Réagir à une attaque informatique :

10 préconisations

POLICE NATIONALE

Réagir à une attaque informatique : 10 préconisations

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 des autorités judiciaires et d'entreprendre une action en justice par voie de dépôt de plainte.

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 la direction d'une entreprise :

- 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 ?
- Vers qui dois-je me tourner pour rapporter à la justice un incident délictuel survenu au sein de mon SI ?
- Qui peut déposer plainte et comment procéder ?

Beaucoup de questions sont en relation avec la collecte de la preuve numérique, sa loyauté, son authenticité, son intégrité et sa sécurité.

Les préconisations contenues dans ce livret constituent des repères essentiels pour appréhender la marche à suivre après un ou plusieurs incidents caractérisés d'origine délictueuse.

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

POLICE NATIONALE

Préconisation n°1

Définir la nature de l'incident

La France possède un arsenal juridique complet dans les domaines liés à la cybercriminalité.

Les infractions de la cybercriminalité se classent en deux catégories :

- Les infractions spécifiques aux technologies de l'information et de la communication (TIC) ;
- Les infractions dont la commission est liée ou facilitée par les TIC.

La lutte contre la cybercriminalité s'organise notamment autour de :

- La loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (dite loi informatique et liberté) n°78-17 du 6 janvier 1978 ;
- La loi relative aux atteintes aux systèmes de traitement automatisé de données (dite loi GODFRAIN) n°88-19 du 5 janvier 1988 ;
- La loi relative au secret des correspondances émises par la voie des communications électroniques ;
- La loi pour la confiance dans l'économie numérique (LCEN) n°2004-575 du 21 juin 2004 ;
- La loi sur la liberté de la presse ;
- La loi relative aux jeux de hasard n°2010-476 du 10 mai 2010 (ARJEL).

Ces infractions sont déclinées dans :

- Le Code Pénal (définition des infractions et peines encourues) ;
- Le Code de Procédure Pénale (règles de l'enquête judiciaire) ;
- Le Code Monétaire et Financier (paiements et transactions financières) ;
- Le Code des Postes et des Communications Electroniques (dispositions relatives au service postal et aux communications électroniques) ;
- Le Code de la Propriété Intellectuelle (contrefaçons, atteintes aux droits d'auteurs et à la propriété littéraire et artistique).

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

POLICE NATIONALE

Les infractions spécifiques aux technologies de l'information et de la communication :

- **Art 323-1 à 323-7 du Code Pénal :** les atteintes aux systèmes de traitement automatisé de données (accès ou maintien frauduleux, entrave au fonctionnement, détention de matériel ou logiciel spécifique, groupement formé ou entente établie) ;

- **Art 226-16 à 226-20 du Code Pénal :** les infractions à la loi « informatique et libertés » (collecte frauduleuse, traitement de données à caractère personnelles, usurpation d'identité numérique) ;

- **Art. L163-3 à L163-12 du Code Monétaire et Financier :** les infractions aux cartes bancaires (contrefaçon, falsification de moyens de paiement, détention de matériel ou logiciel spécifique) ;

- **Art. 434-15-2 du Code Pénal :** les infractions au chiffrement (refus de remettre une clé de déchiffrement ou de la mettre en œuvre) ;

- **Art. 226-1 à 226-4 du Code Pénal :** violation de la vie privée par captation à l'aide d'un dispositif technique, divulgation publique d'un enregistrement de la vie privée, conception, importation, location, détention, offre, d'outils de captation de la vie privée et des correspondances.

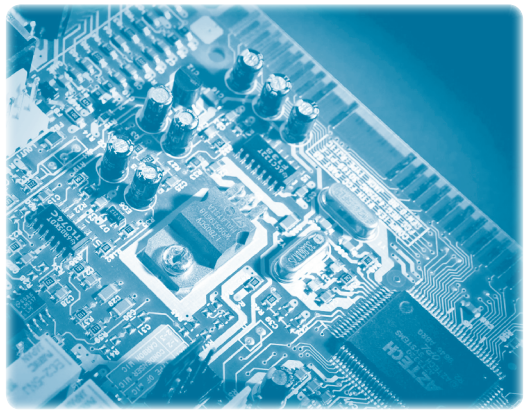
DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

POLICE NATIONALE

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 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.

Ce qui n'est pas exclusif d'une plainte.
Suivre les préconisations ci-après (3 à 9).

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

POLICE NATIONALE

Préconisation n°3

Quelles mesures conservatoires prendre au sein du SI ; à qui confier ces missions ?

Quelles informations communiquer au service enquêteur ?

Même sans connaître 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 :

➤ Confiner :

- mettre en quarantaine les postes informatiques concernés par l'incident ;
- écarter et protéger les supports informatiques concernés avec l'incident : clé USB, CD, DVD, disques durs (internes/externes) ;

➤ Isoler :

- couper tous les accès réseaux pour stopper l'incident ;

➤ Sauvegarder :

- les journaux d'activités (connexions Web, événements systèmes, …) ;
- les documents, emails, fichiers ;
- le trafic réseau supervisé (firewalls, IDS, etc...) ;
- copie de supports informatiques ;
- l'acquisition de mémoire vive ;

➤ 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, …) ;

➤ Communiquer :

- aux personnels ciblés de l'entreprise les recommandations adaptées à la gestion de l'incident ;

Ces dispositions exceptionnelles seront prises en compte par l'unité chargée de la sécurité des systèmes d'information, composée de généralistes capables d'appréhender tous les aspects de l'incident (système, réseau, …).

Le processus de gestion d'un incident ne peut s'improviser. Il doit être organisé et dans la mesure du possible avec :

➤ des procédures ;

➤ des moyens matériels *(stockage notamment);*

➤ des moyens humains *(identifications des rôles clés).*

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

POLICE NATIONALE

La rapidité de réaction et de gestion de l'incident est évidement cruciale.

Les informations utiles pour le service enquêteur seront principalement :

➤ La topologie (périmètre de l'incident) :

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

➤ L'historique :

- Contexte de l'incident ;
- Evolution 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…).

➤ L'acquisition :

- Duplication des systèmes touchés par l'incident avant et après sa survenance.

➤ La documentation :

- Archiver dans un rapport tous les détails et l'analyse de l'incident.

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

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'attaque informatique.

Il deviendra alors difficile de différencier celles laissées par l'attaque et celles générées par le traitement de l'incident. Il est donc préférable de figer le système en l'état et de faire une copie des données utiles avant de résoudre l'incident.

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

À titre d'exemple :

- En cas de copie d'un support (disque dur, clé USB,…), 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 prévision d'une contre-expertise.
- 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 huissier de justice.

Les informations fournies doivent nécessairement avoir été obtenues légalement. Par exemple : accéder frauduleusement au système de l'attaquant dans le but d'obtenir des informations, constitue une infraction.

Le travail d'investigation se fera ensuite sur des copies de sauvegardes. Les données originales seront protégées et conservées dans des conditions de sécurité spécifiques.

Une empreinte numérique (hash MD5, SHA1, etc…) de la donnée originale et de sa copie permettra d'en confirmer l'authenticité.

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

=

79054025
255fb1a2
6e4bc422
aef54eb4

« **la preuve numérique** » s'exprime en binaire :

01110000011100100110010101110101011
11011001100101001000000110111001110
10101011011011100001110101001011100
10011010010111000101110101011001010

Le hash MD5 de « preuve numérique » donne la signature suivante (représentation en hexadécimal) :

32B188336481493D2264E40CF68B036D

L'algorithme MD5, pour Message Digest 5, est une fonction de hachage cryptographique codée sur 128 bits qui permet d'obtenir l'empreinte numérique d'une donnée, d'un support en entier (une empreinte qui comporte 128 bits représente environ 400 sextillions soit 4x1038 possibilités).

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

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

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

POLICE NATIONALE

Préconisation n°6

Vers qui se tourner pour déposer plainte et remettre les preuves collectées ?

La 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 du fait soit identifié ou non. Dans ce dernier cas, la plainte est déposée contre X.

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 cybercriminalité 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.

Vers quels services se tourner pour déposer plainte ?

le service territorial de police ou de gendarmerie le plus proche de votre entreprise

Au sein des services, des investigateurs sont spécialisés dans la lutte contre la cybercriminalité.

Vous pouvez également déposer une plainte auprès du procureur de la République du Tribunal de Grande Instance de votre ressort géographique par courrier avec ou sans constitution de partie civile.

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

Préconisation n°7

Faut-il un statut particulier pour déposer plainte ?

Quels éléments communiquer lors du dépôt de plainte ?

Qui peut déposer plainte ?

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

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 ;
- 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'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 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 sera remise au plaignant.

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

POLICE NATIONALE

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 de la République 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 enquêteur spécialisé en cybercriminalité.

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, de suspects ;
- accèder 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.

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

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 motiver 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.

POLICE NATIONALE

Préconisation n°10

Anticiper, prévenir ; qu'est-il possible de faire pour améliorer la sécurité du SI afin de réduire les risques et menaces ?

Mettre en place une politique de sécurité des systèmes d'information (cybersécurité) SSI

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, garanties et technologies qui peuvent être utilisés pour protéger le cyber-environnement et les actifs des organisations, entreprises et des utilisateurs.

Recommandation UIT–T X.1205

(http://www.itu.int/fr/Pages/default.aspx)

Protéger les actifs

Les actifs des organisations, des entreprises et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication et la totalité des informations transmises dans le cyber-environnement.

La cybersécurité cherche à garantir que les propriétés de sécurité des actifs sont assurées et maintenues par rapport aux risques et menaces pouvant affecter la sécurité par rapport au cyber-environnement.

Les objectifs généraux en matière de sécurité sont les suivants :

- ✔ Disponibilité
- ✔ Intégrité
- ✔ Authenticité
- ✔ Non-répudiation
- ✔ Confidentialité

POLICE NATIONALE

Quelques principes de base

- ➔ Voir plus loin que la technologie ;
- ➔ Penser à la mise en conformité légale, aux aspects juridiques de l'information et de la sécurité ;
- ➔ Soutenir la direction de l'entreprise dans la mise en place d'une politique de la SSI ;
- ➔ Dédier une ressource humaine responsable de la SSI ;
- ➔ Prévenir et former le personnel à la SSI ;
- ➔ Rester maître de son SI ;
- ➔ Toujours se remettre en cause ;
- ➔ Poser les fondamentaux : qu'est-ce qui est vital au sein du SI pour le fonctionnement a minima de l'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 ?

❶ Bien communiquer sur la SSI : informer, sensibiliser, prévenir et former la direction et le personnel (charte de bon usage du SI, guide d'hygiène informatique) ;

❷ Toujours maintenir le SI à jour (systèmes d'exploitation, antivirus,firewalls, applications) ;

❸ Protéger les données stockées et transmises par des accès contrôlés et chiffrés ;

❹ Sécuriser les équipements nomades (portables, tablettes, intelliphones) et éviter l'usage mixte « professionnel/personnel » ;

❺ Limiter l'accès aux informations les plus sensibles à un nombre restreint de personnes ;

❻ Fixer des règles de bon usage de l'internet et mettre en place des dispositifs de filtrage adaptées (listes noires/listes blanches) ;

❼ Mettre en place une politique de droits d'accès par des mots de passe fort régulièrement changés, avec des identifiants uniques et exclusifs ;

❽ Mettre en place des systèmes de sauvegarde contrôlés et redondants ;

❾ Contrôler et tester régulièrement le niveau de sécurité du SI (tests d'intrusion, tests antivirus, etc…) ;

❿ Savoir prévenir, agir et avoir une stratégie de retour à une situation normale en cas d'incident : cataloguer, catégoriser ; capitaliser la connaissance.

Guides et recommandations de l'ANSSI *(**A**gence **N**ationale de la **S**écurité des **S**ystèmes d'**I**nformation)*
http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

POLICE NATIONALE

Notes :

Contacts :

NOM :
PRÉNOM :
Tél. :
Mel :
Adresse :

NOM :
PRÉNOM :
Tél. :
Mel :
Adresse :

NOM :
PRÉNOM :
Tél. :
Mel :
Adresse :

NOM :
PRÉNOM :
Tél. :
Mel :
Adresse :

DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

MINISTÈRE DE L'INTÉRIEUR

DIRECTION GÉNÉRALE DE LA POLICE NATIONALE
DIRECTION CENTRALE DE LA POLICE JUDICIAIRE (DCPJ)
Sous-Direction de Lutte contre la Cybercriminalité (SDLC) – 101, rue des Trois Fontanot – 92000 NANTERRE

Conception et réalisation : DCPJ / SDPTS / SCDC - 2015