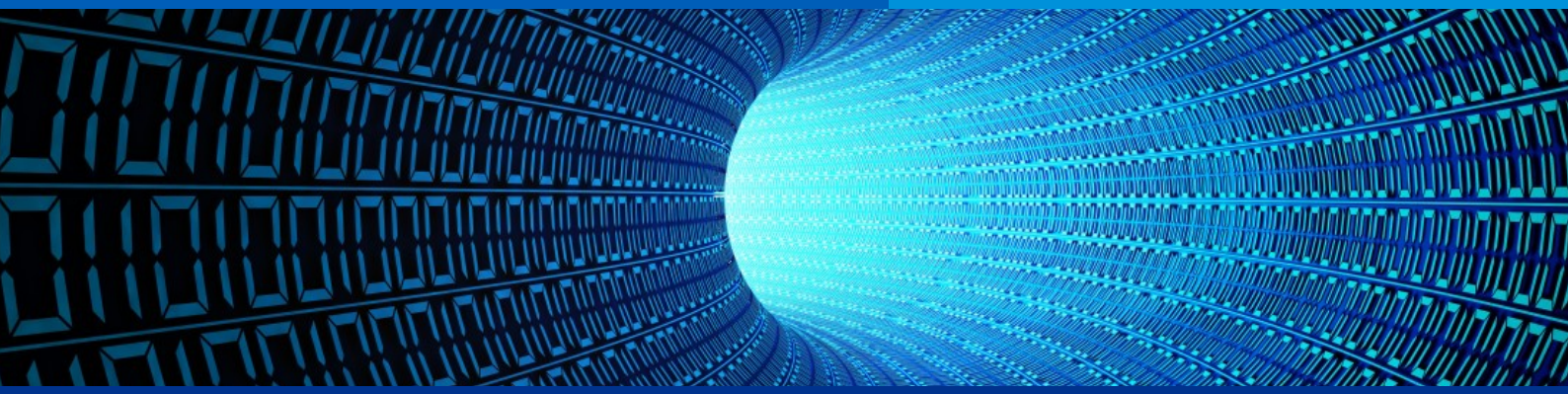
KPMG GLD & Associés Monaco

IT Advisory

Octobre 2020



Cybersécurité à Monaco : risques et prévention pendant la COVID-19

KPMG Monaco fait le point sur l'impact accru de la cybercriminalité en temps de COVID-19 (piratages, fraudes, chantages, attaques informatiques…) et les mesures de protection en Principauté de Monaco, des réflexes élémentaires aux obligations réglementaires.

Sommaire

COVID-19 : une pandémie digitale ?

Un contexte propice aux cyber-attaques

Source de "disruption" protéiforme, la pandémie de la COVID-19 a non seulement poussé les entreprises à repenser leurs objectifs à court terme, mais les a en outre obligé à se réorganiser en profondeur – au-delà de la préservation de la santé de leurs collaborateurs – pour protéger leur activité économique.

Les défis à court et moyen terme des entreprises face à la COVID-19 sont ainsi nombreux et variés :

- ✓ Priorisation du maintien de l'activité ;
- ✓ Déploiement rapide du télétravail à grande échelle ;
- ✓ Mise à disposition des outils et ressources à distance ;
- ✓ Disponibilité aléatoire des dirigeants et employés ;
- ✓ Impact négatif sur les clients, partenaires et fournisseurs.

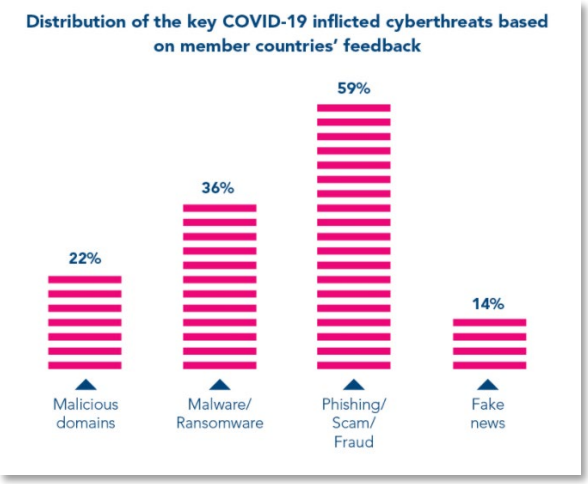
Ces profondes perturbations, remises en question et réorganisations ont fourni un terreau propice aux cyber criminels pour tenter de mettre à mal les défenses des systèmes informatiques.

A titre d'exemple, le FBI a ainsi rapporté une multiplication par quatre du nombre de plaintes pour cyber-attaques aux États-Unis depuis le début de la pandémie (4.000 par jour contre 1.000 précédemment).

Même son de cloche du côté d'Interpol : « *Les cybercriminels développent et renforcent leurs attaques à un rythme alarmant* », explique son Secrétaire Général Jürgen Stock, « *exploitant la peur et l'incertitude causées par la situation sociale et économique instable créée par COVID-19* ».

Le télétravail, talon d'Achille de la SSI

Loin des pares-feux et mesures de sécurité intra-muros usuelles en entreprise, le personnel en télétravail est une proie d'autant plus facile. Une aubaine pour les hackers qui peuvent d'autant plus facilement attaquer les réseaux des entreprises de l'extérieur.



Source : Interpol

Signe des temps, le piratage via les réseaux sociaux (social engineering) est de plus en plus répandu, mais on note surtout une envolée des cyber-attaques via les courriers électroniques par hameçonnage (*phishing*) impliqués dans 59% des cyber attaques ciblées sur des thèmes liées à la COVID-19, devant les rançongiciels (ransomware) et logiciels malveillants (*malware*).

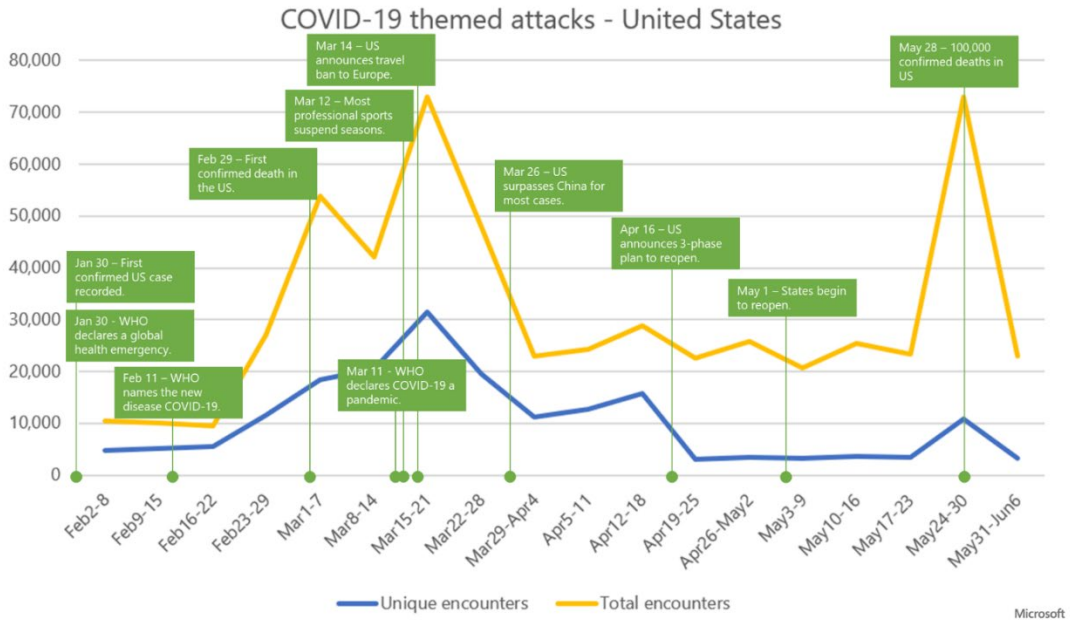
Loin d'être anodines, les attaques par hameçonnage permettent aux pirates de collecter des données personnelles qui peuvent être exploitées par exemple à des fins de "compromission de la messagerie en entreprise" (*BEC - Business Email Compromise*). Cette dernière technique a coûté à elle seule plus de 2 Milliards $ USD de pertes directes en 5 ans aux seules entreprises américaines.

En pratique, le *phishing* est généralement activé en cliquant sur un lien internet vers un "faux site" (imitation du site de l'entreprise, de fournisseurs connus, de l'administration…), soit par le téléchargement et l'activation d'une pièce jointe piégée.

Des attaques thématiques, ciblées localement

Afin de renforcer leurs chances de succès, ces types de piratage ont une nette tendance à surfer sur des sujets sensibles et l'actualité du moment, qui est bien entendu dominée par les conséquences de la pandémie toujours en cours.

En juin dernier, Microsoft a ainsi publié des statistiques mettant en évidence la corrélation entre le nombre d'attaques répertoriées et les moments clés de la pandémie de COVID-19 aux États-Unis.



Source : Microsoft

« Les cybercriminels recherchent constamment le point d'entrée ou de compromission le plus facile.(…) Lors de l'épidémie de COVID-19, ils ont étroitement imité les développements locaux de la crise et leurs réactions », note le rapport.

La nouvelle menace : réputation contre rançon

Mais les pirates informatiques ne se limitent pas à suivre l'actualité. À l'instar de leurs victimes – en priorité des grandes entreprises - ils ont ainsi profité du contexte de la pandémie pour adapter leurs objectifs.

Face à une double crise globale - économique et de confiance - les entreprises particulièrement soucieuses de leur réputation, notamment en termes de sécurité des données et de leur capacité à les protéger, font ainsi face à une nouvelle menace.

Ainsi, plutôt que de voler des données ou se lancer dans de complexes et longues opérations de "*BEC* " et / ou "*FOVI*" (faux ordres de virement), les pirates (*"threat actors"*) utilisent leur *malware* pour des gains moins ambitieux, plus court-termistes mais redoutablement efficaces.

« *Les criminels ont fait évoluer les ransomwares vers ce qu'on appelle des "doxwares"* », explique Zohar Pinhasi, expert en cyberterrorisme. « *Si vous ne payez pas, nous vendrons vos données et, en plus, informerons vos clients que vous avez été piraté et que leurs données ont été compromises. Cela change la donne depuis le début du coronavirus - nous l'avons vu dans le passé, mais pas à ce degré* ».

Le risque cybersécurité à Monaco

Un développement accéléré de Monaco vers la Smart City

Bien que le secteur du numérique représente moins de 5% du PIB monégasque, la Principauté a mis en œuvre ces dernières années un ambitieux plan de transition digitale à l'échelle du pays.

Pilotée par la Délégation Interministérielle chargée de la Transition Numérique dirigée par M. Frédéric Genta, cette nouvelle politique numérique a notamment permis à Monaco de déployer le premier réseau commercial en 1 Gigabit/s au monde, puis en avril 2017 de devenir le premier pays au monde intégralement couvert par la 5G.

Plus récemment, la Principauté est Le Gouvernement princier a lancé plusieurs initiatives d'ampleur dont la création d'une infrastructure « cloud » sécurisée et souveraine, fer de lance de l'initiative Extended Monaco dont l'objectif à terme est de faire de Monaco une ville intelligente "*Smart City*" unique en son genre.

Ce développement au pas de charge s'accompagne forcément de nombreux questionnements en termes de cybersécurité notamment en raison des particularités de l'écosystème économique monégasque.

La cybersécurité, priorité de la transition numérique

Pour répondre à ces problématiques, le Gouvernement Princier a créé dès 2016 l'Agence Monégasque de Sécurité Numérique (AMSN) qui traite de toutes les questions de sécurité et de confidentialité dans l'espace digital.

« *La Principauté comme tous les Etats est une cible potentielle par son image et ses positions affichées dans le monde, mais également les affaires financières et économiques qu'elle génère* », a ainsi déclaré le Contre-Amiral M. Dominique RIBAN, Directeur de AMSN.

« *La sécurité, c'est l'ADN de Monaco. Et c'est ma priorité numéro 1, ma ligne rouge.* », a renchéri M. Genta.

L'arsenal monégasque se compose notamment d'un volet législatif (3 lois appuyées par une dizaine d'arrêtés) renforcé par la création d'un centre de réponse aux incidents de sécurité numérique (CERT-MC) internationalement reconnu et intégré au *Forum of Incident Response of Security Team* (FIRST) regroupant des centaines d'entités publiques, privées et universitaires à travers 86 pays.

À l'occasion de la 19e édition des Assises de la sécurité et des systèmes d'information (Octobre 2019), M. Riban avait estimé qu'il était « *essentiel de préparer la Principauté de Monaco à faire face à une crise informatique majeure* ».

Le Directeur de l'AMSN ne s'attendait peut-être pas à devoir y faire face de sitôt, mais la menace est devenue réalité avec la pandémie COVID-19.

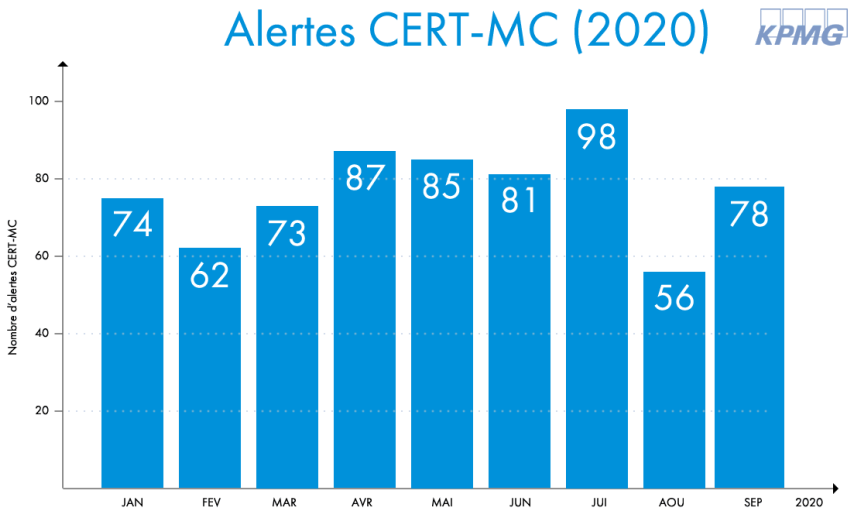
Ses services avaient ainsi noté dès mars 2020 « *une augmentation, en Principauté, du nombre d'accès distants ouverts (RDP, VNC). (…) Profitant de ces accès ouverts vers des réseaux qui leur sont inaccessibles en temps normal, les attaquants sont actuellement très actifs* ».

Début septembre, l'ASMN a alerté la Principauté sur « une campagne de phishing sans précédent »

L'analyse de Microsoft confirme par ailleurs que « les campagnes de malware, l'infrastructure des attaques et les attaques de phishing ont tous montré des signes de ce comportement opportuniste ».

Microsoft explique en outre que « l'industrie se concentre parfois fortement sur les attaques avancées qui exploitent les vulnérabilités de type "jour zéro"*, mais chaque jour, le plus grand risque pour un plus grand nombre de personnes est d'être amené à exécuter des programmes inconnus ou des documents cheval de Troie ».

** Vulnérabilité informatique n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu.*



Nombre mensuel d'alertes publiées par le CERT-MC en 2020

Cybersécurité en entreprise : 5 clés pour une nouvelle réalité

L'un des défis chroniques du leadership en cybersécurité consiste à trouver un équilibre entre l'amélioration proactive de la sécurité et la réaction instinctive à court terme aux événements. Nous constatons souvent que les considérations tactiques détournent l'attention des problèmes stratégiques à long terme. Mais avec la pandémie COVID-19, il y a eu une réinitialisation matérielle.

Les professionnels de KPMG ont travaillé avec le Centre pour la cybersécurité du Forum Economique Mondial (WEF) pour établir un ensemble de cinq principes directeurs pour aider les dirigeants de la cybersécurité à se préparer à la nouvelle réalité de la COVID-19.

Le document du WEF, qui décrit ces principes plus en détail, est un effort collectif des partenaires publics et privés du WEF C4C pour aider les clients à traverser ce changement de phase numérique et à passer à la nouvelle réalité.

1. Favorisez une culture de la cyber-résilience : les entreprises doivent chercher à abolir les barrières entre les services, unifier la culture de la résilience à travers l'informatique, la technologie opérationnelle et les fonctions commerciales et promouvoir la résilience dès la conception dans toute l'entreprise. Il ne s'agit pas seulement de cocher des cases. Il doit y avoir un sentiment d'urgence collective concernant les besoins en cybersécurité au-delà des seules fonctions de sécurité et de protection de la vie privée, et la Direction devrait se responsabiliser - en s'assurant que les risques sont bien compris, que les plans sont conçus et que la coordination est efficace.

2. Concentrez-vous sur la protection des capacités et des services critiques : la pandémie a révélé à quel point nous en savons peu sur nos ressources et services essentiels, ainsi que sur la meilleure approche pour les protéger. Les entreprises doivent rétablir une culture de "cyber-hygiène" au sein de la main-d'œuvre, passer à de nouveaux modèles de gestion des accès et de surveillance des activités sur les actifs critiques et prioriser les investissements dans la cyber-automatisation.

3. Équilibrez les décisions tenant compte des risques pendant la crise et au-delà : la gestion des "cyber risques" nécessite une remise à plat. La pandémie a

prouvé que les anciennes hypothèses de risque de la chaîne d'approvisionnement étaient erronées, les mesures traditionnelles de cyber-résilience se révélant déconnectées du risque réel. Les entreprises doivent revoir leur approche des chaînes d'approvisionnement; définir des mesures pratiques et significatives des cyberrisques; et se concentrer sur les risques opérationnels lors de la conception de nouvelles stratégies numériques.

4. Mettez à jour et en pratique vos plans de réponse et de continuité d'activité : l'une des hypothèses sous-jacentes à la plupart des plans de continuité d'activité cybernétique est l'indépendance du reste de l'écosystème, qui peut s'appuyer sur les fournisseurs et les partenaires habituels. La pandémie nous oblige à remettre en question cette perspective. Les entreprises doivent revoir les processus de planification de la résilience et les tester, en dotant les équipes de gestion de crise des compétences et de l'expérience nécessaires pour gérer sous une pression intense. Ils doivent également revoir les "scénarios du pire" dans cette nouvelle réalité.

5. Renforcez la collaboration à l'échelle de l'écosystème : l'union fait la force, et un des rares côtés positifs de la pandémie aura été de démontrer la nécessité d'une coopération efficace à l'échelle globale. Les gouvernements collaborent pour lutter contre les cybermenaces internationales; les grandes entreprises mettent en commun leurs données sur les menaces; et les régulateurs voient la valeur de la transparence et de l'action collective dans la planification de la résilience des écosystèmes. Les entreprises devraient réfléchir à la meilleure façon de coopérer avec leurs réseaux industriels, tout en mettant en place des sessions de sensibilisation et de partage de renseignements en collaboration, travailler ensemble pour perturber les activités cybercriminelles et enfin adopter une approche systémique de la gestion des risques dans un cadre sectoriel global.

Plus que jamais, les systèmes d'information sont un élément fondamental de maîtrise de l'activité.

En Principauté de Monaco, l'Agence Monégasque de Sécurité Numérique (AMSN) est une aide précieuse en termes de détection et de traitement des attaques informatiques, cependant il appartient aux entreprises et plus particulièrement aux OIV (Opérateurs d'Importance Vitale) d'assurer leur propre sécurité.

Dans cette optique, tous les OIV doivent entreprendre une démarche d'homologation PASSI auprès d'auditeurs qualifiés tels que KPMG Monaco (voir Homologation PASSI à Monaco).

Comment se protéger ?

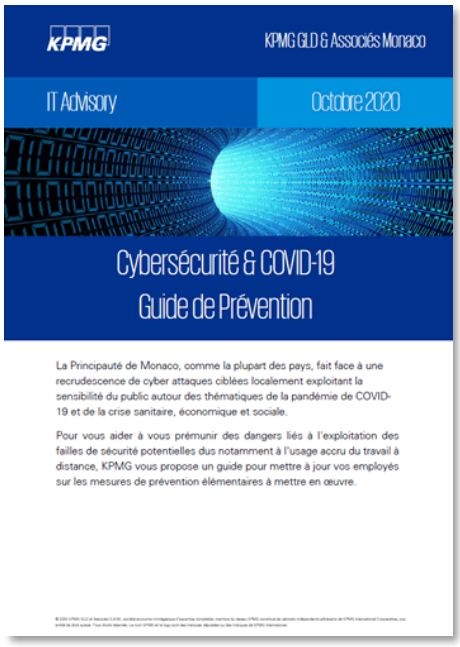
Développer des réflexes élémentaires

Face au développement d'attaques de *phishing* et *malware* profitant du contexte sanitaire et économique, la plus grande vulnérabilité des entreprises étant désormais le personnel recourant de plus en plus au télétravail, ces derniers sont aussi la première ligne de défense.

La plupart des grandes entreprises ont mis en place des protocoles de sécurité stricts, mais les recommandations usuelles doivent désormais s'adapter au risque et d'attaques exploitant les sensibilités accrues aux thématiques liées à la COVID-19.

Afin de mieux protéger votre entreprise, vous pouvez aider vos collaborateurs à mettre en œuvre les bonnes pratiques pour faire face à ces menaces grâce aux guides pratiques ci-dessous.

Téléchargez les guides pratiques KPMG Monaco et AMSN



Pour vous aider dans votre démarche d'actualisation de vos protocoles et informer vos collaborateurs des risques de cybersécurité spécifiques durant la période COVID-19, nous vous invitons à télécharger notre Guide de Prévention Cybersécurité COVID-19.

Vous pouvez aussi consulter régulièrement les alertes sur les cyber-attaques publiées par le CERT-MC sur le site de l'AMSN ou télécharger les Guides Pratiques de l'ASMN.

Homologation PASSI à Monaco

Les entreprises qualifiées PASSI à Monaco sont en capacité d'auditer la sécurité des systèmes informatique en suivant un processus strict de certification et le référentiel PASSI, ainsi que défini par l'Arrêté Ministériel 2017-625 du 16 août 2017.

L'homologation PASSI permet notamment de certifier les points suivants :

- ✓ Garantie de compétences des auditeurs en charge de l'audit
- ✓ Garantie de déontologie, de protection et de confidentialité des données, rapports et documents échangés
- ✓ Garantie d'une méthodologie appropriée aux audits de sécurité
- ✓ Recours possible auprès de l'Agence Monégasque de Sécurité Numérique (AMSN) si la prestation réalisée s'avère non conforme au référentiel PASSI.

Nos services homologation PASSI à Monaco

KPMG GLD & Associés Monaco fait désormais partie du cercle très restreint des entreprises ayant obtenu le diplôme de qualification de Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) auprès des autorités monégasques.

PASSI QUALIFIÉ AMSN PRINCIPAUTÉ DE MONACO

- ✓ + de 100 collaborateurs basés à Monaco au sein du cabinet ;
- ✓ + de 120 missions d'audit / conseil SI à Monaco ;
- ✓ Pour la 3ème année consécutive, KPMG leader mondial en Cyber Sécurité ;
- ✓ Qualifié PASSI sur toutes les activités d'audit de sécurité avec un « Lab » dédié ;
- ✓ 1er « Big Four » avec une équipe « Audit et Conseil en SI » à temps plein à Monaco ;
- ✓ Données collectées et stockées exclusivement à Monaco ;
- ✓ Réseau mondial de plus de 2.500 experts en cybersécurité dans 50 pays ;
- ✓ Spécialisé dans l'accompagnement des OIV et les audits d'homologation PASSI ;

Pour plus d'informations, contactez notre service IT Advisory.

Liens utiles / Plus d'informations

KPMG - Cyber sécurité à Monaco : risques et prévention pendant la COVID-19 : https://home.kpmg/mc/fr/home/insights/2020/09/cybersecurite-covid-19-guide-de-prevention.html

KPMG Monaco : Homologation PASSI à Monaco https://home.kpmg/mc/fr/home/services/advisory/it-advisory-homologation-passi.html

KPMG Monaco : Cyber Sécurité : évaluations et accompagnement https://home.kpmg/mc/fr/home/insights/2020/01/kpmg-monaco-technologie-securite.html

Agence Monégasque de Sécurité Numérique : https://amsn.gouv.mc

Alertes CERT-MC (AMSN) : https://amsn.gouv.mc/Alertes-CERT-MC/

Voir le site de l'ASMN pour plus d'informations sur la qualification de Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) à Monaco.

L'Homologation de sécurité en neuf étapes : https://amsn.gouv.mc/var/amsn/storage/original/application/1eef84da244679829afb98664c63a2f5.pdf

Recommandations de sécurité informatique pour le télétravail en situation de crise : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

KPMG - Key cyber security considerations for 2020 *(en anglais)* : https://assets.kpmg/content/dam/kpmg/xx/pdf/2020/03/all-hands-on-deck-key-cyber-security-considerations-for-2020.pdf

Références

- ✓ Arrêté Ministériel n° 2017-625 du 16 août 2017 portant application de l'article 3 de l'Ordonnance Souveraine n° 5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique, modifiée
  https://amsn.gouv.mc/var/amsn/storage/original/application/63ed32e77a07e18d54292f87bfbd2db1.pdf

- ✓ Stratégie nationale pour la sécurité du numérique
  https://amsn.gouv.mc/var/amsn/storage/original/application/822de9d606448af4e900f566abd3e00c.pdf

- ✓ AMSN : L'Homologation de sécurité en neuf étapes
  https://amsn.gouv.mc/var/amsn/storage/original/application/1eef84da244679829afb98664c63a2f5.pdf

- ✓ Loi n. 1.435 du 08/11/2016 relative à la lutte contre la criminalité technologique
  https://www.legimonaco.mc/305/legismclois.nsf/ViewTNC/071DFB732FED8FFAC125807A0031956B!OpenDocument

- ✓ Loi n°1402 – Loi portant approbation de ratification de la Convention sur la cybercriminalité du Conseil de l'Europe
  https://www.conseil-national.mc/2013/11/27/1402-loi-portant-approbation-de-ratification-de-la-convention-sur-la-cybercriminalite-du-conseil-de-leurope/

- ✓ Délégation Interministérielle chargée de la Transition Numérique
  https://www.gouv.mc/Gouvernement-et-Institutions/Le-Gouvernement/Ministere-d-Etat/Delegation-Interministerielle-chargee-de-la-Transition-Numerique

- ✓ World Economic Forum (WEF) – Cybersecurity Strategic Intelligence
  https://intelligence.weforum.org/topics/a1Gb00000015LbsEAE?tab=publications

- ✓ FIRST is the global Forum of Incident Response and Security Teams
  https://www.first.org/

- ✓ Identifying & responding to COVID-19 themed cyber threats
  https://home.kpmg/xx/en/home/insights/2020/03/covid-19-staying-cyber-secure.html

Sources

- ✓ La société KPMG obtient sa qualification de Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI) à Monaco
  https://www.gouv.mc/A-la-Une-du-Portail/La-societe-KPMG-obtient-sa-qualification-de-Prestataire-d-Audit-de-la-Securite-des-Systemes-d-Information-PASSI-a-Monaco
- ✓ Communiqué de l'AMSN - Accès distants
  https://amsn.gouv.mc/Actualites-AMSN2/Communique-de-l-AMSN-Acces-distants/
- ✓ INTERPOL report shows alarming rate of cyberattacks during COVID-19
  https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19
- ✓ Exploiting a crisis: How cybercriminals behaved during the outbreak
  https://www.microsoft.com/security/blog/2020/06/16/exploiting-a-crisis-how-cybercriminals-behaved-during-the-outbreak/
- ✓ Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic
  https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html
- ✓ Quand Monaco se saisit des enjeux stratégiques du numérique
  https://sd-magazine.com/securite-numerique-cybersecurite/quand-monaco-se-saisit-des-enjeux-strategiques-du-numerique
- ✓ La fraude : une menace globale protéiforme
  https://home.kpmg/mc/fr/home/insights/2019/05/fraude-menace-proteiforme-banques-defi-secteur-bancaire-rapport.html
- ✓ Cybersécurité : à Monaco, des Assises sous le signe de la détection des menaces
  https://www.industrie-techno.com/article/cybersecurite-a-monaco-des-assises-sous-le-signe-de-la-detection-des-menaces.57474
- ✓ US Federal Bureau of Investigation : Common Scams and Crimes
  https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/
- ✓ US Federal Bureau of Investigation : Alert Number I-040620-PSA
  https://www.ic3.gov/media/2020/200406.aspx
- ✓ Hacking against corporations soars as staff work from home
  https://eandt.theiet.org/content/articles/2020/04/hacking-against-corporations-surges-as-people-work-from-home/
- ✓ Cloud monégasque - Une cible de choix pour les hacktivistes ?
  https://www.monacohebdo.mc/dossier/cloud-monegasqueune-cible-de-choix-hacktivistes%E2%80%89/

- ✓ Recommandations de sécurité informatique pour le télétravail en situation de crise
  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/recommandations-securite-informatique-teletravail

- ✓ CORONAVIRUS – COVID-19 : Appel au renforcement des mesures de vigilance cybersécurité
  https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/coronavirus-covid-19-vigilance-cybersecurite

- ✓ Identifying & responding to COVID-19 themed cyber threats
  https://home.kpmg/xx/en/home/insights/2020/03/covid-19-staying-cyber-secure.html

Contactez-nous

Bettina Ragazzoni
Associé
bragazzoni@kpmg.mc

André Garino
Associé
agarino@kpmg.mc

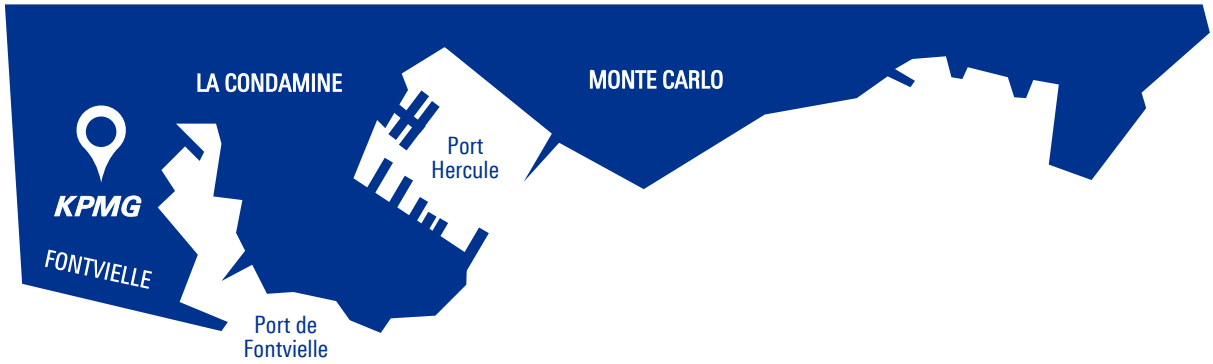
Bernard Squecco
Associé
bsquecco@kpmg.mc

Tony Guillemot
Associé
tguillemot@kpmg.mc

Stéphane Garino
Associé
sgarino@kpmg.mc

Gérard de Gregori
Associé
gdegregori@kpmg.mc

2, rue de la Lüjerneta - “Athos Palace” - 98000, Monaco



+377 97 777 700

www.KPMG.mc

mc-contact@kpmg.mc

@kpmg-monaco

@KPMGMonaco

@KPMG_Monaco