Agence Monégasque de Sécurité Numérique

Rapport d'Activité 2017

de l'Agence Monégasque de Sécurité Numérique

AMSN · Sécurité Numérique
PRINCIPAUTÉ DE MONACO

www.gouv.mc

RAPPORT D'ACTIVITÉ 2017

L'Agence Monégasque de Sécurité Numérique

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

Le mot du Directeur

Le 23 décembre 2015, l'Agence Monégasque de Sécurité Numérique (AMSN) voyait officiellement le jour par Ordonnance Souveraine, sous la forme d'une Direction placée sous l'autorité du Conseiller de Gouvernement- Ministre de l'Intérieur. 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). Le travail n'a réellement commencé qu'avec mon arrivée, conjointe à celle du Directeur adjoint Fréderic FAUTRIER, le 05 juillet 2016. Dix-huit mois plus tard, il apparaît évident que l'univers dans lequel évolue l'Agence a considérablement changé. Les attaques n'ont fait que s'accroître en nombre, peut-être parce que mieux détectées, en efficacité et en complexité. L'année 2017 marque d'ailleurs une évolution significative dans le monde cyber, avec la concrétisation de nouvelles menaces visant à porter atteinte à la stabilité de nos démocraties.

Je veux aussi souligner que cette période écoulée a vu une progression très notable et rapide dans la prise de conscience du risque, et ce à tous les niveaux. La sécurité numérique tend à s'imposer rapidement comme un véritable enjeu de gouvernance et de souveraineté tant dans les services de l'État que dans les entreprises. Les Monégasques, les résidents ou les pendulaires se montrent de plus en plus vigilants quant à la protection de leurs données personnelles.

Freiner la révolution digitale ? La question ne se pose pas : aujourd'hui 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. Dans ce contexte, l'autorité nationale qu'est l'AMSN, agit de toutes ses capacités, pour mettre en place le cadre réglementaire et les moyens techniques indispensables à la confiance numérique et à la protection de la souveraineté.

Pour ce faire, l'agence dispose d'atouts de poids : la confiance des plus hautes autorités, ses missions uniquement concentrées sur la protection et la défense, et, bien sûr, ses capacités opérationnelles, certes encore perfectibles mais déjà de très haut niveau technique. L'autre force tient au choix qu'a fait la Principauté d'imposer la sécurité aux acteurs critiques, tout en veillant à maintenir en permanence un dialogue de qualité et de confiance. Cela devrait se concrétiser en 2018 avec la parution des arrêtés sectoriels définissant les obligations des opérateurs d'importance vitale (OIV) en matière de sécurité des systèmes d'information.

Bien sûr, toutes ces actions et tout ce travail effectué, grâce à la qualité et la disponibilité exceptionnelles de mon équipe, n'empêcheront pas les attaques, mais une dynamique positive a été enclenchée auprès de tous les acteurs, qu'ils soient gouvernementaux ou privés, et nous avançons tous ensemble d'un pas déterminé. Avec la loi n°1.435 relative à la lutte contre la criminalité technologique, du 08 novembre 2016, nous sommes, malgré un départ tardif, en avance sur beaucoup de pays européens qui devraient s'aligner sur cette voie avec la directive (UE) 2016/1148 du parlement européen et du conseil du 6 juillet 2016, concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'union (dite directive NIS - Network and Information Security). C'est un signal positif pour la Principauté, qui confirme ainsi sa volonté et sa capacité à développer la confiance dans le cyber espace.

Ce document effectue un bilan du travail réalisé depuis juillet 2016 jusqu'à début janvier 2018 et ouvre une vue sur les travaux à venir. J'espère que ce rapport d'activité vous permettra d'avoir une meilleure connaissance de notre agence, du travail que nous accomplissons avec détermination et que cela permettra encore d'améliorer la confiance qui doit tous nous unir pour faire de la Principauté un exemple en matière de sécurité numérique.

Dominique RIBAN

Sommaire

rapport annuel AMSN

Présenter

En un coup d'œil

L'AMSN en 6 questions

Direction, sous l'autorité du Conseiller de Gouvernement-Ministre de l'Intérieur, l'Agence Monégasque de Sécurité Numérique est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique. Acteur majeur de la cyber sécurité, 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, l'AMSN instruit et prépare les décisions relatives à la sécurité du numérique et à celles concernant des données sensibles. Elle a établi un corpus juridique et réglementaire important, complet et clair, permettant d'avoir une organisation compréhensible et solide encadrant les activités cyber et contribuant largement à la confiance dans le numérique. Elle participe également à la construction et à la maintenance des réseaux et des terminaux sécurisés pour les services de l'État. L'agence accompagne ainsi le Palais Princier, la Direction des Services Judiciaires, 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.

Cette sécurisation passe entre autres par l'application de 21 règles de sécurité, définies conjointement par l'AMSN et les opérateurs, ainsi que par la mise en place de dispositifs de détection d'attaques.

3 Quelle mission auprès des entreprises et des citoyens ?

L'AMSN est un acteur de la promotion d'une culture de cyber sécurité auprès des entreprises de toutes tailles ainsi que des particuliers, les uns et les autres étant peu au fait de ces problèmes. Cela se traduit par des actions de sensibilisation et d'accompagnement ainsi que prochainement de développement d'une véritable politique relative à la formation et à l'aide aux entreprises et aux particuliers.

4 Quelles relations avec les autres acteurs de la sécurité numérique ?

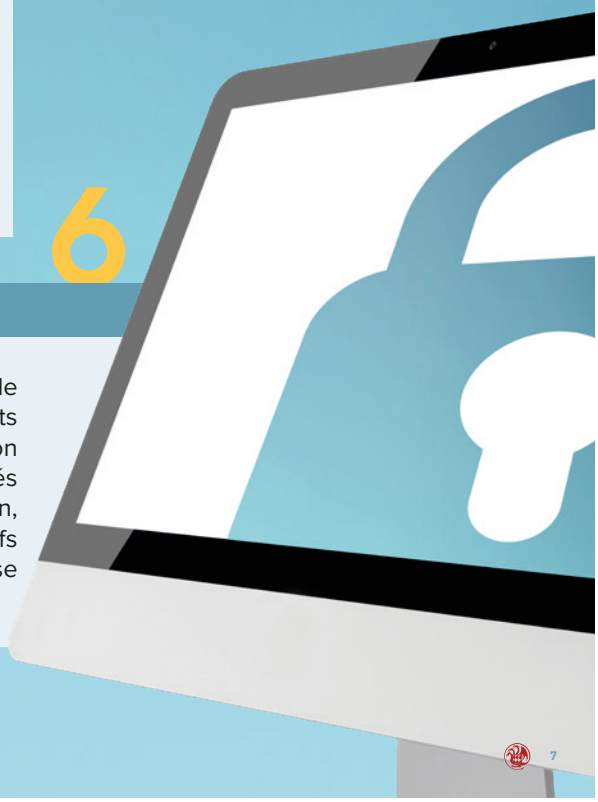
Parce qu'une agence ne peut pas, à elle seule, répondre à tous les besoins en matière de sécurité numérique, l'AMSN se donne les moyens de contribuer au développement d'un écosystème fiable.
Pour ce faire, elle s'appuie sur ses propres savoir-faire, sur des coopérations avec des partenaires de confiance par la qualification d'entreprises dans le domaine cyber, sur des programmes de travail en coopération avec quelques organismes étrangers (ANSSI, FIRST, ...). Un programme de travail est en cours de préparation avec EURECOM.

5 Quelle place dans le contexte international ?

Le cyber espace n'a pas de frontières. L'agence a donc entrepris de rentrer dans le dispositif du FIRST mettant en relation plus de 410 centres d'expertise et de réponse à incidents, permettant des échanges d'information améliorant la prévention et le traitement des attaques. Par ailleurs, elle a établi des relations privilégiées avec les Agences Nationales de la Sécurité des Systèmes d'Information française, grâce à un protocole signé en octobre 2015 par S.E.M. Michel ROGER, et luxembourgeoise, qui devra se formaliser là aussi par la signature un protocole.

6 Et en cas d'attaque ?

En cas d'attaque avérée ou soupçonnée, le centre d'expertise et de réponse aux incidents de sécurité (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.



L'AMSN en quelques chiffres

Une agence

7 personnes

120 m²

1 Direction

(directeur,
directeur adjoint,
chef de bureau)

Pôle expertise
(une personne
et une prévue
début 2018)

1

1

Pôle réglementation et relations internationales
(assuré aujourd'hui
par la Direction)

1

Pôle opérationnel
le CERT-MC
(3 chargés de mission).

opérations de cyberdéfense

Plusieurs **dizaine** de tickets d'incidents qualifiés, traités depuis septembre 2017

326
« Actualités cyber » diffusées

50
« Essentiels de la cyber » diffusés aux autorités ou responsables d'entreprise

25
alertes de sécurité

12
audits de sécurité

60
matériels (serveurs, postes, autres) installés pour construire le CERT-MC

10
assistances à la conception de système d'information ou à l'homologation

200
millions de fichiers reconstitués permettant la détection de 8 000 malwares et 3 000 fichiers considérés comme suspects

Documentations

Contribution à la rédaction d' **1** loi

Rédaction de

4
Ordonnances Souveraines

7
Arrêtés Ministériels

7
guides et recommandations

Sensibilisations

Formations

Plus de **80** entretiens formels avec les autorités, directeurs ou chefs de service de l'État, et responsables d'OIV

Plus de **50** opérations de sensibilisation

8
formations reçues

Participation à **4** forums de cybersécurité

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 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 crises** provoquées par 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 et d'inciter 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 opérateurs d'importance vitale (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), les prestataires d'informatique en nuage et d'hébergement (PINH) ;

- **d'élaborer les fonctions de sécurité** prévus 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.

rapport annuel AMSN

Stratégie

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 initiales et continues, 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 stratégique de la sécurité numérique comprend, sous la présidence de S.E. M. le Ministre d'État, les membres suivants :

- Monsieur le Président du Conseil National ou son représentant ;
- Monsieur le Directeur des Services Judiciaires ou son représentant ;
- Madame le Conseiller de Gouvernement-Ministre de l'Équipement, de l'Environnement et de l'Urbanisme ou son représentant ;
- Monsieur le Conseiller de Gouvernement-Ministre des Finances et de l'Économie ou son représentant ;
- Monsieur le Conseiller de Gouvernement-Ministre de l'Intérieur ou son représentant ;
- Monsieur le Conseiller de Gouvernement-Ministre des Relations Extérieures et de la Coopération ou son représentant ;
- Monsieur le Conseiller de Gouvernement-Ministre des Affaires Sociales et de la Santé ou son représentant ;
- Monsieur le Maire de Monaco ou son représentant ;
- Monsieur le Secrétaire Général du Gouvernement ou son représentant ;
- Monsieur le Directeur de la Direction Informatique ou son représentant ;
- Monsieur le Directeur de l'Agence Monégasque de Sécurité Numérique ou son représentant ;
- Monsieur le Directeur de la Direction des Communications Électroniques ou son représentant ;

- Monsieur le Président du Conseil Économique et Social ;
- Monsieur le Conseiller Interministériel pour le numérique auprès du Ministre d'État ;
- Monsieur André Saint-Mleux.

Le Comité s'est réuni 2 fois en 2017. Les orientations validées par le Comité sont :

- **Publication sous la forme d'un arrêté ministériel d'une 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 ;

- **Adhésion de l'AMSN au « Forum of Incident Response and Security Teams » (FIRST)**, qui permettra d'officialiser internationalement l'existence de son centre d'expertise, de réponse et de traitement en matière de sécurité et d'attaques numériques : CERT-MC. Le FIRST est une société à but non lucratif qui compte plus de 410 membres répartis sur 85 pays, parmi lesquels des opérateurs publics et privés. Cette adhésion facilitera à l'AMSN les interactions de confiance, et lui permettra d'accroître ses capacités de communication avec ses homologues pour une résolution plus rapide des incidents de sécurité indépendamment de leur origine, destination ou chemin de transit ;

- **Le principe de mise à disposition aux clients de Monaco Telecom d'un antivirus** pour leurs ordinateurs et leurs smartphones, les modalités restant à définir ;

- **L'étude d'un « réseau gouvernemental mutualisé »** permettant de mieux identifier les réseaux existants, de mieux organiser leur gestion, leur contrôle, leur administration, leur maintenance et la maîtrise de leur coût ;

- **Étude de la mise en place d'une Infrastructure de Gestion des Clés souveraine** qui permettra à terme de générer des certificats électroniques donnant valeur probante à des signatures électroniques, notamment dans la relation en l'Administration et l'administré, et à tout autre service électronique de confiance.

2 Deux axes de travail prioritaires

La stratégie nationale pour la sécurité du numérique, adresse 5 objectifs qui vont permettre à la Principauté de s'engager dans une transition numérique sécurisée. Ces objectifs sont :

- **Objectif n°1** : 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 ;

- **Objectif n°2** : la confiance numérique, le respect de la vie privée numérique, la protection des données personnelles et l'appréhension de la cyber malveillance ;

- **Objectif n°3** : la sensibilisation, les formations initiales et les formations continues ;

- **Objectif n°4** : faire de la sécurité du numérique un facteur de compétitivité ;

- **Objectif n°5** : l'établissement de liens internationaux en matière de sécurité numérique, la contribution de la Principauté à la stabilité du cyber espace.

L'AMSN, dans le souci d'accompagner cette transition numérique par la sécurité, a décidé de concentrer sa première année d'existence autour des deux premiers objectifs considérés comme axes de travail prioritaires, sans pour autant ignorer les autres.

Protéger les intérêts fondamentaux

L'urgente nécessité de protéger les intérêts fondamentaux de la Principauté appelle une prise de conscience généralisée sur les enjeux liés à l'exercice de sa souveraineté dans le domaine du numérique. Pour y parvenir, l'AMSN développe des réponses proportionnées, évolutives et collaboratives afin d'élever le niveau de sécurité des systèmes d'information de l'État comme des opérateurs d'importance vitale (OIV).

Développer la confiance dans le numérique

La sécurité n'est plus une option pour réussir une transition numérique. L'enjeu du développement des échanges numériques avec l'Union Européenne qui reste, hors France, le principal partenaire commercial de la Principauté, avec 64,9% des exportations et 58,5% des importations, a conduit l'AMSN à définir un cadre réglementaire évolutif 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.

rapport annuel AMSN

Créer

Créer un environnement fiable

1 Accompagner

L'année 2017 marque un tournant par la prise de conscience des enjeux numériques en matière stratégique, économique, sociale et géopolitique. Le positionnement de l'Agence Monégasque de Sécurité Numérique au sein des services exécutifs de l'état lui permet de favoriser l'instauration d'un environnement de confiance et de sécurité propice à la transition numérique.

La concertation et l'implication de tous les acteurs, privés et publics, contribuent à faire de la cyber sécurité 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, hélas, de nouvelles menaces et donc... de nouvelles victimes. La sécurité numérique doit donc accompagner ce changement jamais sans s'y opposer mais toujours en apportant la confiance.

Le cadre réglementaire de la Principauté doit donc permettre ces évolutions en toute sécurité, permettre de suivre et anticiper ces changements en offrant aux différents acteurs, publics comme privés, un environnement sécurisé.

En tant qu'autorité nationale, l'AMSN a pour mission de proposer la Stratégie pour la Sécurité du Numérique ainsi que 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.

3 L'activité de l'agence dans ce domaine a notamment été marquée par :

- **Une contribution à la finalisation de la loi n°1.435 du 08 novembre 2016 relative à la lutte contre la criminalité technologique**. Le titre III de cette loi crée les notions de secteurs d'importance vitale et d'opérateurs d'importance vitale, et prévoit également les obligations qui peuvent être imposées à ces derniers ainsi que les sanctions possibles.

- **La modification de l'Ordonnance Souveraine n°5.664 du 23 décembre 2015 créant l'Agence Monégasque de Sécurité Numérique**, afin d'intégrer :

  a) le contrôle des prestataires de services de confiance qualifiés, avancés ou simples, afin de s'assurer, à tout moment, que lesdits prestataires et les services qu'ils fournissent satisfont aux exigences fixées par arrêté ministériel ;

  b) la mise en place, l'actualisation et la publication de la liste des prestataires de services de confiance qualifiés ainsi que des informations relatives aux services qu'ils fournissent, dénommée « liste de confiance » ;

  c) la mise en place, si besoin, d'un service de certification électronique pour les services de l'État.

- **La mise en place de l'Ordonnance n°6.486 du 25 juillet 2017 instituant un Comité stratégique de la sécurité numérique.**

Elle concerne la création d'un Comité stratégique de la sécurité numérique ayant pour rôle de valider et de suivre les plans d'action découlant de la stratégie nationale pour la sécurité numérique.

- **L'Ordonnance n°6.525 du 16 août 2017 portant application des articles 18, 19 et 25 de la loi n°1.383 du 2 août 2011 sur l'économie numérique, modifiée.**

Elle concerne la création de la signature électronique, de l'horodatage et introduit la notion de Prestataire de confiance. Cette ordonnance concerne principalement les organismes du secteur public et les prestataires de services de confiance. Elle instaure en outre un cadre en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence d'un marché numérique avec l'ambition d'accroître la confiance dans les transactions électroniques.

- **L'Ordonnance n°6.526 du 16 août 2017, portant application des articles 36 et 37 de la loi n°1.383 du 2 août 2011 sur l'économie numérique, modifiée.**

Elle concerne les déclarations relatives à la cryptologie qui permet d'assurer la confidentialité des données, leur authentification ou le contrôle de leur intégrité pendant l'archivage ou leur transmission.

- **Le projet d'arrêté ministériel définissant la « Charte Administrateurs Réseaux et Systèmes d'Information » de l'État.**

La Charte des systèmes d'information de l'État a été rendue applicable par la publication de l'arrêté ministériel n°2015-703 du 26 novembre 2015 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. Les administrateurs réseaux et systèmes d'information de l'État, mentionnés dans la charte précitée, sont titulaires de privilèges importants sur le système d'information et il était nécessaire d'encadrer strictement leurs activités par le biais d'une charte spécifique. Après explication du contenu de la charte auprès des personnels concernés, l'arrêté sera publié début 2018.

- **L'Arrêté ministériel n°2016-723 du 12 décembre 2016, portant application de l'article 18 de la loi n°1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale et fixant les niveaux de classification des informations, modifié.**

Cet arrêté définit les dispositions relatives à la classification, à l'habilitation et à la protection du secret de sécurité nationale. Il définit les moyens de protection physique et organisationnels à mettre en place pour garantir l'intégrité et la confidentialité des informations classifiées. Il a permis la signature d'un Accord Général de Sécurité avec la France entré en vigueur, à Monaco, le 14 décembre 2017.

- **L'Arrêté ministériel n°2017-42 du 24 janvier 2017, portant application de l'article 26 de la loi n°1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique.**

Cet arrêté définit les secteurs d'importance vitale constitués d'activités concourant à un même objectif ayant trait à la production et la distribution de biens ou de services indispensables à la satisfaction des besoins essentiels pour la vie de la population monégasque, à l'exercice de l'autorité de l'État, au fonctionnement de l'économie ainsi qu'à la sécurité de l'État. Cet arrêté a été suivi de plusieurs dizaines d'arrêtés désignant chaque opérateur d'importance vitale.

- **L'Arrêté ministériel n°2017-56 du 1er février 2017 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.**

Cet arrêté définit la Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E) qui contribue à assurer la continuité des activités régaliennes, à prévenir la fuite d'informations sensibles et à renforcer la confiance des administrés et des entreprises dans les télé-procédures.

- **L'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.**

Cet arrêté définit les exigences pour les Prestataires d'Audit de Sécurité des Systèmes d'Information (PASSI). Il contribue à la confiance des entités publiques ou privées dans les prestataires d'audit et garantit la qualité et la fiabilité des audits commandités.

- **L'Arrêté ministériel n°2017-626 du 16 août 2017, portant application de l'Ordonnance Souveraine n°6.526 du 16 août 2017 portant application des articles 36 et 37 de la loi n°1.383 du 2 août 2011 sur l'économie numérique, modifiée.**

Cet arrêté précise les modalités de déclaration d'importation et d'exportation des moyens de cryptologie.

- **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.**

Cet arrêté met en place le Référentiel Général de Sécurité (RGS) qui traite de l'identification électronique, des règles applicables aux systèmes d'information et des services de confiance pour les transactions électroniques. Ce référentiel a été rédigé pour être compatible avec le règlement européen eIDAS. Ce document doit être suivi d'une dizaine d'arrêtés précisant les modalités techniques des sujets traités dans celui-ci tels que : la signature électronique, les certificats électroniques, les authentifications, les règles techniques de la cryptographie, etc.

rapport annuel AMSN

Sensibiliser

4

Sensibiliser aux enjeux de la sécurité numérique

1 Action de sensibilisation

Face à la montée de la menace cyber, la prise de conscience du risque par les décideurs de l'État, les OIV et l'ensemble des acteurs de la Principauté constitue un enjeu majeur. Dans cette optique, l'AMSN a développé une action de sensibilisation.
La sécurité des systèmes d'information a longtemps été un non sujet en Principauté, puis perçue comme un sujet contraignant de spécialistes. Mais les quelques attaques ayant émergé au moment de la création de l'agence ont changé la donne.

Aujourd'hui, après seulement un an et demi, le sujet est pris plus au sérieux, et commence à entrer peu à peu dans le champ de vision des décideurs, et des responsables des systèmes d'information. Si le processus de prise de conscience ne progresse pas encore au rythme souhaité pour parer les menaces de plus en plus omniprésentes, la mission de sensibilisation que mène l'AMSN apparaît d'une grande nécessité et est de mieux en mieux accueillie.

2 Sécurité informatique et pédagogie

En tant que chef de file de la sécurité du numérique à Monaco, l'AMSN défend une approche pédagogique, positive et ancrée dans la réalité de l'exécution des missions avec une prise de conscience des risques pris qui doivent être compris, calculés et assumés par les responsables.

En 2017, 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 des entreprises ou encore des compagnies d'assurances s'est traduite par plus d'une cinquantaine de communications, conférences, dialogues, à chaque fois avec une adaptation au cas par cas.

3 Une action au profit des opérateurs d'importance vitale

Dans le cadre de la loi n°1.435 du 08 novembre 2016, des liens directs avec les opérateurs d'importance vitale ont permis d'expliquer les risques cyber, la finalité de la loi et le travail à accomplir ensemble. Le volume des sollicitations reçues des OIV indique une prise de conscience importante et une attente forte de l'action de l'AMSN.

Réunion d'information du 22 juin 2017 destinée aux Opérateurs d'Importance Vitale (OIV) de la Principauté sur les cybers risques et les mesures législatives prévues, en présence de SEM Serge Telle, Ministre d'Etat, et de M. Patrice Cellario, Conseiller de Gouvernement-Ministre de l'Intérieur, l'Amiral Dominique Riban, Directeur de l'AMSN.

L'AMSN a rencontré la quasi-totalité des OIV. Les arrêtés définissant les mesures à mettre en œuvre sont en cours d'écriture en liaison étroite avec chaque secteur voire chaque OIV. De nombreux OIV ont été rencontrés en tête à tête afin de mieux comprendre les difficultés et les situations de chacun.

Douze secteurs d'importance vitale ont été définis par les autorités de tutelle, par arrêté ministériel :

Secteurs	Coordinateurs
Audiovisuel et Information	Le Ministre d'État
Informatique	Le Ministre d'État
Activités Civiles de l'État	Département de l'Intérieur
Activités judiciaires de l'État	Direction des Services Judiciaires
Alimentation	Département des Affaires Sociales et de la Santé
Communication électronique	Département de l'Équipement, de l'Environnement et de l'Urbanisme
Énergie	Département de l'Équipement, de l'Environnement et de l'Urbanisme
Banque, finance	Département des Finances et de l'Économie
Gestion de l'eau	Département de l'Équipement, de l'Environnement et de l'Urbanisme
Industrie, commerce	Département des Finances et de l'Économie
Santé	Département des Affaires Sociales et de la Santé
Transports	Département de l'Équipement, de l'Environnement et de l'Urbanisme

4 Une vigilance sur les systèmes industriels

Les systèmes industriels, autrement appelés SCADA (systèmes d'acquisition et de contrôle de données) sont aujourd'hui quasiment tous pilotés par ordinateurs. Ces systèmes, parfois anciens, n'ont aucune protection contre les cyber-attaques. Une sensibilisation particulière a été effectuée pour tous les services de l'État, les établissements publics et les OIV, soit dans des réunions restreintes, soit lors de conférences avec l'appui des industriels fabriquant ces matériels et notre partenaire, l'ANSSI française.

Réunion de sensibilisation sur les risques et la sécurité des systèmes industriels, 21 décembre 2017, Auditorium Rainier III.

5 Une action permanente d'information et de sensibilisation

Chaque jour depuis juillet 2016, l'AMSN rédige des actualités sur le cyber espace, afin de sensibiliser et informer les acteurs de la Principauté inscrits sur une liste. Par ailleurs, chaque vendredi est adressé à une liste d'autorités un document, intitulé « Les essentiels de la cyber », résumant en deux pages, sans éléments techniques, les faits les plus marquants. L'objectif est de sensibiliser les autorités et les hauts responsables.

L'AMSN a participé au salon de l'AGORA des métiers organisé par la Direction de l'Education Nationale, de la Jeunesse et des Sports afin de sensibiliser les jeunes à la fois aux risques cyber mais surtout aux débouchés des métiers cyber.

6 Formation et recrutement

Afin de faire mieux prendre en compte la sécurité dans les projets et dans les différentes directions de l'État, les cadres de l'AMSN ont participé à près d'une douzaine d'entretiens d'embauche afin de mieux appréhender les compétences informatiques et de sécurité des candidats.

Par ailleurs pour ses besoins propres, le personnel de l'AMSN a participé à 8 formations spécialisées de 2 à 5 jours à l'ANSSI, (« Principes et organisation des audits de sécurité des systèmes d'information », « Pratique des audits en sécurité des systèmes d'information », « Incidents de sécurité », ...) Ces formations s'inscrivent dans un cursus complet qui devrait continuer en 2018.

Enfin, l'AMSN a effectué une dizaine de formation et sensibilisation sur des sujets de sécurité informatique, tels que la charte administrateurs systèmes et réseaux, et l'homologation de sécurité et analyse de risques au sein des services de l'État.

rapport annuel AMSN

Sécuriser

Sécuriser les communications et informations de l'Etat

1 Sécuriser les communications téléphoniques des autorités

Afin de sécuriser les communications les plus sensibles au sein de l'État, sur l'impulsion de l'AMSN et en étroite collaboration avec elle, les services informatiques ont déployé 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.

2 Le secret de sécurité nationale

Suite à la publication de la loi n°1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale, l'AMSN a rédigé l'arrêté d'application de l'article 18 ainsi qu'un guide afin de faciliter la mise en place des procédures et des mesures physiques ou techniques de protection qui entrainent un changement dans le fonctionnement de l'État.

Ce dispositif a permis la signature le 13 juillet 2017 d'un Accord Général de Sécurité avec la République française, rendu exécutoire par l'Ordonnance Souverain°6.762 du 25 janvier 2018, créant une reconnaissance mutuelle des niveaux de confidentialité et de traitement des informations, permettant ainsi l'échange d'informations les plus sensibles entre les deux pays.

Signature le 13 juillet 2017 de l'accord général de sécurité en présence de S.E. M. Serge Telle, Ministre d'Etat et du Secrétaire général de la Défense et de la Sécurité nationale, M. Louis Gautier.

Toujours dans l'application de ces mesures a été mis en place le processus d'habilitation des personnes. Cette habilitation permet de garantir que les données classifiées seront traitées par des personnes de confiance, sensibilisées aux risques et conscientes de leurs responsabilités.

Enfin, les études pour la mise en place, au sein des services de l'État, d'un réseau permettant le traitement des informations classifiées ont été lancées. Ce réseau devrait entrer en service prochainement.

3 Une Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E)

L'AMSN a fait publier par arrêté ministériel une PSSI-E applicable aux services de l'État et aux établissements publics.

Celle-ci prévoit 161 mesures classées en plusieurs priorités. Tous les services exécutifs de l'État et les établissements publics concernés doivent effectuer un rapport annuel de progression en utilisant l'outil développé par l'AMSN afin de faciliter ce travail.

Chaque année, l'AMSN adresse un compte rendu à SEM le Ministre d'État sur l'avancement du déploiement de ces mesures, pour chaque service ou établissement, et plus globalement pour l'ensemble des entités concernées.

Cette politique contribue largement à protéger les informations détenues dans les systèmes d'information.

Une des mesures phares de cette politique de sécurité est l'obligation d'homologuer les systèmes d'information à l'issue d'une analyse de risques. Les risques résiduels devant être assumés, de façon formelle, par l'autorité d'homologation choisie au niveau des responsables métiers.

4 Soutiens et conseils dans la conception des systèmes d'information

L'AMSN a contribué à l'architecture de 10 systèmes d'information de service de l'État de manière à prendre en compte, dès le début des projets, la sécurité des systèmes d'information (confidentialité, disponibilité, intégrité). Lors de ces contributions, l'AMSN a recommandé l'utilisation de matériels de confiance dont la sécurité et le fonctionnement ont été vérifiés par des laboratoires indépendants.

L'AMSN, en tant que membre de droit de la 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.

5 Prestataire d'audit de sécurité de systèmes d'information (PASSI)

L'AMSN a mis en place un référentiel pour les prestataires d'audits de sécurité des systèmes d'information (PASSI). L'objectif de celui-ci est d'apporter aux commanditaires d'audit la garantie d'un audit impartial, effectué suivant un référentiel garantissant la complétude, la qualité du travail, la compétence des auditeurs. Par ailleurs, les prestataires ont l'obligation d'effectuer un rapport complété de recommandations classées par ordre de priorité.

Cette qualification est attribuée par l'AMSN sur un rapport de certification effectué par un organisme indépendant lui-même contrôlé par le COFRAC (comité français d'accréditation).

Le premier prestataire devrait être qualifié début 2018 et quatre autres sont en cours de qualification.

rapport annuel AMSN

Protéger

Protection et coopération internationale

1 Veille et publication

L'AMSN, avec le concours entre autres du CERT-FR, assure une veille des informations et des alertes cyber afin de pouvoir sensibiliser et réagir rapidement à toutes menaces sur les systèmes d'information de l'État et de l'ensemble des acteurs de la Principauté.

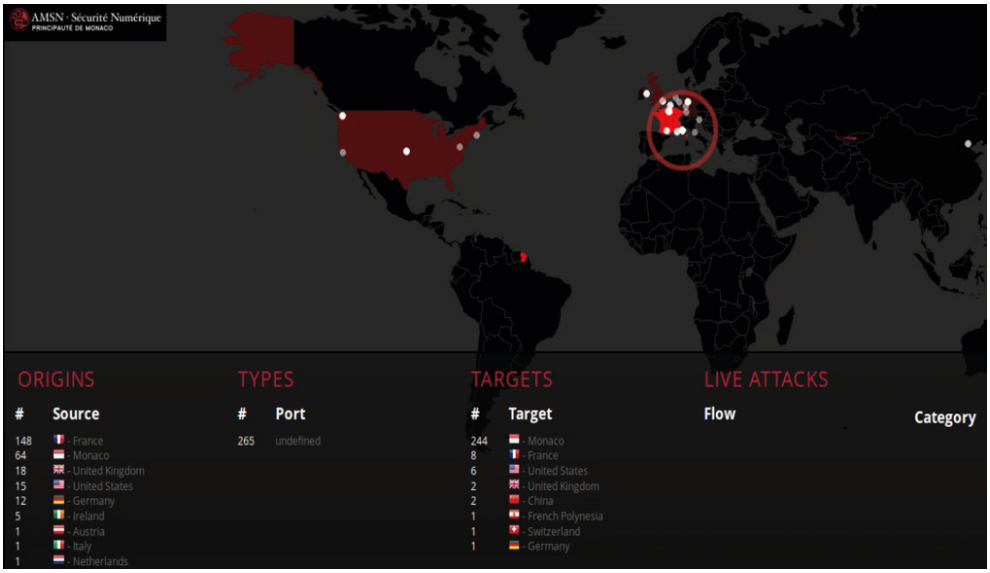
Ainsi, plus d'une centaine d'alertes de sécurité (vulnérabilités, failles, etc.) ont pu être rapidement diffusées vers les OIV ou les services de l'État afin d'éviter la compromission de leurs systèmes d'information.

2 CERT-MC

L'AMSN s'est attelée, dès juillet 2016, à créer un centre d'expertise et de réponse aux incidents de sécurité, mis en place initialement sous le nom CSIRT-MC. Depuis fin 2017, le centre est devenu CERT-MC, après avoir validé les conditions réglementaires imposées par cette marque déposée.

Le CERT-MC dispose de moyens matériels importants qui lui permettent d'effectuer la veille des systèmes d'information de l'État. Ce dispositif coûteux et long à mettre en place est maintenant opérationnel (fin novembre 2017) et permet d'assurer la collecte, l'analyse et la qualification des vulnérabilités et des incidents. 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 affaire, permettant une démarche d'amélioration continue.

Depuis le 22 décembre 2017 l'AMSN est autorisée à utiliser la marque CERT™ sous la forme CERT-MC et CERT Monaco par CARNEGIE MELLON UNIVERSITY.



Etat de la menace en direct du CERT-MC.

Aujourd'hui, la quasi-totalité des services de l'État est ainsi supervisée. Ce service pourrait également être proposé à certains OIV de la Principauté afin de mutualiser les coûts d'exploitation. L'étude de cette possibilité a débuté fin 2017.

Depuis juin 2017, le CERT-MC a qualifié et traité plusieurs dizaine d'alertes, parmi les détections qu'il a effectuées et les signalements qui lui ont été faits. Parmi ces alertes, plusieurs 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.

Aujourd'hui, le système de détection rassemble une batterie d'antivirus différents, plus de 60 000 marqueurs techniques et permet de revenir régulièrement sur les anomalies constatées ou soupçonnées. Le CERT-MC est en mesure de créer ses propres marqueurs et de les intégrer dans le dispositif.

3 Les audits

L'AMSN a effectué 12 audits, soit dans le cadre des interventions de remédiation d'incidents de sécurité, soit dans le cadre de la prévention. Tous ces audits ont été suivis de recommandations afin d'améliorer la situation.

Les recommandations sont systématiquement classées avec un ordre de priorité. Un suivi régulier est ensuite assuré afin de s'assurer que l'ensemble des sujets sont traités dans un temps raisonnable et réaliste.

Parmi ces 12 audits, plusieurs comprenaient des audits organisationnels, et ont été effectués pour améliorer à la fois l'organisation de la gestion de la sécurité informatique mais également la sécurité physique des locaux hébergeant les systèmes d'information ; la sécurité physique étant un élément essentiel de la sécurité en général.

4 La coopération internationale et le FIRST

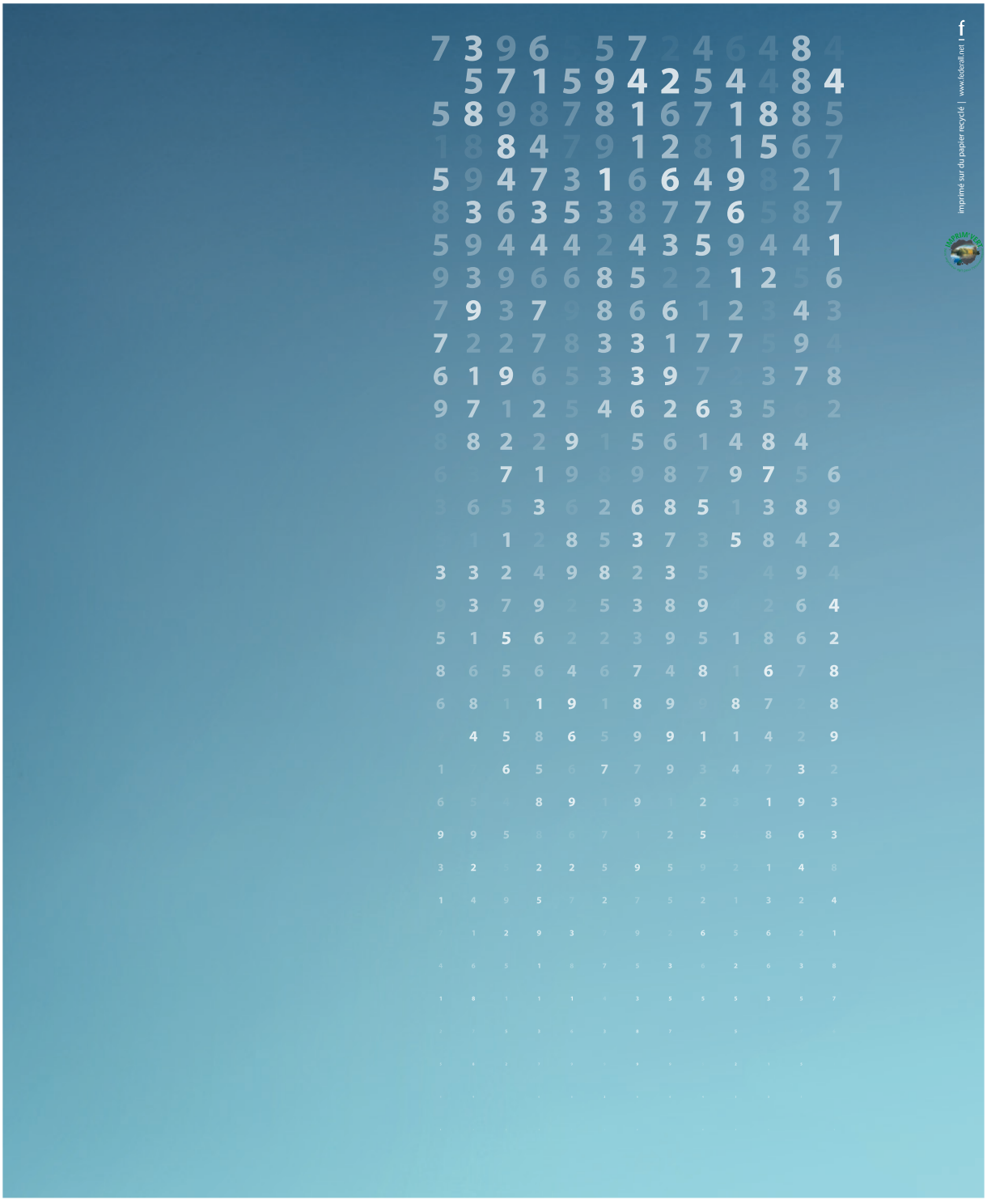
Sur le plan international, l'Agence Monégasque de Sécurité Numérique (AMSN) a développé une collaboration étroite avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) française.

L'accord de travail, qui avait été signé en octobre 2015 entre le Gouvernement de la Principauté et l'Agence Nationale de la Sécurité des Systèmes d'Information s'est traduit par de très nombreuses réunions à Paris ou à Monaco.

L'ANSSI a apporté un soutien extrêmement utile pour le démarrage de l'AMSN en l'autorisant à réutiliser une bonne partie du travail déjà effectué entre 2009 et 2017.

Ainsi les textes législatifs et réglementaires ont pu être réalisés beaucoup plus rapidement que s'il avait été nécessaire de partir d'une feuille blanche.

Le CERT-MC a entrepris d'adhérer à l'organisation FIRST (Forum of Incident Response and Security Teams). Cette adhésion nécessite une organisation et des processus de travail extrêmement précis et exigeants. Ce travail a été accompli dans un temps record (moins de 4 mois). La mise en place de ces prérequis est contrôlée par un audit de deux parrains, membres du FIRST. A ce titre, le CERT-FR et le GOVCERT.LU ont effectué l'audit début décembre 2017. Le résultat n'a fait apparaître aucun défaut ; en conséquence l'approbation de l'adhésion devrait être prononcée lors de l'assemblée générale du FIRST le 28 juin 2018 à Kuala Lumpur (Malaisie).



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