SPARRING CAPITAL

ÉDITO

LA CYBERSÉCURITÉ

Deux sur trois : c'est le nombre d'entreprises françaises qui auraient été confrontées à une attaque de leur système informatique en 2018. Alors que pendant de nombreuses années, ce risque a été perçu comme un sujet de « grande entreprise », la cybersécurité est aujourd'hui un enjeu pour l'ensemble du tissu économique, notamment parce que les PME / ETI sont souvent moins bien protégées que les grands groupes tout en disposant d'informations critiques. Facteur aggravant : elles disposent souvent de moins de moyens pour répondre efficacement à un acte de malveillance et, dès lors, toute attaque sérieuse peut durablement impacter leur exploitation.

La protection des systèmes informatiques de l'entreprise passe par le déploiement d'une approche construite autour de quelques piliers tels que la mise en place d'un plan de prévention, la construction et la mise à l'épreuve d'un système de sauvegarde, la constitution d'une force de réaction rapide et la souscription à une assurance.

Pour approfondir ce sujet, nous avons choisi d'associer à cette newsletter de l'automne Messieurs Lari Lehtonen (responsable de l'équipe « cyber risques » chez Marsh France) et Jean-François Louâpre (expert en cybersécurité), dans le cadre d'une interview croisée.

Bonne lecture !

L'équipe Sparring Capital

ACTUALITÉS DU PORTEFEUILLE

Acquisition de Cesacap

Sparring a réalisé en avril l'acquisition de Cesacap, acteur majeur du génie électrique en Ile-de-France, auprès de Capzanine, de SG Capital Partenaires et des fondateurs du groupe dans le cadre de sa transmission à une nouvelle équipe dirigeante.

Fondé en 1981, le groupe Cesacap dispose d'une expertise en courants forts et en courants faibles, avec une forte présence en Ile-de-France. Cesacap possède la capacité d'accompagner ses clients sur toutes tailles de projets, en rénovation comme en neuf. Le groupe bénéficie également d'une belle répartition de son activité, avec en particulier une forte reconnaissance en tertiaire (société Cesa), en habitat social (société Perrin) ou encore en résidentiel neuf (société Meusnier).

Le groupe, qui a réalisé en 2018 un chiffre d'affaires de l'ordre de 50 millions d'euros pour 250 employés, a connu ces dernières années une solide évolution sous l'impulsion de Franck Petit, son Président, qui a su renforcer les équipes avec notamment l'arrivée de Fabrice Gaté en tant que Directeur Général en 2017. Cette croissance repose aussi bien sur les savoir-faire historiques du groupe que sur sa politique de diversification maitrisée.

Un plan de développement ambitieux a été mis au point par l'ensemble des partenaires du projet afin de poursuivre la stratégie de croissance organique et de relancer la politique de croissance externe du groupe.

Acquisition de Softair par Cesacap

Quatre mois après l'arrivée de Sparring Capital, le groupe Cesacap (renommé Weecap à l'été 2019) a réalisé sa première opération de croissance externe en intégrant la société Softair, spécialisée dans le génie climatique.

Softair intervient dans l'installation, la maintenance et le dépannage d'équipements de chauffage, de ventilation et de climatisation. La société opère principalement en Ile-de-France sur des chantiers de rénovation de bâtiments non résidentiels et a réalisé plus de 10M€ de chiffre d'affaires en 2018.

Grâce à ce rapprochement, le Groupe diversifie son offre de service et bénéficie de synergies commerciales et opérationnelles comme le positionnement sur des appels d'offres combinant les lots génie électrique et génie climatique (un premier chantier commun ayant d'ores et déjà été remporté par les équipes), des prestations additionnelles offertes aux clients de chacune des deux entreprises et l'ouverture à de nouveaux types de projets.

Acquisition de Nalys

Sparring Capital s'ouvre à l'international avec l'acquisition de Nalys, groupe de conseil en ingénierie belge.

Créé en 2011, le groupe connaît une dynamique de croissance très soutenue, notamment grâce à son savoir-faire sur le recrutement de profils pertinents et la mise en place d'un institut de formation interne. Nalys s'adresse à la fois à des clients grands comptes et des PME, principalement dans les domaines de la Santé et des Systèmes Embarqués.

Fort de plus de 220 consultants, le groupe affiche plus de 23 millions d'euros de chiffre d'affaires et compte dans les prochaines années poursuivre sa croissance organique en Belgique et se développer en France où elle réalise aujourd'hui 10-15% de son chiffre d'affaires.

Cette opération a permis la sortie de deux des trois fondateurs, tandis que le dirigeant-fondateur Patrice Serange, ancien dirigeant d'Alten Belgique, se renforce au capital.

INTERVIEW

Lari Lehtonen **est le responsable de l'équipe « cyber risques » chez Marsh France.**

Jean-François Louâpre **exerce des missions de conseil et de formation en matière de**

cyber sécurité. Après avoir été RSSI de CNP Assurance et d'AG2R La Mondiale, Jean-François accompagne des entreprises de plus petite taille, principalement dans le secteur financier.

Pouvez-vous nous donner une perspective sur l'ampleur du risque « cyber » pour les entreprises ?

Lari Lehtonen : *« De l'ordre de deux entreprises françaises sur trois ont été confrontées à une attaque de leur système informatique en 2018. Même si ce type de statistique est difficile à confirmer, nous notons chaque année une forte progression dans la mise en jeu des assurances « cybersécurité » par les entreprises, avec une progression de 70% entre 2017 et 2018 et, pour 2019, un niveau équivalent à l'ensemble de l'année 2018 atteint dès fin juin 2019.*

Le top-3 des sinistres est (1) les attaques de type « ransomware » avec tentative d'extorsion de fonds pour redonner accès aux données (2) les attaques de type « denial of service » qui conduisent à la mise hors ligne d'un serveur informatique et (3) les fuites de données personnelles, qu'elles soient malveillantes ou accidentelles. »

Jean-François Louâpre : *« D'après une étude publiée par le CESIN[(1)] en début d'année, de l'ordre de 80% des 200 plus grandes entreprises françaises ont subi une attaque en 2018 et je suis d'accord avec l'ordre d'idée évoqué par Lari.*

En effet, les grosses PME / ETI deviennent des cibles de plus en plus attractives pour les cybers criminels car elles sont généralement moins bien préparées, et protégées, que les grands groupes, tout en disposant de données très intéressantes. On note également une recrudescence des attaques de plus petites sociétés avec pour objectif de s'en servir comme « porte d'entrée » pour ensuite pénétrer le système informatique de plus grandes entreprises avec qui elles seraient en relation d'affaires. »

[(1)] Club des Experts de la Sécurité de l'Information et du Numérique

De votre expérience, quelles sont les conséquences pour les entreprises concernées ?

Lari Lehtonen : *« La première conséquence est d'ordre organisationnel avec très rapidement des conséquences financières, qu'il s'agisse de pertes d'exploitation provenant d'une incapacité à produire ou à vendre à cause d'une défaillance du système informatique ou qu'il s'agisse des coûts engagés pour restaurer à la fois le système informatique et les données qui auraient pu être corrompues.*

En ce qui concerne le coût pour les entreprises subissant ces attaques, celui-ci est naturellement très variable, en fonction de la taille des entreprises concernées et des typologies d'attaque, et peut schématiquement aller de quelques dizaines de milliers d'euros à plusieurs millions d'euros. Il est toutefois raisonnable de considérer que pour une grosse PME ou une ETI, ce montant peut vite atteindre quelques centaines de milliers d'euros. De notre perspective, une attaque de type ransomware impacte l'activité pendant en moyenne 3 semaines. Dans certains cas, les effets des attaques se sont prolongés jusqu'à 9 semaines avant de retrouver la situation nominale. »

Jean-François Louâpre : *« Effectivement, il faut parfois compter en semaines, voire en mois pour revenir à une situation normale. Sur les conséquences, il est utile de rappeler également que les enjeux financiers ne sont qu'une partie du problème. L'enjeu réputationnel est au moins aussi important car une attaque massive engendre une perte de confiance de la part des partenaires de l'entreprise : perte de confiance de la part des consommateurs en cas de vol de données personnelles ou encore perte de confiance des partenaires commerciaux si cette attaque a permis à des tiers d'avoir accès à de la propriété intellectuelle sensible, voire d'accéder à leur propre système. On note d'ailleurs que de plus en plus d'appels d'offres contiennent des demandes d'information relatives à la sécurité des systèmes d'information. »*

Pour se protéger efficacement, quels sont les grands principes à respecter par une PME / ETI ?

Jean-François Louâpre : *« Il faut, avant tout, arrêter de se dire « je ne suis pas concerné » et « c'est trop compliqué ». Comme indiqué dans la première partie de nos échanges, toutes les entreprises sont aujourd'hui concernées, sachant que certaines attaques telles que les ransomware ne visent pas spécifiquement une entreprise et ont pour objectif, au contraire, d'en toucher le plus grand nombre comme ce fut le cas pour Wannacry.*

Sur le degré de complexité associé à la protection informatique, j'invite les dirigeants d'entreprise à se procurer le guide ANSSI - CPME[2] qui reprend ce que l'on peut appeler des « règles d'hygiène » en matière informatique : les mesures proposées dans cet ouvrage sont simples à mettre en oeuvre, s'appliquent à toutes les entreprises et permettent de sensiblement limiter le risque. Les entreprises les plus matures pourront également appliquer les mesures, les plus pertinentes dans leur contexte, des 40 règles préconisées par l'ANSSI[3].

Toutefois, une entreprise ne pourra que limiter la probabilité du risque car, en matière de sécurité informatique, le risque zéro n'existe pas. C'est pourquoi il est important d'aller au-delà de la prévention et de prévoir un filet de sécurité pour le jour où un problème survient. »

[2] « Guide des bonnes pratiques de l'informatique » préparé par l'Agence Nationale de la Sécurité des Systèmes d'Information et la Confédération des PME
[3] Guide d'hygiène informatique

Justement, en quoi consiste un tel « filet de sécurité » ?

Jean-François Louâpre : *« Ce filet de sécurité comprend, d'une part, la préparation d'un « plan de réponse opérationnel » à mettre en oeuvre suite à une attaque et, d'autre part, la mise en place d'une assurance, sujet sur lequel je laisserai Lari s'exprimer plus spécifiquement car il s'agit d'une dimension essentielle du filet de sécurité. La préparation à une éventuelle attaque peut se décomposer en deux grands volets : la réponse à l'attaque proprement dite et la mise en place du plan de continuité.*

Pour ce qui concerne la réponse à l'attaque, la clé est d'avoir identifié des experts en amont, afin de pouvoir les faire intervenir dans les plus brefs délais si un problème survient. Le recours à un professionnel de la cybersécurité est nécessaire pour permettre à l'entreprise de prendre rapidement les meilleures décisions, circonscrire les risques et éviter le suraccident, encore faut-il savoir qui appeler lorsque le problème arrive ! L'initiative « Cyber malveillance », à destination des PME, professionnels et particuliers va réellement dans le bon sens et facilite cette mise en relation[4]. Il ne faut pas non plus négliger de s'entourer de professionnels en matière de droit et de communication lorsque l'attaque informatique touche ou risque de toucher des partenaires de l'entreprise, qu'il s'agisse de vol de données personnelles ou d'accès à des documents sensibles. Sur ce sujet, notons d'ailleurs qu'il existe des obligations d'information en cas d'incident dans certains contrats commerciaux ou encore dans la réglementation RGPD[5].

Pour ce qui concerne la préparation du plan de continuité, celui-ci doit permettre de s'assurer, à minima, que les sauvegardes de données ne puissent également être attaquées et ont été testées « à froid ». Enfin, il faut entrainer les équipes pour que l'organisation de la reprise d'activité soit la plus fluide possible le moment venu. »

Lari Lehtonen : *« Même s'il est important d'investir en cybersécurité comme l'indiquait Jean-François, ceci n'exclut pas le risque et l'assurance est donc la clé de voute de ce « filet de sécurité » : la cybersécurité réduit la fréquence mais l'intensité reste là même. Finalement, c'est un peu comme lorsqu'une entreprise protège un bâtiment avec des sprinklers : ce système permet de limiter la survenance de feux mais personne n'envisage de résilier sa police d'assurance incendie pour autant. Ainsi la cybersécurité va de pair avec l'assurance.*

Cette assurance cyber comprend trois grandes dimensions. En premier lieu, il y a la

prévention : cela peut passer par des tests de phishing, des tests d'intrusion, de la préparation à incidents... c'est quelque chose qui a tendance à se développer. La deuxième partie concerne l'assistance mise à disposition de l'entreprise lors de la réalisation de l'événement cyber : les assureurs fournissent une ligne d'urgence à partir de laquelle les sociétés victimes d'un événement cyber peuvent obtenir l'intervention de plusieurs experts (informatique, juridique, ou communication de crise) avec pour objectif de gérer au mieux et au plus vite l'événement en donnant tous les moyens possibles à la société pour repartir le plus vite possible. Enfin, la troisième et dernière dimension repose sur l'indemnisation où l'on retrouve les mécanismes usuels de l'assurance.

Il est utile de rappeler que la dimension « risque cyber » n'est généralement pas couverte dans les polices d'assurance usuellement souscrites par les entreprises. Une assurance cyber permet de couvrir les pertes d'exploitation occasionnées spécifiquement par une attaque malveillante ou un événement accidentel sur les systèmes d'information de la société, mais aussi tous les frais liés à cet événement et enfin les éventuelles réclamations liées à cet événement. Pour résumer, cette garantie couvre les préjudices subis par la société ainsi que ceux subis par les tiers suite à un événement cyber sur les systèmes d'information de la société.

En termes de coûts associés à la mise en place d'une telle police d'assurance, chaque cas est naturellement un cas spécifique mais disons que, de manière très illustrative, pour une société réalisant 50M€ de chiffre d'affaires, le coût annuel d'une couverture « cybersécurité » avec un plafond de l'ordre d'un million d'euros est de l'ordre de 5.000 à 7.000€ par an. »

[4] Liste d'experts sur le site https://www.cybermalveillance.gouv.fr/annuaire-des-specialistes/
[5] Règlement Général sur la Protection des Données