SOUS-DIRECTION DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ

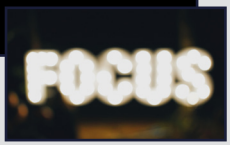
L'ENQUÊTE
EN CYBERCRIMINALITÉ

5 ÉTAPES À RESPECTER LORS D'UNE ATTAQUE INFORMATIQUE

SOUS-DIRECTION DE LA LUTTE CONTRE LA CYBERCRIMINALITÉ
POLICE NATIONALE


POLICE NATIONALE
POLICE
©DGPN-SICOP


fabrice Balsamo
GENDARMERIE NATIONALE


FOCUS

ÉTAPE 1 : COMMENT FAIRE LE POINT ?

Une attaque informatique a eu lieu, qui va effectuer les premières constatations techniques ?

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

Plusieurs solutions peuvent être mises en place :

- Contacter un service de police ou de gendarmerie pour faire intervenir un spécialiste en cybercriminalité aux fins de constatations immédiates ;

  ou

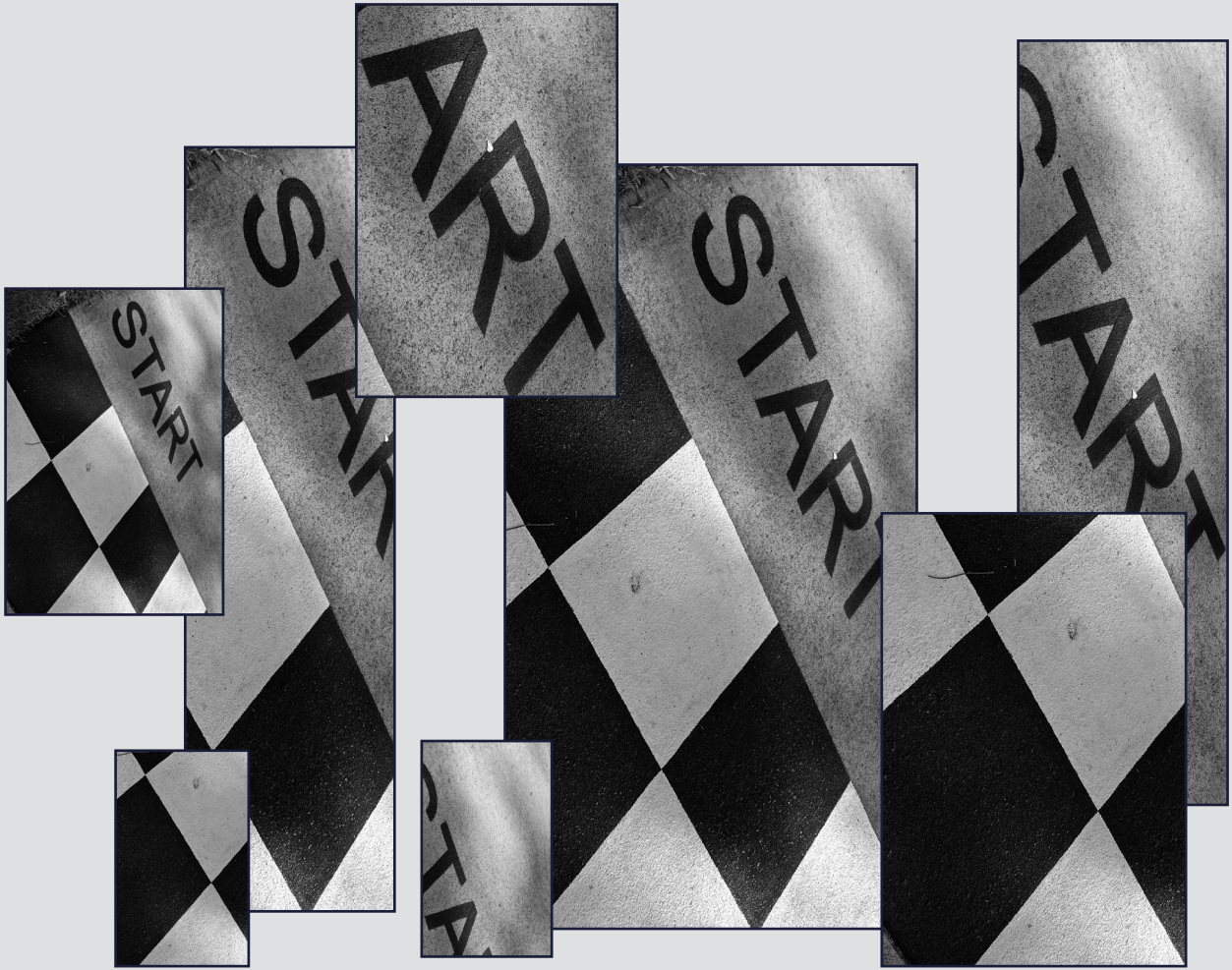
- Procéder soi-même aux constatations ;

  ou

- Faire appel à un huissier ;

  ou

- Faire appel à un expert ou une société spécialisée dans la réponse à incident. Le dispositif d'assistance aux victimes d'actes de cybermalveillance (https://www.cybermalveillance.gouv.fr) peut vous aider à faire les premières constatations ou à trouver un prestataire informatique proche de chez vous susceptible de pouvoir vous assister.


START
START
START
START

ÉTAPE N° 2 : COMMENT RÉAGIR ?

Quelles sont les premières actions à mettre en place ?

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

➤ **Isoler :**

• Ne pas débrancher le poste informatique mais couper immédiatement tous les accès réseaux pour stopper l'incident ;

Nota : *Il est important, dans une démarche de collecte d'éléments utiles à l'analyse et à l'enquête, de ne pas éteindre les machines impactées afin de permettre la récupération des données qui disparaissent lorsque l'alimentation électrique est interrompue (mémoire volatile).*

➤ **Confiner :**

• Mettre en quarantaine les postes informatiques concernés par l'incident ainsi que les supports amovibles ;

• Ecarter et protéger les supports informatiques concernés par l'incident : clé USB, CD, DVD, disques durs (internes/externes).

➤ **Sauvegarder :**

• Les journaux d'activités (connexions Web, événements systèmes, etc.) ;

• Les documents, emails, fichiers ;

• Le trafic réseau supervisé (firewalls, IDS, etc.) ;

• Procéder à une copie des supports informatiques ;

• Procéder à l'acquisition de mémoire vive sur les machines impactées.

➤ **Collecter les renseignements internes :**

• Auprès des premières personnes à avoir détecté l'incident et à avoir donné l'alerte ;

• Auprès des employés témoins de l'incident.

➤ **Collecter les renseignements externes :**

• Auprès des prestataires de services (télécommunications, développement d'application, maintenance matériels, etc.).

ÉTAPE N° 2 : COMMENT RÉAGIR ?

➤ **Communiquer :**

• aux personnels ciblés de l'entreprise les recommandations adaptées à la gestion de l'incident et déclinées par l'unité chargée de la sécurité des systèmes d'information ;

• à la CNIL lorsqu'on est en présence d'une violation de données à caractère personnel et qu'elle est susceptible d'engendrer un risque pour les droits et libertés des personnes physiques concernées (article 33 du règlement général sur la protection des données) ;

La notification doit être transmise par le responsable de traitement à la CNIL dans les meilleurs délais et, si possible, dans les 72 heures au plus tard après en avoir pris connaissance. Pour les organismes privés ou publics, elle peut être réalisée par le biais du téléservice suivant : https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles ;

• aux personnes concernées (clients ou salariés) par la violation de données à caractère personnel dans les meilleurs délais lorsque la violation est susceptible d'engendrer un risque élevé pour leurs droits et libertés (article 34 du règlement général sur la protection des données) ;

Cette communication individuelle n'est pas nécessaire si le responsable de traitement :

- a appliqué aux données à caractère personnel affectées par ladite violation des mesures de protection techniques et organisationnelles appropriées qui rendent ces données incompréhensibles telles que le chiffrement ;

- a pris des mesures ultérieures qui garantissent que le risque élevé n'est plus susceptible de se matérialiser.

Si une communication individuelle exige des efforts disproportionnés, il est conseillé de procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière efficace.

➤ **La documentation :**

• Archiver dans un rapport tous les détails connus et les éléments d'analyse de l'incident.

FOCUS : BIEN PRÉSERVER ET COLLECTER LES DONNÉES

Que la collecte des données soit effectuée par le service enquêteur, par un prestataire extérieur ou en interne, il est impératif de procéder à des actions permettant à la fois d'effectuer une analyse ultérieure optimale de l'incident et de constituer le cas échéant un élément de preuve dans une affaire judiciaire.

- Méthodologie et technicité
- Préserver l'état initial des données
- Éviter l'altération ou la destruction des données
- Bloquer l'écriture sur le support source (original)

Afin de permettre l'exploitation des traces et indices par les enquêteurs, il est indispensable de figer le système en l'état et de faire une copie des données utiles AVANT de résoudre l'incident.

Déterminer le support à l'origine du déclenchement de l'incident est un travail complexe. Il est néanmoins indispensable de s'assurer que les données et systèmes fournis aux enquêteurs sont extraits de supports concernés par l'incident.

➤ Bonnes pratiques en matière de copie de données :

En cas de copie d'un support (disque dur, clé USB, etc.), la copie intégrale, dite « bit à bit », est à privilégier.

En cas de sauvegarde de données réseaux, il est souhaitable de fournir au service enquêteur la totalité des journaux de connexion et non les seules données relatives à l'attaque.

En cas de fourniture de données provenant d'un prestataire de service, il est important de communiquer en même temps son identité et ses coordonnées précisément afin qu'il puisse être contacté si besoin.

Il est recommandé de documenter les actions mises en œuvre et les procédures appliquées.

En fonction des enjeux, il pourra être utile de réaliser ces actes en présence d'un huissier de justice.

Il est également nécessaire de procéder au calcul d'une empreinte numérique unique (hash MD5, SHA1, etc.) afin de garantir l'intégrité et l'identité des données copiées aux données originales.

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

La durée importante d'acquisition des preuves ;

Les limitations techniques liées au volume des supports (en téra, péta-octets), au chiffrement , etc.

ÉTAPE N° 3 : COMMENT DÉPOSER PLAINTE ?

Qui peut déposer plainte?

Toute personne physique ou morale (sociétés et associations) victime d'une infraction peut déposer plainte, que l'auteur des faits soit identifié ou non. Dans ce dernier cas, la plainte est déposée contre X.

Pour les personnes morales, **seuls les mandataires sociaux ou les titulaires d'une délégation de pouvoir** (générale ou spécifique) sont habilités à déposer plainte en qualité de représentant légal.

Délais pour porter plainte

Le plaignant dispose de délais au-delà desquels il ne peut plus porter plainte sauf situation particulière, les délais de prescription sont les suivants :

- 1 an pour les contraventions,
- 6 ans pour les délits,
- 20 ans pour les crimes,
- 30 ans pour les crimes graves (terrorisme, grand banditisme,etc.).

Ces délais commencent en principe à partir du jour où l'infraction a été commise. Les infractions liées à la cybercriminalité sont pour la majorité des délits. En matière d'infractions cybercriminelles, la plainte doit être déposée dans les plus brefs délais afin de ne pas voir des preuves disparaître.

Vers quels services se tourner pour déposer plainte ?

Vous pouvez vous rendre dans un commissariat de police ou dans une brigade de gendarmerie de votre choix. Il est toutefois généralement préférable, dans la mesure du possible, de se rendre rapidement dans le service de police nationale ou la brigade de gendarmerie le plus proche du lieu de commission de l'infraction car c'est en principe ce service / unité qui sera chargé de l'enquête.

Les officiers et agents de police judiciaire sont tenus de recevoir les plaintes y compris lorsque ces plaintes sont déposées dans un service ou une unité de police judiciaire territorialement incompétents (article 15-3 CPP). Vous pouvez également déposer plainte par courrier directement auprès du procureur de la République du tribunal judiciaire du lieu de l'infraction ou du domicile de l'auteur de l'infraction.

FOCUS POURQUOI DÉPOSER PLAINTE ?

Porter à la connaissance des autorités judiciaires l'existence d'un incident permet de :

- Vous aider à réagir de façon adéquate.
- Identifier, interpeller et présenter les auteurs à la justice.
- Contribuer à l'amélioration de la cybersécurité à l'échelon national et international, grâce à la collaboration policière.
- Déterminer la volumétrie et le type d'attaques afin d'évaluer l'état de la menace.
- Permettre à l'État d'affecter des ressources à la lutte contre ces menaces identifiées.
- Obtenir le droit à réparation du préjudice subi.
- Déterminer les responsabilités, internes et externes, liées à l'attaque.
- Récupérer tout ou partie des fonds ou des données dérobés par l'action policière ou le développement d'outils spécifiques.
- Faire des recoupements et analyses sur les méthodes et modes opératoires utilisés par les cybercriminels afin de faciliter leur identification.

ÉTAPE N° 4 : QUELS DOCUMENTS PRODUIRE ?

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 l'établissement : extrait Kbis de moins de trois mois pour une société, les statuts (pour une association) ;

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

Les éléments intéressant l'enquête :

- Descriptif précis de l'incident ;
- Coordonnées de l'ensemble des intervenants ou prestataires susceptibles d'apporter des informations aux enquêteurs ;
- 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) ;
- 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).

Il peut être opportun de venir accompagner du responsable de la sécurité informatique ou de la personne désignée pour la gestion de l'incident. A l'issue du dépôt de plainte, un récépissé ainsi qu'une copie de la plainte seront remis au plaignant.

ÉTAPE N° 4 : QUELS DOCUMENTS PRODUIRE ?

Quelles informations seront utiles au service enquêteur outre les supports ou données informatiques ?

La topologie (périmètre de l'incident) :

- Un descriptif de l'architecture du système informatique compromis.

L'historique :

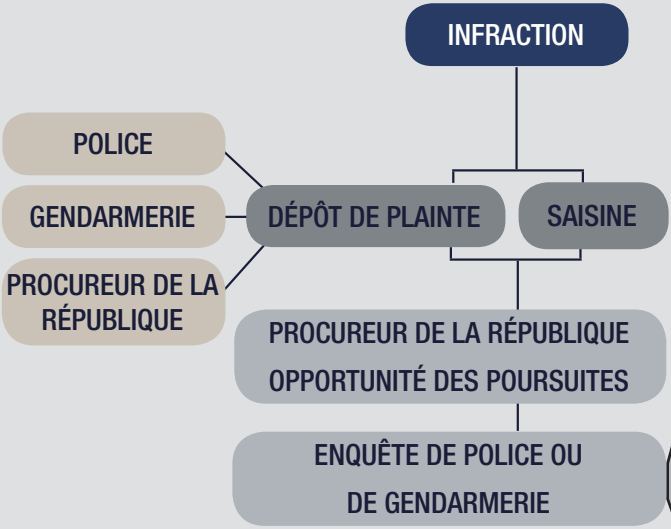
- Contexte de l'incident ;
- Évolution dans le temps ;
- Début et fin de l'incident.

L'observation :

- De l'ensemble des données réseaux sur la période de l'incident (protocoles, statistiques de flux, etc.).

ÉTAPE N° 5 : QUELLES SUITES SONT DONNÉES À L'ENQUÊTE ?

Que se passe t-il après le dépôt de plainte?



Le procureur de la République dirige l'enquête.

Les policiers effectuent les investigations, faisant appel aussi bien à des actes purement techniques (recherches forensic sur les disques durs, interception du trafic réseau) qu'à des techniques strictement policières (notamment écoutes et filatures très utilisées dans les cas d'escroquerie en bande organisée).

Le procureur de la République reçoit la plainte et apprécie la suite à lui donner conformément aux dispositions de l'article 40-1 du code de procédure pénale.

Lorsqu'il estime que les faits qui ont été portés à sa connaissance constituent une infraction commise par une personne dont l'identité et le domicile sont connus et pour laquelle aucune disposition légale ne fait obstacle à la mise en mouvement de l'action publique, le procureur de la République décide s'il est opportun :

- Soit d'engager les poursuites ;
- Soit de mettre en œuvre une procédure alternative aux poursuites ;
- Soit de classer sans suite.

Il avise le plaignant et les victimes si elles sont identifiées, de la décision prise.

Le classement sans suite ne fait pas obstacle à l'exercice direct des poursuites

par la victime. La victime peut porter plainte avec constitution de partie civile ou saisir elle-même le tribunal de grande instance (TGI) avec citation directe.

La plainte avec constitution de partie civile permet à la victime d'une infraction de demander en parallèle de l'action pénale la réparation de son préjudice. Elle entraîne automatiquement la saisine d'un juge d'instruction et l'ouverture d'une enquête.

Par ailleurs, pour obtenir réparation du préjudice subi, la victime doit impérativement se constituer partie civile. Elle peut le faire à tout moment de la procédure, lors du dépôt de plainte jusqu'au jour de l'audience.

Le juge d'instruction peut soit décider d'ouvrir une information judiciaire, soit prendre une décision de refus d'informer.

Le procureur de la République ou le juge d'instruction procède ou fait procéder à tous les actes nécessaires à la recherche et à la poursuite des infractions à la loi pénale.

Au cours de l'enquête, les enquêteurs peuvent être amenés à se transporter dans les locaux de l'entreprise pour :

- Analyser au besoin certaines machines de l'entreprise (notamment pour déceler une infection par malware) ;
- Réaliser des copies complémentaires des supports numériques ayant un intérêt pour l'enquête ;
- Auditionner des personnes qualifiées (techniciens informatiques, responsable de la sécurité des systèmes d'information, etc.) ;
- 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.

Une fois que le procureur de la République estime avoir assez d'éléments de preuve, il peut décider :

- soit du classement sans suite ;
- soit de l'ouverture d'une information judiciaire ;
- soit du renvoi devant la juridiction de jugement.

Une fois que le juge d'instruction estime avoir assez d'éléments, il rend soit une ordonnance de non lieu, soit de renvoi devant la juridiction de jugement et en avise les parties. Les parties peuvent interjeter appel de sa décision.

Cybermalveillance :

https://www.cybermalveillance.gouv.fr

Signal Spam :

https://www.signal-spam.fr

Phishing-Initiative :

https://phishing-initiative.fr/contrib/

No More Ransom :

https://www.nomoreransom.org

Le Youtube de la Police nationale :

https://www.youtube.com/channel/UC_ZalkAU093VIS6nvLloGSg/featured

POLICE NATIONALE

Direction Centrale de la Police Judiciaire
Sous-direction de la lutte contre la cybercriminalité
101 rue des Trois Fontanot
92 000 NANTERRE