PORTRAIT

OROL

Le cyber-pompier des PME-ETI

À Bourges, la société Orol Cyber Solutions intervient au chevet des PME-ETI attaquées ou menacées. Ses dirigeants Ramzi et Sabri Khechaimia déploient une panoplie de solutions pour gérer les crises ou prévenir les cyberattaques.

Sabri et Ramzi Khechaimia fondateurs et dirigeants d'Orol Cyber Solutions.

Texte et photo
Thomas Migault

Bardés de qualifications et de certifications dans de nombreuses normes de cybersécurité, Ramzi et Sabri Khechaimia cultivent la discrétion. « La confidentialité et l'éthique », ajoutent aussi les deux frères à la tête de l'entreprise Orol Cyber Solutions. « On est très à cheval sur ces valeurs humaines. » Depuis dix ans, la forte croissance de cette société est à la mesure de la menace exponentielle du risque cyber qui pèse sur les entreprises. Dans leurs locaux berruyers, un grand écran projette à l'instant T les cyberattaques dans le monde entier. Plus de 10 millions d'actes ou de tentatives de piratages ont lieu d'un pays à un autre, rien que pour la journée du 4 décembre. « Mais c'étaient 60 millions d'attaques quotidiennes pendant le Covid », compare Ramzi Khechaimia.

Orol a été fondée à Bourges par deux frères : Sabri et Ramzi Khechaimia. Le premier est un hacker éthique, ingénieur sécurité de formation, il est passionné par la sécurité offensive ; le second accompagne les structures, les gouvernances pour être conformes avec les normes et réglementations. Leur projet est né d'un constat : « L'augmentation alarmante de la vulnérabilité des entreprises face à la menace grandissante des cyberattaques ».

« Empêcher la souris de manger le fromage »

En 2018, ils ont choisi de fonder Orol Cyber Solutions qui déploie ses services essentiellement en région Centre-Val de Loire. Leur entreprise s'est rapidement spécialisée dans la cybersécurité au fil des années, alors qu'à la création en 2014, Orol était davantage centrée sur l'infogérance « avec tout de même une particularité liée à la sécurité ». La cybersécurité représente aujourd'hui 99 % de son activité.

Remédiation (gestion d'incidents), audit, formation aux réglementations, « la cybersécurité c'est un peu l'histoire du chat et la souris. Notre travail ce n'est pas d'attraper la souris, mais l'empêcher de manger le fromage », illustre Ramzi Khechaimia. « On sait comment les hackers fonctionnent, on ne peut pas défendre les sociétés si on ne connaît pas le côté obscur... », confie le chef d'entreprise.

Les deux frères associés s'imposent la même confidentialité qu'ils promettent à leurs clients. Pas de chiffre d'affaires, ni de nombre de clients. Chaque mot est pesé. Seule leur plaquette de communication évoque plus d'une trentaine d'audits déjà réalisés. L'entreprise emploie une dizaine de salariés et cinq consultants en France. Et cherche à recruter des ingénieurs sécurité avec une sélection des profils drastique.

Du sur-mesure

Les locaux berruyers de la société sont tirés à quatre épingles. La décoration, moderne, est soignée. Hyper-sécurisée. Ici, tout respire le sérieux. Car si les équipes d'Orol Cyber Solutions se déplacent beaucoup dans les entreprises pour gérer les crises ou faire des audits, ici aussi l'activité est intense. Dans leur Security Operation Centre, où les téléphones portables sont interdits, plusieurs collaborateurs, rivés sur leurs écrans, scrutent en direct dans un silence religieux les attaques quotidiennes que subissent leurs clients. « On surveille, on fait remonter à nos clients les alertes, les menaces », résume Ramzi Khechaimia. Des surveillances qui s'organisent en astreinte ou sont automatisées. Dans une autre pièce, qui fait office de laboratoire, des tests de malwares (programmes malveillants), des décommissionnements (effacement sécurisé des données) sont réalisés. « On fait du sur-mesure », assurent les dirigeants.

Motivations lucratives, techniques ou ludiques

Si de grandes entreprises sont de manière récurrente victimes de cyberattaques avec des fuites de données personnelles à répétition, les plus petites sont également dans le viseur de la cybercriminalité. « On pense que le cybercriminel va attaquer une entreprise parce qu'il va la cibler, mais c'est souvent des attaques massives », observent les deux entrepreneurs.

Les motivations peuvent être lucratives avec une demande de rançon *(ransomware)* après la paralysie des systèmes d'information et le chiffrement des données qui se sont souvent déjà envolées dans le dark-web pour y être vendues ; elles peuvent viser la saturation des serveurs, du cyber-sabotage pour porter atteinte à l'image d'une entreprise ; ou être plus politiques, en attaquant de manière persistante des gouvernements.

La démarche du cybercriminel peut tout aussi être pathologique (vengeance d'un salarié ou d'un prestataire mécontent), technique (des groupes de hackers cherchent à démontrer qu'ils sont bons), que ludique. Les mauvaises intentions ne manquent pas. « On intervient surtout sur la partie lucrative », explique Ramzi Khechaimia qui aide aussi les entreprises à se mettre en conformité avec la RGPD *(règlement général de protection des données)*, qui s'applique obligatoirement depuis 2018. Et « on voit de plus en plus d'arnaques au président avec des faux ordres de virement », relèvent aussi les dirigeants d'Orol Cyber Solutions.

« On imagine que la cybersécurité, c'est mettre en place des mesures techniques. Mais il faut aussi des mesures organisationnelles et humaines pour protéger les actifs informatiques et les données des entreprises », insistent les deux frères. ■

Réglementations et normes

De nombreuses normes et directives s'imposent aux entreprises. Après Nis 1 (Network and Information Security Directive) qui est apparue en 2016 et a été transposée dans le droit français en 2018, la directive européenne Nis 2 se met en place. Nis 1 concernait 500 à 600 entreprises, des opérateurs d'importance vitale (santé, énergie...) et leur imposait de monter en maturité en matière de cybersécurité. Avec Nis 2, 20.000 entreprises qui ont plus de 10 millions de chiffre d'affaires et plus de cinquante salariés vont être concernées. Il y a aussi la réglementation Dora qui va s'imposer dès janvier 2025 aux sociétés de finances et d'assurances. Il y a enfin le règlement sur la cyberrésilience (CRA) qui va concerner les constructeurs d'objets connectés (caméras, montres, smartphones...). Des objets de plus en plus vulnérables qui offrent de nombreuses portes d'entrées aux cybercriminels. L'objectif est d'imposer des exigences minimales de cybersécurité pour les produits comportant des éléments numériques et garantir que les produits mis sur le marché de l'Union européenne respectent les normes de sécurité.

LE « CHAOS » d'une cyberattaque

Chez Orol Cyber Solutions, gérer une crise peut parfois prendre plusieurs semaines dans une entreprise. Les conséquences économiques et psychologiques sont parfois lourdes.

Texte et photo
Thomas Migault

« Lorsqu'une société est attaquée, on intervient pour la sauver, on est un peu comme des pompiers, expliquent Ramzi et Sabri Khechaimia, codirigeants d'Orol Cyber Solutions, à Bourges. C'est ultra-stressant. » Spécialisée dans les secteurs de la santé, l'industrie et la finance, particulièrement chez les PME et ETI, Orol Cyber Solutions fait de la remédiation, notamment à travers le programme régional CybeRéponse, le Centre de réponse aux incidents de cybersécurité en Centre-Val de Loire. Objectif : répondre à l'incident cyber, en mettant en place une gestion de crise et de l'investigation.

Son activité est aussi mobilisée sur les audits (techniques, tests d'intrusion) pour améliorer la sécurité des systèmes d'information.

« Lorsqu'une société est attaquée, on intervient pour la sauver, on est un peu comme des pompiers », expliquent Ramzi et Sabri Khechaimia, codirigeants d'Orol Cyber Solutions.

« Quand on arrive dans une entreprise victime d'une cyberattaque, on ne touche à rien, il y a des recommandations, souligne Ramzi Khechaimia. Mais toutes les entreprises ne connaissent pas les bons réflexes. On nous appelle souvent quand tout est bloqué. On peut reconstituer les systèmes mais on ne peut pas déchiffrer. On peut juste parfois reconstituer des données avec des laboratoires avec lesquels on travaille. » Objectif : permettre à la société de redémarrer en mode dégradé, essayer de trouver des sauvegardes. « On l'accompagne, on constitue une équipe. Et, en investiguant, on essaye de repérer le « patient zéro », là par où est entré le hacker malveillant. » Il faut aussi surveiller que d'autres attaques ne surviennent pas.

Jour et nuit

« On a déjà géré des cyberattaques jour et nuit, se souviennent les deux frères. Ça prend parfois une semaine voire trois semaines. »

« L'humain est primordial, il faut sensibiliser, former », insistent les dirigeants de l'entreprise. La liste des conseils en matière de cyber-protection est aussi longue que les menaces sont diverses : mots de passe de 14 caractères minimum, sécurisés dans un coffre-fort numérique ; mise en place d'un environnement « zéro trust » (remise en cause, a priori, de la confiance envers les utilisateurs, applications, appareils...) ; sauvegardes régulières ; sécurisation des mobiles, des ordinateurs portables, des messageries ; séparation des activités perso et pro, contrôle les traces numériques...

Les préjudices subis par l'entreprise victime d'une cyberattaque peuvent coûter cher : des clients ou prestataires qui fuient, des pertes de traçabilité de paiements en cours. Certaines sociétés déposent le bilan après une cyberattaque. « Et il y a l'impact psychologique pour le chef d'entreprise, ajoutent les frères Khechaimia. C'est comme un cambriolage nous disent certains. Les collaborateurs sont aussi touchés. Quand il y a une cyberattaque dans une entreprise, c'est le chaos. » ■