Dossier
IT for BUSINESS
STRATÉGIES ET MANAGEMENT DU NUMÉRIQUE

Sécurité

Comment faire face à l'explosion des cybermenaces

Face à l'éventualité de moins en moins hypothétique des attaques qu'elle aura à subir, l'entreprise doit intégrer le risque cyber comme un risque classique, développer une cyber-culture d'entreprise et industrialiser ses politiques et procédures de sécurité.

Dossier réalisé par Stéphane Darget

Au fil des derniers mois, la cybersécurité est devenue l'un des enjeux les plus importants dans une majorité de comités de direction. Dans un contexte d'ouverture toujours plus importante des systèmes d'information devant sous-tendre la transformation numérique, deux facteurs principaux sont la cause de ce changement. Tout d'abord, la législation européenne sur la protection des données personnelles (RGPD) accélère la prise de conscience. Son application en mai 2018 incite à avancer rapidement. Ensuite, l'actualité des malwares — Wannacry, Petya, Not Petya… — montre que toute entreprise peut en être victime. Et elle oblige les boards à intégrer cette menace aux risques majeurs auxquels l'entreprise doit être préparée.

Comme l'illustre Gilles Berthelot, RSSI Groupe de la SNCF, *« de gros efforts de pédagogie ont été nécessaires pour éveiller les consciences des dirigeants. Ce* →

De gros efforts de pédagogie ont été nécessaires. Ce n'est que depuis deux ans que le risque cyber est classé parmi les risques majeurs de notre entreprise.

→ *n'est que depuis deux ans que le risque cyber est classé parmi les risques majeurs de notre entreprise, aux côtés des risques industriels et humains. Désormais, le sujet n'est plus simplement un problème de la DSI, mais une préoccupation du Comex. L'actualité nous a permis de mieux parler des enjeux et des conséquences pour le business. La cartographie réalisée par la direction des risques montre que tous les métiers sont devenus dépendants du SI. Seule l'approche top-down permet de pénétrer tous les process de l'entreprise* ».

Hervé Schauer, expert en sécurité, insiste sur l'importance des aspects organisationnels trop souvent sous-estimés, selon lui, y compris financièrement. « *La sécurité n'est pas un produit mais un processus* », rappelle-t-il.

L'AVIS DU RSSI


DR

GILLES BERTHELOT
RSSI GROUPE DE LA SNCF

La transformation numérique de l'entreprise implique une évolution du rôle du RSSI. Dans un premier temps, à la SNCF, cette fonction était rattachée à la DSI de l'entreprise. Son rôle était opérationnel et non visible de l'équipe dirigeante : il était « à la cale ». En rejoignant la direction des risques, le RSSI change de paradigme, et peut efficacement insuffler ses messages. Enfin, en intégrant la direction de la transformation numérique, il retourne dans l'action, tel un chef de guerre sur le terrain.

Selon Michael Bittan, responsable des activités Cyber Risk Services de Deloitte France, « *c'est en développant une "culture cybersécurité", étendue à l'ensemble des échelons et des métiers dans le cadre d'une démarche collaborative, que les organisations pourront réellement se protéger des cyber-menaces* ».

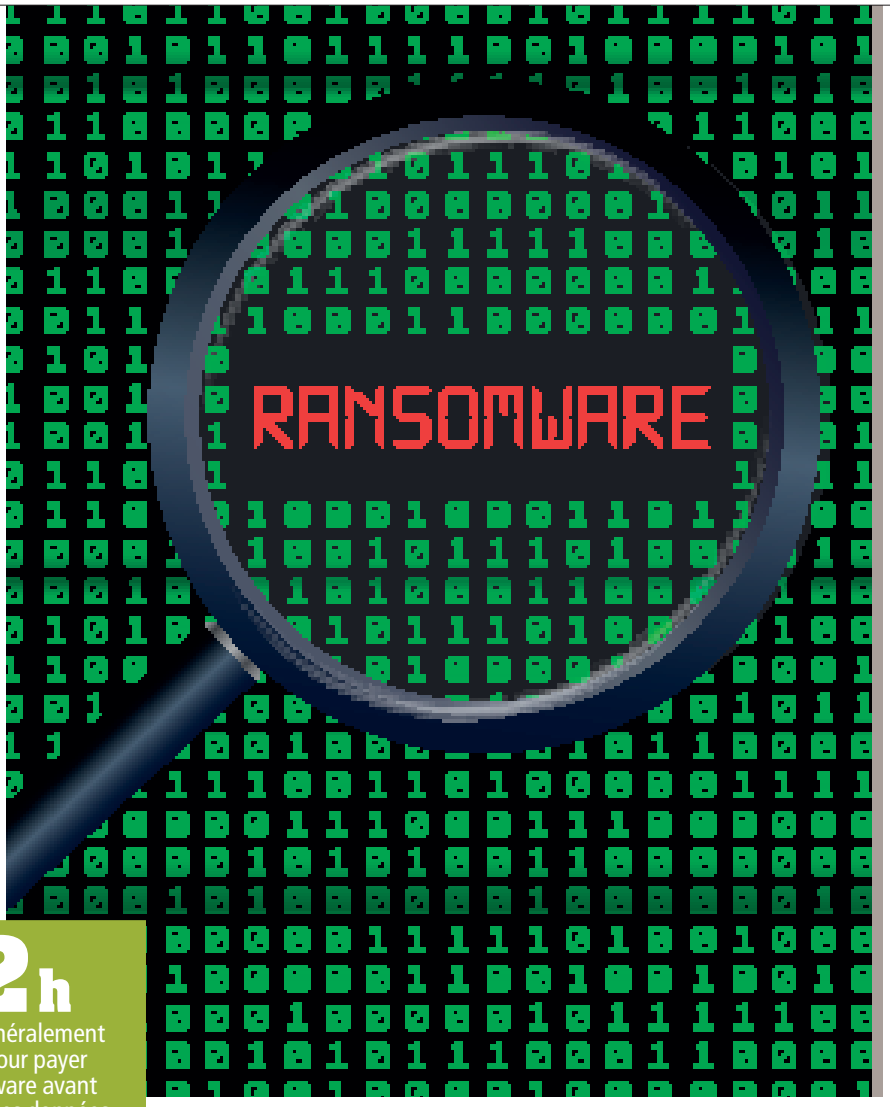
L'organigramme de la sécurité dans l'entreprise subit de profondes modifications. La DSI n'est plus toute puissante dans ce domaine. Par exemple, le RGPD oblige à recenser l'ensemble des projets contenant des données personnelles et à analyser les risques associés. Même s'il dispose à la fois de compétences sécurité, conformité et juridiques, le nouveau responsable des données personnelles (Data Privacy Officer) va devoir s'appuyer sur un réseau de correspondants métiers. Selon Alain Bouillé, président du Cesin, « *une grande collaboration entre DPO et RSSI est indispensable, afin de ne pas doublonner les analyses, et éviter aux différents métiers d'avoir à répondre plusieurs fois aux mêmes questions. De plus, beaucoup de pans de l'organisation du RGPD sont déjà pris en compte par le RSSI* ».

Pour Gilles Berthelot, « *le management par le risque a fait ses preuves dans l'organisation de la sûreté : il sensibilise l'intégralité de la chaîne managériale, des plus hautes instances aux plus basses. En traitant le risque cyber comme un risque classique, il devient possible d'utiliser l'ensemble des processus déjà mis en place et qui ont fait leurs preuves. Ainsi, de la même manière qu'ils le font pour le port du casque et la conformité des machines-outils, les structures Hygiène et Sécurité au Travail deviennent légitimes pour vérifier le bon usage des outils informatiques et l'application des "règles d'hygiène informatique" au quotidien. À la SNCF, chaque entité dispose d'un risk manager. Intégrer le risque cyber à sa palette de compétences simplifie fortement son intégration dans tous les projets et le suivi qui en est fait.*

LE « BON » HACKER EST UN SOCIOLOGUE ET UN PSYCHOLOGUE


DR

La connaissance de la psychologie des victimes et de leurs habitudes est un facteur déterminant dans la réussite des campagnes de phishing et de ransomware. Sans aller jusqu'à une personnalisation très poussée, les hackers peuvent déjà s'appuyer sur des statistiques reconnues. Ainsi, en France, les utilisateurs qui ouvrent les pièces jointes ou les URL contenues dans un e-mail malveillant le font plutôt en début de matinée et avec un pic vers 13h. Sur les 4,6 % des utilisateurs qui cliquent sur ces liens, environ la moitié le font dans la première heure suivant l'expédition. D'autres études montrent que les e-mails malveillants sont surtout envoyés le jeudi, et très peu le dimanche.
Pour faire en sorte que les utilisateurs cliquent, le hacker joue sur les ressorts psychologiques (envie, curiosité,…) et en particulier sur la peur, en utilisant par exemple des logos d'agences gouvernementales. Une fois le ransomware activé, les messages affichés sont aussi judicieusement choisis. Ils créent d'abord la panique (horloges qui décomptent, messages en rouge…), et ensuite rassurent (en expliquant comment payer, en proposant même de l'assistance technique), jusqu'à chercher à instaurer une certaine confiance afin de maximiser le nombre de paiements de rançon.



DR

Bien entendu, pour évaluer précisément les aspects techniques, le risk manager doit pouvoir s'appuyer sur les RSSI ».

Pour obtenir une cyber-résilience efficace, outre les RSSI et les risk managers, Gérôme Billois, senior manager chez Wavestone, rappelle qu'il faut également impliquer deux autres familles d'acteurs. D'une part, les responsables des plans de continuité, capables de gérer les crises, d'imaginer des scénarios et de contrôler les sites de secours. D'autre part les spécialistes de l'assurance, capables de définir le niveau de risque résiduel acceptable et d'estimer les coûts potentiels de telles attaques pour l'entreprise. Et d'ajouter : *« parmi nos clients, certaines sociétés disposent désormais d'un comité cyber au niveau du groupe, qui se réunit chaque mois. Sa mission est d'opérer un reporting commun auprès de la direction générale. Mois après mois, le rapport est consolidé, en intégrant les nouveaux risques qui entrent alors dans le radar de la direction générale ».*

72 h
Le temps généralement annoncé pour payer un ransomware avant destruction des données

42 %
Le ratio des clics sur des URL malveillantes provenant d'appareils mobiles

Alain Bouillé propose également d'appliquer ce concept au niveau des projets. *« Aujourd'hui le RSSI a un rôle de plus en plus central, mais a du mal à être sur tous les fronts. Pour accompagner la transformation numérique de l'entreprise, le chief digital officer constitue souvent des équipes non hiérarchiques autour de projets. Dans cette "pizza team", où tous les membres travaillent dans un même lieu, une personne doit être dédiée à la sécurité ».*

Les achats ont également un rôle indirect non négligeable dans la mise en œuvre de la politique de sécurité. En particulier s'il s'agit de mettre en place une politique de bug bounty et, de ce fait, d'allouer un budget pour les « récompenses ». *« Le RSSI doit faire changer les habitudes. Il doit par exemple convaincre le service achats de créer une réserve pérenne »*, explique Alain Bouillé. Arnaud Cassagne, directeur des opérations chez Newlode, pointe également la politique de sélection des prestataires. *« Dans certaines sociétés, les achats ne référencent qu'un ou deux acteurs dans le domaine de la cybersécurité. Ils sont souvent choisis sur des critères exclusivement tarifaires. Compte tenu du contexte de pénurie de compétences, l'accompagnement risque alors d'être également au rabais. Si la contractualisation est indispensable, la sécurité repose aussi sur la confiance ».* Les directions des achats des grands groupes sont heureusement de plus en plus réceptives à cette problématique, permettant à leurs RSSI de « contourner » les procédures établies pour accéder à certaines prestations. Ce fut ainsi le cas au Crédit Agricole pour recourir à Oppida, à la Société Générale pour utiliser les outils de BufferZone et chez LVMH pour exploiter les services de surveillance de CybelAngel.

2 QUESTIONS À...

ALAIN BOUILLÉ
RSSI DE LA CAISSE DES DÉPÔTS ET PRÉSIDENT DU CESIN


DR

Comment simplifier la sécurisation des projets des métiers en particulier dans le cloud ?
Quel que soit le projet, il faut donner aux métiers des outils simples afin qu'ils puissent déterminer la sensibilité des données concernées par le projet et du coup ajuster leurs exigences en matière de sécurité. Lorsqu'il s'agit de recourir à des solutions tierces, en particulier dans le cloud, il faut également disposer d'un document contractuel type. Élaboré par le juridique en collaboration avec le RSSI, il précise les engagements attendus des prestataires.

Tous les prestataires acceptent de signer ?
Ce contrat est conçu pour que la plupart des prestataires puissent le signer. En cas de refus, le RSSI vient aider le métier à trouver une solution compatible avec la politique de l'entreprise.

À la recherche de solutions industrielles

Face à l'ampleur et à la prolifération des menaces, la réaction au coup par coup n'est plus possible. L'entreprise doit transformer ses process et changer de paradigme afin d'industrialiser la sécurité.

Chaque entreprise doit disposer d'une cartographie des risques. Les audits montrent les ressources critiques (applications, serveurs, réseaux, données,…) et l'usage qui en est fait. Pour suivre les différentes étapes des audits puis rassembler et suivre les rapports, RSA Archer, Nasdaq BWise et autres SAP GRC représentent autant de plateformes dites de GRC (Governance, risk management, and compliance). Elles permettent en outre de suivre les plans de continuité ou de reprise d'activité, ainsi que la mise en œuvre de politiques de conformité.

Si le RGDP met l'accent sur les données personnelles, l'entreprise doit étendre l'audit à toutes les données sensibles de l'entreprise (comptabilité, bases de clients, données de production,…). Outre la cartographie des données proprement dites, l'audit doit déterminer qui peut y accéder et quelles procédures sont alors associées. Selon un RSSI, *« ces données critiques sont bien trop souvent accessibles à une large part des employés sans justification, et sans traçabilité. Sans parler des comptes génériques "administrateur", non nominatifs, qui sont toujours légion et qui autorisent tous types d'actions, y compris effacer les traces de méfaits… »* Ce que confirme un rapport de Varonis réalisé en avril dernier : les employés de 47 % des entreprises auditées pouvaient accéder librement à plus de 1 000 fichiers sensibles. Éric Cole, doctorant et formateur chez SANS Institute, explique : *« bon nombre d'entreprises peinent à réaliser qu'une attaque externe consiste bien souvent à cibler et piéger un utilisateur interne légitime pour causer des dégâts. Bien peu d'entreprises sont alors en mesure ne serait-ce que de détecter ce qu'il s'est passé. »* Directeur commercial de Balabit France, Yves Mimeran précise : *« les utilisateurs les plus à risques sont les utilisateurs privilégiés, tels que les administrateurs systèmes, car ils sont les cibles les plus intéressantes pour des cybercriminels. Surveiller ces utilisateurs permet de détecter des activités anormales ou suspicieuses et prévenir les fuites de données ».* Le machine learning vient largement à la rescousse dans ces processus d'analyse des comportements sur le réseau interne. Ainsi, Varonis surveille les accès aux ressources (qui, quand, à quelle


DR

TÉMOIGNAGE


DR

KHALED SOUDANI
DIRECTEUR DE L'EXPLOITATION DES INFRASTRUCTURES IT, SOCIÉTÉ GÉNÉRALE

Les acteurs internes de la sécurité doivent descendre dans l'arène, mettre la main à la pâte et co-construire les nouveaux services de sécurité avec leurs partenaires : sécurité et agilité ne peuvent plus s'opposer. Pour ce faire, ils doivent adapter leur gouvernance et leur posture. Les compétences doivent également s'adapter pour permettre de créer les plateformes ouvertes de services. Enfin, les solutions et produits apportés par les acteurs externes vont devoir également s'adapter à ce nouveau monde, de plus en plus basé sur le cloud, les API et l'automation. C'est cela la sécurité de demain, et c'est ainsi qu'elle tiendra sa promesse de transparence et d'agilité.

heure, depuis quelle adresse IP…). Balabit monitore également le trafic réseau afin de profiler les frappes clavier ou la souris lors de sessions d'administration distante afin de détecter une éventuelle usurpation de compte. Dans le contexte d'hybridation du SI, les sondes réseau et les outils d'analyse de flux prennent une nouvelle dimension au sein des architectures de sécurité.

Une terra incognita de la DSI est par exemple l'usage réel qui est fait des services cloud. Entre les métiers qui en souscrivent directement et les utilisateurs qui, de leur propre initiative, les utilisent (tels que des outils de partage, de modification de PDF…), difficile pour un DSI de dire ce qui se passe réellement sur son réseau. C'est l'un des challenges qu'il va s'agir de résoudre alors que le RGPD — qui entre en vigueur en mai 2018 — impose d'identifier où sont les données et de n'utiliser que des prestataires respectant eux-mêmes le réglement européen. Une cartographie des usages peut être obtenue à partir des fichiers de logs des points d'accès à Internet. Les fournisseurs de CASB (Cloud access security broker) proposent des outils automatisés. Selon Sanjay Beri, CEO de Netskope, « *une entreprise utilise en moyenne 1 000 services différents. Or seuls un quart des services actuellement proposés sont compatibles RGPD ; un tiers des services précisent où sont stockées les données ; et un service sur cinq autorise le chiffrement des données.* » Directeur Europe du Sud et Moyen-Orient de Skyhigh Networks, Joël Mollo précise : « *la gouvernance des services cloud est mise en place par le service juridique — ou par le DPO s'il existe — plutôt que par l'IT ou le RSSI. Les audits déclaratifs réalisés auprès des différentes directions sont nécessaires mais pas suffisants : souvent une bonne moitié des outils sont oubliés. Une même société peut utiliser plusieurs dizaines de services de stockage différents, alors qu'un service a été explicitement validé par l'IT* ». Les CASB permettent de contrôler l'usage des services cloud. Ils sont basés sur des proxys réalisant un décodage du protocole http, voire https, et utilisent, quand elles existent, les API des fournisseurs pour obtenir une fine granularité des droits d'accès. Toutefois, la protection contre les fuites de données (Data Loss Prevention) reste relativement limitée et nécessite une configuration complexe, telle que déployer un agent sur tous les postes ou, au minimum,

DR

changer la configuration des proxys et des certificats SSL. Elle sera surtout efficace contre une erreur involontaire. Par contre, un hacker pourra continuer à dissimuler


DR

« L'industrialisation de la *threat intelligence* permet d'automatiser les actes de gestion et donc de recentrer les analystes sur leur valeur ajoutée. La conflictualité est un choc des volontés, des intelligences : obtenir la supériorité informationnelle est stratégique. »
Lieutenant-colonel Victor Le Bihan, de l'État Major des armées, chaîne cyberdéfense

des fichiers chiffrés en les plaçant dans des vidéos, un salarié indélicat les copiera sur une clé USB…

Limiter les failles de sécurité

Comme la lutte contre le phishing par e-mail est de plus en plus efficace, l'entrée et ensuite l'installation des hackers dans les réseaux de l'entreprise se font de plus en plus souvent à la faveur des failles de sécurité. Il devient donc encore plus indispensable de « *patcher* » très rapidement l'ensemble des postes et serveurs, le plus tôt possible après réception des mises à jour fournies par les éditeurs de logiciels. Initialement spécialisé dans ce domaine, Qualys a, depuis, largement étendu sa gamme de solutions et coordonne désormais à la fois des outils de tests externes (implémentant notamment une recherche automatisée de failles), des agents sur les postes, et des sondes d'analyse de flux réseau. « *Notre volonté est d'intégrer dans une seule plateforme ouverte un grand nombre d'outils afin de réduire les redondances dans le stock d'applications de sécurité installées, faciliter l'administration, augmenter la réactivité et contrôler les politiques de conformité mises en œuvre* », explique Philippe Courtot, dirigeant de l'entreprise.

La problématique est différente lorsque l'entreprise développe elle-même des applications : c'est à elle de limiter les →

Sensibilisation et formation obligatoires

La sécurité n'est pas un produit, mais un processus : l'humain doit être placé au centre. Formations, simulations, sensibilisation, améliorations continues : toute l'entreprise doit voir ses compétences progresser afin de créer une chaîne cohérente, efficace et agile.

DR

En sécurité, *le mode projet est devenu obsolète : déployer puis oublier est impossible* », explique Arnaud Cassagne, directeur des opérations chez Newlode. Il faut sans cesse suivre, mettre à jour, améliorer, compléter, explique Laurent Petroque, responsable avant-vente chez F5 Networks : « *il faut consolider les fonctions et éviter l'entassement des technologies. Suivre les projets dans le temps permet de limiter les pertes de compétence, dont les conséquences sont parfois très onéreuses* ». Ainsi, Gilles Berthelot, RSSI Groupe de la SNCF, ne préconise pas systématiquement d'utiliser la meilleure brique du marché, mais plutôt celle qui va limiter les problèmes aux interfaces. « *Le burin ne fait pas le Rodin ! Il faut veiller à créer une chaîne cohérente. De plus, le secteur de la sécurité est en pleine consolidation. Dans ce contexte, les solutions très innovantes font souvent l'objet de rachats par des tiers. Il vaut donc mieux éviter les produits trop exotiques* ». Selon ces experts, il est préférable d'opter pour des éditeurs proposant des gammes de solutions intégrées, que l'on complètera au fur et à mesure. Cette stratégie correspond par exemple à celle d'éditeurs comme Palo Alto Networks ou Qualys. Alexandre Souillé, fondateur et président d'Olfeo, conseille juste de se méfier des généralistes qui se contentent d'aligner des offres hétérogènes non intégrées dans leurs catalogues.

Mais de bons produits ne suffisent pas : encore faut-il savoir les utiliser. Et la formation théorique ne remplace pas la pratique. Comment faire, alors, pour tester des scénarios — pertinence des processus, réactivité, efficacité de la gestion de l'incident — en conditions quasi-réelles sans pour autant toucher au système en production ? Plusieurs start-up françaises ont développé des compétences et une certaine notoriété en la matière. Ainsi, Hns-Platform de Diateam utilise les techniques de virtualisation pour créer des ensembles de serveurs, de postes clients et d'équipements réseaux. « *Il est possible de reproduire le réseau de l'entreprise dans ses moindres détails, y compris des automates industriels, de tester les conséquences d'un malware et de revenir à l'état initial en quelques clics* », explique Guillaume Prigent, fondateur et directeur technique de la société. Une autre start-up, CyberTestSystems, simule du trafic réseau et applicatif, ce jusqu'à 400 Gbit/s. Tester les performances en montée de charge ou valider des politiques de sécurité (telles que des filtrages) devient alors plus facile. Le produit va même beaucoup plus loin : il permet l'injection de flux malveillants, tels que des malwares ou des dénis de services. Enfin, la start-up Bluecyforce est un centre de formation et d'entraînement (ou CyberRange). Elle utilise justement ces produits pour permettre à toutes les entreprises de confronter ses équipes aux situations réelles. Côté poids lourds, Airbus Cybersecurity dispose d'une offre CyberRange dédiée à ses clients, en particulier autour de ses offres de SOC, mais aussi à destination d'étudiants. En effet, la pénurie de compétences est criante, y compris chez les jeunes diplômés : « *en dehors de rares écoles* "up-to-date", *il existe un fossé entre le monde de l'éducation et celui du travail* », explique Arnaud Cassagne. Pour tenter de le combler, Airbus s'est ainsi associé à quatre écoles d'ingénieurs pour en renforcer les cursus.

IL EXISTE UN FOSSÉ ENTRE LE MONDE DE L'ÉDUCATION ET CELUI DU TRAVAIL

Former les équipes informatiques ne suffit pas : tous les collaborateurs doivent être sensibilisés. Le phishing est un bon exemple : des campagnes de sensibilisation couplées à des envois de type Phish.me (outil de génération de vraies-fausses campagnes de phishing) sont efficaces, comme l'atteste Gilles Berthelot, et permettent de repérer les organisations les plus vulnérables. Les serious games, des plus simples aux plus complexes, sont également de bons vecteurs. Pierre Raufast, manager du CERT Michelin, a ainsi composé un jeu de 42 cartes qui a permis de sensibiliser 200 personnes en 2h ! À la SNCF, des jeux sur smartphone permettent la mise en situation. « *Il ne faut plus stigmatiser les utilisateurs. Il faut faire appel à leur intelligence, et valoriser les signalements. Il faut leur dire : "on compte sur vous" et non plus "ne touchez pas"* », conclut Gilles Berthelot.

Se préparer à la crise

Même basé sur les meilleures technologies, aucun système de défense n'est infaillible. L'entreprise doit se préparer à une crise majeure afin d'améliorer sa résilience.

Sans avoir besoin d'évoquer des attaques ciblées complexes, un simple ransomware peut conduire à la faillite d'une entreprise. 34 % des PME touchées en France en début d'année ont vu leurs activités commerciales suspendues, et 16 % ont subi des pertes de revenus, selon un rapport d'Osterman Research réalisé pour MalwareBytes. Les conséquences ont été nettement plus importantes en France qu'aux États-Unis ou en Allemagne.

Se préparer et se former à la crise bien en amont est indispensable : « *une crise est une situation exceptionnelle, déstabilisante. Les procédures classiques ne répondent plus. Il faut se préparer en amont et organiser un process de gestion d'incident, tel que par exemple décrit dans la norme ISO 27035* », explique Hervé Schauer. En particulier, il faut constituer une cellule de crise, qui sera chargée de piloter les actions, de définir des moyens de défense et des moyens logistiques, d'activer un SI alternatif — s'il existe… Comment limiter la casse en amont ? L'hétérogénéité du parc (Mac, Windows, Linux, iOS, Android…) est, par exemple, à privilégier. Il faut ensuite échafauder des scénarios et vérifier que les plans de continuité et de reprise d'activité sont opérationnels et en adéquation.

DR

« *Une fois que les process sont bien formalisés et que les équipes sont formées, il faut organiser des exercices. Tant que ce n'est pas testé, on n'est pas sûr que ça marche* », ajoute Hervé Schauer.

Ensuite, durant la remédiation, attention à ne pas détruire les preuves : celles-ci permettront de comprendre comment s'est passée l'attaque et de déposer plainte auprès des services de police. Raynald Lasota, chef de service chez France Télévision, précise qu'il faut également identifier les prestataires pouvant être impactés en cas d'attaque, et s'intéresser aux relations contractuelles : « *une omerta très importante pèse sur ces sujets, il est très difficile d'obtenir des informations sur les engagements des fournisseurs dans ce type de situation* ».

Damien Lachiver, Cybersecurity and Digital Trust Manager de Wavestone, ajoute quelques conseils : « *il faut clairement répartir les rôles et les responsabilités entre les membres de la cellule, centraliser les informations, créer une main courante de toutes les actions prises. La précipitation n'est pas bonne : il faut prendre le temps d'identifier les impacts d'une décision, et se mettre dans la peau de l'attaquant. Enfin, il faut maîtriser sa communication et rester discret sur sa stratégie de défense* ». →

2 QUESTIONS À…

DR

HENRI LAUDE

CHIEF DATA SCIENTIST ET COFONDATEUR D'ADVANCED RESEARCH PARTNERS

Pourquoi l'intelligence économique rejoint-elle la *threat intelligence* ?

Une attaque n'est pas forcément l'œuvre d'un escroc ni même d'un collaborateur mécontent. Bien que la plupart des entreprises semblent l'ignorer, les actions offensives d'intelligence économique sont courantes. Provenant d'États ou d'entreprises concurrentes, elles sont souvent plus discrètes que les techniques classiques telles que le « *market abuse* ».

Comment bien se préparer ?

Se défendre de manière purement réactive ne suffit pas. Il faut protéger un modèle économique et pas simplement des assets. L'entreprise doit notamment surveiller la stratégie et les mouvements de ses concurrents, mais aussi savoir quels sont ses assets sensibles et qui ils peuvent intéresser. En accumulant ces informations contextuelles et en les modélisant, il est possible de faire émerger des signaux d'alerte en cas de déviance. Il est par ailleurs important de se préparer à toute éventualité et en particulier intégrer dans la cellule de crise des personnes ayant une bonne connaissance du marché et des concurrents. Les décisions à prendre ne sont pas de même nature que lors de l'attaque par un « simple » malware.

DR

→ Frédéric Malmartel, RSSI de l'Agence centrale des organismes de sécurité sociale, insiste sur ce point : « *il faut communiquer en interne et en externe avec authenticité, reconnaître qu'on est en crise, dire ce qu'on sait, ce qu'on fait, rassurer, et faire des points réguliers. Il faut nommer les porte-paroles, les faire connaître, coordonner leur expression et ne pas laisser les acteurs non habilités s'exprimer. Il ne faut ni laisser planer le doute, ni trop en dire, afin d'éviter une crise dans la crise. Il est possible de s'appuyer sur une agence de communication si cela a été préparé en amont* ». Attention toutefois : « *comme le montrent les explications invraisemblables données lors de l'attaque d'Equifax, ces sujets sont encore nouveaux et peu maîtrisés par les agences* », déplore Gérôme Billois.

La cyber-assurance est-elle une solution ? « *Il existe trois types de risques. Le risque qu'on traite, celui qu'on accepte, et celui qu'on n'accepte pas et qu'on assure* », rappelle Alain Bouillé. Pour Hervé Schauer, la couverture des risques informatiques n'est pas tant une nouveauté, et de rappeler que le Clusif a été créé il y a 30 ans par des assureurs. « *Il y a quelques années, le risque cyber était également pris en charge dans les contrats classiques. Il en est désormais exclu et fait l'objet d'une contractualisation séparée. C'est le jackpot pour les assureurs : les primes sont importantes et les dédommagements en cas d'attaque restent rares. Pour cause : un très faible pourcentage des sinistres feraient l'objet de déclaration, soit par manque d'information au sein de l'entreprise, soit même pour éviter toute publicité en interne sur l'attaque* ». Car il s'agit également de communiquer habilement en interne sur les responsabilités des différentes parties impliquées.


DR

« Les entreprises ne sont pas aussi résilientes qu'elles souhaiteraient l'être »
Jean-Marc Gremy, président du Clusif

Il n'empêche, l'offre en cyber-assurance s'étoffe et son marché, estimé à 3, 4 Md$ en 2016, devrait plus que doubler d'ici 2020, selon le réassureur Munich Re.

Comme l'explique Éric Doyen, RSSI d'Humanis, la souscription à une assurance est un processus complexe, mais qui néanmoins se simplifie en raison du gain en maturité des assureurs : « *la première étape consiste à identifier les risques majeurs et à définir les plans de traitement en cas de perte d'intégrité et de rupture d'activité. Ces informations vont être fournies à l'assureur qui va dans la seconde étape auditer ces rapports, contrôler sur pièce, effectuer des sondages, etc. La troisième étape vise à créer ensemble une* "big picture" *de l'ensemble des risques majeurs à couvrir. Peu de normes existent encore pour la construire. Le cyber-assureur va y associer ses propres éléments de mesure. Dans notre cas, ces indicateurs sont révisés tous les 2 ans. Ils permettent de calculer les primes et de définir les exigences de garanties, ainsi que la franchise. Enfin, la dernière étape est la phase de négociation commerciale* ». En excluant la première étape, il lui a fallu environ six mois pour contractualiser.

Comme le fait remarquer Guillaume Poupard, directeur général de l'Anssi, la cyber-assurance a un rôle important à jouer, en dehors des garanties financières, particulièrement vis-à-vis des PME qui sont souvent démunies en cas d'attaque. Car la mise en relation avec des professionnels dédiés, le service, ou encore l'assistance permettraient de limiter les impacts. La prévention pourrait également être améliorée. Axa et Allianz-Gan proposent déjà des contrats simplifiés pour cette catégorie d'entreprises. En avril dernier, Generali s'est pour sa part associé avec Europe Assistance (pour le support) et Engie Ineo (pour les interventions techniques).

L'entreprise doit également savoir qui contacter si elle n'arrive pas à faire face à l'attaque. Les opérateurs d'importance vitale (OIV) peuvent espérer compter sur le soutien de l'Anssi. Les autres devront se tourner vers un prestataire privé. Les opérateurs de SOC, mais également certaines sociétés de conseil spécialisées en sécurité, disposent d'équipes « commandos ». Ces « pompiers » sont capables d'intervenir sur sites 7 jours sur 7, 24 heures sur 24. Là encore, avoir identifié les bons partenaires permettra de tisser les relations de confiance nécessaires et de réduire les dommages. Comme le prétend le logo de Hns-Platform, « *Si tu veux la paix, prépare la cyber-guerre* »…