REAGIR A UNE ATTAQUE INFORMATIQUE :

10 PRECONISATIONS.

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

Préambule

Lorsqu'un incident se produit au sein d'un système d'information (SI), il peut engendrer des conséquences plus ou moins graves et variées.

La nature de l'incident détermine s'il y a lieu de le porter à la connaissance de l'Agence Monégasque de Sécurité Numérique (AMSN) et/ou à la Commission de Contrôle des Informations Nominative (CCIN), voire d'entreprendre une action en justice par voie de dépôt de plainte auprès de la Direction de la Sûreté Publique ou auprès du Parquet Général.

Préalablement à cette étape, il est important de s'assurer de la nature de l'incident (intentionnel ou accidentel), de vérifier qu'il n'est pas consécutif à une défaillance matérielle, ni à une opération de maintenance liée à la politique de mises à jour au sein du SI.

Les questions qui se posent à l'entité ou la personne concernée par l'incident (entreprise, service,…) :

- Suis-je face à une attaque informatique : un acte de malveillance, un sabotage, un piratage, … ?
- Est-ce un incident en cours ou passé ?
- Que dois-je faire et si j'agis quelles mesures dois-je prendre ?
- Puis-je restaurer mon SI dans son état initial sans risque pour la sauvegarde ?
- Vers qui dois-je me tourner pour rapporter l'incident sur le plan technique et sur le plan juridique ?
- Qui peut déposer plainte et comment ?
- Comment procéder pour réparer ?

Sur le plan juridique, beaucoup de questions sont en relation avec la collecte de la preuve numérique, sa valeur probante, son authenticité, son intégralité et sa sécurité.

Les préconisations contenues dans ce document constituent les repères essentiels pour appréhender la marche à suivre après des incidents caractérisés d'origine délictueuse.

1. Préconisation n° 1 : Définir la nature de l'incident

La Principauté possède désormais un arsenal juridique complet et une agence spécialisée dans la sécurité numérique.

1.1. Les infractions de cyber sécurité se classent en plusieurs catégories :

- Les infractions proprement liées à des défauts de sécurité dans les SI, tels que :
  - L'atteinte à l'image par défiguration de site, ou par déni de service des SI
  - L'espionnage dans les SI
  - Le sabotage de SI
- Les infractions commises via les systèmes informatiques, tels que
  - L'arnaque au président
  - L'utilisation frauduleuse de carte bancaire
  - Etc..

1.2. La lutte contre la cybercriminalité s'organise notamment autour des textes législatifs et réglementaires suivants :

- loi n°1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;
- loi n°1.430 du 13 juillet 2016 portant diverses mesures relatives à la préservation de la sécurité nationale ;
- loi n° 1.402 du 5 décembre 2013 portant approbation de ratification de la Convention sur la cybercriminalité du Conseil de l'Europe ;
- loi n°1.383 du 02 août 2011 sur l'économie numérique ;
- loi n°1.165 du 23 décembre 1993, modifiée, relative à la protection des informations nominatives ;
- les Ordonnances Souveraines et les arrêtés ministériels pris pour l'application de ces lois.

2. Préconisation n° 2 : Une attaque informatique a eu lieu, quelles sont les démarches techniques envisageables ?

S'il y a une suspicion d'attaque informatique, il est important que des constatations techniques soient effectuées dans les meilleurs délais.

Plusieurs solutions sont envisageables :

- Contacter la Direction de la Sûreté Publique pour faire intervenir un spécialiste en cybercriminalité aux fins de constatations immédiates ;
- Procéder soi-même aux constatations ;
- Faire appel à un huissier ;
- Faire appel à l'Agence Monégasque de Sécurité Numérique ;
- Faire appel à un prestataire qualifié dans la réponse à incident[1] ;
- En cas de suspicion de vol de données, informer la Commission de Contrôle des Informations Nominatives.

Ces démarches ne sont pas exclusives les unes des autres ni d'un dépôt de plainte devant un officier de police judiciaire.

[1] Voir https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-reponse-aux-incidents-de-securite-pris/

3. Préconisation n° 3 : Quelles mesures conservatoires prendre au sein du Système d'Information ; à qui confier ces missions ? Quelles informations communiquer aux services enquêteurs ou spécialisés, aux personnels ?

Même sans connaitre précisément la nature de l'incident, son origine et son impact réel, des mesures d'urgence doivent être prises afin de limiter les dommages et préserver les traces utiles :

3.1. Confiner

- Mettre en quarantaine les postes informatiques concernés par l'incident si celui-ci est bien apparent. Dans le cas d'une attaque sophistiquée il peut être préférable de ne pas isoler les postes concernés afin de ne pas donner d'alerte à l'attaquant en lui faisant comprendre qu'il est repéré (il pourrait dans ce cas faire disparaitre des traces qui donneraient des informations sur la méthode utilisée pour l'attaque et ainsi recommencer plus tard)
- Ecarter et protéger les supports informatiques qui pourraient servir à la propagation de l'attaque ou qui sont concernés par celle-ci (clé USB, disque dur amovible, DVD, CD,…) toujours en prenant soin de vérifier qu'il n'y a pas trop de risque d'éveiller l'attention de l'attaquant.

N'HESITEZ PAS A DEMANDER L'AVIS DE L'AMSN.

3.2. Isoler

Couper tous les accès réseaux sauf si cela peut mettre en éveil l'attaquant, par contre ne pas hésiter à couper les connections vers les autres systèmes pour éviter la propagation si vous êtes sûr que les autres systèmes ne sont pas encore atteints.

3.3. Sauvegarder :

- Les journaux d'activités (connexions, web, évènements systèmes,…) ;
- Les documents, emails, fichiers,… ;
- Le trafic réseau supervisé (firewalls, IDS, etc…) ;
- Original ou copie de supports informatiques ;
- Fichiers de mise à jour.

3.4. Collecter les renseignements internes :

- Auprès des premières personnes à avoir détecté l'incident et à avoir donné l'alerte ;
- Auprès des personnes témoins de l'incident.

3.5. Collecter les éléments externes :

- Auprès des prestataires de services ;
- Auprès des opérateurs de télécommunications
- Auprès des prestataires de maintien en condition opérationnel ou en condition de sécurité des matériels

3.6. Communiquer :

- Auprès du personnel de l'entreprise directement concerné, en veillant à ne pas laisser se répandre l'information d'une attaque ;
- Préparer un plan de communication avec les autorités et tous les intervenants sur le traitement de cette attaque pour le cas où l'information devienne publique.

Ces dispositions seront prises en compte par les services informatiques et les responsables de la sécurité informatique mais ces dispositions doivent être validées par les plus hautes autorités ou responsables qui doivent s'impliquer personnellement sur ces sujets.

Le processus de gestion d'un incident ne peut s'improviser. Il doit être organisé, en avance de phase, avec :

- Des procédures
- Des moyens matériels (stockage, PRA, PCA, …) ;
- Des moyens humains (identification des rôles, renfort, contrat avec des sociétés qualifiées par l'AMSN,…).

3.7.Les informations utiles pour la DSP et l'AMSN seront principalement :

3.7.1. La topologie du système :

- Descriptif de l'architecture du SI
- Caractéristiques des matériels en place
- Nombre et méthode de connexion du système à des réseaux

3.7.2. L'historique :

- Contexte de l'incident
- Evolution dans le temps
- Début et éventuellement fin de l'incident

3.7.3. L'observation :

- De l'ensemble des données réseaux (protocoles, statistiques de flux, …)
- Du comportement du système et du réseau

3.7.4. La documentation

- Toute la documentation du réseau
- Toute la documentation du SI
- Tous les détails et analyse de l'incident.

La rapidité de réaction et de gestion de l'incident est évidemment cruciale, mais ne pas confondre vitesse et précipitation.

4. Préconisation n°4 : comment préserver la preuve numérique et valider son authenticité, son intégrité, sa probité ?

Le travail d'analyse d'un incident peut dans certains cas, modifier voire effacer les traces laissées par l'attaquant.

Il deviendra alors difficile de différencier celles laissées par l'attaque et celles générées par le traitement de l'attaque. Il est donc préférable de figer le système voire de le laisser fonctionner comme si de rien était et de faire une copie des données utiles avant de résoudre l'incident. A titre d'exemple : réinstaller rapidement le système ne garantit aucunement que l'attaquant ne soit pas toujours présent voire qu'il ne va pas revenir par le même procédé que lors de l'attaque initiale.

La valeur des informations collectées dépend de la manière dont elles ont été acquises. La méthode de collecte varie selon le type d'informations ciblées.

A titre d'exemple :

- En cas de copie d'un support (disque dur, clé USB,…) la copie intégrale, dit « bit à bit » est à privilégier
- En cas de sauvegarde de données réseaux, il est souhaitable de fournir à la Direction de la Sûreté Publique et l'Agence Monégasque de Sécurité Numérique la totalité des journaux de connexion et non les seules données relatives à l'attaque, en prévision d'une aide à la compréhension de l'attaque et d'une contre-expertise éventuelle.
- En cas de fourniture de données provenant d'un prestataire de service, il conviendra d'identifier précisément ce dernier qui attestera de leur origine.

Il est nécessaire de préciser clairement la liste des personnes qui procèdent à la collecte de ces données ainsi que les procédures appliquées.

En fonction des enjeux, il pourra être utile de réaliser ces actes en présence d'un membre de l'Agence Monégasque de Sécurité Numérique, de la Direction de la Sûreté Publique voir d'un huissier de justice pour le traitement juridique.

Sur le plan juridique, les informations fournies doivent avoir été obtenues légalement. Par exemple : accéder frauduleusement au système de l'attaquant dans le but d'obtenir des informations constitue une infraction sauf pour l'autorité administrative habilitée.

Les travaux d'investigation techniques ou judiciaire se font sur des copies de sauvegardes. Les données originales seront protégées et conservées dans des conditions spécifiques afin, pour la justice, d'avoir les éléments originaux et pour l'AMSN de retrouver les éléments techniques d'origine si besoin.

5. Préconisation n°5 : Quels sont les moyens techniques de collecte de la preuve numérique ?

La preuve numérique revêt plusieurs aspects qu'il convient de maîtriser avant d'entreprendre sa collecte.

La compréhension de ses caractéristiques permet de ne pas commettre d'erreurs irrémédiables au moment de son acquisition.

La preuve numérique est :

- Physique : elle est fixée sur un support de stockage, persistante indépendamment de l'alimentation électrique.
- Logique : elle n'existe que sous la forme binaire (suite de « 0 » et « 1 ») représentant l'information et traduite par un système d'exploitation et des applications correspondantes.
- Volatile : car elle se trouve au sein d'un stockage dépendant de l'alimentation électrique (mémoire et réseau).
- Polymorphe : elle est à l'état brut, formatée, chiffrée, compressée, exécutable.

La collecte de preuve numérique peut être faite « in vivo » sur un système d'information en état de fonctionnement (mémoire vive ou réseau).

La collecte de preuve peut être effectuée « post-mortem », le système d'information est arrêté. Attention, tout ce qui est volatile a disparu.

Cette approche conditionne la méthodologie de copie.

Des contraintes opérationnelles s'ajoutent au processus de collecte de la preuve numérique telles que :

- Des problèmes sécuritaires pour les personnes et les données elles-mêmes, peuvent entraver la collecte de la preuve ;
- La durée d'acquisition des preuves peut- être démesurément longue ;
- Des limitations techniques liées au volume des supports (en téra, péta- octets) le chiffrement, l'accessibilité par des mots de passe, etc.

Principes fondamentaux de la collecte de la preuve :

- ➡ MÉTHODOLOGIE ET TECHNICITÉ
- ➡ PRÉSERVER L'ÉTAT INITIAL DE LA PREUVE
- ➡ ÉVITER L'ALTÉRATION OU DESTRUCTION DE LA PREUVE
- ➡ BLOQUER L'ÉCRITURE SUR LE SUPPORT SOURCE (ORIGINAL)
- ➡ UTILISATION D'OUTILS SPÉCIFIQUES COMMERCIAUX

6. Préconisation n°6 : Vers qui se tourner pour déposer plainte et remettre les preuves collectées ?

Le dépôt de plainte est l'étape préalable à l'ouverture d'une enquête judiciaire.

Toute personne morale ou physique qui s'estime victime peut déposer plainte, que l'auteur des faits soit identifié ou non. Dans ce dernier cas, la plainte est déposée contre X.

6.1. Délais pour porter plainte

Le plaignant dispose de délais au-delà desquels il perd ses droits à saisir la justice pénale (prescription).

Sauf situation particulière, ces délais sont les suivants :

1 an pour les contraventions,

3 ans pour les délits,

10 ans pour les crimes.

La majorité des infractions à la cyber- criminalité sont des délits.

En matière d'infractions cybercriminelles, la plainte doit être déposée dans les plus brefs délais en raison des temps de conservation des données numériques des différents prestataires susceptibles d'être sollicités par les services enquêteurs.

6.2. Vers quels services se tourner pour déposer plainte ?

La Direction de la Sécurité Publique

Au sein de cette direction, des investigateurs sont spécialisés dans la lutte contre la cybercriminalité.

Vous pouvez également déposer une plainte auprès du procureur par courrier avec ou sans constitution de partie civile.

7. Préconisation n°7 : Faut-il un statut particulier pour déposer plainte ? Quels éléments communiquer lors du dépôt de plainte ?

7.1. Qui peut déposer plainte ?

Seule la direction de l'organisme ou une personne mandatée est habilitée à déposer plainte en qualité de représentant légal.

7.2. Quels documents apporter ?

Les documents attestant de l'identité du plaignant et de celle de la personne morale concernée :

Il conviendra de produire une pièce d'identité, un document attestant de l'existence juridique de la personne morale : extrait du registre du commerce de moins de trois mois (pour une société ou les statuts pour une association.

En l'absence de mandat du représentant légal, un pouvoir spécial autorisant le dépôt de plainte est nécessaire.

7.3. Les éléments intéressant l'enquête :

- Descriptif précis de l'incident ;
- Communiquer les coordonnées de l'ensemble des intervenants ou prestataires susceptibles d'apporter des informations aux enquêteurs ;
- Communiquer l'ensemble des éléments techniques qui ont pu être collectés: traces informatiques des dégâts engendrés par l'attaque (exemple : logs de connexion), l'adresse précise de la ou les machine(s) attaquée(s) (préciser s'il s'agit d'un poste de travail professionnel, d'un mobile ou encore d'une attaque du site internet, du serveur hébergé auprès d'un fournisseur d'accès internet).
- L'Agence Monégasque de Sécurité Numérique a-t-elle été prévenue ?
- L'architecture du réseau informatique.
- Tout élément susceptible d'être utile à l'enquête: les mails en lien avec l'infraction, l'organigramme de la société, liste du personnel, coordonnées des différents prestataires (hébergeur, société de sécurité).

Lors du dépôt de plainte, il peut être opportun d'être accompagné du responsable de sécurité informatique ou de la personne désignée pour la gestion de l'incident.

A l'issue du dépôt de plainte, un récépissé sera remis au plaignant.

8. Préconisation n°8 : Que se passe-t-il après le dépôt de plainte ?

Dès le dépôt de plainte, l'infraction commise ou tentée est portée à la connaissance du Procureur Général qui apprécie la suite judiciaire à donner.

Selon la décision du magistrat, les agents ou officiers de police judiciaire diligenteront des investigations, en collaboration avec un spécialiste en cyber- criminalité.

Quelles sont les attentes des enquêteurs ?

Les enquêteurs peuvent être amenés à se transporter dans les locaux de l'entreprise pour :

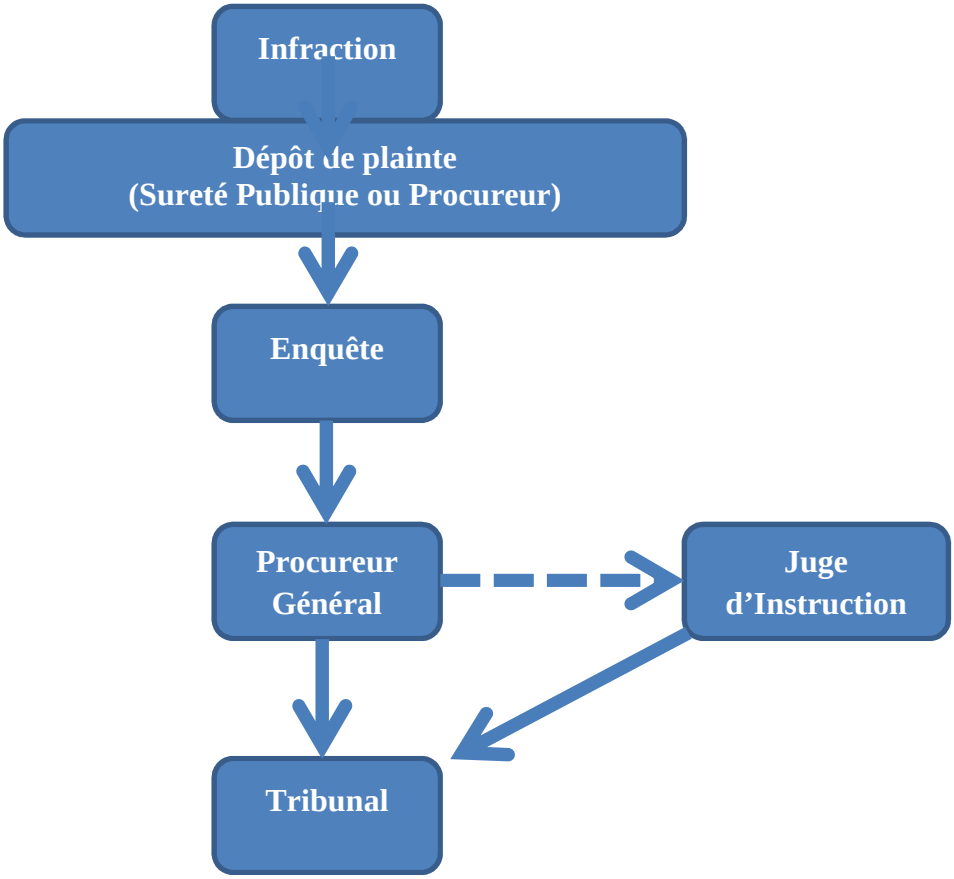
- analyser au besoin les ordinateurs des salariés, avec leur accord ou celui de l'employeur (notamment pour déceler une infection par malware) ;

- réaliser une copie des supports numériques ayant un intérêt pour l'enquête ;

- auditionner des personnes qualifiées (techniciens informatiques, responsable de la sécurité des systèmes d'information...), des témoins ou éventuellement des suspects ;

- accéder à certains lieux ou bureaux de l'entreprise, notamment lorsque l'attaque ou l'infraction a été commise par une personne de l'entreprise ou un sous-traitant ayant eu un accès à l'organisme.

9. Préconisation n°9 : Quelles sont les suites judiciaires de l'enquête ?



Comment obtenir réparation du préjudice ?

Il est important de distinguer les investigations pénales, réalisées à partir de la plainte, du préjudice financier argué. En effet, la plainte permettra de déclencher une enquête pour rechercher les auteurs de l'infraction et les traduire devant la justice.

S'agissant de la réparation du préjudice, deux solutions sont envisageables :

- soit l'entreprise se rapproche de son assurance ou de l'opérateur (notamment en cas de piratage de PABX / IPBX), pour envisager une compensation des pertes subies ;

- soit l'entreprise joint à sa plainte une constitution de partie civile, pour que le tribunal statue à la fois sur les sanctions pénales prononcées à l'encontre des auteurs et sur le montant des réparations allouées à la victime.

10. Préconisation n°10 : Anticiper, prévenir ; qu'est-il possible de faire pour améliorer la sécurité du Système d'Information afin de réduire les risques et menaces ?

10.1. Suivre les recommandations de l'AMSN

10.2. En particulier : mettre en place une politique de sécurité des systèmes d'information (cybersécurité) PSSI

La cybersécurité est un thésaurus qui rassemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, technologies qui peuvent être utilisés pour protéger le cyber-environnement et les actifs des organisations, entreprises et des utilisateurs.

10.3. Protéger les actifs

Les actifs (savoir-faire, dossiers sensibles, technologies, recherches, etc.) des organisations, des entreprises et des utilisateurs sont détenus dans les dispositifs informatiques connectés tels que l'infrastructure, les applications, les services, les systèmes de télécommunication et la totalité des informations transmises dans le cyber-environnement, sans oublier le personnel.

La cybersécurité cherche à garantir que la sécurité de ces actifs est assurée et maintenue par rapport aux risques et menaces pouvant affecter ceux-ci.

Les objectifs généraux en matière de sécurité sont les suivants :

✔ Disponibilité

✔ Intégrité

✔ Authenticité

✔ Non-répudiation

✔ Confidentialité

Pour cela l'AMSN rappelle les principes de bases.

Quelques principes de base

Il faut :

- Voir plus loin que la technologie ;
- Penser à la mise en conformité légale, aux aspects juridiques de l'information et de la sécurité;
- Faire une analyse de risque et accepter les risques résiduels
- La direction de l'entreprise doit soutenir la Direction des Systèmes d'Information dans la mise en place d'une politique de sécurité des systèmes d'information ;
- Dédier une ressource humaine Responsable de la Sécurité des Système d'Information (RSSI);
- Prévenir et former le personnel à la Sécurité des Systèmes d'Information ;
- Rester maître de son Système d'Information ;
- Toujours se remettre en cause ;
- Poser les fondamentaux : qu'est-ce qui est vital au sein de mon Système d'Information pour le fonctionnement a minima de mon entreprise ?
- Être prêt à faire face à l'incident, avoir une stratégie de réponse.

Mots clés

✔ Protection

✔ Détection

✔ Réaction

✔ Rétablissement

Que faire face aux risques et aux menaces en 10 bonnes actions ?

1. Bien communiquer sur la Sécurité des Systèmes d'Information: informer, sensibiliser, prévenir et former la direction et le personnel (charte de bon usage du Système d'Information, guide d'hygiène informatique) ;
2. Toujours maintenir le Système d'Information à jour (systèmes d'exploitation, antivirus, firewalls, applications) ;
3. Protéger les données stockées et transmises par des accès contrôlés et chiffrés ;
4. Sécuriser les équipements nomades (portables, tablettes,) et éviter l'usage mixte «professionnel / personnel» ;
5. Limiter l'accès aux informations les plus sensibles à un nombre restreint de personnes ;

6. Fixer des règles de bon usage de l'internet et mettre en place des dispositifs de filtrage adaptées (listes noires/listes blanches) ;
7. Mettre en place une politique de droits d'accès par des mots de passe fort régulièrement changés, avec des identifiants uniques et exclusifs ;
8. Mettre en place des systèmes de sauvegarde contrôlés et redondants ;
9. Contrôler et tester régulièrement le niveau de sécurité du Système d'Information (tests d'intrusion, tests antivirus, etc…) ;
10. Savoir prévenir, agir et avoir une stratégie de retour à une situation normale en cas d'incident : cataloguer, catégoriser ; capitaliser la connaissance.