# PLAN BLEU

# ANNEXE 5

# Fiche réflexe Cyberattaque

*(Source : guide ANSSI et CPME Les bonnes pratiques de l’informatique)*

|  |
| --- |
| Situations possibles |

Intentionnelle et planifiée, la cyberattaque est l’une des méthodes pour affaiblir, paralyser, corrompre ou détruire une cible dépendant totalement ou en partie de la cybersphère.

Les agressions dans la cybersphère se répartissent en plusieurs familles, notamment :

* Les ADS (neutraliser un système informatique pour le rendre inopérant)
* Le cyberespionnage
* La cyberfraude (falsification de documents officiels, etc.)
* La cyberfinance criminelle
* le cybermarché noir (achat en ligne de marchandises illégales)
* La cyberusurpation d'identité
* Le cybercambriolage (vol de données)
* Le défaçage (modifier l'apparence d'un site, d'un blog, etc.)

Certains signes indiquent que le système a peut-être été compromis :

* Impossibilité de se connecter à la machine ;
* Fichier(s) disparu(s) ;
* Système de fichiers endommagé ;
* Connexions ou activités inhabituelles ;
* Activité importante ;
* Services ouverts non autorisés ;
* Modification intempestive du fichier de mots de passe, date de modification suspecte ;
* Création ou destruction de nouveaux comptes ;
* Création de fichiers, y compris de fichiers cachés.

|  |
| --- |
| Enjeux et impacts de l'événement |

Une cyber-attaque peut générer une crise majeure pouvant remettre en cause la pérennité même de l’entreprise. Les principales conséquences d’une cyber-attaques:

* Des conséquences financières
* Des conséquences juridiques
* Des conséquences réputationnelles

|  |
| --- |
| Actions à réaliser en prévention |

1. Sensibiliser les professionnels aux bonnes pratiques de sécurité informatique

* Choisir avec soin ses mots de passe

Pour bien protéger ses informations, il faut choisir des mots de passe difficiles à retrouver à l’aide d’outils automatisés ou à deviner par une tierce personne.

Définissez un mot de passe unique pour chaque service sensible. Les mots de passe protégeant des contenus sensibles (banque, messagerie professionnelle...) ne doivent jamais être réutilisés pour d’autres services.

Ne pas conserver les mots de passe dans des fichiers ou sur des post-it.

Ne pas préenregistrer les mots de passe dans les navigateurs, notamment lors de l’utilisation ou la connexion à un ordinateur public ou partagé (salons, déplacements...).

* Mettre à jour régulièrement ses logiciels
* Sécuriser l’accès à internet

Le réseau informatique de l’établissement n’est pas directement raccordé à internet, cela diminue les risques de piratage. L’accès à internet se fait de façon centralisée au niveau du datacenter avec des équipements de type firewall protégeant l’ensemble du réseau informatique de la fondation OVE.

Un Wi-Fi mal sécurisé peut permettre à des personnes d’intercepter vos données et d’utiliser la connexion Wi-Fi à votre insu pour réaliser des opérations malveillantes malintentionnées.

* Etre aussi prudent avec son smartphone ou sa tablette qu’avec son ordinateur

Bien que proposant des services innovants, les smartphones sont aujourd’hui très peu sécurisés. Il est donc indispensable d’appliquer certaines règles élémentaires de sécurité informatique :

* N’installez que les applications nécessaires et vérifiez à quelles données elles peuvent avoir accès avant de les télécharger (informations géographiques, contacts, appels téléphoniques...). Certaines applications demandent l’accès à des données qui ne sont pas nécessaires à leur fonctionnement, il faut éviter de les installer ;
* En plus du code PIN qui protège votre carte téléphonique, utilisez un schéma ou un mot de passe pour sécuriser l’accès à votre terminal et le configurer pour qu’il se verrouille automatiquement ;
* Ne préenregistrez pas vos mots de passe
* Être prudent lors de l’utilisation de sa messagerie

Les courriels et leurs pièces jointes jouent souvent un rôle central dans la réalisation des attaques informatiques (courriels frauduleux, pièces jointes piégées, etc.).

Lorsque vous recevez des courriels, prenez les précautions suivantes :

* L’identité d’un expéditeur n’étant en rien garantie : vérifiez la cohérence entre l’expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l’émetteur du mail ;
* N’ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts ;
* Ne répondez jamais par courriel à une demande d’informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire). En effet, des courriels circulent aux couleurs d’institutions comme les Impôts pour récupérer vos données. Il s’agit d’attaques par hameçonnage ou « phishing » ;
* N’ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;
* Être vigilant lors d’un paiement sur Internet

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre smartphone, vos coordonnées bancaires sont susceptibles d’être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d’effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

* Contrôlez la présence d’un cadenas dans la barre d’adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n’est pas visible sur tous les navigateurs) ;
* Assurez-vous que la mention « https:// » apparait au début de l’adresse du site Internet ;
* Vérifiez l’exactitude de l’adresse du site Internet en prenant garde aux fautes d’orthographe par exemple.
* Séparer les usages personnels des usages professionnels

Les usages et les mesures de sécurité sont différents sur les équipements de communication (ordinateur, smartphone, etc.) personnels et professionnels.

Il est recommandé de séparer vos usages personnels de vos usages professionnels :

* Ne faites pas suivre vos messages électroniques professionnels sur des services de messagerie utilisés à des fins personnelles ;
* N’hébergez pas de données professionnelles sur vos équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne ;
* De la même façon, évitez de connecter des supports amovibles personnels (clés USB, disques durs externes, etc.) aux ordinateurs de l’entreprise.

Si vous n’appliquez pas ces bonnes pratiques, vous prenez le risque que des personnes malveillantes volent des informations sensibles de la Fondation après avoir réussi à prendre le contrôle de votre machine personnelle.

1. Analyser les risques et protéger les systèmes d’information sensibles

Il est essentiel de savoir quels sont les systèmes d’information les plus cruciaux pour le bon fonctionnement des structures afin de pouvoir traiter les risques susceptibles de les fragiliser.

Les données présentes sur les serveurs d’établissements sont sauvegardées au niveau du datacenter tous les jours. En cas de soucis sur l’établissement, leurs données peuvent être restituées au cours de la journée.

Les données liées au dossier des personnes accompagnées ne sont pas présentes sur site, elles sont hébergées chez le prestataire dans un datacenter agréé HAS.

La gestion du contrôle d’accès n’est pas accessible depuis la structure, il y a une console centrale gérant le contrôle d’accès de l’ensemble des structures équipées an niveau du datacenter.

Le système antivirus et l’installation des mises à jour de sécurité est centralisé. Le service SI veille à ce que chaque poste soit bien à jour.

|  |
| --- |
| Actions à réaliser en cas de crise |

En cas de comportement inhabituel de l’ordinateur, on peut soupçonner une intrusion (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation, …).

Déconnectez la machine du réseau, pour stopper l’attaque. En revanche, maintenez-là sous tension et ne la redémarrez pas, pour ne pas perdre d’informations utiles pour l’analyse de l’attaque.

Prévenez rapidement votre hiérarchie, ainsi que le PRSI de votre établissement ou le responsable du SI de la Fondation, au téléphone ou de vive voix, car l’intrus peut être capable de lire les courriels.

|  |
| --- |
| Actions à réaliser après l’événement |

La direction peut déposer une plainte auprès de la brigade de gendarmerie ou d’un service de police judiciaire compétent ou adresser un courrier au Procureur de la République auprès du Tribunal de Grande Instance compétent. Ceci est recommandé pour :

* Potentiellement éviter une récidive
* Se prémunir d’une plainte à l’encontre de la Fondation, dans le cas où le SI corrompu serait utilisé à des fins malveillantes (attaque d’autres SI via vos infra, hébergement de site illégal à notre insu…)

La DSI soit signaler l’incident : <https://signalement.social-sante.gouv.fr/>

|  |
| --- |
| Personnes à contacter |

* En interne : le directeur de territoire, le PRSI de votre établissement ou le responsable du SI de la Fondation ;
* En externe : l’ARS et les autorités judiciaires.

-------------------------------