux incidents de sécurité informatique parrainé par la direction.

En France, les cyber-attaques posent encore problème, les chiffres sont sans appel puisque l'entreprise n'est pas préparée à se remettre d'une cyberattaque pour 73 % et le niveau de cyber-résilience n'est pas « élevé » au sein de l'entreprise pour 79 %.

Les 5 indices d'une sécurité inefficace

La complexité des procédures de l'entreprise est perçue comme un frein par 47 % des personnes interrogées.

Découvrons maintenant les 5 éléments qui nuisent à la cyber-résilience :

1. Le manque d'organisation et de préparation (69 %), le manque de sensibilisation au risque, d'analyse et d'évaluation (52 %) et le manque d'implication du leadership. Ainsi, seulement 39 % déclarent que les dirigeants de leur entreprise reconnaissent le rôle de la cyber-résilience dans la réputation de la marque.

2. Le manque d'un plan de réponse aux incidents de sécurité informatique : un plan CSIRP n'est pas systématiquement appliqué dans l'entreprise (77 %).

3. L'augmentation de la durée de résolution d'un incident informatique (48 %).

4. La non-prise en compte de l'erreur humaine. Ainsi les incidents vécus impliquent une erreur humaine (pour 70 %). Les incidents ou les dangers les plus récurrents sont les logiciels malveillants (70 %) et le phishing (62 %), suivis par l'erreur de communication (58 %).

5. La négligence de la réglementation mondiale sur les données privées. Seuls 22 % estiment que leur organisation respecte scrupuleusement le règlement général européen sur la protection des données. Il y a urgence en la matière qu'il s'agisse du GDPR ou des lois internationales de chaque pays.

Les 5 clés d'une cyber-résilience optimale

Plusieurs éléments contribuent à renforcer la cyber-résilience, à savoir :

1) Un investissement dans le recrutement, la formation du personnel et dans les fournisseurs en services managés.

2) La participation à une initiative, plate-forme de réaction aux incidents**,** programme de partage d'informations sur les menaces. Toutefois, si le partage d'informations améliore la sécurité de l'entreprise (69 %), on note des réticences, 54 % ne partagent pas d'informations sur les menaces, en raison d'absence d'avantages (55 %), de manque de ressources (29 %) ou de coûts trop élevés (29 %).

3) La flexibilité**,** une équipe compétente et une bonne préparation permettent d'atteindre un haut niveau de cyber-résilience.

4) La mise en place d'un plan de de réponse aux incidents de sécurité informatique (CSIRP).

5) La mise en place de fonctionnalités technologiques clés pour :
   - empêcher les dispositifs non sécurisés d'accéder aux systèmes de sécurité (80 %),
   - contrôler les terminaux et les connexions mobiles (77 %),
   - sécuriser les données stockées dans le cloud (77 %) et contrôler les dispositifs mobiles non sécurisés, dont le BYOD (71 %).

Le « plus » sécurité : ne pas négliger la gestion et authentification de l'identité, les systèmes de prévention et de détection d'intrusion, l'encodage des données inactives, les solutions antivirus/anti-malware, la plateforme de réaction aux incidents l'encodage des données en mouvement et la surveillance du trafic sur le réseau !

Sabine Terrey

Succès de l'exercice de crise cyber de la Place financière de Paris

Le Groupe de Place Robustesse[1], avec le soutien de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a organisé un exercice de crise cyber le 9 octobre 2018. Cet exercice s'inscrit dans la stratégie de test pluriannuelle du Groupe et marque une étape importante, avant l'organisation en 2019, sous présidence française du G7, d'un exercice cyber à l'échelle internationale en 2019.

Piloté par le Secrétariat du Groupe de Place Robustesse (Banque de France) en partenariat avec l'ANSSI, cet exercice a mobilisé près de 350 personnes au sein des 24 entités participantes.

Cette année, le scénario de test avait comme objectif :

- d'éprouver le protocole de coordination établi entre le Groupe de Place Robustesse et l'ANSSI,
- de valider l'adéquation et la réactivité du dispositif de crise de la Place financière de Paris, en cas d'attaque cyber.

L'exercice a confirmé la bonne coordination entre les membres du Groupe dans le cadre d'une crise cyber de grande ampleur, ainsi que l'importance d'une implication de l'ANSSI dans le dispositif. Ce test a été également l'occasion pour les participants d'éprouver leurs processus de gestion de crise interne.

Le scenario articulé autour de plusieurs processus critiques du secteur financier (approvisionnement des distributeurs de billets, gestion de la liquidité du système bancaire), développait également une dimension de communication de place (suite aux rumeurs, articles et sollicitations de la presse…). La combinaison de ces différents éléments, la forte implication des acteurs de la place ont permis à cet exercice d'être un véritable succès, riche d'enseignements.

[1] *Le Groupe de Place Robustesse, créé en 2005 à l'initiative de la Banque de France, s'est fixé un double objectif de résilience (capacité du système financier à faire face à des chocs affectant ses fonctions critiques) et de crédibilité (maintenir la Place de Paris parmi les Places reconnues par les investisseurs internationaux comme l'une des plus robustes en cas de crise opérationnelle majeure). Le Groupe de Place Robustesse rassemble les principaux groupes bancaires français des infrastructures de marché, des gestionnaires de systèmes de paiement, le SHFDS du ministère de l'Économie et des Finances, la Direction générale du Trésor, la Fédération bancaire française, la Banque de France, des autorités de régulation : Autorité de contrôle prudentiel et de résolution, Autorité des marchés financiers.*

Best Cyber Resilience Initiative: Bank of England

Central Banking FinTech RegTech Global Awards 2018

As the world becomes increasingly financially interconnected, new types of risk are being introduced into the financial system. Never more present on central banks' radars than they are currently, cyber attacks have emerged as the number-one risk for regulators and financial firms worldwide. But cyber resilience no longer means being able to tackle known dangers. Central banks now require the ability to uncover and detect threats while they are still unknown, and it is time they get ahead of the curve

In response to this, for the past two years the Bank of England's (BoE's) Security Operations Centre (SOC) has been undertaking an initiative – SOC 2.0 – which has fundamentally altered how the central bank detects and responds to cyber attacks. Switching from a reactive to a proactive approach, staff have focused on studying patterns of adversarial behaviour in an attempt to respond to unknown threats.

Key to this initiative was a new way of thinking about the problem and developing an operating model that supported continual research, behavioural profiling and the implementation of data analysis techniques. Given this shift, the BoE decided an industry 'black box'[1] solution that promised to detect attacks would not suffice.

Instead, the central bank allowed its experts to design their own tools. Using a standard data-mining platform, teams of experts were given freedom to develop sophisticated analytical techniques to detect behaviour, rather than individual attacks that change over time and with increasing frequency. This approach would appear to be working.

Following the attack on Bangladesh Bank in 2016, the SOC team set out to ensure the BoE's own systems would not be breached. Even without access to the malware used in the attack, the SOC was able to quickly ascertain that the BoE's analytical techniques would be able to identify these attackers' behaviours if it was targeted.

Since developing the system, the SOC has worked to ensure it evolves to support the latest advances in technology. Taking inspiration from the rise of sophisticated 'bots' – including Siri and Google Assistant – the SOC developed SOC Assistant to ensure members of the team have the right contextual information on hand to triage security incidents appropriately.

Taking its approach out to the community, the group chairs the UK's Government Security Monitoring Group – a forum for government bodies to share cyber security techniques. The BoE's group has also partnered with a number of central banks worldwide to help those looking to evolve their systems.

Rachael King

[1] *Black box is the term commonly used to describe technically sophisticated electronic devices attached directly to a system to control its functions.*

Fin du cash : pourquoi les banques centrales travaillent aux monnaies numériques d'État

La directrice générale du FMI, Christine Lagarde, a invité les États à embrasser les idées nouvelles comme une version électronique du cash, à la Bitcoin. Selon une enquête de la BRI, 69 % des 80 banques centrales sondées travaillent à un projet de monnaie digitale, utilisant la technologie de registre distribué. L'Uruguay a lancé une expérimentation, la Suède s'y prépare.

« Il me semblerait imprudent de ne pas prendre les monnaies virtuelles au sérieux » avait estimé en septembre 2017 Christine Lagarde. Un an plus tard, alors que la bulle de spéculation entourant le Bitcoin et les autres crypto-monnaies a largement dégonflé, la directrice générale du Fonds monétaire international (FMI) a persisté dans sa vision à plus long terme, en livrant un « plaidoyer pour des monnaies numériques émises par les banques centrales ». Elle ne recommande pas aux États de passer au Bitcoin mais d'embrasser « *le changement et les idées nouvelles* ».

Lors d'un discours prononcé jeudi 14 novembre à Singapour, où elle assistait au Fintech Festival, la patronne du FMI a souligné « *la nature changeante de la monnai*e » à travers les âges, depuis l'invention du papier monnaie au IX^{e} siècle.

« Quel sera le rôle de l'argent liquide dans ce monde numérique ? » s'est-elle interrogée, ajoutant : *« Dans dix, vingt ou trente ans, qui échangera encore des morceaux de papier ? ».*

L'hypothèse d'une « *nouvelle forme numérique de monnaie* », qui serait « *un jeton garanti par l'État* », voire un « *compte auprès de la banque centrale* » pour les particuliers ou les entreprises « *n'est pas de la science-fiction* », a-t-elle relevé, citant les exemples de « *plusieurs banques centrales [qui] examinent sérieusement ces pistes, dont celles du Canada, de la Chine, de la Suède et de l'Uruguay* ».

« Je pense qu'il faut envisager la possibilité d'émettre de la monnaie numérique. L'État peut avoir un rôle à jouer pour apporter de l'argent à l'économie numérique », a estimé la directrice générale du FMI.

L'un des intérêts des monnaies de banques centrales pour les citoyens serait de pouvoir créer un substitut de cash plus liquide (pas d'échange physique requis) restant respectueux de la vie privée, en conservant le caractère anonyme du paiement, à différents degrés (totalement jusqu'à un certain plafond) ou pseudo-anonyme, pour des raisons de lutte contre le blanchiment et le financement du terrorisme.

Pas avant dix ans ?

Le sujet n'a effectivement plus rien de théorique et nécessite de s'y préparer dès maintenant. Selon une récente enquête révélée le 15 novembre par le Comité sur les paiements et les infrastructures de marchés, une des instances de coopération internationale hébergées par la Banque des règlements internationaux (la BRI, la banque des banques centrales), la préoccupation est largement partagée : 69 % des 80 banques centrales sondées travaillent actuellement ou s'apprêtent à mener des travaux sur une monnaie numérique de banque

centrale, en utilisant les technologies de registre distribué (comme la Blockchain, née avec le Bitcoin).

Celles qui ont répondu par la négative sont de petites institutions, faisant face à d'autres problèmes plus pressants ou s'appuyant sur des initiatives régionales, a analysé Benoît Cœuré, le président de ce comité, qui est également membre du directoire de la Banque centrale européenne (BCE). Plus de la moitié de ces institutions en cours de réflexion envisagent à la fois une monnaie numérique pour les paiements interbancaires et une version grand public.

« La plupart des banques centrales en sont encore au début de leur étude des monnaies numériques » a relativisé Benoît Cœuré. *« De l'avis général, il est peu probable qu'une monnaie numérique de banque centrale, quelle que soit sa forme, ne soit émise au cours de la prochaine décennie, même chez les quatre banques centrales qui ont indiqué avoir atteint le stade du développement de projet pilote ».*

Le banquier central, qui a qualifié, dans son discours jeudi, le Bitcoin de « *rejeton maléfique de la crise financière* », avait exprimé, dans un rapport publié en mars dernier, bon nombre de réserves à l'égard des monnaies numériques de banque centrale, qui « *pourraient rendre plus efficace le règlement des échanges d'action et des changes à l'avenir* » mais pourraient aussi avoir des « *implications pour la stabilité financière et la politique monétaire ».*

Pas de cas d'usage universel

Une étude des économistes du FMI publiée le 12 novembre a passé au crible les avantages et les inconvénients, pour les institutions monétaires, les utilisateurs et le secteur bancaire, des monnaies numériques de banques centrales, et tiré les enseignements des premières expérimentations. Près d'une quinzaine de banques centrales y travaillent activement, dans les économies développées et dans les pays émergents, avec des objectifs souvent bien différents.

« La monnaie numérique de banque centrale pourrait être la prochaine étape de l'évolution de la monnaie » conclut l'étude mais « il n'y a pas encore d'argument universel pour son adoption », chaque pays ayant des situations de marché spécifiques.

Dans les pays développés, les banques centrales envisagent ces monnaies digitales légales du fait du déclin du cash, dans l'optique de réduire le coût de toute la filière, voire de freiner l'essor des monnaies « privées » (les porte-monnaies électroniques à la Alipay ou WeChat pay par exemple), qui créent des risques de monopole naturel dans le paiement, de plus grands risques de piratage et des possibilités de profilage des consommateurs. Les pays émergents cherchent davantage à remplir un objectif d'inclusion financière, pour mieux atteindre les populations non-bancarisées et/ou éloignées.

En Suède, pays qui connaît la plus forte baisse d'utilisation des espèces, la Riksbank a proposé fin octobre au gouvernement suédois de modifier la loi et de lancer un programme pilote pour développer des solutions techniques afin d'émettre une e-couronne (qui fonctionnerait aussi en mode « offline » sans connexion, avec des jetons pré-chargés). En revanche, son homologue au Danemark voisin a décidé en décembre 2017 de ne pas aller plus loin, estimant qu'une e-couronne danoise n'apporterait pas de meilleure solution de paiement par rapport aux existantes.

L'Uruguay a mené pendant six mois, entre novembre 2017 et avril 2018, avec 10.000 utilisateurs, l'expérimentation en conditions réelles d'un e-peso avec une application mobile dédiée, qui s'est déroulée sans incident, selon un bilan dressé par un économiste du Banco Central del Uruguay, devant le Comité sur les paiements et les infrastructures de marchés. Le paiement était instantané, anonyme mais traçable, et ne nécessitait pas de connexion internet. Le pays va désormais débattre des suites à donner, du coût de la mise en place d'un tel e-peso digital dont l'objectif initial était une meilleure inclusion financière, ce qui n'a pu être vraiment démontré à travers ce pilote.

L'Équateur, à l'économie fortement dollarisée, a mis un terme en février dernier à son « dinero electrónico » lancé en 2015, faute d'adoption, et a passé la main au privé pour trouver une solution de paiement électronique plus efficace.

L'étude du FMI souligne qu'il reste de nombreux points à clarifier. Une monnaie numérique de banque centrale pourrait déstabiliser le système bancaire d'un pays, qui verrait les dépôts lui échapper et son coût de financement augmenter, l'incitant à prendre plus de risques pour compenser la baisse de marge. Cette monnaie devrait-elle être accessible aux touristes ? aux non-résidents à l'étranger, quitte à accentuer l'attrait de monnaie refuge de certaines devises ? Doit-elle servir pour les paiements transfrontaliers ? Ne risquerait-elle d'aggraver le risque de panique bancaire en cas de crise ? Christine Lagarde estime cependant cette idée très prometteuse.

« Si elles devenaient trop populaires, les monnaies numériques de banques centrales pourraient étouffer l'innovation, ce qui serait ironique » a-t-elle relevé.

Delphine Cuny

15

En quoi la capacité de résistance informatique est-elle importante ?

Les technologies de l'information font désormais partie intégrante de nos vies. Elles sont omniprésentes, dans notre vie privée, quand nous commandons un café ou partageons des photos de famille, mais aussi dans le domaine professionnel, pour la conception de machines ou l'achat et la vente d'actions, par exemple. Grâce à elles, nos sociétés sont davantage connectées et nos économies plus riches. Mais elles supposent également de nouveaux risques.

Que faire si les choses tournent mal ? Si vos photos tombent entre de mauvaises mains ? Si quelqu'un pirate votre smartphone pour vous voler de l'argent ?

Ce type de risques est tout aussi critique pour l'économie, y compris pour le secteur financier. Les attaques informatiques peuvent coûter très cher aux entreprises. Elles peuvent bloquer les réseaux électriques, menacer la stabilité du système financier. Il est donc primordial que les entreprises et les organisations soient préparées et armées pour affronter ces dangers.

Comment la BCE favorise-t-elle la résilience informatique ?

Nous prenons les menaces informatiques très au sérieux et nous nous efforçons constamment d'améliorer nos défenses afin de protéger nos données et nos systèmes d'information. Nous élaborons des stratégies de crise en vue d'attaques éventuelles. De plus, nous coopérons avec les banques centrales nationales de l'Union européenne pour protéger le Système européen de banques centrales dans son ensemble, et ses données.

Mais nous ne nous soucions pas uniquement de notre propre capacité de résistance informatique. Nous encourageons la sécurité informatique à plus grande échelle, notamment dans le secteur financier.

Nous collaborons ainsi avec d'autres institutions de l'Union européenne, comme le Parlement européen, le Conseil et la Commission, ainsi qu'avec des organisations internationales et des institutions financières en partageant des informations en vue d'améliorer la compréhension des risques informatiques et de mettre en place des meilleures pratiques concernant leur traitement.

En tant qu'instance de réglementation de l'infrastructure de marché, notamment des systèmes de paiement et de règlement, nous définissons des règles et des bonnes pratiques permettant d'assurer un niveau élevé de résilience informatique au sein des différents établissements de crédit et de leurs fournisseurs.

Dans notre rôle de superviseur bancaire, nous demandons aux plus grandes banques de la zone euro de nous signaler immédiatement tout incident informatique significatif. Nous pouvons ainsi identifier et suivre les évolutions en matière d'attaques informatiques et serons donc en mesure de réagir plus rapidement en cas de crise causée par une cyber-attaque. Nous formulons en outre des orientations spécifiques concernant la gestion des risques informatiques dans le but d'aider les banques et les institutions financières à être mieux armées face à ces menaces.

À qui incombe la responsabilité de la résilience informatique ?

La BCE collabore activement avec de nombreux partenaires pour sensibiliser les parties prenantes aux risques informatiques. Toutefois, de la même manière qu'il nous appartient à tous de fermer nos portes à clé, de ne pas laisser nos fenêtres ouvertes en notre absence et d'installer des dispositifs de sécurité si nécessaire, les entreprises, les banques et les institutions publiques sont, en dernier ressort, responsables de leur propre sécurité. Elles doivent disposer de systèmes de sécurité modernes, s'informer des attaques informatiques potentielles et lancer l'alerte si elles en font l'objet, dans leur intérêt mais aussi dans celui des autres.

La BRI lance une réflexion sur les monnaies numériques émises par les banques centrales

La banque des règlements internationaux (BRI) a publié lundi un rapport sur l'éventuelle création de monnaies numériques par les banques centrales en amont du sommet du G20 qui doit se tenir les 19 et 20 mars à Buenos Aires.

Préparé conjointement par le Comité sur les paiements et les infrastructures de marchés (CPMI) et par le Comité des marchés, ce rapport a soupesé les mérites et les inconvénients de monnaies numériques qui pourraient être émises par des banques centrales, et non par des opérateurs privés comme le sont actuellement les crypto-monnaies. Selon ce rapport, elles pourraient révolutionner la façon dont les monnaies sont proposées, mais aussi avoir d'importantes répercussions sur les politiques monétaires ou la stabilité du système financier. Parmi les arguments en leur faveur, elles pourraient notamment fournir des instruments fiables si l'usage de l'argent liquide venait à diminuer, contribuer à renforcer les systèmes de paiement et accroître les outils à la disposition des banques centrales.

Le rapport, qui établit une distinction entre la monnaie utilisée comme instrument de transactions entre une poignée d'institutions financières sur les marchés monétaires et le moyen de paiement pour un large public, l'envisage également comme une alternative sûre aux crypto-monnaies émises par des opérateurs privés. Actuellement, celles-ci sont trop volatiles pour être considérés comme des moyens communs de paiement ou d'épargne. Mais elles comportent également des risques importants. Elles pourraient entre autres accroître le poids des banques centrales dans l'économie, peser sur les dépôts au détriment des banques et in fine sur leur capacité à octroyer des crédits ou encore exposer les banques centrales à d'avantage de risques en termes de cyber-sécurité.

« Il faut encore d'avantage de travail et d'expériences pour évaluer leurs bénéfices », a estimé Benoît Coeuré, le président du CPMI, également membre du directoire de la Banque centrale européenne, tout en soulignant que ce rapport vise avant tout à apporter une base de réflexion sur le sujet. Pour l'heure, la question reste plutôt théorique. Aujourd'hui, les banques n'ont pas besoin d'émettre des monnaies numériques pour mettre en œuvre leur politique monétaire, selon ce rapport.