paloalto NETWORKS | LA TRIBUNE

GOUVERNER À L'ÈRE DU NUMÉRIQUE

LE GUIDE DE LA CYBERSÉCURITÉ POUR LES DIRIGEANTS D'ENTREPRISE

FRANCE

EN COLLABORATION AVEC

CESIN | SOLUTIONS numériques

GOUVERNER À L'ÈRE DU NUMÉRIQUE :
Le guide de la cybersécurité pour les dirigeants d'entreprise

EN COLLABORATION AVEC

CESIN

SOLUTIONS numériques

Gouverner à l'ère du numérique : Le guide de la cybersécurité pour les dirigeants d'entreprise

Gouverner à l'ère du numérique : Le guide de la cybersécurité pour les dirigeants d'entreprise
Edité par : K-Now SARL, 21 rue de Fécamp 75012 Paris, pour le compte de Palo Alto Networks
Responsable éditorial : Jérôme Saiz
Editeur: Jean Kaminsky
Imprimé en France par Point 44

Les opinions exprimées dans la présente publication sont celles des auteurs. Elles ne prétendent pas nécessairement refléter les opinions ou les vues de Palo Alto Networks.
Cet ouvrage est un guide généraliste à but d'information. Il n'est pas destiné à se substituer à un conseil personnalisé en cybersécurité.

Gouverner à l'ère du numérique : Le guide de la cybersécurité pour les dirigeants d'entreprise
Dépôt légal septembre 2016

Pourquoi un guide sur la cybersécurité pour les dirigeants d'entreprise ?

Les dirigeants d'entreprise et les membres des Comités de Direction prennent quotidiennement des décisions stratégiques. Que celles-ci soient d'ordre financier, commercial ou industriel leurs conséquences auront toujours un impact considérable sur l'avenir de leur entreprise.

Mais il s'agit là de domaines historiques bien maîtrisés pour lesquels les dirigeants disposent d'une expérience considérable.

Ces derniers sont toutefois désormais amenés à prendre des décisions tout aussi stratégiques, et aux conséquences tout aussi sérieuses, dans un domaine mouvant et en création permanente pour lequel ils n'ont bien souvent aucune expérience significative : le numérique. Or si ignorer l'évolution numérique serait risqué pour l'entreprise, s'y engager aveuglément pourrait l'être tout autant.

Ce guide a été conçu comme un outil pratique destiné à aider les dirigeants à acquérir les connaissances stratégiques essentielles en matière de cybersécurité, afin qu'ils soient en mesure de prendre les bonnes décisions dans le cadre de leur stratégie numérique.

Il ne s'agit toutefois pas d'un manuel de cybersécurité. Notre objectif en créant ce guide est tout autre. Nous avons souhaité :

- Que chaque dirigeant d'entreprise y trouve un éclairage synthétique sur les points stratégiques de cybersécurité qu'il ne peut se permettre d'ignorer.
- Que pour chacun de ces points il dispose d'éléments concrets pour faire avancer le sujet à l'issue d'une réunion du Comité de Direction.

Ce guide est rédigé par des experts français reconnus du monde de la cybersécurité, dont l'activité professionnelle les conduit à intervenir au plus près des dirigeants d'entreprise.

Chaque chapitre couvre un domaine stratégique, allant des aspects juridiques jusqu'à la transformation numérique en passant par la cyberassurance, le recrutement ou l'usage du Cloud.

Chacun est destiné à donner au dirigeant une vision synthétique du sujet et lui permettre de répondre aux questions essentielles : de quoi parle-t-on exactement ? En quoi cela est-il stratégique pour mon entreprise ? Quels sont les risques ? Quel est le lien avec la cybersécurité ?

Chaque chapitre se conclut par un élément actionnable : soit une liste d'actions-clés afin d'anticiper sur la problématique en question (des missions à lancer, des projets à mettre en oeuvre afin de préparer le terrain...), soit une série de questions pertinentes à poser aux équipes afin de contrôler que la thématique est bien suivie au sein de l'entreprise.

C'est d'ailleurs le scénario d'utilisation que nous avons imaginé lors de la conception de ce guide : nous souhaitions qu'un dirigeant s'apprêtant à animer une réunion du Comité de Direction dans laquelle un sujet de cybersécurité va être abordé puisse ouvrir ce guide au chapitre concerné, le parcourir durant son trajet et arriver avec une connaissance synthétique des enjeux et des éléments concrets pour faire avancer le sujet (à qui confier la mission ? Quels sont les points de vigilance ? Comment préparer le terrain ?)

Alors si vous lisez ces lignes en route pour rencontrer votre Comité de Direction, nous espérons que ce guide vous aidera à alimenter votre réflexion, saura répondre à vos interrogations et vous permettra de jouer pleinement le rôle qui est le vôtre : celui du capitaine de votre entreprise. Bon vent ! ■

Palo Alto Networks

SOMMAIRE

III. Actions

IV. Témoignages

Fiches Auteurs

Introduction

Les cybermenaces, à l'ère du numérique

1

Paysage des menaces à l'ère numérique

Par Greg Day

Greg Day est Vice-Président et CSO EMEA chez Palo Alto Networks, responsable de la stratégie de cybersécurité et du développement de la Threat Intelligence.

Depuis cinq ans, les autorités sanitaires commencent à reconnaître la dépendance à la technologie comme une véritable addiction. Il suffit de voir le temps passé par un utilisateur moyen sur son smartphone et l'utilisation qu'il en fait. En général, le smartphone est affecté à un usage à la fois personnel et professionnel : de l'achat en ligne au suivi des mesures de santé, tout passe par des systèmes interconnectés, des applications et des données. De cette tendance ont émergé de nouveaux modes de vie. Mais surtout, l'extension du réseau et la numérisation de la société ont amené les responsables du monde entier à reconnaître la place prépondérante qu'occupe désormais l'hyperconnectivité, une tendance qui n'est pas prête de s'inverser et devrait même s'accélérer.

Face à ce constat, l'Union européenne a introduit deux changements majeurs qui prendront effet en mai 2018. Le premier est la révision des exigences de protection des données garantissant à tout citoyen que les informations qu'il fournit sont traitées conformément aux normes en vigueur et qu'en cas d'incident notable, il sera averti du problème dans un délai raisonnable. Ces dispositions sont celles du Règlement général sur la protection des données.

Le second reconnaît que le fonctionnement des services publics au sens large, comme les services financiers, les transports, la santé et les services de distribution de l'eau, entre autres, est devenu indissociable de la technologie et qu'en cas de cyberattaque, les conséquences pourraient être désastreuses et affecter le PIB de tout un pays. La Directive sur la sécurité des réseaux et de l'information reconnaît ce danger et oblige chaque pays à identifier les services

concernés, à garantir qu'une cybersécurité tenant compte de l'état de l'art soit mise en place *(voir le chapitre 4, « Qu'est-ce que l'état de l'art en matière de cybersécurité »)* et à travailler avec les autorités nationales compétentes pour garantir la continuité de ces services et préserver la confiance des ménages.

Les États ont pris conscience du caractère vital des technologies. Et votre entreprise ?

Si les Nations ont conscience de l'importance de la technologie, en est-il de même de votre côté ? Et quid de votre entreprise ?

Le problème pour beaucoup d'entreprises est que la technologie évolue avec une telle rapidité qu'elles peinent à suivre le rythme. Et puis, le monde numérique et la cybersécurité utilisent ce que beaucoup considèrent comme une langue étrangère : des nouveaux termes, des abréviations à foison qui changent aussi vite que la technologie. Au final, beaucoup ont le sentiment d'être perdus et de ne pas tirer entièrement profit de l'avantage concurrentiel que pourraient leur offrir les nouvelles technologies.

En tant que responsable, vous pouvez difficilement éviter d'aborder cette question, car elle peut avoir d'importantes retombées, positives ou négatives, sur votre activité.

En outre, les modifications introduites par la législation européenne marquent un tournant majeur dans l'univers de la cybersécurité, et pourraient avoir des implications pour les équipes de cybersécurité. Emparez-vous donc de l'occasion pour révolutionner vos connaissances de la cybersécurité, mais aussi votre approche de la question.

Pourtant, emportés dans le tourbillon du quotidien, beaucoup ont atteint un point de rupture, souhaitant désespérément marquer une pause. Mais le moment est enfin venu. Les entreprises vont pouvoir réévaluer non seulement ce que doit être une cybersécurité au niveau de l'état de l'art, mais aussi la manière dont nous organisons le traitement de nos données, vouées à se multiplier de manière exponentielle.

Un plan cybersécurité en trois volets

Par où commencer ? La cybersécurité comprend trois volets majeurs.

(1) La dépendance de votre activité au numérique ; il s'agit en l'occurrence des systèmes technologiques utilisés en interne et dans le Cloud. Et les données que vous stockez sur ces systèmes, qu'il s'agisse d'informations client, de processus métier, de propriété intellectuelle ou autre. Ces éléments peuvent être très différents selon votre cœur de métier (prestataire de services, détaillant ou organisation financière).

(2) Les risques encourus du fait de cette dépendance technologique, dont certains sont plus faciles à qualifier que d'autres, comme le délit d'initié. Ils peuvent provenir d'une erreur humaine, d'un employé mécontent ou encore d'une source externe. Les menaces externes sont les plus difficiles à qualifier, car plus volatiles du fait d'une grande variété de techniques, d'acteurs et de motivations. Cela nous conduit trop souvent à nous perdre dans un flot de détails de bas niveau relatifs au fonctionnement, alors que nous devrions nous concentrer sur les conséquences et les

« La cybersécurité peut, et doit, fonctionner à la même vitesse que la technologie qu'elle vise à protéger »

« Il devient impossible d'éviter le débat sur notre dépendance à la technologie »

probabilités de ces attaques, ainsi que sur les scénarios optimistes et pessimistes en cas d'incident avéré. Mais en nous appuyant sur l'expérience militaire et celle du secteur des assurances, qui abordent différemment ce qui reste pourtant le même problème, nous pouvons essayer d'y voir plus clair.
Ce qui nous amène au dernier point de ce triptyque sur la cybersécurité : quelle forme de résistance adopter face aux risques ?

(3) La cyber-résilience est une lutte permanente opposant esprit du bien contre esprit du mal dans laquelle chacun tente de prendre le pas sur l'autre. Nous devons prévoir le meilleur, mais aussi nous préparer au pire. Ce qui pose quelques difficultés au vu du nombre d'adversaires, tandis que les limites de ce qu'on pourrait appeler le champ de bataille sont sans cesse repoussées. Ce que je veux dire, c'est que la technologie poursuit son évolution et les menaces font de même.
Pour beaucoup, cette instabilité est devenue notre talon d'Achille. En nous adaptant perpétuellement aux nouvelles menaces, nous avons fini par créer un ensemble complexe de solutions à des problèmes spécifiques ayant des niveaux de maturité différents. La cybersécurité implique généralement une intervention humaine poussée. À l'instar d'une voiture de sport haut de gamme, la cybersécurité peut repousser les limites tout en montrant une très grande fragilité.
C'est un peu comme vouloir lire simultanément de la musique sur cassette, CD, VHS, DVD et support numérique HD et attendre du lecteur qu'il gère tout cela de manière transparente pour nous.

Observer l'existant avant de décider

Avant de procéder à un changement quelconque, il est impératif de faire un point sur la situation réelle de votre entreprise. Pour cela, plusieurs méthodes s'offrent à vous.

Vous pouvez demander à un tiers d'effectuer une analyse différentielle, vous pouvez étudier les données de mesures fournies par votre équipe de cybersécurité ou tout simplement tester l'efficacité de vos capacités actuelles. De plus en plus d'entreprises appliquent un vieil adage : la connaissance vient avec l'expérience.

Faire procéder à des simulations d'intrusion par ceux que l'on appelle parfois la Red Team (l'équipe en charge des tests d'intrusion) est un excellent moyen de tester ses capacités de protection et de réponse aux incidents. Ces tests portent bien évidemment sur les capacités techniques, mais aussi sur les compétences individuelles, les compétences inter-équipes et même sur la capacité de la direction à prendre des décisions stratégiques à la lumière des informations disponibles, en cas d'attaque.

En cybersécurité comme dans la vie, rien n'est garanti. La technologie est un alignement de uns et de zéros que beaucoup estiment parfaitement prévisible. Bien au contraire, en réalité, des choses inattendues peuvent se produire ; et c'est même inéluctable. Accepter cette fatalité est une première étape. Décider des compromis que l'on sera prêts à accepter lorsqu'un incident se produit, est la

« Les directives Européennes sur la protection des données représentent une rare opportunité d'amélioration pour les entreprises »

deuxième étape. Cela nous ramène au triptyque de la dépendance des entreprises à la technologie, aux risques et à leurs conséquences sur l'activité. Il faut décider en toute connaissance de cause où placer le curseur entre risques acceptables et investissements pour parvenir à limiter les risques.

La cyberassurance à la rescousse

Lorsque vous répondrez à cette question, vous devrez également identifier les éléments sur lesquels porteront ces investissements. Pendant plusieurs décennies, nous avons mis l'accent sur la défense dans le but d'éviter tout incident de cybersécurité. Mais ces dernières années, les lignes ont bougé et nous avons commencé à accepter l'inéluctable à savoir que certaines attaques ne pourront être évitées et que, le cas échéant, l'important est de se concentrer sur la réponse à apporter pour limiter les risques. Cette prise de conscience a permis le développement phénoménal, quoique précoce, du marché de la cyberassurance *(lire à ce sujet le chapitre 10, « L'avenir de la cyberassurance »).*

Cette tendance consiste à transférer une partie du risque, notamment l'aspect financier, à un tiers. Ce faisant, la gestion du risque permet d'atténuer nettement les conséquences des incidents (comme pour de nombreux aspects de la vie courante, d'ailleurs).

Par ailleurs, en s'appuyant sur les compétences et l'expérience d'experts en assurance, une entreprise pourra bénéficier d'informations précieuses à la fois sur les risques encourus et sur les meilleures pratiques pour les combattre.

Lorsque vous prenez en considération ces meilleures pratiques et procédez à vos exercices de simulation, demandez-vous si vous allez mettre en place votre propre équipe d'intervention ou faire appel à un service externe.

Les équipes d'intervention d'urgence sont généralement des professionnels qui utilisent des connaissances et des outils coûteux que, idéalement, nous n'appelons que ponctuellement.

Prévenir, détecter et répondre : où placer le curseur ?

La législation européenne (la Directive sur la sécurité des réseaux et de l'information et le Règlement général sur la protection des données – *lire le chapitre 2, « Cybersécurité et droit : que faut-il retenir ? »)* exige des organisations qu'elles informent les autorités nationales concernées, dans un laps de temps donné, lorsque des incidents précis se produisent. Vous ne pouvez donc pas vous passer d'une telle équipe d'intervention d'urgence.

Mais cela soulève une autre question de taille : quel est le juste milieu entre investir dans la prévention et la détection, et investir dans une capacité de réponse aux incidents ? Comment trouver le juste équilibre entre protection et cyberassurance ?

Pour trouver ce juste milieu, vous devrez donc être capable d'arbitrer en fonction de l'état de l'art du moment et des coûts.

Recrutement difficile et coûts d'exploitation élevés

Pour reprendre l'analogie du lecteur de musique évoquée plus haut, dans la réalité, un tel système aurait besoin pour fonctionner de convertir les différents formats sur un support unique commun qui pourra être lu par un seul lecteur.

Et il en va souvent de même pour la cybersécurité : de nombreuses capacités ou solutions différentes nécessitent une intervention humaine pour fonctionner comme un ensemble cohérent. Dans un monde toujours plus numérique cela peut sembler être (et je pense que ce n'est pas qu'une impression) une solution archaïque.

En outre, la dimension humaine se révèle être particulièrement coûteuse dans le domaine de la cybersécurité, et ce à double titre : d'une part parce qu'elle représente des coûts d'exploitation élevés (sans même évoquer la pénurie d'experts sur le marché) et d'autre part elle ralentit la capacité de réaction numérique. Dans ces conditions, comment trouver le bon équilibre ?

De nombreuses entreprises se tournent alors vers des tableaux de bord de cybersécurité pour connaître l'état dans lequel se trouvent leurs capacités de protection. Selon l'activité, cela peut aller de l'affichage de données triviales à collecter, jusqu'à des mesures incroyablement détaillées.

Hélas beaucoup se concentrent sur les indicateurs de performances médiocres, qu'il s'agisse d'un retard au niveau des contrôles de sécurité ou du nombre d'événements qui se sont produits sur un temps donné.

Unifier les capacités de cybersécurité

Nous devrions réfléchir aux moyens d'exploiter la technologie afin de rendre la cybersécurité plus efficace. Pour cela, nous devrions nous pencher sur l'architecture d'une plateforme commune, permettant aux différentes capacités requises de coexister tout en limitant au maximum l'intervention humaine.

Mais surtout, cette plateforme devra être tournée vers l'avenir. Pour reprendre l'analogie du lecteur, celui-ci pourra lire le nouveau format sans que personne n'ait besoin de le convertir dans un format compatible.

Malheureusement, la cybersécurité, tout comme la technologie qu'elle protège, est plus complexe qu'un lecteur multimédia. Mais plus l'automatisation prend le dessus et plus nous pouvons passer d'un système de détection/réponse à un système de prévention *(lire le chapitre 7, « La prévention peut-elle être efficace ? »)*.

La cybersécurité peut, et doit, fonctionner à la même vitesse que la technologie qu'elle vise à protéger. Cette technologie va continuer à progresser à grand pas, et pendant que les responsables de la cybersécurité seront occupés à suivre le rythme, ils perdront du terrain.

Les changements juridiques de l'Union européenne qui entreront en vigueur en 2018 sont une rare opportunité. Grâce à leur portée, la question de la cybersécurité pourra enfin, si ce n'est déjà fait, s'inscrire à l'agenda du comité de direction *(lire à ce sujet le chapitre 12 : « Horizon 2020 : les priorités du comité de direction »)*. Ils offrent l'occasion d'impliquer les membres de l'entreprise qui doivent l'être et de trouver un langage commun avec lequel tous pourront communiquer.

De même, les exigences spécifiques relatives à la prise en compte des risques, à l'état de l'art et à l'obligation de notification fournissent à chaque entreprise l'occasion unique de prendre du recul et d'échapper au tourbillon des activités quotidiennes. Elles pourront ainsi repenser leur approche afin de suivre le rythme des exigences actuelles et à venir, et trouver ainsi un meilleur équilibre entre détection, protection et réponse. Elles pourront le faire en fonction de leur appétence au risque, en appliquant une approche axée sur l'état de l'art, aussi dynamique que le monde dans lequel nous vivons. ■

Pour anticiper

1. **Familiarisez-vous avec les principes de base de la cybersécurité**
   Rome ne s'est pas faite en un jour, et si vous ne vous êtes pas jusqu'à présent intéressé directement à la question de la cybersécurité, vous allez découvrir un univers qui vous est probablement – pour l'instant – opaque. La lecture de ce guide est un bon début, mais n'en restez pas là !

2. **Entamez une réflexion au plus haut niveau sur votre dépendance à la technologie**
   De qui êtes-vous dépendant parmi vos fournisseurs de technologie ? Quels sont les systèmes dont vous ne pourriez entièrement vous passer ? Qu'arriverait-il si vous en étiez soudain privés ?

3. **Lancez un recensement des informations stratégiques et des systèmes numériques qui les traitent**
   On ne protège bien que ce que l'on connaît. Si un tel recensement n'a pas déjà été réalisé, initiez le projet. S'il a été fait (ce qui devrait être le cas), prenez le temps de parcourir sa synthèse afin de vous familiariser avec votre paysage informationnel.

I Législation et réglementation

2

Cybersécurité et droit, que faut-il retenir ?

Par Maître Olivier Iteanu.

Maître Olivier Iteanu est Avocat à la Cour d'Appel de Paris depuis Décembre 1988, arbitre et médiateur agréé par le Centre de Médiation et d'Arbitrage de Paris (CMAP). Il est également chargé d'enseignement à l'Université de Paris XI (Faculté Jean Monet) et à l'Université de Paris I Sorbonne.

Les juristes considèrent que le sujet de la cybersécurité concerne toutes attaques ayant pour objectif bien évidemment un système d'information, mais également toutes infractions commises au moyen d'un système d'information. Le terme de cybersécurité a d'ailleurs fait son apparition il y a quelques années pour remplacer celui de cybercriminalité parce que la cybersécurité intègre des dimensions nombreuses et autres que la seule politique pénale que traduisait le mot « criminel ».

Le contrat par exemple, participe à la cybersécurité *(lire à ce sujet le chapitre consacré à l'usage du Cloud)*, de même que toutes les formes de prévention touchant à l'organisation jusqu'à la formation des personnels. Par l'adoption de ce terme, les professionnels du Droit ont pris acte que la lutte contre la cybercriminalité prend place bien en amont de l'incident ou de l'attaque, et que ces actes préventifs entrent dans le phénomène rebaptisé plus globalement cybersécurité.

Ce phénomène, les législateurs nationaux et communautaires, ainsi que les Tribunaux, ont été amenés à se pencher dessus et conduits à prendre des décisions depuis plusieurs années déjà.

Et si au fil du temps de nombreux textes ont été votés et promulgués, pour le dirigeant d'entreprise l'attention doit aujourd'hui se porter en priorité sur les deux derniers en date, qui sont le fait de l'Union Européenne. Il s'agit du Règlement Général sur la

[1] Règlement n° 2016/679 du 27 avril 2016 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

« En matière de cybercriminalité on peut se trouver à la fois victime et responsable »

Protection des Données (RGPD) à caractère personnel publié au Journal Officiel le 4 mai 2016[1] et la Directive sur la sécurité des réseaux et des systèmes d'information dite Directive NIS adoptée par le Parlement européen le 6 Juillet 2016[2].

Mais ces textes communautaires, comme la plupart des textes de Lois d'aujourd'hui, sont d'une grande complexité et difficiles d'accès. Ainsi, le RGPD comporte pas moins de cent soixante-treize « considérants » pour le seul préambule du texte, qui donnent suite à quatre-vingt-dix-neuf articles. Dans ces conditions, pour assimiler ces nouvelles règles impératives, comprendre quelles sont ses nouvelles obligations, il faut tenter d'appréhender le sens de l'histoire, le mouvement donné par la Loi. Dans le cas de la cybersécurité, cela peut se résumer par la formule « toujours plus ».

Toujours plus de sanctions

Les sanctions se multiplient et gagnent en volume depuis maintenant près de dix ans. Ainsi, un délit comme celui « *d'accès ou de maintien frauduleux à un système de traitement automatisé de données* » qui correspond à la violation de domicile dans le monde physique, sans qu'aucune perturbation du système, aucun « vol » ou destruction de données n'ait été commis, a vu ses peines doublées par la Loi relative au renseignement du 24 juillet 2015, passant aux peines maximales de deux ans d'emprisonnement et de 60.000 euros d'amende.

Mais le plus spectaculaire n'est pas là, il se trouve dans le RGPD et ses sanctions en matière de données à caractère personnel. La réglementation en matière de données personnelles connaît un système de double peine. Le responsable d'un traitement de données personnelles, s'il manque à une obligation de la Loi informatique et libertés, peut être lourdement sanctionné à la fois par une sanction pénale pouvant toucher son dirigeant à titre personnel et par une sanction pour non-conformité prononcée, en France, par la CNIL. Or dans les faits toute entreprise est responsable d'un traitement de données personnelles ne serait-ce que pour ses salariés et l'élaboration des fiches de paie, tout e-marchand l'est vis-à-vis de ses clients et de ses prospects, etc. Cette obligation concerne donc, potentiellement, toutes les entreprises.

Ainsi le respect de la confidentialité des données personnelles collectées connaît ce double régime de sanctions. l'article 226-22 du Code pénal prévoit que « *Le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.* »

La sanction est la même en cas d'accès par des tiers non autorisés à des données personnelles en raison d'un manquement aux règles de sécurité, ce que la Loi prévoit par le fait de ne pas avoir pris « *toutes précautions utiles* »[3]. Cela signifie que l'accès aux données personnelles a

[2] Directive 2016/1148.

[3] Article 34 de la Loi modifiée n°78-27 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

pu avoir lieu parce que les mesures de sécurité - techniques et organisationnelles - ne reflétaient pas au jour de l'attaque, les règles de l'art attendues en pareille situation *(voir le chapitre sur la difficulté à traduire les « règles de l'art » en mesures concrètes).*

Or, de son côté, la CNIL ne disposait jusqu'alors que de la possibilité, d'une part, de sanctionner jusqu'à 150.000 euros (300.000 en cas de réitération), d'autre part, de publier la décision rendue. Des sanctions plutôt faibles... Mais dans le RGPD, qui est applicable au 25 mai 2018, ces sanctions passent à 20 millions d'euros ou 4% du chiffre d'affaires annuel et mondial du contrevenant si ce chiffre est supérieur. Le moins que l'on puisse dire est que la sanction paraît ainsi plus dissuasive.

Plus de diligences

Les Lois prévoient également plus de diligences à la charge des responsables de système d'information. Cela signifie par exemple la généralisation de ce que l'on a appelé la notification d'une faille de sécurité. Prévue pour la première fois dans le dernier Paquet Télécom européen transposé en droit français par une Ordonnance n°2011-1012 du 24 aout 2011, cette obligation ne concernait à l'origine que les violations de données à caractère personnel et les seuls « *fournisseurs de services de communications électroniques* ». Ces fournisseurs semblaient correspondre aux opérateurs de communications électroniques (les ex-opérateurs télécoms) et à tous ceux qui offrent un accès aux réseaux numériques (boutiques avec un accès Wi-fi offert aux clients et accès publics notamment). On se demandait bien pourquoi une telle obligation ne concernait qu'une seule catégorie d'acteurs économiques. Cette anormalité est désormais corrigée. Désormais, le RGPD prévoit que tout responsable de traitement de données personnelles est concerné par cette notification d'une violation de données personnelles. Et comme nous l'avons évoqué précédemment, toute entreprise est désormais potentiellement « responsable de traitement de données personnelles », ne serait-ce que dans le cadre de l'élaboration des salaires…

Bien évidemment pour rendre cette obligation de notification obligatoire, le défaut de notification est puni de 5 ans d'emprisonnement et de 300.000 euros d'amende[4].

S'agissant de la Directive NIS, elle prévoit que cette notification est même étendue au-delà des seules données personnelles, lorsque l'attaque concerne un « *opérateur de services essentiels* » ayant subi une cyberattaque.

Dans la même idée, le RGPD a promu de nouveaux concepts juridiques aux doux noms *d'accountability* et de *privacy design*. Là encore, le responsable de traitement doit montrer très tôt qu'il a fait diligence.

Le premier des deux concepts signifie « *L'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données* » selon la définition donnée par la CNIL, tandis que le second concept signifie que dès la conception de son système d'information les questions de protection de la vie privée ont été prises en compte.

La multiplication de ces obligations de diligence signifie que l'on est passé d'une simple obligation de moyens à une obli-

[4] Article 226-17-1 du Code pénal.

« L'esprit de la Loi en matière de cybersécurité : toujours plus ! »

gation de moyens dite renforcée. Nous ne sommes finalement plus très loin de l'obligation de résultat, bien que celle-ci serait ridicule en matière de sécurité. Toutefois les législateurs exigent désormais des acteurs économiques qu'ils montrent en permanence une diligence dans leurs actes anticipant les questions de cybersécurité et qu'ils soient en mesure de le prouver en cas d'attaque ayant des conséquences néfastes.

Plus de responsables

Enfin, la notion de responsable juridique prend une toute autre ampleur avec les derniers textes promulgués. On savait déjà, par une jurisprudence constante des tribunaux depuis plusieurs années, qu'en matière de cybercriminalité on pouvait se trouver à la fois victime et responsable sur le plan juridique. Le cas de figure typique est celui d'un système d'information auxquels des attaquants avaient eu frauduleusement accès. Le responsable de ce système est alors dans ce cas bien évidemment la victime. Mais il se trouve que les attaquants ont rebondi pour attaquer un second système cible qui, lui, a connu des dégâts importants. Or, l'attaque n'a été possible que parce que le premier système était défaillant en matière de sécurité. Dans un cas comme celui-là, bien que victime, le responsable du premier système d'information peut être jugé responsable juridiquement.

Cette mésaventure est devenue un classique en la matière. Orange l'a d'ailleurs connu dans une affaire jugée par la CNIL[5]. En l'occurrence, 1,3 million de données clients d'Orange s'étaient trouvées dans la nature. L'enquête menée par la CNIL avait révélé un certain nombre de manquements du sous-traitant de l'opérateur.

Ça n'était donc pas Orange le responsable d'un point de vue technique de la défaillance, mais en quelque sorte la victime. Pourtant, la CNIL avait relevé notamment, que l'opérateur avait communiqué les données concernées à son sous-traitant *« de manière non sécurisée »*, c'est-à-dire non chiffrée. C'est donc Orange que la CNIL a choisi de sanctionner sévèrement.

Aujourd'hui toutefois le RGPD est en voie de permettre également de sanctionner le sous-traitant. Ainsi, le Règlement européen élargit ainsi le nombre de personnes pouvant être jugées responsables dans le cadre d'une même affaire.

En conclusion

Le message clair adressé par les législateurs, notamment le législateur européen, à tous les acteurs économiques nous paraît être le suivant : la technique et l'organisation sont le préalable de la cybersécurité. La Loi s'intéressera désormais à savoir si vous, organisations de toutes sortes, de droit privé comme public, avez mis en place à temps les mesures techniques et organisationnelles suffisantes pour anticiper les attaques informatiques. A défaut, non seulement vous ne bénéficierez pas de la protection de la Loi mais votre responsabilité juridique pourrait être engagée. Autant donc entendre au plus tôt ce message et s'organiser en conséquence. ■

[5] Délibération 2014-298 du 27 aout 2014.

« De nouvelles sanctions jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel et mondial »

Pour anticiper

1. **Préparez la nomination d'un DPO**
   Si l'activité de l'entreprise l'exige, celle-ci devra nommer un Data Protection Officer (DPO) à partir de 2018. S'il n'y a à ce jour pas de Correspondant Informatique & Libertés dédié au sein de l'organisation, ou si ce poste est confié au RSSI en sus de ses missions de sécurité des systèmes d'information, il est conseillé d'anticiper en sanctuarisant la fonction de protection des données personnelles et en la faisant évoluer à terme vers un profil de DPO.

2. **Documentez clairement les mesures de protection appliquées aux données à caractère personnel**
   L'entreprise doit pouvoir prouver rapidement et de manière claire qu'elle applique les bonnes pratiques du moment en matière de protection des données à caractère personnel. Cela peut être exigé par la Justice ou demandé par un auditeur.

3. **Renforcez les exigences de protection de l'entreprise vis-à-vis de ses sous-traitants et partenaires, et les moyens d'échange avec ces derniers**
   La jurisprudence Orange montre que sous certaines conditions l'entreprise peut être jugée responsable d'une fuite de données personnelles de ses clients même si celle-ci a eu lieu chez un partenaire.

3

Engagements et responsabilités de l'équipe dirigeante

Par Avi Berliner et Gregory Albertyn

Gregory Albertyn est Directeur Senior et Avi Berliner est responsable Financial Services, Application Strategy & Integration, tous deux chez PwC.

Le Conseil d'administration prend régulièrement des décisions et fonde ses choix sur le jugement des « gardiens » : des personnes clairement identifiées chargées de protéger les données les plus stratégiques de l'entreprise. Or, le Conseil ne peut pas se permettre de tout examiner en détail ; il doit consacrer son temps à des aspects plus stratégiques.

Pourtant, avec l'évolution permanente des cyber-risques en termes de complexité réglementaire et technique, et leur caractère constant, le Conseil d'administration est amené à élargir de plus en plus son champ d'intervention.

Pour l'aider à répondre à la future législation européenne (pour plus d'informations, voir le chapitre *« Cybersécurité et droit : que faut-il retenir ? »)*, vous devrez *« envisager d'adopter les technologies les plus récentes en termes de cybersécurité »*, dit en substance le texte.

Face à cette définition laissée volontairement vague par les législateurs européens, une définition plus précise devrait se dessiner pour votre propre organisation dès que cette dernière aura une meilleure vision de la nature, de l'étendue et du positionnement des cybermenaces auxquelles elle est confrontée.

Définir concrètement « Les technologies les plus récentes »?

Or, l'intégration des *« technologies les plus récentes »* mentionnées par le législateur passe impérativement par la mise en place d'une structure de gouvernance durable en matière de cybersécurité et de respect de la vie privée. Cette structure, supervisée par la Direction, est chargée de surveiller les cyber-risques et les risques relatifs au respect de la vie privée, et l'adéquation des

mesures correctives prises par l'entreprise. Traditionnellement, la protection et la confidentialité des données poussaient à la mise en œuvre d'un ensemble de modèles de gouvernance aux objectifs divers: maturation des possibilités de gouvernance de données, réalisation d'évaluations en vue de définir un point de référence, création d'un modèle cible destiné à la hiérarchisation et à la gestion des risques.

A partir de ces approches, des outils de surveillance et de génération de rapports en réaction aux menaces ont ainsi vu le jour.

Or cela ne suffit plus : de par l'évolution de la nature même de l'adversaire, la cybersécurité de dernière génération se doit d'être dynamique afin de tenter non seulement d'identifier et de répondre à la totalité des nouvelles menaces, mais surtout de le faire quasiment en temps réel.

L'architecture de protection de la vie privée évolue au gré des nouveaux systèmes.

Nous assistons en outre aujourd'hui à une nouvelle évolution avec l'apparition de l'architecture de protection de la vie privée. Cette architecture regroupe un ensemble de recommandations et de principes qui sont directement intégrés dans les processus technologiques et métiers, et non plus rajoutés après coup *(il s'agit du concept de « Privacy by Design » selon le terme consacré).*

La cyber-résilience fait désormais partie intégrante de votre structure opérationnelle. Les coûts de mise en conformité et les besoins en ressources sont donc réduits. Vous pouvez ainsi inscrire une gouvernance contre les cyber-risques et les risques liés à la vie privée directement dans vos plans stratégiques, à l'instar de vos activités quotidiennes.

Par ailleurs, les technologies les plus récentes exploitent également les possibilités exponentielles du Big Data. Elles tirent parti non seulement de ses capacités de stockage et d'analyse visant à améliorer constamment les écosystèmes applicatifs, mais également de ses possibilités d'analyse prédictive en temps réel par lot.

Grâce à ces technologies, vous pouvez déployer des outils d'apprentissage machine et d'autres outils d'intelligence artificielle pour protéger les fonctions et données métiers stratégiques contre les vecteurs d'attaque encore inconnus.

Vous devez adopter de plus en plus largement des mesures de respect de la vie privée dès la conception (« Privacy by design ») pour vous assurer que l'architecture de sécurité et d'entreprise répond aux exigences de conformité en matière de cyber-résilience et de respect de la vie privée lors de l'évaluation initiale. Vous devez, par ailleurs, veiller à son examen par toutes les parties prenantes concernées.

La cybergouvernance devrait faire partie intégrante de la stratégie de l'entreprise.

Pour maîtriser au mieux votre programme de mise en conformité dans le domaine de la cybersécurité et du respect de la vie privée, vous devez vous familiariser (inutile d'être expert) avec la nomenclature adoptée par un grand nombre de professionnels concernant les « technologies les plus récentes », à savoir :

- Chiffrement
- IAM (*« Identity and Access Management »* ou gestion des identités et des accès)
- Anonymisation
- Masquage des données
- Indicateurs basés sur les risques et tableaux de bord

Si cette terminologie vous est inconnue, demandez au responsable de la sécurité des systèmes d'information de vous expliquer leur importance en matière de

risques réglementaires et opérationnels.

D'autre part, en tant que dirigeant, vous devez être conscient des risques liés aux points suivants :

- Décentralisation des données, et plus particulièrement lors de leur utilisation dans le Cloud *(lire à ce sujet le chapitre 8, « Le Cloud, vous y êtes déjà »)*
- Données non structurées et non gérées dans des environnements sécurisés et protégés à l'aide de contrôles adaptés
- Accès et transfert global des données à vos systèmes par votre personnel, vos clients et les parties prenantes

Qui doit gérer les risques ?

Dans un grand nombre d'organisations, les capacités d'analyse des menaces sont éclatées entre plusieurs fonctions, sites physiques et systèmes.

Pour remédier à cela, vous devez disposer d'une fonction d'analyse des menaces, puissante et centralisée, et d'une possibilité de réponse efficace et coordonnée, là encore de façon centralisée.

D'après notre expérience, les fonctions de cybersécurité et de gouvernance des données des entreprises doivent inclure une combinaison de ces trois groupes et être organisées pour mener à bien ces tâches et responsabilités.

Voici les principaux membres de l'équipe de direction qui devront être impliqués au sein de l'organisation :

- Directeur de la sécurité informatique (CISO)
- Président Directeur Général
- Responsable de la gestion des risques (CRO)
- Responsable de la sécurité
- Directeur du respect de la vie privée (CPO)
- Directeur des données (CDO)
- Directeurs métiers et fonctionnels, par exemple planification de la continuité de l'activité, service juridique, risques et réglementation.

Leurs principales responsabilités :

- Collabore avec les membres de la direction pour définir une stratégie de lutte contre les cyber-risques.
- Classe et hiérarchise les ressources stratégiques.
- Définit le budget alloué à la lutte contre les cyber-risques.
- Surveille le positionnement de l'organisation en termes de cyber-risques et en réfère à la direction et au Conseil d'administration.
- Examine les rapports établis par les équipes opérationnelles et de suivi des cyber-risques, et aide à hiérarchiser les cyber-menaces émergentes.
- Révise la stratégie afin d'adapter le programme en fonction de l'évolution des cyber-risques.

L'équipe de Direction devra ensuite s'appuyer sur plusieurs équipes (ou des groupes d'équipes) aux rôles et responsabilités clairement définis :

Equipe : supervision des cyber-risques

Membres : les équipes en charge des technologies de l'information, du support, de la mise en conformité/gouvernance des données, et les équipes de travail.

Responsabilités :

- Évalue les risques actifs rencontrés par l'organisation, leurs auteurs et les ressources menacées.
- Évalue l'efficacité de l'équipe opérationnelle.
- Identifie les nouvelles menaces et amé liore la protection des ressources d'informations.
- Identifie en quoi l'évolution du marché

modifie le cyberpérimètre (par exemple, offres de nouveaux services, fournisseurs, vendeurs ou partenaires commerciaux).
- Surveille le contrôle des changements, et garantit le respect de la vie privée et la sécurité dès la conception en cas de changements des systèmes stratégiques et des principales activités de traitement des données.
- Supervise les programmes de formation des employés.
- Examine les nouvelles obligations réglementaires et de mise en conformité.

Équipe : gestion des cyber-risques
Membres : responsables et experts en matière de réseaux, de sécurité de l'information, de fraude et de sécurité d'entreprise, le centre de gestion de la sécurité (SOC)
Responsabilités :
- Premier dispositif de défense chargé de détecter les cyberévénements et d'y répondre.
- Collecte des informations en temps réel auprès de tous les groupes surveillant les cybermenaces.
- Génère des rapports pour le suivi et la gouvernance des cyber-risques, en précisant notamment le nombre, le type et la durée des cyberattaques.
- Gère un cadre *DevOps* mature garantissant la qualité du code et des applications, et proposant des fonctionnalités d'analyse et de suivi des cybermenaces.

En adoptant une telle structure, vous pourrez bénéficier au mieux des technologies les plus récentes en matière de cybersécurité.

Pour cela, vous devrez également vous renseigner auprès des techniciens sur toutes les possibilités existantes, qu'elles soient nouvelles, en cours de maturation ou de développement.

Le programme de lutte contre les cyber-risques et les risques relatifs aux données doit permettre d'identifier les ressources métiers les plus stratégiques et de connaître à tout moment leur emplacement ainsi que les personnes autorisées à y accéder. Ces ressources regroupent les informations et processus qui, s'ils étaient subtilisés, endommagés ou utilisés à des fins malveillantes, pourraient causer d'importantes difficultés à votre entreprise et altérer la réputation de sa direction en termes de prudence et de fiabilité.

Il s'agit, par exemple, des secrets commerciaux, des stratégies de marché, des algorithmes de négociation, des méthodes de conception de produits, des nouveaux plans marketing, les données relatives au marché ou aux clients ou bien d'autres processus métiers vitaux.

Identifiez clairement les personnes en charge des jeux de données

Ces ressources stratégiques sont importantes à bien des niveaux. Elles sont de la responsabilité des dirigeants, à l'instar du directeur financier vis-à-vis du résultat financier de l'entreprise (et il est donc vital d'identifier clairement les personnes responsables de chacune des ressources stratégiques).

Votre équipe de gouvernance, qui s'appuie sur un niveau approprié de connaissances, d'expertise et d'implication à tous les niveaux de l'organisation, a en charge de répondre aux cyberévénements. Pour cela, elle doit anticiper ces événements pour éviter toute catastrophe.

L'équipe doit pour cela parfaitement maîtriser les risques, les outils disponibles et les possibilités existantes pour

réagir avant qu'un cyberévénement ne se produise. Le développement de réponses préparées et testées (programme) est nécessaire à la planification et à la préparation efficaces des réponses à donner aux cyberévénements.

Exploitez les renseignements collectés tout au long du processus de développement de ces programmes. Chaque programme indique la personne qui doit intervenir, ses responsabilités et ce qu'elle doit faire exactement.

L'utilisation des technologies les plus récentes implique également de repasser régulièrement en revue chaque programme en fonction de la classification et de la hiérarchisation des risques, pour bénéficier en permanence de techniques de collecte de cyber-renseignements, de cyber-technologies et d'options d'assurance actualisées *(Lire à ce sujet le chapitre 10, « L'avenir de la cyberassurance »).*

En cas de doute, posez des questions !

Les cybermenaces et les obligations réglementaires demeurent fluides et dynamiques. En cas de doute, demandez conseil à un expert et pensez à évaluer les technologies les plus récentes pour développer une feuille de route adaptée et vérifier ainsi que vous disposez d'un niveau de résilience le plus élevé qui soit. ■

4

Qu'est-ce que l' « état de l'art » en matière de cybersécurité, et pourquoi doit-on s'y intéresser ?

Par Greg Day

Greg Day est Vice-Président et CSO EMEA chez Palo Alto Networks, responsable de la stratégie de cybersécurité et du développement de la Threat Intelligence.

C'est incontestable, nous dépendons de plus en plus de la technologie *(lire le chapitre précédent au sujet de notre dépendance à la technologie).*

Face à ce constat, l'Union européenne a revu sa législation afin d'introduire la notion « d'état de l'art» dans l'article intitulé **« Protection des données dès la conception et protection des données par défaut »** du Règlement général sur la protection des données.

Cette expression apparaît également dans la Directive sur la sécurité des réseaux et de l'information, relative à la cybersécurité des services de confiance et aux fournisseurs de services de confiance *(dite directive NIS).* Aussi simple soit-elle, cette expression aura pourtant des conséquences majeures sur votre activité à venir. Il est donc judicieux de voir dès maintenant ce qu'elle implique pour vous comme pour d'autres acteurs (les auditeurs, les clients et les partenaires, par exemple).

À première vue, le sens de cette expression peut sembler évident ou confus, selon le secteur d'activité dans lequel vous évoluez. Les acteurs du secteur financier, par exemple, sont habitués à des exigences beaucoup plus prescriptives émanant de leurs propres autorités de régulation. A l'inverse, d'autres pourront y voir ce qu'eux-mêmes, en tant d'équipe de sécurité, font au quotidien : à savoir surveiller les risques en permanence et s'adapter aux cybermenaces afin de gérer ces risques. C'est surtout cette dernière vision qui nous pousse à nous interroger sur la signification précise de l'expression « état de l'art ».

Adapter la réponse de la cybersécurité aux menaces du moment

Cela peut sembler anodin. Pourtant, nous devons nous y intéresser afin d'évaluer la réponse apportée par notre équipe de cybersécurité, pour plusieurs raisons : en l'absence de capacités de cybersécurité bien adaptées aux menaces émergentes, votre entreprise s'expose inutilement à des risques qui peuvent non seulement se révéler plus coûteux à gérer par la suite, mais peuvent également avoir de lourdes conséquences sur votre activité.

Désormais, notre univers est centré autour de la technologie, et les changements en la matière se font à un rythme effréné. C'est pourquoi la cybersécurité doit continuer à s'adapter au même rythme, qu'il s'agisse des menaces émergentes ou de l'évolution des pratiques métier.

Cela fait 30 ans que je travaille dans le secteur de la cybersécurité et depuis tout ce temps, ce secteur a affiché un rythme d'évolution soutenu. Chaque année, nous devons résoudre de nouveaux problèmes et tenter en parallèle de consolider les capacités existantes. Cela suscite un défi majeur : pendant que nous évoluons, nous ne prenons pas le temps d'envisager les choses sous un angle plus large. Les fondamentaux de la cybersécurité sur lesquels nous nous sommes appuyés il y a déjà quelques années sont-ils toujours d'actualité ? Pendant des siècles, nous avons pensé que la terre était plate, jusqu'à ce que la science prouve le contraire. Notre capacité en matière de cybersécurité est-elle limitée par d'antiques croyances similaires ?

Ne pas hésiter à remettre en cause sa vision de la cybersécurité

Quels sont donc les préceptes à revoir ?

(1) Comme dans tout autre aspect économique, l'information est la clé. Des pans entiers de notre activité prennent le chemin du numérique. La question essentielle est donc de savoir quels sont ceux qui vont vraisemblablement passer au numérique, et parmi eux quels sont ceux qui auront un impact majeur sur notre activité.
Pour apporter une réponse fiable à cette question vous devez non seulement vous appuyer sur des sources commerciales, mais aussi accéder aux connaissances sectorielles et aux groupes de partage pertinents, et tirer parti de vos connaissances organiques.
La nouvelle législation indique de « *tenir compte de l'état de l'art* ». En clair, vous devez être en mesure de démontrer que vous possédez des informations actuelles sur les menaces existantes et des conséquences qu'elles peuvent avoir sur votre activité et sur vos clients. Vous devez donc demander à votre équipe non pas de confirmer le problème, mais plutôt la manière dont elle l'a qualifié, et surtout, sa capacité à le maîtriser, soit en acceptant le risque soit en mettant en place une prévention.

(2) Les cyberattaques sont passées de l'équivalent d'un organisme unicellulaire à une forme de vie complexe. En quoi cela est-il important ? C'est important car la cybersécurité a résolu les problèmes les uns après les autres, le plus souvent

« Les cyberattaques sont passées de l'équivalent d'un organisme unicellulaire à une forme de vie complexe »

« Testez votre cybersécurité en situation réelle en exécutant régulièrement des tests d'intrusion »

sans considérer les risques qui peuvent naître de l'interaction de ces problèmes individuels entre eux. En d'autres termes, pour reprendre l'analogie précédente, nous recherchons des cellules individuelles ; dans le monde moderne, nous nous retrouvons avec beaucoup de résultats d'analyses, qui nécessitent une intervention humaine, lente et coûteuse et génèrent souvent de piètres résultats.
Pour prendre une autre analogie, une maison doit reposer sur des fondations solides. Mais la cybersécurité, elle, n'a jamais eu de telles fondations. Il est donc temps de prendre du recul et de vous interroger sur les fondations qui permettront à votre cybersécurité de fonctionner de manière cohérente et efficace, à court comme à long terme. Rappelez-vous que la technologie est là pour automatiser les processus humains, et pas l'inverse !

(3) Dans le monde physique, lorsque l'on manque de coordination entre les parties prenantes, chacun creuse un trou dans son coin et dans un but différent. Dans le monde de la cybersécurité, c'est pareil. Plusieurs technologies répètent des processus clés (comme le décodage du trafic réseau) afin d'effectuer leur part d'analyse de la sécurité. Cela est inefficace et dans un monde toujours plus numérique, l'inefficacité technique devient vite inexcusable.
Il faut donc couper les branches mortes. Lorsqu'un processus fonctionne depuis des années, il est difficile de le remettre en cause. Mais lorsque son efficacité commence à décroître, c'est alors nécessaire. Engagez votre équipe de sécurité dans une réflexion visant à identifier et à se débarrasser des processus, des projets et des pratiques qui n'ont plus lieu d'être parce que leur efficacité n'est plus au même niveau que lors de leur mise en œuvre.

(4) Intéressez-vous à la manière dont la technologie est réellement utilisée plutôt qu'à savoir comment elle devrait l'être en théorie. La technologie, tout comme la cybersécurité d'ailleurs, doit faciliter l'activité en s'adaptant aux usages réels, et non l'inhiber en imposant une utilisation spécifique à laquelle il faudrait se plier.

(5) Nous devons tenter d'identifier les méthodes employées par les cybercriminels avant que nous ne soyons touchés. Les cybercriminels ont besoin de temps pour s'attaquer à des systèmes publics ou intercepter des flux monétaires. Ce paramètre devrait être pris en compte lorsque nous tentons d'identifier le mode d'action complexe des attaquants. Hélas cela est difficile avec les solutions de cybersécurité actuelles, qui répondent généralement au coup par coup sans une vision globale de l'action de l'adversaire. Il nous faut trouver une solution plus systématique.

La législation européenne : une opportunité

La nouvelle législation européenne nous donne une occasion unique de prendre du recul afin d'échapper à la spirale du quotidien et d'évaluer ce qu'il « convient » de faire avec la cybersécurité. Une cybersécurité tenant compte de l'état de l'art est une exigence dynamique qui nécessite de revoir régulièrement ce qui est de

l'ordre du possible, à travers le prisme des risques réels et pertinents. Mélanger des capacités modernes et héritées revient à prendre le départ d'une course avec un handicap : la cybersécurité devra s'adapter aux éléments hérités et ne pourra donner toute la mesure de son efficacité.

Si j'ai un conseil à vous donner à mesure que nous nous ancrons dans l'ère de la technologie de pointe, ce serait d'avoir une idée claire de ce à quoi doit ressembler la réussite dans votre domaine *(par du benchmarking, par exemple),* et de ce que l'état de l'art doit vous apporter pour y parvenir.

Testez ensuite votre cybersécurité en condition réelle en exécutant des tests d'intrusion qui simulent une attaque ciblée, portant notamment sur différentes fonctions de l'entreprise afin de déterminer comment votre défense s'en sort face à un attaquant minutieux. Rappelez-vous que tenir compte de l'état de l'art est une tâche dynamique. Cela exige une attention régulière afin de rester conforme à la fois aux exigences réglementaires et aux meilleures pratiques. Pour finir, discutez avec d'autres acteurs du secteur afin d'obtenir un point de comparaison et profiter ainsi de la sagesse collective de vos pairs ! ■

Les bonnes questions à poser à l'équipe

1. **Quelle est la fréquence de nos tests d'intrusion ?**
   Il n'y a pas de bonne réponse ici, car cela est fortement dépendant de votre organisation et du périmètre concerné. Mais il y a une mauvaise réponse : « jamais » ! Considérez qu'une fois par an est un strict minimum.

2. **Quand a été revue notre politique de sécurité (PSSI) ?**
   Là aussi, il y a surtout une mauvaise réponse : « jamais » ! Pour le reste, la PSSI doit être revue régulièrement, ainsi que ses annexes (chartes informatiques, etc.)

3. **Quel dispositif a-t-on mis en place afin de s'assurer d'être toujours informé des dernières menaces ?**
   Un dispositif de veille technologique et réglementaire dédié à la cybersécurité est indispensable. C'est notamment lui qui dictera en partie la réponse aux questions précédentes : des tests d'intrusion supplémentaires peuvent s'avérer nécessaires quand le périmètre s'agrandit ou quand de nouvelles menaces sont identifiées, et une révision de la PSSI ou de ses annexes peut s'imposer pour prendre en compte ces dernières, ainsi que de nouveaux usages.

III Tendances

5

La cybersécurité, ingrédient majeur de la transformation numérique.

Par Olivier Ligneul

Olivier Ligneul est Responsable de la Sécurité des Systèmes d'Information du Groupe EDF, impliqué dans le projet de transformation numérique du groupe. Il livre ici sa vision de la transformation numérique au sein d'un groupe industriel et du rôle central que doit jouer la cybersécurité.

La transformation numérique est désormais passée d'un effet de mode à une nécessité impérieuse pour les entreprises. En effet, la concurrence s'est accrue au niveau mondial. Rapides et agiles, les modèles économiques émergents s'appuient désormais sur des concepts tels que la désintermédiation *(réduction du nombre d'intermédiaires),* la coproduction et l'entreprise étendue.

Ainsi, afin de gagner en flexibilité et en vitesse, il est nécessaire de travailler en filière et de partager la création de la valeur ajoutée. Cette nouvelle ère se caractérise par l'utilisation de multiples canaux de communication et le stockage d'importants volumes de données. Le *cloud computing, le big data* et les solutions de collaboration deviennent ainsi les vecteurs essentiels de ces nouveaux processus de production.

Plus récemment, l'internet des objets a engendré une autre révolution, qui promet de relier l'humain et le monde qui l'entoure à l'espace digital. Une fois traitées dans le monde numérique, ces données permettent de générer une plus-value dans le capital de l'entreprise, améliorent sa compétitivité et orientent ses choix stratégiques. Mais cette révolution se fait au prix de la collecte d'un gigantesque volume d'information (les méga-données) relatives aux personnes, aux processus de l'entreprise et à ses organes de production et de distribution.

On le devine ainsi clairement : les choix technologiques qui soutiennent ces promesses de flexibilité et de compétitivité sont donc naturellement porteurs, aussi, de risque numérique, y compris pour les grandes

« Les données générées par l'Internet des Objets améliorent la compétitivité et orientent les choix stratégiques »

entreprises censées y être mieux préparées.

Pour autant, ce risque numérique n'est pas le plus important. Un risque accru réside dans le fait que la transformation numérique est inéluctable mais que l'entreprise peut ne pas être prête à l'assumer. Ce déni aboutirait alors potentiellement sur un débordement par des acteurs plus agiles, de plus petite taille, qui pratiqueraient l'intermédiation. Dans ce cas de figure, la transformation numérique constitue donc l'assurance de la survie pour l'entreprise.

Bien qu'elle semble ainsi inéluctable il ne s'agit évidemment pas d'aborder la transformation numérique sans y être préparé. Puisqu'elle s'appuie sur des volumes de données très importants , elle se traduit par une exposition beaucoup plus forte du capital informationnel et des processus immatériels, notamment à cause de leur volatilité.

Il est donc nécessaire d'intégrer au plus tôt la problématique cybersécurité dans la stratégie et la gouvernance de l'entreprise.

Au sein du groupe EDF, cette dynamique s'est matérialisée dans le cadre d'une stratégie baptisée Cap 2030[1] qui porte l'ambition du groupe impulsée par son Président Directeur General Jean-Bernard Lévy.

Les contraintes propres à un groupe industriel tel EDF sont fortes : il est nécessaire, entre autres, que cette transformation numérique ne mette pas en difficulté les organes de production ou de distribution. Elle doit donc être mise en œuvre en veillant à ne jamais impacter les conditions de sûreté et doit bénéficier des moyens de sécurité du système d'information afin de garantir son accomplissement et sa pérennité.

Et tout ceci avant même de parler d'« entreprise étendue »…

L'entreprise étendue

« L'entreprise étendue » est le terme employé pour designer un groupe d'entreprises qui s'associent et collaborent à travers des outils et des processus communs. Très utilisée dans l'aéronautique, principalement à des fins d'amélioration de la collaboration et des chaînes logistiques, cette dynamique s'étend sur différents processus, dont ceux de l'ingénierie, à tous les acteurs du monde industriel.

Le domaine de l'énergie n'échappe pas à ce mouvement. Ce décloisonnement des relations entre les acteurs économiques d'une même filière est vertueux car il apporte de la fluidité, de l'efficacité dans la réalisation des travaux et une plus grande rapidité.

Cependant, connecter les différents systèmes d'information d'organisations ayant leur propre historique et une architecture particulière à chacune d'entre elles pose la problématique de la maîtrise des processus et des informations qui y circulent, notamment dans une perspective de sécurité globale.

La solution passe ici par la définition de cercles de confiance associés à chaque niveau de sensibilité. Ceux-ci doivent être identifiés et communément admis très en amont au même titre que le niveau de confidentialité et de criticité des différents processus.

Cette vision commune des risques doit en outre être maîtrisée par les dirigeants

[1] https://www.edf.fr/groupe-edf/premier-electricien-mondial/strategie-cap-2030

car tout ne pouvant être protégé, il est nécessaire de faire des choix informés et consentir des efforts portés par des mesures de sécurité adéquates au regard de ces exigences. C'est d'ailleurs là tout le principe d'une homologation de sécurité telle que décrite dans la loi de programmation militaire qui s'applique aux opérateurs d'importance vitale (OIV).

Une forte maturité nécessaire au sein de l'entreprise

En matière de protection des systèmes d'information, il convient désormais de ne plus opposer les experts de la sécurité aux responsables opérationnels des entreprises, car la transformation numérique a fait voler en éclats cette frontière.

Mais cela exige une bonne coordination et une bonne communication entre tous les acteurs, non seulement au sein de l'entreprise elle-même mais aussi avec ses partenaires dans le cadre de l'entreprise étendue.

Il devient donc impératif de chercher à mettre en œuvre des modes de communication efficaces, notamment à « haut niveau » entre les responsables des métiers, le RSSI et les dirigeants de l'entreprise. Cela exige, évidemment, une forte maturité de la part de l'organisation.

Fluidité, agilité et rapidité

Ainsi qu'évoqué précédemment, la rapidité est devenue autant un avantage concurrentiel qu'une contrainte de survie de l'entreprise. Cela s'est traduit dans les systèmes d'information par un recours grandissant aux méthodes agiles et à l'approche « DevOps » *(rapprochement des fonctions de développement et d'exploitation dans un mode d'intégration continue).*

Dans cette recherche d'agilité il est pourtant difficile de délivrer de nouvelles applications sécurisées à la volée, en fonction des besoins immédiats des différents métiers. Car la sécurité nécessite du temps, à la fois pour s'approprier le projet mais aussi pour prendre le recul nécessaire à l'élaboration des scenarii d'attaques pertinents.

Face à ce constat l'entreprise pourrait être tentée de ne pas faire appel à ces nouvelles méthodes pour des raisons de sécurité. Cela serait pourtant suicidaire, car elle serait alors condamnée à « mourir en bonne santé » !

La solution à ce dilemme est en réalité de faire évoluer la sécurité des systèmes d'information vers une fonction métier et non une fonction support. Celle-ci doit être prise en compte dès la genèse du projet, lors de l'expression de la demande ou du besoin. Cette activité n'étant plus anecdotique - dans le cadre de la transformation numérique un système d'information non sécurisé pourrait également être létal - il convient alors d'associer formellement le RSSI à la direction générale et à la gouvernance des projets, afin qu'il puisse y jouer pleinement son rôle de conseil et d'influence, et ainsi contribuer au succès attendu.

Plus de données, plus de sécurité

Nous l'avons vu, une transformation numérique réalisée dans de bonnes conditions génère une masse considérable d'informations. Celle-ci a de la valeur et doit donc faire l'objet d'une protection accrue, car

« La transformation numérique est inéluctable et constitue une assurance de la survie pour l'entreprise. Elle doit se préparer à l'aborder. »

« Le dirigeant doit connaître, sans jargon ni opacité, quels sont les moyens qu'il a à sa disposition en matière de supervision »

l'impact d'un vol d'informations sera d'autant plus fort que l'entreprise est avancée dans son processus de transformation numérique. Ainsi celle-ci s'accompagne-t-elle nécessairement d'un effort accru sur la protection de la propriété intellectuelle.

Mais comment y parvenir ? Partant du principe que l'on ne peut bien protéger que ce que l'on connaît, la première étape sera d'appréhender les données et les processus générés par la transformation numérique dans une dynamique stratégique pour l'entreprise, en particulier autour d'un programme de gouvernance des données. Celui-ci intègre notamment, sous leur forme quasi-régalienne, les politiques en matière de cybersécurité et de protection des données personnelles *(se référer au chapitre 2 pour en apprendre davantage au sujet des obligations et des stratégies liées au traitement des données à caractère personnel).*

Le dirigeant doit être à la manœuvre

L'attaquant a désormais pleinement conscience de l'Eldorado que constituent les données dont regorgent les entreprises, et il cible sans relâche ces dernières.

Celles-ci doivent alors en retour bâtir un chaînage de survie qui leur permettra de réaliser leur transformation numérique dans de bonnes conditions en dépit d'une menace omniprésente. Un socle générique de sécurité doit donc être organisé pour répondre à ces agressions potentielles. Celui-ci s'appuie sur des outils, des experts, une capacité opérationnelle démontrée et une coordination sans faille entre tous les acteurs de l'entreprise. Le dirigeant doit donc impérativement connaître, sans jargon ni opacité, quels sont les moyens à sa disposition en matière de supervision (Security Operations Center , SOC), de défense, d'investigation, de gestion de crise et de sensibilisation *(à commencer par sa propre sensibilisation, voir chapitre 11).*

C'est également à lui d'arbitrer et valider au niveau du CODIR les orientations stratégiques en cybersécurité à moyen et long terme, au regard des synthèses des incidents de sécurité majeurs dont son organisation a dû se défendre. Ainsi, la tête de l'entreprise pourra trouver le juste milieu entre l'indispensable injection de cybersécurité et la nécessité d'innover et de se transformer dans le monde numérique, sans mettre pour autant en danger cette dernière par un excès de prudence. Le dirigeant jouera alors ici pleinement son rôle de pilote.

Stabilisation de la protection et sécurisation des effets de la transformation numérique

Ayant constaté l'avènement de la transformation numérique, les DSI ont su adapter leurs méthodes et leurs systèmes d'information. De même la sécurité du SI doit désormais faire l'objet d'une industrialisation, ne serait-ce que pour en maîtriser et contenir les coûts.

Cette intégration dans l' « usine informatique » aura également comme effet vertueux d'être en mesure d'apporter de la valeur à tous les projets issus de la transformation numérique, en limitant au maximum le sur-mesure «par projet».

Cette accélération qui s'impose aux organisations entraîne un cycle d'émergence de nouvelles technologies et de ruptures beaucoup plus court qu'auparavant.

Cela oblige la sécurité à s'approprier ces nouveaux concepts plus en amont.

C'est le cas, par exemple, des blockchains, qui apportent de la fluidité dans les transactions financières et les échanges numériques, grâce à des techniques basées sur la cryptographie, mais qui influencent également les futurs usages des métiers (digitalisation sans intermédiaire des transactions financières, de biens et de services). Sans sécurité, l'émergence de cette technologie et son utilisation par et au sein de l'entreprise sera freinée au profit des plus agiles et des plus rapides.

Au confluent de tous ces nouveaux modes de fonctionnement des entreprises, le RSSI est en première ligne pour intégrer les nouveaux codes de la fonction Sécurité du Système d'Information. Pluridisciplinaire, communicant et adaptable, il est le mieux placé pour se mettre au service des métiers et du dirigeant afin de compléter les éclairages qui leur étaient traditionnellement fournis.

Il est l'homme-clé pour faire adopter par l'entreprise, sous l'impulsion décisive de son dirigeant, un socle de cybersécurité fort, capable d'assurer le processus de transformation numérique, lui-même essentiel à la survie de l'organisation.

Car en matière de sécurité du système d'information, l'entreprise doit faire face aux mêmes règles que celles qui régissent sa survie : elle doit évoluer ou disparaître. ■

« La transformation numérique fait voler en éclats la frontière entre experts de la sécurité et responsables opérationnels »

Les bonnes questions à poser à l'équipe

1. **La Sécurité des Systèmes d'Information (SSI) est-elle partie prenante de notre effort de transformation numérique ?**
   Il est possible, surtout en phase de démarrage, que seuls le marketing et la DSI soient associés au projet de transformation numérique. Mais la SSI doit impérativement l'être également.
2. **La communication entre la SSI et les métiers est-elle efficace et sans obstacles ?**
   Vue des métiers, la SSI peut être perçue comme un frein aux projets en mal d'agilité, tandis que celle-ci peut considérer les métiers comme étant trop friands de risque. Il est impératif pourtant que les deux parviennent à travailler de concert, et donc à communiquer efficacement.
3. **Toutes les initiatives numériques font-elle l'objet d'une validation, même rapide, par la SSI ?**
   Il est courant que de nombreux projets annexes échappent entièrement à la SSI car ils n'apparaissent pas sur son radar. Il est important qu'existent des procédures capables d'alerter la SSI dès le démarrage d'un projet impliquant le numérique.

6

Définir le profil du RSSI 3.0

Par Ahmad Hassan

Ahmad Hassan est Partner au sein de la Practice Technologies et Services du Cabinet parisien Heidrick & Struggles. Il se consacre au recrutement des dirigeants et au conseil en leadership dans le domaine des technologies de l'information.

Avec l'accélération de la transformation numérique menée par un grand nombre d'entreprises *(lire à ce sujet le chapitre 5 consacré à la transformation numérique)*, nous avons tous constaté la prolifération du terme « CxO », qui signifie que certains rôles sont soit très proches, soit font partie intégrante du Comité de Direction. L'on peut rencontrer ainsi le Chief Information Officer (DSI), le Chief Technology Officer, le Chief Digital Officer, le Chief Data Officer et maintenant le CISO (le Chief Information Security Officer), que nous avons nommé en français le RSSI !

Les vraies questions que nous devons soulever sont de savoir si tous ces CxO de connotation technique ont la place dans un Comité de Direction, comment définir leurs mandats et surtout comment les sélectionner !

Quelles sont donc les compétences, expériences, expertises et comportements indispensables pour mieux protéger l'entreprise contre les cyberattaques ?

Avant d'essayer de décrire le « portrait-robot » du RSSI idéal, il est intéressant de porter un regard rapide sur l'évolution de la fonction et des compétences exigées pour l'exercer au mieux.

La prévention

Le rôle principal du RSSI est la protection du Système Informatique de son entreprise. Historiquement, les compétences requises sont surtout d'ordre technique. Comment utiliser les outils, les équipements et les logiciels pour empêcher la pénétration des malfaiteurs au cœur du système informatique, ou comment envisager la protection de la citadelle ? Mais a peine a-t-on prononcé le mot « citadelle » que déjà le monde a changé ! Les clients et les collaborateurs sont devenus mobiles et très exigeants : une entreprise B2C qui ne fournirait pas à ses clients un service

« *anytime, anywhere, any device* » ou ne prendrait pas en compte le phénomène BYOD (Bring Your Own Device) pour ses collaborateurs aurait un handicap compétitif.

Mais l'augmentation de ces points d'accès au réseau d'entreprise favorise naturellement et de façon conséquente le risque d'infractions, car le mur de la citadelle doit être ouvert en de nombreux endroits pour accommoder les clients et les utilisateurs mobiles.

Ainsi, de nos jours, un RSSI qui préconiserait la construction d'un mur de protection autour de son entreprise comme seule solution ne lui rendrait pas un grand service !

L'évaluation du risque

Si la solution d'un mur électronique impénétrable autour de la société n'est plus adaptée, c'est que le rôle du RSSI doit évoluer avec les besoins. Il doit désormais se tourner aussi vers l'évaluation et la gestion des risques.

A ce stade, toute la difficulté est de trouver le juste milieu entre une nécessaire ouverture vers le monde extérieur et un contrôle efficace des risques ; le rôle d'un RSSI commence alors à devenir varié...

Cette nouvelle exigence a fait beaucoup évoluer le rôle du RSSI. Il a dû acquérir un véritable sens de l'écoute, la capacité de comprendre les besoins et les contraintes des métiers, de dialoguer avec les Dirigeants, tout en étant capable d'intégrer une somme importante d'éléments dans le cadre de son évaluation des risques.

La gestion des crises

Il est acquis que beaucoup d'attaques contre le système d'information passent inaperçues, et parfois même pendant plusieurs centaines de jours. Et cela quelle que soit la taille ou les ressources mises en œuvre par les entreprises visées : même des géants tels Gemalto, LinkedIn,TV5, ou Ebay ont été victimes ! Le rôle du RSSI doit alors à nouveau évoluer vers la gestion des crises, afin d'être en mesure de mieux accompagner son entreprise si celle-ci dit être victime d'une attaque. Cela exige encore de sa part de nouvelles compétences : du sang-froid, une grande capacité d'écoute, d'analyse et de communication, la prise de décisions rapides et la capacité à coordonner l'action. Cela passe, entre autres, par une excellente maîtrise de la communication à la fois interne (pour écouter et donner des directions très claires) et externe, pour donner les informations qui permettront au service de la communication de rassurer les actionnaires, marchés, partenaires et clients.

Ainsi, après toutes ces mutations, le RSSI nouvelle génération est désormais un cadre aux compétences très diverses dont les « soft skills » sont au moins aussi développés que l'expertise technique.

Les bonnes questions à poser à l'équipe

1. **Qui a établi la fiche de poste de notre RSSI, et quand ?**
   Il est important d'avoir une vision claire de ce que l'organisation attend de son RSSI, et de faire évoluer cette dernière dans le temps.
2. **La dimension des soft skills a-t-elle été prise en compte dans ce recrutement ?**
   L'importance croissante des compétences de communication et d'écoute du RSSI exige que ces dernières soient prises en compte lors du recrutement.
3. **Notre RSSI a-t-il été formé à la gestion de crise ?**
   Si le domaine de la gestion de crise ne relève pas toujours directement des attributions du RSSI, celui-ci doit évidemment faire partie de la cellule de crise, voire, selon les organisations, être en mesure d'organiser lui-même la gestion de crise. Il devra alors être formé en conséquence.

Mais il reste encore à lui trouver un positionnement efficace dans l'organisation.

Le Positionnement du RSSI

Si l'intégration du RSSI au Comité de Direction n'est plus le vrai sujet, il est évident que le RSSI 3.0 doit être en mesure d'interagir efficacement avec le Comité de Direction et le Conseil de Surveillance. Ainsi certaines sociétés anglo-saxonnes autorisent-elles désormais leur RSSI à interrompre des processus critiques de l'entreprise, en acceptant l'impact financier et/ou juridique que cela peut impliquer.

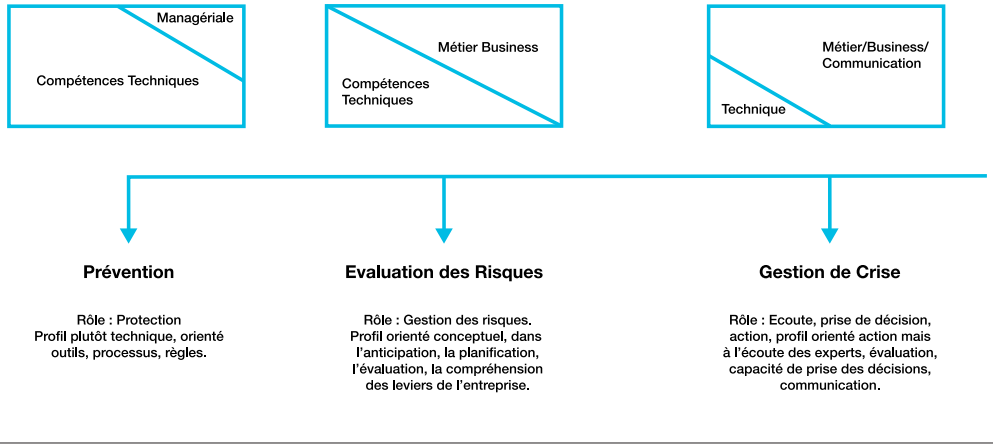
Le positionnement du RSSI pourra également dépendre de l'industrie dans laquelle opère son organisation. Dans une banque ou une institution financière, où les risques financiers et juridiques sont très élevés, il pourra avoir un accès facilité aux organes de décision.

De la même manière les sociétés du domaine de l'énergie, du transport ou des télécoms, qui utilisent des systèmes informatiques pour la signalisation de réseau, sont particulièrement sensibles au risque cyber car une interruption d'un processus clé peut entraîner l'arrêt complet de leurs opérations. Là aussi, le RSSI pourra conseiller plus directement le Comité de Direction.

Dans le monde de la distribution, avec la montée en puissance du e-commerce, les risques sont davantage localisés au niveau de l'information client et du système logistique, et le RSSI sera alors positionné en conséquence.

Dans tous les cas, pour un Comité de Direction ou même un Conseil de Surveillance, prendre la décision d'arrêter les opérations de leur entreprise sur les conseils de leur RSSI est la preuve d'une confiance absolue dans le jugement de ce dernier. Afin de gagner cette confiance, le RSSI doit non seulement bien entendu être crédible aux yeux des organes de direction (par son expérience, son cursus, ses réussites passées) mais il doit être également lui aussi à l'écoute de ses dirigeants, et parfaitement informé des différentes activités de l'entreprise, de ses stratégies en cours , tout en ayant une compréhension profonde du cœur de métier.

FIGURE 1



Les qualités cardinales du RSSI 3.0 sont ainsi avant tout une grande capacité de communication en interne comme en externe, la maîtrise d'un discours très clair et argumenté et une crédibilité à tous les niveaux de l'entreprise – des métiers jusqu'aux dirigeants. ■

7

La prévention peut-elle être efficace ?

Mark McLaughlin

Mark McLaughlin est Chairman et CEO de Palo Alto Networks. Avocat, il a été nommé Chairman of the National Security Telecommunications Advisory Committee par le Président Obama.

La presse se fait régulièrement l'écho du piratage massif d'une grande entreprise, d'une administration publique ou d'une organisation. Elle pose alors la question du pourquoi de ces attaques et s'il est possible d'y mettre fin.

Si la cybersécurité s'invite aussi souvent dans les médias, et si elle attire autant d'intérêt et d'investissements dans le monde entier, c'est en raison de la prise de conscience croissante que ces violations mettent en danger notre style de vie numérique. Et ce n'est pas une exagération. Nous évoluons dans un monde de plus en plus numérique dans lequel ce qui était réel et tangible est maintenant généré par des machines, voire n'existe que sous forme de bits et d'octets.

Prenez l'exemple de votre compte en banque : il se caractérise par l'absence totale d'argent ou de monnaie légale sous forme tangible. Vous espérez que vos actifs existent car ils sont « visibles » lorsque vous vous connectez à votre compte sur le site Web de votre établissement bancaire. De même que vous espérez bénéficier des services de distribution d'eau, d'électricité ou autres sur simple commande, bien que vous n'ayez qu'une vague (voire aucune) idée de la manière dont la commande aboutit au résultat. N'est-il pas réconfortant, aussi, d'admettre que les centaines de milliers d'avions qui traversent le globe chaque jour circulent aux distances de sécurité requises et décollent et atterrissent selon les intervalles appropriés ?

Dans cette ère numérique nous espérons de plus en plus que cela va simplement « marcher ».

Ce recours aux systèmes numériques explique pourquoi les préoccupations au sujet des cyberattaques

augmentent si rapidement. Dirigeants d'entreprise, chefs de gouvernement et chefs militaires sont conscients qu'il existe une infime séparation entre le bon fonctionnement de la société numérique basée sur la confiance et l'effondrement chaotique de la société dû à l'érosion de cette confiance. Et l'érosion peut être rapide. Sait-on l'expliquer ? Existe-t-il des analogies ? Et, surtout, peut-on y remédier ?

La machine par rapport à l'Homme

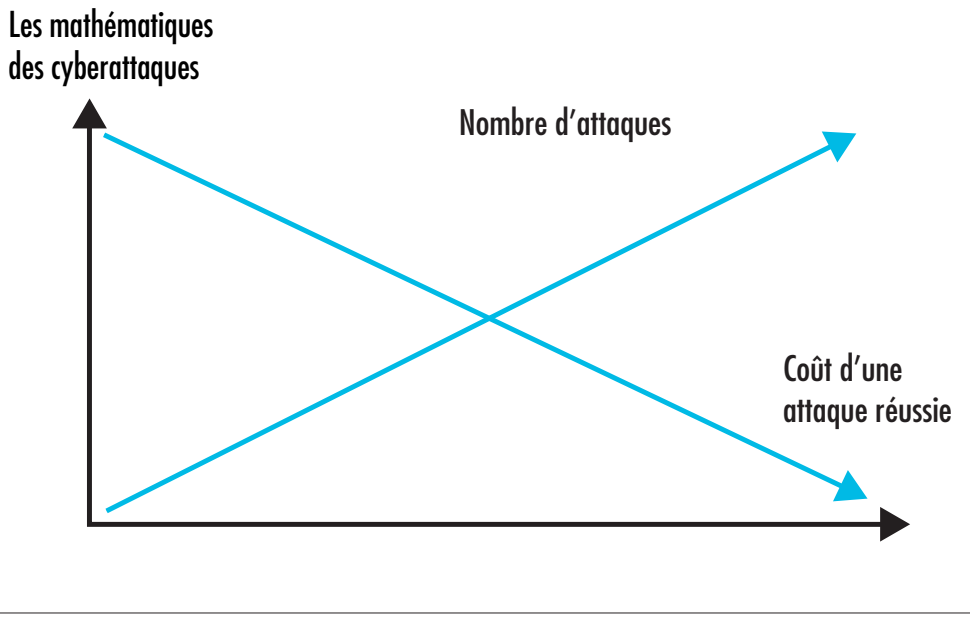
Paradoxalement c'est un problème mathématique qui est au cœur de la bataille de la cybersécurité ! Malheureusement, il est assez simple à comprendre mais difficile à corriger.

Une des conséquences négatives de la baisse constante du coût de la puissance de calcul informatique est la capacité accrue dont bénéficient désormais les cybercriminels pour perpétrer des attaques de plus en plus nombreuses et sophistiquées, à moindre coût.

Aujourd'hui, les pirates qui ne sont pas capables de développer leurs propres outils peuvent utiliser des logiciels malveillants et des failles qu'ils se procurent sur Internet gratuitement ou pour des sommes modiques. De même, des pirates compétents, des organisations criminelles et des États sont eux aussi en mesure d'utiliser ces outils largement disponibles pour réussir des intrusions tout en brouillant leur identité. Bien entendu, ces adversaires sophistiqués développent et utilisent également de manière sélective des outils uniques bien plus perfectionnés, capables de provoquer des dégâts encore

FIGURE 1

La puissance informatique étant plus abordable, le coût du lancement d'attaques automatisées est en baisse. Cela permet l'augmentation du nombre d'attaques pour un coût donné.



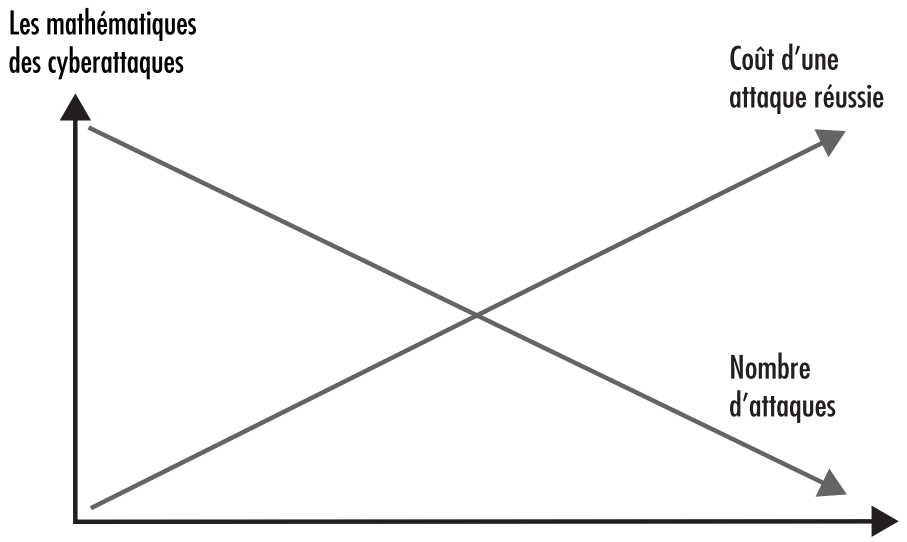
plus graves. Cela vient s'ajouter au pouvoir de nuisance considérable des pirates. *(Voir Figure 1).*

Face à cette offensive grandissante qui voit augmenter à la fois le nombre des attaques et leur niveau de sophistication, le spécialiste a généralement recours à des technologies de protection conçues il y a plusieurs décennies, empilées au gré des menaces et des défenses. Ces produits ne sont cependant pas conçus pour communiquer entre eux. Par conséquent, si des attaques sont détectées ou si des leçons ont été tirées d'une attaque, les réponses sont essentiellement manuelles et doivent être implémentées sur chaque produit. Malheureusement, dans cette course, l'homme ne fait guère le poids face à la machine et les compétences en matière de cyberdéfense se font de plus en plus rares. Si l'on veut avoir un jour l'espoir de ne plus voir d'attaques massives à la Une des journaux, il faudra alors parvenir à retourner la courbe des coûts évoquée précédemment afin d'augmenter sans cesse le coût d'une attaque réussie pour l'attaquant. Ceci afin d'en réduire, en définitive, le nombre. Mais seule l'automatisation des défenses permettra d'y parvenir. *(Voir Figure 2).*

Sans cela il est peu probable que le nombre d'attaques diminue au cours du temps. Au contraire, tout porte à croire que leur nombre ne va cesser de croître. En fait, nous pouvons également nous attendre à ce que la surface d'attaque et les cibles potentielles continuent également leur progression au rythme de l'intensification des éléments connectés à Internet.

FIGURE 2

L'exploitation de l'automatisation et des renseignements intégrés peut augmenter de manière continue le coût d'une attaque réussie, pour finalement en réduire le nombre.



A la lecture de ce qui précède l'on pourrait être tenté de prétendre que la prévention est impossible. Notre rôle se réduirait alors à détecter et à réagir à temps à toutes les intrusions. Le problème de cette approche est que sans prévention significative, personne, ni aucun processus et aucune technologie, n'est en mesure de hiérarchiser et de répondre à chaque intrusion. Ce problème mathématique est tout simplement insurmontable. La détection et la réponse doivent donc, en définitive, s'ajouter au lieu de se substituer à la prévention.

Ainsi, la stratégie doit viser la forte baisse de la probabilité et l'augmentation du coût à payer par un pirate pour *mener à bien* une attaque. Autrement dit, nous ne devons pas supposer que les attaques vont disparaître ni que toutes les attaques peuvent être stoppées. Cependant, nous devons admettre que nous continuerons d'être attaqués et veiller à ce que le coût d'une attaque réussie soit considérablement augmenté, jusqu'à ce que l'incidence d'une attaque réussie diminue fortement.

Après avoir atteint ce point, sachant que cela n'arrivera pas du jour au lendemain, nous serons en mesure de quantifier et de compartimenter le risque par rapport à quelque chose que nous acceptons et comprenons. C'est une fois ce point atteint que les cyber-risques, bien que toujours très réels et persistants, ne feront plus les gros titres des journaux et seront relégués au second plan de notre quotidien, du commerce, ou des communications. Nous devrions poursuivre cet objectif. Ne pas écarter tout risque, mais le réduire à quelque chose que nous pouvons compartimenter. Et il se trouve qu'il existe une analogie historique à ce problème, et même une méthode pour le résoudre !

Analogie avec Spoutnik

Cette analogie, imparfaite mais cependant utile, concerne la conquête spatiale. En 1957, l'Union soviétique a lancé le satellite Spoutnik. L'idée que cette technologie pouvait procurer aux Soviétiques un avantage de taille par rapport aux États-Unis dans la course au nucléaire a soulevé un vent de panique. Tout à coup, le mode de vie occidental était considéré, à raison, comme menacé. Le confort et la confiance de vivre dans un environnement protégé et prospère se sont trouvés ébranlés dès lors que les citoyens n'ont plus cru qu'ils pourraient profiter librement de leur vie quotidienne. C'était comme si une avancée technologique incontrôlable avait eu lieu, et partout régnait l'inquiétude et son cortège de mauvaises nouvelles.

Au cours des années qui ont immédiatement suivi le lancement de Spoutnik, la principale problématique consistait à savoir comment survivre dans le monde de l'après-guerre nucléaire. Les abris anti-nucléaires privés et les denrées non périssables ont connu une forte demande, et dans les écoles, on apprenait à se mettre à couvert. Autrement dit, les gens supposaient qu'il était impossible d'empêcher les attaques et se préparaient à trouver des solutions une fois l'attaque perpétrée.

Fort heureusement, ce point de vue fataliste était temporaire. L'Amérique a eu recours à la diplomatie et aux moyens traditionnels de dissuasion tout en canalisant son innovation technologique et son ingéniosité vers le programme de conquête spatiale, à l'instar du programme Mercury de la NASA. Après une décennie de mobilisation des ressources, de collaboration, d'essais et d'efforts, le programme Mercury et ses accomplissements ont modifié les termes de l'équation. La menace d'une attaque spatiale n'était certes pas

totalement écartée, mais elle était suffisamment « compartimentée » pour être reléguée au second plan en tant qu'événement possible mais non probable. Ce fut à ce moment-là que la panique et la confusion ont disparu des gros titres et des actualités quotidiennes. Nous saurons que nous sommes parés à livrer bataille à la cybercriminalité une fois que nous aurons atteint ce point.

Mais comment y parvenir ?

Comme pour beaucoup de domaines de la vie, commencer par chercher à avoir une vision claire du problème et du but recherché peut s'avérer fort utile lorsque l'on est plongé dans le doute ! Car si vous ne savez pas ce que vous essayez de faire, vous risquez fort de ne pas y parvenir.

Dans l'analogie avec la conquête spatiale, l'approche a évolué au cours du temps : d'abord, on présumait qu'une attaque était imminente et inéluctable et on se consacrait à prévoir les ressources nécessaires pour vivre l'après-attaque. Puis, on est passé à une approche de la prévention, selon laquelle la majorité des ressources et de la planification visait à réduire la probabilité et l'efficacité d'une attaque.

Il est important de souligner que le risque d'attaque n'était pas écarté, mais la probabilité de son occurrence et de son succès était réduite par l'augmentation conséquente du coût d'une attaque réussie. Bien entendu aucune analogie n'est parfaite : la structure de coût d'une attaque spatiale est évidemment très différente de celle d'une cyberattaque ! Les cybermenaces ne sont pas du seul ressort des superpuissances. Dans le domaine cyber l'innovation technologique visant à inverser le coût des attaques couronnées de succès sera vraisemblablement le fruit des efforts consentis par l'industrie et non par les gouvernements. Cependant, le principe de base reste valable : une philosophie privilégiant la prévention a plus de chance d'aboutir au développement, à l'utilisation et à l'amélioration continue de fonctionnalités de prévention.

La prévention est-elle possible ?

C'est évidemment à ce stade la question qui vient immédiatement à l'esprit. Et je pense que tous les professionnels et spécialistes de la sécurité s'accordent pour dire que la prévention totale n'est pas possible.

Le constat est certes décourageant mais il ne diffère finalement pas beaucoup des autres facteurs de risque majeurs que nous devons traiter habituellement. Aussi, la vraie question devient plutôt de savoir si la prévention est possible jusqu'au point où l'incidence des attaques réussies se réduit à quelque chose de gérable en termes de risque.

Et je pense que cela sera possible avec du temps. Mais pour parvenir à ce résultat il est impératif de réduire aussi les coûts de la lutte contre la cybercriminalité. Au sein d'une organisation cette réduction peut être obtenue grâce à l'amélioration et la coordination continues de plusieurs éléments clés : la technologie, les processus et les personnes, et enfin le partage du renseignement.

Technologie

Il est évident que la technologie traditionnelle ou existante en matière de sécurité échoue de façon alarmante. Trois principales raisons expliquent cet échec :

« Les cyberattaques doivent devenir des événements possibles mais non probables »

La première est que les réseaux ont été conçus sur une longue période de temps, d'où leur nature compliquée. Les technologies en matière de sécurité ont été développées et déployées selon une approche cloisonnée, adaptées ponctuellement aux produits qu'elles devaient protéger. En d'autres termes, une solution de sécurité dans une architecture réseau traditionnelle - quelle que soit sa taille - comprend plusieurs produits provenant de fournisseurs différents. Ces produits sont tous conçus pour servir une tâche spécifique, avec des capacités de collaboration et d'ouverture à d'autres produits souvent très limitées. Cela signifie qu'en matière de sécurité l'efficacité du réseau est globalement celle du dispositif ou de la solution la moins intelligente.

De même, si l'on considère que des milliers de menaces quotidiennes sont détectées, la protection est essentiellement manuelle car il est impossible de communiquer automatiquement ces informations à d'autres fonctionnalités du réseau, et encore moins celles de réseaux extérieurs à votre organisation. C'est un vrai problème, étant donné que pour protéger leur réseau les organisations ont de plus en plus recours à la ressource la moins exploitable dont ils disposent, à savoir les hommes, pour lutter contre les attaques générées par des machines.

La disparition du périmètre

Deuxièmement, ces nombreuses solutions ponctuelles s'appuient souvent sur des technologies vieillissantes, à l'instar de l'inspection d'état *(stateful inspection)*. Elle a certes fait ses preuves à la fin des années 1990, mais elle est désormais incapable de proposer des fonctionnalités de sécurité adaptées au paysage des attaques d'aujourd'hui.

Et troisièmement, le concept de « réseau » connaît une mutation rapide et sa nature tend à devenir amorphe : l'avènement des fournisseurs SaaS (logiciel sous forme de service), l'apparition du Cloud Computing, la mobilité, l'Internet des objets, ainsi que d'autres tendances macro-technologiques conduisent les professionnels de la sécurité à perdre progressivement le contrôle des données, puisque celles-ci vivent désormais bien souvent hors de l'organisation.

Plus d'intégration

Face à ces problématiques il est indispensable de s'assurer de plusieurs points dans l'architecture de la sécurité du futur :

Tout d'abord, le déploiement de systèmes de sécurité avancés, conçus d'après une bonne connaissance des utilisateurs du réseau (humains et machines). Pas de place pour les devinettes.

Deuxièmement, il faut que ces fonctionnalités soient intégrées autant que possible de manière native dans une plateforme globale. De sorte que toute action menée par n'importe quelle fonctionnalité aboutisse à une reprogrammation automatique des autres fonctionnalités.

Troisièmement, cette plateforme doit également faire partie d'un écosystème global à plus grande échelle, qui favorise le partage constant et quasi instantané des informations sur les attaques. Elles peuvent alors servir à appliquer sur-le-champ des protections empêchant d'autres organisations de l'écosystème d'être victimes des mêmes attaques.

Enfin, il convient que la position vis-à-vis de la sécurité soit cohérente quel que soit l'endroit où résident les données ou le modèle de déploiement du « réseau ». Par exemple, la sécurité intégrée avancée et les résultats automatisés doivent être les mêmes, que le réseau soit sur site,

« Nous devons favoriser le partage constant et quasi-instantané des informations sur les attaques »

dans le Cloud ou qu'il ait des données stockées ailleurs, par exemple dans des applications tierces. Toute incohérence dans la sécurité est en général un point de vulnérabilité. Et puis en matière de productivité, la sécurité ne doit pas venir freiner la mise en œuvre de scénarios de déploiement à haut rendement basés sur le Cloud, sur la virtualisation, SDN, NFV et sur d'autres modèles du futur.

Processus et personnes

La technologie seule ne suffit évidemment pas pour résoudre le problème. Il incombe à l'équipe de direction de veiller à ce que les experts techniques gèrent les risques en matière de cybersécurité au sein de l'organisation. La plupart des dirigeants d'aujourd'hui n'ont pas accédé à leur fonction au vu de leurs compétences technologiques ou de leur expertise en cybersécurité. Il n'en demeure pas moins que les dirigeants efficaces comprennent la nécessité d'évaluer le risque de l'organisation, d'allouer les ressources nécessaires et de consentir les efforts selon les priorités. Étant donné l'état de la menace et la rentabilité des attaques couronnées de succès, les dirigeants doivent impérativement cerner à la fois la valeur et les vulnérabilités de leurs réseaux puis hiérarchiser leurs efforts de prévention et de protection en conséquence.

Sous la responsabilité du dirigeant, il est également très important d'assurer l'amélioration continue des processus utilisés pour gérer la sécurité des organisations. Les employés doivent suivre en permanence des formations sur la manière d'identifier les cyberattaques et sur les mesures à prendre en cas d'attaque. Nombre des incidents signalés aujourd'hui commencent ou se terminent à cause de processus inefficaces ou d'une erreur humaine.

Par exemple, avec la masse d'informations personnelles publiées sur les réseaux sociaux par les internautes, il est facile pour les pirates de reconstituer des profils très précis des collaborateurs d'entreprises qu'ils ciblent et de lancer des attaques par ingénierie sociale. Ces attaques peuvent être difficiles à repérer en l'absence de formation adéquate, et délicates à maîtriser en l'absence de processus et procédures performants, quelle que soit l'efficacité de la technologie de protection déployée.

Ainsi la fraude aux faux ordres de virements internationaux (FOVI) est une attaque courante dont sont victimes de nombreuses entreprises. Elle consiste à détourner d'importantes sommes d'argent par le biais de virements et elle est rendue possible grâce à la présence de personnes très occupées et peu formées, mettant en œuvre des processus sporadiques. Lors d'une attaque de ce genre, le pirate utilise des données personnelles accessibles au public, glanées sur les réseaux sociaux. Sur la base de ces informations, il peut aisément identifier qui est habilité à émettre un virement au sein d'une entreprise.

Le pirate utilise ensuite une attaque par hameçonnage, par exemple depuis une adresse de messagerie factice scrupuleusement imitée qui, au premier coup d'œil, semblera provenir du responsable de cette personne au sein de l'entreprise. C'est par le biais de cette messagerie que le pirate demandera à sa victime d'envoyer immédiatement un virement aux coordonnées bancaires mentionnées.

Si l'employé n'est pas formé à rechercher les bonnes configurations d'adresse de messagerie ou si l'entreprise ne dispose

pas de processus efficaces pour valider les demandes de virement, comme une double approbation par exemple, ce genre d'attaque a de fortes chances d'aboutir. Il est donc primordial de coordonner la technologie, les processus et les personnes, et en particulier de former celles-ci de manière régulière.

Partage

Étant donné l'intensification des cyberattaques et leur degré de sophistication, il est difficile de croire qu'une entreprise ou une organisation quelconque disposera de suffisamment de renseignements sur les menaces pour pouvoir mettre à mal la majorité des attaques dont elle pourrait être victime. En revanche, il est facile d'imaginer que si plusieurs entreprises partagent ce qu'elles savent d'une attaque en quasi temps réel, le cumul des renseignements réduirait mécaniquement le nombre d'attaques réussies.

C'est ce vers quoi nous devrions tendre, car si nous parvenions à ce stade cela signifierait que les pirates devraient alors concevoir et élaborer des attaques uniques chaque fois qu'ils souhaiteraient menacer une organisation (ce qui n'est pas le cas aujourd'hui, car ils peuvent utiliser à l'envie des variantes d'une même attaque à l'encontre de nombreuses cibles). Concevoir des attaques uniques à chaque fois ferait augmenter naturellement le coût d'une attaque réussie et obligerait les pirates à mutualiser leurs ressources (humaines et pécuniaires). Cela les exposerait cependant davantage et les rendrait plus visibles aux yeux des défenseurs de la cybersécurité, de la loi et des gouvernements qui les traquent.

L'effet réseau dont peut bénéficier la défense justifie de s'intéresser de près au partage du renseignement sur les menaces. Sur ce front, nous n'en sommes qu'aux prémices, mais tout progrès est bon à prendre ! Et puis, surtout, les entreprises utilisent plus souvent désormais des systèmes automatisés de partage des renseignements. Dans le même temps, les fonctionnalités analytiques connaissent un développement rapide et permettent d'utiliser et d'exploiter tous ces renseignements de manière à créer des plateformes avancées capables de reprogrammer rapidement les fonctionnalités de prévention. De cette façon, les réseaux connectés pourront constamment mettre à jour les fonctionnalités de prévention des menaces dans un écosystème toujours plus grand. Cela procure un atout de poids dans la lutte en matière de cybersécurité.

En conclusion

Le nombre toujours plus grand de cyberattaques suscite une inquiétude et une attention compréhensibles. Toutefois, si nous nous projetons à plus long terme et adoptons une stratégie privilégiant la prévention, les technologies de nouvelles générations, l'amélioration des processus internes, la formation du personnel et le partage en temps réel des informations sur les menaces, le tout associé à des plateformes pouvant reconfigurer automatiquement la posture de sécurité de l'organisation, nous pourrons sensiblement réduire le nombre d'attaques réussies et ainsi restaurer la confiance numérique dont nous avons besoin pour construire notre économie mondiale. ■

8

Le Cloud : vous y êtes déjà

Par Alain Bouillé.

Alain Bouillé est le Directeur de la Sécurité des Systèmes d'Information du Groupe Caisse des Dépôts depuis 2001. Il préside depuis juillet 2012 le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) regroupant plus de 250 RSSI de grandes entreprises.

Il y a de grandes chances pour que votre entreprise stocke déjà des données dans le Cloud, qu'elle en soit consciente ou non.

Ainsi un sondage réalisé en début d'année auprès de 125 entreprises membres du CESIN (Club des experts de la sécurité de l'information et du numérique) montrait que 85% des répondants était utilisateurs de solutions Cloud.

La véritable question devient alors plutôt de savoir quelles données conserver et dans quels Cloud...

Nous observons que l'adoption du Cloud commence souvent par ce que nous appelons du « *Shadow IT* », ou de l'informatique cachée.

Le «Shadow IT», ou l'externalisation subie

Il s'agit d'initiatives individuelles dans lesquelles des utilisateurs impatients préfèrent utiliser directement sur Internet un service qui leur sera utile au quotidien plutôt que d'en faire la demande au service informatique. Ils estiment gagner ainsi du temps et s'éviter, outre des procédures administratives qu'ils considèrent fastidieuses, de devoir systématiquement justifier leur besoin et d'attendre que le service informatique leur propose une solution qui ne sera pas toujours celle qu'ils espéraient.

Et le phénomène ne touche pas seulement les individus : parfois ce sont les métiers eux-mêmes qui, ne se sentant pas écoutés par la DSI ou jugeant celle-ci peu réactive, achètent directement des services sur Internet. Et certains vont même jusqu'à faire des notes de frais pour les régler !

Evidemment cette pratique pose plusieurs soucis : Des données quittent l'entreprise pour être traitées et

stockées sans aucune évaluation formelle de leur sensibilité et des conditions de traitement.

Lorsque ces informations sont à caractère personnel et que le fournisseur du service n'est pas situé au sein de l'Union Européenne, elles peuvent faire courir à l'entreprise un risque juridique fort *(se référer au chapitre 2 pour les risques liés aux données à caractère personnel).*

L'entreprise n'a aucun contrôle sur l'authentification et le contrôle d'accès à ces services. En particulier, les utilisateurs peuvent conserver leur accès même après avoir quitté l'entreprise.

Dans de telles circonstances c'est au DSI et au RSSI de rattraper les choses, et la première question à se poser est évidemment de savoir pourquoi la pratique du Shadow IT se développe dans l'entreprise.

Deux possibilités peuvent l'expliquer. La première, bénigne, est liée à des usages limités sur des outils et des données non stratégiques, avec laquelle l'entreprise peut vivre à condition de l'encadrer à minima. La seconde est quant à elle le signe d'une DSI qui ne joue plus totalement son rôle.

Mieux encadrer la souscription à des services externes

Dans le premier cas le Shadow IT naît du constat qu'il n'est pas toujours nécessaire de développer tous les services en interne si ceux-ci sont déjà disponibles sur le Web. Cela peut même être une preuve de maturité que de l'accepter, et d'encadrer alors formellement le recours à des services externes.

L'encadrement prendra alors la forme d'un processus rapide dans lequel une mini-analyse de risque sera réalisée par la SSI, en s'intéressant notamment au fournisseur du service, à sa réputation, et en prenant en compte les risques juridiques, la nature et la localisation des données traitées. On peut alors ajouter les clauses contractuelles ad-hoc qui permettront de limiter les risques (mais je reconnais que cela peut relever parfois du combat du pot de terre contre le pot de fer, cela dépend grandement de l'organisation que l'on représente).

La SSI peut par exemple ici exiger des fournisseurs de service d'effectuer des tests d'intrusions sur la solution pressentie. Si ça n'est pas possible, les résultats de tests d'intrusion récents peuvent être demandés afin de s'assurer que ces derniers ne présentent pas de vulnérabilités évidentes et à tout le moins vérifier qu'ils sont conscients de ces sujets de SSI.

Quand la DSI ne joue pas pleinement son rôle

La seconde origine potentielle du Shadow IT est plus inquiétante : elle est le signe que la DSI n'est plus en mesure de répondre aux attentes des utilisateurs sur des services de base, qui constituent pourtant son coeur de métier (le partage de fichiers volumineux, la vidéo-conférence, les usages collaboratifs, etc). Nous avons l'exemple d'une entreprise chez qui de nombreux utilisateurs se servaient d'un service gratuit en ligne pour générer des fichiers PDF à partir de documents Office, alors même qu'ils disposaient d'un logiciel pour cela sur leur poste de travail, mais qu'ils estimaient inadapté. Cela créait évidemment les conditions d'une fuite de données importante pour l'entreprise, tout simplement parce que la DSI n'avait pas pris la mesure du besoin des utilisateurs.

Cette situation, aux causes plus structurelles, est bien entendu la plus sérieuse et celle qu'il conviendra de traiter en priorité. Tant qu'existera une défiance de la part des utilisateurs vis-à-vis de leur propre Direction Informatique, aucune des mesures

d'encadrement visées ci-dessus ne sera efficace. Il est donc nécessaire de comprendre pourquoi la DSI ne joue plus entièrement son rôle, au point de ne plus répondre aux attentes des utilisateurs, et d'y remédier.

Le Cloud choisi

Vient ensuite, évidemment, le Cloud «voulu» : lorsque l'entreprise décide d'externaliser tout ou partie de son Système d'Information. Les modalités peuvent être diverses : externalisation de l'infrastructure, avec les offres de Platform as a Service ou d' Infrastructure as a Service (PaaS et IaaS) ou d'externalisation d'applications avec les services en mode SaaS (Software as a Service). Mais dans tous les cas il s'agira d'un choix stratégique de la part de l'entreprise, qui devra être traité comme tel.

Avant de prendre la décision, le dirigeant doit porter son attention sur plusieurs points-clés, autant juridiques, techniques que stratégiques.

Il est ainsi d'abord nécessaire d'estimer la valeur des informations que l'on envisage d'externaliser, et estimer les conséquences de leur perte ou leur divulgation éventuelles. Y a-t-il des données stratégiques ? Si oui, c'est alors au trio RSSI / DSI / Gestionnaire des risques d'évaluer l'opportunité d'externaliser ces données. Et cela peut être long : l'un de nos membres a évalué pendant un an le recours à une solution de messagerie externalisée, avant de décider de ne pas y aller. C'est donc au RSSI / DSI / Risk Manager de mener un travail sérieux, en prenant le temps nécessaire, afin que la Direction Générale puisse trancher.

Mieux vaut commencer par mettre de l'ordre chez soi avant d'externaliser

Il est ensuite vital d'évaluer comment sont protégées les données actuellement. Si le niveau de maturité de l'entreprise n'est pas suffisamment élevé sur ce point (la gestion des droits et des accès est perfectible, il n'y a pas d'audit des accès, etc.) il vaut mieux mettre de l'ordre dans sa gestion des données sensibles avant d'envisager de les externaliser.

La capacité du prestataire à apporter un niveau de protection au moins équivalent à ce que l'entreprise met en oeuvre en interne est également un point important à prendre en considération. Car si pour de nombreuses petites et moyennes entreprises leurs données seront souvent mieux protégées chez un prestataire Cloud sérieux, ce n'est pas automatiquement le cas pour un grand groupe. Les prestataires Cloud nivellent leur niveau de sécurité afin qu'il soit adapté aux besoins de la majorité de leurs clients, ce qui ne sera pas toujours suffisant pour les plus exigeants.

La réversibilité est un leurre

Evidemment il faut aussi se poser la question de la réversibilité : comment cela se passe-t-il si l'on décide de changer de fournisseur ? Il n'est pas suffisant que le prestataire mentionne ce point dans le contrat. Concrètement, que fait-on lorsqu'on récupère un gros «camion» de données à la fin du contrat ? Cela doit faire partie de l'analyse de risque, et de manière très concrète (avec des tests !). Ce n'est pas tant la présence d'une clause de réversibilité que la capacité à l'exécuter qui importe.

Autre point crucial à ne pas négliger : l'aspect social et les Ressources Humaines. Si l'entreprise a externalisé, elle a potentiellement réduit ses effectifs techniques. Comment cela se passera-t-il si au bout de cinq ans elle décide de faire machine arrière ? Aura-t-elle toujours les personnels et les compétences pour reprendre l'exploitation en interne dans de bonnes conditions ? Certainement pas !
Lorsque l'on considère l'externalisation

dans le Cloud, il faut aussi réaliser que l'on devient beaucoup plus dépendant de sa connectivité à Internet. Aujourd'hui, si celle-ci ne fonctionne plus pendant une journée l'on peut encore bien souvent travailler, même en mode dégradé - y compris envoyer des messages internes via la messagerie. Mais si demain l'essentiel est externalisé, l'accès Internet devient un point individuel de défaillance. L'architecture de l'accès à Internet doit donc être revue et considérée comme étant critique. Et cela sans compter l'augmentation des débits souvent nécessaires pour accommoder toutes ces solutions dans le Cloud.

Une attention particulière devra également être apportée au chiffrement des données : ce n'est pas tout que le prestataire mentionne sa présence. Encore faut-il pouvoir savoir précisément comment sont gérées les clés, qui les détient, où sont-elles stockées... ?

Enfin, il ne faut pas oublier le volet juridique : même si la vocation du DSI et du RSSI est de devenir un peu plus juristes, il faut systématiquement impliquer le service juridique dans ces questions, voire de recourir à un juriste spécialisé car les questions juridiques et contractuelles deviennent de plus en plus complexes à appréhender dans ce paradigme.

En définitive, la question n'est pas de

Les 10 recommandations du CESIN face aux projets Cloud

1. Estimez la valeur des données que vous comptez externaliser ainsi que leur attractivité en terme de cybercriminalité.
2. S'il s'agit de données sensibles voire stratégiques pour l'entreprise, faites valider par la Direction Générale le principe de leur externalisation.
3. Evaluez le niveau de protection de ces données en place avant externalisation.
4. Adaptez vos exigences de sécurité dans le cahier des charges de votre appel d'offres en fonction du résultat du point 1.
5. Effectuez une analyse de risque du projet en considérant les risques inhérents au cloud comme la localisation des données, les sujets de conformité et de maintien de la conformité, la ségrégation ou l'isolement des environnements et des données par rapport aux autres clients, la perte des données liée aux incidents fournisseur, l'usurpation d'identité démultipliée du fait d'une accessibilité des informations via le web, la malveillance ou erreur dans l'utilisation, etc.
   Sans oublier les risques plus directement liés à la production informatique : la réversibilité de la solution et la dépendance technologique au fournisseur, la perte de maîtrise du système d'information et enfin l'accessibilité et la disponibilité du service directement lié au lien Internet avec l'entreprise.
6. Outre ces sujets, exigez un droit d'audit ou de test d'intrusion de la solution proposée.
7. A la réception des offres analysez les écarts entre les réponses et vos exigences.
8. Négociez, négociez.
9. Faites valider votre contrat par un juriste. Si vous êtes une entreprise française, ce contrat doit être rédigé en français et en droit français.
10. Faites un audit ou un test d'intrusion avant démarrage du service (si cela est possible) et assurez-vous du maintien du niveau de sécurité de l'offre dans le temps.

rejeter ou accepter en bloc l'usage du Cloud. L'entreprise souffrirait de se retrouver coincée entre un DSI qui pousse à une externalisation massive tandis que le RSSI refuserait en bloc pour des raisons de sécurité.

Une équipe constituée de la DSI, du RSSI, du Risk Manager et du département juridique doit plutôt travailler de concert pour éclairer le choix de la Direction Générale de manière concrète et réaliste, et en considérant que, dans les faits, l'usage du Cloud est déjà là et qu'il peut être porteur d'opportunités. ■

Pour anticiper

- **Sachez précisément les compétences que vous perdez en externalisant**
  Faites collaborer DSI et RH afin d'établir précisément les compétences nécessaires à l'exploitation des solutions internes que l'entreprise s'apprête à externaliser. Le livrable devrait permettre d'accélérer la recherche de profils adéquats sur le marché du travail. Ce travail devrait également être régulièrement mis à jour.

Actions

9

« Faute de pouvoir empêcher toutes les cyberattaques, les entreprises doivent être en mesure de riposter »

Par Michel Van Den Berghe

Michel Van Den Berghe est CEO d'Orange Cyberdefense depuis le 1er juillet 2014. Il a rejoint le groupe en janvier 2014 suite au rachat d'Atheos dont il était le Président Fondateur depuis 2002.

Les risques d'intrusions informatiques vont de pair avec l'accroissement de la numérisation des entreprises. Celles-ci produisent de plus en plus de données et fondent leur développement sur l'interconnexion avec leurs fournisseurs, partenaires et clients.

C'est le principe même de l'économie en réseau où la création de valeur se nourrit de la circulation et de l'enrichissement continu des données. Cela suppose que des accès aux différents systèmes d'information soient ouverts afin de permettre ces échanges légitimes *(lire à ce sujet le chapitre 5 consacré à la transformation numérique).*

La fluidité de ces transferts informatiques est devenue une condition de leur performance et de leur rentabilité : plus l'information est rendue rapidement accessible, plus vite elle peut être exploitée. Mais cette ouverture de l'entreprise vers le monde extérieur ne peut évidemment s'envisager sans prendre en compte la sécurisation de ce qui constitue l'essentiel de son activité : c'est-à-dire l'ensemble des savoir-faire et des pratiques qui font sa spécificité et sa raison d'être sur son marché. Or, il suffit à peine de quelques secondes pour extraire des fichiers d'un système d'information et divulguer sur la place publique des éléments techniques ou commerciaux qui constituent l'actif stratégique d'une société.

Dans le même esprit, la non-disponibilité pendant quelques minutes ou plusieurs heures d'un site Internet ou de données sensibles peut se révéler fatale à bien des organisations.

Se donner les moyens de déceler continuellement et sans délai toute opération malveillante

C'est là tout l'enjeu de l'indispensable maîtrise de la réponse à incidents. Faute de pouvoir empêcher avec certitude la survenance d'un incident, l'entreprise doit se donner les moyens de déceler sans délai toute opération malveillante. Pour en mesurer l'impact, la stopper et restaurer les éléments infectés afin de revenir à une situation normale.

Outre la défense de ses intérêts stratégiques, cette capacité à répondre rapidement et efficacement aux incidents de sécurité va devenir une obligation légale. En effet, l'article 31 du Règlement européen[1] du 27 avril 2016, qui entrera en vigueur en mai 2018, fixe un délai de 72 heures pour alerter l'autorité de tutelle, en France la Commission Nationale de l'Informatique et des Libertés (CNIL), en cas d'atteinte aux données personnelles détenues par l'entreprise visée par la cyberattaque.

Des pénalités extrêmement lourdes pour les entreprises qui ne réagiraient pas à temps

En situation de crise, le temps est compté. Et l'improvisation n'est guère de mise quand on sait que les sanctions financières établies par ledit Règlement européen peuvent s'élever par fuite constatée jusqu'à 4 % du chiffre d'affaires mondial de la société ou au minimum vingt millions d'euros. Des sommes qui, si elles devaient se cumuler dans l'année et se multiplier par pays européen, pourraient s'avérer fatales à la plus prospère des compagnies.

Consciente de la nécessité de faire appel à des professionnels expérimentés pour faire face à ces situations qui exigent la mise à disposition rapide de personnel, un haut niveau de compétences et une confiance totale dans le respect de la confidentialité par les équipes impliquées, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)[2] a établi un Référentiel[3] d'exigences en vue de labelliser les Prestataires[4] de Réponse aux Inci-

Article 31

En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.
Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

[2] ANSSI : http://www.ssi.gouv.fr

[3] Texte intégral du référentiel (version 0.3 du 7 juillet 2014) http://www.ssi.gouv.fr/uploads/IMG/pdf/PRIS_Referentiel_d_exigences_anssi.pdf

[4] Liste des prestataires en cours de labellisation PRIS, par l'ANSSI, parmi lesquels LEXSI/Orange Cyberdefense http://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/

dents de Sécurité (PRIS). Les critères requis pour déployer une réponse efficace sont aux nombres de trois : la réactivité, une confiance forte dans la probité des intervenants et un niveau d'expertise élevé.

Une indispensable réactivité

L'assaillant a naturellement l'avantage car c'est lui qui choisit sa cible et le calendrier de l'attaque. Il n'optera pas pour la date qui vous arrange ou pour viser une infrastructure que vous savez inutile. La gestion de crise liée au constat d'une cyberattaque viendra s'ajouter à la conduite de vos contraintes quotidiennes : concurrence commerciale, satisfaction des clients, production des commandes enregistrées, préservation de l'image de marque… Ce n'est pas alors que la crise débute et enfle que vous pourrez tranquillement compulser les Pages Jaunes à la recherche d'un réparateur informatique. Les fuites de données sont de celles qui peuvent véritablement mettre en péril mortel votre organisation. Il convient donc d'avoir bien en amont identifié les partenaires capables de vous accompagner dans les délais courts qu'imposent ces situations d'urgence.

La disponibilité de personnels qualifiés nécessite de consacrer des moyens importants en matière de formation et de gestion des équipes. Seules des entités dotées de ressources conséquentes peuvent assumer de tels investissements sur la durée. Le traitement de la crise exige une mobilisation rapide de personnels qui seront amenés à travailler en continu jusqu'à l'identification et à la résolution du mode d'attaque.

La confiance est une exigence

Les professionnels qui sont sollicités juste après la découverte d'une cyberattaque abordent l'entreprise alors que celle-ci traverse une phase de fragilisation, tant de son infrastructure que de son management. Une intervention dans un contexte aussi sensible suppose que les cadres dirigeants puissent échanger en toute sincérité sur l'état des équipements, le périmètre des dommages subis et sur la réponse technique, médiatique et économique qu'il convient d'apporter.

Car le prestataire va être amené à entrer dans l'intimité numérique de l'entreprise. Il devra collecter des données appartenant à celle-ci afin de les analyser. D'autant plus que ces actions seront conduites alors même que l'attaquant aura pu prévoir des dispositifs de surveillance afin d'adapter son mode d'attaque à la réaction de sa cible.

Une véritable relation de confiance doit alors s'établir entre le prestataire et les représentants de l'entreprise victime afin d'adapter le mode opératoire et remédier ainsi à la compromission du système d'information. C'est de la qualité des échanges que dépendra la réussite de la préservation des actifs de l'entreprise.

Des adaptations constantes de posture seront nécessaires pour le cas échéant contourner les moyens mis en œuvre par le pirate pour entrer dans le système, mener son action offensive, se maintenir dans les équipements de sa cible et ensuite parvenir à extraire les informations désirées. La modularité de la réponse ne pourra être pleinement bénéfique que si elle se bâtit dans une étroite collaboration entre le management et le prestataire en sécurité auquel ils auront accordé leur confiance. C'est une dimension éminemment humaine dans cet univers de haute technologie.

La diversité des modes d'attaques possibles implique une réponse d'expert

Les attaquants sont très opportunistes et conçoivent des modes d'action destinés à coller à l'environnement de leurs cibles. Il convient alors de mener les investigations nécessaires pour déterminer, par

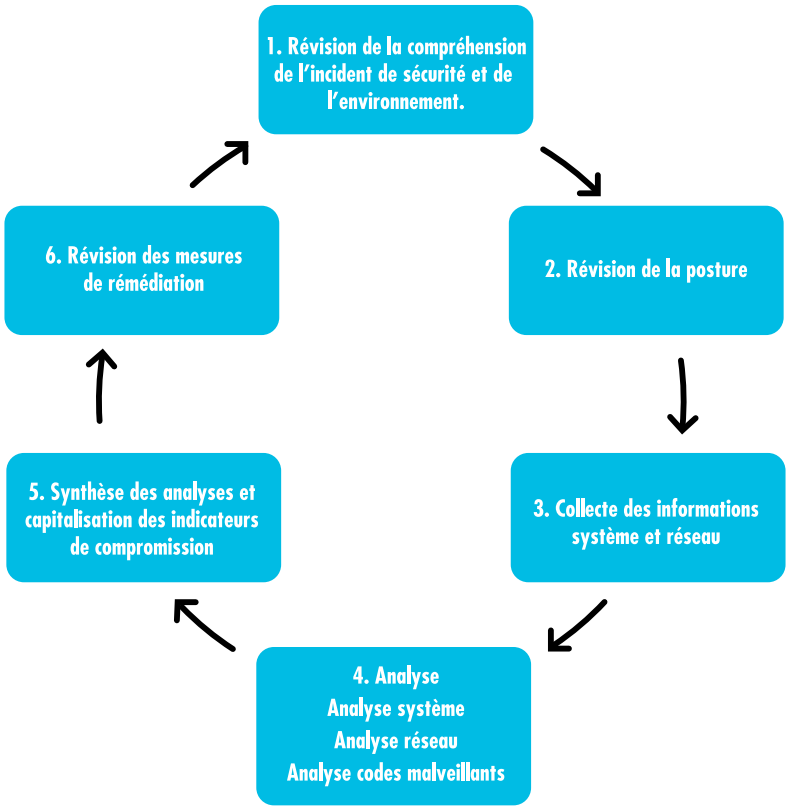
exemple, la date de compromission initiale et les mutations successives des logiciels malveillants utilisés.

Il est souvent nécessaire de faire preuve d'une grande agilité technique pour prendre la mesure des forces de l'assaillant, comprendre sa tactique et circonscrire son champs d'action. Ces contre-mesures requièrent une maîtrise des procédures, fondée sur des années d'expériences professionnelles dans le domaine de la sécurité. C'est une guerre de mouvements avec des innovations constantes et des motivations souvent difficiles à identifier.

Voici schématisé le déroulement des opérations *(Voir figure)*.

Outre la préservation des actifs numériques de l'entreprise, le prestataire aguerri veillera également à fournir les éléments techniques permettant de conduire d'éventuelles procédures judiciaires. Voire d'obtenir de possibles réparations de la part de la compagnie d'assurances si les contrats souscrits prévoient la prise en charge de tels dommages. Cet accompagnement mêle donc l'expertise technique à une connaissance des règles juridiques permettant la bonne résolution de ces intrusions informatiques. ■

Etapes de l'exécution des prestations de réponse aux incidents de sécurité
Source : ANSSI – Référentiel PRIS – 2014.



Pour anticiper

1. **Intégrez la crise de nature cyber aux scénarios de votre cellule de crise**
   Si les scénarios de crise ne portent encore que sur les risques sociaux, naturels ou de production, il est temps de les faire évoluer afin d'intégrer des crises de nature cyber : mise en cause de l'entreprise qui aurait servi de relais à une attaque – *voir le chapitre juridique* –, écoute des moyens de communication réseau, prise en otage de systèmes informatiques (ransomware), etc.

2. **Challengez vos fournisseurs et prestataires sur leur capacité à réagir en cas de crise dans l'entreprise**
   Ce n'est pas lorsque la crise frappe qu'il faudra réaliser que les prestataires ne sont pas en mesure de déployer les personnels nécessaires à la gestion des évènements.

3. **Assurez-vous de pouvoir produire des comptes rendus d'incidents utiles**
   Il est important que les équipes internes, potentiellement assistées d'experts externes, soient en mesure de formaliser la phase post-incident par la création d'une documentation solide couvrant les causes de l'incident, le bilan, les mesures de correction prises et les enseignements tirés.

4. **Testez régulièrement sa capacité de fonctionnement en mode dégradé et de reprise d'activité**
   Seules des mises en situation régulières permettront de déceler des points de blocages tels que l'incompatibilité entre des matériels ou des solutions de nature différentes, l'incapacité des équipes à exploiter tel ou tel outil en mode dégradé, etc.

10

L'avenir de la cyberassurance

Par Laure Zicry

Laure Zicry est Responsable Technique Institutions Financières et Cyber Risks Practice Leader dans un grand groupe international. Elle est également l'auteur d'un ouvrage consacré à la maîtrise des risques cyber et membre du CEFCYS, le Cercle des Femmes de la Cybersécurité. Elle livre ici une vision très pratique de la cyberassurance.

Identifier les risques qui pèsent sur l'entreprise constitue un préalable indispensable pour le dirigeant.
Car réaliser la cartographie des risques lui permet de connaître les scenarii majeurs auxquels l'entreprise est susceptible de faire face. Il conviendra de quantifier financièrement *ces* scénarii afin d'apprécier l'impact sur le bilan si l'un d'entre eux devait survenir.

Cette démarche est *importante* car tout dirigeant d'entreprise doit se préparer à subir une cyberattaque ou un vol de données et prendre conscience que cet incident, même si l'entreprise en est victime, aura des impacts sur le bilan.

Certains risques peuvent certes être réduits par des mesures techniques (sondes de détection d'intrusion, chiffrement des données, SOC, CERT...), mais il demeurera toujours un risque résiduel.

Pour faire face à ce risque résiduel, le dirigeant peut alors se tourner vers le marché de l'assurance, qui lui permet de transférer le risque à un prestataire *(un assureur)* et ainsi protéger le patrimoine informationnel de son entreprise et donc son bilan.

La cyberassurance : un nouveau contrat d'assurance pour un nouveau risque

Nés aux États Unis il y a une dizaine d'années, les contrats d'assurance cyber ont été développés pour répondre aux obligations issues des lois fédérales relatives à la protection des données. Celles-ci contraignent les entreprises à prévenir à l'issue d'une fuite de données personnelles non seulement les autorités locales mais aussi chaque personne concernée. On

entend par personne concernée, toute personne dont les données à caractère personnel sont collectées, stockées et traitées par l'entreprise.

S'il est déjà bien ancré aux États-Unis, ce marché est en revanche assez récent en France, mais il évolue très vite.

A ce jour plus d'une quinzaine d'assureurs proposent des contrats d'assurance Cyber avec des montants de garantie qui varient entre 5 M d'euros et 50 M d'euros. Il est possible de souscrire des *programmes* d'assurance *avec plusieurs assureurs* et ainsi de souscrire plus de 400 M d'euros de garantie. Alors que les premières souscriptions se faisaient rares en 2013, le nombre d'entreprises assurées est désormais en forte croissance. La recrudescence des attaques informatiques visant des entreprises françaises publiques comme privées ainsi que le vote du Règlement Européen à la Protection des Données *(voir le chapitre 2 consacré aux obligations légales européennes)*, a incité de plus en plus d'entreprises à se couvrir contre les conséquences de tels risques cyber.

A noter que l'une des *particularités* de ce marché est que le contrat d'assurance Cyber de votre entreprise ne ressemblera pas forcément à celui d'une autre. Il y a certes, un socle commun de garanties, mais votre contrat devra répondre précisément à vos propres cyber-risques : ceux que vous avez identifiés, qui sont propres à votre entreprise et à leur probabilité de survenance. Vous pourrez alors choisir de ne couvrir que certains d'entre eux (probabilité élevée et intensité forte) et de supporter les autres pertes, ou au contraire de faire assurer l'ensemble des risques.

Comment souscrire ? Association, Concertation et Prévention

Avant la souscription d'un contrat d'assurance cyber, il est recommandé d'associer vos collaborateurs dans le processus de souscription. Il faut en effet identifier en amont qui, dans l'entreprise, va être impliqué. Cela peut être dans la phase de souscription (réponse au questionnaire d'assurance) ou bien sûr dans la phase de déclaration, en agissant vis-à-vis de l'assureur mais aussi des autorités compétentes (CNIL ou son équivalent à l'étranger, ANSSI ainsi que toute autorité de contrôle dont votre entreprise dépend).

Les personnes-clés le plus souvent impliquées sont les suivantes : le Risk Manager ou Responsable assurance, le RSSI (Responsable de la sécurité des systèmes d'information) ou le DSI (Directeur des Systèmes d'Information), le CIL (Correspondant Informatique et Libertés) et bientôt le DPO (Délégué à la Protection des Données), et bien sûr la Direction Juridique et la Direction des Ressources Humaines.

Chacune de ces personnes a un rôle clé et il faudra solliciter les bonnes ressources en interne lors, notamment, de la collecte d'informations nécessaires au remplissage du questionnaire d'assurance. Les assureurs souhaiteront en effet avant toute souscription comprendre l'organisation de l'entreprise et avoir connaissance des mesures déjà en place qui seront actionnées en cas de crise. Il y a donc un vrai travail de concertation à mener en interne avant de souscrire à un tel contrat.

Enfin, la prévention est un des maîtres mots de la bonne gestion de l'incident *(lire à ce sujet le chapitre 9 consacré à la réponse aux incidents de sécurité)*. Sans prépa-

« Des consultants experts pour négocier la rançon des données volées »

« L'assureur pourra prendre à sa charge les frais de surveillance du Dark Web »

ration ni anticipation, si aucun plan n'a été élaboré en amont pour minimiser les effets d'une cyberattaque, l'entreprise ne pourra qu'être en mode réactif, sans pouvoir mettre en œuvre de réelle stratégie de protection.

Se préparer à réagir à un incident et réaliser des stress tests est donc vital. D'ailleurs les agences de notations S&P et Moody's ont d'ores et déjà intégré ces paramètres dans leurs critères d'évaluation.

Au delà de l'impact d'une cyberattaque sur la notation par les grandes agences, les conséquences pour l'entreprise victime sont nombreuses. Elle devra non seulement engager des frais importants pour répondre à la crise (première période qui suit la découverte de l'incident) mais aussi répondre des conséquences mêmes de l'incident (perte de chiffres d'affaires, pertes de marge brute, amendes et sanctions pécuniaires en cas de non respect des dispositions législatives ou réglementaires, ainsi que les conséquences de la responsabilité civile sur les tiers).

Cyberassurance : des garanties spécifiques face aux risques d'atteintes aux données ou aux systèmes

Les garanties délivrées par les contrats d'assurance cyber ont été spécifiquement conçues pour prendre en charge les frais et pertes qui seront engagés par l'entreprise pour répondre des conséquences d'une atteinte aux données et/ou aux systèmes d'information. Ces contrats d'assurance contiennent généralement trois volets, qui correspondent aux trois phases de la gestion d'un incident.

Le premier volet est celui qui correspond à la phase de crise et comprend des couvertures d'assistance et de gestion de crise. Les assureurs mettront à la disposition des assurés des prestataires extérieurs, ou bien ils rembourseront les honoraires des prestataires avec lesquels l'entreprise a l'habitude de travailler (et qui auront été nommés au contrat).

Il s'agit ici de prestataires aux profils très divers. On y trouve des experts en gestion de crise, en analyse forensique (pour mener l'expertise informatique légale), des avocats (rédaction de la lettre de notification aux autorités compétentes et aux personnes concernées), ou encore de *monitoring* et surveillance des réseaux de cyber-criminels (pour surveiller si les données volées sont utilisées sur Internet ou revendues sur le dark web...). Il y a également besoin d'experts en matière de reconstitution des données, en Relations Publiques (pour assister l'entreprise lors de la communication de l'incident) ainsi que des experts et des consultants pour aider l'entreprise à répondre aux enquêtes des autorités de contrôle (CNIL, ANSSI...).

Le second volet délivre quant à lui des garanties qui seront actionnées en cas de réclamations de tiers, c'est-à-dire les conséquences sur les clients ainsi que sur les employés de l'entreprise.

Car votre entreprise, bien que victime d'un incident, devra malgré tout répondre des fautes qu'elle a commises *(voir à ce sujet le chapitre 2).*

Pourront ainsi lui être reprochés le non-respect d'une obligation de confidentialité en cas d'atteinte aux données personnelles (vol de données telles que les noms, prénoms, date de naissance, numéro de carte bancaire, numéro de sécurité sociale...) ou encore le non-respect ou l'absence de mesures de sécurité des systèmes

d'information qui aura permis à un pirate informatique d'accéder aux systèmes (attaque DoS ou DDoS, attaque virale, intrusion sur un autre système d'information à partir de celui de l'entreprise …).

Enfin, il existe un troisième et dernier volet qui a pour objet de prendre en compte les conséquences sur l'entreprise elle-même. Il s'agit ici soit des frais supplémentaires d'exploitation que l'entreprise aura engagés afin d'éviter une perte de marge brute (location de nouveaux locaux, recours à la sous-traitance, location de nouveau matériel informatique...), soit des pertes d'exploitation qui sont la conséquence de l'incident. Est également inclus dans ce volet ce que l'on appelle la garantie cyber extorsion qui est appelée à intervenir lorsque l'entreprise est victime de ransomware *(un logiciel malveillant destiné à chiffrer les données présentes sur un système informatique et proposer le déchiffrement contre une rançon, souvent payable en bitcoins)*. Dans ce dernier cas l'assureur prendra en charge le coût des consultants engagés pour négocier la rançon le cas échéant, mais aussi pour rembourser celle-ci, jusqu'aux frais bancaires si l'entreprise a dû emprunter pour régler la somme.

Pour anticiper

1. **Identifiez les personnes-clés capables de répondre au questionnaire de l'assureur**
   Avant même de se lancer dans un projet de cyberassurance il faut s'assurer que l'on dispose des ressources nécessaires pour répondre de manière fiable et complète aux questions de l'assureur.

2. **Préparez les plans de réponse aux incidents**
   Le contrat de cyberassurance n'est qu'un élément de la stratégie globale de réponse aux incidents. Il convient donc d'avoir déjà formalisé sa capacité de réponse pour en tirer le meilleur parti.

3. **Connaissez vos consultants**
   Si l'assureur est bien sûr en mesure de vous conseiller des intervenants fiables, intervenir sur un incident de sécurité implique que les consultants auront accès à de nombreuses informations sensibles concernant l'entreprise. Il est alors préférable de faire intervenir vos propres prestataires experts, qui connaissent déjà votre environnement. A condition d'avoir pris le temps de les trouver, de les tester et de les avoir nommés dans le contrat d assurance.

Comment actionner son contrat lors de l'incident ?

Une fois le contrat d'assurance souscrit, il faut se préparer à l'actionner en cas d'incident. Il faudra donc réunir les personnes-clés du dispositif et auxquelles vous aurez révélé l'existence du contrat *mais uniquement à elles*. Attention à la confidentialité ! Ce type de contrat doit rester confidentiel sous peine que certaines clauses ne jouent pas si celui-ci est dévoilé, notamment en ce qui concerne la garantie cyber-extorsion.

Si l'entreprise a des filiales ou succursales à l'étranger, il faudra également leur adresser un résumé afin de les informer des modalités de mise en jeu.

Dès que l'entreprise a connaissance d'un incident, il lui faut immédiatement déclarer le sinistre à l'assureur et/ou à son courtier en assurance. Celui-ci la mettra en relation avec les experts et les consultants spécialisés en gestion de crise qui guideront l'entreprise dans les démarches à suivre selon le type d'incident.

S'il s'agit d'un vol de données, par exemple, il conviendra d'informer les autorités compétentes et les personnes

concernées dans un délai précis et dans les formes prévues par la règlementation applicable.

Lorsque le Règlement Européen à la Protection des Données sera entré en vigueur (en 2018), toute entreprise française devra informer la CNIL du vol de données à caractère personnel dans un délai de 72 heures à compter du moment ou l'entreprise en aura eu connaissance. Le contrat d'assurance devra donc être actionné dès la connaissance de l'incident afin que les coûts engendrés par la notification (frais d'avocat pour rédiger la lettre et frais d'envoi aux personnes concernées) puissent être pris en charge par le contrat d'assurance.

Dans l'hypothèse ou l'entreprise victime d'un vol de données a signalé l'incident aux personnes concernées et que ces dernières mettent en cause la responsabilité civile de l'entreprise, l'assureur devra être immédiatement informé dès la réception d'une mise en cause afin de défendre les intérêts de son assuré. En aucun cas l'entreprise ne devra transiger sans l'accord préalable de l'assureur.

Quelle que soit la nature de l'incident, bénéficier d'un contrat de cyberassurance permettra à l'entreprise de démontrer qu'elle a pris des mesures visant à réduire l'impact d'une cyberattaque sur le bilan de l'entreprise et a ainsi œuvrer pour protéger son entreprise et par ricochet, sa propre responsabilité civile personnelle.

Cela lui permettra dans un premier temps de limiter l'impact sur le bilan et ne pas engager la responsabilité civile personnelle de son dirigeant.

On peut considérer que le contrat de Cyberassurance est, au delà de la garantie supplémentaire, une preuve de maturité en matière de gestion des risques cyber. ■

11

« Messieurs les dirigeants, vous saviez que cette attaque allait arriver… Qu'avez-vous fait pour l'empêcher ? »

Par Jean-Paul Mazoyer

Directeur général du Crédit Agricole Pyrénées-Gascogne, Jean-Paul Mazoyer a été de 2013 à 2016 directeur informatique et industriel du groupe Crédit Agricole.

Le 8 avril 2015, une chaîne de télévision se faisait « hacker » par des activistes qui prenaient le contrôle de l'antenne pendant quelques heures. La réaction des médias et de l'opinion publique a été la sidération : comment cela avait-il été possible ? Nos systèmes informatiques sont-ils vulnérables à ce point ?

Aujourd'hui je suis convaincu que la réaction lors de la prochaine attaque d'envergure (celle dont le grand public entendra parler, et qui ne manquera pas d'arriver tôt ou tard) sera tout autre : *Messieurs les dirigeants, vous saviez que cette attaque allait arriver… Qu'avez vous fait pour l'empêcher ? Comment vous êtes-vous préparés ?*

Les dirigeants des organisations (publiques ou privées, petites ou grandes…) ne peuvent désormais plus ignorer le risque cyber. Outre la nécessité de le définir et de l'analyser, ils doivent se préparer à prouver qu'ils ont mis en œuvre les moyens nécessaires pour le circonscrire.

Mon propos n'est pas ici de détailler les mesures techniques qui permettent de protéger les systèmes de l'entreprise, ni les moyens d'analyse et de surveillance, ni les organisations spécialisées (Security Operation Centers, Computer Emergency Response Teams…), ni les procédures de recouvrement rapide en cas d'attaque… Tout cela est bien sûr absolument indispensable : des budgets importants doivent y être consacrés, des équipes doivent être mises en place, des compétences recrutées, des contrats de prestation signés…

Mon propos est plutôt de souligner que le risque majeur qui pèse sur une organisation face à ce risque

cyber est de deux natures, qui vont souvent de pair : le **désintérêt** porté à ce sujet par son dirigeant suprême et l'absence de **sensibilité** de la part du personnel.

Le désintérêt du dirigeant pour le risque cyber conduit à l'impréparation de l'entreprise

Ces deux causes mènent à l'impréparation et constituent *in fine* le terreau de la prochaine attaque.

Durant les trois années où j'ai exercé la responsabilité de l'informatique d'une grande banque et la présidence du Cercle cybersécurité du CIGREF (Club Informatique des Grandes Entreprises de France)[1], j'ai souvent été confronté à ces deux lacunes. Nous avons réussi à convaincre tous les Directeurs des Systèmes d'Information (DSI) de la nécessité de se saisir de ce sujet. Et grâce au soutien de 30 grandes entreprises, de l'ANSSI, du Ministère de l'Intérieur, de la Réserve Citoyenne de cyberdéfense (État Major des Armées) et de certains médias, nous avons même lancé la première campagne de communication grand public sur les risques Internet : *la Hack Academy*[2].

C'est pourquoi la sensibilisation aux menaces cyber en général, et celle du dirigeant de l'entreprise en particulier, est un sujet essentiel. Le dirigeant doit être en mesure de faire naître au sein de son entreprise une véritable « *culture de la cyberdéfense* » et cela passe d'abord par sa propre prise de conscience de l'enjeu.

Cette prise de conscience est par ailleurs nécessaire car la réglementation qui encadre la gestion des risques cyber évolue (se référer entre autres à la loi de Programmation Militaire pour les Organismes d'Importance Vitale ou aux différents projets de règlements européens) et oblige les entreprises à s'adapter aux nouvelles menaces, et à exiger une adaptation similaire de leurs partenaires.

Et cela a déjà commencé : désormais les analystes financiers posent des questions sur leur niveau de préparation aux entreprises cotées lors des roadshow de ces dernières. Les actionnaires interrogent les dirigeants lors des assemblées générales, les comités d'audit et des risques des conseils d'administration se saisissent évidemment de ces sujets. Même les comités d'entreprise et les représentants du personnel interpellent les directions générales.

De nombreux colloques sont organisés, y compris à destination des TPE et des artisans/commerçants. Dans un pays voisin, une réunion ad hoc a été organisée avec les plus grandes entreprises autour du Premier Ministre.

On ne peut pas dire que les occasions manquent pour un dirigeant de se sensibiliser à la cybersécurité. Mais combien d'entre eux s'y intéressent-ils vraiment ? Durant ces dernières années, j'ai entendu nombre de dirigeants m'expliquer que *« l'informatique, moins j'en entends parler, mieux je me porte ! »…*

Il suffit pourtant d'écouter le dirigeant de cette chaîne de télévision raconter son expérience pour comprendre qu'une attaque informatique d'envergure sera désormais traitée au plus haut niveau de l'entreprise, au même titre que la destruction physique de ses locaux, et que le dirigeant suprême sera en première ligne…

Face à des experts techniques lui exposant alors des sujets abscons, il devra néanmoins se plonger très vite dans les méandres de son système informatique

[1] Jean-Paul Mazoyer a été DSI du Crédit Agricole entre 2013 et 2016, Vice-Président du CIGREF et Président-Fondateur de son cercle cybersécurité. Il est également membre de la Réserve Citoyenne de cybersécurité.

[2] hack-academy.fr

et de ses protections pour prendre, dans l'urgence, les décisions qui s'imposeraient. Alors autant s'y préparer avant !

En prenant le temps d'une réunion approfondie et régulière avec son DSI pour comprendre, en se faisant expliquer les menaces, les risques, les enjeux, en « sanctuarisant » le budget adéquat sans exiger un retour sur investissement (de toute façon impossible à calculer), en organisant un exercice régulier de « cyber-crise » (au minimum annuel), en conditions réelles, avec tous les membres du Comité Exécutif, avec un scénario crédible et réaliste. Il est également possible d'inviter à ces exercices de crise des témoins extérieurs devant les dirigeants (consultants, spécialistes, autorités civiles et militaires, et même dirigeants d'entreprises ayant été attaquées…).

L'ouverture réelle et sincère sur son environnement et la connaissance de son système d'information me semblent deux conditions sine qua non d'une bonne préparation.

Comment sensibiliser le personnel des organisations?

La plupart des attaques informatiques concernant les entreprises ont un point commun : elles ont réussi grâce à la complicité passive (et malheureusement quelquefois active) d'un salarié. Elles réussissent donc trop souvent par naïveté et par manque de sensibilité au risque cyber. Mais comment blâmer un salarié de la DRH qui a ouvert un mail qu'il croyait être un CV, ou un salarié des services comptables qui a fait de même avec une facture contenant un virus , s'il n'a jamais été sensibilisé à ces risques particuliers ? A l'inverse, beaucoup de ces attaques ont été déjouées par la vigilance d'un salarié. L'information, la formation du personnel devient donc un enjeu majeur.

Il existe de nombreux « serious games »[3] qui allient le côté ludique d'un jeu avec la découverte des techniques pour se protéger. Leur déploiement dans l'entreprise me semble très utile. Des journées de sensibilisation (avec ateliers, conférences, jeux…) ont été organisées dans de nombreuses entreprises avec succès et efficacité. Des bagages de formation ont été construits par des entreprises, la vidéo étant souvent le meilleur média.

Des MOOC (cours en ligne) ont également été déployés permettant ainsi des échanges plus interactifs et un questionnement immédiat. De façon plus directe, des campagnes de faux mails envoyés par la DSI à tous les salariés peuvent être déployées pour une prise de conscience « choc ». Et on peut même intercaler une formation entre deux campagnes de faux mails pour mesurer la prise de conscience, par population, âge, fonction, pays…

Dans le domaine de la sensibilisation aux risques cyber, à l'instar des campagnes

[3] A l'instar du serious game « Keep an eye » du CIGREF

5 mesures de sensibilisation efficaces

1. Organisez des journées de sensibilisation (ateliers, conférences, jeux…).
2. Pensez à déployer un Serious Game.
3. Envisagez un bagage de formation à la cyberdéfense au sein de l'entreprise (par des cours en ligne de type MOOC ou des supports vidéo notamment).
4. Menez des campagnes de faux mail (« phishing ») afin d'évaluer les comportements des collaborateurs face à cette menace.
5. Ne pas oublier de sensibiliser en particulier les informaticiens de l'entreprise.

de la sécurité routière, l'alternance de messages soft et plus directs peut servir à la prise de conscience. La forme de cette sensibilisation est laissée à l'imagination de l'entreprise. A la condition explicite qu'on en parle régulièrement : tout relâchement dans l'effort de communication se traduira immanquablement par une augmentation des comportements risqués.

Les populations de salariés visés par ces actions doivent aussi être segmentées : entre des jeunes générations pouvant pratiquer un véritable « naturisme numérique » sur les réseaux sociaux à titre personnel et ayant tendance à reproduire ce comportement dans les entreprises, et des salariés se limitant à l'usage d'une messagerie interne, l'entreprise devra adapter son discours. Sans oublier une population insuffisamment sensibilisée selon moi : les informaticiens eux-mêmes, qui n'intègrent pas toujours les basiques de la sécurité dans les programmes qu'ils développent ou dans les actions qu'ils mènent (habilitations).

Une prise de conscience impérative

Le monde se divise désormais entre les entreprises qui ont été attaquées et celles qui ne savaient pas qu'elles l'ont été ! Et il faut en moyenne 200 jours à une organisation pour détecter une attaque sur son système d'information…Et ce n'est pas à l'aide d'une seule assurance protection cyber qu'une entreprise se protègera ! Et ce n'est pas non plus en niant les risques et en considérant que cela n'arrive qu'aux autres, aux grandes organisations, aux entreprises intervenant sur des secteurs sensibles.

Dans un récent colloque sur « Cybersécurité et territoires »[4], un intervenant me

Les bonnes questions à poser à l'équipe

1. **Notre RSSI a-t-il dans sa fiche de poste l'organisation d'actions de sensibilisation régulières ?**
   Il est important que cette thématique soit dotée d'un propriétaire désigné de manière officielle, et non que l'on assume simplement que le RSSI s'en chargera.

2. **De quelle nature étaient nos dernières actions de sensibilisation, et quels ont été les résultats ?**
   Ce n'est pas tout de mener des actions : il est nécessaire de suivre les résultats (en terme de nombre de collaborateurs participants, de résultats aux tests, d'ouverture des documents et messages…) et de pouvoir définir des tendances.

3. **Sensibilise-t-on également les populations techniques (informaticiens, administrateurs systèmes & réseau, administrateurs de bases de données…)**
   Parce qu'elles sont dotées de connaissances plus pointues et d'accès plus larges aux systèmes, les populations techniques sont parfois plus à risque que les collaborateurs non-techniciens.

4. **Fait-on émarger les collaborateurs ayant suivi une action de sensibilisation ?**
   Les auditeurs peuvent demander à consulter les preuves de l'organisation de séances de sensibilisation régulières au sein de l'entreprise.

5. **Archive-t-on les supports de sensibilisation (vidéo, messages, brochures, affiches…) ?**
   Toujours dans une optique de justification vis-à-vis des auditeurs.

racontait l'histoire de cette petite entreprise ayant fait faillite à la suite du blocage de son Système d'Information par un virus de type « crypto-locker »… Nous sommes bien désormais tous concernés, à titre personnel comme au titre de nos fonctions de salarié, de cadre ou de dirigeant d'une organisation. Il nous faut passer collectivement et individuellement d'une sensibilisation lointaine à une action de protection concrète, bâtie sur le socle d'une culture du risque cyber. Sans devenir paranoïaque, en étant simplement informé et vigilant. « *Sur Internet, je reste en alerte* » comme le dit la hack Academy ! ■

[4] Colloque annuel lancé par le Sénateur Maire de Fleurance (Gers) et organisé avec la Réserve Citoyenne de cybersécurité et la Gendarmerie

12

Horizon 2020 : les priorités du CODIR

Par Jérôme Saiz.

Jérôme Saiz est consultant expert en protection des entreprises et fondateur de la société OPFOR Intelligence. Il travaille sur la convergence des protections logiques et physiques au sein des organisations.

De quoi pourra-t-on bien parler dans les réunions des Comités de Direction en 2020 ? La cybersécurité sera-t-elle encore à l'ordre du jour ?

Pour tenter de le découvrir, glissons-nous dans la salle de réunion du CODIR d'un grand groupe, au printemps 2020. Y parle-t-on encore de cybersécurité ? Non. Du moins pas directement.

Le groupe a décidé, en 2016, d'entamer une réflexion globale sur sa protection. Cela s'est notamment traduit par une sérieuse optimisation de fonctions qui, jusqu'à présent, contribuaient à protéger ses actifs en ordre dispersé.

Qu'il s'agisse du service informatique, de la sécurité des systèmes d'information (SSI), du service juridique, de la Communication ou de la Sûreté, le groupe a réalisé que tous étaient susceptibles d'être impliqués dans la préservation de ses actifs, qu'il s'agisse de ses collaborateurs, mais aussi de son image, de sa protection juridique ou de ses informations sensibles.

Deux facteurs ont contribué à cette prise de conscience au sein du groupe. Le premier est interne : l'impulsion donnée par le mouvement de transformation numérique de l'entreprise a mis en lumière le caractère parfois artificiel de la distinction entre les métiers et les fonctions support, en particulier la SSI *(voir le chapitre 5, "La cybersécurité, ingrédient majeur de la transformation numérique").*

Le second facteur est externe : une attaque ciblée sophistiquée a visé le groupe au début de l'année

« Les attaquants ont mené des intrusions physiques et cyber parfaitement coordonnées »

« La direction sécurité groupe offre à l'année les atouts d'une cellule de crise : focus sur la mission et pluridisciplinarité »

2016. Les attaquants ont mené des intrusions physiques et cyber parfaitement coordonnées, associées à des pressions physiques à l'encontre de collaborateurs clés identifiés grâce à leurs publications sur les réseaux sociaux. Des données extrêmement sensibles ont été dérobées et des informations à caractère personnel ont été diffusées dans le but de nuire au groupe. L'impact a été violent sur tous les fronts : il a fallu se défendre face à l'opinion publique, à la presse, à la justice et aux pirates eux-mêmes, parvenus à conserver un accès persistant aux systèmes. Il a ensuite fallu déterminer l'étendue de la brèche et identifier les informations dérobées, tout en collaborant avec les autorités et les services de l'État afin de déterminer l'implication éventuelle d'un concurrent étranger.

Mais cet événement a également été le cadre d'une prise de conscience : à voir ainsi travailler la Communication, le Juridique, la Sûreté et la SSI au sein d'une cellule de crise, certains cadres du groupe ont commencé à se demander pourquoi il fallait attendre une crise pour réunir toutes ces fonctions autour d'une mission commune de protection des intérêts du groupe. Ne pourrait-on pas bénéficier de cette synergie toute l'année ?

La route est longue

Evidemment la route fut longue jusqu'à ce CODIR de 2020. Il a tout d'abord fallu repartir en amont des analyses de risque existantes et créer un cadre formel qui permette d'associer de manière extrêmement modulaire les actifs, les menaces associées et les apports potentiels des métiers ou des fonctions support susceptibles de contribuer à leur protection.

Technologie, dépendances aux tiers, canaux de distribution, flux de production, organisation interne, menaces externes, contrats... tout y passe. L'approche de la Sûreté qui consiste à raisonner en termes de croisement des flux (humains, matériels, produits finis, valeurs) s'est ici révélée précieuse.

Réfléchir à un tel modèle a vite permis de mettre en évidence la nécessité d'une communication horizontale efficace afin de partager en temps quasi-réel les informations relatives aux menaces, aux changements stratégiques ou tactiques susceptibles d'avoir un impact sur la sécurité ou d'exposer à de nouveaux risques, ou bien encore de remonter des alertes face à une déviation du standard.

Et il a fallu se rendre à l'évidence qu'une telle horizontalité dans les échanges serait difficile à atteindre avec l'organisation en silos actuelle. Et qu'elle ne se justifiait d'ailleurs pas nécessairement dans tous les domaines.

Pour être viable cette ébauche de framework de sécurité globale devait donc s'incarner au sein d'une structure adaptée. C'est pourquoi l'un des premiers chantiers organisationnels a été de créer une Direction Sécurité Groupe ou l'horizontalité et la multi-disciplinarité y régnerait en maître.

Une telle direction est, par exemple, la plus à même de prévenir efficacement une fuite de données massive en coordonnant les mesures nécessaires à la fois avant, pendant et après les projets. Elle peut ainsi intervenir depuis l'identification des initiatives sensibles jusqu'au choix des solutions techniques de prévention, en passant par les consignes juridiques de moindre exposition, l'audit des

réalisations, la contractualisation avec les prestataires ou la sensibilisation des métiers. Et elle le fera d'une manière extrêmement agile en communiquant en temps réel en son sein.

A bien y regarder il s'agit, en définitive, de pérenniser les atouts d'une cellule de crise au sein d'une structure bâtie sur un cadre formel et appuyée sur des critères d'évaluation clairs.

Se protéger en meute

La tâche est complexe, mais il n'est toutefois pas nécessaire de mener cette réflexion seul. Les acteurs de même taille au sein de la même industrie connaissent probablement les mêmes contraintes, et ils subissent certainement les mêmes attaques. Pourquoi alors ne pas échanger des informations avec eux ?

Se protéger "en meute" permet notamment d'anticiper sur les attaques à venir, lorsque celles-ci ont déjà frappé un membre de la communauté. Couplée à la notion de benchmarking (s'évaluer par rapport aux bonnes pratiques d'acteurs de son domaine), cette approche collaborative a permis au groupe d'entrer dans une dynamique vertueuse avec certains de ses "coopétiteurs" présents dans la même industrie, voire sur les mêmes marchés (la coopétition étant l'art de coopérer avec ses concurrents sur un périmètre clairement défini et mutuellement profitable).

Des échanges sur les acteurs malveillants, les modes opératoires et les menaces en cours dans sa propre industrie contribuent grandement à la capacité d'anticipation du groupe et permettent de mieux prioritiser ses efforts de protection.

Mais partager sans maîtriser peut s'avérer risqué. Et si les premières initiatives de partage d'information se sont révélées fructueuses, le groupe a ressenti le besoin de mieux maîtriser l'information, à la fois celle qu'il échange aves ses partenaires, mais aussi celle qu'il collecte. Et c'est ainsi que deux ans après le début du projet est venue s'y greffer une composante de veille et d'analyse.

En étant constamment à l'écoute à la fois des métiers (pour servir leur besoin d'information) et de l'écosystème concurrentiel, la veille est un chaînon idéal entre l'entreprise et le monde extérieur. Elle permet en outre, au delà de répondre aux besoins d'information des métiers, de faire remonter de précieux éléments de sécurité et de sûreté du terrain.

Pour que les informations remontées par la veille puissent être exploitées, il est nécessaire de les analyser. L'intégration de la fonction analyse à la direction sécurité a ainsi permis de faire bénéficier cette dernière d'une vision précise et à jour des facteurs extérieurs susceptibles d'impacter le groupe, ce qui en retour lui permet d'adapter immédiatement la posture de sécurité en conséquence. Une telle agilité et un tel niveau d'anticipation n'aurait jamais été possible sans la coordination naturelle apportée par un positionnement au sein de la direction sécurité groupe.

L'information maîtrisée

Un autre gain, imprévu celui-ci, a été obtenu par l'intégration d'une véritable fonction de veille et d'analyse à la direction de la sécurité : le groupe a découvert, non sans une certaine gêne, qu'il laissait "fuir" - à travers ses publications sur Internet notamment - une quantité non négligeable d'informations publiques qui, pour un adversaire compétent, pouvait permettre par recoupement d'obtenir des renseignements précieux.

« Se protéger en meute permet d'anticiper sur les attaques à venir »

Bien que le groupe n'ait pas décidé d'utiliser cette nouvelle capacité de veille à des fins offensives (après tout, s'il laissait fuir des informations il est fort probable que certains concurrents en fassent autant !), cela lui a tout de même permis de colmater ses propres fuites involontaires.

Notre CODIR de 2020 touche à sa fin. A-t-on prononcé le mot "cybersécurité" ? Pas vraiment. En a-t-on parlé ? Constamment.

L'omniprésence de l'outil informatique a fait de sa protection une évidence : la sécurité des systèmes d'information irrigue tous les projets, au sein de toutes les directions. Même les outils historiques de la sûreté, du contrôle d'accès à la vidéosurveillance, reposent désormais sur des réseaux informatiques qu'il est nécessaire de protéger.

La transformation numérique traversée par le groupe a, quant à elle libéré les données et créé de la valeur nouvelle à travers des API et de nouveaux usages numériques, seulement rendus possibles par un socle fort de sécurité numérique *(voir le chapitre 5)*.

En 2020, la cybersécurité est ainsi clairement une priorité du CODIR. Elle est au cœur de toutes ses discussions... sans pour autant qu'il y ait besoin de prononcer son nom ! ■

Pour anticiper

1. Identifiez l'intégralité des actifs générateurs de valeur.

2. Sachez mesurer leur niveau de protection face à des menaces à la fois logiques et physiques.

3. Mettez en place des exercices de crise réunissant les services informatiques, la SSI, la communication et le juridique.

4. Assurez-vous d'allouer suffisamment de ressources à la cybersécurité.

5. Mettez en place un système formel d'évaluation de l'efficacité de votre programme de cybersécurité.

6. Assurez-vous que la cybersécurité soit prise en compte dans toutes les initiatives prises par les métiers.

7. N'abordez pas votre transformation numérique sans une visibilité claire sur l'efficacité de votre programme de cybersécurité.

V Témoignages

13

Les stratégies de cyberdéfense de l'OTAN

Par Ian West

Ian West est directeur de la cellule de lutte contre la cybercriminalité au sein de l'agence de l'OTAN pour la Communication et l'Information (NCI).

Nous sommes véritablement en première ligne dans la lutte contre les cyberattaques. Il ne se passe pas un jour, une heure, une minute sans que nous identifions différents niveaux de menace. Nous devons donc être vigilants et réactifs pour résister à des attaques dont l'intensité et le degré de complexité ne cessent d'augmenter.

La cyberdéfense fait partie des tâches fondamentales de l'OTAN et ceci, pour deux raisons : d'abord parce que l'Alliance est dépendante de son infrastructure de TIC, et ensuite parce que l'informatique, déjà partie intégrante des conflits, constituera inévitablement un composant de plus en plus important dans les conflits à venir.

La bonne nouvelle est que pratiquement toutes les entreprises en exercice actuellement ont fait de la cyberdéfense l'une de leurs priorités.

Nous dépendons tous de nos réseaux, utilisons tous une technologie similaire et faisons tous face à des menaces similaires. Pour cette raison, l'OTAN s'est très rapidement inscrite dans une démarche collaborative, notamment avec les différents secteurs de l'industrie, pour lutter contre ceux qui cherchent à ébranler et à détruire nos modes de vie *(lire le chapitre 12, « Horizon 2020 : les priorités du CODIR » pour découvrir tout l'intérêt d'une approche collaborative à la cybersécurité).*

« La cybersécurité est une valeur forte de l'OTAN »

L'OTAN, en sa qualité d'Alliance transatlantique composée de 28 (et bientôt 29) nations, partage les valeurs que sont une défense collective puissante et la protection des territoires et populations de ses membres.

La cybersécurité fait partie de ces valeurs.

En vertu des dispositions fondamentales de son traité, l'Alliance se tient prête à agir d'une même voix et à prendre les décisions nécessaires pour défendre la liberté, et les valeurs communes que sont les libertés individuelles, les droits de l'Homme, la démocratie et l'État de droit.

De nos jours, le Dark Web (ou Web sombre) attire un nombre sans cesse croissant de personnes et d'organisations malveillantes. Ces utilisateurs y collaborent entre eux, affinent leurs compétences et s'organisent.

C'est entre autres sur cette face cachée du Web qu'ils se rassemblent pour commettre leurs opérations cybercriminelles.

« Nous nous concentrons sur la détection des attaques ciblées »

Celles-ci peuvent être de différents types, et représenter des menaces très diverses. Nous recensons par exemple les menaces non spécifiques, comme les logiciels malveillants qui vont infecter les systèmes, et les menaces spécifiques, qui sont des attaques dirigées contre l'OTAN et sur lesquelles nous nous concentrons plus particulièrement.

L'auteur de ces attaques spécifiques peut être une nation hostile ou des criminels organisés qui préparent des attaques pour inciter les utilisateurs à cliquer sur un lien et à ouvrir un document infecté, et ainsi accéder à nos systèmes et à nos informations stratégiques. Ces dernières années, la fréquence et la complexité de ce type d'attaque se sont accentuées. Avec un ordinateur portable et un minimum de connaissances, un attaquant peut accéder à votre organisation et causer d'importants dégâts.

Mais l'on trouve également des « hacktivistes » aux aspirations politiques ou sociales souvent radicales, qui piratent le site Web d'une organisation pour y publier des messages illicites, bloquer l'accès au site ou subtiliser des informations confidentielles. Ils s'en prennent de plus en plus souvent à des sociétés commerciales, à des organisations non gouvernementales ou à des gouvernements pour les railler, les ridiculiser ou détruire des réputations.

Ensuite, il existe les menaces internes dont nous, les utilisateurs, sommes à l'origine. Nous pouvons en effet causer de graves incidents de sécurité, que ce soit de façon délibérée ou non.

Toutes ces menaces démontrent que les réseaux peuvent être affectés tant de l'extérieur que de l'intérieur. Il est donc indispensable de pouvoir également détecter les attaques depuis l'intérieur des réseaux.

Au sein de l'OTAN, notre travail consiste à prévenir au mieux de tels incidents, mais nous n'y parvenons malheureusement pas à 100 %. Nous devons donc être en mesure de détecter ces incidents, d'y répondre et de permettre ensuite la reprise des activités normales *(pour en savoir plus au sujet de la réponse aux incidents, lire le chapitre 9, « Faute de pouvoir empêcher les cyberattaques, les entreprises doivent être en mesure de riposter »).*

Il est également important que nous puissions retrouver les personnes à l'origine de ces attaques ciblées, et découvrir leurs motivations. Ainsi, lorsque une attaque se produit nous procédons à des recherches approfondies et examinons chaque pièce du puzzle afin d'identifier les auteurs d'une attaque et leur objectif.

Un programme de cyberdéfense efficace

Les stratégies suivantes sont éprouvées et nous les utilisons pour limiter les risques en cas de cyberattaques. Elles pourront servir d'inspiration à la mise en œuvre d'un programme efficace de cyberdéfense.

1. Identification des ressources stratégiques de l'entreprise

Il est impossible de vous protéger à 100 % des cyberattaques. À l'OTAN, nos commandants en sont pleinement conscients. La cybersécurité est relativement onéreuse. À l'instar des organisations commerciales, nous ne pouvons pas nous permettre de tout protéger avec le même niveau de protection.Nous devons néanmoins déployer des cyber-ressources, limitées et onéreuses, en nous basant sur l'évaluation des risques pesant sur l'ensemble de l'entreprise.

Pour identifier nos ressources stratégiques et nos forces, nos commandants se posent les questions suivantes :

- Quelles sont les informations les plus importantes que nous détenons ?
- Quels sont les services les plus importants que nous proposons à nos clients, et quels cyber-risques leur sont liés ?
- Où protégeons-nous les informations relatives à nos processus et à notre entreprise ?
- Sont-elles sécurisées ?
- Comment continuer à évaluer et à surveiller les risques ?
- Disposons-nous d'un registre sur les cyber-risques ?
- Comment répondons-nous à chaque type de risque ?

Bien entendu, il est pour cela nécessaire de connaître parfaitement le degré de risque que l'entreprise est prête à prendre. Une fois ce point défini, il est alors possible de planifier, de mettre en œuvre et d'évaluer les contrôles et procédures de sécurité.

2. Sécurité préventive

Au sein de l'OTAN, nous mettons tout particulièrement l'accent sur la sécurité préventive. Car comme le dit si bien le proverbe, « *mieux vaut prévenir que guérir* » !

Nous nous attachons pour cela notamment à renforcer la sécurité et les réseaux, et à limiter la surface d'attaque d'un grand nombre de menaces. La stratégie de réduction de la surface d'attaque (ASR) a pour but de bloquer toutes les portes d'accès non essentielles à l'infrastructure technique et de limiter l'accès aux portes ouvertes par le biais d'une surveillance, d'une évaluation des risques et d'un contrôle des accès permanent.

A l'OTAN nous appliquons la méthode suivante : prévenir, détecter, répondre et reprendre. Le tout formant un processus itératif.

Enfin, bien que nous parlions ici de prévention, n'oublions pas que les attaques de type « zero day », qui visent les vulnérabilités jusque-là inconnues d'un logiciel, sont quasi impossibles à bloquer à 100 %. Il restera donc toujours un élément de risque quel que soit le degré de prévention / protection mis en place.

Mais il est malgré tout possible d'adopter certaines mesures afin de limiter ce type d'attaque :

- Analysez les menaces existantes. De nombreuses informations sur le renforcement de la sécurité des systèmes sont disponibles et peuvent être implémentées gratuitement *(pour en apprendre plus sur l'intérêt d'une veille efficace, reportez-vous au chapitre 12).*
- Vérifiez, autant que possible, la robustesse et l'adéquation des technologies et des méthodes de chiffrement déployées chez vous.
- Si vous ne possédez pas les capacités ou les ressources nécessaires pour procéder à une analyse approfondie de tous les logiciels exploités chez vous, faites réaliser un audit ou un échantillonnage des principaux points de tension.

- Procédez aussi souvent que possible à des vérifications standard, à des évaluations de la vulnérabilité et à des tests de pénétration.
- Définissez des protocoles de formation sur les modalités d'utilisation des technologies et des appareils mobiles personnels par les employés sur leur lieu de travail.
- Définissez le plan à suivre en cas de problème.

Ces mesures vous aideront à détecter tous les éléments infectés et exploités *(par des pirates)* au sein de votre organisation.

3. Capacité de réponse

Notre cyberdéfense n'est pas forcément parfaite. Des violations de notre cyberespace sont possibles. L'important est toutefois de pouvoir identifier très rapidement l'intrus et les dommages potentiels, et de pouvoir y remédier rapidement.

Si vos systèmes ont été infectés à la suite d'une attaque ou d'une violation de sécurité, gardez votre sang-froid. Le plus important est la réponse que vous donnerez à l'incident.

Votre entreprise doit faire preuve d'une forte capacité de résilience et disposer de solides solutions de sauvegarde. Au sein de l'OTAN, nos équipes chargées de gérer les incidents sont à même de répondre immédiatement à une attaque sur nos différents systèmes et d'en limiter ainsi les effets.

Ces équipes peuvent être envoyées sur site ou travailler en ligne pour restaurer les services ayant fait l'objet d'une attaque.

4. Capacité de reprise

Vous devez également être à même de rétablir rapidement le fonctionnement normal des services. Ce point est tout particulièrement important.

Vous devez en effet prouver rapidement à vos clients que vos systèmes sont à nouveau accessibles et sécurisés.

Là encore, le partage d'informations sur les attaques (lire plus haut) facilite la reprise des activités. Autour du globe, on trouve des similitudes entre les organisations et entreprises qui utilisent des systèmes identiques et subissent le même type d'attaques.

Il est également intéressant de communiquer et de partager ses expériences avec des tiers de confiance et les organismes judiciaires.

Plus ce partage d'expérience est important, plus nous disposons d'informations sur les attaquants.

5. Répondre au manque de compétences

Dans le monde entier, les personnes qualifiées, capables de protéger nos libertés et notre société civile contre les cyberattaques, sont trop peu nombreuses.

Les dirigeants doivent être conscients qu'une telle tâche nécessite des compétences hautement spécialisées et que les experts capables de cerner la moindre vulnérabilité sont très recherchés.

Cette demande est valable dans les secteurs commercial, militaire, public et gouvernemental.

En 30 ans d'expérience dans le domaine de la sécurité, j'ai vu la position du responsable sécurité évoluer. Le mordu de technologie qui répondait autrefois « NON ! » avant même d'écouter la question, n'est plus aussi répandu. Il faut dire que ces « gardiens » n'étaient pas très utiles au reste de l'entreprise, d'où leur surnom de *« gendarme endormi de l'autoroute de l'information » (ou d'empêcheurs de travailler, selon les métiers).*

Aujourd'hui ils ont fort heureusement laissé leur place à une nouvelle catégorie de professionnels de la sécurité beau-

coup plus engagés et en phase avec les besoins de la société.

Des reliquats de ce type d'attitude subsistent certes encore parfois à l'heure actuelle, mais la plupart de nos cyber-défenseurs les plus compétents sont désormais des personnes plus jeunes, qui ont baigné très tôt dans les jeux vidéo, le piratage licite et la programmation informatique.

Si vous souhaitez obtenir des résultats solides et approfondis, il est vital de s'entourer d'une équipe aux expériences et aux parcours variés, composée tant de vétérans que de jeunes nés à l'ère de la connectivité informatique.

L'importance stratégique de plus en plus marquée de l'infrastructure numérique a conduit à une véritable révolution qui a propulsé les experts en sécurité de l'information au cœur même du processus de prise de décisions. En retour, cela implique toutefois que ces experts soient en mesure de s'exprimer dans un langage compréhensible par les autres cadres et de comprendre les stratégies de l'entreprise. Il s'agit donc d'un nouveau profil à rechercher *(lire à ce sujet le chapitre «Définir le profil du RSSI 3.0 »).*

6. Collaboration avec des entreprises de confiance

Depuis longtemps, l'OTAN a compris que quel que soit son propre niveau de compétence, il est impossible d'avoir une bonne vision d'ensemble. La collaboration est donc incontournable.

Nous travaillons notamment au côté de l'Alliance et de ses 28 alliés et États membres. Depuis la Déclaration du sommet du Pays de Galles en septembre 2014, un paquet « Planification de défense » a d'ailleurs été voté pour renforcer les capacités des membres de l'Alliance.

Depuis, la cyberdéfense figure parmi les priorités de l'OTAN.

Par ce paquet, l'OTAN reconnaît que les cyberattaques peuvent atteindre un seuil qui menace la prospérité, la sécurité et la stabilité nationales. Leur impact peut être aussi dramatique pour les sociétés modernes qu'une attaque conventionnelle.

À l'OTAN, la cyberdéfense est donc devenue une tâche fondamentale de la défense collective. Dans cette organisation, nous nous attachons à développer des possibilités de cyberdéfense nationales et d'améliorer la cybersécurité des réseaux nationaux sur lesquels l'OTAN s'appuie pour ses tâches fondamentales.

Une collaboration bilatérale et multinationale joue un rôle majeur dans le renforcement des possibilités de cyberdéfense de l'Alliance.

La solidité des partenariats est essentielle et l'OTAN continue à s'engager activement sur ce type de problème informatique auprès des nations partenaires concernées.

Les innovations et l'expertise technologiques du secteur privé sont essentielles, car elles permettent à l'OTAN et aux alliés d'atteindre les objectifs fixés par la politique de cyberdéfense renforcée.

Une collaboration public-privé est indispensable

Souvent, le secteur privé comprend mieux la technologie que nous, et parvient à identifier l'origine de ces menaces. Ces dernières années, nous avons donc développé et renforcé des relations avec les entreprises, et conclu notamment des accords de partage d'information.

Nous échangeons et travaillons activement pour partager nos informations sur les vulnérabilités. Nous appelons ce quatrième vecteur d'avancée la « défense intelligente ». L'OTAN a signé un mémorandum d'entente avec un certain nombre d'entreprises

du secteur privé. Cette expérience s'est révélée très profitable au fur et à mesure du développement de ce partenariat.

Par ailleurs, l'OTAN a renforcé ses activités d'éducation, de formation et ses exercices sur la cyberdéfense au sein de sa propre école, l'École des systèmes d'information et de communication, et dans le cadre de partenariats avec d'autres établissements de formation et d'enseignement.

Dans cette ère du numérique, l'une des seules choses prévisibles est qu'un événement imprévisible se produira cette année. Votre entreprise doit donc être en mesure de départager le « certain » de l'«incertain »…

Protéger votre entreprise contre les cyberattaques est un problème crucial qui concerne chacun de nous, quel que soit notre niveau. Unissons donc nos forces. ■

14

Comment mesurer l'efficacité de votre programme de cybersécurité ?

Par Alan Jenkins et Greg Day

Alan Jenkins est l'ancien RSSI d'une entreprise cotée au FTSE100 et associé d'IBM Security. Greg Day est Vice-Président et CSO EMEA chez Palo Alto Networks, responsable de la stratégie de cybersécurité et du développement de la Threat Intelligence.

Le PDG de votre entreprise est en phase de négociations avancées au sujet d'une acquisition importante. Il souhaite en effet acquérir un réseau social en pleine croissance qui s'appuie sur ce qui semble être une nouvelle technologie intelligente.

Cette acquisition est décisive.

Le directeur financier et le responsable du service juridique ont examiné la situation avec toute la diligence nécessaire. Les chiffres et les actifs qui leur ont été présentés, dont la propriété intellectuelle, leur semblent intéressants.

Le directeur marketing est certain que cette acquisition boostera les ventes.

Pourtant, dans la salle de négociations, le RSSI déclare : *« Attendez ! Cette société pose de nombreuses questions en matière de cybersécurité. »*

Tout le monde est conscient que la question de la cybersécurité est décisive pour les entreprises. Mais vous-même, dans une situation similaire, quelle importance accorderiez-vous à ce que pense votre RSSI au sujet d'une décision aussi stratégique ?

De plus, les membres du Conseil d'administration (qui sont rarement au fait des dernières technologies – *lire le chapitre 12 à ce sujet)* sont-ils véritablement à même de mesurer objectivement la réussite ou même simplement la qualité du programme de cybersécurité mise en place par votre RSSI ?

Dans l'exemple précédent, le RSSI considère que la propriété des données du client est discutable, que le logiciel est truffé de défauts, et que le coût lié à l'aménagement de l'infrastructure existante risque d'être

supérieur au coût de rachat de l'entreprise.

Prenez-vous son avis en compte ou l'ignorez-vous, en considérant que votre RSSI ou votre DSI pourront procéder aux aménagements nécessaires après l'acquisition ?

Dans une situation similaire que nous avons vécue au sein d'une entreprise cotée au FTSE100, la solution a consisté à souligner les risques sous-jacents sans pour autant interrompre le processus d'acquisition. Il a ainsi été convenu que la nouvelle entreprise serait exploitée de façon autonome jusqu'à ce que l'équipe en charge des technologies puisse « nettoyer » l'infrastructure informatique de la nouvelle entité.

Après cela seulement, diverses formes d'intégration ont pu être envisagées. Le coût de l'acquisition a certes été considérablement augmenté, mais le Conseil d'administration a estimé qu'un tel surcoût était nécessaire.

Il faut cependant reconnaître qu'une telle décision est pour le moins inhabituelle. Votre propre Conseil d'administration est-il capable d'entendre de tels arguments et prendre de telles décisions ?

Il est pourtant crucial, dans un tel contexte, de pouvoir vous appuyer sur le niveau de leadership informatique nécessaire.

Tiendrez-vous compte de l'avis négatif de votre RSSI ?

Toutes les entreprises n'ont pas atteint le même stade de cybermaturité.

Certaines sont plus matures sur le plan informatique que d'autres.

Cela conduit à se poser deux questions fondamentales :

- Le niveau de notre direction de la sécurité informatique est-il suffisant au regard des besoins de notre entreprise ?
- Devons-nous faire appel à un conseiller en fusions/acquisitions à même de répondre à nos questions d'ordre stratégique, ou avons-nous seulement besoin d'un expert technique ?

Il appartient au Conseil d'administration de décider du niveau de sécurité à atteindre. Ce niveau dépendra de la technologie exploitée et de l'environnement réglementaire dans lequel l'entreprise évolue. Vous pourrez alors déterminer plus précisément ce que vous attendez de votre Directeur de la sécurité du SI (DSSI) avant de le nommer.

Evaluer son DSSI sur la crise

Lors de la nomination à un tel poste demandez au futur DSSI de souligner les risques informatiques qui pèsent sur l'entreprise mais dont les autres membres du Conseil n'avaient pas connaissance, et évaluez la pertinence de sa réponse.

À ce stade, une décision doit être prise : confirmer ou non la nomination. Mais comment être véritablement certain que le DSSI retenu sera suffisamment compétent pour siéger au Conseil d'administration ?

Pour mesurer sa réussite, l'idéal serait d'étudier de quelle manière il a su répondre à une situation de crise. Mais il y a fort à parier que les membres du Conseil d'administration demanderont à être rassurés bien avant qu'une situation de crise ne se pose ! De plus, il est préférable qu'un tel directeur soit en place aux premières heures de la crise, si tel devait être le cas.

Des exercices de crise comme indicateurs avancés

Cela nous amène aux indicateurs. De nombreux indicateurs permettent de mesurer le niveau de cybersécurité de votre entre-

« Il peut être décourageant de rechercher le bon RSSI ! »

prise, mais tous ne coïncident pas parfaitement avec le cycle de l'entreprise.

Beaucoup d'indicateurs correspondent généralement à ce qu'on a coutume d'appeler les « *indicateurs décalés* » : ceux-ci présentent en effet des événements passés. Ils offrent donc un éclairage sur des faits antérieurs.

En général, ces indicateurs décalés sont regroupés sur un tableau de bord de sécurité. Des témoins de couleurs rouge, orange et verte y indiquent le nombre de systèmes protégés par un antivirus, le nombre de correctifs déployés et le nombre de logiciels malveillants bloqués, etc.

La plupart de ces statistiques mesurent de manière factuelle ce qui s'est passé et non l'incidence de ces événements sur la protection de l'entreprise face aux événements à venir.

Par exemple, le calendrier de déploiement des correctifs a été respecté sur tous les systèmes : l'indicateur est alors au vert. D'autres indicateurs peuvent indiquer le nombre de systèmes antivirus en place ou de mots de passe fiables vérifiés, mais aucun ne donne d'informations directes sur la probabilité et l'impact d'une attaque ciblant l'entreprise *(ils doivent pour cela être exploités dans le cadre d'une analyse de risque formelle).*

Des indicateurs « avancés» tournés vers la préparation à la crise

Mais il peut être difficile pour les membres du Conseil d'administration d'anticiper des événements en s'appuyant uniquement sur des performances passées. Pour cette raison, il est plus intéressant de disposer d'indicateurs dits « avancés », plus évolués et tournés vers l'anticipation.

Mais comment quantifier de tels indicateurs avancés ? Car ceux-ci doivent, par définition, tenir compte du caractère incertain de la cybersécurité et (souvent également) son caractère aléatoire…

Une marge d'anticipation très réduite

Dans une entreprise traditionnelle, la mise au point d'un nouveau produit, sa mise en production et sa commercialisation prennent en général 12 mois minimum. Mais il faudra cependant souvent bien moins de six mois à une personne malveillante pour identifier les faiblesses de votre entreprise et s'introduire dans son système d'information. Et malheureusement les membres du Conseil d'administration ont parfois du mal à apprécier cette nouvelle dynamique, car ils ne sont pas habitués à une évolution aussi rapide.

Les indicateurs avancés pourront contribuer à donner au Conseil d'administration une vision du caractère dynamique de la cybersécurité.

Ils illustreront la manière dont l'équipe informatique répond aux événements et limite les temps d'arrêt de l'activité ou encore comment vos dispositifs de défense ont été conçus et déployés dans l'entreprise. En clair, les indicateurs avancés sont de méta-indicateurs : ils s'intéressent aux capacités d'action de votre programme cybersécurité (à travers ses ressources, son organisation et son leadership) plutôt qu'à ses réalisations passées.

L'équipe de cybersécurité en première ligne

Dans le cas d'une cyberattaque l'équipe en charge de la sécurité doit affronter le problème jusqu'à ce que le danger soit contenu, sous contrôle et si possible, éliminé. L'un des indicateurs avancés, pertinent ici, est le temps nécessaire à la résolution

d'une crise ou d'une attaque, car il donne, entre autres, une estimation de la qualité du leadership de la fonction cybersécurité.

Mais à l'inverse d'une attaque très visible, il se peut qu'une attaque présentant de faibles risques n'ait pas été détectée pendant plusieurs années, mais que son impact à long terme soit très important.

Une fois celle-ci identifiée, un indicateur décalé permettra certes ici de « remonter le temps » et de mesurer l'impact sur les actifs de l'entreprise *(quels systèmes étaient corrigés, à quel moment, etc.).* Mais pour en faire un indicateur avancé, il vous faudra alors vous en servir pour modéliser un nouveau scénario d'attaque et le faire « jouer » par des tests et des exercices proactifs afin de confirmer (ou améliorer !) la capacité d'action de votre équipe de cybersécurité.

Pensez également à associer à ces exercices le porte-parole du conseil d'administration, épaulé par les équipes des services juridique et RH. Cela permettra, entre autres, de rendre compréhensibles par les autres membres de l'entreprise l'action et la méthodologie de l'équipe de cybersécurité.

On peut comparer cette approche au fait d'utiliser directement un extincteur pour éteindre un incendie au lieu d'actionner l'alarme incendie qui est au mur.

La mise en place de tels exercices est plus percutante et aide tous les membres de l'entreprise, à tous les niveaux, à comprendre qu'ils ont un rôle à jouer.

Le Conseil d'administration dispose alors d'une vision plus claire (un indicateur avancé) sur l'organisation, le fonctionnement et l'efficacité des mesures de cybersécurité en place. Il lui sera alors possible de déterminer plus aisément la valeur commerciale potentielle d'un nouvel investissement en cybersécurité lorsque le service SSI en fera la demande.

Souvenez-vous également que sur le plan de la gouvernance – et selon le concept de la défense en profondeur - la cybersécurité ne doit pas relever de la seule responsabilité du RSSI / DSSI, mais de l'ensemble de l'organisation. La SSI « n'est que » le responsable exécutif et le maître du projet, à l'échelle de l'entreprise. C'est pourquoi le conseil d'administration doit avoir, à son niveau, une vision claire des actions prises pour protéger l'entreprise.

Grâce à ces informations, le conseil d'administration peut se poser les questions suivantes :

- Nous sommes-nous améliorés ?
- Le délai séparant une attaque et sa détection a-t-il été réduit ?
- Le déploiement des correctifs est-il plus efficace ?
- Notre entreprise est-elle plus sécurisée ?

Ne pas oublier la continuité d'activité

Un point important à contrôler est l'intégration de vos scénarios de crises cyber à votre programme de continuité d'activité (car celui-ci n'est pas tombé dans l'oubli, n'est-ce pas ?). Vous devez absolument vérifier que tous les détails, comme par exemple les coordonnées des dirigeants, des partenaires et des prestataires à contacter, sont à jour en cas de cyberattaque.

Bien entendu, il n'existe aucune garantie de réussite. Vous pouvez dépenser des fortunes pour doter l'entreprise des toutes

« Toutes les entreprises n'ont pas atteint le même stade de cybermaturité. »

dernières technologies et faire malgré tout l'objet d'une attaque si l'un des employés, en ouvrant un e-mail, clique sur un lien contenant un cheval de Troie.

La sécurité à 100% n'existe pas : ne demandez pas la tête de votre RSSI !

Ce rappel n'est en rien une excuse en cas d'échec, mais une réalité : la sécurité ne peut pas être garantie à 100 %. Et pourtant, la première tête à tomber lors d'une attaque est souvent celle du DSSI / RSSI, car la Direction s'attend (à tort) à ce qu'ils bloquent toutes les attaques. C'est absurde : il n'existe en réalité jamais de mauvaise réponse à une cyberattaque, mais que des enseignements pour l'avenir.

Nous apprenons tous de nos erreurs. Il serait donc vraiment déplacé de sacrifier votre RSSI, sauf à prouver sa négligence ou sa malveillance manifeste.

Appuyez-vous sur cette expérience pour améliorer vos défenses pour l'avenir, car il y aura très certainement « une prochaine fois » ! ■

Pour anticiper

1. **Faites intervenir votre RSSI durant certains comités de direction**
   Si vous n'avez pas nommé de DSSI au comité de direction, il est profitable que les membres du CODIR connaissent tout de même votre RSSI et que celui-ci puisse y présenter régulièrement ses actions et leur impact sur la protection des actifs de l'entreprise.
2. **Organisez des visites de votre SOC pour les membres du CODIR**
   Si vous disposez d'un SOC (Security Operations Center) ou tout autre lieu dédié à la surveillance continue de votre cyber-sécurité (y compris s'il est externalisé), organisez une visite des membres de votre comité de direction, afin qu'ils prennent conscience de l'infrastructure nécessaire et des processus humains qui sont en jeu en matière de cyberdéfense.
3. **Faites réaliser un point sur les indicateurs à votre disposition**
   Avant de chercher à améliorer le fonctionnement de votre programme de cybersécurité, vous allez avoir besoin d'une vision objective de l'existant. C'est le bon moment pour recenser les tableaux de bord et les indicateurs existants, ainsi que l'organisation de votre SSI.

Les auteurs

GREGORY ALBERTYN

Gregory Albertyn est Directeur senior. Il est spécialiste des questions de conformité réglementaire et de l'optimisation des processus de gouvernance des données. Il était auparavant Global Privacy Officer pour Biogen, une société américaine de biotechnologie. ■

AVI BERLINER

Avi Berliner est responsable dans le domaine des services financiers, de la stratégie applicative et de l'intégration. Il a travaillé auparavant chez Standard & Poor's en tant que Data Associate et Directeur des solutions & architectures IT. Il est diplômé de la Polytechnic School of Engineering de l'Université de New-York. ■

Plus d'information :
- https://www.pwc.fr
- https://twitter.com/pwc_france

ALAIN BOUILLE

Alain Bouillé est le Directeur de la Sécurité des Systèmes d'Information du Groupe Caisse des Dépôts depuis 2001. Il est en charge de l'élaboration de la politique de sécurité du Groupe, de la coordination et du pilotage de sa mise en œuvre dans les entités du Groupe et du contrôle de son efficacité. Il était auparavant RSSI du Groupe La Poste où il exerçait des fonctions similaires.

Alain Bouillé est certifié CISM et est membre du CLUSIF, du club R2GS, du CIGREF, du Cercle Européen de la Sécurité et préside depuis juillet 2012 le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN) regroupant près de 150 RSSI de grandes entreprises. ■

Plus d'information :
- https://www.cesin.fr/
- https://twitter.com/cesin_france

GREG DAY

Greg Day est Vice-Président et CSO EMEA chez Palo Alto Networks, responsable de la stratégie de cybersécurité et du développement de la Threat Intelligence. Précédemment il a occupé divers rôles stratégiques chez l'éditeur Dr Solomon, puis a été CTO EMEA chez Symantec, puis Vice-Président et CTO EMA pour l'éditeur FireEye.

Greg Day est également membre du comité de pilotage de l'agence nationale UK National Crime Agency, du UK-CERT/CISP et de la communauté de recherche antivirale VFORUM. ■

Plus d'information :
- https://www.paloaltonetworks.fr
- https://www.paloaltonetworks.com
- https://twitter.com/PaloAltoNtwksFR

HEIDRICK & STRUGGLES

AHMAD HASSAN

Ahmad Hassan est Partner au sein de la Practice Technologies et Services du Cabinet parisien Heidrick & Struggles. Fondée en 1953 à Chicago, Heidrick & Struggles est l'une des premières sociétés mondiales de conseil en leadership, spécialisée dans la recherche de dirigeants par approche directe et dans le conseil aux dirigeants. Ingénieur en Electronique et Communications, Ahmad Hassan dispose d'un MBA obtenu à l'INSEAD. Il est co-inventeur (US Patent) de plusieurs produits en imagerie numérique.

Ahmad se consacre autant au recrutement des dirigeants qu'au conseil en leadership dans le domaine des technologies de l'information et digitale, aussi bien côté DSI et CDO d'entreprises utilisatrices que côté fournisseurs (les dirigeants des éditeurs de logiciels, équipementiers, opérateurs télécoms, intégrateurs). ■

Plus d'information :
- http://www.heidrick.com/
- https://twitter.com/HSIItweets

ITEANU
Société d'Avocats | Law Office

OLIVIER ITEANU

Maître Olivier Iteanu est avocat à la Cour d'Appel de Paris, fondateur et dirigeant de la société d'Avocats Selarl ITEANU. Il est également chargé d'enseignement à l'Université de Paris XI (Faculté Jean Monet), dans les Master 2 (DESS) du droit du numérique, du droit des activités spatiales et des télécommunications, de la gestion de l'information, ainsi qu'à l'Université de Paris I Sorbonne dans le Master droit de l'administration électronique.

Maître Olivier Iteanu est également administrateur et responsable de la commission juridique de l'ASP Forum devenu Eurocloud France depuis 2004. Il est également l'un des derniers Français à avoir été désigné par le conseil d'administration de l'Internet Corporation for Assigned Names and Numbers (ICANN) comme un des 9 membres du Comité d'Etude At Large Membership. ■

Plus d'information :
- http://www.iteanu.com/
- https://twitter.com/iteanu

IBM

ALAN JENKINS

Alan Jenkins est Associates Manager à IBM Security. Après avoir servi au sein de la police de l'Armée de l'Air britannique jusqu'en 2006, Alan Jenkins a notamment été Chief Security Officer UK pour CSC et T-Systems, puis consultant sécurité avant de rejoindre IBM en 2015. Il est également membre du comité consultatif de ClubCISO, une association britannique de cadres du domaine de la SSI, et membre du comité Convergence & Cyber de l'association ASIS International (chapitre UK). ■

Plus d'information :
- http://www.ibm.fr
- https://twitter.com/IBM_France

OLIVIER LIGNEUL

Olivier Ligneul est CTO & RSSI du groupe EDF. Il a auparavant été chef de la mission CTI au sein de la DSI ministères économiques et financiers, ainsi que chef du Bureau Assistance et Conseil pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI) / SGDSN. Titulaire d'un diplôme d'ingénieur de l'Ecole supérieure d'Informatique, Electronique et Automatique (ESIEA), il intervient régulièrement à l'INHESJ et est également vice-président du Club des experts de la sécurité de l'information et du numérique CESIN. ■

Plus d'information :
• https://www.edf.fr/

JEAN-PAUL MAZOYER

Jean-Paul Mazoyer est Directeur général du Crédit Agricole Pyrénées-Gascogne. Il a été auparavant directeur informatique et industriel du groupe Crédit Agricole entre 2013 et 2016.

Jean-Paul Mazoyer a également été Vice-Président du CIGREF et Président-Fondateur de son cercle Cyber-Sécurité, dans le cadre duquel il est notamment le créateur de la campagne Hack Academy.
Enfin, il est membre de la Réserve Citoyenne de Cyber Sécurité et Colonel de réserve de l'Armée de l'Air. ■

Plus d'information :
• http://www.cigref.fr/
• https://twitter.com/cigref

MARK McLAUGHLIN

Mark McLaughlin est Président et CEO de Palo Alto Networks. Il a été avant cela Président et CEO de Verisign, ainsi que Vice-Président en charge des ventes et du business développement pour Signio,un éditeur de solutions de signature électronique. Avocat, il a conseillé le groupe Caere Corporation et travaillé pour le cabinet Cooley Godward Kronish.

Mark McLaughlin a été nommé Chairman of the National Security Telecommunications Advisory Committee par le Président Barack Obama. Il est titulaire d'un diplôme de droit de l'université de Seattle et diplômé de l'Académie Militaire de West Point. ■

Plus d'information :
• https://www.paloaltonetworks.fr
• https://www.paloaltonetworks.com
• https://twitter.com/PaloAltoNtwksFR

JEROME SAIZ

Jérôme Saiz est consultant en protection des entreprises et fondateur de la société OPFOR Intelligence. Il est auditeur INHESJ, titulaire du titre 1 RNCP d'expert en protection des entreprises, et certifié CT CERIC en sûreté et lutte contre la malveillance (CNPP).
Il a été auparavant expert sécurité responsable de la communauté RSSI au sein de la société Qualys, et journaliste spécialisé dans les questions de cyberdéfense.

Jérôme enseigne depuis 2007 à l'EPITA et intervient depuis 2016 auprès du Centre National de Prévention et de Protection. Il est Lieutenant-Colonel dans la réserve citoyenne de la Gendarmerie Nationale et membre de la Réserve Citoyenne de Cyberdéfense. ■

Plus d'information :
- https://opforintel.com
- https://twitter.com/jeromesaiz

Orange Cyberdefense

MICHEL VAN DEN BERGHE

Michel Van Den Berghe est CEO d'Orange Cyberdefense. Il a rejoint le groupe à la suite du rachat d'Atheos, dont il était le Président Fondateur depuis 2002.

Il est également le fondateur des Rencontres de l'Identité, de l'Audit et du Management de la Sécurité (RIAMS) qui rassemblent depuis 2004 les principaux responsables et donneurs d'ordre du domaine de la sécurité des Systèmes d'Information.

Orange Cyberdefense rassemble toute l'expertise en Cybersécurité d'Orange Business Services et compte 1 200 collaborateurs dans 220 pays.
Michel Van Den Berghe est diplômé de la Faculté polytechnique de Mons. ■

Plus d'information :
- http://www.orange-business.com/fr/securite
- https://twitter.com/orangecyberdef
- https://twitter.com/vandenbergheocd

NATO OTAN

IAN WEST

Ian West est directeur de la cellule de lutte contre la cybercriminalité au sein de l'agence de l'OTAN pour la Communication et l'Information (NCI).

Il a reçu le SC Magazine Europe Award dans la catégorie « Meilleur Directeur de la sécurité informatique en 2016 », et son équipe a reçu la distinction de « Highly Commended Security Team » pour l'année 2016. ■

Plus d'information :
- https://www.ncia.nato.int/
- https://twitter.com/nciagency

CEFCYS

LAURE ZICRY

Laure Zicry est avocate, spécialiste de l'assurance responsabilité civile depuis plus de quinze ans, notamment avec une spécialisation dans les lignes financières. Elle a développé en janvier 2011 le premier contrat couvrant le transfert à l'assurance des risques cyber.

Aujourd'hui Laure Zicry est Responsable Technique Institutions Financières et Cyber Risks Practice Leader dans un grand groupe international. Elle est également l'auteur d'un ouvrage consacré à la maîtrise des risques cyber et membre du CEFCYS, le Cercle des Femmes de la Cybersécurité.

Laure est diplômée de l'Ecole du Barreau de Paris et de l'Université Paris X Nanterre. ■

AUTEURS

- **Gregory Albertyn**
  PwC
- **Avi Berline**
  PwC
- **Alain Bouillé**
  Groupe Caisse des Dépôts
- **Greg Day**
  Palo Alto Networks
- **Ahmad Hassan**
  Heidrick & Struggles
- **Maître Olivier Iteanu**
  Iteanu Avocats
- **Alan Jenkins**
  IBM
- **Olivier Ligneul**
  EDF
- **Jean-Paul Mazoyer**
  Crédit Agricole Pyrénées-Gascogne
- **Mark McLaughlin**
  Palo Alto Networks
- **Jérôme Saiz**
  OPFOR Intelligence
- **Michel Van Den Berghe**
  Orange Cyberdéfense
- **Ian West**
  OTAN (Communications and Information Agency)
- **Laure Zicry**
  Avocate