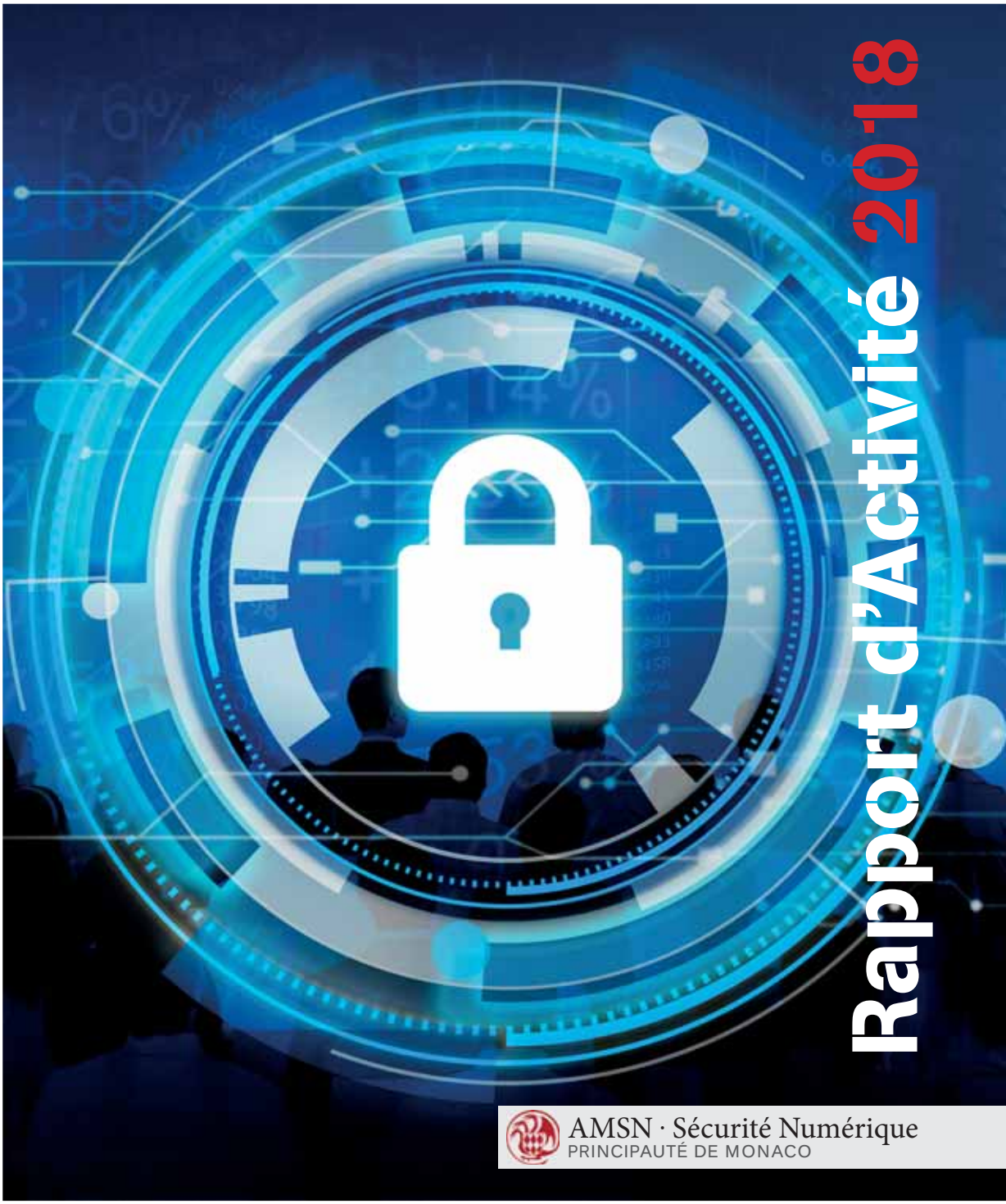
Agence Monégasque de Sécurité Numérique



Rapport d'Activité 2018

AMSN · Sécurité Numérique
PRINCIPAUTÉ DE MONACO

amsn.gouv.mc

RAPPORT D'ACTIVITÉ

de L'AGENCE MONÉGASQUE DE SÉCURITÉ NUMÉRIQUE

JANVIER 2018 – DÉCEMBRE 2018

« Ils ne savaient pas que c'était impossible …
Alors, ils l'ont fait »

Le mot du Directeur

Les démocraties sont la cible d'attaques de plus en plus discrètes et sophistiquées.

Voici maintenant deux ans et demi que l'Agence Monégasque de Sécurité Numérique (AMSN) voyait réellement le jour par l'arrivée de son directeur et de son directeur adjoint. Autorité administrative et autorité nationale, elle est dédiée essentiellement à la sécurisation des systèmes d'information de l'État et des Opérateurs d'Importance Vitale (OIV). Après ce temps de construction des fondations, est venu le temps des opérations. Les attaques sont devenues une réalité prégnante en Principauté. L'AMSN a trouvé en cette année 2018, s'il était besoin de le prouver, sa vraie raison d'être, par le traitement de plusieurs attaques complexes.

J'écrivais, dans le rapport de 2017 : « il est urgent d'aller vers le tout numérique. Le vrai sujet est d'instaurer les conditions de sécurité indispensables à l'accompagnement de cette transition ». La sécurité numérique n'est plus une option, c'est un véritable enjeu de gouvernance et de souveraineté, tant dans les services de l'État que dans les entreprises. La vie, le travail, la sécurité, le bien-être des Monégasques, des résidents ou des pendulaires dépendent de la sécurité numérique. Et ce d'autant plus, qu'une volonté très forte du gouvernement d'effectuer une transition numérique rapide a été décidée. La protection des données personnelles pour cette transition est impérative, que ce soit pour réussir, pour la souveraineté de la Principauté ou pour la reconnaissance par l'Europe.

Dans ce contexte, l'AMSN a continué de mettre en place le cadre réglementaire et les moyens techniques indispensables à la confiance numérique et à la protection de la souveraineté de la Principauté dans ce domaine.

La confiance des plus hautes autorités de la Principauté, dans l'AMSN et ses équipes, a été à nouveau confirmée et des moyens importants ont été attribués par le Gouvernement et le Conseil National. Grâce à ces moyens, tant humains que matériels, l'AMSN, en se concentrant sur la protection et la défense des systèmes d'information des services de l'État et des OIV, a pu mettre en place des capacités opérationnelles d'un très haut niveau technique et des processus efficaces de traitement d'attaque.

La publication de l'Arrêté Ministériel définissant les obligations des OIV en matière de sécurité des systèmes d'information est maintenant effective. Le dialogue de qualité et de confiance qui a été établi et qui perdure, est un gage de réussite. L'AMSN devrait concrétiser en 2019 une offre de détection qualifiée des incidents de sécurité, à destination des OIV.

Au service de la Principauté, le premier Prestataire d'Audit de la Sécurité des Systèmes d'Information (PASSI), a été qualifié au terme d'une année de travail acharné. Il est à noter que cette entreprise est monégasque. Devraient suivre en 2019 quatre autres qualifications d'entreprises monégasques ou françaises qui se sont implantées en Principauté pour obtenir cette qualification.

Bien sûr, toutes ces actions et tout ce travail ont été effectués, grâce aux ressources humaines de l'Agence, ressources de très grande qualité et d'une disponibilité exceptionnelle, mais aussi grâce à l'écoute et au travail des services de l'État ou des OIV concernés par la cybersécurité.

Je tiens aussi à souligner le travail effectué par les entreprises monégasques de l'écosystème cyber. Pour la première fois les entreprises de la Principauté ont pu se regrouper autour de l'AMSN sous le nom de « Monaco Cyber Initiative », à l'occasion de la 18ème édition des Assises de la Sécurité du 10 au 12 octobre 2018 à Monaco; un des salons les plus importants en Europe sur ce sujet. Cela montre que notre pays est bien présent et a toute sa place dans la cybersécurité. Je forme le vœu que cette initiative puisse perdurer pour les futurs évènements de cybersécurité.

Par ailleurs, aujourd'hui, toute la réglementation pour les services électroniques de confiance (signature, authentification, identité, horodatage, cachet) est en place. L'AMSN travaille depuis quelques mois pour permettre la délivrance de certificats électroniques d'ici la fin 2019, préalable indispensable à la mise en place de ces services.
Ainsi, la maturité en matière de sécurité numérique de la Principauté, évaluée par l'ONU en 2018, montre une progression exceptionnelle. En 2016, la Principauté se plaçait 103ème sur 175 pays dans le monde ayant répondu au questionnaire et 38ème sur 43 pays européens. En 2018, la Principauté est 43ème sur 175 au classement mondial et 26ème sur 43 en Europe.

Ce deuxième rapport d'activité effectue le bilan du travail réalisé entre janvier 2018 et janvier 2019 et présente les principaux travaux de 2019. J'espère qu'il vous permettra de comprendre tout l'intérêt et le sens du travail de l'AMSN. Je peux vous affirmer que notre volonté et notre détermination pour améliorer la confiance dans le numérique sont intactes et plus fortes que jamais.

Dominique RIBAN

Sommaire

Présentation

L'AMSN en 6 questions

Direction, placée sous l'autorité de Son Excellence Monsieur le Ministre d'État, l'Agence Monégasque de Sécurité Numérique est l'autorité nationale chargée de la cyber défense de la Principauté. Acteur majeur dans l'accompagnement du développement du numérique, l'AMSN apporte son expertise et son assistance technique aux services de l'État et aux entreprises avec une mission renforcée au profit des opérateurs d'importance vitale (OIV). Elle assure un service de veille, de détection, d'alerte et de réaction aux attaques informatiques.

1 QUEL RÔLE AUPRÈS DES AUTORITÉS ET DES ADMINISTRATIONS ?

En collaboration avec les services et directions compétents et en particulier avec ceux du Délégué Interministériel pour la Transition Numérique (DITN), l'AMSN instruit et prépare les décisions relatives à la sécurité du numérique et à celles concernant des données sensibles. Elle établit le corpus juridique et réglementaire encadrant les activités de sécurité numérique, contribuant à la confiance dans le numérique. Elle participe à la construction et à la maintenance des réseaux et des systèmes d'information. L'agence accompagne ainsi le Palais Princier, la Direction des Services Judiciaires, le Conseil National, la Mairie, ainsi que tous les services exécutifs de l'État et les établissements publics dans la sécurisation de leurs systèmes d'information.

2 QUELLE MISSION AUPRÈS DES OPÉRATEURS D'IMPORTANCE VITALE ?

L'AMSN accompagne les opérateurs d'importance vitale dans la sécurisation de leurs systèmes d'information critiques, rendue obligatoire par la loi n°1.435 du 08 novembre 2016 relative à la lutte contre la criminalité technologique. Cette sécurisation passe par l'application de 21 règles de sécurité (dont la mise en place de dispositifs de détection d'attaques) définies avec les OIV et annexées à l'Arrêté Ministériel 2018-1053 du 8 novembre 2018.

3 QUELLE MISSION AUPRÈS DES ENTREPRISES ET DES CITOYENS ?

L'AMSN est un promoteur, par la sensibilisation, d'une culture de cybersécurité auprès des entreprises de toutes tailles ainsi que des particuliers, les uns et les autres étant insuffisamment au fait de ces problèmes. Elle promeut et soutient toute initiative permettant d'améliorer la sécurité de tous, comme par exemple la mise en place gratuite, pour tous les clients de Monaco Telecom titulaires d'un contrat internet, d'un antivirus pour smartphone et ordinateur personnel, la présence aux « Assises de la Sécurité » d'un village regroupant, autour de l'AMSN, sous le nom de « Monaco Cyber Initiative », 10 entreprises des secteurs informatique, assurance, télécommunications, sécurité des systèmes d'information et conformité.

4 QUELLES RELATIONS AVEC LES AUTRES ACTEURS DE LA SÉCURITÉ NUMÉRIQUE ?

Parce qu'une agence ne peut, à elle seule, répondre à tous les besoins en matière de sécurité numérique, l'AMSN se donne les moyens de contribuer au développement d'un écosystème fiable. Pour ce faire, elle s'appuie sur ses propres savoir-faire, sur des coopérations avec des partenaires de confiance par la qualification d'entreprises monégasques et françaises dans le domaine de la sécurité numérique.

5 QUELLE PLACE DANS LE CONTEXTE INTERNATIONAL ?

Le cyber espace n'a pas de frontières. L'agence est membre du TF-CSIRT regroupant 383 centres d'expertise et de réponse à incidents privés et publics européens, ainsi que du FIRST regroupant, quant à lui, 450 structures de même nature dans le monde. Elle est membre de droit de la réunion annuelle des CERT gouvernementaux (NatCSIRT), permettant des échanges d'information, améliorant la prévention et le traitement des attaques. Par ailleurs, elle a établi des relations privilégiées avec l'Agence Nationale de la Sécurité des Systèmes d'Information française.

6 ET EN CAS D'ATTAQUE ?

En cas d'attaque avérée ou soupçonnée, le centre d'expertise et de réponse aux incidents de sécurité de l'agence (CERT-MC) assure la protection des services de l'État et des opérateurs privés les plus sensibles. Pour mener à bien sa mission, le CERT-MC met en œuvre des dispositifs de veille, de détection, d'analyse et de réponse aux incidents de sécurité qualifiés.

Les chiffres de l'année

UNE AGENCE 120m2
8 PERSONNES

OPÉRATIONS DE CYBERDÉFENSE

30

incidents qualifiés

2

incidents critiques ayant nécessité 1500 heures de réponse à incident, soit 9 mois et demi équivalent temps plein pour un analyste CERT

244

« Actualités cyber » diffusées

50

« Essentiels de la cyber » diffusés aux autorités ou responsables d'entreprise

8

audits de sécurité

612

avis de sécurité et 13 alertes de sécurité diffusées

50

millions de fichiers reconstitués ayant permis la détection de 830 malwares et 580 **fichiers considérés** comme suspects, dont plusieurs se sont révélés par la suite être des virus très récents, non détectés par les anti-virus

60

matériels (serveurs, postes, autres) installés

8

assistances à la conception de système d'information ou à l'homologation

2,6

milliards d'événements analysés par les outils de détection de l'AMSN

DOCUMENTATIONS

Rédaction de **12** Arrêtés Ministériels avec le support de la Délégation Interministérielle chargée de la Transition Numérique

SENSIBILISATIONS - FORMATIONS

Plus de **50** entretiens formels avec les autorités, directeurs ou chefs de service de l'État, et responsables d'OIv

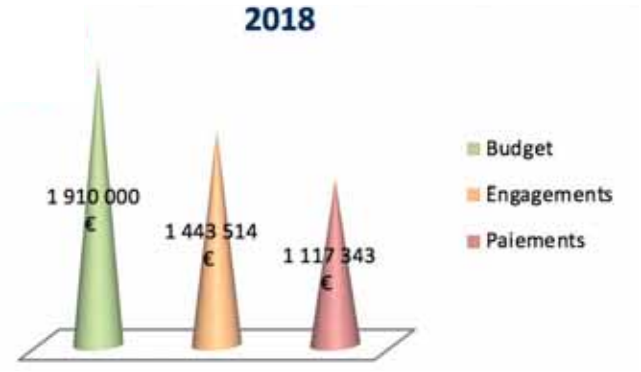
Plus de **30** opérations de sensibilisation

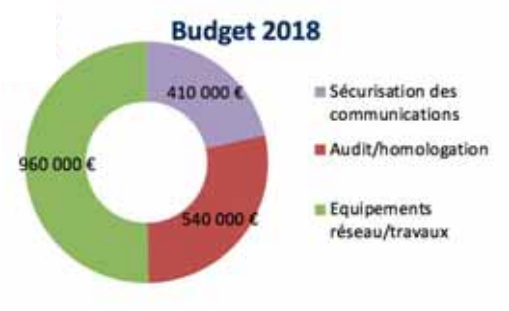
3 formations reçues

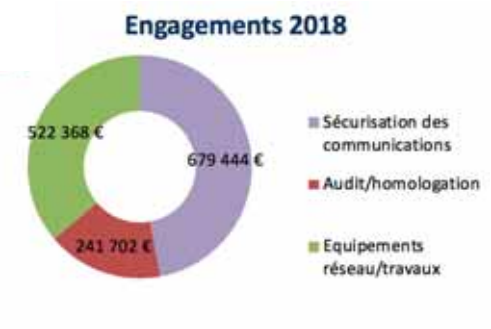
Participation à **5** forums de cybersécurité

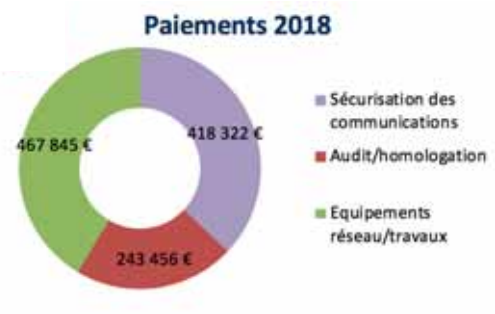
FINANCEMENT

La loi n° 1.460 du 22 décembre 2017 portant fixation du budget général primitif de l'exercice 2018, adoptée par le Conseil National dans sa séance du 21 décembre 2017, prévoit les crédits pour la sécurité numérique à l'article 708.946. Cet article regroupe les besoins de tous les services de l'État en matière de sécurité numérique ; sur les 2,8M€ alloués à cet article, 1,9M€ l'étaient pour l'AMSN.









Le « non engagé » est principalement dû :

- Aux délais administratifs de la République française, pour l'achat de certains types de matériels permettant la sécurisation des communications, beaucoup plus longs que prévu, décalant d'autant le démarrage du projet ;

- A l'engagement des personnels de l'AMSN pendant plusieurs mois dans le traitement d'un incident de sécurité majeur, les rendant ainsi indisponibles pour la réalisation de projets ;

- Aux retards dans la réalisation de travaux de mise en conformité de certains locaux.

AUTRES

3600 capsules de café

18 kg de bonbons et gâteaux

400 cannelés

10 kg de chocolat

Rappel sur les missions de l'AMSN

L'Agence Monégasque de Sécurité Numérique, créée par l'Ordonnance Souveraine n°5.664 du 23 décembre 2015, modifiée, est l'autorité nationale en charge de la sécurité des systèmes d'information. Elle est désormais directement placée sous l'autorité de S.E.M. le Ministre d'État. Elle constitue un centre d'expertise, de réponse et de traitement en matière de sécurité et d'attaques numériques et a, à ce titre, en particulier pour missions :

- de prévenir, détecter et traiter les cyberattaques, notamment par l'élaboration de plans, de procédures, de dispositifs de protection et de précaution et, plus généralement, de toutes mesures à proposer au titre de la sécurité numérique ;
- de réagir en situation de crise lors des cyberattaques et de coordonner les actions de réaction ;
- de représenter la Principauté dans les instances internationales de sécurité numérique et auprès des autres centres d'expertise, de réponse et de traitement en matière d'attaques informatiques ;
- de sensibiliser les services publics et les opérateurs d'importance vitale (O.I.V.) aux exigences de la sécurité numérique ;
- de contrôler le niveau de sécurité des O.I.V. ;
- de contrôler les prestataires de services de confiance, afin de s'assurer, à tout moment, que lesdits prestataires et les services qu'ils fournissent satisfont aux exigences fixées par Arrêté Ministériel ;
- de mettre en place, actualiser et publier la liste des prestataires de services de confiance qualifiés ainsi que les informations relatives aux services qu'ils fournissent, dénommée « liste de confiance » ;
- d'évaluer et certifier la sécurité des produits et systèmes des technologies de l'information ;
- de qualifier les prestataires de services de confiance (PSCO) et les services de confiance, les prestataires d'audit de la sécurité des systèmes d'information (PASSI), les prestataires de réponse aux incidents (PRIS), les prestataires de détection d'incidents de sécurité (PDIS) et les prestataires d'informatique en nuage et d'hébergement (PINH) ;
- d'élaborer les fonctions de sécurité prévues au titre IV de l'Ordonnance Souveraine n° 3.413 du 29 août 2011, modifiée, portant diverses mesures relatives à la relation entre l'Administration et l'administré ;
- De mettre en place une infrastructure de gestion de clés pour les services numériques.

STRATÉGIE

La Stratégie pour la Sécurité du Numérique

1 Le Comité stratégique de la sécurité numérique

Le Comité stratégique de la sécurité numérique, institué par l'Ordonnance Souveraine n°6.486 du 25 juillet 2017, a pour rôle :

- de valider et de suivre les plans d'action découlant de la stratégie nationale pour la sécurité du numérique ;
- d'identifier les technologies-clés pour le développement d'un environnement numérique de confiance ;
- d'évaluer les besoins en formation initiale et continue ;
- de suivre les travaux de recherche et d'en accompagner leurs valorisations ;
- d'analyser la veille technologique et économique permettant d'anticiper les évolutions des questions liées au numérique.

Le Comité s'est réuni 2 fois en 2018. Parmi les sujets entérinés, les principaux sont :

- La charte à destination des administrateurs des réseaux et systèmes d'information de l'État afin de les informer et de les sensibiliser à leurs obligations, publiée par l'Arrêté Ministériel n° 2018-281 du 04 avril 2018 ;
- Les séances de sensibilisation des agents de l'État à la sécurité des systèmes d'information ;
- L'adhésion de l'AMSN au « Forum of Incident Response and Security Teams » (FIRST[1]) ;
- Les modalités[2] de la mise à disposition aux clients de Monaco Telecom d'un antivirus pour leurs ordinateurs et leurs smartphones ;
- La mise en place d'une Infrastructure de Gestion de Clés souveraine par l'AMSN pour générer des certificats électroniques donnant valeur probante aux services électroniques[3], notamment dans la relation entre l'Administration et l'administré, et à tout autre service électronique de confiance ;
- L'adhésion de l'AMSN au TF-CSIRT.

2 Les rÉalisations sur les 5 objectifs de la StratÉgie

Protéger les intérêts fondamentaux, la défense et la sécurité des systèmes d'information des institutions officielles de la Principauté et des infrastructures critiques, ainsi que la gestion des crises informatiques majeures :

- Mise en œuvre opérationnelle des systèmes de détection pour le Palais, les services exécutifs de l'État, le Conseil National et la Justice ;
- Définition des obligations pour les Opérateurs d'Importance Vitale (OIV) avec les intéressés, publication de l'Arrêté Ministériel fixant celles-ci ;
- Traitement de plusieurs attaques sur des systèmes d'information de l'État et des OIV ;
- Diffusion des alertes et vulnérabilités.

[1] Le FIRST est une société à but non lucratif qui compte plus de 450 membres répartis sur 85 pays, parmi lesquels des opérateurs publics et privés.
[2] 5 licences seront gratuitement mises à disposition des clients de Monaco Télécom ; extension gratuite à 10 en cas de besoin.
[3] Les services électroniques comprennent : la signature, le cachet électronique pour une entité, l'authentification, le chiffrement, l'identité.

Développer la confiance dans le numérique, le respect de la vie privée numérique, la protection des données personnelles et l'appréhension de la cyber malveillance :

- 8 systèmes d'information de l'État ont fait l'objet d'une démarche d'homologation (réalisées ou démarrées en 2018) afin de s'assurer de leur sécurisation ;
- 8 audits ont été effectués, soit par l'AMSN soit par un PASSI, afin de vérifier le niveau de sécurité appliqué aux systèmes d'information ;
- L'enjeu du développement des échanges numériques avec l'Union Européenne a conduit l'AMSN à terminer la mise en place du cadre réglementaire compatible avec le règlement européen « eIDAS » n°910/2014 du 23 juillet 2014, sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur ;
- Le lancement de l'étude et de la réalisation d'une infrastructure de gestion de clés pour permettre la délivrance de certificats qualifiés pour les services de signature électronique, de cachet électronique pour les entités de l'État ou les entreprises monégasques, d'authentification électronique ou de chiffrement.

Développer les sensibilisations et les formations initiales et continues :

- De nombreuses séances de sensibilisation et interventions lors de colloques ou forums ont été effectuées pour continuer de sensibiliser tous les acteurs de ce domaine et les entreprises monégasques ;
- Plus de 500 personnes de l'État ont assisté aux séances de sensibilisation à la cybersécurité ; l'objectif étant que pour mi 2019 la totalité des agents de l'État aient assisté à ces conférences ;
- Le personnel de l'AMSN et de la DITN a participé à 4 formations spécialisées de 2 à 5 jours dispensées par l'ANSSI. Ces formations, s'inscrivant dans un cursus complet, se poursuivront en 2019.

Faire de la sécurité du numérique un facteur de compétitivité :

- Pour la première année, 10 entreprises monégasques ont pu participer aux « Assises de la Sécurité » autour de l'AMSN sous l'enseigne de « Monaco Cyber Initiative ». Cette participation a permis de faire connaître les entreprises monégasques spécialisées dans la cybersécurité à la fois aux acteurs de la Principauté mais également aux sociétés internationales présentes permettant de créer des liens et des contacts entre ces différents acteurs ;
- Participation aux Assises de la Sécurité, au Forum International de la Cybersécurité, au forum de recrutement dédié à la cybersécurité qui a contribué à faire connaître l'intérêt de la Principauté pour les métiers de la cybersécurité ;
- A noter l'ouverture à Monaco de plusieurs filiales d'entreprises d'origine française avec pour objectif de devenir des prestataires d'audit (PASSI) et des acteurs reconnus dans ce domaine.

S'ouvrir à l'international par l'établissement de liens internationaux en matière de sécurité numérique, la contribution de la Principauté à la stabilité du cyber espace :

- Adhésion à différentes organisations internationales permettant des échanges d'information sur les attaques et les vulnérabilités des systèmes d'information.


3

Un environnement de confiance

1 Accompagner

L'année 2018 marque un tournant du numérique par la décision du Gouvernement d'accélérer la transition numérique pour servir les enjeux stratégiques, économiques et sociaux de la Principauté. Le repositionnement de l'Agence Monégasque de Sécurité Numérique directement sous les ordres de S.E.M. le Ministre d'État permet de favoriser l'instauration d'un environnement de confiance et de sécurité propice à cette transition et de faire prendre rapidement les décisions d'arbitrage entre le besoin de sécurité et de souveraineté et le service offert. La concertation et l'implication de tous les acteurs, privés et publics, contribuent à faire du numérique sécurisé un sujet clé de la politique du Gouvernement.

2 UN CADRE RÉGLEMENTAIRE ÉVOLUTIF AU SERVICE DE LA TRANSITION NUMÉRIQUE

De nouvelles technologies, de nouveaux usages, apparaissent en permanence. Ils s'accompagnent de plus en plus de menaces discrètes et sournoises. La sécurité numérique doit donc accompagner ce changement sans jamais s'y opposer mais en veillant toujours à apporter toute la confiance et donc la sécurité, nécessaires.

Le cadre réglementaire de la Principauté doit donc permettre ces évolutions en toute sécurité, assurer le suivi et l'anticipation de ces changements en offrant aux différents acteurs, publics comme privés, un environnement sécurisé.

En tant qu'autorité nationale, l'AMSN a terminé en 2018, avec les derniers arrêtés ministériels du RGS, la mise en place de l'ensemble des textes législatifs et réglementaires en matière de sécurité des systèmes d'information qui garantissent la protection de la souveraineté nationale et favorisent l'attractivité de la Principauté.

L'AMSN participe à l'encadrement des bonnes pratiques en matière de sécurité des systèmes d'information, à l'élaboration de référentiels normatifs en matière de sécurité numérique, à l'intégration des normes juridiques et techniques ainsi qu'à la mise à jour des textes réglementaires. En outre, l'agence assiste les services de l'État et les OIV dans l'élaboration et la mise en œuvre des mesures ou dispositifs issus des textes, en particulier la démarche d'homologation. Cette démarche a permis aux autorités de mesurer les risques pris par la numérisation des processus et ainsi de faire mettre en place les moyens nécessaires pour en diminuer la vraisemblance et/ou la gravité. Le gouvernement a ainsi conduit, avec l'appui et les conseils de l'AMSN, l'homologation de 8 systèmes d'information particulièrement sensibles.

Pour mémoire, l'homologation consiste à évaluer les risques et, in fine, à faire assumer la responsabilité des risques résiduels à l'autorité ayant la charge du système d'information homologué.

3 L'ACTIVITÉ DE L'AGENCE DANS LE DOMAINE RÉGLEMENTAIRE

- Ordonnance Souveraine n° 6.762 du 25 janvier 2018 rendant exécutoire l'Accord entre la République française et la Principauté de Monaco relatif à l'échange et à la promotion réciproque des informations classifiées, signé à Paris le 13 juillet 2017.
  Elle définit le règlement commun de sécurité applicable à tout échange d'informations classifiées entre les Parties ou tous autres organismes publics ou privés régis par leurs lois et règlements nationaux.
  Elle peut éventuellement servir, après accord entre les Parties, à couvrir l'échange et la protection d'informations classifiées issues d'organisations internationales échangées entre les Parties. Une assurance de sécurité sera alors mise en place entre les Parties dans le cadre des échanges envisagés.

- Arrêté Ministériel n° 2018-65 du 30 janvier 2018 portant application de l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Il décrit les règles permettant aux organismes d'évaluation de la conformité de vérifier que les prestataires de services de confiance remplissent les exigences fixées par le Référentiel Général de Sécurité (RGS) et d'élaborer des rapports d'évaluation de la conformité recevables par l'AMSN, organe de contrôle.

- Arrêté Ministériel n° 2018-66 du 30 janvier 2018 portant application de l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Il décrit, dans le respect des règles posées par le Référentiel Général de Sécurité, les exigences générales relatives à la qualification de l'ensemble des prestataires de services de confiance, indépendamment de la nature des services de confiance qualifiés qu'ils fournissent.

- Arrêté Ministériel n° 2018-67 du 30 janvier 2018 portant application de l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Il décrit, dans le respect des règles posées par le Référentiel Général de Sécurité, les exigences relatives à la qualification de l'ensemble des services d'horodatage électronique.

- Arrêté Ministériel n° 2018-68 du 30 janvier 2018 portant application de l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.

Il décrit, dans le respect des règles posées par le Référentiel Général de Sécurité, les critères d'évaluation de la conformité des services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet.

- Arrêté Ministériel n° 2018-69 du 30 janvier 2018 portant application de l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Il décrit, dans le respect des règles posées par le Référentiel Général de Sécurité, les exigences générales relatives aux critères d'évaluation de la conformité des services de validation qualifiés des signatures électroniques qualifiées et des cachets électroniques qualifiés.

- Arrêté Ministériel n° 2018-70 du 30 janvier 2018 portant application de l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Il décrit, dans le respect des règles posées par le Référentiel Général de Sécurité, les exigences générales relatives aux critères d'évaluation de la conformité des services de conservation qualifiés des signatures et des cachets électroniques qualifiés.

- Arrêté Ministériel n° 2018-281 du 4 avril 2018 portant application de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Il a pour objet, par l'intermédiaire de la Charte en annexe, de formaliser les règles spécifiques de déontologie et de sécurité applicables d'une part, aux fonctionnaires et agents non titulaires de l'État et d'autre part, aux tiers appelés à réaliser des missions pour le compte de l'Administration, lorsqu'ils exercent, au sens de la présente Charte, des fonctions « d'Administrateur réseaux et systèmes d'information ». Cette Charte complète la Charte des systèmes d'information de l'État et s'inscrit dans la logique de la Politique de Sécurité des Systèmes d'Information de l'État.

- Arrêté Ministériel n° 2018-634 du 2 juillet 2018 portant application de l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Il a pour objet la liste de confiance, visée au paragraphe 26 du Référentiel Général de Sécurité, annexé à l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017, susvisé. Cette dernière comporte outre les informations sur les prestataires de service de confiance qualifiés et les services qu'ils fournissent, des spécifications techniques ainsi que les formats de la liste.

- Arrêté Ministériel n° 2018-635 du 2 juillet 2018 portant application de l'arrête ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.

Sont définies dans l'annexe du présent arrêté, les règles et recommandations concernant le choix et le dimensionnement de l'ensemble des mécanismes cryptographiques, énoncées au paragraphe 8 du Référentiel Général de Sécurité, annexé à l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017.

- Arrêté Ministériel n° 2018-636 du 2 juillet 2018 portant application de l'arrête ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Sont définies dans l'annexe du présent arrêté, les règles et recommandations concernant les mécanismes d'authentification, énoncées au chiffre 1 du paragraphe 8 du Référentiel Général de Sécurité, annexé à l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017.

- Arrêté Ministériel n° 2018-637 du 2 juillet 2018 portant application de l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017 portant application de l'article 54 de l'Ordonnance Souveraine n° 3.413 du 29 août 2011 portant diverses mesures relatives à la relation entre l'Administration et l'administré, modifiée.
  Sont définies dans l'annexe du présent arrêté, les règles et recommandations concernant la gestion des clés cryptographiques utilisées dans l'ensemble des mécanismes cryptographiques, énoncées au paragraphe 8 du Référentiel Général de Sécurité, annexé à l'Arrêté Ministériel n° 2017-835 du 29 novembre 2017.

- Arrêté Ministériel n° 2018-1108 du 26 novembre 2018 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.
  Il définit le référentiel pour qualifier les Prestataires d'Informatique en Nuage et d'Hébergement (PINH) et a pour but de traiter le problème de la sécurité de manière globale pour les services de type IaaS, PaaS, SaaS, ainsi que pour les services d'hébergement. Les usagers peuvent ainsi fonder leur confiance envers leurs prestataires sur cette qualification.

- Arrêté Ministériel n° 2018-1053 du 8 novembre 2018 portant application de l'article 27 de la loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique.
  Il définit les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale.

SENSIBILISATION

Implication des décideurs et responsables dans la sécurité numérique

La sécurité des systèmes d'information est aujourd'hui un vrai sujet en Principauté. Les attaques traitées montrent que la Principauté est une cible comme les autres pays.

L'évolution de la maturité mesurée par l'ONU montre l'implication des autorités et des responsables de la Principauté dans ce domaine.

En 2018, l'action de sensibilisation et de promotion des bonnes pratiques de l'agence vers les autorités, les services de l'État, les opérateurs d'importance vitale, les responsables informatiques d'entreprises s'est traduite par plus d'une trentaine de communications, conférences, dialogues, à chaque fois avec une adaptation au cas par cas.

Dans le cadre de la loi n°1.435 du 08 novembre 2016, les liens directs, établis en 2017 avec les opérateurs d'importance vitale ont permis d'expliquer les risques cyber et la finalité de la loi. Le travail accompli avec les OIV a permis de concrétiser l'Arrêté Ministériel 2018-1053 fixant les règles de sécurité à appliquer par ces derniers. Le calendrier de déploiement de ces mesures a été arrêté pour trois secteurs d'activité d'importance vitale (Banque Finance, Communication électronique, Energie) et est en cours de finalisation avec les autres, pour tenir compte de leur capacité d'investissement, de la disponibilité de leur ressources humaines, ainsi que de leur niveau de maturité.

Le volume des sollicitations reçues de la part des OIV indique une très forte volonté d'avancer dans la protection des systèmes d'information.

L'année 2019 devrait voir la finalisation de ce travail de prescription et le début de la mise en œuvre par les OIV des mesures les plus urgentes avec l'aide de l'AMSN qui proposera alors un service de détection des attaques aux OIV voire de « Security Operational Center » (SOC) pour les plus petits d'entre eux.

Par ailleurs, dans le cadre de la transition numérique de la Principauté, l'AMSN a apporté son concours à de nombreux entretiens avec différentes entreprises, contribuant ainsi à mieux définir les besoins numériques en appliquant le juste niveau de sécurité.

Sécurisation des systèmes d'information

1 SÉCURISER LES COMMUNICATIONS TÉLÉPHONIQUES DES AUTORITÉS

Afin de sécuriser les communications téléphoniques les plus sensibles au sein de l'État, les services informatiques ont terminé le déploiement d'un système de communications chiffrées permettant d'assurer la sécurité des communications de la voix et des données, mais également la sécurité du terminal et des informations stockées sur celui-ci.

Par ailleurs, l'évaluation d'une application de messagerie instantanée sécurisée pour smartphone, qualifiée par l'Agence Nationale de la Sécurité des Systèmes d'Information, a débuté ; cent licences ont été acquises. Cette application permet d'avoir des conversations téléphoniques via internet, d'échanger des messages et des documents, et de créer des groupes d'échange de messages.

2 LE SECRET DE SÉCURITÉ NATIONALE

Les études pour la mise en place, au sein des services de l'État, d'un réseau permettant le traitement des informations classifiées sont désormais terminées. Ce réseau sera testé au premier trimestre 2019 et entrera en service en 2019 dès que les locaux devant recevoir les équipements seront mis en conformité.

Toujours dans ce domaine, l'AMSN a assisté cinq services de l'État pour la sécurisation de leurs systèmes d'information et financé une partie des travaux de mise en conformité de leurs locaux ; ce qui représente plus d'une centaine de réunions.

3 La politique de sÉcuritÉ des systèmes d'information de l'ÉTAT (PSSI-E)

Dans le cadre de la PSSI-E, publiée par Arrêté Ministériel, un suivi est effectué annuellement.

Pour mémoire, cette politique a pour objectif d'améliorer la protection des informations détenues dans les systèmes d'information.

Celle-ci prévoit 161 mesures classées en plusieurs priorités. Tous les services exécutifs de l'État et les établissements publics doivent adresser un rapport annuel de progression à l'AMSN, qui adresse ensuite une synthèse à S.E.M. le Ministre d'État.

Même si la progression peut paraître parfois un peu lente, elle est indéniable et les efforts consentis commencent à porter leurs fruits à la fois techniquement mais également dans la prise de conscience des responsables.

4 SOUTIEN ET CONSEILS DANS LA CONCEPTION DES SYSTèMES D'INFORMATION

L'AMSN a continué à apporter son soutien dans la conception des architectures des systèmes d'information de l'État mais également des OIV.

Cette contribution permet de prendre en compte, dès le début des projets, la sécurité des systèmes d'information (confidentialité, disponibilité, intégrité).

Dans le cadre de la transition numérique de la Principauté, l'AMSN a apporté son concours à de nombreux entretiens avec différents éditeurs de logiciel et fournisseurs de solution, contribuant ainsi à mieux définir les besoins numériques en appliquant le niveau nécessaire de sécurité.

La nécessité d'utiliser des matériels de confiance dont la sécurité et le fonctionnement ont été vérifiés par des laboratoires indépendants, reste d'actualité et commence à être effective dans les nouveaux systèmes.

L'AMSN, en tant que membre de droit de toute commission d'homologation, a participé à de nombreuses réunions pour l'étude et l'homologation des systèmes d'information des différents services exécutifs de l'État. Ainsi, quatre systèmes ont pu être homologués et plusieurs sont en cours d'homologation.

5 PRESTATAIRES QUALIFÉS

Alors qu'en 2017, le référentiel pour les « Prestataires d'Audit de la Sécurité des Systèmes d'Information » (PASSI) était publié, l'année 2018 a vu Monaco Informatique Service (MIS), première société monégasque, obtenir cette qualification. L'AMSN a fait passer en 2018 des examens écrits aux personnels de deux sociétés françaises qui ont créé ou étendu leur activité en Principauté afin de réaliser des prestations d'audit de sécurité des systèmes d'information.

Remise de la qualification par Dominique RIBAN, Directeur de l'AMSN, à Antony BOIRA Directeur de MIS (mai 2018).

Le référentiel pour les « Prestataires d'Informatique en Nuage et d'Hébergement » (PINH) annexé à l'Arrêté Ministériel n°2018-1108 du 26 novembre 2018 a été publié au Journal de Monaco le 7 décembre 2018.

Ce référentiel apporte aux commanditaires d'une prestation d'hébergement informatique ou de solution « Cloud », des garanties quant aux compétences du prestataire et de son personnel, à la qualité de sa prestation, à la confiance qu'il peut accorder au prestataire et au niveau de sécurité apporté à la prestation.

Ce référentiel prévoit deux niveaux de sécurité : un niveau essentiel qui peut concerner des prestataires dans et en dehors de la Principauté et un niveau avancé qui oblige le prestataire à assurer le service en Principauté et à partir de la Principauté.

RÉALISATIONS

L'activité opérationnelle

1 veille et publication

L'AMSN, avec le concours entre autres du CERT-FR, assure une veille des informations issues de la presse spécialisée, des éditeurs de logiciels, des constructeurs de matériel informatique, des laboratoires de recherche spécialisés en sécurité numérique afin de pouvoir sensibiliser l'ensemble des acteurs de la Principauté, et réagir rapidement à toutes menaces qui pourraient concerner les systèmes d'information de l'État et des opérateurs d'importance vitale.
Ainsi, l'AMSN a diffusé :

- 244 « actualités » sur le cyber espace, afin de sensibiliser et informer les acteurs spécialisés de la Principauté ;

- 50 synthèses « Les essentiels de la cyber » adressées à différentes autorités. Ce document résume, sans élément technique, les faits les plus marquants. Ainsi les autorités et les hauts responsables peuvent être sensibilisés aux grands évènements mondiaux dans le domaine de la cybersécurité ;

- 13 alertes de sécurité sous forme de documents destinés à prévenir d'un danger immédiat ;

- 612 avis de sécurité sous forme de documents faisant état de vulnérabilités et des moyens de s'en prémunir, vers les OIV ou les services de l'État afin d'éviter la compromission de leurs systèmes d'information.

2 CERT-MC

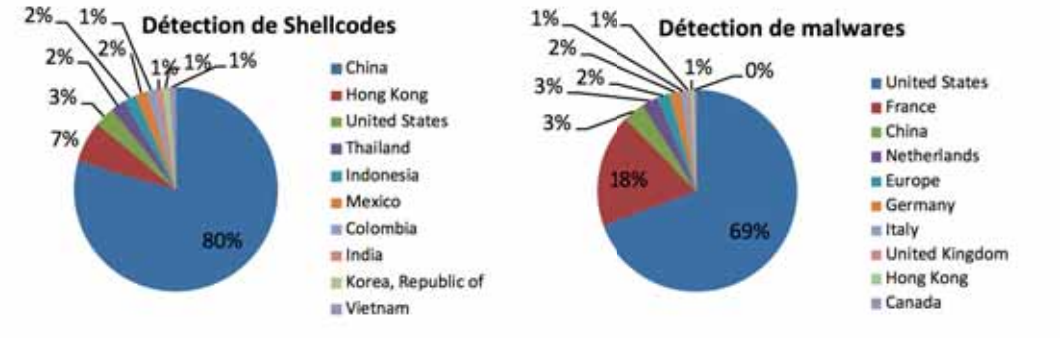
✔ Le CERT-MC dispose de moyens matériels et logiciels qui lui permettent d'effectuer la détection d'attaques sur les systèmes d'information de l'État. Ces dispositifs, mis en service en novembre 2017, sont maintenant totalement opérationnels et permettent d'assurer la collecte d'informations techniques dans les flux informatiques, de réaliser en temps réel leurs analyses et de qualifier s'il s'agit d'incident de sécurité ou non.

Deux grandes catégories d'attaques peuvent être détectées par ces systèmes :

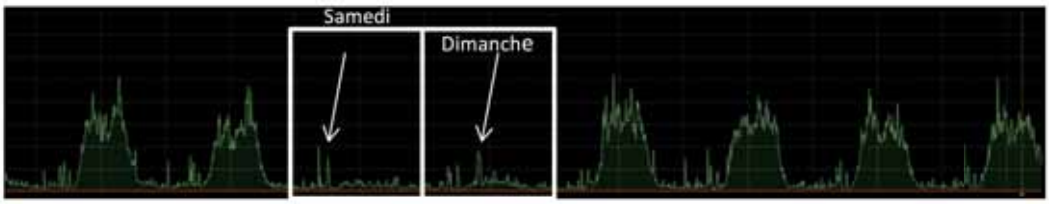
- Les « shellcodes » : codes informatiques malveillants qui détournent un programme de son exécution normale ;

- Les « malwares » : programmes développés dans le but de nuire à un système informatique.

Les graphiques ci-dessous illustrent l'origine géographique des attaques de type shellcode et de type malware en 2018.



Les systèmes de détection d'attaques permettent aussi d'alerter sur des sorties anormales de données. Le diagramme, ci-dessous, montre la mesure du trafic sortant faite en fonction des heures de la journée et des jours de la semaine. Ainsi une quantité de données anormalement grande par rapport au trafic habituel, pendant les jours non ouvrés ou en pleine nuit, peut signifier une exfiltration de données suite à une attaque.



Aujourd'hui, la totalité des systèmes d'information de l'État bénéficient de ces systèmes de détection. Ce service sera également proposé à certains OIV de la Principauté en 2019.
Par ailleurs, un système de gestion de tickets permet d'assurer un suivi précis de toutes les actions effectuées et de réaliser un retour d'expérience sur chaque cas, dans une démarche d'amélioration continue.

✔ Le CERT-MC a déployé la plateforme MISP[4] avec le support du CERT-AG[5] et du CIRCL[6] dans le cadre de relations établies au FIRST[7]. MISP est plateforme de renseignements sur les menaces, permettant le stockage et la corrélation d'indicateurs de compromission d'attaques ciblées, l'échange d'informations sur les menaces et sur les vulnérabilités ou même d'informations sur la lutte contre le terrorisme. MISP est déployé aujourd'hui dans plusieurs organisations, non seulement pour stocker, partager, collaborer sur les indicateurs de cybersécurité et l'analyse des logiciels malveillants, mais également pour utiliser les indicateurs de compromission et les informations afin de détecter et prévenir les attaques ou les menaces contre des infrastructures informatiques, des organisations ou des personnes.

[4]Malware Information Sharing Platform
[5]CERT Crédit Agricole
[6]Computer Incident Response Center Luxembourg
[7]Voir section coopération internationale.

La plateforme MISP mise en place a renseigné, tout au long de l'année 2018, le CERT-MC sur les menaces en cours. Par ce biais, le CERT-MC a reçu des CERTs étrangers 2322 communiqués de sécurité, et 228 000 indicateurs de compromission.

https://www.misp-project.org

✔ Depuis janvier 2018, le CERT-MC a qualifié et traité de nombreuses alertes, au travers des détections qu'il a effectuées et des signalements qui lui ont été faits. Parmi ces alertes, 30 se sont révélées être de vrais incidents, nécessitant plusieurs dizaines de jours/hommes de travail avec les différentes équipes concernées, pour rétablir la situation et éviter qu'elle ne dégénère en catastrophe.

Parmi les incidents traités par le CERT-MC, deux ont plus particulièrement été marquants :

- Le premier a nécessité plus de 4 mois de travail, l'analyse de centaines de milliers de fichiers sur une quarantaine de machines, plus de 80 heures de développement pour permettre la mise au point d'un logiciel de nettoyage spécifique du système d'information touché. Mais surtout, ce traitement de l'attaque a permis de constater que l'attaque initiale remontait à 2014 sans qu'aucune anomalie n'ait été constatée précédemment ;

- Le second a nécessité de nombreux jours de travail étalés sur l'année. Etant donné le niveau d'expertise des attaquants, la compréhension de l'attaque et de son ampleur, l'analyse de plusieurs millions de fichiers, 480 heures de développement, ainsi que 52 réunions de suivi ont été nécessaires.

3 Les audits

L'AMSN a effectué ou a fait réaliser 8 audits, soit dans le cadre des interventions de remédiation d'incidents de sécurité, soit dans le cadre de la prévention ou de démarches d'homologation. Tous ces audits ont été suivis de recommandations afin d'améliorer le niveau de sécurité des systèmes d'information audités.

Les recommandations issues des audits font l'objet d'un suivi régulier afin de s'assurer qu'elles sont traitées dans un temps raisonnable et réaliste.

COOPÉRATION

7

La coopération internationale

✔ ANSSI

Sur le plan international, l'Agence Monégasque de Sécurité Numérique (AMSN) collabore étroitement avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) française.
L'accord de travail, d'octobre 2015 entre le Gouvernement de la Principauté et l'Agence Nationale de la Sécurité des Systèmes d'Information, a montré en 2018 tout l'intérêt qu'il représente pour l'agence. Une entraide est maintenant effective pour le traitement opérationnel des attaques en veillant scrupuleusement à l'anonymisation des éléments.

✔ FIRST

Le CERT-MC est depuis mai 2018 membre effectif de l'organisation FIRST (Forum of Incident Response and Security Teams). Cette adhésion a nécessité la mise en place d'une organisation et de processus de travail extrêmement précis et exigeants. L'approbation de l'adhésion a été prononcée lors de l'assemblée générale du FIRST le 28 juin 2018 à Kuala Lumpur (Malaisie).

Bruno Valentin, Chargé de Mission à l'AMSN et Frédéric Fautrier, Directeur adjoint de celle-ci, à la 30ème réunion annuelle du FIRST, 24 au 29 juin 2018.

✔ NatCSIRT

En tant que CERT national, le CERT-MC a participé à la 13ème réunion annuelle du NatCSIRT qui a eu lieu les 29 et 30 juin 2018 en marge du FIRST. Le NatCSIRT regroupe toutes les entités ayant une responsabilité nationale de réponse à incident de sécurité informatique.

✔ TF-CSIRT

Le CERT-MC a adhere, apres accord du « Comité Stratégique pour la Sécurité Numérique », au TF-CSIRT. L'adhésion doit se faire en deux temps ; l'AMSN est aujourd'hui « listée » ce qui lui permet d'être présente aux réunions sans avoir de droit de vote. La prochaine étape sera d'être « accréditée » afin d'être membre à part entière.

L'AMSN a participé à la 55ème réunion du TF-CSIRT qui a eu lieu les 27 et 28 septembre 2018 à Vilnius, Lituanie.

Le TF-CSIRT est une structure associative européenne pour les CERTs européens ; la structure légale est GÉANT qui est coordinateur des projets de réseaux cofinancés par l'UE et des organisations de réseau national de recherche et d'éducation européennes comme RENATER.
L'ensemble de ces coopérations internationales permettent :

- Des échanges d'informations techniques (avec anonymisation des éléments échangés) ;
- L'anticipation des menaces ;
- Une meilleure compréhension des attaques ;
- Une facilitation des remédiations suite à des attaques ;
- Une reconnaissance internationale.

✔ Visite du Coordinateur de l'Union européenne pour la lutte contre le terrorisme

Gilles de KERCHOVE, Coordinateur de l'Union européenne pour la lutte contre le terrorisme, a effectué une visite de travail en Principauté, les 14 et 15 juin 2018 accompagné de Elie CAVIGNEAUX, responsable de la coordination des politiques de l'Union européenne. Cette visite a permis aux plus hautes autorités monégasques de présenter l'engagement de la Principauté dans la lutte contre le terrorisme et les différentes actions menées tant au niveau national qu'international, ainsi que d'étudier les différentes pistes pour renforcer la coopération de Monaco avec les instances européennes en matière de sécurité.

Elie CAVIGNEAUX, Christophe PRAT, Gilles de KERCHOVE, Dominique RIBAN

Il s'est ainsi rendu dans les locaux de l'Agence Monégasque de Sécurité Numérique où les questions liées à la cybersécurité ont été abordées.

✔ International Telecommunication Union

L'ITU est l'agence spécialisée des Nations Unies pour les technologies de l'information et de la communication (TIC).

Le Global Cybersecurity Index (GCI) proposé par l'ITU est une référence fiable qui permet de mesurer dans la durée l'engagement des pays en faveur de la cybersécurité au niveau mondial, et de sensibiliser le public à l'importance et aux différentes dimensions de la sécurité numérique.

La cybersécurité ayant un vaste domaine d'application, qui touche de nombreuses industries et secteurs d'activité, le niveau de développement ou d'engagement de chaque pays est évalué, avant d'être agrégé dans un score global, selon cinq piliers :

- (i) mesures juridiques ;
- (ii) mesures techniques ;
- (iii) mesures organisationnelles ;
- (iv) renforcement des capacités ;
- (v) coopération.

Par ailleurs, les États membres sont classés en fonction de leur niveau d'engagement :

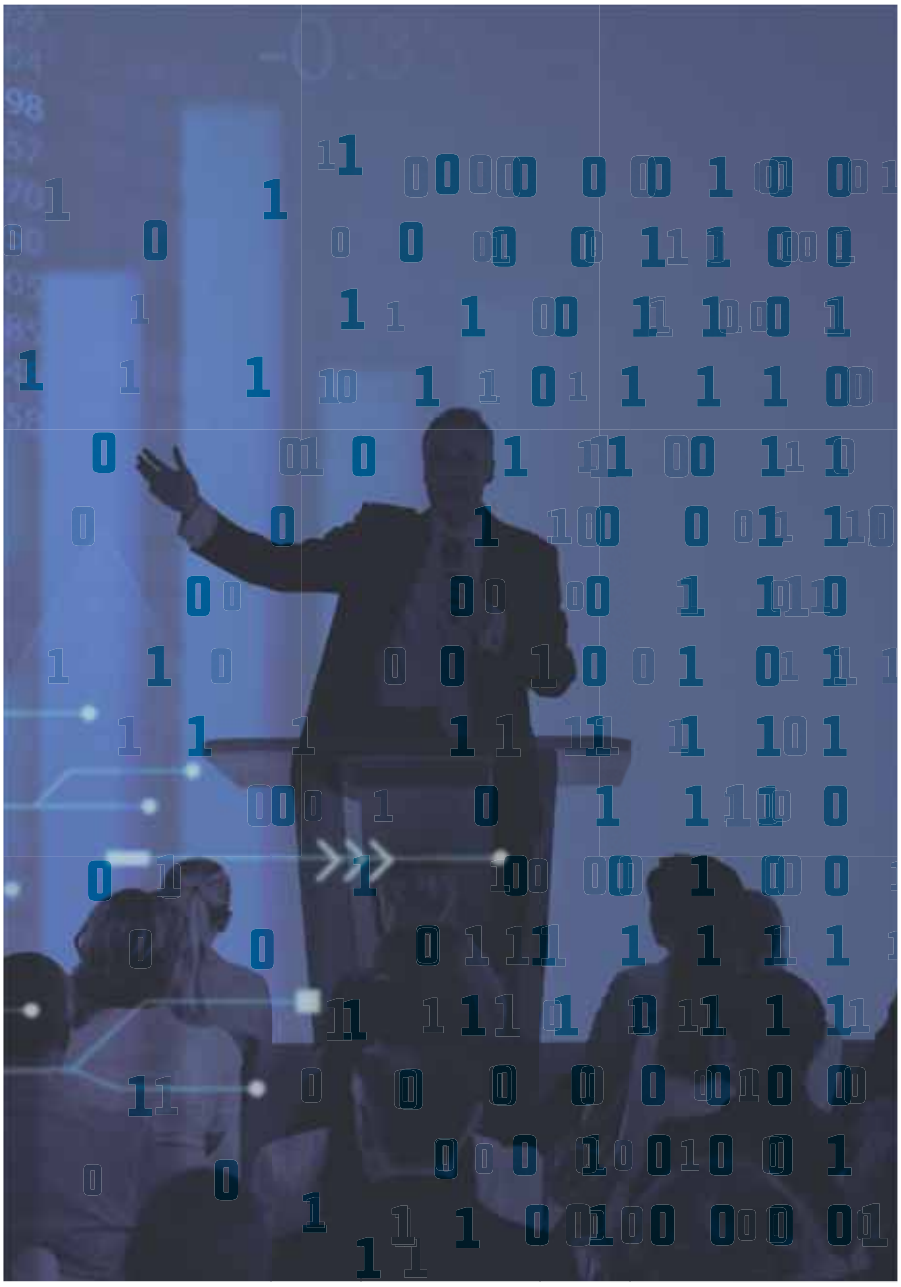
- Elevé : pays qui font preuve d'un fort engagement dans les cinq piliers de l'indice ;
- Moyen : pays ayant pris des engagements complexes et mis en œuvre des programmes et des initiatives en matière de cybersécurité ;
- Faible : pays ayant commencé à prendre des engagements en matière de cybersécurité.

L'AMSN, correspondant de l'ITU dans le domaine de la cybersécurité, a répondu en juin 2018 pour la Principauté au questionnaire GCI.

Les résultats montrent que la Principauté est un des 54 pays, sur les 175 ayant répondu, à avoir un niveau d'engagement élevé avec un score de 0.751. La Principauté se retrouve 43ème sur 175 au classement mondial et 26ème sur 43 en Europe. La France est classée 2ème pays européen et 3ème pays mondial, le Luxembourg 7ème pays européen et 11ème pays mondial.

Les points faisant partie de l'évaluation du GCI qui n'étaient pas traités en Principauté ou formalisés lors de l'évaluation sont :

- Une structure clairement identifiée pour traiter la cybercriminalité ;
- La réalisation d'exercices réguliers de cybersécurité ;
- L'adhésion à des organismes régionaux de cybersécurité ;
- L'absence d'une législation, règlementation et des moyens techniques pour lutter contre les emails non sollicités ;
- L'élargissement des campagnes de sensibilisation vers le grand public, adultes et enfants ;
- La notion de plan de continuité absente dans la Stratégie nationale pour la sécurité du numérique ;
- La formation professionnelle en cybersécurité pour la Police, la Justice, le secteur public, la société civile ;
- Les programmes éducatifs ou des programmes universitaires en cybersécurité ;
- L'investissement dans des programmes de recherche et développement liés à la cybersécurité ;
- L'absence de stratégie nationale pour la protection des enfants sur internet ;
- L'absence de structure pour traiter la problématique de la protection des enfants sur internet ;
- L'absence de mécanismes et de capacités pour la protection des enfants contre les risques sur internet.



Agence Monégasque de Sécurité Numérique

24 rue du Gabian
MC 98000 Monaco
Tél : +377 98 98 24 93
www.amsn.gouv.mc

Gouvernement Princier
PRINCIPAUTÉ DE MONACO