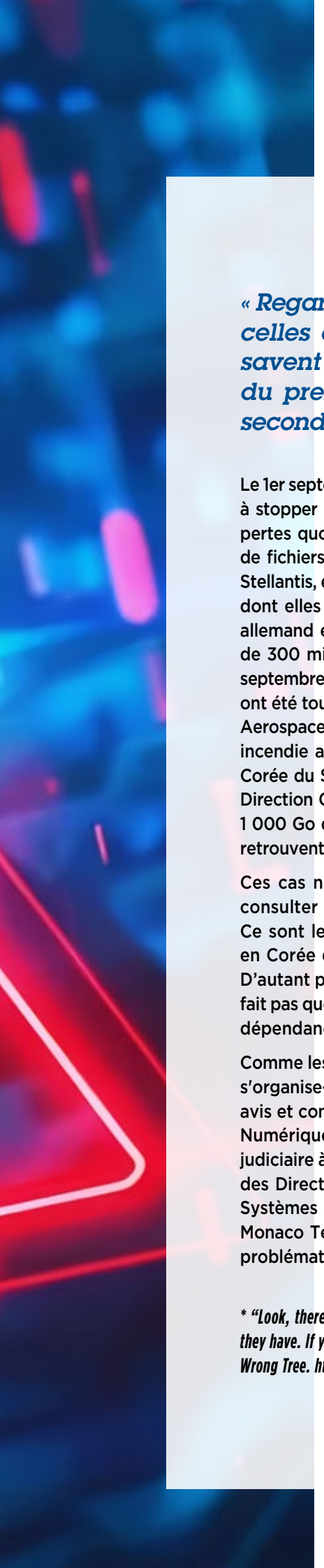
CYBERSÉCURITÉ : TOUS CONCERNÉS !



« Regarde, il y a deux types de personnes dans le monde : celles qui n'ont jamais été escroquées et celles qui ne savent pas qu'elles l'ont été. Si vous pensez faire partie du premier groupe, félicitations : vous faites partie du second », Eric Barker*

Le 1er septembre 2025, une cyberattaque a contraint le constructeur automobile Jaguar à stopper net toutes ses usines mondiales, entraînant près de 85 millions d'euros de pertes quotidiennes pendant plus d'un mois. Quelques semaines après, 1,5 milliards de fichiers de 750 organisations, dont des très connues (Google, Air France / KLM, Stellantis, etc.), ont été exposées suite à un hack contre l'éditeur de logiciels Salesforce dont elles étaient clientes. Le 18 septembre, un rapport conjoint du renseignement allemand et de la fédération Bitkom a révélé que les cyberattaques ont coûté près de 300 milliards d'euros à l'économie allemande depuis le début de l'année. Le 20 septembre, plusieurs aéroports européens, dont Bruxelles, Heathrow à Londres et Berlin, ont été touchés par une cyberattaque qui visait un logiciel fourni par la société Collins Aerospace, et qui a entrainé des annulations et retards de vols. Le 26 septembre, un incendie a détruit définitivement 858 000 Go de données gouvernementales de la Corée du Sud, il n'y avait pas de sauvegarde (backup). Et, toujours en septembre, la Direction Générale des Impôts et des Domaines (DGID) du Sénégal s'est fait voler de 1 000 Go de données administratives et fiscales sur les citoyens du pays, lesquels se retrouvent vulnérables aux usurpations d'identités et autres fraudes.

Ces cas ne sont que quelques exemples parmi de nombreux autres, il suffit de consulter les sites spécialisés pour en découvrir quotidiennement de nouveaux. Ce sont le plus souvent des cyberattaques mais, comme le démontre le désastre en Corée du Sud, la cybersécurité ne se limite pas à se protéger, elle est un tout. D'autant plus que tous ces risques tendent à s'accroître : la transition numérique ne fait pas que nous ouvrir de nouvelles possibilités, elle augmente en même temps notre dépendance, ce que certains individus mal intentionnés savent très bien exploiter.

Comme les autres pays, la Principauté est une cible, mais a ses spécificités. Comment s'organise-t-elle pour se défendre ? Pour mieux saisir les enjeux, le MBN a sollicité les avis et conseils de Frédéric Fautrier, Directeur de l'Agence Monégasque de Sécurité Numérique (AMSN), et du Commissaire Émilie Moreau, Chef de la division police judiciaire à la Sûreté Publique de Monaco. Franck Chiniard, Président de l'Association des Directeurs Informatiques de Monaco (ADIM), Thomas Cartereau, Directeur des Systèmes d'Information du groupe SMEG, et Martin Péronnet, Directeur Général de Monaco Telecom, apportent aussi leur éclairage et leur expérience terrain sur cette problématique majeure qui nous concerne tous.

** "Look, there are two kinds of people in the world: those who've never been conned, and those who don't know they have. If you think you're in the first group, congratulations: you're in the second", Eric Barker. Barking Up The Wrong Tree. https://bakadesuyo.com/2025/09/scammed/*


© Photo Michael Alesi / Direction de la Communication

Frédéric Fautrier :

« Les vulnérabilités à exploiter resteront sensiblement les mêmes, d'où l'importance d'augmenter le niveau de maturité numérique des PME/TPE, associations et particuliers de Monaco »

L'Agence Monégasque de Sécurité Numérique (AMSN) est en charge de la sécurité des systèmes d'information, en particulier pour les services publics et les Opérateurs d'Importance Vitale (OIV) étatiques et privés. Son Directeur, Frédéric Fautrier, fait le point sur les évolutions de la menace cybercriminelle en Principauté et les actions de prévention mises en place pour lutter contre ce fléau.

MMBN/ Quel est l'état de la menace cyber ?

Frédéric Fautrier : Nous surveillons chaque jour les activités cybercriminelles en provenance du monde entier. Ces données quotidiennes alimentent notre rapport mensuel, et sont ensuite consolidées et présentées annuellement pour donner une meilleure visibilité de la situation et de ses perspectives. Nous constatons que les chiffres augmentent d'une année sur l'autre. Nous observons aussi que les individus qui génèrent des attaques, ou font des actions de reconnaissance avant d'opérer ces attaques, sont de plus en plus agiles, ce qui tend à confirmer qu'ils utilisent l'I.A. pour les automatiser. Selon l'utilisation qui en est faite, l'I.A. est à la fois un outil puissant pour détecter et neutraliser les menaces, et un levier pour décupler le pouvoir de nuisance des personnes mal intentionnées.

MBN/ Quelles sont les grandes tendances en matière de cybersécurité ?

F. F. : Depuis 2018, nous avons mis en place un plan de travail pluriannuel pour aider les OIV étatiques et privés à atteindre un niveau de maturité conforme aux exigences de sécurité numérique. Pour autant, les chiffres de 2024 montrent une augmentation de 63% des actions de reconnaissance et de 32% des attaques par rapport à 2023, ce qui est assez significatif pour Monaco. Les rapports internationaux consacrés à ce phénomène confirment cette même tendance, avec bien sûr certains secteurs (banque, finance, santé) plus ciblés que d'autres. En 2024, la Sûreté Publique de Monaco, qui instruit les plaintes en lien avec la cybercriminalité (Voir l'interview dans ce même dossier), a reçu 627 signalements, dont 65 nouvelles procédures ouvertes, attestant aussi la tendance haussière.

MBN/ Quelles sont les principales formes d'attaques ?

F. F. : Les campagnes d'hameçonnage (phishing en anglais) sont les plus plébiscitées par les cyberattaquants, qui les utilisent comme points d'entrée via des emails piégés ou des sites web frauduleux.

2 scénarios sont alors possibles : si la cible est un particulier, les pirates informatiques vont plutôt usurper l'identité de la personne ou de l'organisation de confiance en contact avec celle-ci (banque, administration, service en ligne, ...), dans le but de dérober des informations personnelles sensibles (documents d'identité, numéros de cartes ou de comptes bancaires, identifiants de connexion, ...) pour les revendre à d'autres pirates qui les utiliseront pour des escroqueries. Si la cible est une entreprise, la méthodologie employée est plutôt celle du chiffrement de son système d'information pour le rendre inopérant, et à partir de là, demander une rançon (d'où le nom de « ransomware » en anglais). Dans tous les cas, cela se traduit pour la victime par un coût financier et souvent aussi réputationnel. C'est pour cela qu'il est important, maintenant que nous avons bien avancé avec les services publics et les OIV, de mieux accompagner les entreprises, les particuliers et les associations de Monaco.

MBN/ Quels sont les objectifs du sous-comité Cybermalveillance récemment créé ?

F. F. : Ce sous-comité a pour missions d'animer la prévention, l'accompagnement et l'assistance aux particuliers, aux entreprises et associations victimes d'actes de cybermalveillance, qui ne disposent pas nécessairement de gros moyens financiers, ni de personnels informatiques dédiés.

Ce sous-comité, que je préside et qui comprend 6 membres, parmi lesquels des acteurs du public, mais aussi des sachants du privé et du monde associatif (Voir l'encadré ci-après), a été institué par l'Ordonnance Souveraine n°11.326 du 10 juillet 2025.

Il pilotera la labélisation « CyberExpert Monaco » encadrée par l'Arrêté Ministériel n° 2025 342 du 3 juillet 2025, qui valorisera les Entreprises de Services du Numérique (ESN) de Monaco justifiant d'une expertise en cybersécurité assurant des prestations d'installation (sécurisation), de maintenance en conditions opérationnelle et de sécurité, d'assistance (réponse à incident). L'écosystème numérique de la Principauté est riche de compétences, aussi l'idée est de le faire connaitre.

MBN/ Concrètement, quelles seront les prochaines étapes ?

F. F. : La première a été lancée le 8 octobre dernier avec la mise en ligne de la page d'atterrissage d'une plateforme dédiée : **https://cybermalveillance.gouv.mc/** pour permettre tout d'abord aux candidats à la labélisation de s'informer sur les critères d'éligibilité et les étapes à suivre pour obtenir ce label. La seconde étape, prévue d'ici la fin de l'année, consistera à densifier la plateforme avec des informations à l'attention des victimes, afin de les orienter vers les bons interlocuteurs, que ce soient les prestataires techniques (selon les technologies utilisées, les profils d'attaques et les domaines de compétences des prestataires), la Sûreté Publique de Monaco, ou l'Autorité de Protection des Données Personnelles.

C'est l'Association Française de Normalisation (AFNOR), et plus précisément AFNOR Certification, qui se chargera de la certification des ESN candidates. Une fois le travail d'AFNOR Certification effectué, le dossier sera présenté au sous-comité qui validera, ou non, la labélisation. Les prestataires labélisés se verront ensuite attribuer

par l'AMSN un certificat témoignant de leur expertise technique et technologique et de leur capacité à accompagner les victimes.

MBN/ Quels conseils et messages de sensibilisation souhaitez-vous transmettre à nos lecteurs ?

F. F. : La première chose à faire pour les petites entreprises et les associations est la mise à jour immédiate et systématique de leurs logiciels informatiques lorsque l'éditeur les invite à le faire. En effet, dans les heures qui suivent la publication d'une vulnérabilité, la faille est exploitée par les cybercriminels. C'est une course sans fin. La seconde initiative est de bien paramétrer les fonctions de firewall de la box de l'opérateur. Il faut aussi être très attentifs à la gestion des courriels, en étant vigilants sur leur origine, l'URL utilisée, et leur contenu, sans oublier de sélectionner des protocoles sécurisés d'envoi et de réception. En sécurisant les systèmes d'information, ces actions permettent de réduire la surface d'attaque. Selon la taille de l'entreprise et de son système d'information, des dispositions complémentaires sont à prendre.

MBN/ Quel regard portez-vous sur l'évolution de la menace cyber ?

F. F. : Selon toute logique, le nombre d'attaques continuera de croître, et l'utilisation de l'I.A. se banalisera pour les attaques autant que pour les réponses à y apporter. Les vulnérabilités à exploiter resteront sensiblement les mêmes, d'où l'importance d'augmenter le niveau de maturité numérique des PME/TPE, associations et particuliers de Monaco, et de professionnaliser l'accompagnement.

L'implication de tous les acteurs, privés et publics, est et sera indispensable pour faire face à ce fléau. Or, si la banque publique d'investissement Bpifrance, qui a pour mission le financement et le développement des entreprises, dispose de statistiques montrant que ses clients sont conscients du risque cyber, elle a aussi constaté qu'ils ne savent pas toujours comment le traduire en actions de protection, faute de ressources internes et d'accompagnement. Nous nous mobiliserons donc de plus en plus pour répondre à ces besoins, notamment au travers de la plateforme Cybermalveillance.

Le sous-comité Cybermalveillance est composé comme suit :

- le Directeur de l'Agence Monégasque de Sécurité Numérique, Président ;
- le Directeur de la Direction de la Sûreté Publique de Monaco, ou son représentant ;
- le Directeur de la Direction des Services Numériques, ou son représentant ;
- le Secrétaire Général de l'Autorité de Protection des Données Personnelles, ou son représentant ;
- le Président de la Chambre Monégasque du Numérique, ou son représentant ;
- le Président de l'Association des Directeurs Informatiques de Monaco, ou son représentant.

Émilie Moreau :

« la Sûreté Publique est à la fois un acteur clef et un soutien de proximité, y compris dans le champ numérique. La police ne peut lutter seule car la cybersécurité est un travail collectif, chacun doit être vigilant et nous contacter au plus tôt en cas de doute »

Le Commissaire de Police Émilie Moreau est depuis le 4 août Chef de la division de police judiciaire de la Sûreté Publique de Monaco. Dotée de plus de 24 ans d'expérience dans la Police, elle a déjà travaillé plus de 5 années sur les crimes sexuels à l'encontre des mineurs, incluant la pédocriminalité en ligne, 5 ans en anti-terrorisme, et son dernier poste était orienté sur la coopération européenne et internationale. Le MBN l'a interrogée sur l'état de la menace cyber en Principauté et sur les actions de la Sûreté Publique de Monaco pour nous en défendre.

MBN/ Quelles sont les particularités de Monaco en matière de risque cyber ?

Émilie Moreau : La cybersécurité constitue un véritable enjeu de sécurité nationale pour lequel Monaco se doit d'avoir un haut niveau de réponse. La notoriété de la Principauté sur la scène internationale, son attractivité économique et financière, tout comme le profil à risque de sa population sont de nature à attirer les cybercriminels. Face à cette menace protéiforme, la taille du pays, les partenariats tant étatiques qu'institutionnels, avec notamment l'unique opérateur en matière de télécommunication et le secteur privé constituent une force significative. Nous avons la chance de pouvoir travailler en lien étroit avec l'ensemble des acteurs impliqués dans ce domaine et coordonner nos actions respectives pour une plus grande efficacité. Néanmoins, l'écosystème cybercriminel étant par essence dématérialisé et non territorialisé, une coopération internationale s'impose.

MBN/ Comment s'organise la Sûreté Publique de Monaco pour y faire face ?

E. M. : La lutte contre la cybercriminalité est un travail collectif. Pleinement mobilisée, la Sûreté Publique de Monaco développe une approche globale : expertise humaine, outils technologiques, proximité avec les usagers, formations, coopération nationale et internationale. La police s'est dotée d'une organisation renforcée et dispose de ses propres équipes d'experts cyber. Pour remplir le mieux possible notre mission d'enquête, nous mettons en place une véritable synergie de compétences, c'est à dire que l'on associe le travail des enquêteurs à celui d'ingénieurs. De plus, notre service travaille en collaboration étroite avec l'AMSN et les autres services de l'Etat, et au-delà, avec des organisations tel qu'Interpol et Europol. Monaco a ratifié la Convention de Budapest qui facilite les échanges internationaux en matière de lutte contre la cybercriminalité, et nous accentuons le partenariat avec Europol avec qui la Principauté dispose d'un accord de travail stratégique et opérationnel. Nous mettons également l'accent sur la formation et la prévention, aussi bien en interne au sein de nos équipes qu'auprès des usagers. Comme par exemple, le projet cybermalveillance initié par notre direction et piloté par l'AMSN. Nous sommes très engagés sur toutes les actions à destination du public et des entreprises pour les sensibiliser et les accompagner en cas de besoin.

MBN/ Quel message voudriez-vous faire passer ?

E. M. : En matière de cybersécurité, la menace est en constante évolution et est amplifiée par le contexte géopolitique actuel. Cela se traduit par une forte hausse du volume de tentatives d'attaques. Si le courriel reste la porte d'entrée privilégiée par les cybercriminels, le phishing (hameçonnage) et le rançongiciel (logiciel malveillant d'extorsion) constituent les principaux risques. Le premier message est que chacun peut être victime tant dans son environnement personnel que professionnel. Il faut en avoir conscience et parvenir à une prise de conscience individuelle et collective. Chacun doit être sensibilisé dès le plus jeune âge, être vigilant dans son utilisation des outils numériques, savoir où s'informer et comment signaler. Ensuite, il faut se rappeler que la Sûreté Publique est à la fois un acteur clef et un soutien de proximité, y compris dans le champ numérique. La police ne peut lutter seule car la cybersécurité est un travail collectif, chacun doit être vigilant et nous contacter au plus tôt en cas de doute, car il est toujours essentiel d'agir vite.

telis 25 ans de passion & d'innovation au service de Monaco

Communication Unifiée

Vidéosurveillance

Réseaux Informatiques

Système de sécurité

Réseaux WIFI

Multimédia

DataCenter

telis 25 YEARS ANNIVERSARY

Merci...et on n'a pas fini !

GROUPE telis

Actis

easyOne Customized Software

DC monaco DATACENTER

Franck Chiniard :

« La question n'est pas sur la possibilité du hack, mais sur la date de celui-ci, ce n'est pas "si" mais "quand" »

Pour mieux comprendre le risque cyber à Monaco, le MBN a donné la parole à Franck Chiniard, Président de l'Association des Directeurs Informatiques de Monaco (ADIM).

MBN/ Qu'est-ce que l'ADIM et quel est son rôle ?

Franck Chiniard : L'ADIM a été créée il y a 25 ans pour permettre le partage d'expérience entre les Directeurs Informatiques (Directeur des Systèmes d'Information : DSI) autour du bug de l'an 2000. Ce partage est toujours la raison d'être de l'association, qui rassemble maintenant plus de 160 membres, et entretient d'excellentes relations avec le Club Informatique Provence Méditerranée (CIPmed), son équivalent régional en région PACA. Nous organisons aussi des événements à Monaco et avons notamment reçu le CTO (Directeur Technique) de Dell Technologies France, et le RSSI (Responsable de Sécurité des Systèmes d'Informations) de Virbac en 2023, qui est venu apporter un retour d'expérience après une cyberattaque subie. Et tous les ans, en novembre, nous organisons une rencontre avec l'Agence Monégasque de Sécurité Numérique (AMSN) et une société spécialisée dans le risque cyber, dans le but de faire encore plus de partage. Et comme la formation est un élément fondamental de la protection et que les DSI ont trop de travail pour pouvoir suffisamment rester informés au quotidien, l'ADIM édite des Livres Blancs.

MBN/ Que représente le risque cyber pour les entreprises monégasques ?

F. C. : Monaco a deux particularités. Tout d'abord, beaucoup d'entreprises y sont de petite taille, ce qui fait qu'en dehors des Opérateurs d'Importance Vitale (OIV), qui ont tellement de contraintes auprès de l'AMSN que cela leur impose quasiment d'y affecter une ressource à temps plein, il y a trop peu de RSSI, le DSI se retrouvant donc trop souvent seul. Ensuite, Monaco se distingue par le fait qu'il n'y a qu'un seul opérateur télécom. C'est une force, notamment en termes de réactivité et de communication, mais aussi une faiblesse, comme on avait pu le remarquer il y a 3 ans quand un groupe diesel était tombé en panne pendant une maintenance. Ce n'était pas une cyberattaque, rien qu'une simple panne, mais déjà le rétablissement progressif des services avait demandé 6 heures.

Au niveau des cyberattaques en elles-mêmes, il y a eu à Monaco quelques cas de ransomware, où le système est encrypté pour obliger l'entreprise à payer une rançon pour récupérer ses données, mais surtout des fraudes au Président, où un interlocuteur qui se fait passer pour un décideur de l'entreprise parvient à faire transférer des sommes importantes en sa faveur. Il y a aussi des fraudes à la facture, où le numéro du compte du bénéficiaire est modifié, et bien sûr les multiples campagnes actuelles de phishing sur les comptes Monaco Telecom. Au global, ce sont surtout des micro-incidents, et il y a même des buzz non fondés, certaines entreprises n'ont pas été victimes de fuites de données, contrairement à ce que la rumeur pourrait faire croire.

Pour répondre à ces risques, le Gouvernement Princier lance un portail de cybersurveillance, qui va référencer les entreprises monégasques labellisées « ExpertCyber » qui sont aptes à aider les victimes, entreprises comme particuliers ou associations. L'ADIM fait partie de la sous-commission cybermalveillance récemment mise en place et va aider à construire le contenu de ce portail. Un des sujets sur lesquels nous travaillons est celui de la protection de son domaine Internet et de l'image qui y est associée, la cybersécurité est importante à tous les niveaux et la réputation a une valeur recherchée.

MBN/ Quelles évolutions de ce risque avez-vous constaté ces dernières années ?

F. C. : Le plus grand changement constaté est l'utilisation croissante de l'Intelligence Artificielle, qui transforme les risques. L'excellente chaîne YouTube "Micode", spécialisée sur le sujet du risque cyber, avait interviewé deux ingénieurs cybersécurité de Doctolib, qui avait déjà pu noter il y a 2 ans lors d'une attaque par surcharge (DDoS : Distributed Denial Of Service) que la réactivité des attaquants était inhabituelle, beaucoup trop rapide. Je ne pense cependant pas que nous allons arriver à un monde de guerres uniquement entre IA, sans intervention humaine, car le facteur humain sera toujours primordial pour piloter. Bien sûr, il faut d'abord s'entendre sur la définition de l'IA, dans les faits celle-ci est déjà utilisée depuis des années pour reconnaître des signaux faibles. Elle est particulièrement efficace pour détecter les premiers signes des attaques, par exemple des comportements particuliers, et à les associer à des patterns connus, là où un être humain ne pourrait pas suivre. Mais pour y répondre efficacement il faut de la créativité, ce qui reste notre point fort.

Un autre aspect important est que nous sommes maintenant dans un contexte géopolitique compliqué, avec des guerres en cours, où l'information a beaucoup de valeur. Même s'il n'y a pas de coût financier immédiat, une fuite d'informations peut avoir un impact stratégique important qu'il ne faut absolument pas négliger.

Enfin, les attaques peuvent maintenant venir de partout. Un phénomène de plus en plus observé est celui du hack d'un éditeur de logiciels ou de services qui met en péril tous ses clients. Par exemple, un logiciel peut être livré avec une porte dérobée non détectée. Alors les hackers peuvent attendre plusieurs mois que le maximum de clients l'ait installé, puis lancer une attaque massive. Ils savent qu'ils vont être détectés, mais aussi qu'il faudra quelques heures ou quelques jours pour que l'information soit diffusée, ce qui leur laisse le temps de faire beaucoup de dégâts.

Mais l'industrie s'organise. Frédéric Fautrier, Directeur de l'AMSN, a permis d'organiser à Monaco une rencontre de la Task Force-CSIRT (TF-CSIRT), une association mondiale de tous les centres de réponses à incidents de sécurité informatique. Les vulnérabilités sont de plus en plus cataloguées, il y en a maintenant plus de 50 000 répertoriées, et ce nombre augmente très fortement d'une année sur l'autre.

SMEG

La Boutique by SMEG

11, allée Guillaume Apollinaire • 98000 Monaco
92 05 66 44 • commercial@smeg.mc

SMEG proche de Vous

D'ailleurs l'Europe est en train de créer son propre catalogue, pour ne plus dépendre de celui américain. Des exercices grandeur réelle sont pratiqués, comme en France récemment avec l'exercice de simulation de crise conçu par l'Agence nationale de la sécurité des systèmes d'information (ANSSI), Rempart 25, et nous en pratiquons à Monaco avec des partenaires prestataires. Et, au niveau logiciel, l'industrie fournit un gros effort de consolidation des outils, ce qui va simplifier la gestion de la protection, et donc accroître la sécurité.

MBN/ Quels vont être les grands enjeux en matière de cybersécurité des prochaines années ?

F. C. : C'est une course sans fin. Les hackers ont, par principe, toujours un coup d'avance, mais on peut dire que l'industrie « propre » reste gagnante face à eux parce qu'elle est toujours debout. Elle a su s'adapter au marché, par exemple avec les programmes de Bug Bounty, des récompenses pour la découverte de failles de sécurité qui incitent les hackers à basculer du côté honnête. Ce n'est pas parfait, il faut en permanence continuer à se sensibiliser, s'informer, se protéger, continuer à mettre à jour ses appareils, nous devons tous être vigilants, mais c'est faisable. Apple alerte maintenant les utilisateurs d'iPhone qui ont été infectés par Pegasus, un logiciel d'espionnage. Ce n'est pas préventif, mais cela montre que l'industrie est consciente du problème. Et la régulation aide aussi beaucoup, en obligeant à la diffusion d'informations en cas de hack et en imposant des normes de test très strictes avant diffusion.

Notre société est devenue extrêmement dépendante de la technologie et est donc fragile, et pas seulement aux cyberattaques. En complément de celle déjà citée, le blocage de plus de 8 millions de systèmes Windows impactant des aéroports, des banques, des hôpitaux… le 19 juillet 2024 à cause d'une mise à jour défaillante d'un système de protection, et celui de nombreuses cartes bancaires en France le 30 août dernier méritent d'être rappelés. Là encore, il ne s'agissait pas de cyberattaques, mais les impacts ont été visibles et ont bien montré notre dépendance, d'autant que l'humain est souvent le maillon faible de la chaîne. Malgré toute la sensibilisation et toutes les formations, certains vont connecter une clé USB piégée parce qu'elle montrait le logo d'une société et qu'ils croyaient qu'elle contenait des documents intéressants, ou obéir à un inconnu au téléphone et cliquer sur un lien vérolé parce que cet interlocuteur s'est présenté comme étant du service informatique, voire réinitialiser un mot de passe parce que l'individu s'est présenté comme un utilisateur. Marks & Spencer a ainsi perdu 300 millions de Livres Sterling, presque 350 millions d'euros, en avril dernier.

MBN/ Quel message voudriez-vous faire passer ?

F. C. : La question n'est pas sur la possibilité du hack, mais sur la date de celui-ci, ce n'est pas "si" mais "quand". Il est donc crucial de s'entraîner pour savoir réagir, limiter les dégâts, et reconstruire. Et pour cela, il faut s'informer en permanence, effectuer toutes les mises à jour nécessaires, et ne surtout pas relâcher la pression.

Thomas Cartereau :

« La transition numérique dans tous les secteurs a entraîné une multiplication des points d'entrée, et a donc imposé une exigence de cybersécurité partout »

Thomas Cartereau est Directeur des Systèmes d'Information du groupe SMEG (Société Monégasque d'Électricité et de Gaz). Le MBN l'a interrogé sur les particularités du risque cyber dans son secteur.

MBN/ Que représente le risque cyber pour une entreprise comme la vôtre ?

Thomas Cartereau : La cybersécurité est un enjeu systémique pour une entreprise comme la SMEG. Nous ne devons pas protéger seulement notre système informatique interne, mais aussi tout notre système industriel, c'est-à-dire que le risque pour nous n'est pas que financier et réputationnel, mais concerne toute la production. Nous sommes donc actifs pour assurer la protection des données sensibles, garantir la continuité d'activité, afin de toujours fournir une énergie stable et ininterrompue, et conserver la confiance de nos clients et partenaires. Nous appliquons à toutes nos activités (Efficacité énergétique, production PV, bornes de recharge…) les mêmes exigences de cybersécurité que pour la distribution d'énergies.

MBN/ Quelles évolutions de ce risque avez-vous constaté ces dernières années ?

T. C. : Au niveau de l'évolution du risque cyber nous observons plusieurs tendances. La première est une forte professionnalisation des attaques, qui sont plus sophistiquées, et en provenance d'organisations plus structurées, y compris une hausse du nombre d'attaques de groupes cyber liés à des États. Aussi, l'Intelligence Artificielle est maintenant massivement utilisée pour durcir les attaques, ce qui nous oblige à une vigilance accrue. Une autre tendance est celle de l'élargissement de la surface d'attaque. La transition numérique dans tous les secteurs a entraîné une multiplication des points d'entrée, et a donc imposé une exigence de cybersécurité partout. Nous nous retrouvons confrontés à une menace diffuse qui dépasse largement le cadre des entreprises ciblées, avec des effets collatéraux qui vont très au-delà de la cible initiale. Cela implique que la cybersécurité ne se limite pas à une démarche individuelle, mais doit être une coopération étroite avec les autorités locales monégasques et nos pairs au travers de l'ADIM (Association des Directeurs Informatiques de Monaco, voir interview dans ce numéro).

MBN/ Quels seront les grands enjeux en matière de cybersécurité des prochaines années ?

T. C. : Il y a plusieurs axes. Le premier, et principal, est l'importance de la formation et de la sensibilisation des utilisateurs. La cybersécurité

gsmonaco
imprimeur depuis 1980

FOURNISSEUR BREVETÉ DE
S.A.S. LE PRINCE SOUVERAIN
DE MONACO

Imprim Luxe®
Monaco imprime sa marque

1980–2025

Atelier *Impression*

- Brochures
- Magazines
- Flyers
- Dépliants
- Papeterie
- Affiches
- Adressage

Atelier *Créatif*

- Mise en page
- Infographie
- Design
- Conception
- Pré-presse

45 ANS D'IMPRESSION, D'INNOVATION ET D'ENGAGEMENT HUMAIN.

Atelier *Grand Format*

- Bâches
- Adhésifs
- Signalétique
- Film électrostimulé
- Films solaires
- Trophées

9, Avenue Albert II
Immeuble "Le Copori"
98000 Monaco

+377 92 05 97 97
info@gsmonaco.com

gsmonaco.com

ne se limite pas à des outils techniques dont même les meilleurs sont inutiles face à un clic malheureux qui ouvre une brèche. Cela signifie que chaque collaborateur est un moyen de lutter contre les cybermenaces. Le deuxième axe est celui de la résilience. Il faut prévoir les attaques et être prêts à continuer de fonctionner le cas échéant. Nous devons donc pratiquer des tests réguliers des plans de reprise et de continuité. Le troisième axe est celui de la gouvernance de la donnée. C'est un axe stratégique, il faut renforcer encore davantage la protection et la valorisation des données privatives. Le quatrième axe est celui du développement de l'Intelligence Artificielle (I.A.) qui entraîne une menace croissante avec de nouveaux types d'attaques qui deviennent quotidiennes. L'I.A. permet de massifier les attaques et de les enrichir de données, les rendant plus dangereuses, mais en même temps aide à se défendre : c'est une course entre les robots attaquants et ceux défenseurs. Mais l'humain aura toujours quelque chose à apporter, il bénéficie d'une intelligence supérieure et d'une finesse qui n'existent pas, ou pas encore, en I.A. Enfin, en cinquième axe, il faut développer la confiance numérique, qui est une condition sine qua non du développement du pays, et pour cela renforcer la cybersécurité.

MBN/ Quel message voudriez-vous faire passer ?

T. C. : Il y a trois messages fondamentaux. Tout d'abord, la lutte contre la cybercriminalité oblige à une collaboration à l'échelle du territoire entre les autorités et les entreprises, et l'ADIM occupe un rôle important pour l'animer. Ensuite, il est essentiel de former et sensibiliser tous les utilisateurs, car tous les jours des courriels malveillants posent des risques. Enfin, le contexte géopolitique est particulièrement complexe et renforce encore le risque. Il faut donc se rappeler en permanence que personne n'est à l'abri, qu'une simple erreur d'adresse IP suffit pour une attaque, et qu'Internet n'a pas de frontière.

Martin Péronnet :

« L'avenir de la cybersécurité, c'est que chacun, particuliers comme entreprises, comprenne qu'il est un maillon de la chaîne »

Opérateur historique de la Principauté, Monaco Telecom est une entreprise qui fournit des services essentiels à ses clients. Martin Péronnet, son Directeur Général, décrypte les risques liés à la cybersécurité, la stratégie développée pour y répondre, et explique comment la gouvernance accélère la transformation en cours.

MBN/ Comment votre entreprise gère-t-elle les menaces liées à la cybersécurité dans son activité ?

Martin Péronnet : Premier élément, notre cybersécurité s'envisage d'abord dans le cadre de l'écosystème de Monaco. Au début des années 2010, au cours d'exercices de gestion de crise cyber, nous nous étions rendus compte de la nécessité d'avoir un interlocuteur national, représentant la Principauté, pour orienter efficacement notre stratégie de réponse à incident. Cette réflexion rejoignait les priorités du Gouvernement de l'époque. Nous avons alors travaillé avec les services concernés et Frédéric Fautrier, qui faisait partie de nos équipes, à la mise en place d'une autorité monégasque en matière de défense et de sécurité des systèmes d'information. Cela s'est traduit par la création de l'AMSN, qui a considérablement œuvré à la maturité des acteurs publics et privés dans ce domaine. C'est le véritable chef d'orchestre de la politique cyber de Monaco, ce qui est indispensable.

En interne, nous avons aussi mis en place un comité cyber afin de se donner une visibilité trimestrielle sur les risques majeurs identifiés, prioriser les investissements, suivre l'exploitation des projets, pour progressivement structurer et renforcer l'entreprise autour de cet axe stratégique. Année après année, cela nous a permis de construire une connaissance collective et évolutive, et de progresser constamment dans ce domaine, en toute humilité au vu de l'ampleur de la tâche.

Dans le cadre des réunions annuelles des opérateurs de télécommunications des petits États, nous faisons également en sorte que chacun partage ses problématiques, pour profiter au maximum du retour d'expérience de chacun.

Enfin, faire partie du groupe N.J.J. Holding, contrôlé par Xavier Niel, nous aide également à travailler en réseau pour atteindre des objectifs communs, ce qui apporte beaucoup à chacun. Ceci nous permet notamment d'investir ensemble, à plus grande échelle donc, sur un certain nombre de sujets. C'est le cas par exemple dans le domaine des attaques par DDoS (en anglais : Distributed Denial of Service). Ces attaques, très fréquentes et de plus en plus puissantes, utilisent un grand nombre d'ordinateurs relais malgré eux pour solliciter massivement un serveur et saturer les ressources d'un système, d'un réseau ou du service web d'une entreprise ou d'une organisation, les rendant indisponibles pour les utilisateurs légitimes. Nous avons mis en place, à partir de Monaco, un « parapluie » accessible à l'ensemble des opérateurs du groupe, en complément des protections locales de chacun. Nous avons également des réflexions communes sur le monitoring de nos systèmes, qui est fait à partir de solutions souvent similaires, appelées SOC (Security Operations Center). Ceci dans l'objectif d'améliorer la prévention, la détection et la réponse aux menaces.

MBN/ Quels changements avez-vous observés dans la nature ou la fréquence des risques cyber ces dernières années ?

M. P. : Les virus informatiques existent depuis très longtemps, les menaces cyber ont collé aux développements de la technologie. Dans

les années 2010, on parlait déjà des Anonymous. Les ransomwares, les crypto lockers existent depuis des années. Les grands principes de la cybercriminalité ne datent donc pas d'hier, mais nous constatons en revanche un renforcement de la fréquence et de la puissance des attaques.

En parallèle, le numérique étant de plus en plus indispensable au fonctionnement d'un État, d'une entreprise ou même d'un foyer, les obligations qui s'imposent à nous en matière de protection se sont renforcées. Au-delà de l'arsenal juridique dont s'est notamment doté Monaco, certains secteurs sensibles ont aussi des obligations réglementaires spécifiques à respecter pour se conformer aux exigences en matière de cybersécurité. C'est le cas des banques, qui doivent appliquer les règlements européens, notamment le « Digital Operational Resilience Act » (DORA). Celui-ci entre en application en 2025. Son objectif est de renforcer la résilience opérationnelle numérique des entités financières face aux cybermenaces et aux risques liés aux technologies de l'information et de la communication. Avec DORA, les banques, dont celles de Monaco, doivent répondre d'un certain niveau de protection sur les services numériques qu'elles utilisent. Leurs fournisseurs principaux, à l'instar de Monaco Telecom, sont soumis aux mêmes exigences.

En résumé, les menaces se renforcent, et face à elles la façon de considérer la notion de sécurité et de la traduire sur le terrain a considérablement évolué.

MBN/ Quelles perspectives anticipez-vous pour les années à venir ?

M. P. : La cybersécurité ne s'arrête pas à nos équipements, elle concerne aussi la façon dont nos clients utilisent leurs services, et notamment comment ils gèrent leurs emails. L'email est un protocole utilisé depuis longtemps par tout le monde, et ses modes d'utilisation ne sont pas toujours en phase avec l'évolution des exigences de cybersécurité. Aujourd'hui, les emails sont devenus des vecteurs d'attaques très importants. Par le biais d'envoi de mails copiant des messages légitimes, les pirates amènent les clients à divulguer des informations personnelles, et récupèrent progressivement des données sensibles comme des accès à des comptes bancaires. C'est ce qu'on appelle communément de l'hameçonnage ou du phishing.

Dès qu'un attaquant réussit à connaître le mot de passe d'accès à l'adresse mail d'un utilisateur, cette adresse devient un vecteur d'attaque potentiel pour les autres clients. Un mail venant d'une adresse en monaco.mc paraîtra plus légitime à son récepteur, qui sera plus enclin à y répondre, prolongeant ainsi l'attaque. Les mots de passe trop simples et/ou réutilisés sur plusieurs sites sont dangereux pour soi-même, mais également un fléau pour

la communauté. Nous travaillons avec l'AMSN pour renforcer les protections collectives. Par exemple, en forçant tous les utilisateurs à n'utiliser que le serveur d'envoi monaco.mc et à configurer chaque device permettant de télécharger ses mails sur des serveurs de réception et d'envoi d'emails sécurisés (POP S, IMAP S, SMTP S). L'évaluation bénéfice-risque montre que ces restrictions progressives d'utilisation sont nécessaires. Car le risque est énorme, et Monaco, comme les autres pays, est une cible. Nous mettons également en place progressivement une politique de double authentification. C'est déjà le cas sur l'espace client MyMT, seule interface permettant de changer le mot de passe de son adresse mail. Ce sera également le cas dans les mois à venir sur l'accès au webmail.

Plus généralement, la gouvernance mise en place par l'AMSN accélère la transformation en cours en obligeant les acteurs concernés à se conformer à des exigences légales et réglementaires, à des procédures. L'avenir de la cybersécurité, c'est que chacun, particuliers comme entreprises, comprenne qu'il est un maillon de la chaîne.

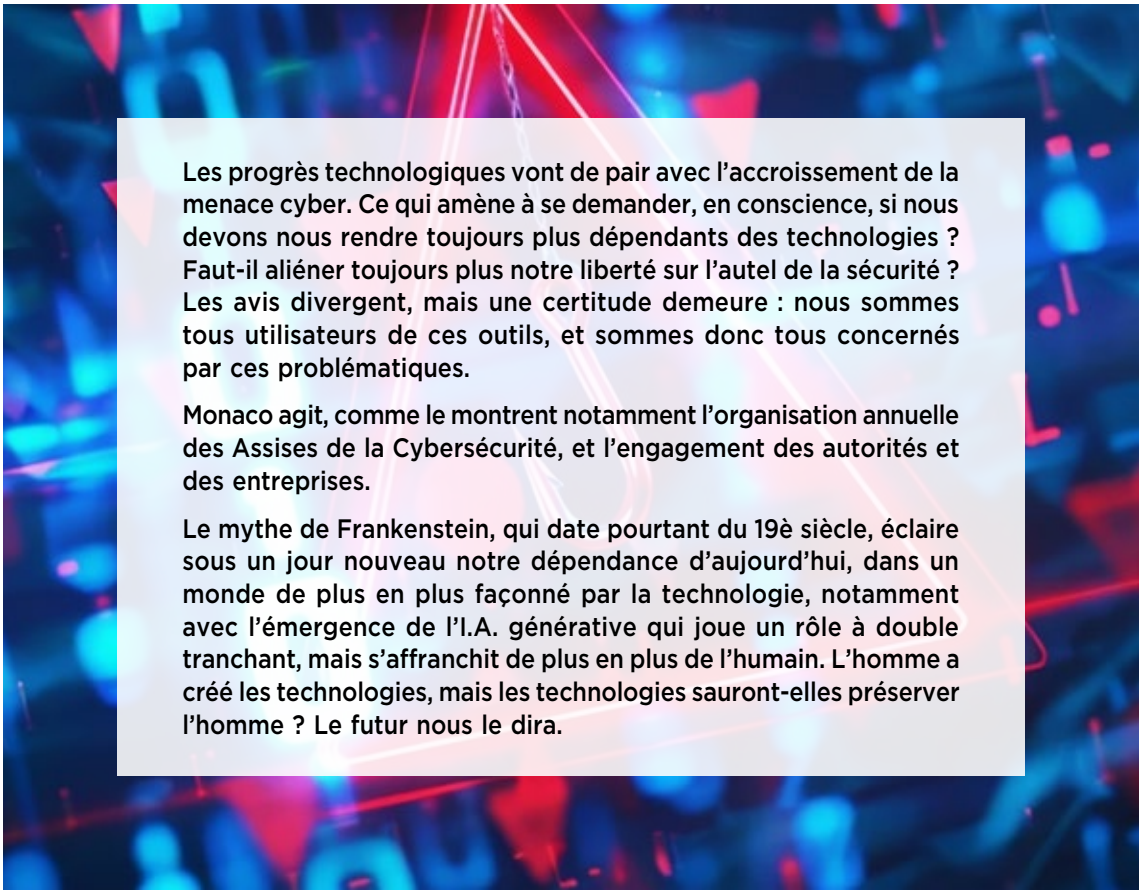
MBN/ L'I.A. est-elle un facteur aggravant ?

M. P. : Oui. Par exemple, avant le développement de l'I.A., les emails de phishing étaient truffés de fautes d'orthographe, aujourd'hui ils paraissent totalement crédibles. L'I.A. oblige donc à un renforcement des procédures de sécurité avec entre autres conséquences une restriction des espaces de liberté. Mais cet effort est indispensable pour pouvoir continuer d'utiliser les outils numériques. La sécurité est à ce prix.

Arnaqué en ligne ? Tout n'est peut-être pas perdu : réagissez vite !

Depuis 2022, INTERPOL a mis en place le mécanisme mondial I-GRIP de blocage rapide des paiements. En accélérant la coopération entre les forces de police, de renseignement, et les banques des 196 pays membres, il a déjà permis d'intercepter des centaines de millions de dollars.

Concrètement, cela signifie que si vous avez été amené à effectuer un paiement à un escroc, il sera peut-être possible de le bloquer, et donc que vous récupériez votre argent. Mais il vous faut agir vite : dès que vous avez conscience de vous être fait avoir, contactez les Autorités !



Les progrès technologiques vont de pair avec l'accroissement de la menace cyber. Ce qui amène à se demander, en conscience, si nous devons nous rendre toujours plus dépendants des technologies ? Faut-il aliéner toujours plus notre liberté sur l'autel de la sécurité ? Les avis divergent, mais une certitude demeure : nous sommes tous utilisateurs de ces outils, et sommes donc tous concernés par ces problématiques.

Monaco agit, comme le montrent notamment l'organisation annuelle des Assises de la Cybersécurité, et l'engagement des autorités et des entreprises.

Le mythe de Frankenstein, qui date pourtant du 19è siècle, éclaire sous un jour nouveau notre dépendance d'aujourd'hui, dans un monde de plus en plus façonné par la technologie, notamment avec l'émergence de l'I.A. générative qui joue un rôle à double tranchant, mais s'affranchit de plus en plus de l'humain. L'homme a créé les technologies, mais les technologies sauront-elles préserver l'homme ? Le futur nous le dira.

Dossier réalisé par Carole Quazzolo & Philippe Gouillou