# Comment réagir efficacement lors d'une cyberattaque de votre entreprise ?

Procédure type détaillée étape par étape

## 1. Identifier et contenir l'attaque

**Détection immédiate :**

- [ ] Surveiller les alertes de sécurité (logiciels antivirus, systèmes de détection d'intrusion, logs de serveurs).
- [ ] Identifier rapidement les signes d'une attaque (ralentissement des systèmes, messages suspects, données inaccessibles, demandes de rançon).

**Isoler les systèmes compromis :**

- [ ] Déconnecter immédiatement les ordinateurs, serveurs ou équipements réseau concernés.
- [ ] Interdire temporairement l'accès (la connexion) à certains services critiques pour limiter la propagation.

**Interrompre les communications externes suspectes :**

- [ ] Fermer les connexions avec des adresses IP suspectes.
- [ ] Désactiver temporairement les comptes compromis.

## 2. Mobiliser l'équipe de réponse à la crise

**Constituer une cellule de crise :**

- [ ] Réunir les responsables IT, la direction, les experts en cybersécurité et, si possible, un représentant légal.
- [ ] Informer l'équipe concernée en interne mais éviter toute communication publique prématurée.

**Faire appel à des experts externes :**

- [ ] Contacter les partenaires informatiques et d'autant plus s'ils ont des spécialistes en cybersécurité.
- [ ] Informer le prestataire d'hébergement (si les serveurs sont externes) ou le fournisseur de services cloud.

## 3. Analyser et contenir l'incident

**Identifier la nature de l'attaque :**

- [ ] Malware, ransomware, attaque par phishing, déni de service (DDoS), etc.
- [ ] Déterminer les données ou systèmes impactés.

**Collecter des preuves :**

- [ ] Capturer les journaux d'événements, les captures d'écran et les fichiers malveillants.
- [ ] Ne pas modifier ou supprimer les preuves pour faciliter l'enquête.

**Évaluer les dommages :**

- [ ] Identifier les données perdues, volées ou compromises.
- [ ] Mesurer les impacts financiers, opérationnels et juridiques potentiels.

**Mettre en œuvre des mesures de confinement :**

- [ ] Bloquer les utilisateurs ou processus malveillants identifiés.
- [ ] Appliquer des mises à jour de sécurité urgentes ou des correctifs.

## 4. Eradiquer l'attaque et restaurer les systèmes

**Supprimer la menace :**

- [ ] Scanner les systèmes avec des outils d'analyse antivirus et anti-malware.
- [ ] Nettoyer les fichiers infectés ou restaurer les systèmes à partir de sauvegardes saines.

**Restaurer à partir de sauvegardes :**

- [ ] Vérifier que les sauvegardes ne sont pas compromises avant de les utiliser.
- [ ] Prioriser la restauration des systèmes critiques.

**Tester les systèmes restaurés :**

- [ ] S'assurer que l'activité normale peut reprendre sans risque.
- [ ] Vérifier les correctifs appliqués.

**Changer les identifiants et mots de passe :**

- [ ] Réinitialiser tous les accès aux systèmes pour éviter une nouvelle intrusion.

## 5. Informer les équipes

**Notifier les autorités compétentes (Si nécessaire):**

- [ ] Signaler l'incident à l'Office fédéral de la cybersécurité.
- [ ] Déposer plainte auprès des autorités spécialisées dans la cybercriminalité.

**Communiquer en interne et en externe :**

- [ ] Établir un plan de communication pour rassurer les employés, clients et investisseurs.
- [ ] Informer les clients ou partenaires concernés si leurs données sont impactées.
- [ ] Rester transparent tout en évitant de nuire à la réputation de l'entreprise.

## 6. Préparer l'avenir

**Analyser les failles :**

- [ ] Identifier ce qui a permis l'attaque (manque de formation, vulnérabilités techniques, etc.).
- [ ] Evaluer la rapidité et l'efficacité de la réponse.

**Améliorer la sécurité :**

- [ ] Mettre en œuvre des solutions renforcées (pare-feux, segmentation réseau, etc.).
- [ ] Former les employés à reconnaître et prévenir les cybermenaces.

**Mettre à jour les procédures :**

- [ ] Rédiger ou améliorer le plan de réponse aux incidents.
- [ ] Planifier des tests réguliers pour s'assurer de la robustesse des systèmes.

**Renforcer les sauvegardes :**

- [ ] Mettre en place des sauvegardes fréquentes et les stocker hors ligne ou dans un environnement sécurisé.

**Effectuer des audits réguliers :**

- [ ] Auditer les systèmes de sécurité pour détecter les failles avant qu'elles ne soient exploitées.

---

Besoin d'assistance ? Notre équipe reste à votre service :

**EMAIL :** support@azinformatique.ch
**TELEPHONE :** **+41 32 466 1212**