La cybergouvernance est à inventer dans l'entreprise

Pour conjurer des attaques toujours plus dévastatrices, une cybergouvernance globale commence à émerger dans les entreprises, qui dépasse le cadre trop étroit de la sécurité informatique. Mode d'emploi. //

Par Gilmar Sequeira Martins

Ukraine, décembre 2016. Pour la première fois, des hackers prennent le contrôle d'un réseau de distribution électrique. En quelques minutes, 230000 personnes sont plongées dans l'obscurité. Six mois plus tard, bis repetita. Un nouveau virus venu d'Ukraine touche de nombreuses entreprises et administrations locales avant de se répandre dans le monde. En France, il s'introduit, entre autres, dans le système informatique de Saint-Gobain. Très vite, tout s'arrête. Plus aucun ordinateur n'est utilisable. « Pendant quinze jours, ils se sont retrouvés contraints de fonctionner quasiment en mode "gomme-crayon" », résume Alain Bouillé, président du Club des experts de la sécurité de l'information et du numérique (Cesin). Au final, le manque à gagner s'est élevé à 220 millions d'euros, soit 4,4 % du résultat d'exploitation du semestre... Si l'ampleur de l'impact est inédite, les cyberattaques sont désormais monnaie courante et aucune entreprise n'est plus à l'abri. La liste des victimes accueille sans cesse de nouveaux venus: Sony, Yahoo, Target, Equifax, Deloitte, Forever, Renault ou encore Vinci...

Le danger est d'autant plus grand que les outils et les techniques pour mener à bien une cyberattaque se diffusent à une grande échelle. Ils sont désormais à la portée du premier venu ou presque, constate Emmanuel Germain, directeur général adjoint de l'Agence nationale de la sécurité des systèmes d'information (Anssi): « Il suffit de disposer d'un budget de 500 dollars et de savoir utiliser un logiciel d'anonymisation. Régulièrement, des sites de mairies ou de lycées sont attaqués et, plus grave encore, des cas d'espionnage détectés. »

Des entreprises très exposées.

Face à ce fléau, le niveau de protection des entreprises est pour le moins disparate. Les enseignes de vente de vêtements, qui dégagent de faibles marges sont des proies très prisées car elles n'ont pas les moyens d'investir massivement dans la sécurité informatique, de même que les entreprises très décentralisées. « Les SI sont placés sous la responsabilité de dirigeants opérationnels dont la priorité n'est pas la sécurité des données », explique Philippe Trouchaud, associé responsable du département cybersécurité de PwC. Pour ne rien arranger, la frontière entre l'interne et l'externe est désormais poreuse: « Les entreprises utilisent au quotidien des outils externes, comme LinkedIn, qui est devenu une base de données pour les RH ou un outil de communication pour les collaborateurs. L'idée même de verrouillage au sens technique relève de l'illusion. Il est en revanche possible d'envisager un usage sécurisé des outils non internes », estime Pascal Junghans, directeur de projet en charge de l'activité prospective d'Entreprise & Personnel. Anti-virus et autres dispositifs techniques ne sont pas vraiment à la hauteur d'un défi de cette ampleur, estime Jean-Marie Pivard, président de l'Institut français de l'audit et du contrôle interne (Ifaci): « Il y a les attaques globales, comme

Wannacry, qui n'a été détecté que par un tiers des anti-virus, mais aussi les attaques ciblées, ayant pour objectif le sabotage, comme dans les cas de TV5 ou des hôpitaux londoniens, ou l'espionnage, pour voler des brevets, sans oublier le piratage de comptes sociaux pour diffuser de fausses nouvelles... »

Devant la montée des périls, de nombreux spécialistes de la sécurité informatique réclament la mise sur pied d'une cybergouvernance. « La dimension technique ne suffit pas, il faut l'intégrer dans une problématique plus large incluant la sécurité des infrastructures physiques et des personnes », résume Emmanuel Germain. Même son de cloche à la Cnil : « L'informatisation croissante, la complexité toujours plus forte et l'éparpillement des données impliquent né- ▶

« Aujourd'hui, c'est l'âge de pierre de la gouvernance et cela laisse l'avantage aux délinquants. »

Adobe Stock

EN CHIFFRES

4000 attaques par jour en 2016 dans l'Union européenne avec des logiciels rançonneurs de type WannaCry ou CryptoLocker.

300% de croissance de ce type d'attaque en 2016.

80% des entreprises de l'UE ont connu au moins un incident de ce type en 2016.

Source Club des experts de la sécurité de l'information et du numérique (Cesin)

▶ cessairement, pour assurer une bonne gestion, à la fois une cartographie mais aussi une gouvernance des données au sens large », renchérit Gwendal Legrand, directeur des technologies et de l'innovation. Tergiverser ne fera qu'aggraver la situation, conclut Philippe Trouchaud : « Aujourd'hui, tous les acteurs du process sont dans une situation difficile : les directions ne comprennent pas grand-chose et les hommes de l'art ne sont mobilisés que dans l'urgence. C'est l'âge de pierre de la gouvernance et cela laisse l'avantage aux délinquants, qui peuvent attaquer autant qu'ils veulent, sans que les incidents donnent lieu à une capitalisation utile. »

Définition, objectifs... action !

Pour sortir de cette impasse, c'est d'abord la vision du problème qu'il faut faire évoluer : « La cybersécurité, et plus largement, la cybergouvernance, ne doit pas être considérée comme un handicap, un coût, mais comme un risque systémique, au même titre que d'autres risques, financiers ou climatiques », soutient Emmanuel Germain. Reste à tracer les contours de cette cybergouvernance. Le cabinet de conseil EY a une vision bien arrêtée. « Aujourd'hui, le terme cybergouvernance induit la maîtrise de ses données, de son SI mais aussi de sa présence sur Internet à travers les réseaux sociaux ou le cloud, assure Marc Ayadi, partenaire chez EY en charge de la technologie, du cyber et des services data. Elle doit avoir deux objectifs : une plus grande efficacité, tant en termes de productivité que de pénétration sur les marchés, mais aussi l'assurance d'une conformité vis-à-vis des exigences réglementaires. La question de la sécurité est présente dans ces deux dimensions. »

François Beaume, directeur risques et assurances groupe BureauVeritas mais aussi administrateur de l'Amrae et président de sa commission SI, est encore plus ambitieux : « La cybergouvernance est un outil de décision et de management pour renforcer la résilience et la performance des organisations. Son objet est le risk management, plus large que la sécurité IT. Elle doit avoir au moins trois objectifs : donner aux organes de direction les informations nécessaires à une prise de décision basée sur une identification des risques et une évaluation des impacts ; démontrer que le sujet est traité afin d'assurer la protection de l'entreprise et des mandataires sociaux ; et enfin montrer au marché que ce sujet a le rang de priorité numéro un. »

Une fois franchi ce cap, reste à trouver un modèle de cybergouvernance... « Il faut mettre l'enjeu de la sécurité au bon niveau de commandement, qu'elle soit en lien avec les métiers, le comex, les RH et ceux en charge du digital. Tous doivent contribuer à la sécurité », estime Alain Bouillé. Orange a une longueur d'avance dans ce domaine : « La cybergouvernance implique la DSI, les directions métiers, mais aussi les directions juridiques et les responsables des assurances. Au sein de chaque métier, nous avons un responsable sécurité », détaille Arnaud Jules, directeur délégué politiques de sécurité du Groupe. Chaque entité a un niveau de responsabilité spécifique, en appliquant un principe de subsidiarité, avec une boucle d'amélioration continue pour le perfectionner.

Inutile pour autant d'espérer un modèle standard car les organisations ont toutes leurs spécificités. « La liste des fonctions impliquées ne peut pas être établie une fois pour toutes, admet François Beaume. Elle doit prendre en compte le métier de l'entreprise, son exposition, sa maturité digitale et bien d'autres paramètres. » Mais l'aéronautique et le monde hospitalier font figure d'exemples à analyser. « Dans les deux cas, on a vu se développer des cultures de la sûreté qui englobent l'ensemble de la boucle, depuis le recrutement, jusqu'à l'amélioration des process existants grâce à une analyse minutieuse des incidents », explique Philippe Trouchaud.

Ce type de démarche comporte cependant des écueils : « Les entreprises peuvent effectivement puiser une inspiration dans ces filières, en fonction de ce qui est transposable à leur

Les RH, acteurs clefs

Sans être informaticien, les RH jouent un rôle clef dans la sécurité IT. Déjà bien réelle, la pénurie de spécialistes de la cybersécurité va empirer, selon Philippe Trouchaud, associé responsable du département cybersécurité de PwC : « En 2020, il manquera 2 millions de spécialistes de la cybersécurité dans le monde. Les RH doivent donc travailler dès aujourd'hui sur l'attractivité des entreprises. » Trouver et attirer ces profils toujours plus rares va devenir une priorité de plus en plus stratégique, pour Audrey Richard, porte-parole de l'ANDRH : « L'enjeu pour l'entreprise est de conserver une souveraineté et de réduire sa dépendance vis-à-vis des sous-traitants. » Comment ? En se rapprochant des écoles formant à la cybersécurité et en nouant des partenariats privilégiés afin d'intégrer les meilleurs éléments, au fil de leur parcours, afin de faciliter leur embauche ultérieure. Pour Audrey Richard, la gestion du parcours de ces spécialistes est capitale car ce sont des compétences rares. Il faut qu'ils se sentent reconnus comme tels. Bien gérer les parcours sera d'autant plus crucial que les équipes de spécialistes de la cybersécurité sont réduites, même dans les grandes organisations. Plus encore peut-être que pour le sourcing, les RH ont un rôle clef à jouer, à ce stade. « À la SNCF, où j'ai été en charge des équipes IT, j'ai contribué à leur donner de la visibilité. J'ai expliqué au Comex l'importance de cette équipe grâce à la rédaction d'un livre blanc sur ces problématiques », souligne Audrey Richard. Un programme de sensibilisation des utilisateurs a également été mis en œuvre afin de réduire de façon drastique le nombre de clics sur des documents et liens suspects. Et c'est la cybergouvernance globale de l'entreprise qui a pu être améliorée.

situation mais il leur faudra être attentives à la disproportion entre les besoins et les coûts. Cela passera nécessairement par un ciblage des actifs les plus essentiels où l'effort de sécurité devra se concentrer », note Marc Ayadi. Pour installer un modèle, encore faut-il enclencher le mouvement qui aboutira à des décisions. Pour Jean-Marie Pivard, tout doit être lancé à partir du sommet : « Il faut que les dirigeants s'emparent du sujet et identifient qui va le porter. Cela peut être un acteur interne ou externe. » D'où l'intérêt de cartographier les données : « Les entreprises doivent établir une cartographie et une gouvernance des données en ciblant plusieurs objectifs : la sécurité, la conformité mais aussi l'efficacité. Elles doivent être capables de savoir qui traite quelles données, où, et dans quelles conditions elles peuvent être exploitées », estime Gwendal Legrand, directeur des technologies et de l'innovation (Cnil).

Le RGPD, un levier et un risque

L'entrée en vigueur du Règlement général sur la protection des données (RGPD) peut-elle booster la cybergouvernance ? Pour Gwendal Legrand, directeur des technologies et de l'innovation de la Cnil, le moment est opportun : « C'est en effet une occasion à saisir pour les entreprises car cela devrait leur permettre d'une part de gagner en visibilité, en conformité, en cohérence et en pertinence sur l'ensemble de leurs services, et d'autre part de revoir leurs processus de gestion de projet afin de favoriser le dialogue entre les métiers, les DPO, les RSSI et les responsables de traitements. » Mais attention à l'excès de zèle, prévient Alain Bouillé, président du Club des experts de la sécurité de l'information et du numérique (Cesin) : « Le RGPD va nous aider à adresser l'enjeu de cybergouvernance mais il comporte un risque, celui de se concentrer sur les données personnelles alors que les autres données ont elles aussi un caractère stratégique, il suffit de penser à tout ce qui concerne les brevets ou les secrets de fabrication. »

L'utilisateur au cœur du dispositif. Il faut ensuite établir des scénarios, constituer une cellule de gestion de crise, mais aussi des solutions incluant différents volets (prévention, assurance ainsi que des plans de continuité d'activité). Une liste que Philippe Trouchaud complète à son tour : « Il faut intégrer une cybergouvernance dans les projets dès leur lancement pour qu'ils incluent dès le départ la protection des données ; établir un tableau de bord listant les incidents mais aussi le niveau de protection ; enfin, lancer un programme d'évaluation pluriannuel pour enregistrer les progrès. » Sans oublier la protection des SI, qui permet de fiabiliser le contrôle d'accès aux bâtiments, ni la dimension humaine. Selon l'Anssi, 80 % des attaques ont pour origine une défaillance humaine, comme par exemple un simple clic sur un lien ou une pièce jointe porteuse d'un logiciel malveillant. Réaliser un audit est donc une étape obligatoire et essentielle dans la construction d'un dispositif de cybergouvernance.

Et bien sûr former car les utilisateurs sont aussi l'objet de manipulations de la part des cyberattaquants. « Le recueil de données par des potentiels concurrents mal intentionnés peut prendre des formes très élaborées, confirme Pascal Junghans. Par exemple, les collaborateurs d'une entreprise ont reçu des propositions d'emploi qui les ont poussés à rencontrer des recruteurs dont les questions leur ont mis la puce à l'oreille. Il était clair que ces prétendus recruteurs souhaitaient en savoir plus sur leur entreprise. Ils ont donc averti leur hiérarchie. C'est l'une des vertus de la formation que de diffuser les bons réflexes. » Mais une telle démarche a un coût. « Aujourd'hui, pour avoir un degré d'efficacité réel, un budget cybersécurité doit représenter entre 5 % et 10 % du budget total de l'IT », préconise Emmanuel Germain.

ETI et PME : une autre voie ? Seule une minorité d'entreprises disposent des compétences internes pour gérer l'ensemble de ces processus et des ressources financières suffisantes. Il y a fort à parier que les PME se tourneront vers leur cabinet d'expertise comptable. Une opportunité dont ce secteur compte bien faire un levier de développement. « Les cabinets d'expertise comptable ont recruté des "sachants", spécialisés dans l'univers de l'IT, pour répondre aux problématiques de leurs clients », confirme Xavier Larbalette, DSI du cabinet Fideliance. Portée sur les fonts baptismaux par une multitude d'acteurs, la cybergouvernance reste cependant en devenir, même si le Règlement général sur la protection des données va entrer en vigueur cette année (voir encadré). Pour Arnaud Jules, trois facteurs vont déterminer l'avènement de la cybergouvernance : « l'évolution des cybermenaces, l'Internet des objets qui va connecter des milliards de machines dotées d'un nombre croissant de fonctionnalités, et la dimension géopolitique, qui risque de faire un nombre croissant de victimes collatérales. » En tout cas, dans son discours sur l'état de l'Union européenne, mi-septembre, le président de la commission européenne Jean-Claude Juncker a proposé la création d'une agence européenne de cybersécurité ? S'il y a peu de chances que ce projet aboutisse rapidement, tant les États sont attachés à leur souveraineté, son évocation a le mérite de rappeler que le temps de l'action est venu. ◆

« Il faut intégrer une cybergouvernance dans les projets dès leur lancement pour qu'ils incluent dès le départ la protection des données. »