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 relais 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.

Parmi les impacts à considérer, ceux causés par les *ransomwares* ont trouvé un large écho dans les médias, le nombre de ces attaques, sur des hôpitaux, des collectivités ou des entreprises, ayant explosé ces derniers temps. Dans ce cas, le but de l'attaquant est de pénétrer dans le système informatique d'une structure, afin d'identifier puis de chiffrer ses données pour les rendre indisponibles jusqu'à ce qu'une rançon lui soit versée. S'il parvient à rester des semaines ou des mois dans le système sans être détecté, il pourra alors être en mesure non seulement d'infecter les systèmes de production de la structure, mais aussi de corrompre ses systèmes de sauvegarde si ceux-ci sont constamment connectés au système et trop rarement vérifiés. Les technologies récentes visent à pallier ces vulnérabilités en rendant les sauvegardes hermétiques. Le jour où une attaque est lancée, si les sauvegardes censées pouvoir restaurer les données ne fonctionnent plus, l'entreprise sera alors sans défense et aura, par exemple, perdu toutes ses informations de commande ou de facturation. Le problème des *ransomwares* est mondial, car les robots procédant à ce type d'attaque peuvent être basés n'importe où et visent prioritairement les systèmes largement exposés sur Internet et peu protégés. La détection précoce est donc un enjeu majeur, de même que la compréhension des stratégies d'intrusion, afin d'éviter qu'après avoir restauré l'intégrité du système, une nouvelle attaque puisse avoir lieu selon les mêmes méthodes.

Les vecteurs d'entrée soit résident dans une faille d'un système exposé à Internet par laquelle le *ransomware* est introduit, soit résultent d'interventions humaines intempestives – l'ouverture d'une pièce jointe infectée, par exemple. À cause d'un e-mail malveillant ouvert par inadvertance, le centre hospitalier universitaire de Rouen a subi l'attaque d'un *ransomware* durant plusieurs jours, imposant à tous ses services de se réorganiser à la hâte avec d'anciennes procédures physiques. En Allemagne, une patiente est récemment décédée lors de son transfert vers un autre hôpital, celui qui était prévu ne pouvant l'accueillir à la suite d'une attaque de ce type. Statistiquement, de tels accidents sont malheureusement appelés à se reproduire. Les établissements de santé sont particulièrement vulnérables, car les arbitrages budgétaires privilégient toujours la réponse à un risque immédiat pour le patient à la sécurisation à terme de la structure.

D'autres impacts sont dus à des mécanismes de fraude plus classiques, bien qu'utilisant des vecteurs numériques. Le département du Nord a ainsi été victime d'une énorme arnaque aux faux ordres de virement. Dans ce cas, l'escroc a discrètement pris le contrôle de l'adresse mail du responsable financier d'une entreprise dont il a ensuite usurpé les identifiants et changé le RIB, afin de se faire indûment régler une facture d'un montant de 800 000 euros. Dans certains cas, l'arnaque se fait en passant par le bais d'un fournisseur avertissant d'un prétendu changement de coordonnées bancaires, sans que le système de l'entreprise visée n'ait été corrompu. La question qui se pose est donc celle du durcissement des procédures de contrôle internes, qui doivent désormais prendre en compte une éventuelle corruption des systèmes d'information (SI) des partenaires extérieurs de l'entreprise.

Qontrol a elle-même été indirectement victime d'une telle "cyberarnaque" lors de sa levée de fonds auprès de ses *business angels*. L'un d'entre eux, un particulier qui s'était engagé à investir 50 000 euros, a été cyberarnaqué par des processus d'intelligence sociale et a perdu plus que cette somme sur son argent personnel. Ne pouvant plus honorer son engagement, il s'est désisté. Cette anecdote illustre bien le fait que l'attaque sur l'un de vos partenaires peut aussi indirectement vous affecter.

La mainmise sur le site web d'une entreprise ou d'une institution est un autre type d'attaque. Dans ce cas, il s'agit de modifier des messages existants (défiguration), voire d'en publier d'autres, indésirables (graffitis numériques) ou malveillants. Fréquemment, de petites mairies, parfois sans contrat de maintenance de leur site ou le gérant approximativement, sont l'objet de telles attaques.

Le partenaire, vecteur du risque

Les menaces sur les PME peuvent devenir des menaces pour leurs grands donneurs d'ordres de plusieurs façons.

La première est l'infection et la compromission par contagion. Naguère, la protection d'une entreprise était envisagée comme devant être "périmétrique", c'est-à-dire être constituée de remparts censés empêcher toute intrusion. Du fait des partages croissants d'informations entre un groupe et son écosystème de start-up,

de clients et de fournisseurs, ce périmètre s'étend aujourd'hui à l'ensemble de ses partenaires. Désormais, pour lui dérober des informations sensibles, un potentiel adversaire économique ne s'attaquera plus directement au grand groupe dont il connaît les défenses, mais passera par ses partenaires, plus vulnérables aux intrusions. L'aéronautique a connu ce problème avec des attaques coordonnées sur 15 sous-traitants d'Airbus détenant chacun les informations sur le sous-ensemble qu'ils fabriquaient. Un concurrent indélicat n'a alors plus eu qu'à agréger les informations ainsi dérobées pour obtenir non seulement les caractéristiques de l'équipement complet, mais aussi, ce qui l'intéressait davantage, les processus de certification sur les marchés français et européens mis en œuvre par ces sous-traitants.

Une autre menace réside dans la perturbation d'une chaîne d'approvisionnement du fait de la défaillance de l'un de ses maillons à la suite d'une cyberattaque. La base de données de la police de New York a ainsi été totalement bloquée, le sous-traitant qui l'opère ayant été la cible d'une attaque. Une étude de 2019 estime que 65 % des grandes entreprises ont dû gérer, cette année-là, un tel cyberincident. Alors que le risque de faillite d'un sous-traitant est depuis longtemps pris en compte dans les processus actuels des grands groupes, il devient urgent que ces derniers intègrent également le risque numérique dans leur stratégie. D'autres incidents, de nature proche, sont liés aux détournements d'outils marketing sur Instagram ou d'autres sites, par exemple à la suite de l'utilisation, sur un site vierge, d'un mot de passe déjà utilisé sur un site infecté.

L'usage des réseaux sociaux par les employés au sein de l'entreprise peut également être source de problèmes importants. Ainsi, la diffusion sur Internet de photos d'employés grimés en femmes noires lors d'une soirée privée a déclenché une vague d'indignation sur le Web. Leur entreprise a dû se désolidariser de ces pratiques jugées racistes afin de couper court à un boycott de ses produits. Une charte des bonnes pratiques, partagée et comprise, peut parfois suffire à protéger l'image d'une start-up, mais le problème est complexe et c'est pourquoi nous sensibilisons nos clients à la survenue de tels risques.

Outre le paiement d'une éventuelle rançon, ces incidents coûtent du temps de gestion de crise et entachent la réputation de l'entreprise. Aspect souvent méconnu, ils affectent également les équipes en créant de fortes tensions internes, voire des détresses psychologiques quant à la responsabilité de tel ou tel salarié dans leur survenue. Dans le cas de start-up, il est aussi arrivé que des employés mécontents quittent la structure en mettant en cause les mesures prises pour sécuriser, par exemple, des bases de données personnelles ou médicales, ce qui mine la confiance des usagers. Tout cela nécessite alors des stratégies de gestion de crise classiques qu'une prévention et des pratiques inattaquables, pourtant censées être la règle, auraient pu éviter.

Enfin, l'incendie survenu récemment chez OVH à Strasbourg est venu rappeler que le cloud reposait avant tout sur des matériels, susceptibles de défaillir comme tout autre matériel physique. Cela pose alors la question de la sécurité de ces serveurs, mais aussi celle des données hébergées, certains services ne garantissant que le stockage des données et non leur sauvegarde, en se gardant parfois de le préciser. Face à ce risque de perte de données, il est prudent de payer un service de sauvegarde en plus du seul hébergement. Nous recommandons à nos clients d'appliquer leur plan de continuité d'activité, qu'ils ont chacun la responsabilité de mettre en place dans leur propre structure, sans s'en remettre aux seules solutions externes.

Le risque systémique majeur, décrit dans un rapport de l'Institut Montaigne en 2018, serait d'être confronté à la chute simultanée d'un grand nombre de PME à la suite d'une cyberattaque, ce qui aurait pour effet de déstabiliser massivement les chaînes de sous-traitance. Au sein de notre écosystème largement interconnecté, la cybersécurité des PME est ainsi devenue un bien commun qu'il faut défendre.

Une nouvelle fonction support

Il est désormais temps de considérer la cybersécurité comme une fonction support des entreprises, au même titre que la gestion de leurs salariés ou la comptabilité. C'est d'autant plus nécessaire que les responsables de la sécurité des systèmes d'information (CISO) des grands groupes durcissent leurs politiques de sécurité et imposent contractuellement à leurs partenaires, PME ou start-up, d'avoir à prouver leur conformité

à des règles de plus en plus strictes. C'est donc pour que nous les aidions à faire face à ces obligations croissantes, souvent complexes et longues à mettre en place, que les clients sollicitent les services de Qontrol.

Ainsi, une start-up va devoir fournir les preuves que son personnel a été formé à ses règles de sécurité interne, que sa politique globale de sécurité est régulièrement auditée, qu'elle engagera dans les six mois une démarche de certification ISO 27001 ou SOC 2, ce qui représente, outre les coûts de gestion, une dépense d'au moins 100 000 euros. Des contraintes techniques particulières peuvent aussi s'imposer, tout comme des obligations de service, telle celle d'engager tous les ans un prestataire externe pour une mission premium de conseil. Évidemment, certaines de ces exigences sont parfaitement hors de portée pour des entreprises d'une quinzaine de personnes. Un jeu de dupes peut alors s'engager, la PME voulant obtenir le contrat coûte que coûte, quitte à masquer ses failles de sécurité, et le donneur d'ordre s'estimant dédouané de toute responsabilité en cas d'incident, dès lors que son sous-traitant n'a pas respecté ses obligations contractuelles.

La cybersécurité est donc bien devenue une fonction support comme les autres, puisqu'elle est désormais indispensable pour structurer l'activité d'une entreprise et asseoir la confiance qu'elle se doit de garantir à ses partenaires. Les start-up et les PME rencontrent cependant des difficultés fondamentales lorsqu'elles essaient d'atteindre un tel niveau. Tout d'abord, il s'agit d'un sujet hautement technique et les arbitrages sont complexes, du fait de la difficulté à appréhender ce qui sous-tend les attaques comme les défenses et à anticiper d'éventuels effets dominos. C'est également un problème organisationnel et humain, car la conduite d'un tel changement des comportements n'est pas simple. Surtout, il n'existe pas de solution rentable économiquement qui rende ce changement possible, voire désirable. Ainsi, l'obligation de disposer d'une ressource humaine interne dédiée à la cybersécurité est irréaliste pour une PME, tant pour des raisons économiques – le coût étant le plus souvent disproportionné face à celui du risque encouru – que de manque de spécialistes disponibles sur le marché.

La réponse de Qontrol

Malheureusement, il n'existe rien pour exprimer un niveau de cybersécurité intermédiaire entre la norme ISO 27001 et l'absence de mesures. Un référentiel exprimant différents niveaux de sécurité et guidant les dirigeants dans la structuration de cette nouvelle fonction support est donc nécessaire. Chaque donneur d'ordre devrait également pouvoir exprimer ses exigences en les reliant à tel ou tel niveau de sécurité préalablement défini par ce référentiel. Le futur de la cybersécurité devrait s'inspirer du rôle des directions régionales de l'environnement, de l'aménagement et du logement (DREAL) en matière de sécurité physique et environnementale des sites industriels.

Notre ambition est d'apporter des réponses relativement légères aux PME, sous forme d'une boîte à outils destinée à orchestrer leur politique de sécurité. Nous ne leur demandons évidemment pas de connaître tout de la cybersécurité, mais nous automatisons la prise d'information et le diagnostic sur leur structure. Pour cela, nous posons à chacun de leurs salariés des questions adaptées à son degré de connaissance dans ce domaine et formulées dans un langage qu'il comprend. Un utilisateur pourra en effet ne pas savoir s'il utilise le cloud ou un "filtre 365", mais il saura toujours expliquer comment il sauvegarde ses documents. Sur la base de ses réponses, nous identifions les informations techniques qui nous intéressent et en déduisons automatiquement des plans d'action priorisés, efficaces et adaptés à la grande variabilité des situations de chaque PME. Un plan d'action type comporte toujours plusieurs options, qui sont soumises à l'arbitrage des dirigeants. Celle qui est retenue est ensuite déployée auprès des salariés par la plateforme Qontrol, avec des tutoriaux et, parfois un outil, parfois la mise en place d'un *process* simple.

L'enquête automatisée de Qontrol donne lieu à un rapport qui permet à la PME de décider de sa politique de cybersécurité en toute clarté sur les trois volets que sont la prévention, la détection et la réponse. Ce rapport pouvant être partagé en confiance avec ses donneurs d'ordre, il devient un avantage compétitif pour la PME en renforçant sa crédibilité, en constituant un argument marketing auprès de ses clients et en représentant un avantage dans ses négociations avec sa banque ou son assureur.

Qontrol permet ainsi de déployer une politique organisée, mise en œuvre par sa plateforme de la même façon que si elle l'était par un spécialiste à demeure dans l'entreprise. Nous délivrons alors un Passeport Sécurité, à plusieurs niveaux, dont nous ambitionnons que l'usage puisse être généralisé en France avant que des référentiels anglo-saxons ne s'imposent chez nous.

Débat

Un modèle économique simple

Un intervenant : *Concrètement, que propose Qontrol à de petites structures associatives, comme l'École de Paris du management ?*

Michael Monerau : Tout d'abord, chaque personne intervenant dans la structure est identifiée dans un compte ouvert sur la plateforme Qontrol, qui exerce alors sa fonction support dans le cadre d'un abonnement mensuel. Notre premier travail est de recueillir quotidiennement auprès de chacune d'elles, en trois minutes, par le biais de la plateforme, le maximum d'informations pour comprendre le fonctionnement de la structure : qui reçoit quoi ? quels périphériques sont utilisés par qui ? qui travaille sur quels fichiers ? quels sont les actifs informationnels de la structure ? certaines informations personnelles sensibles relèvent-elles du RGPD ? qui y a accès ? etc.

En une quinzaine de jours, on obtient généralement suffisamment d'informations pour comprendre les intérêts de la structure et identifier les points à protéger. Dès lors, nous établissons un plan d'amélioration continue, justifié par des faits concrets. La plateforme définit ensuite le parcours et les *process* à mettre en œuvre pour corriger les vulnérabilités identifiées. Si la direction valide ce plan, des *playbooks* sont installés sur le poste de travail de chacun afin de le guider dans les 15 ou 20 tâches qu'il aura à effectuer, à son rythme, au fil de son parcours utilisateur personnalisé.

Notre modèle économique est simple : nous ne facturons que 10 euros par personne et par mois pour l'abonnement à la plateforme. Ce tarif peut paraître faible, mais nous préservons ainsi la capacité des petites structures à investir dans des solutions de sécurité quand elles en ont un besoin avéré. Dès lors que nous recommandons telle ou telle solution à un problème, nous agissons ensuite en tant que *market place*, en touchant une commission versée par le vendeur de cette solution si l'achat se concrétise. Nous ambitionnons de gagner en moyenne 5 euros supplémentaires, par personne et par mois, avec cette activité de *market place*.

Int. : *En quoi vos interventions se distinguent-elles de celles des infogérants ?*

M. M. : Le rôle des infogérants étant de fournir des moyens techniques, nous travaillons avec eux pour avoir accès aux données qu'ils traitent. En revanche, ils n'interviennent pas sur la nature de ces informations, pas plus qu'ils n'éduquent les usagers aux bonnes pratiques. L'intérêt, pour l'infogérant, de cette collaboration avec nous est double. Tout d'abord, par la prévention, nous réduisons le nombre de sinistres qu'il a indûment à traiter, les PME l'appelant en priorité pour remettre en état un SI suite à des attaques dont il n'est en rien responsable. En second lieu, si notre client a besoin d'une mise à niveau de son équipement, nous le renvoyons systématiquement vers son infogérant dans le cadre de notre *market place*.

Int. : *Vos propositions sont-elles des engagements de moyens ou de résultat ?*

M. M. : Nous proposons uniquement d'externaliser une politique de sécurité de l'information par le biais d'une plateforme. Nous garantissons non pas que l'entreprise ne subira pas d'incident, mais qu'elle l'aura

suffisamment anticipé pour, le moment venu, être en mesure d'en minimiser l'impact et de restaurer au plus vite son activité. Une telle capacité est, en elle-même, rentable. Nous ne sommes donc pas là pour protéger des ordinateurs, mais pour préserver l'activité de l'entreprise. Un risque mesuré, sous contrôle et de moindre coût qu'une protection sophistiquée, peut aussi être délibérément assumé. En dernier ressort, c'est le dirigeant qui choisit ce à quoi il est en mesure de faire face. Nous le conseillons alors pour mettre en place son plan de continuité d'activité.

Int. : *Lorsque vous faites une proposition à une entreprise, évaluez-vous le coût interne de la mise en œuvre de vos recommandations, qui doit dépasser largement le montant que vous lui facturez ?*

M. M. : Le coût interne, tant financier qu'en matière de ressources humaines, est effectivement important et, pour l'instant, il nous est difficile de l'évaluer compte tenu de notre manque de recul. C'est la raison pour laquelle nous aidons prioritairement les entreprises à organiser leur démarche en établissant des étapes et en échelonnant leurs échéances. La psychologie cognitive nous y aide, en donnant des clés pour apprendre aux gens comment modifier, dans leur propre intérêt, leur comportement. L'approche que nous privilégions est celle du *microlearning*, qui s'attache à mettre en lumière quelques points d'intérêt spécifiques plutôt que d'accabler les personnes de consignes impératives.

Int. : *Qui vérifie que vos recommandations sont régulièrement suivies par les collaborateurs de vos clients ?*

M. M. : Actuellement, nous le faisons indirectement par le biais du recueil d'indicateurs sur les usages, dont nous suivons l'évolution par nos questions régulières et dans le cadre de la relation de confiance que nous créons. Même si ces photographies ne peuvent être certifiées conformes, elles valent infiniment mieux que leur absence ! On peut imaginer qu'à terme, selon les différents niveaux du Passeport Sécurité, on ne se contente plus de déclaratifs et que des audits de contrôle puissent être menés.

Int. : *Comment communiquez-vous avec vos abonnés en détresse ?*

M. M. : Nous sommes une start-up, nous traitons donc en direct et immédiatement tous les appels qui arrivent sur nos portables, sans avoir, pour le moment, à organiser une vraie permanence téléphonique. C'est un sujet sur lequel nous devrons nous pencher avec la structuration de l'entreprise et l'augmentation du nombre d'incidents à traiter. Aujourd'hui, notre formule d'abonnement comporte une clause garantissant notre intervention d'urgence pour sécuriser le SI en attendant l'intervention des spécialistes qui rétabliront son intégrité. Notre rôle est d'abord de stabiliser les choses et de rassurer notre abonné. Dans le même temps, nous captons les signaux d'incident qui contribuent ensuite à nourrir notre modèle statistique de recommandations et à les prioriser en fonction des menaces réelles qui pèsent sur les entreprises.

La fragilité des réseaux

Int. : *Que pensez-vous de la fragilité d'Internet en général et des outils Windows en particulier ?*

M. M. : L'infrastructure d'Internet et celle des télécoms n'ont pas été pensées pour être sécurisées, ce qui explique le succès actuel des attaques, en particulier sur les cartes SIM avec le détournement de SMS ou d'appels. Il faut donc sans cesse ajouter des couches de sécurité sur les protocoles existants, non sécurisés tel TCP/IP, avec des VPN (*virtual private network*), des passerelles sécurisées, etc., qui alourdissent à la fois la lisibilité et les coûts opérationnels, sans traiter le problème à sa source. Windows, en revanche, a beaucoup amélioré son niveau de sécurité dans ses dernières versions. Encore faut-il les utiliser et faire les mises à jour…

Int. : *Les antivirus sont-ils réellement efficaces ?*

M. M. : Bien que les grands noms du marché ne soient pas fiables à 100 %, ils captent la majeure partie des *ransomwares*. Ils peuvent aussi empêcher qu'une menace ne se répande dans le réseau de manière automatique. Ils font donc partie des mesures qu'il faut prendre, mais ce ne sont que l'un des outils de la panoplie, car votre patrimoine informationnel ne réside majoritairement plus sur votre ordinateur. S'il reste important de sécuriser votre point d'accès pour que, par exemple, personne ne copie ce que vous

tapez sur votre clavier et obtienne ainsi votre mot de passe, l'antivirus utilisé ne protège pas pour autant l'accès à vos informations dans un espace partagé comme le cloud. La protection des mots de passe et des modes d'identification devient alors plus importante que celle de l'ordinateur.

Int. : *Votre proposition comporte-t-elle des* stress tests *?*

M. M. : Notre analyse stratégique repose sur le constat que tous les outils et services nécessaires à une excellente protection sont disponibles sur le marché. Il existe donc des spécialistes de ces *stress tests* et nous ne sommes là que pour faire les mises en relation en permettant à la PME de choisir le cocktail de mesures qui a le plus de sens pour elle. Cependant, le coût de ce genre de service risque très rapidement de dépasser le retour sur investissement attendu par la PME.

Int. : *Aujourd'hui, les attaques peuvent venir par le biais de n'importe quel smartphone. Comment peut-on intégrer cette nouvelle donne ? Faudrait-il n'autoriser que des téléphones sécurisés dans les entreprises ?*

M. M. : Si l'on contraint trop les gens, ils cherchent à contourner les mesures restrictives en s'exposant encore plus aux risques, par exemple, en utilisant des services gratuits non sécurisés pour leurs transferts de fichiers. Il vaut alors mieux accompagner ce que les gens souhaitent faire en leur donnant le moyen le plus sûr de le faire. Si la culture de l'entreprise est de donner des téléphones pros qui servent aussi aux usages personnels, nous prodiguons des conseils sur le meilleur usage possible. Il reste certes des risques, le tout est d'en être conscient et de les assumer.

Int. : *Pourquoi n'attaque-t-on pas en retour les très profitables entreprises de hackers qui nous attaquent ?*

M. M. : C'est une question complexe, qui touche aux stratégies militaires et de défense. Il est difficile d'attribuer avec certitude la responsabilité d'une attaque à tel ou tel acteur, privé ou étatique, et la discrétion la plus totale entoure les éventuelles ripostes. Dans le cas de l'attaque de mai 2021 menée par un *ransomware*, aux États-Unis, contre Colonial Pipeline, qui a été contraint de fermer à la suite du vol de plus de 100 gigaoctets de données, la rançon de 4,4 millions de dollars a été payée en bitcoins. Bien que les transactions en bitcoins soient censées être invisibles, le département de la Justice américain a pu retracer les transferts et récupérer la quasi-totalité des fonds. Des opérations de rétorsion ont ensuite été menées contre les attaquants et rendues publiques, dans le but de dissuader les hackers de toute nouvelle tentative sur des intérêts publics vitaux.

Savoir grandir

Int. : *Concrètement, comment s'est passé votre développement ?*

M. M. : Pour moi, tout a commencé il y a trois ans, seul et en partant de rien. Je me suis interrogé sur la possibilité de réaliser un diagnostic par le seul biais d'un questionnaire et j'ai commencé à le rédiger, alors que tout le monde me disait que pour réaliser un audit cyber, il fallait aller sur le système. Très vite, j'ai pu vérifier auprès de mes premiers clients, volontaires pour tenter cette expérience, que ma proposition avait du sens. J'ai ensuite signé un premier contrat avec Orano, fournisseur de référence dans le secteur du nucléaire, qui m'a introduit dans le monde de ses sous-traitants, ce qui m'a permis d'asseoir ma crédibilité et a renforcé la confiance de mes interlocuteurs.

Ayant quitté le secteur public, il fallait que cette activité puisse aussi me rémunérer. Une première levée de fonds de type BSAR (bons de souscription d'actions remboursables) de 125 000 euros a apporté à l'entreprise ses premiers moyens. La deuxième version de la plateforme à peine terminée, et alors qu'un contrat devait être signé avec un autre grand groupe, la pandémie de la Covid-19 a mis un coup d'arrêt à la prospection commerciale. J'ai profité des premiers confinements pour réaliser des itérations du produit et, à leurs levées, j'ai pu tester ces idées chez quelques nouveaux clients. À la fin de la deuxième année, quand mon associé m'a rejoint, l'idée était stabilisée et les retours d'expérience nous ont permis de réajuster la plateforme durant l'été 2021.

L'État nous a alors soutenu en nous allouant une subvention de 230 000 euros, obtenue dans le cadre du Grand Défi Cyber du PIA (programme d'investissement d'avenir), dont nous avons gagné le Grand Prix. Tout cela conjugué a donné confiance à des *business angels*, moins préoccupés de retours rapides sur leur

investissement que les financiers classiques. Ils nous ont apporté 415 000 euros et nous sollicitons aujourd'hui, auprès de Bpifrance, un prêt de 400 000 euros pour le développement de l'innovation. Nous avons ainsi pu lancer avec succès notre nouvelle formule, qui a engendré 2 000 euros d'abonnements mensuels dès les premières semaines. Notre objectif est aujourd'hui de dépasser les 10 000 euros d'abonnements mensuels, limite au-delà de laquelle l'ajustement du produit au marché (*market fit*) sera trouvé.

Désormais, notre principal souci est de constituer l'équipe qui servira au mieux notre projet. Nous avons confié à un cabinet spécialisé l'embauche la plus importante pour nous, celle de l'expert cyber qui va contribuer à créer l'automatisation des conseils. Nous recrutons deux développeurs pour l'application, un commercial et un designer pour le marketing du produit.

En ce qui concerne la normalisation, nous avons des discussions au sein de la sphère publique avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et avec des responsables du ministère de l'Intérieur pour bien comprendre comment se positionnent les différents acteurs. Je travaille également avec le groupement d'entreprises Hexatrust et l'Alliance pour la Confiance Numérique (ACN), un cluster qui représente les entreprises du secteur et aborde notamment les questions de sécurité sous l'angle des assurances. Les référentiels existent, il faut simplement organiser leur version française.

Présentation de l'orateur

Michael Monerau : Normalien et ingénieur du Corps des mines, agrégé de mathématiques et d'informatique, il a débuté une carrière dans le domaine de la cybersécurité à l'École normale supérieure, puis dans le privé au sein de Microsoft Research, dans des start-up françaises du numérique et dans la Silicon Valley (Exalead, Qosmos). Au ministère de l'Économie et des Finances, il a ensuite œuvré à la modernisation et à la numérisation des PME françaises (Programme d'investissement d'avenir 3, Industrie du Futur). Constatant les problématiques de cybersécurité qu'elles rencontrent, il a créé Qontrol pour les accompagner dans leur transition digitale en leur apportant des solutions immédiatement actionnables et en parfait alignement avec leurs intérêts économiques.

Diffusion juin 2022

Retrouvez les prochaines séances et dernières parutions du séminaire Management de l'innovation sur notre site www.ecole.org.