La cybersécurité, nouvelle fonction support des PME et des start-up

par

Michael Monerau
Fondateur et *CEO*, Qontrol

En bref

Le rythme des cyberattaques s'accélère et la raison en est simple : les chaînes de valeur dépendent de manière croissante du numérique. Troubler le monde numérique devient donc un moyen efficace d'organiser une délinquance rémunératrice. Le risque est systémique, les interconnexions entre grands et petits se multipliant. La vision d'une cybersécurité "périmétrique" ne tient plus et il faut désormais s'assurer de la bonne sécurisation de son environnement proche, en plus de celle de ses propres systèmes. C'est pourquoi les entreprises, en particulier les plus petites, sont confrontées à de nouvelles exigences en matière de cybersécurité. Mais sans moyens dédiés suffisants, comment y faire face ? Quels sont les impacts sur la gestion des PME de demain ? Michael Monerau, fondateur de la start-up Qontrol, leur propose une plateforme d'accompagnement sur la cybersécurité et analyse ici les opportunités pour l'écosystème français.

Compte rendu rédigé par Pascal Lefebvre

Lorsque j'ai intégré le Corps des mines, mon premier poste, au contact quotidien des PME locales, m'a confronté aux problématiques du développement économique en région, en particulier celles concernant les questions d'intelligence économique. Quantité de PME sont en effet attaquées et perdent de l'argent ou des secrets de fabrication. Ce problème de cybersécurité est d'autant plus regrettable qu'au regard des techniques généralement peu sophistiquées employées par les hackers, il serait simple pour ces entreprises de se prémunir contre la plupart des risques encourus. L'écart constaté sur le terrain entre ce que l'on sait faire en matière de cybersécurité – tant du point de vue des outils que des *process* – et les pratiques quotidiennes de ces entreprises est donc énorme.

Les capacités d'intervention de l'État étant limitées et les nécessaires politiques publiques n'étant qu'incitatives, l'implication d'acteurs privés, parlant le même langage que ces entrepreneurs, m'a semblé être le moyen le plus efficace pour les aider à passer à l'action tout en se consacrant, de manière sécurisée, au développement de leur activité. L'aventure Qontrol est donc née de ma double expérience dans la tech et sur le terrain.

Les trois fonctions de la sécurité de l'information

La sécurité de l'information peut être considérée soit sous l'angle des matériels qui la délivrent, ordinateurs et périphériques divers, soit dans sa dimension immatérielle, sous forme de données numériques. Classiquement, cette sécurité se définit selon trois fonctions :

- la confidentialité (*confidentiality*) garantit que seules les personnes habilitées ont accès à l'information ;
- l'intégrité (*integrity*) garantit que la donnée reste valide et non corrompue au fil du temps, personne ne l'ayant modifiée ou rendue illisible entre deux accès ;
- la disponibilité (*availability*) garantit que l'accès à l'information est possible à chaque fois que cela est nécessaire.

Ces trois fonctions sont les bases de l'analyse d'une attaque et de la mise en place de défenses adaptées. Ainsi, la simple divulgation du mot de passe d'une messagerie lui fait perdre sa confidentialité, un tiers non autorisé ayant alors la possibilité d'accéder, par exemple, à vos mails ; elle lui fait éventuellement perdre son intégrité, ce tiers pouvant supprimer ces mails ou les modifier à votre insu ; elle lui fait également perdre sa disponibilité, la modification du mot de passe par l'intrus vous en interdisant alors l'accès. Certaines attaques vont préférentiellement cibler telle ou telle fonction. Ainsi, un *ransomware* va cibler la seule disponibilité, celle-ci étant rétablie contre le paiement d'une rançon.

Une *attaque* est définie comme étant toute action altérant l'une de ces fonctions, une *défense* visant, quant à elle, à protéger ces mêmes fonctions.

Une véritable politique de sécurité de l'information ne se limite pas à se protéger des conséquences d'un incident. Comme pour la sécurité physique d'un site industriel, il faut intervenir avant l'incident pour en empêcher l'occurrence. C'est ce à quoi contribuent, entre autres, les antivirus, les mises à jour, les sauvegardes et le travail sur les procédures internes.

Si cette prévention en amont n'a pas été possible, il devient nécessaire de détecter l'incident au plus tôt, une attaque étant d'autant plus puissante qu'elle reste invisible longtemps. Il faut donc l'identifier avant que l'attaquant ne puisse nuire davantage, tout en se préparant à affronter un éventuel effet maximal de l'attaque sur le système.

Enfin, le troisième temps est celui du correctif visant à limiter les conséquences de l'attaque. On s'efforce alors de contenir la contagion, avant de remettre le système en état de fonctionnement et de le protéger afin d'éviter qu'un tel incident ne se reproduise.

L'état de la menace

Le besoin de se protéger résulte de l'existence d'une menace crédible et à grande échelle. La plupart des PME estiment pourtant leur activité sans grand intérêt pour un acteur malveillant et pensent ne pas avoir à redouter une menace telle que celles qui visent spécifiquement de grands groupes et qui requièrent des moyens informatiques considérables. En cela, elles n'ont pas tort. Cependant, elles sont tout de même, à leur insu, la cible d'attaques automatisées massives, qui ratissent large et prennent indistinctement dans leurs filets toutes les entreprises dont le système est vulnérable pour ensuite les racketter.

Les attaquants détiennent des dictionnaires d'attaques, testées à grande échelle, qui leur permettent des actions soit directes, soit indirectes. Dans le cas d'attaques indirectes, l'entreprise infectée est utilisée comme un relai pour attaquer ses fournisseurs ou ses clients. Un casino s'est ainsi fait détrousser par le biais des aquariums qui le décoraient et qui étaient connectés à son réseau interne. En 2013, une énorme attaque a utilisé le système de facturation du fournisseur d'appareils de climatisation du réseau américain de distribution Target pour prendre le contrôle des caisses enregistreuses de ses supermarchés et, ainsi, détourner un tiers des paiements. La prise de conscience de ce type de risque par les PME et la modification de leur modèle mental sont donc deux enjeux essentiels.

Malheureusement, la vulnérabilité est devenue la norme et les attaquants savent de mieux en mieux en tirer profit. Une étude de 2020 a montré que 64 % des entreprises étaient totalement novices en matière de cybersécurité, chiffre qui serait très supérieur si l'on excluait de ce panel les grandes entreprises bien protégées. Selon cette même étude, entre 2019 et 2020, le coût des incidents a, en moyenne, quadruplé en France et aux États-Unis, voire décuplé dans certains pays européens comme l'Irlande, les fonctions business, très interconnectées, dépendant de plus en plus du numérique. Outre leur coût financier, de telles attaques affectent les salariés de ces entreprises en les privant de leur outil de travail, voire de leur revenu.

En partenariat avec OpinionWay, Qontrol a mené une enquête auprès de PME qui montre que la frontière entre usages professionnels et personnels de l'informatique est très peu perçue par les employés, les pratiques quotidiennes les entremêlant largement. Ainsi, 49 % des salariés accèdent à des informations professionnelles et 38 % en transmettent via leur compte personnel. Par ailleurs, 54 % des personnes interrogées estiment n'avoir aucun rôle à jouer concernant la cybersécurité, s'en remettant pour cela à leur employeur, attitude qui serait inconcevable en matière de sécurité physique. Il est donc urgent de faire comprendre à tous, employeurs comme salariés, qu'un profond changement de culture est nécessaire et que croiser les doigts ne suffit plus pour se préserver du risque.

Les raisons profondes d'un tel blocage des mentalités sont cependant très rationnelles et ne peuvent être imputées à l'ignorance ou à la négligence des seuls individus. Tout d'abord, le risque cyber est insaisissable pour un non spécialiste et les effets d'une intrusion sont difficiles à anticiper. Ensuite, le marché de la protection est très obscur, les moyens proposés étant pléthoriques, mais trop techniques et peu compris des responsables de la sécurisation de leur entreprise. Enfin, il est difficile de valoriser une bonne cybersécurité qui, dans l'esprit d'un dirigeant, n'apparaît pas comme un avantage compétitif pour son entreprise, mais comme une charge supplémentaire. Face à ce blocage, il est de notre responsabilité, en tant que professionnels, d'apporter aux différents acteurs des PME les outils nécessaires pour appréhender les risques et y répondre, en leur proposant des solutions qui aient du sens pour eux.

Pourquoi se protéger ?

Si les grands groupes et les ETI commencent à mieux se structurer en créant des équipes dédiées à leur sécurisation, une telle démarche n'est guère à la portée des PME. Cela peut cependant leur coûter fort cher, tant financièrement qu'en matière de confiance et d'image de marque, en particulier dans le cas d'une start-up. Il en va de même pour des entreprises de service, comme des cabinets de conseil ou de recrutement, pour qui la perte de données personnelles peut être fatale.