RAPPORT D'ACTIVITÉ 2024

Ils ne savaient pas que c'était impossible,
alors ils l'ont fait.

amsn.gouv.mc

SOMMAIRE

EDITO 3

LES FAITS MARQUANTS 4

LES CHIFFRES CLÉS 7

LE TOP 5 DES TECHNOLOGIES CIBLÉES 12

TEXTES RÈGLEMENTAIRES PUBLIÉS 12

INFORMATION-SENSIBILISATION 12

RECYCLAGE DES SUPPORTS NUMÉRIQUES 13

LA STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE 14

INDICE MONDIAL DE LA CYBERSÉCURITÉ 17

FOCUS SUR L'ÉVOLUTION DE LA MENACE 18

EDITO

L'année 2024 a été intense pour l'Agence Monégasque de Sécurité Numérique (AMSN) et ses Agents et Prestataires que je remercie pour leur dévouement à la protection des systèmes d'information de la Principauté et au développement des services numériques de confiance.

2024 aura été une année charnière pour l'AMSN car l'évolution des textes encadrant ses missions lui demandent plus de structuration et plus de rigueur.

Dans un contexte où les actions de reconnaissance malveillante et les tentatives d'attaques sur les systèmes d'information de la Principauté ont augmenté respectivement de 63% et 32% par rapport à 2023, l'AMSN a continué à renforcer ses moyens de détection, automatiser certaines tâches courantes, et fluidifier la relation opérationnelle avec ses parties prenantes.

Les évolutions règlementaires et normatives européennes récentes concernant les services numériques de confiance ont nécessité le renforcement du pôle en charge de ces sujets pour moderniser son socle technique et anticiper l'arrivée de la cryptographie post-quantique.

Cette sixième édition du rapport d'activité présente le bilan du travail réalisé sur l'année 2024 par l'AMSN, les services exécutifs de l'État et toutes les parties prenantes engagées dans la sécurité numérique.

Je profite de cet éditorial pour remercier nos partenaires et homologues français, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et le Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA), qui permettent à l'AMSN, et à la Principauté, respectivement depuis 2015 et 2024, de faire face plus rapidement à certains enjeux de cybersécurité.

Frédéric FAUTRIER
Directeur

LES FAITS MARQUANTS

Bruno VALENTIN-Sébastien MASSE-Frédéric FAUTRIER

Frédéric FAUTRIER - Bruno VALENTIN

13 – 14 MAI

71ÈME RÉUNION DE LA TF-CSIRT

Les représentants de l'équipe de réponse aux incidents de sécurité de l'AMSN (CERT-MC) et de la société Monaco Cyber Sécurité (CERT-MCS) ont assisté à la 71ème réunion de la TF-CSIRT qui s'est tenue à Copenhague du 13 au 14 mai. A cette occasion, Monaco Cyber Sécurité s'est présentée à la communauté de la Task Force-CSIRT. Le CERT-MC est membre de la TF-CISRT depuis 2018, le CERT-MCS depuis le 14 novembre 2023.

9 - 14 JUIN

36ÈME CONFÉRENCE ANNUELLE DU FIRST

L'AMSN a participé à la 36ème conférence annuelle du FIRST, association qui regroupe 748 équipes de réponse à incident représentant 111 pays, et qui s'est déroulée du 9 au 14 juin à Fukuoka – Japon. Cette édition, très constructive et bénéfique, a donné l'occasion à Bruno VALENTIN, responsable du CERT-MC, et Frédéric FAUTRIER, Directeur de l'AMSN, d'échanger largement avec leurs homologues étrangers sur les sujets ayant trait à la cybersécurité, la détection des incidents de sécurité et les moyens d'y remédier.

10 – 14 JUIN

CAPTURE THE FLAG (CTF) ORGANISÉ PAR LE FIRST

L'équipe de réponse aux incidents de sécurité de l'AMSN, le CERT-MC, a participé au CTF organisé par le FIRST en marge de la conférence annuelle.
Le CTF consiste en une série d'exercices techniques (défis) où les participants doivent trouver une réponse ou un indicateur et le soumettre à la plateforme CTF.
Chaque indicateur soumis contribue au score de l'équipe. De nouveaux défis sont publiés chaque jour pendant la conférence et sont classés par catégorie : réseau, web, système de contrôle industriel, cryptographie, rétro-ingénierie, programmation, divers, casse-tête, etc.
Le CERT-MC était engagé dans cet exercice avec le CERT-AG (l'équipe de réponse aux incidents de sécurité du groupe Crédit Agricole) sous la bannière «WeMissedOneHour». Cette équipe de circonstance a terminé 4ème sur les 91 équipes engagées dans cette compétition de cybersécurité.

25 JUIN

EXERCICE NATIONAL DE GESTION DE CRISE CYBER

Un exercice national de cybersécurité dénommé « TARTARE », destiné à évaluer les capacités de réaction de l'Agence Monégasque de Sécurité Numérique (AMSN) et des directions de la Délégation Interministérielle chargée de la Transition Numérique (DITN), s'est déroulé le mardi 25 juin 2024 au Centre National de Gestion de Crise, activé pour l'occasion. Elaboré par la société française Orange Cyber Défense, le scénario complexe et protéiforme qui a été joué était inspiré de faits réels dont sont victimes au quotidien de nombreuses entités dans le monde. En plus de la dimension technique, l'État, au travers du Département de l'Intérieur avec le concours actif de plusieurs autres Départements Ministériels, s'est également mobilisé en organisant une mise en situation permettant d'affiner le dispositif final du plan de Gestion des Evénements Importants (GEVIM) qui entrera prochainement en vigueur.

La Tour-Maubourg, siège de l'ANSSI

13 NOVEMBRE

RÉUNION BILATÉRALE ANSSI-AMSN

Dans le cadre du programme de coopération entre l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) de la République française et l'AMSN, renouvelé en 2020, les deux agences ont tenu leur réunion bilatérale annuelle le 13 novembre.

† S.E.M. Didier GUILLAUME, Ministre d'État

9 -11 OCTOBRE

LES ASSISES DE LA CYBERSÉCURITÉ

Ce rendez-vous incontournable des acteurs de la sécurité numérique rassemble près de 3300 participants et 180 partenaires, parmi lesquels des startups, des PME, des grands groupes industriels français, européens, nord-américains, du Moyen-Orient et d'Asie, dont certains interviennent en Principauté.
Avec un espace dédié parmi les professionnels, l'Agence Monégasque de Sécurité Numérique (AMSN) réunit aux 24ème Assises les acteurs de la sécurité numérique de la place.

Jérôme NOTIN - Frédéric FAUTRIER

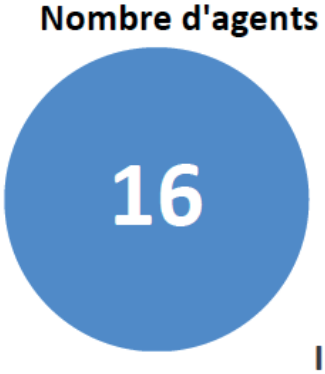
14 NOVEMBRE

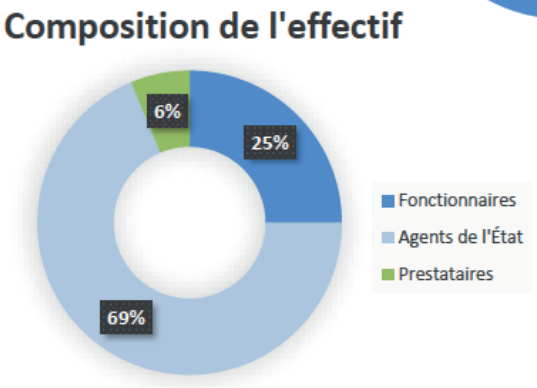
LE GOUVERNEMENT PRINCIER S'ENGAGE CONTRE LA CYBERMALVEILLANCE

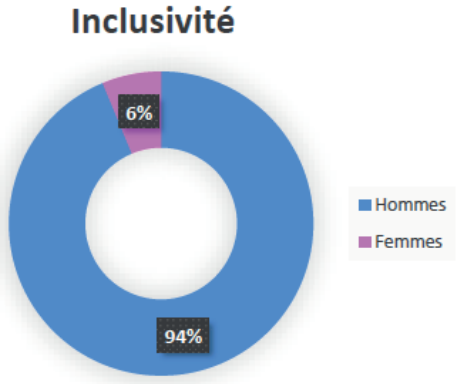
Le Groupement d'Intérêt Public Action contre la Cybermalveillance (GIP ACYMA) et l'Agence Monégasque de Sécurité Numérique (AMSN), représentés respectivement par le Directeur Général du GIP ACYMA, Jérôme NOTIN et le Directeur de l'AMSN, Frédéric FAUTRIER, ont signé le 14 novembre 2024, un programme de coopération en matière de sensibilisation, de prévention et d'assistance aux victimes d'actes de cybermalveillance pour les particuliers et les entreprises.

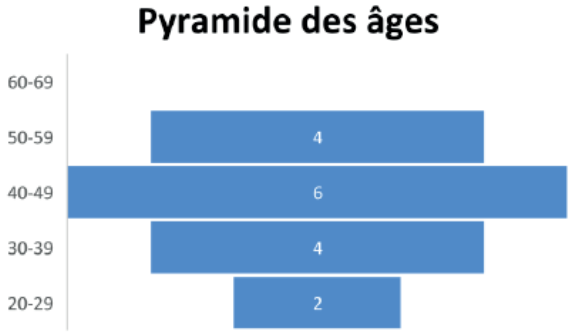
LES CHIFFRES CLÉS

LES EFFECTIFS DE L'AMSN

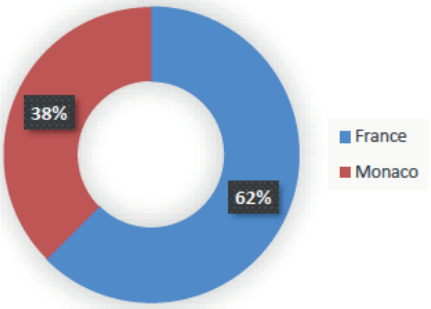




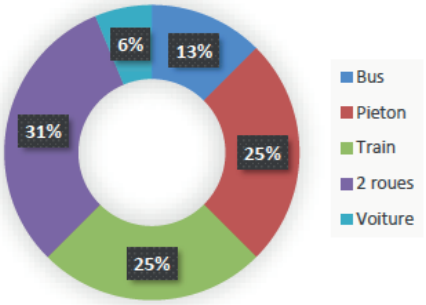




Pays de résidence des agents

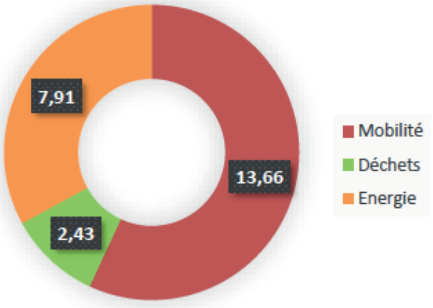


Modes de transport

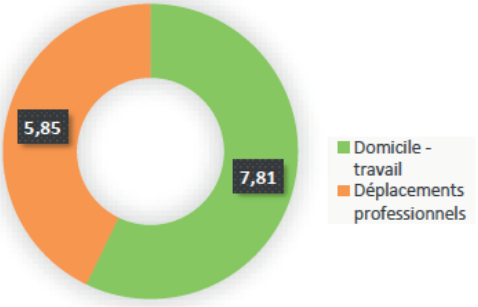


Bilan d'émissions de gaz à effet de serre de l'AMSN (tonne d'équivalent CO_2)

Ensemble des émissions



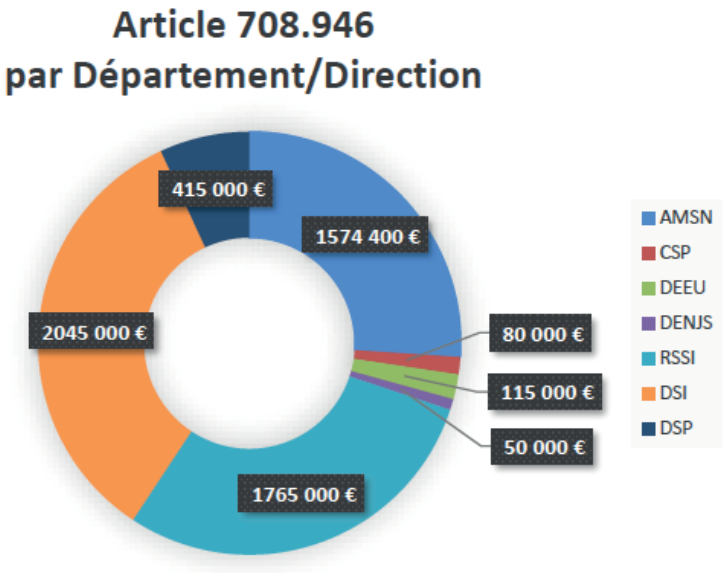
Emissions liées à la mobilité

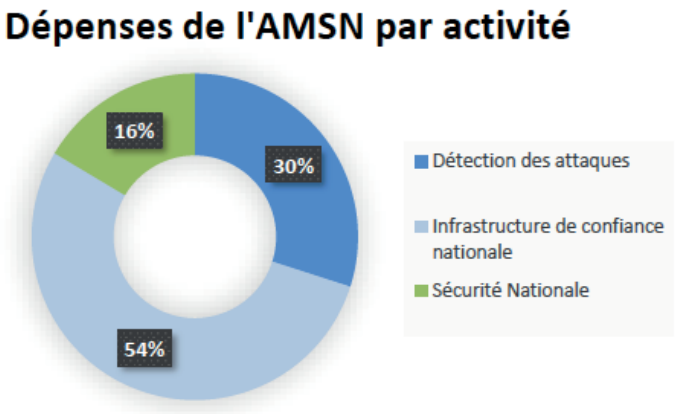


LE FINANCEMENT DE LA SÉCURITÉ NUMÉRIQUE

La loi n° 1.557 du 22 décembre 2023 portant fixation du budget général primitif de l'exercice 2024, adoptée par le Conseil National dans sa séance du 21 décembre 2023, prévoyait 6,91 M€ pour la sécurité numérique à l'article 708.946.

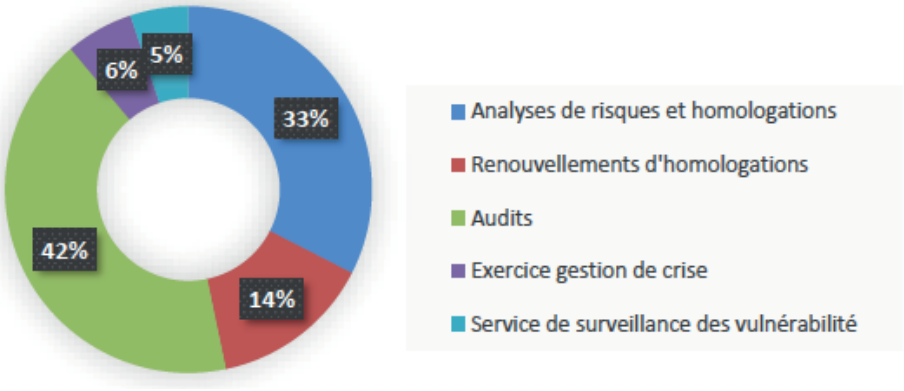
Cet article budgétaire, permettant de décliner les objectifs stratégiques prioritaires du Gouvernement en matière de sécurité numérique, regroupe les besoins de tous les services exécutifs de l'État ainsi que les participations de l'État dans des opérations de cybersécurité bénéficiant aux entreprises et aux résidents de la Principauté.





La ventilation des dépenses de l'AMSN a évolué en 2024. Les crédits concernant l'Infrastructure de Confiance Nationale qui permet de délivrer aux Monégasques, Résidents, Fonctionnaires, Agents de l'État et Entreprises une signature électronique, ont permis de préciser et d'étendre le périmètre d'intervention de l'infogéreur et de démarrer le renouvellement des matériels et logiciels qui sont arrivés en fin de vie. Ce renouvellement se prolongera sur les exercices 2025 et 2026.

Dépenses du RSSI du Gouvernement par activité



Le Responsable Sécurité des Système d'Information (RSSI) du Gouvernement a continué d'animer la mise en oeuvre des analyses de risques et des audits, prévus par la Politique de Sécurité des Systèmes d'Information de l'État (PSSI-E), pour les projets numériques des services exécutifs de l'État. Ainsi, en 2024 :

- **35** systèmes d'information ont été **homologués ;**
- **33** systèmes d'information ont fait l'objet d'un **renouvellement de leur homologation ;**
- **16** systèmes d'information ont fait l'objet d'un **audit.**

LES ÉVÉNEMENTS DE SÉCURITÉ TRAITÉS PAR L'AMSN

L'AMSN a comptabilisé, en 2024, en amont des logiciels et matériels de sécurité de ses parties prenantes étatiques, **17 millions** d'alertes de sécurité, composées de 15,2 millions d'actions de reconnaissance (↗**+63%**), et **1,7 million** de tentatives d'attaques ou d'utilisation d'outils malveillants destinés à les commettre (↗**+32%**).
Sur **1,7 million** de tentatives d'attaques visant les entités de l'État en 2024 :
– **822** événements de sécurité ont fait l'objet d'un suivi avec les entités concernées (↘ **-31%**).
– **6** incidents de sécurité sont à dénombrer, qui ont nécessité des investigations approfondies par le CERT-MC (↘ **-40%**).
Malgré la menace croissante, illustrée par l'augmentation des alertes de sécurité, le nombre d'événements et incidents de sécurité est en baisse. Cela illustre, au fil des années, de la part de l'AMSN et de ses parties prenantes, une montée progressive en maturité dans le domaine de la cybersécurité.

LES RISQUES CONSTATÉS EN PRINCIPAUTÉ

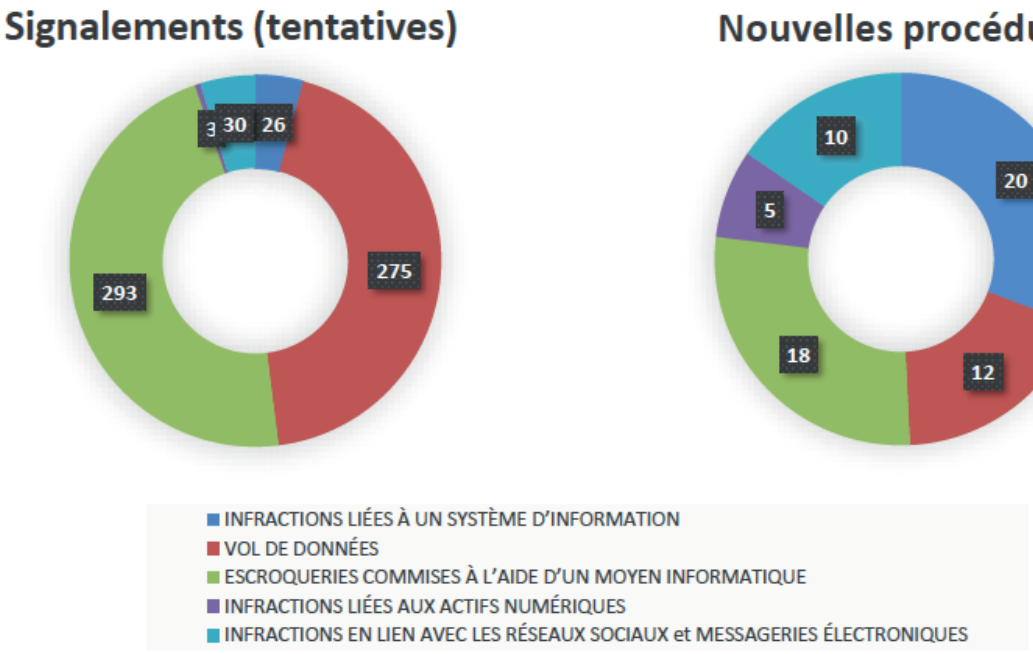
L'Agence répertorie chaque semaine la totalité des serveurs informatiques de la Principauté qui utilisent des protocoles de communication non sécurisés ou qui ont des vulnérabilités exposées sur Internet. Dans les deux cas, leurs propriétaires prennent des risques pouvant entraîner le vol de leurs données, la prise de contrôle à distance de leurs serveurs par des attaquants, ou encore un rançonnement.
– **159** serveurs ont utilisé des protocoles de communication non sécurisés (↘**77%**).
– **535** serveurs ont exposé des vulnérabilités exploitables (↘ **-53%**).

LA CYBERCRIMINALITÉ

La Direction de la Sûreté Publique contribue à la lutte contre la criminalité technologique en exerçant le volet répressif des dispositions introduites dans les codes par la loi n° 1.435.

Forte d'une unité spécialisée dans la lutte contre la criminalité technologique, elle a été amenée en 2024 à apporter une assistance aux victimes ayant signalé des tentatives d'attaques et à intervenir dans le cadre de procédures judiciaires sur de nombreux dossiers.

Les courriels constituent le vecteur d'attaque le plus utilisé. 264 signalements d'hameçonnage ont été faits auprès de la Direction de la Sûreté Publique en 2024.



Evolution des infractions, vols et escroqueries en 2024	
INFRACTIONS LIÉES À UN SYSTÈME D'INFORMATION	↗ +171%
VOL DE DONNÉES :	↗ +54%
Courriels frauduleux (Phishing)	↗ +49%
Sites web ou annonces frauduleux	↗ +260%
ESCROQUERIES COMMISES À L'AIDE D'UN MOYEN INFORMATIQUE	↘ -55%
INFRACTIONS LIÉES AUX ACTIFS NUMÉRIQUES	↘ -20%
INFRACTIONS EN LIEN AVEC LES RÉSEAUX SOCIAUX et MESSAGERIES ÉLECTRONIQUES	↗ +90%

LE TOP 5 DES TECHNOLOGIES CIBLÉES

Sur le périmètre qu'elle supervise, l'Agence a comptabilisé en 2024 de nombreuses tentatives d'exploitation de vulnérabilités. Etaient principalement concernés :

1° La bibliothèque **Log4j** qui, utilisée de manière directe ou indirecte dans de nombreux logiciels, figure toujours en tête des technologies ciblées en 2024 ;

2° Le langage de programmation **PHP**, utilisé pour produire des sites web dynamiques. Ce dernier a fait l'objet de nombreuses tentatives d'exploitation sur diverses vulnérabilités répertoriées ;

3° L'équipementier **Realtek**, produisant principalement des cartes réseau. Il figure en troisième place dans ce classement des technologies visées par les attaquants ;

4° Les produits de l'éditeur **F5 Networks**, spécialisé dans les pare-feu web applicatifs. Les attaquants ont tenté de nombreuses exploitations de vulnérabilités sur ces logiciels de sécurité ;

5° Le constructeur de matériel réseau **Cisco Systems**.

TEXTES RÈGLEMENTAIRES PUBLIÉS

3 textes règlementaires dans le domaine de la sécurité numérique ont été publiés en 2024 :

– l'Ordonnance Souveraine n° 10.350 du 25 janvier 2024 qui définit l'organisation de l'AMSN et introduit dans le cadre règlementaire de la cybersécurité les prestaires de vérification d'identité à distance (PVID), d'administration et de maintenance sécurisées (PAMS), et d'accompagnement et de conseil en sécurité des systèmes d'information (PACS) ;

– l'arrêté ministériel n° 2024-51 du 25 janvier 2024 qui précise les missions du Centre de réponse et de traitement en matière d'attaques numériques de l'AMSN (CERT-MC) et les moyens à mettre oeuvre ;

– l'arrêté ministériel n° 2024-164 du 22 mars 2024 qui porte le référentiel de qualification des prestataires de vérification d'identité à distance (PVID).

INFORMATION-SENSIBILISATION

Chaque année, de nombreuses publications sont transmises aux parties prenantes de l'AMSN. En 2024 :

– **244** « actualités » sur le cyberespace ont été publiées, afin de sensibiliser et informer les acteurs spécialisés de la Principauté.

– **52** « Les essentiels de la cyber » ont été adressés 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 événements mondiaux dans le domaine de la cybersécurité.

– **50 alertes de sécurité, dont 35 nécessitant une prise en compte immédiate,** ont été émises, nombre stable par rapport à l'année dernière. Ces documents sont destinés à prévenir les équipes techniques opérationnelles des parties prenantes de l'AMSN, d'un danger imminent sur des logiciels ou équipements informatiques. Leur prise en compte rapide est cruciale, l'AMSN observant une très grande réactivité des attaquants, toujours plus prompts à exploiter les vulnérabilités dès leur publication.

– 1109 avis de sécurité, documents faisant état de vulnérabilités sur des logiciels ou équipements informatiques et des moyens de s'en prémunir, ont été diffusés afin d'éviter la compromission des systèmes d'information (↗**+30%**).

RECYCLAGE DES SUPPORTS NUMÉRIQUES

En 2024, la Société Monégasque d'Assainissement (SMA) a détruit 1899 supports de données numériques (disques, bandes, clés USB, mémoires SSD, etc.), grâce à son offre DataDestruction accessible aux professionnels et particuliers.
Prestation entièrement réalisée sur le territoire monégasque par un personnel dédié et avec une traçabilité garantie, elle consiste en une destruction physique selon la norme DIN 66399 / ISO 21964. Les particules résultantes, totalement inutilisables, suivent ensuite la filière de recyclage des Déchets d'Équipements Électriques et Électroniques (D3E).

Résidus de supports numériques après broyage
suivant deux niveaux de destruction : P4 à gauche, P5 à droite.

LA STRATÉGIE NATIONALE POUR LA SÉCURITÉ DU NUMÉRIQUE

Publiée en 2016 et signée par le Ministre d'État, la stratégie nationale pour la sécurité du numérique reste d'actualité. Elle fixe les orientations qui sont mises en oeuvre par les services de l'État concernés :
– Les intérêts fondamentaux, la défense et la sécurité des systèmes d'information des institutions officielles de la Principauté et des infrastructures critiques, la gestion des crises informatiques majeures ;
– La confiance numérique, la vie privée, les données personnelles, la cybermalveillance ;
– Sensibilisation, formations initiales, formations continues ;
– Faire de la sécurité du numérique un facteur de compétitivité et de confiance ;
– Les liens internationaux et la stabilité du cyberespace.

Le rapport d'activité de l'AMSN permet de faire un point d'avancement annuel sur les objectifs fixés.

PROTÉGER LES INTÉRÊTS FONDAMENTAUX, LA SÉCURITÉ DES SYSTÈMES D'INFORMATION DES INSTITUTIONS OFFICIELLES DE LA PRINCIPAUTÉ ET DES INFRASTRUCTURES CRITIQUES, AINSI QUE LA GESTION DES CRISES INFORMATIQUES MAJEURES

La mise en place des mesures règlementaires de sécurité pour les Opérateurs d'Importance Vitale (OIV), débutée en 2018, s'est poursuivie en 2024. Certains secteurs d'activité sont plus avancés que d'autres. Les calendriers d'implémentation des mesures règlementaires ont été revus avec les OIV ; certains ont demandé une modification du calendrier car les chantiers étaient plus complexes qu'initialement prévu. Globalement, la mise en conformité devrait donc aboutir en 2025.

La protection des établissements, installations ou ouvrages exploités par les OIV a été renforcée et fait l'objet d'un plan particulier de protection qui doit être validé par la Direction de la Sûreté Publique, faisant suite à la publication de l'arrêté ministériel n° 2020-902 du 21 décembre 2020. A date, 33 Plans Particuliers de Protection ont été validés par la Direction de la Sûreté Publique.

Au 31 décembre 2024, 11 OIV bénéficient du service de détection des attaques mis en oeuvre par l'AMSN et opéré par le CERT-MC. Les raccordements vont se poursuivre en 2025.

Le CERT-MC a pris en charge 6 incidents de sécurité majeurs (↘**-63%**), à la suite de compromissions de systèmes d'information de l'État et des OIV, d'attaques par hameçonnage ou encore de fuite d'informations.

1109 avis de sécurité ont été diffusés en 2024 vers les OIV et les services de l'État. Ce nombre est en augmentation (↗**+30%**). Ces documents font état de vulnérabilités et des moyens de s'en prémunir, afin d'éviter la compromission des systèmes d'information concernés. 35 alertes urgentes ont été émises en parallèle pour les plus critiques d'entre eux.

En février 2024, la société Monaco Cyber Sécurité (MCS) a lancé son service de Security Operation Center (SOC) souverain. Ce service, proposé aux entités publiques et privées, analyse en quasi-temps réel les journaux d'événements générés par les systèmes d'information afin de détecter les tentatives d'attaques.

Un exercice national de cybersécurité, destiné à évaluer les capacités de réaction des services de l'État, s'est déroulé le mardi 25 juin 2024 au Centre National de Gestion de Crise, dans le cadre du plan d'organisation monégasque des secours (Or.mo.se).

DÉVELOPPER LA CONFIANCE DANS LE NUMÉRIQUE, LE RESPECT DE LA VIE PRIVÉE NUMÉRIQUE, LA PROTECTION DES DONNÉES PERSONNELLES ET L'APPRÉHENSION DE LA CYBERMALVEILLANCE

35 systèmes d'information de l'État ont fait l'objet d'une démarche d'homologation en 2024 afin de s'assurer de leur sécurisation. Par ailleurs, 33 systèmes d'information ont vu leur homologation renouvelée.

16 audits ont été effectués par des Prestataires d'Audit de la Sécurité des Systèmes d'Information (PASSI) qualifiés par l'AMSN, afin de vérifier le niveau de sécurité appliqué aux systèmes d'information de l'État.

Monaco Care Safety, service gratuit pour les clients de Monaco Télécom lancé en juillet 2019, offert par le Gouvernement Princier, permet d'obtenir 5 à 10 licences d'antivirus et un contrôle parental pour la navigation sécurisée sur Internet. Au 31 décembre 2024, 2231 clients « grand public » ont souscrit ce service (↗**+20%**) ; ces derniers ont ainsi sécurisé 3410 équipements (↗**+22%**).

Les lois n° 1.565 du 3 décembre 2024 relative à la protection des données personnelles et n° 1.566 portant approbation de ratification du Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ont été adoptées par le Conseil National dans sa séance du 28 novembre 2024 et publiées au Journal de Monaco le 13 décembre 2024. Ces textes prennent en compte la Convention 108+ du Conseil de l'Europe et le « paquet européen de protection des données » de l'Union européenne, c'est-à-dire, respectivement, le Règlement Général sur la Protection des Données (RGPD) et la Directive dite « Police-Justice ».

Attendue depuis plusieurs années, cette législation crée une nouvelle Autorité de Protection des Données Personnelles (APDP) avec des pouvoirs renforcés. Elle reprend les principes essentiels en matière de protection des données personnelles, renforce les droits des personnes concernées, supprime un très grand nombre de formalités préalables en vertu du nouveau principe de responsabilisation des acteurs en charge du traitement, encadre le recours à la sous-traitance et les transferts de données, introduit l'obligation de sécurité renforcée des données et des traitements et prévoit des sanctions renforcées.

DÉVELOPPER LES SENSIBILISATIONS ET LES FORMATIONS INITIALES ET CONTINUES

Le personnel de l'AMSN a suivi 20 formations spécialisées, en présentiel ou à distance. Ces formations se poursuivront en 2025, en particulier pour les nouveaux recrutements :

o 8 stages au CFSSI1 sur les thématiques suivantes :

- Audits techniques et organisationnels ;
- Gestion des incidents de sécurité ;
- Administration Windows sécurisée ;
- Sécurité des architectures virtualisées ;
- Analyste SOC.

o 3 formations sur le système de gestion des événements de sécurité Splunk ;
o 5 passeports annuels de formation donnant accès à une plateforme technique permettant de s'entrainer à la détection et à la gestion des menaces cyber ;
o 2 formations destinées aux managers de services de réponse à incident ;
o 2 formations à la gestion d'infrastructure de clés publiques (certificats électroniques).

Dans le cadre de la Politique de Sécurité des Systèmes d'Information de l'État, une campagne de sensibilisation à l'hameçonnage a été initiée en 2024 sur 434 agents de l'État. Cette sensibilisation, accessible en ligne, est composée de 14 modules de 1 à 3 minutes que chacun peut suivre à son rythme. Elle a pour objectif d'aider à reconnaître les tentatives d'hameçonnage, à adopter les bons réflexes face à ces attaques et à contribuer activement à la protection des données et des systèmes d'information de l'État. Cette campagne sera étendue à l'ensemble des agents de l'État en 2025.

FAIRE DE LA SÉCURITÉ DU NUMÉRIQUE UN FACTEUR DE COMPÉTITIVITÉ

Pour la sixième année consécutive, les entreprises monégasques étaient représentées aux « Assises de la Sécurité » autour de l'AMSN, sous l'enseigne de « MONACO CYBER SECURITY INITIATIVE ».

Cette participation permet à ces entreprises monégasques de prendre la place qui leur revient dans le monde de la cybersécurité et de démontrer que la Principauté est aujourd'hui un acteur à part entière dans ce domaine.

Les Assises ont réuni, lors de cette 24ème édition, 176 sociétés partenaires, 21 startups, 105 experts et journalistes et 3305 participants dont 1484 invités.

Au 31 décembre 2024, 6 entreprises sont qualifiées « Prestataire d'Audit de la Sécurité des Systèmes d'Information » (PASSI) et 38 auditeurs en sécurité des systèmes d'information ont obtenu leur attestation de compétence pour réaliser des audits en Principauté.

Stand de Monaco Cyber Security Initiative Assises de la sécurité 2024 Grimaldi Forum

[1] Centre de Formation à la Sécurité des Systèmes d'Information de l'Agence Nationale de la Sécurité des Systèmes d'Information française

INDICE MONDIAL DE LA CYBERSÉCURITÉ

Lancé en 2015 par l'Union Internationale des Télécommunications (UIT), agence spécialisée de l'Organisation des Nations Unies pour les technologies numériques, l'indice vise à aider les pays à identifier les domaines d'amélioration et à les encourager à agir pour renforcer leurs capacités suivant plusieurs axes.

Tous les 2/3 ans, l'UIT effectue une enquête sur le niveau d'engagement en matière de cybersécurité des pays membres.

L'indice a été continuellement adapté au fil des éditions pour répondre à l'évolution des risques, des priorités et des ressources, afin de fournir un aperçu plus pertinent des mesures de cybersécurité prises par les pays.

Lors de la 5ème édition, 194 pays ont répondu à l'enquête. La collecte, la vérification et la consolidation des informations ont été faites entre juin 2023 et juin 2024.

83 questions ont été abordées sur les différentes mesures mises en oeuvre par les pays selon cinq axes : juridique, technique, organisationnel, développement des capacités, coopération.

La note, sur 20, de la Principauté pour chacun des axes d'évaluation est :

Juridique	Technique	Organisationnel	Développement des capacités	Coopération
18.6	13.68	15.16	13.7	14.28

Cette note positionne la Principauté en milieu de peloton des pays de la zone Europe, incluant la Turquie, l'Ukraine et Israël.

En outre, les résultats de l'enquête permettent de définir certains axes d'amélioration.

Dans le domaine du développement des capacités, le dispositif cybermalveillance.gouv.mc, rendu possible par la signature du programme de coopération avec le GIP ACYMA en 2024, aura notamment pour missions :

– la prévention, l'accompagnement et l'assistance aux particuliers, aux entreprises et aux associations, victimes d'actes de cybermalveillance ;

– la sensibilisation du public sur les enjeux de la sécurité et de la protection de la vie privée numérique en lien avec les autorités compétentes et le développement de campagnes de prévention en la matière.

Dans le domaine de la coopération, la formalisation d'échanges et de partenariats existants permettra de mettre en visibilité les actions déjà menées par la Principauté.

FOCUS SUR L'ÉVOLUTION DE LA MENACE

Le CERT-MC exploite un réseau de capteurs sur le territoire de la Principauté qui lui permet d'identifier les menaces pesant sur les infrastructures critiques monégasques qui l'ont souhaité, et également de détecter les attaques.

Ce réseau de capteurs joue un rôle essentiel pour identifier les schémas d'attaques et permet une réaction rapide.

Dans les cas où une attaque aurait pu passer inaperçue, le réseau de capteurs permet, grâce à l'analyse des données de l'ensemble des infrastructures critiques, d'identifier les attaquants et leurs méthodes.

11 capteurs ont été déployés en Principauté depuis le lancement de ce service en 2020. Le raccordement de nouveaux capteurs va se poursuivre en 2025.

Pour arriver à leurs fins, les attaquants procèdent à la découverte des services numériques offerts par chaque serveur - on parle de reconnaissance - puis recherchent la présence de vulnérabilités exploitables qui leur permettent alors de s'introduire au sein de réseaux et d'en prendre le contrôle.

Les principales technologies qui ont été l'objet de cette reconnaissance en 2024 sont :

- Les bases de données (86%) : identifier une base de données ouverte sur Internet ou vulnérable peut permettre aux attaquants d'entrer en possession des multiples informations qu'elles contiennent et de les valoriser par la suite, soit par une revente, soit par leur exploitation dans le cadre de campagnes d'hameçonnage ou d'escroqueries par exemple.

- Les accès à distance (10%) : l'exploitation d'une vulnérabilité sur ces technologies permet de contrôler à distance le serveur ou la station de travail. Au regard des applicatifs testés (SSH, RDP), les attaquants recherchent aussi bien des systèmes Windows que Linux.

- Le contrôle d'accès (3%) : les technologies de contrôle d'accès font également l'objet de repérages de la page des pirates. Dans ce domaine, c'est principalement l'équipementier HID qui est visé avec sa technologie vertX. Les attaquants continuent de tester la présence de ces systèmes et des vulnérabilités qu'ils présentent, utilisant de codes d'exploitation disponibles sur Internet depuis près de 9 ans. Ces derniers permettent des actions malveillantes allant de la récupération des bases de données des badges, au verrouillage/déverrouillage des portes.

Parmi ces millions de tentatives effectuées en 2024, figurent des actions de reconnaissance beaucoup plus limitées en termes de volume, et plus ciblées en termes de technologies, qu'il faut traiter avec la même vigilance (Fortinet, Ivanti, Microsoft, Atlassian, etc.). Ces actions de reconnaissance permettent aux attaquants de découvrir des vulnérabilités présentes sur les systèmes examinés et d'en tirer profit pour s'introduire dans les systèmes d'information.

Comme pour les années précédentes, l'AMSN constate que les principales vulnérabilités ciblées par les attaquants ne sont pas nouvelles. Ces derniers continuent de tester des failles anciennes et connues, qui persistent sur les systèmes informatiques non mis à jour. A titre d'exemple, parmi les 4 vulnérabilités les plus visées en 2024, 2 d'entre-elles datent de 2017, 1 de 2021 et la dernière de 2014.

Une bonne hygiène informatique, des systèmes d'information à jour et l'application des correctifs de sécurité permet donc la plupart du temps d'éviter l'intrusion initiale qui évolue en compromission plus profonde.

L'année 2024 était particulière en termes de niveau de menace, en raison de l'organisation par

la France des Jeux Olympiques et Paralympiques. Malgré une intensité élevée des attaques enregistrées en France par l'ANSSI, et quelques compromissions sporadiques qui ont pu être contenues, le déroulement de ces jeux n'a globalement pas été perturbé.

L'AMSN a porté une vigilance accrue sur les infrastructures monégasques pendant cette période, mais n'a pas constaté d'augmentation particulière du rythme d'attaques sur les systèmes d'information supervisés.

Du point de vue de l'AMSN, le secteur qui a connu une augmentation significative de la reconnaissance et des tentatives d'attaques en 2024 est celui de la santé (+122% sur la reconnaissance par rapport à 2023). Les attaques enregistrées ciblent particulièrement les équipements réseau de bordure, comme les firewalls.

Le secteur santé est, depuis plusieurs années, une cible pour les attaquants, quel que soit le pays, en raison d'infrastructures pour certaines vieillissantes, de l'utilisation de matériels peu suivis au niveau sécurité, utilisant des protocoles anciens et non sécurisés et constituant souvent le maillon faible permettant l'accès au réseau hospitalier auxquels ils sont connectés.

Agence Monégasque de Sécurité Numérique

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