Recommandations relatives à la règle 9 de l'A.M. n° 2018-1053

Version : 1.4.0
Date : 31/10/2019

24, rue du Gabian
98000 MONACO
Tél. : (+377) 98 98 24 93
amsn@gouv.mc

Index

1- Contexte réglementaire

L'Arrêté Ministériel n° 2018-1053 du 8 novembre 2018 définit dans son annexe, 21 règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs d'importance vitale.

La règle 9 de cette annexe, relative au traitement des incidents de sécurité est définie comme telle :

« L'opérateur d'importance vitale élabore, tient à jour et met en œuvre une procédure de traitement des incidents affectant le fonctionnement ou la sécurité de ses systèmes d'information d'importance vitale (SIIV), conformément à sa politique de sécurité des systèmes d'information.

L'opérateur ou le prestataire mandaté à cet effet procède au traitement des incidents en s'appuyant sur les recommandations publiées par l'Agence Monégasque de Sécurité Numérique.

Un système d'information spécifique, isolé d'internet, doit être mis en place pour traiter les incidents, notamment pour stocker les relevés techniques relatifs aux analyses des incidents. Ce système spécifique de traitement des incidents est cloisonné vis-à-vis du SIIV concerné par l'incident.

L'opérateur conserve les relevés techniques relatifs aux analyses des incidents pendant une durée d'un an. Il tient ces relevés techniques à la disposition de l'Agence Monégasque de Sécurité Numérique.

Les relevés techniques ainsi réunis sont des documents susceptibles de contenir des informations soumises au secret professionnel dont la divulgation est réprimée par les dispositions de l'article 308 du Code pénal. Ils sont, le cas échéant, couverts par le secret de sécurité nationale tel que prévu par la loi n° 1.430 du 13 juillet 2016, précitée. »

Le présent document formule un certain nombre de recommandations relatives à la mise en place du système d'information spécifique, dédié au traitement des incidents de sécurité par les opérateurs d'importance vitale. Dans la suite de ce document l'opérateur d'importance vitale sera désigné sous le terme « opérateur ».

2- Définition

2.1- RELEVES TECHNIQUES

Les relevés techniques dont il est fait mention dans l'arrêté 2018-1053 sont les éléments techniques utiles à la résolution de l'incident, relevés par l'opérateur ou son prestataire, ainsi que ceux relevés par l'AMSN et remis à l'opérateur pour conservation.

Ils sont définis ci-après :

- Images/Acquisitions de supports de stockage ;
- Images/Acquisitions de machines virtuelles ;
- Images/Acquisition de mémoire vive ;
- Journaux historiques des événements (logs) des systèmes ;
- Journaux historiques des événements (logs) des périphériques réseau;
- Fichiers d'enregistrement de traces réseau (fichiers PCAP).

En sus des relevés purement techniques, le poste isolé doit pouvoir permettre de lire, rédiger et stocker les rapports et correspondances échangés dans le cadre du traitement de l'incident qui seront transmis en utilisant les moyens de chiffrement définis au paragraphe 3.4.3-. A cet effet sera donc installée sur le poste isolé une suite bureautique, comme mentionné dans le paragraphe 3.5.1-.

Il est demandé à l'opérateur de ne pas stocker la cartographie ou l'inventaire du parc informatique sur ce poste isolé, sauf à appliquer les règles de l'Arrêté Ministériel n°2019-791 du 17 septembre 2019.

2.2- DUREE DE CONSERVATION

Comme le définit la règle 9, la durée de conservation des relevés techniques par l'opérateur d'importance vitale est fixée à un an.

La date de début de conservation est fixée à la date de déclaration d'incident par l'opérateur.

3- Recommandations

3.1- MATERIEL

L'ordinateur isolé est dédié au traitement des incidents de sécurité. En aucun cas il ne sera utilisé pour assurer une autre fonction.

La machine utilisée sera, de préférence, constituée d'un ordinateur portable, plus facile à déployer, et mettre sous clé. Elle pourra si besoin être transportée dans les locaux de l'AMSN pour faciliter l'échange mutuel de données avec l'agence.

S'il s'agit d'un portable utilisé sous système d'exploitation Windows, il sera utile d'opter pour un modèle équipé d'une puce TPM permettant d'accroitre le niveau de protection du système.

L'accès au paramétrage BIOS/UEFI de ce poste sera restreint par mot de passe. Le mot de passe sera conservé dans un coffre sous enveloppe scellée. A aucun moment, ce mot de passe ne devra être stocké en format numérique sur le système d'information de l'opérateur, sous quelque forme que ce soit.

Durant la période de traitement d'un incident de sécurité, le poste isolé devra disposer d'une imprimante dédiée, connectée par l'intermédiaire d'une prise USB. Aucune imprimante réseau ne sera employée, celles-ci disposant fréquemment de disques durs pour assurer le stockage temporaire des données imprimées. Les imprimantes wifi sont, elles-aussi, à proscrire.

Si le poste dédié au traitement de l'incident est employé dans des locaux non sécurisés, il sera utilement équipé d'un système antivol de type Kensington.

3.2- CONFIGURATION RESEAU

Par nature, le poste isolé ne doit être connecté à aucun moment au système d'information de l'opérateur. Il conviendra de désactiver les fonctionnalités de réseau sans fil (WLAN et Bluetooth) au niveau du BIOS/UEFI de la machine.

Si aucun incident n'est en cours de traitement, le poste peut être connecté à un réseau internet dédié de manière occasionnelle, et pour la durée strictement nécessaire aux opérations de mises à jour du système et de l'antivirus.

A compter du déclenchement d'un incident de sécurité, le poste isolé doit être déconnecté de tout réseau et ne devra plus être reconnecté avant que l'incident ait été intégralement traité.

3.3- SYSTEME D'EXPLOITATION

3.3.1- Type du système

Il est impératif que le système d'exploitation installé sur le poste soit un système récent, dont le suivi des mises à jour de sécurité est assuré par l'éditeur pendant une période suffisamment longue.

Si le poste isolé est équipé d'un système Windows, l'opérateur optera pour une version 10.

Un ordinateur Apple peut également être utilisé. Dans ce cas, il devra être équipé de la dernière version de MacOS (version 10.15 Catalina à la date de rédaction du présent document).

Si le système utilisé est de type Linux, il conviendra d'opter pour un système bénéficiant d'un support long terme (LTS).

3.3.2- Pare-feu

Le poste dédié, même s'il n'est connecté que de manière sporadique à un réseau pour des raisons de mises à jour, devra être équipé d'un pare-feu.

Les systèmes d'exploitation disposent d'outils natifs qui peuvent être utilisés à cet effet (firewall Windows, Linux IP Tables, firewall Mac).

L'opérateur qui le souhaite pourra substituer à ces outils des logiciels gratuits ou commerciaux qu'il maitrise ou dont il dispose au sein de son entité. Dans ce cas, les outils utilisés doivent pouvoir assurer, a minima, les mêmes fonctions que les outils pare-feu natifs des systèmes.

3.3.3- Mise à jour du système et de l'antivirus

Hors période de traitement d'un incident de sécurité, lorsqu'aucune donnée sensible ne figure sur le poste isolé, les mises à jour du système d'exploitation et de l'antivirus s'effectuent en connectant le poste une fois par mois, à un accès internet distinct du système d'information de l'opérateur. Le poste sera connecté de manière temporaire, pour une durée strictement limitée à l'exécution de ces opérations de mise à jour.

Une fois les mises à jour terminées, le poste sera déconnecté de cet accès internet dédié.

3.4- CHIFFREMENT DES DONNEES

3.4.1- Chiffrement des disques durs

Les disques durs du poste isolé seront chiffrés intégralement (partition système comprise), à l'aide d'un système de chiffrement natif au système d'exploitation (Bitlocker pour Windows, LUKS pour linux, Filevault pour Mac).

Les mots de passe permettant d'accéder à ces volumes chiffrés seront conservés dans un coffre sécurisé. À aucun moment, ces mots de passe ne devront être stockés en format numérique sur le système d'information de l'opérateur, sous quelque forme que ce soit.

3.4.2- Chiffrement des supports externes

Si des disques externes (USB, FireWire) doivent être utilisés pour stocker les relevés techniques ou effectuer des sauvegardes de ces éléments, ils seront eux aussi protégés par les mêmes systèmes de chiffrement natifs.

À l'instar du poste dédié, ces supports externes devront être conservés également sous clé.

3.4.3- Chiffrement des échanges de données

Le poste isolé étant par nature déconnecté de tout réseau, il ne pourra pas être utilisé pour transmettre de manière directe par internet les relevés techniques.

Pour communiquer à l'AMSN, à un prestataire ou à des tiers clairement identifiés, les relevés techniques relatifs à l'incident, l'opérateur utilisera un des deux systèmes de chiffrement de données :

- ZED!
- PGP/GnuPG

Il conviendra donc d'avoir, préalablement au déclenchement de l'incident, installé ces outils sur le poste isolé, et les avoir pris en main.

L'AMSN a mis en ligne sur son site internet sa clé publique PGP. Cela permet à l'opérateur de lui transmettre de manière chiffrée les éléments. La clé PGP est disponible à l'adresse suivante :

- https://amsn.gouv.mc/CERT-MC/

3.5- LOGICIELS COMPLEMENTAIRES

3.5.1- Suite bureautique

Pour pouvoir prendre connaissance des rapports produits par l'AMSN ou le prestataire et rédiger ses propres comptes rendus, l'opérateur doit installer sur ce poste la suite bureautique de son choix :

- Microsoft Office
- Libre Office

Il sera nécessaire de disposer également d'une visionneuse PDF et d'une visionneuse d'images, documents dont les formats sont couramment utilisés pour l'échange d'informations.

3.5.2- Logiciels d'analyse de traces numériques

Enfin, dans le cadre du traitement de l'incident, il pourra être demandé ponctuellement par l'AMSN à l'opérateur d'effectuer des recherches sommaires dans les relevés techniques effectués par ailleurs. (journaux de logs, traces réseau)

Il est donc recommandé à l'opérateur de s'assurer de l'installation sur le poste isolé, a minima des logiciels suivants :

- Recherche dans les logs :
  - GLOGG (multiplateforme) : https://glogg.bonnefon.org/
- Recherche de texte
  - GREP (natif sous linux et mac)
  - FINDSTR (sous Windows), ou logiciels équivalents à GREP
- Analyse de traces réseau :
  - Wireshark (multiplateforme) : https://www.wireshark.org/