# Cyberattaque – comment se protéger?
## Aide-mémoire à l'intention de la direction d'entreprise

## Rapport de gestion

1. Une bonne stratégie contre les cyberattaques commence avant tout incident:
   La direction d'entreprise doit réfléchir au préalable comment elle réagira.

2. En cas d'attaque, il est indiqué d'agir rapidement:
   Des processus rôdés et des voies de recours à la hiérarchie sont très utiles pour garder le contrôle de la situation.

3. Une attaque peut en cacher une autre:
   Le traitement ultérieur systématique d'une cyberattaque est essentiel.

## 1. Préparation

Mesures générales de la direction:
> Votre entreprise dispose-t-elle d'une cellule de crise en cas de cyberattaque? Les domaines de responsabilité et les compétences ont-ils été clairement définis et entraînés avec la cellule de crise?
> Votre cellule de crise est-elle dotée des ressources et compétences nécessaires? (Notamment soutien dans la gestion de crise, communication interne et externe, droit, ressources humaines et experts techniques)
> La cellule de crise dispose-t-elle d'un manuel à jour comportant les données utiles (et récentes) pour contacter les représentants (importants) de vos partenaires extérieurs?
> Cette équipe se soumet-elle à des exercices réguliers, afin que ses membres se connaissent entre eux, ainsi que leurs rôles et leurs responsabilités?
> Cette équipe est-elle familiarisée aux processus de poursuite pénale ou aux conseils techniques de la police / de son interlocuteur/interlocutrice?
> Existe-t-il des relations personnelles entre votre entreprise ou sa cellule de crise et la poursuite pénale?

Mesures juridiques:
> Les responsabilités sont-elles clairement définies en matière de conduite, de communication ou droit, pour savoir si (et quand) il est opportun de contacter la police pour être conseillé ou lui demander une enquête?
> Les responsables font-ils clairement la différence entre la police qui conseille et celle qui effectue une poursuite pénale?[1]

## 2. En cas d'attaque

> En cas d'ennuis privés, le poste de police le plus proche est conseillé.
> En cas de nécessité, c'est-à-dire lors d'une cyberattaque sévère contre votre entreprise, il s'agit de trouver rapidement des spécialistes. Contactez immédiatement la police. Sur le site Suisse-ePolice (www.suisse-epolice.ch), vous trouvez le numéro de téléphone du poste de police le plus proche.
  > Des entreprises spécialisées privées vous aident à réparer votre infrastructure et le cas échéant à la restaurer.

1 Cf. les explications de la page 2.

> La police vous conseille et vous seconde quant à la procédure à adopter, notamment si une éventuelle rançon doit être payée.
  La police ne s'intéresse ni à vos secrets commerciaux, ni à agir sur votre infrastructure. Par contre, elle dépend du bon vouloir d'une entreprise attaquée de lui communiquer les traces que les pirates ont laissées sur ses systèmes.
  Lorsqu'une entreprise est durement attaquée, il est recommandé qu'elle mette directement en contact un(e) de ses technicien(ne)s chevronné(e)s avec les spécialistes de la police. Cette personne a absolument besoin d'une autorisation interne, en général de la gestion ou du service juridique. L'entreprise a également besoin d'un contrat ad hoc, précisant si le service juridique peut suivre l'appel en direct.
> La Centrale d'enregistrement et d'analyse (MELANI) de la Confédération vous aide à évaluer quel logiciel malveillant est en cause et si d'autres entreprises sont concernées.

## 3. Traitement ultérieur

Les attaques (ou celles qui ont été évitées de justesse, sans causer de dommage) sont-elles systématiquement traitées afin de vous améliorer en permanence?

Un traitement ultérieur comporte un potentiel d'améliorations pour les éléments suivants:
> la détection préventive rapide d'un incident,
> la qualité et la rapidité de l'estimation d'un incident (ampleur des dégâts, criticité, etc.),
> la réaction adaptée et rapide / au besoin avec recours à la hiérarchie,
> la maîtrise de l'incident, aussi bien au niveau des mesures d'urgence pour contenir l'ampleur des dégâts qu'au niveau de l'identification des causes véritables et des vulnérabilités pour y remédier,
> les mesures et les aides pour maintenir un service d'urgence approprié pendant que l'on maîtrise l'incident,
> la communication interne et externe,
> l'efficacité et l'efficience des mesures organisationnelles et techniques, aides et procédures ainsi que
> la collaboration interne et avec des instances extérieures.

Un autre instrument pour un traitement ultérieur efficace consiste à échanger activement ses expériences en matière de maîtrise d'incidents avec d'autres instances de la même branche, région ou du même environnement juridique. Les connaissances acquises doivent être systématiquement intégrées pour améliorer la qualité des processus internes, de la documentation, des exercices ainsi que dans la conduite et la culture de l'entreprise.

En collaboration avec MELANI et Swiss Cyber Experts