Check-list

Ce qu'il faut inclure dans votre plan d’intervention aux incidents de cybersécurité

Avant un incident

- [ ] Dresser une liste des données et des systèmes clés
- [ ] Sauvegarder les données
- [ ] Mettre en œuvre des antivirus, des pare-feu et d'autres outils de sécurité
- [ ] Créer des protocoles de sécurité normalisés
- [ ] Sensibiliser les employés aux meilleures pratiques de cybersécurité
- [ ] Élaborer un plan d'intervention et répartir les rôles
- [ ] Élaborer des plans de communication interne et externe
- [ ] Tester et répéter les plans (exercices sur table, simulations)
- [ ] Surveiller les menaces telles que l'activité inhabituelle du réseau, les fichiers modifiés et les connexions suspectes

Lors d'un incident

- [ ] Déclencher le plan d'intervention
- [ ] Isoler les systèmes affectés
- [ ] Supprimer les malwares et les portes dérobées
- [ ] Corriger les vulnérabilités
- [ ] Rétablir les systèmes dans leur version initiale
- [ ] Préserver les preuves (journaux, fichiers, images de disque)

Après un incident

- [ ] Analyser les journaux pour comprendre comment la fuite s'est produite
- [ ] Déterminer la portée de la compromission
- [ ] Informer les clients, les parties prenantes et les régulateurs dans le respect des règles légales
- [ ] Faire appel à des fournisseurs tiers et aux forces de l'ordre
- [ ] Procéder à un examen après l'incident
- [ ] Mettre à jour les plans et les contrôles de sécurité, les politiques et la formation sur la base des enseignements tirés