Aide-mémoire des premières mesures à prendre en cas d'attaque informatique

Le présent document rend compte des principales mesures à prendre en cas d'attaque de votre infrastructure informatique. Il présente les principaux résultats issus de l'atelier tenu lors de la soirée d'information « cybersécurité » de l'UCV du 3 septembre 2020. Les actions ci-dessous ne sont pas exhaustives et nombre d'entre-elles nécessitent **une préparation en amont de la crise !** La réalisation du Label cyber-safe.ch augementera fortement votre résilience en cas d'attaque informatique, pensez-y !

Actions	Commentaires
Isoler l'infection, si possible (tirer la prise)	
Activer la cellule de crise	En l'absence d'une cellule de crise préalablement définie, définir qui sont les membres de cette cellule. Le responsable IT ne doit pas nécessairement en faire partie ; en cas d'attaque, il sera déjà fortement sollicité sur le terrain.
Plan de communication (interne, externe, embargo ?)	Déterminer qui est en charge de communiquer, quoi, à qui et dans quels délais (quand). Attention aux éventuelles conséquences légales, le recours à un bureau de communication ou autre spécialiste peut s'avérer judicieux.
État des lieux et activation plan de reprise	En l'absence d'un plan de reprise préalablement établi, déterminer quels sont les activités/systèmes de base à rétablir en priorité (chaufferie communale ? Contrôle de qualité des eaux ? Alarmes incendies ? Autres fichiers et données?).
Évaluer les impacts possibles (sécurité des personnes, confidentialité, financière)	Le questionnaire disponible en ligne (www.cyber-safe.ch) vous permet d'effectuer une première évaluation de votre sécurité et des impacts en termes de confidentialité, intégrité et disponibilité des données.
Sécuriser les personnes et les données	Sur la base des impacts possibles identifiés, sécuriser en priorité les personnes, puis les données
Contacter les autorités (MELANI, police cantonale)	
Investiguer (forensics)	
Démarche légale et auprès des assurances (si couverture cyber)	
Informer de manière complète (employés, population, toutes les parties concernées par les données)	
Tirer un bilan, améliorer la structure et le plan de crise	