JUTHEAU HUSSON
GROUPE ASCOMA
Conseil & Courtier en Assurances

MONACOINFORMATIQUE SERVICE

À propos d'Anthony BOIRA

Anthony BOIRA est PDG de Monaco Informatique Service. À ce titre, il conseille les entreprises monégasques dans leurs projets numériques pour leur proposer des solutions adaptées.

Cyber-Risques : Protection et assurance à l'ère numérique

La vision d'Anthony Boira - Partenaire d'Ascoma Jutheau Husson

MIS EN CHIFFRES :

- 120 Collaborateurs en 2018
- CA : 15M€ en 2017

« La démarche proposée par Ascoma est saine et cohérente : l'idée est de rencontrer les clients de la Principauté, de les sensibiliser sur les risques de cyber sécurité, et de faire intervenir Monaco Informatique Service en tant qu'experts. »

L'ESSENTIEL

- **La cybercriminalité s'est organisée et se renouvelle ciblant toutes les entreprises, peu importe leur taille.**
- **Les entreprises doivent tenir compte de nouvelles responsabilités pour protéger leurs données confidentielles.**
- **Dans le cadre d'un partenariat avec Ascoma Jutheau Husson, l'entreprise Monaco Informatique Service intervient au bénéfice des clients du courtier monégasque.**

Dans le cadre du partenariat entre le courtier Ascoma Jutheau Husson et Monaco Informatique Service (MIS), MIS assiste les clients d'Ascoma souscrivant une assurance cyber-risques. Anthony BOIRA, PDG de MIS et partenaire d'Ascoma Jutheau Husson, s'exprime pour sensibiliser les entreprises de la Principauté à ces risques grandissants.

Entretien

- Quels que soient la taille et le domaine d'activité de votre entreprise ou de votre organisation, vous êtes une cible potentielle des cybercriminels.
- Nous sommes avec Ascoma dans une approche de conseil et de juste partage des risques avec leurs assurés.
- La difficulté est de respecter le bon processus qui permettra d'éradiquer l'attaque, de rétablir la situation, et si possible de traquer le criminel.

Extraits

Nous entendons de plus en plus souvent parler de cyber-risques, leur recrudescence est-elle une véritable tendance de fond ?

Anthony BOIRA (AB) : Les cyberattaques sont devenues de nos jours pratique courante. La cybercriminalité se pratique de manière organisée ; en fonction de leur profil, les entreprises peuvent se trouver confrontées dans ce domaine à la petite criminalité ou à la grande criminalité, mais toutes les structures sont concernées. Parmi les attaques les plus courantes, tout le monde a entendu parler des *cryptolockers*[1] qui bloquent les systèmes de fichiers, et peuvent occasionner une paralysie totale des traitements et des communications, avec pour conséquence des pertes d'exploitation importante.

Mais on rencontre aussi d'autres types d'attaques, beaucoup plus techniques, plus ciblées et plus graves, orchestrées par des filières internationales. Les cybercriminels recherchent des failles, s'introduisent dans le système d'informations, dérobent des données et opèrent toutes formes de chantage, tout en organisant des démonstrations de force pour mettre leur victime sous pression. Au fur et à mesure des négociations, et dès qu'ils sentent une hésitation, les hackers peuvent envoyer par exemple des attaques *DDos*[2] ou du *mail bombing*[3]. Dans ce type de cas, les hackers utilisent des adresses IP confidentielles rebondissant sur divers continents à travers le monde, et donc impossibles à localiser. Ce genre de scénario est devenu courant.

Aujourd'hui, quels que soient la taille et le domaine d'activité de votre entreprise ou de votre organisation, vous êtes une cible potentielle des cybercriminels. Les menaces sont là, elles sont actives sur le net ; elles se multiplient de jours en jour, se renouvellent en permanence et deviennent de plus en plus sophistiquées.

Vous avez parlé du blocage de l'exploitation, ce type d'attaque organisée peut-il avoir d'autres conséquences sur une entreprise ?

AB : Une cyber attaque peut causer une dégradation importante de la réputation d'une entreprise. Il peut y avoir des vols de données, et notamment des données de vos clients, ce qui peut causer une perte de confiance ou même des plaintes juridiques et des pénalités en conséquence.

De plus, souvent en cas d'attaque, l'entreprise entre dans une période de doute et de suspicion internes, avec potentiellement une perte de la cohésion interne et des conséquences importantes sur le personnel et l'organisation.

À une époque où l'informatique touche toutes les activités et ouvre le champ des possibles, il faut être conscient des risques et protéger le business.

Le Règlement Général de la Protection des Données (R.G.P.D), qui arrivera en vigueur vers janvier 2019 à Monaco, soulève-t-il de nouveaux enjeux pour les entreprises en termes de cyber sécurité ?

AB : La Principauté de Monaco a une position particulière, puisqu'elle n'est pas dans la Communauté Européenne. Cependant, les entreprises monégasques sont concernées puisqu'elles manipulent des informations concernant des collaborateurs issus de la Communauté, et elles communiquent avec les pays de la Communauté Européenne ; elles doivent donc pouvoir prouver qu'elles respectent les règles européennes de protection des données personnelles. Et dans le R.G.P.D., les règles de sécurité préconisées visent la sécurisation de l'ensemble du système d'informations.

Dans le cadre de la protection du risque cyber, vous avez établi un partenariat avec Ascoma Jutheau Husson. Quelles ont été les motivations de ce partenariat ?

AB : Les motivations sont évidentes puisque nous avons les mêmes intérêts qu'Ascoma : accompagner nos clients pour faire face aux risques, de préférence de manière préventive, mais aussi en cas d'attaque avérée. Le risque de la cyber sécurité est réel, et les clients en prennent de plus en plus conscience. La démarche proposée par Ascoma est saine et cohérente : l'idée est de rencontrer les clients de la Principauté, de les sensibiliser sur les risques

de cyber sécurité, et de faire intervenir Monaco Informatique Service en tant qu'experts, pour être force de conseils, proposer des solutions concrètes et personnalisées, et faire bénéficier les clients de nos retours d'expérience.

Dans ce partenariat, chacun exerce son métier et son savoir-faire : nous proposons à l'assuré d'établir un diagnostic de l'état de son système d'information. Il peut ainsi concrètement savoir quels sont ses risques critiques et peut décider ceux qu'il veut traiter avant de se faire assurer. S'il informe l'assureur sur ses risques résiduels, celui-ci pourra lui proposer le bon niveau de cotisation. Finalement, c'est un accord tripartite, résultat d'un échange d'informations pertinentes entre l'assuré, l'assureur et l'expert en sécurité. Nous sommes avec Ascoma dans une approche de conseil et de juste partage des risques avec leurs assurés.

Si l'entreprise a des doutes une fois le contrat établi sur une faille de sécurité, avant même d'appeler l'assureur, est-elle à même de vous appeler pour lever ce doute ?

AB : Le premier geste doit être d'appeler son prestataire de services. S'il y a suspicion d'attaque, ou si l'attaque cyber est avérée, ce dernier fera appel à un spécialiste. Le bon réflexe est aussi d'informer les instances locales comme l'AMSN. Elle est organisée pour conseiller les entreprises de Monaco, et pourra proposer des solutions, ou orienter le client vers les organismes ou les prestataires adéquats.

La difficulté est de respecter le bon processus qui permettra d'éradiquer l'attaque, de rétablir la situation, et si possible de traquer le criminel. Il faut respecter une logique de décisions et d'actions, qui doit être partagée entre l'entreprise, le prestataire, et l'assureur, avec, si besoin, l'aval de l'AMSN. En cas d'accord contractuel en amont avec l'assureur, nous intervenons comme prestataire cyber, et allons tout de suite agir en tant que correspondant auprès de l'AMSN.

En tant que correspondant avec l'AMSN, au travers de quel(s) dispositif(s) intervenez-vous ? Comment faites-vous pour identifier si oui ou non il y a une faille ?

AB : Nous avons des consultants spécialisés en cyber sécurité, qui travaillent selon les règles établies par l'AMSN, et en collaboration avec elle. Pour détecter les failles, nous utilisons des outils spécifiques et surtout le savoir-faire et l'expérience de nos consultants. Pour détecter une attaque ou une intrusion, il faut rechercher les traces de compromission en isolant le système compromis dès suspicion d'attaque.

En cas de faille avérée et détectée par vos consultants, quel(s) moyen(s) de secours pouvez-vous proposer aux entreprises touchées ?

AB : Nous nous rendons sur place pour procéder avec le client à isoler le périmètre de l'attaque, analyser les traces, et évaluer la situation. En fonction du périmètre des systèmes compromis et de la situation du client, nous allons définir avec le client et son service informatique le plan d'action de reprise de l'activité. Si le client ne souhaite pas que son service informatique ou son prestataire informatique s'en charge, nous pouvons lui proposer de faire appel à nos services d'infrastructures techniques ; nous pouvons aussi, si besoin, prendre en charge la gestion de crise, pour piloter l'ensemble des actions jusqu'au rétablissement de l'activité. ■

Lexique technique

[1] **Cryptolockers :**
Les *cryptolockers* sont des logiciels malveillants, qui, après avoir infecté un ordinateur, cryptent ses données et se répandent dans le réseau local de l'entreprise. Ces logiciels rendent impossible l'accès aux fichiers, et paralysent l'exploitation. Ils sont généralement utilisés pour demander des rançons contre le moyen d'accéder aux fichiers.

[2] **Attaque DDoS :** Attaque par *Distributed Denial of Service* ou Déni de Service
Ce type d'attaque a pour objectif de rendre indisponible une infrastructure, un serveur ou un service. Elle a pour conséquence l'impossibilité pour les utilisateurs légitimes (employés, consommateurs ou partenaires…) d'utiliser les ressources normalement proposées (sites internet, serveurs de sauvegarde, etc…).

[3] **Mail bombing** :
Ce type d'attaque informatique automatisé saturant la messagerie, peut avoir pour conséquence un déni de service. Dans la plupart des cas, elle bloque la réception de messages légitimes à destination de l'entreprise.

Monaco Informatique Service
9, Avenue Albert II
98000 Monaco
(+377) 97 97 30 20
(+377) 97 97 30 29
contact@monacoinformatiqueservice.mc

Monaco Informatique Service est une Entreprise des Services Numériques opérant en Consulting, Délégation de services, et en Intégrant et distribuant des logiciels. Des centres de services dédiés à l'infrastructure, l'infogérance, l'ingénierie logiciel, le consulting et la cybersécurité, ainsi que des fonctions supports communes à ces centres soutiennent ses opérations.

MIS a obtenu la qualification de Prestataire d'Audit de la Sécurité des Systèmes d'Informations (P.A.S.S.I). Cette qualification leur permet de répondre à des exigences de sécurité importantes et d'auditer les systèmes d'information pour le compte de l'AMSN. Cette reconnaissance démontre la prise en compte de l'aspect sécurité dans leur gestion des données.

Ascoma Jutheau Husson
24, bd Princesse Charlotte
98000 Monaco
(+377) 97 97 22 22
(+377) 93 25 08 22
jutheau-husson@ascoma.com

Jutheau Husson est la filiale monégasque d'Ascoma, Groupe de courtage d'assurances indépendant au capital entièrement familial, comptant près de 700 collaborateurs dans 24 pays. Le Groupe Ascoma est partenaire des plus grands courtiers mondiaux, ce qui lui permet d'accompagner ses clients partout où ils exercent et de leur offrir des solutions d'assurances les plus pointues.

Jutheau Husson, implanté à Monaco depuis 1950, est le courtier d'assurances leader en Principauté. Notre département Entreprises accompagne nos clients : grandes entreprises internationales, PME-PMI, organismes publics et internationaux sur l'ensemble de leurs risques et dans tous les domaines d'activités.