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