nice-matin
Vendredi 3 mars 2023

« Une cyberattaque peut faire fermer une entreprise »

Le Prince a inauguré les locaux de Monaco Cyber Sécurité, une filiale de Monaco Digital chargée de protéger les données informatiques des entreprises et des les aider à répondre aux cyberattaques.

D'un Département à une entité à part entière. En octobre 2021, à l'occasion des Assises de la Cybersécurité, Monaco Digital lançait sa filiale Monaco Cyber Sécurité pour aider les entreprises du privé et du public à opérer leur transition numérique avec une sécurité accrue à tous les niveaux. Objectif : assurer l'intégrité des données informatiques face à des cyberattaques de plus en plus nombreuses et sophistiquées, face à des cybercriminels qui attaquent, impunément et indépendamment, les petites comme les grosses entreprises.

Dirigée par Sébastien Massé, Monaco Cyber Sécurité comptabilise une centaine de clients sur ses différents cœurs d'activité : la protection, l'audit, la réaction et la détection. Depuis mardi, la trentaine de collaborateurs a investi le rez-de-chaussée de l'immeuble Le Copori à Fontvieille. Le même jour, le prince Albert II a inauguré les locaux et découvert les installations, notamment un centre opérationnel de supervision de la sécurité des systèmes d'information pour les entreprises.

Entretien avec Sébastien Massé.

Le prince Albert II a inauguré ce mardi les locaux de Monaco Cyber Sécurité et visité les installations, notamment cet outil de supervision de la sécurité des systèmes d'information pour les entreprises. (Photos Jean-François Ottonello)

Sébastien Massé, directeur général de Monaco Cyber Sécurité.

Quelles sont les missions de Monaco Cyber Sécurité ?

Notre rôle est d'accompagner les entreprises dans leur développement du numérique en intégrant la sécurité. Nos offres sont découpées en quatre briques principales : protéger, auditer, détecter, réagir. Depuis 2018, Monaco Digital est prestataire d'audit de la sécurité des systèmes, une qualification délivrée par l'Agence monégasque de sécurité numérique (AMSN). Cela garantit un niveau d'exigence tant sur la confidentialité des données que sur l'expertise des auditeurs. Cela nous permet de travailler autant avec des acteurs privés, à Monaco et en France, qu'avec des opérateurs d'importance vitale (OIV) ou des entités gouvernementales.

> « Un attaquant peut accéder à toutes les informations »

Vos nouveaux locaux disposent d'une zone de supervision, en temps réel, des systèmes d'information de vos clients. En cas de cyberattaques, que se passe-t-il ?

Le client, que l'on aura dans cette zone de supervision, aura un certain nombre d'outils déployés sur son système d'information. On va collecter les événements et être capable de détecter une attaque ou une tentative sur celui-ci. On va l'alerter et y remédier, toujours avec son autorisation. L'objectif étant de réduire au maximum le temps de réponse entre le moment où l'attaquant tente de s'introduire et celui où on va prendre les mesures pour éviter la tentative d'attaque ou sa propagation.

En combien de temps faut-il réagir ?

Le plus rapidement possible. C'est comme pour le cambriolage d'une maison. Le plus difficile est d'ouvrir la serrure extérieure. Une fois dedans, il est plus aisé d'accéder aux différentes pièces. Si l'attaquant rentre dans le système d'information, qu'il s'y installe et s'y propage, ce sera difficile de le déloger. Il pourra alors accéder à toutes les informations.

Et pour vos clients qui ne sont pas sous votre supervision H-24 ?

On va les accompagner pour répondre à l'incident, pour les démarches administratives, pour prendre les premières décisions afin d'éviter la propagation. On va aussi les aider à investiguer pour savoir par où l'attaquant est rentré et, ensuite, leur faire des recommandations pour éviter que cela ne se reproduise. L'évolution du niveau de sécurité de ces entreprises et le redémarrage de leurs activités seront nécessaires

À quels types de cyberattaques sont confrontés vos clients ?

Il y a l'hameçonnage *(phishing en anglais)* par l'envoi d'e-mails frauduleux ou d'arnaques au président. L'attaquant va tenter de compromettre un collaborateur pour récupérer des informations ou de l'argent. Il existe, aussi, le rançonlogiciel qui est une attaque automatisée visant à chiffrer le système d'information puis à demander une rançon. Sur 2022, tout confondu, on a effectué une vingtaine de réponses à incident.

À combien se chiffrent ces rançons à Monaco ?

Les attaquants demandent des sommes en bitcoins extrêmement importantes, oscillant entre des centaines de milliers d'euros et au-delà du million d'euros pour certains comptes. On suit les recommandations des autorités françaises, l'ANSSI, et monégasques, l'AMSN, en conseillant à nos clients de ne pas payer. D'abord parce qu'il s'agit peut-être d'un hackage de données non sensibles, ensuite parce que cela ne garantit pas qu'ils ne retenteront pas une l'attaque. Les entreprises sont tentées de payer la rançon en l'absence d'autres solutions. Notre rôle va être de les accompagner pour redémarrer leurs activités.

Pourquoi en Bitcoin ?

Comme les autres cryptomonnaies, le Bitcoin permet aux cybercriminels de recevoir des fonds avec un degré élevé d'anonymat, ce qui rend les transactions difficiles à suivre.

Quel est le dernier rempart pour limiter la casse ?

C'est la sauvegarde du système d'information de façon déconnectée. Celle-ci sera alors préservée des attaques. Cela peut être des disques, des bornes dans des data center.

> « Des rançons en Bitcoin dépassent 1 M€ »

Face à l'accroissement et à l'ingéniosité des cyberattaques, vos services sont-ils de plus en plus demandés ?

C'est notamment le cas pour l'accompagnement et la gestion de crises. Les clients sont de plus en plus sensibilisés au fait qu'ils peuvent aussi en être victimes. Une cyberattaque est mieux gérée si vous y êtes préparés. Vous saurez comment monter une cellule de crise, communiquer avec l'extérieur, les clients et les collaborateurs, comment redémarrer votre activité, sur quels postes, si vous pouvez faire du télétravail.

Il faut se poser ces questions en amont sinon vous perdrez du temps pour redémarrer votre activité, avec des impacts financiers très conséquents.

Les hackers ciblent-ils des profils particuliers d'entreprises ?

Une grande partie des attaques automatisées ciblent les petites entreprises comme les grandes, dès lors qu'elles disposent d'un système d'information.

Les attaques sont-elles de plus en plus sophistiquées ?

Pour les attaques ciblées, celles-ci sont de plus en plus complexes et les hackers utilisent des failles dites « *zéro-day* » pas forcément connues. Toutes les semaines, il y a de nouvelles failles et les mises à jour des équipements par les entreprises doivent être faites régulièrement. On les alerte sur ce point.

Comment expliquer le manque de culture du risque cyber ?

Beaucoup d'entreprises pensent, malheureusement, que cela n'arrive qu'aux autres, que leur système d'information n'intéresse pas les attaquants. Elles n'ont pas conscience de l'importance de leur outil informatique, alors que l'évolution des usages et la digitalisation de l'entreprise rendent celui-ci indispensable. Une attaque cyber peut paralyser complètement une entreprise, y compris les plus petites, et avoir des conséquences extrêmement importantes. Cela va des pertes financières, on l'a dit, à la fermeture d'une entreprise.

PROPOS RECUEILLIS PAR THIBAUT PARAT
tparat@nicematin.fr