Gestion des crises cyber : des crises pas comme les autres

Jérôme SAIZ
Président-Fondateur
OPFOR Intelligence

Même au sein des entreprises dont la fonction de gestion des crises traditionnelles est mûre, le domaine cyber est encore trop souvent traité à part, d'un point de vue purement technique. C'est pourtant oublier l'aspect transverse d'une telle crise, dont la résolution échappe à la seule DSI.

Cela concerne essentiellement les crises de type *ransomware* qui, si elles ne représentent pas la totalité des crises cyber, sont aujourd'hui les plus courantes, les plus visibles (mais ceci explique peut-être cela !) et surtout celles dont l'impact est le plus massif.

Car un tel événement paralyse l'ensemble des fonctions de l'entreprise comme peu d'incidents peuvent y prétendre : les salaires ne peuvent être virés, les lignes de production sont à l'arrêt, les commandes ne peuvent être ni reçues ni expédiées (les entrepôts étant gérés par des outils numériques) et les collaborateurs ne peuvent ni téléphoner ni utiliser l'email. Un tel arrêt brutal et simultané de l'ensemble des fonctions vitales de l'entreprise est rarement présent dans les scénarii traditionnels, en particulier quand celle-ci dispose d'implantations multiples. En temps normal, cela est tout simplement impensable.

La faute aussi, peut-être, à l'idée tenace selon laquelle un tel incident sera du ressort exclusif de la direction des systèmes d'information. « *La DSI va nous réparer tout ça en vitesse* » est souvent le premier réflexe de l'entreprise frappée par un *ransomware*. Or, la DSI ne peut, en réalité, pas y faire grand-chose à elle seule.

Sur le plan technique, d'abord : l'investigation numérique nécessaire afin d'identifier les marqueurs de l'attaque, le vecteur de compromission initiale, le parcours de l'attaquant ou le périmètre compromis est rarement à la portée d'une DSI. Il s'agit d'une expertise très spécifique et, en dehors de grands groupes, peu d'entreprises disposent d'une équipe d'analystes forensiques en interne. De même, le chantier de remédiation du système d'information dans le contexte d'un incident cyber est très, très, loin de celui habituellement prévu par le PRA de l'entreprise. Il s'agit de techniques et de procédures très particulières, qui doivent tenir compte de la perte de confiance dans l'ensemble du SI et se coordonner avec l'avancée (et les exigences) de l'investigation numérique. Le tout sans brûler des étapes (risque de reprise de la compromission) tout en réduisant au maximum la perte d'activité. À l'échelle d'un SI étendu, cela devient un jeu combinatoire particulièrement complexe, qui doit tenir compte des priorités des métiers, des impératifs de production, des dépendances en chaînes entre les systèmes.

Sur le plan des impacts, ensuite : la DSI n'est évidemment pas en charge de la relation client. Or, quand la production s'arrête et qu'il devient impossible d'accepter ou de livrer des commandes, il s'agit évidemment d'une question de relation client. Qu'est-ce qui peut être livré malgré tout ? (mode dégradé, commandes déjà préparées…). Qui privilégier ? Quelle sera la durée d'interruption de l'activité ? Comment convaincre les clients de ne pas changer de fournisseur, quand on sait qu'une crise de type *ransomware* au sein d'une entreprise non préparée paralyse généralement l'activité entre 8 et 10 jours à minima. Une étude aux États-Unis annonçait 9 jours de *black-out* moyen en 2019, et d'expérience, il s'agit plutôt de 8 à 15 jours d'interruption. Et il n'est pas rare que cela aille jusqu'à un plus d'un mois pour les incidents ou les périmètres les plus complexes, avec des effets sur l'organisation qui perdurent plus de six mois après la crise.

En outre, les clients s'isolent de l'entreprise victime afin de ne pas courir le risque d'être compromis à leur tour. Comment regagner leur confiance ? Si la réponse passe évidemment par une composante technique, elle se traite essentiellement au niveau de la direction commerciale, voire de la direction générale pour les clients les plus critiques.

Des enjeux similaires émergent également sur le plan juridique, qu'il s'agisse du réglementaire (RGPD) ou du contractuel (engagement de confidentialité pris auprès de clients importants). Le tout dans un contexte d'incertitude très fort : on ne sait rarement d'emblée si des données ont été dérobées, en quel volume et de quelle nature. Or, ce sont des questions pressantes qui se posent dès le début de l'incident.

Et puis la crise frappe aussi les salariés : l'interruption de l'activité va-t-elle conduire à du chômage partiel ? Menacer la survie de l'entreprise ? Doit-on vraiment poser nos RTT en priorité ? Nos congés ? Est-ce obligatoire ? Nos données à caractère personnel sont-elles aux mains de cybercriminels ? Que peuvent-ils en faire ? Comment pouvons-nous nous protéger ? Autant de questions qui exigeront une excellente coordination entre la DSI, les experts techniques, la RH, la communication et la finance.

La coordination, d'ailleurs… La pierre angulaire de la gestion d'une telle crise Cyber est la capacité d'orchestration afin d'apporter du liant entre la DSI (submergée, mais incontournable), les métiers (pressés) et la gouvernance de l'entreprise (souvent d'abord sidérée et ensuite avide de contexte, de conseils et de retours d'expérience afin de prendre les bonnes décisions). Tout en faisant le lien également avec les équipes d'investigation externes et en amorçant au plus tôt le chantier de redémarrage. Du fait de sa forte composante technique transverse, il s'agit là aussi d'une approche différente de celle mise en œuvre lors d'une gestion de crise traditionnelle.

Les crises cyber - en particulier celles de type *ransomware* - sont ainsi très différentes des schémas de crise les plus classiques. Cela tient essentiellement à leur impact immédiat et transverse, par opposition à une situation de crise qui émerge à partir d'un accident localisé et dont les conséquences pourront devenir transverses par effet domino (sinon il ne s'agit pas d'une crise), mais qui n'aura pas le même effet de paralysie soudain et total de l'entreprise dans toutes ses dimensions.

Cela ne doit évidemment pas exclure pour autant l'organisation actuelle de la gestion des crises : ses méthodes, ses outils et surtout son expérience sont précieux. Au même titre que sa capacité à consacrer du temps et de la ressource à la réflexion autour des sujets de crise, au développement de scénarios tenant compte de l'évolution de la menace et à l'organisation d'exercices. Il est toutefois nécessaire de l'inclure dans les approches spécifiquement cyber, peut-être à travers des sensibilisations et des réflexions communes, et peut-être par le biais d'une adaptation du plan de crise existant, afin d'intégrer la composante cyber.

Dans tous les cas, un tel impact massif et transverse exige une réponse massive et transverse elle aussi !