Le pilotage au cœur de la gestion de la crise cyber

Jérôme SAIZ
Président-fondateur d'OPFOR Intelligence
Senior advisor du CyberCercle

L'ingrédient secret au cœur de la crise, c'est le pilotage ! Le séquençage des multiples actions - souvent interdépendantes - et l'alignement d'objectifs parfois opposés exige en effet une vision transverse, unifiée ainsi que la capacité d'alterner sans cesse entre une grande attention aux détails et la prise de décisions rapides, forcément « à la serpe ». Et le tout, généralement, alors qu'aucune de ces décisions n'est véritablement satisfaisante.

C'est pourquoi le casting du pilote, et notamment sa capacité à coordonner les opérations de manière transverse, sera l'un des éléments déterminants du succès de la gestion de crise.

Bien sûr, chaque acteur du dispositif de crise participe activement à son succès. Mais le rôle du pilote est à part : ni expert technique, ni spécialiste métier, ni dirigeant, il doit pourtant faire preuve de bonnes connaissances dans tous ces domaines afin d'organiser l'effort collectif, saisir les enjeux globaux aussi bien que spécifiques, séquencer les opérations ou encore éclairer les risques, autant sur les plans techniques, juridiques ou de la communication.

Le tout au sein du chaos que peut représenter l'état de crise.

Aussi convient-il de se pencher sur le profil et les responsabilités de ce chef d'orchestre qui sera au cœur de la gestion de crise cyber.

Le profil du pilote

Pour l'Agence nationale de la sécurité des systèmes d'information (ANSSI), qui l'a baptisé Responsable des Opérations de Cyberdéfense (ROC), il s'agit d'un rôle relativement récent dont la création a été motivée par la complexité croissante des cyberattaques [1] . Sa mission est alors « *d'accompagner la victime dans son processus de gestion de crise jusqu'au rétablissement de son activité* ».

La complexité croissante des attaques est donc la raison d'être du pilote de crise. Face à une malveillance numérique de plus en plus souvent transverse, et dont l'impact sur l'entreprise l'est tout autant, la réponse ne peut qu'être, elle aussi, transverse. Cette transversalité est le socle même de la valeur ajoutée du pilote de crise. Celui-ci doit être autant à l'aise au sein de la DSI lors des points d'étapes techniques que dans ses échanges avec l'équipe de réponse à incident en charge de

[1] https://www.ssi.gouv.fr/agence/cybersecurite/plans-gouvernementaux/stephane-sans-responsable-doperation-de-cyberdefense-au-sein-du-centre-operationnel-de-lanssi/

l'investigation numérique, qu'auprès du RSSI qu'il conseillera sur le déploiement de nouvelles solutions de cybersécurité, ou encore face au comité de direction de l'entreprise, où il devra faire preuve de pédagogie afin de présenter les situations, les options et les risques. Car, *in fine*, son rôle est de fournir aux dirigeants les moyens de prendre des décisions éclairées dans une situation qui ne l'est pas !

Priorité aux « soft skills »

À un socle de solides connaissances techniques (probablement issues d'un parcours préalable dans le conseil en cybersécurité), le pilote de crise doit ajouter une forte capacité organisationnelle et surtout une série de « *soft skills* », des compétences interpersonnelles et de communication plus difficiles à évaluer de manière formelle. Parmi celles-ci, l'on retrouve notamment les capacités d'écoute, de synthèse, de communication, ainsi que l'empathie, la ponctualité, l'attention aux détails, la capacité à résoudre les conflits, à organiser le chaos, à mener plusieurs tâches de front… et tant d'autres pour lesquelles n'existe aucun diplôme !

Bien que difficiles à évaluer, ces caractéristiques sont pourtant essentielles tant la journée du pilote de crise se déroulera au contact d'interlocuteurs variés aux attentes diverses et aux niveaux de connaissance (technique, notamment) hétérogènes. Pire : chacun aura à cœur de résoudre au plus vite les problèmes sur son propre périmètre, parfois au détriment des autres et surtout en dehors de toute logique de séquençage (certaines activités doivent être opérationnelles avant d'autres). C'est alors le rôle du pilote non seulement de proposer les méthodes et l'organisation qui permettront d'atteindre les objectifs de la gestion de crise sans s'égarer (notamment le redémarrage de l'activité en toute sécurité), mais aussi d'aligner les attentes de chacun et, parfois, de calmer les ardeurs.

Les responsabilités du pilote au déclenchement de la crise

À l'activation du dispositif de crise, le pilote aura la responsabilité de suivre la montée en charge du dispositif, du gréement des différentes cellules au suivi des premières actions techniques, en passant par la compilation des premières synthèses managériales. Il n'est certes pas en charge de ces différentes actions (le plan de gestion de crise en a identifié chacun des responsables au préalable), mais il doit s'assurer qu'elles ont bien lieu, et alerter si ce n'est pas le cas. Ainsi, dès les premiers instants de la crise, le pilote est le garant de la structure du dispositif, quelle que soit la situation sur le terrain. C'est lui qui fait toute la différence entre la théorie (le plan de gestion de crise) et la réalité (composer avec absences, les indisponibilités de solutions techniques essentielles, les erreurs inévitables, l'effet de sidération dû à un impact majeur, etc.)

Enfin, son positionnement hiérarchique est important : si une certaine séniorité est un atout, il est préférable que le pilote ait un statut d'expert autonome et ne soit pas *dans* la hiérarchie, où il pourrait se heurter alors à des conflits d'intérêts ou subir des pressions inutiles. C'est pourquoi le rôle est souvent confié à un expert externe, un consultant soit intégré au dispositif de réponse à incident tiers (l'avantage d'un regard neuf), soit partenaire régulier de l'entreprise (l'avantage de déjà bien connaître le contexte d'intervention).

Le pilote est prêt ? Il est temps de plonger dans la crise…