Convergence sûreté et cybersécurité : du serpent de mer à l'évidence

Jérôme SAIZ
Président-fondateur d'OPFOR Intelligence

La question de la convergence entre sûreté et cybersécurité est l'un des serpents de mer préférés de la profession (à la différence près qu'il existe quand même quelques observations confirmées de la bête !).

Pourquoi un sujet qui ne devrait pas faire débat - aligner deux rôles ayant le même objectif au service de l'entreprise - fait-il couler autant d'encre depuis si longtemps ? Et, surtout, pourquoi est-il désormais plus d'actualité que jamais ?

L'on peut trouver un début de réponse dans l'origine même de ces deux fonctions. La prévention-sûreté existe depuis que les affaires existent. Son objectif est de protéger l'activité contre la malveillance. L'informatique, quant à elle, est évidemment arrivée bien plus tard, et par la petite porte.

À ce titre, il est fascinant d'explorer le site de l'INA à la recherche de reportages illustrant l'arrivée de l'informatique dans l'entreprise. C'est généralement le fait de patrons visionnaires et passionnés, et l'outil est évidemment d'abord aux mains d'experts. À ce stade, l'informatique est donc une affaire de spécialistes, son apport à l'activité de l'entreprise est minime et la malveillance à son encontre quasi inexistante. Il n'y a donc pas vraiment de quoi impliquer la sûreté, qui a déjà fort à faire et dont le personnel n'est, comme beaucoup à cette époque, pas franchement passionné par le sujet.

Mais l'informatique va progressivement s'ouvrir au monde à travers les réseaux de télécommunication et prendre une place grandissante dans les affaires. Ainsi, lorsque la malveillance informatique devient une réalité, qui peut-on aller chercher pour lutter contre ce nouveau phénomène ? Certainement pas le service de sûreté, qui n'a jamais traité du sujet ! C'est ainsi que l'on a tout simplement chargé les experts en place d'assurer eux-mêmes la protection de l'outil, créant au fil du temps un nouveau métier dans l'entreprise : celui de la « sécurité informatique » d'abord puis de la « sécurité des systèmes d'information » ensuite.

La distinction entre le service de sûreté et celui de la protection des systèmes d'information n'est donc pas née d'une stratégie mûrement réfléchie ni d'une doctrine finement travaillée. Elle est plutôt le fruit d'une évolution par défaut qui n'a jamais été remise en cause.

Remise en cause du statuquo

Certes, ces dernières années des organisations ont bien rapproché avec plus ou moins de succès leurs services de sécurité informatique et de sûreté. Mais elles sont encore l'exception plutôt que la norme, probablement car il s'agit d'une initiative structurante et très politique.

Car un tel rapprochement se fait rarement entre ces deux seules entités. Il s'agit plutôt d'associer

cybersécurité et sûreté au sein d'une Direction sécurité Groupe qui intègrera également la gestion du risque de manière transverse, souvent l'Intelligence Économique, et qui leur apportera en prime un soutien juridique et parfois même en communication de crise.

Mais pourquoi se donner autant de mal alors que l'entreprise fonctionne très bien sans tout cela ? Parce qu'aujourd'hui l'irruption de la transformation numérique, des objets connectés, de l'Internet des Objets (IoT), de l'informatique industrielle et du « *edge computing* » (informatique de bordure) change radicalement les scénarios de risque et oblige à penser en termes de stratégie globale plutôt qu'en silos sécuritaires.

Complémentarité des attaques

L'un des premiers arguments techniques pour le rapprochement des deux fonctions (ou a minima leur dialogue régulier) tient au fait qu'une attaque cyber peut permettre ou faciliter une attaque physique et à l'inverse, un accès physique au système d'information facilite grandement sa compromission. Dans les deux cas, le scénario de menace principal est l'ingérence économique.

Dans un sens, la numérisation permanente des outils de la sûreté (enregistreurs vidéo visibles sur le réseau de l'entreprise, caméras désormais connectées en IP, systèmes de contrôle d'accès reposant sur des serveurs et des logiciels aussi faillibles que les autres) fait qu'en confier l'exploitation à un service de sûreté ne disposant d'aucune sensibilisation au risque numérique peut conduire à des pratiques à risque, ainsi qu'à exposer inutilement des systèmes critiques qui n'auraient pas été identifiés comme tels (d'autant que les outils traditionnels de la cybersécurité ne sont pas toujours adaptés à ces outils ou leurs protocoles).

Dans l'autre sens, les experts de la cybersécurité, qui n'ont que peu de notions de protection physique, ignorent par exemple la résistance d'une ventouse électrique ou les moyens de la forcer et ne conçoivent souvent la menace que sous une forme virtuelle, n'adresseront eux aussi pas l'ensemble des risques.

Miniaturisation

En outre, les incroyables progrès réalisés dans la miniaturisation des systèmes ouvrent de nouveaux risques au croisement de la cybersécurité et de la sûreté. Ainsi un externe à l'entreprise peut parfaitement dissimuler sur lui un système de piratage complet (tel que le LAN Turtle ou un équivalent conçu sur la base d'une carte Arduino ou d'un RaspberryPi).

Il lui suffit alors de laisser un tel outil, de la taille d'une boîte d'allumettes, alimenté et connecté au réseau interne pour ouvrir une brèche dans le système d'information. Si le personnel d'entretien ou de sûreté n'est pas sensibilisé à reconnaître ces outils derrière un copieur ou au fond d'un sac lors d'une inspection visuelle, ils peuvent contribuer à matérialiser un risque majeur pour l'entreprise.

Bien sûr, tout ceci peut se régler : à minima par un dialogue entre les deux directions et des sensibilisations communes, mais de préférence dans le cadre d'une stratégie de protection globale qui associera la direction des risques en tant que « chef de projet » transverse capable de consolider les différentes approches (les méthodes d'analyse de risque informatiques intègrent, bien entendu, déjà le risque d'accès physique aux actifs).

Le sens de l'histoire

À vrai dire, tous les arguments avancés jusqu'à présent sont connus depuis longtemps et devraient, à eux seuls, motiver l'étude d'un dialogue renforcé entre la sûreté et la cybersécurité. Mais les évolutions les plus récentes du numérique montrent qu'une telle convergence s'inscrit désormais dans le sens de l'histoire. Pour ne citer que les points les plus saillants, l'ouverture de l'informatique industrielle multiplie les points d'entrées « cyber » sur le terrain, dans des

caissons, des boîtiers, des armoires ou des sites isolés. Tous ne peuvent être protégés de manière équivalente, et il est donc impératif de leur appliquer une analyse de risque cohérente croisant critères de cybersécurité et de sûreté. Au-delà de l'horizon, la tendance du « *edge computing* », qui vise à décentraliser massivement les traitements de données, signifie là aussi que de plus en plus d'actifs « cyber » critiques seront confiés à des sites distants, et devront donc bénéficier d'une protection physique à la hauteur des informations qu'ils traitent.

Plus envahissant encore : l'irruption d'une multitude d'objets connectés (IoT) expose également à des risques inédits, notamment liés à la capacité de l'attaquant à pouvoir détériorer physiquement à distance un équipement installé au sein des locaux (et en particulier en l'échauffant, ce qui pourrait donner à réfléchir aux spécialistes incendie)

Enfin, et bien que ce ne soit pas tout à fait l'objet de ce billet, les plus inquiets (ou prévoyants) imagineront probablement aussi des scénarios de risque autour de la voiture autonome des cadres dirigeants…

Dans tous les cas, il devient difficile de continuer à réfuter l'existence du serpent de mer…