

La startup CSM, sentinelle contre la menace cyber en Corse



Fondée en 2020 à Bastia, la startup CSM s'appuyant sur une équipe de quatre associés et de trois experts de la cybersécurité. (Crédits : DR)

Roland Frias

Aujourd'hui localisée à Bastia et Ajaccio, cette startup se présente comme un acteur-clé dans l'île en matière de cybersécurité et de conformité RGPD. En développant une expertise pointue et de solides partenariats, elle contribue à faire bouger les lignes dans ce secteur soumis à des défis croissants.

Dans un univers numérique en constante mutation, où les cyberattaques sont légion, Cybersécurité Management s'impose comme une sentinelle vigilante de la sécurité des entreprises et collectivités corses. Fondée en 2020 à Bastia, s'appuyant sur une équipe de quatre associés et de trois experts, elle est la seule du genre dans l'île, avec la Société de services informatiques et technologiques de Corse (SITEC), à avoir obtenu le label gouvernemental ExpertCyber 2.0.

Une expertise très utile, face à des menaces grandissantes, qui sert la résilience du tissu économique et institution-

nel régional. Parmi les préconisations « *de base* », explique Boris Brunel, son dirigeant, « *c'est le contexte d'hyper connexion et d'utilisation intensive de l'outil numérique qui l'impose. Il est essentiel de s'astreindre à une certaine hygiène informatique. Les sauvegardes sécurisées sont indispensables, la mise à jour régulière des équipements également, ainsi que l'utilisation d'un mot de passe fort - 12 caractères minimum - et l'activation de la double authentification sur tous les services en ligne* ».

Un SIEM « maison »

Très engagée sur la question de la cybersécurité en Corse, CSM propose un système de surveillance et de reporting des incidents de sécurité personnalisés, un SIEM « *maison* », souligne Boris Brunel. « *Notre logiciel offre une visibilité en temps réel sur les événements de sécurité en se connectant sur tous les équipements de sécurité existants chez nos clients* ».

ENTREPRISES

La startup CSM, sentinelle contre la menace cyber en Corse

Et d'ajouter, « *par exemple, le service informatique ou le chef d'entreprise voit sur son écran l'état de protection de son parc informatique par son antivirus ou les tentatives de connexion aux mails professionnels de son organisation. Notre logiciel détecte également les connexions distantes et peut afficher les alertes si les horaires de ces connexions ne correspondent aux horaires de travail habituels de l'organisation. Si une connexion distante est initialisée à 23 heures, le SIEM produira une alerte du type "grave" et le responsable du système d'information en sera averti par mail ou sms* ».

Selon le chef d'entreprise, « *la mise en sécurité d'une organisation passe aussi et surtout par la sensibilisation des collaborateurs concernant leur utilisation de l'outil informatique, il ne faut pas oublier que le premier pare-feu est humain* ».

« *La prévention et la préparation sont cruciales* », ajoute-t-il. « *Il est important de ne pas sous-estimer la menace cyber. La question n'est pas de savoir si une attaque surviendra, mais quand elle surviendra. Êtes-vous prêt ?* », interroge Boris Brunel. Cyber Sécurité Management contribue activement à sensibiliser et former les TPE-PME aux risques grâce à des outils e-learning et des formations sur la sécurité du numérique et le RGPD (Règlement général sur la protection des données) qui s'appuient par ailleurs sur l'utilisation de guides de bonnes pratiques et des plateformes gouvernementales, « *nécessaires pour obtenir des conseils précieux en matière de sécurité numérique* ».

« Un vrai fléau pour toute structure »

« *Évaluer la capacité des entreprises ou collectivités corse à se relever d'une cyberattaque est complexe* », estime le président de la startup CSM. « *Même si vous étiez prêt, une remise sur pied n'est jamais évidente... la perte ou la fuite des données constitue aujourd'hui un vrai fléau pour toute structure. Il ne faut pas négliger les temps d'arrêt, qui se comptent parfois en semaines avec d'importantes conséquences techniques et financières* ».

Malgré différentes attaques dans l'île qui ont concerné l'Université Pascal Paoli, le Centre Hospitalier de Castelluccio, l'Office d'Équipement Hydraulique de la Corse ou encore plus récemment la compagnie maritime Corsica Ferries, l'expert cyber note toutefois une application des recommandations de sécurité et une mobilisation croissante des acteurs. « *Le chemin est long, mais nous sommes sur la bonne voie* », se réjouit Boris Brunel qui, en cela, salue notamment la création d'un CSIRT (*Computer Security Incident Response Team*) par la Collectivité de Corse.

Un CSIRT bienvenu

« *C'est une excellente chose évidemment* », poursuit-il. « *La mission du CSIRT consiste à qualifier et répondre aux incidents de sécurité informatique en s'appuyant sur des prestataires qualifiés de l'île. Il sera également un agrégateur et un catalyseur des acteurs du territoire, d'ailleurs le CSIRT effectue déjà son travail, car suite à plusieurs réunions, je suis heureux d'annoncer la création du CLUSIR Corsica (Club de la sécurité de l'information en réseau, NDLR). Le CLUSIR aura pour objet la création d'événements, des formations et de sensibilisations concernant la cybersécurité et la sécurité de l'information en général* ».

Autre investissement déployé, celui des services de l'État en Corse qui jouent « *un rôle essentiel dans la prévention et la gestion des cyberattaques, avec un maillage territorial permettant la remontée d'informations et la facilitation des relations avec l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en cas d'incident* », indique Boris Brunel qui, à la lumière de ces bonnes nouvelles, est formel : « *Avec de nouveaux outils, comme le CSIRT ou le CLUSIR, ceux déjà existants comme l'association d'intelligence économique Corsica Sfera, mais également la prise de conscience progressive des utilisateurs et décideurs, je suis optimiste quant au développement d'un vrai savoir-faire au sein de notre région* ». ■