Sécurité informatique : « *Au fait, comment cela se passe-t-il chez nous ?* »

par

Thierry Auger
Responsable des risques SI, groupe Lagardère

En bref

Peut-on encore dormir quand la sécurité d'une centaine de systèmes d'information (SI) dans le monde repose sur vos épaules ? Quand Thierry Auger quitte EADS au début des années 2000 pour prendre en charge la sécurité des SI du groupe Lagardère, il comprend très vite qu'il va devoir radicalement changer de méthode, oublier les préconisations contraignantes et inventer une autre approche fondée sur un référentiel et des règles du jeux raisonnables, mesurables et inattaquables. En 2015, après la médiatisation de plusieurs grandes failles de sécurité, le conseil d'administration s'interroge : « *Mais au fait, comment ça se passe chez nous ?* » Il demande à rencontrer régulièrement le responsable de la sécurité des SI. Depuis, Thierry Auger ne peut que se féliciter des progrès accomplis par le Groupe grâce à une approche pragmatique qui accepte de lâcher sur certains aspects pour se concentrer sur l'essentiel, qui mobilise les expertises et les solidarités de réseaux internes et externes.

Compte rendu rédigé par Sophie Jacolin

Séminaire organisé avec le soutien de la Direction générale des entreprises (ministère de l'Économie et des Finances) et grâce aux parrains de l'École de Paris (liste au 1er octobre 2018) :

Algoé [1] • Caisse des dépôts et consignations • Carewan [1] • Conseil régional d'Île-de-France • Danone • EDF • Else & Bang • ENGIE • FABERNOVEL • Fondation Roger Godino • Groupe BPCE • Groupe OCP • GRTgaz • HRA Pharma [2] • IdVectoR [2] • IPAG Business School • La Fabrique de l'industrie • Mairie de Paris • MINES ParisTech • Ministère de l'Économie et des Finances – DGE • Renault-Nissan Consulting • RATP • SNCF • Thales • UIMM • Ylios [1]

1. pour le séminaire Vie des affaires
2. pour le séminaire Management de l'innovation

C'est à la Société européenne de propulsion, puis chez Matra et EADS, bien loin des métiers de la culture et des médias du groupe Lagardère, que j'ai fait mes premières armes. J'y ai œuvré à la conception du propulseur de la fusée Ariane, avant de participer à des programmes civils et militaires d'observation de la terre. Les questions de sécurité étaient prégnantes dans ces projets touchant à la défense. Pourtant, lorsque j'ai rejoint Lagardère pour assurer la sécurité de ses systèmes d'information (SI), mes acquis ont été largement ébranlés. Alors que la sécurité des systèmes informatiques est en principe une discipline transverse, il m'est apparu évident que je devais revoir mes pratiques à l'aune de la culture et des métiers de mes nouveaux interlocuteurs. En effet, une démarche de cybersécurité n'a d'efficacité que si tous les acteurs d'une organisation se l'ont appropriée. Rien ne sert de mettre la barre trop haut si personne n'est capable, n'a envie ou n'est conscient du besoin de l'atteindre. Dans le cas présent, je ne traitais plus avec des ingénieurs et des militaires, mais avec des éditeurs, des journalistes et des commerçants, un monde totalement différent dont je devais impérativement tenir compte.

La sécurité des systèmes d'information, enjeu vital

Toutes les entreprises ne mesurent peut-être pas la menace qui pèse sur leurs systèmes d'information et qui ne cesse de se renforcer. Pourtant, dans le monde, des données sont volées en permanence, bancaires en particulier. Elles sont revendues quelques dollars pour les plus basiques, et jusqu'à 8 000 dollars pour le numéro d'une carte bancaire réservée à des publics particulièrement choyés et dont les autorisations sont presque illimitées.

À cet enjeu s'ajoute, pour les entreprises, celui de la conformité. L'entrée en vigueur du règlement général pour la protection des données (RGPD), en mai 2018, renforce l'obligation pour les organismes de protéger les informations personnelles qu'ils possèdent.

Les sociétés qui opèrent dans des secteurs sensibles, où la donnée est classifiée, ont intégré depuis longtemps une logique rigoureuse de sécurisation. Les entreprises plus classiques, en revanche, sont moins sensibilisées à la nécessité de protéger leur patrimoine, c'est-à-dire les contenus qu'elles créent et qui constituent, sans qu'elles en aient toujours conscience, le cœur de leur activité. Pour Lagardère, très présent dans l'édition, il s'agit par exemple des albums d'une bande dessinée, désormais disponibles en format numérique, dont le piratage causerait un tort considérable. Nous aurions beau retirer les copies volées et disséminées sur la planète Internet, elles réapparaîtraient sans cesse. Mieux vaut prévenir ce risque et sensibiliser les acteurs de l'organisation aux mesures de protection à prendre.

Une autre faiblesse des organisations réside dans la disponibilité de leur outil de travail. Les processus des entreprises s'appuient en effet sur des moyens technologiques numériques susceptibles d'être attaqués à tout moment, ce qui peut conduire à les rendre indisponibles pour des durées variables qui parfois excèdent plusieurs jours. Prenons le cas des magasins d'aéroport gérés par Lagardère, dont les dizaines de milliers de caisses à travers le monde enregistrent sans cesse des achats. Leur blocage représenterait une perte définitive de chiffre d'affaires de plusieurs millions d'euros car, contrairement à d'autres magasins, les clients d'aéroport ne reviennent pas le lendemain.

Enfin, un groupe comme Lagardère qui porte des marques aussi fortes que Stock, Lattès, Paris Match, Europe 1, RFM ou le Guide du routard doit veiller à les protéger d'attaques directes ou indirectes, voire de destructions. À la protection de ce patrimoine immatériel s'ajoute celle de notre patrimoine matériel. Il en est ainsi des salles de spectacle que nous possédons. En cas d'événement attentant aux personnes, nous avons l'obligation de tenir à disposition des services de secours et des forces de l'ordre les documents liés à la sécurité des infrastructures, ou encore les images de vidéoprotection pouvant nourrir une enquête.

Contenir le risque dans une organisation éclatée

La politique de sécurité des systèmes d'information que je me suis attaché à mettre en œuvre chez Lagardère répond à la configuration particulière de ce groupe, éclaté en 434 sociétés sur tous les continents et opérant dans quatre grands métiers.

J'ai déjà cité quelques-unes de la centaine de maisons d'édition du Groupe. Lagardère est par ailleurs actif dans les médias : radio, télévision, publicité, magazines, production audiovisuelle et sites web (BilletRéduc, MonDocteur, Doctissimo…). Vient ensuite le métier de la vente de détail dans les gares et aéroports, avec l'enseigne Relay et les boutiques de *duty free*. Enfin, notre dernière branche est consacrée au sport, avec la gestion de stades, de droits sportifs et de clubs (comme le Lagardère Paris Racing) ou encore l'organisation d'événements.

Ces multiples activités sont gérées par une centaine de systèmes d'information indépendants. On pourrait voir dans cette configuration un danger de dispersion, mais elle présente au contraire, pour un responsable de la sécurité des systèmes, l'énorme avantage de distribuer le risque. Tout l'enjeu est de minimiser les interfaces entre ces entités et de s'assurer qu'une avanie essuyée par l'une ne se propage pas aux autres. Nous regardons ces sujets au niveau central, tout en tenant compte des réglementations nationales spécifiques.

Dans un tel contexte, il m'a paru nécessaire de quitter le modèle normé dont j'étais familier dans le monde de l'industrie spatiale, qui s'avérait inadapté à la constellation de métiers dans laquelle j'étais désormais plongé et qui m'est apparu au premier regard comme un univers d'artistes épris de liberté, rétifs aux contraintes et parfois gentiment inconscients. Je dois faire œuvre de pédagogie auprès de collaborateurs peu sensibilisés aux enjeux de sécurité, leur démontrer que je saurai les accompagner et leur imposer un niveau de contrainte qu'ils peuvent raisonnablement atteindre, sans aller au-delà. Il faut, pour cela, mettre en place une méthodologie inattaquable. Les équipes ne doivent pas la percevoir comme un frein à leur activité quotidienne, mais se convaincre qu'elles ont intérêt à y consacrer le temps nécessaire.

Dans un univers aussi disséminé que le nôtre, il est indispensable d'instaurer une règle du jeu commune, indiscutable et fermement relayée par les managers. La direction des systèmes d'information n'ayant pas de lien hiérarchique avec les équipes qu'elle accompagne, elle a besoin d'être légitimée et appuyée par le top management. Celui-ci pose sa signature sur la politique de sécurité, afin qu'elle redescende ensuite par la voie hiérarchique via les patrons des filiales. Nous nous référons ainsi à un cadre solide, tout en restant ouverts aux discussions. Pour que les collaborateurs s'approprient la contrainte, nous devons placer le curseur au plus juste, sans viser un niveau d'exigence peut-être louable mais qui serait de fait irréaliste. Notre principe est donc de poser une règle, d'émettre des recommandations opérationnelles non négociables – puisque déjà calées sur le niveau le plus raisonnable – et d'apporter des solutions et un appui aux entités qui en font la demande. Nous tenons par exemple à disposition de nos entités une centaine de contrats types avec des prestataires dans le monde entier, auxquelles elles peuvent facilement recourir pour répondre à leurs besoins spécifiques. Les équipes se réjouissent de pouvoir s'appuyer sur un tel service.

Un risque multiforme

À la difficulté de sécuriser les SI de l'entreprise s'ajoutent des cas particuliers dont les risques sont avérés. Nos données peuvent ainsi être exposées par l'entremise de partenaires, notamment de PME, qui sécurisent insuffisamment leurs systèmes d'information.

Le risque peut aussi provenir d'un salarié qui quitte le Groupe en emportant des données. Il y a fort à parier qu'il les copie sur un disque dur externe qu'il connecte, dès qu'il rentre chez lui, à sa box Internet, système non protégé. Ce faisant, il les rend disponibles sur le Web. Il peut aussi les transférer sur le disque d'un ordinateur personnel insuffisamment protégé...

Rappelons qu'Internet recouvre en fait trois principaux réseaux, à commencer par celui que nous utilisons quotidiennement dans le cadre professionnel ou personnel. Vient ensuite le *deep web*, réseau des objets connectés qui s'invitent dans nos foyers, sans protection : boîtiers assurant la sauvegarde d'ordinateurs, permettant

de regarder des photos sur un écran de télévision, etc. Le *dark web,* enfin, réseau non directement connecté, est le théâtre de toutes les activités illicites : vente de drogue et d'armes, tueurs à gage… Il faut des outils particuliers pour s'y connecter et les transactions s'y monnaient en bitcoins. Pour ce qui nous concerne, on y trouve par exemple des fiches répertoriant les données privées de célébrités gravitant dans l'univers de Lagardère, comme des animateurs stars de radios des pays de l'Est ou d'Asie. Ces éléments de contexte permettent d'élaborer des opérations de déstabilisation et, plus fréquemment encore, de rédiger des e-mails aussi crédibles que possible, incitant ces personnalités à réaliser des paiements.

Les entreprises sont particulièrement exposées à cette forme de fraude, dite de "fraude au président". Prenons un dirigeant d'entreprise qui effectue un déplacement international pour négocier une affaire. De l'information publiée par voie de presse conduira des malfaiteurs à rechercher des renseignements crédibles (ne serait-ce qu'en ayant innocemment appelé son assistante) qu'ils partageront sur le *dark web*. Au final, c'est un e-mail falsifié, au nom du dirigeant, redoublant de détails vraisemblables qui sera adressé au directeur financier de cette société : « *Je suis bien arrivé à Hong Kong, les pourparlers sont en bonne voie, pouvez-vous virer 300 000 euros sur le compte suivant pour sécuriser l'acquisition ?* » La demande étant urgente, exceptionnelle, crédible, venant de son patron, le comptable ne procédera pas aux vérifications qu'il sait pourtant devoir mener. Il n'est pas rare que le courriel arrive un vendredi soir ou en tout cas à une heure particulièrement étudiée pour faciliter les conditions de ce manque de vigilance.

Veille et pédagogie

Pour parer ces menaces, deux stratégies sont possibles. Soit vous déployez une énergie considérable pour rédiger des prescriptions et inculquer des consignes à votre écosystème, sans certitude qu'il les appliquera et avec le risque qu'il les rejette ou les relativise, soit vous laissez une certaine liberté au système et à ses acteurs mais renforcez drastiquement les surveillances (tout en conservant bien entendu une sécurité à l'état de l'art). Nous avons retenu cette seconde option, qui semble la plus adaptée à notre contexte. Dans cette optique, nous recherchons en permanence l'apparition éventuelle, sur le *dark web,* de mots clés très précis nous concernant, qui indiquerait l'existence de fuites de données dans notre périmètre. Lorsque nous apercevons l'un de ces mots-clés, cela prouve de manière irréfutable l'existence d'un problème. Nous pouvons remonter jusqu'à son origine et échanger avec les responsables de la sécurité du système considéré sur des bases indiscutables. C'est autant de temps gagné pour trouver des solutions et le cas devient un exemple parlant pour tous les acteurs de la communauté.

Lorsque nous avons instauré cette solution, il y a deux ans, une alerte nous parvenait tous les quinze jours. La semaine dernière, nous en avons reçu une à deux par jour. Cette accélération tient certes à la digitalisation accrue de nos métiers, mais aussi à l'hyperactivité de hackers qui cherchent en permanence à pénétrer les systèmes des entreprises pour en diffuser le contenu sur des réseaux parallèles.

Nous avons investi dans des moyens de surveillance grâce auxquels nous remontent des événements anormaux survenant dans l'écosystème du Groupe, y compris chez des partenaires et des clients B to B. Nous prenons soin d'en communiquer les retours d'expérience aux équipes, afin de leur démontrer très concrètement combien l'enjeu de la sécurité est central et de les tenir informés de l'évolution des stratégies des hackers et pirates.

Par ailleurs, nous nous efforçons de sensibiliser les collaborateurs à la sécurité des systèmes d'information. Dans cette optique, nous avons élaboré avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) un "jeu sérieux" de formation à ces risques. La participation reste malheureusement modérée. Nous sommes obligés de constater que l'intérêt pour ces opérations de sensibilisation grimpe rapidement dès que l'on annonce un iPad à gagner… L'effort de pédagogie ne doit jamais retomber.

En outre, nous avons instauré une méthodologie autodéclarative, dans laquelle chacun de nos responsables des systèmes d'information et de la sécurité doit répondre aux points de contrôle. Nous en analysons les résultats et élaborons des recommandations personnalisées. Vu le nombre de données à traiter, cet exercice requiert un travail considérable mais, une fois encore, le résultat est factuel et facilite grandement les discussions qui, sans cela, seraient très compliquées. Les rapports sont transmis au directeur général, au directeur des systèmes

d'information et au responsable de la sécurité de l'entité mesurée ainsi qu'aux dirigeants concernés. Cette méthodologie permet d'identifier les priorités et d'accompagner plus particulièrement ceux qui sont en écart.

Le groupe Lagardère n'étant pas un opérateur dit d'importance vitale pour la nation, il n'est pas soumis aux obligations ni aux contrôles prévus par les différents codes associés. C'est donc sur la base de toutes les dispositions légales ou des recommandations des régulateurs que nous démontrons que nous devons renforcer notre politique. De ce point de vue, le RGPD est un véritable atout.

Les quatre piliers de la sécurité

À la suite des grandes attaques médiatisées de type WannaCry ou NotPetya, qui ont proliféré à partir de 2015 et ont eu des conséquences majeures sur des États ou des entreprises (comme Saint-Gobain en France), un échange régulier a été institué avec le comité d'audit du groupe Lagardère. Deux fois par an, nous y dressons un bilan du programme de cybersécurité, expliquons comment la menace évolue et comment nous y répondons. De plus, nous exposons une fois par an notre démarche au conseil de surveillance.

Celle-ci repose sur quatre grands piliers.

Une équipe convaincante

Tous les membres de l'organisation doivent être des relais actifs de la stratégie de cybersécurité. Leur savoir-faire doit se doubler d'un "savoir-être", d'une capacité de conviction auprès d'équipes sur lesquelles ils n'exercent pas de pouvoir hiérarchique. Cette organisation ad hoc s'appuie bien évidemment sur une série d'outils : référentiel actualisé, règle du jeu, plan de sensibilisation, mesure régulière...

Une sécurité périmétrique conforme à l'état de l'art

Nous devons être capables de démontrer que nous avons traité comme il se doit l'ensemble des moyens et systèmes utilisés par les équipes au quotidien. Si, par exemple, une activité repose en grande partie sur un site web, nous prodiguons aux collaborateurs l'accompagnement nécessaire pour qu'il soit géré correctement. La tâche est complexe, consommatrice en temps et en ressources, mais vitale. Elle doit être intégrée dans le *business plan*.

Des données inexploitables une fois piratées

Une fois les deux piliers précédents consolidés, nous pourrions nous croire suffisamment protégés. Il n'en est rien. Dans un groupe distribué comptant pas moins de cent directeurs des systèmes d'information, je n'ai pas la capacité de doter chacune des entités des expertises nécessaires dans tous les domaines. C'est pourquoi je leur demande de se focaliser sur la protection des données, de sorte que lorsque celles-ci seront piratées – ce qui arrivera inéluctablement ici ou là –, elles soient inexploitables par des tiers. C'est l'effort que nous fournissons actuellement.

Un contrôle dissocié de l'accompagnement

Il serait délicat que je double mon rôle d'accompagnateur de celui de contrôleur. La mission de vérification est donc endossée par la direction de l'Audit. De plus en plus formée aux problématiques de cybersécurité, elle est parfaitement outillée pour mener cette mission dans le cadre de prérogatives que personne ne lui conteste.

Vers une ubérisation de la sécurité ?

Les directeurs des services informatiques des grandes entreprises françaises se connaissent et s'entraident. Ils s'informent mutuellement des incursions qu'ils subissent pour en préserver leurs pairs. Il devient naturel, pour cette profession, de travailler en étroite collaboration avec son écosystème.

Progressivement, nous nous dirigeons également vers cette logique en interne. Il y a dix ans, sur mes recommandations, certaines de nos entités ont embauché leurs propres responsables de la sécurité des systèmes

d'information. Après deux ans d'expérience, leurs patrons m'ont fait part de leurs doutes : ces experts leur coûtaient cher et risquaient de se lasser d'intervenir dans des secteurs d'activité intéressants mais restreints, ce qui est toujours frustrant pour des techniciens créatifs désireux de découvrir des problématiques nouvelles. C'est pourquoi désormais, dans une logique que j'appelle *d'ubérisation*, je contractualise avec des spécialistes qui interviennent dans les entités du Groupe au gré des besoins, un ou deux jours par semaine, au cas par cas, mais qui, en cas de problème, peuvent intervenir en urgence le temps nécessaire. Ils accèdent ainsi à toute la variété de nos métiers et enrichissent leur expérience. Je ne doute pas que nous verrons apparaître des plateformes de mise à disposition de profils ciblés garantis, adoubés par la profession. Les entreprises y gagneront collectivement en réactivité et en efficacité. Dans le monde de la sécurité, l'isolement est un gage d'échec.

Débat

Une vigilance en haut lieu

Un intervenant : *Votre présence auprès du comité d'audit et de la gérance a-t-elle été suscitée par un événement particulier ?*

Thierry Auger : En 2015, des entreprises proches de notre univers telles que Sony, TV5 Monde, Target ou Home Depot ont découvert qu'elles avaient fait l'objet d'attaques massives. Des numéros de cartes bancaires avaient notamment été exfiltrés des enseignes de grande distribution Target et Home Depot pendant des mois. Les banques, assaillies de plaintes, avaient fini par identifier que les derniers achats légitimes déclarés par leurs clients étaient toujours effectués auprès d'elles. Il s'est avéré que des prestataires mal intégrés aux travaux de sécurisation du SI mais qui en utilisaient les moyens étaient à l'origine de la captation de données.

À la suite de ces événements, le comité d'audit nous a convoqués pour que nous lui expliquions comment nous nous prémunissions de ce risque. Cela a incité le Groupe à nous octroyer des moyens supplémentaires. Nous avons proposé de financer au niveau central des technologies coûteuses et complexes à déployer pour nos filiales. Progressivement, nous avons également bâti un réseau de partenaires pour assurer une surveillance de nos systèmes dans le monde entier. C'est grâce à cela que, entre autres exemples, nous avons découvert le piratage de certains de nos contenus, souvent fractionnés et revendus là où nous ne sommes pas. C'est dire l'ingéniosité des pirates.

Int. : *La gérance comprend-elle à quel point maintenir des systèmes d'information distincts pour les entités est utile pour éviter les problèmes qu'ont pu connaître Saint-Gobain et tant d'autres, plutôt qu'un dispositif centralisé moins coûteux ?*

T. A. : Notre organisation en systèmes distribués est un atout pour contenir le risque. Nos dirigeants le comprennent. Il est vrai que les responsables informatiques préfèrent souvent les modèles mutualisés, plus faciles à gérer. Or, notre Groupe est vivant ; des activités y entrent et en sortent régulièrement. Pour accompagner ces mouvements de façon réactive, mieux vaut limiter les interfaces nombreuses qui créent toujours plus d'adhérence qu'imaginé lorsqu'on veut détacher une partie du tout. Du reste, nos métiers sont si différents qu'il est plus efficace de miser sur des systèmes locaux, adaptés aux spécificités locales.

Une sensibilisation de longue haleine

Int. : *Comment gratifiez-vous les comportements respectueux des règles de sécurité, sachant que la meilleure preuve de leur performance est… qu'il ne se passe rien ?*

T. A. : C'est effectivement une vraie difficulté dans nos métiers. Les collaborateurs les plus vertueux, y compris les opérationnels, sont invités à rejoindre des comités transversaux en charge de la sécurité. Ils y gagnent une reconnaissance de leurs pairs et de l'entreprise. Nous en faisons des leaders de la démarche dans leur entité. Ils apprécient cette légitimation.

Int. : *Comment parvenez-vous à convaincre les 30 000 collaborateurs de votre Groupe d'adopter des règles de sécurité au quotidien, au point d'en faire un réflexe ?*

T. A. : C'est un combat que nous ne gagnons jamais entièrement et qu'il faut recommencer en permanence. Par exemple, je demande à toutes les entités de me remonter les événements problématiques qu'elles rencontrent : vol d'ordinateur portable, attaque de site web, destruction d'un système d'information par un virus… Ces cas sont rendus anonymes et publiés dans une base de données, avec la mention de l'action qui aurait pu les empêcher. Cela s'avère extrêmement utile pour sensibiliser les collaborateurs et rappeler que rien n'est jamais gagné, même si l'on croit bien travailler. Il faut toujours progresser.

Malgré tout, nous avons l'impression de buter contre un plafond qu'il est difficile de dépasser. Ainsi, nous constatons invariablement qu'environ 10 % de nos collaborateurs ne peuvent s'empêcher de cliquer sur un e-mail douteux. Je précise ici que ces chiffres s'observent peu ou prou ailleurs, sans être une spécificité Lagardère. Nous partons du principe que la citadelle tombera tôt ou tard et que la donnée sera volée. En conséquence, nous déployons des outils ciblés pour protéger le patrimoine de nos métiers. Nous faisons en sorte que les données soient inexploitables après le larcin et que les systèmes puissent redémarrer grâce à des sauvegardes confinées, qui auront échappé à l'attaque. La règle d'or est ainsi de dissocier la production de la sauvegarde, car quand un virus les atteint simultanément et les détruit, rien n'est plus possible. Le dommage est alors immense et irréparable. Nous avons vu un de nos collaborateurs commettre une telle erreur et, pris de panique, s'enfuir comme par un réflexe irrationnel, effondré par sa responsabilité écrasante et se réfugiant temporairement dans le déni. Il était pourtant parfaitement conscient des procédures de sécurité qui lui avaient été maintes et maintes fois rappelées. Peut-être ne lui avions-nous pas fourni les bons outils ou peut-être n'avait-il pas mis en œuvre les protections nécessaires. Des cas comme celui-ci prouvent que personne n'est à l'abri. Les experts sont même particulièrement ciblés et ne sont pas moins faillibles que les autres. Il nous revient de faire en sorte que les erreurs inévitables de nos collaborateurs aient les conséquences les moins graves possibles.

Int. : *Le RGPD vous oblige-t-il à revoir en profondeur votre démarche de sécurité ? Comment vos collaborateurs s'approprient-ils ces nouvelles règles ?*

T. A. : La mise en œuvre du RGPD est extrêmement complexe et requiert un travail important. Outre notre mise aux normes en interne, notre écosystème technologique n'est pas toujours prêt. À titre d'exemple, l'outil de chiffrement des données que nous déployons ne fonctionne pas encore chez tous nos partenaires comme Amazon, Dropbox, Microsoft Office… Or, le manque de compatibilité des technologies présente un risque pour la protection des données. Nous devons avertir nos utilisateurs des traitements de données qu'ils doivent cesser de réaliser, car ils ne remplissent pas les nouvelles conditions imposées par le règlement. Ils doivent par exemple arrêter de recourir à des solutions de *cloud*, qui sont encore insuffisamment sécurisées. Nous étendrons progressivement leur spectre d'action, à mesure que l'écosystème gagnera en maturité et se conformera à cette nouvelle réglementation. Même avec la meilleure volonté, il est difficile de répondre aux attentes des régulateurs. Il nous faudra deux ou trois ans pour nous mettre en conformité totale avec le RGPD, principalement parce que notre écosystème ne sera pas prêt avant. En dépit des difficultés qu'il soulève, je considère malgré tout que ce règlement est un très bon levier pour faire progresser le Groupe sur ces sujets.

L'isolement, gage d'insécurité

Int. : *L'appartenance à un réseau professionnel et le capital social sont manifestement des qualités essentielles pour un responsable de la sécurité des systèmes d'information. En faites-vous un critère de recrutement ? Comment se définit ce réseau ?*

T. A. : Ce réseau est un écosystème de professionnels de confiance, extérieurs à l'entreprise, avec lesquels nous échangeons en cas d'incident ou de doute. Il peut s'agir de prestataires, mais aussi d'entreprises concurrentes ou exerçant dans de tout autres métiers que les nôtres. Il arrive ainsi que de grands industriels équipés de cellules de veille et d'investigation nous alertent d'événements anormaux.

Nous développons également des systèmes de surveillance avec des prestataires qui, au-delà de la détection, sont capables de nous aider à remédier aux attaques. Lorsque nous demandons à un laboratoire de recherche israélien d'analyser en temps réel une ligne de code suspicieuse, nous transmettons ses résultats à notre réseau de pairs. C'est ensemble que nous parvenons à bloquer des attaques. Les acteurs de la sécurité informatique sont humbles et solidaires, car ils se sentent petits face à la menace.

Int. : *Vous arrive-t-il d'embaucher des hackers ?*

T. A. : Nous faisons appel non pas à des hackers, mais à des personnes ayant des aptitudes à "solliciter" les systèmes. Certains de nos partenaires, assez régulièrement des start-up, ont précisément pour métier de déceler des failles. Nous travaillons aussi avec les incubateurs, accélérateurs et autres fonds d'investissement pour soutenir ce type d'entreprises. Nos responsables des systèmes d'information ayant le plus d'appétence pour les solutions innovantes les testent volontiers. De ce point de vue, le fait de ne pas être un opérateur d'importance vitale est un avantage : je suis par exemple libre de déployer rapidement une technologie américaine ou israélienne, et cela peut s'avérer très utile dans certains cas.

Int. : *En matière de sécurisation des systèmes d'information, les entreprises sont de plus en plus dépendantes de leurs partenaires. Jusqu'où peuvent-elles les laisser accéder à des données sensibles ?*

T. A. : Nous mobilisons des ressources pour moitié internes et pour moitié externes. À mon arrivée dans le Groupe, j'ai constaté avec étonnement qu'à la différence du monde industriel, les métiers des médias employaient uniquement des ressources internes pour assurer leur sécurité. Ce n'est pas propice à une régénération des compétences. Je me suis donc attaché à les ouvrir à des experts extérieurs. En revanche, plus on s'approche du patrimoine de l'entreprise, plus il faut s'appuyer sur les capacités internes. Pour une radio, par exemple, la priorité est de garantir la disponibilité de l'antenne. Ce sujet est géré par une cellule technique dédiée, disposant de moyens hautement surveillés et protégés.

Int. : *Comment vous assurez-vous de la loyauté de vos experts freelance, qui ont accès à des informations sensibles ?*

T. A. : Leur contrat définit leurs obligations de confidentialité. Au-delà, s'exerce la force de la réputation et de la légitimation par le réseau. Nous connaissons la quasi-totalité des acteurs de la sécurité. Nous avons aussi les moyens de faire des recoupements pour cerner un profil. Aujourd'hui, grâce à l'habitude, j'ai une perception presque intuitive de la confiance que je peux accorder ou non à un prestataire.

Int. : *Pour avoir également recours à l'expertise extérieure de freelance ciblés, je peux témoigner que les vols de données sont rarement le fait de partenaires, qui mettraient leur réputation en jeu, mais davantage de tiers mal intentionnés ou d'employés ayant des griefs contre l'entreprise.*

Int. : *Vous fournissez une description précise des conditions grâce auxquelles un système peut être collaboratif. À quel point vos dirigeants ont-ils conscience du temps que vous consacrez à aider vos pairs d'entreprises tierces, voire concurrentes ?*

T. A. : Chaque cas est particulier, il faut savoir gérer les limites et, au final, ce sont les résultats qui comptent à leurs yeux. Le Groupe sait que dans ce domaine, les bons profils sont difficiles à capter et à fidéliser. Cela justifie que l'on mobilise l'écosystème tout en gérant au sein des communautés l'équilibre entre la valeur distribuée et la valeur captée. Du reste, ce modèle ouvert tend à se diffuser dans les entreprises, parmi les acteurs de l'innovation notamment.

Présentation de l'orateur

Thierry Auger : diplômé de l'école centrale d'électronique, il a débuté sa carrière à la Société européenne de propulsion (qui a conçu les propulseurs du lanceur Ariane) avant de rejoindre le département de traitement d'images de Matra (de 1989 à 1995) comme responsable technique sur les stations d'acquisition et de traitement des données satellites. Il a ensuite été responsable d'activités SI au sein de filiales de Matra Hautes technologies puis d'EADS (activités civiles et militaires). En 2001, il a rejoint la DSI (direction des systèmes d'information) du groupe Lagardère en tant que directeur des infrastructures avant d'être nommé DSI adjoint et CISO (*Chief information security officer*) du Groupe en 2009. Enseignant vacataire, il est membre du GITSIS (Groupement interprofessionnel pour les techniques de sécurité des informations sensibles), du CESIN (Club des experts de la sécurité de l'information et du numérique) et du jury des prix de l'Innovation des Assises de la sécurité et des systèmes d'information.

Diffusion octobre 2018