Cybercriminalité : Êtes-vous prêts à faire face à une cyberattaque ?

La cybercriminalité est une menace de plus en plus présente. Pour y sensibiliser les acteurs économiques, le 16 novembre, la FEDEM, la Chambre Monégasque de l'Assurance et la Chambre Monégasque des Nouvelles Technologies ont co-organisé un petit-déjeuner débat, avec la participation de l'Agence Monégasque de Sécurité Numérique et le soutien du Conseil Économique et Social.

L'animateur et entrepreneur David Sirour l'a clairement annoncé : *"La cybercriminalité est un enjeu majeur. Depuis l'arrivée des premiers navigateurs internet dans les années 90, la quantité et la sensibilité des données échangées ont cru de façon exponentielle, tout comme le risque lié à la corruption de l'intégrité de ces données. Tous les secteurs sont concernés."*

Un constat confirmé par le Président de la FEDEM Philippe Ortelli : *"Toutes les entreprises peuvent être impactées. Ransomware, arnaque au Président ou email infecté, les risques cyber sont multiples et bien réels. Il est essentiel qu'elles prennent conscience de ces nouveaux dangers et se mettent en capacité de s'en défendre. C'est pourquoi la FEDEM soutient cette initiative."*

© FEDEM

De gauche à droite : Éric Pérodeau, Président de la Chambre Monégasque des NT, Dominique Riban, Directeur de l'Agence Monégasque de Sécurité Numérique, André Garino, Président du Conseil Économique et Social, Michel Gramaglia, Vice-président de la Chambre Monégasque de l'Assurance, Patrice Cellario, Conseiller de Gouvernement-Ministre de l'Intérieur, et Philippe Ortelli, Président de la FEDEM.

Patrice Cellario, Conseiller de Gouvernement-Ministre de l'Intérieur, a également rappelé que la cybersécurité est un axe important de la politique menée par le Gouvernement Princier. *"Monaco offre un haut degré de sécurité physique. Notre ambition est d'atteindre un niveau de sécurité numérique identique."* Pour y parvenir, le pays a mis en place des outils législatifs et réglementaires, et a créé en 2015 l'Agence Monégasque de Sécurité Numérique (AMSN). *"Son action est essentielle, mais ne peut être vraiment efficace que si tous les acteurs prennent conscience des risques"*.

L'occasion pour le Contre-amiral Dominique Riban, Directeur de l'AMSN, d'expliciter les types d'attaques les plus utilisées par les hackers : les arnaques, l'espionnage, le sabotage, l'atteinte à l'image. *"Il existe des solutions pour se défendre efficacement. Elles doivent être adaptées à la taille de l'entreprise. Une TPE et un grand groupe n'ont pas besoin du même niveau de sécurité. Des précautions d'hygiène informatique* doivent être prises : utiliser des mots de passe forts, ne pas administrer son système depuis son poste utilisateur, ne pas mettre les serveurs directement en ligne mais prévoir au moins un pare-feu… Former les personnels est aussi nécessaire, notamment pour les rendre plus vigilants face aux emails reçus. 80 % des cyberattaques débutent par un email malveillant. Une minute pour le lire et des mois pour réparer un système d'information infecté, et c'est très couteux"*.

La parole a ensuite été donnée aux spécialistes en cyber-risques de la Chambre Monégasque de l'Assurance et aux experts en sécurité IT de la Chambre Monégasque des NT, qui ont enchaîné les interventions croisées afin de couvrir aux plans technique et assurantiel les trois phases d'une cyberattaque : avant, pendant et après.

Thomas Graiff, Directeur Général Adjoint d'Ascoma Jutheau Husson, a résumé la nature des risques et précisé comment leur impact financier se traduit en termes d'assurance, de dommages ou de responsabilité. Il a expliqué : *"L'assurance cyber vient dans une très grande majorité des cas compléter un "trou de garantie " des polices de dommages aux biens et de responsabilité civile."*

Côté technique, Sébastien Massé, Directeur Cybersécurité de Monaco Informatique Service, s'est intéressé à l'accompagnement des entreprises dans la mise en œuvre d'une stratégie globale de sécurisation de leur système d'information. *"C'est un vrai projet d'entreprise qui dépasse le cadre strict de l'informatique."* Dans la même dynamique, Jean-Christophe Pari, Directeur Technique de Noeva, a insisté sur l'importance de bien définir en amont le périmètre à protéger. *"C'est la condition sine qua non pour apporter une réponse technologique adaptée à l'environnement de l'entreprise et à la couverture du risque."*

Olivier Boscagli, Administrateur Délégué d'Eurassur, a quant à lui mis l'accent sur les évolutions du marché. *"Aujourd'hui, les professionnels de l'assurance appréhendent mieux l'impact financier de ces risques spécifiques et savent répondre aux besoins des entreprises, petites ou grandes"*. Grâce au questionnaire de souscription, l'assureur estime le degré de maturité de l'entreprise et la pertinence des mesures qu'elle a adoptées pour se prémunir, lui permettant de définir son assurabilité et les conditions de celle-ci.

Thierry Leray, Administrateur de Telis, a ensuite décrit les axes opérationnels d'intervention : *"Nous agissons d'abord en préventif avec la conception d'un réseau plus facile à sécuriser, puis en curatif pour stopper l'attaque, et enfin au niveau de la reprise de l'activité qui doit être très rapide car au-delà de 48 h, le risque de dépôt de bilan s'accroit"*.

Puis, Olivier Labedan, Directeur de Gramaglia Assurances, a détaillé l'implication des assureurs : *"L'entreprise couverte a un accès immédiat à des services, l'assureur s'appuyant sur des experts techniques, juridiques, et de communication, et peut être indemnisée pour la grande globalité de son sinistre. En cas de cyberattaque, elle a à disposition un professionnel qui lui expliquera les étapes pour mettre en place une gestion de crise."*

Enfin, Nicolas Baussart, Directeur Général d'Uriel, a mis en avant les nouveaux risques de l'hyper connectivité pour les entreprises. *"Les objets connectés (IoT) offrent une nouvelle porte d'entrée aux hackers. Mais nous disposons à Monaco de l'expertise IoT à même de maintenir un niveau de sécurité conforme aux enjeux"*.

Si cette rencontre a permis à la centaine d'acteurs économiques présents de poser leurs questions aux experts, elle a aussi confirmé l'intérêt de mettre en place des actions communes de sensibilisation pour permettre la sécurité numérique de tous, et ainsi accroître l'attractivité du pays. ■

* Pour en savoir plus : **https://amsn.gouv.mc**