Guide d'Urgence en Cas de Cyberattaque

UWORKSAFE.ONLINE

1. Isoler et Contenir l'Incident

- Déconnectez immédiatement tous les systèmes touchés du réseau.
- Désactivez le Wi-Fi, les partages réseau et les connexions à distance.
- Ne redémarrez pas les appareils infectés.
- Informez votre équipe informatique.

2. Informer les Responsables Internes

- Contactez les personnes clés de votre organisation.
- Préparez une communication interne pour sensibiliser vos employés.

3. Faire Appel à des Experts

- Analyser l'étendue de l'attaque.
- Limiter les dommages.
- Récupérer des données si possible.

Contacts :

- **Centre pour la Cybersécurité Belgique (CCB)**
  - E-mail : cert@cert.be
- **U Work Safe - Support Cybersécurité 24/7**
  - E-mail : support@uworksafe.online

4. Sauvegarder des Preuves

- Conservez les journaux d'accès, les fichiers de logs.
- Prenez des captures d'écran des messages d'erreurs ou de demandes de rançon.
- Documentez chaque étape de la réponse à l'incident.

5. Communication avec les Clients et Partenaires

- Communiquez rapidement et de manière transparente si des données clients ont été compromises. Référez-vous aux différentes législations en cours (voir plus loin)

Nous sommes là pour vous aider !

Contactez-nous pour une formation en cybersécurité adaptée à vos employés en PME.

U Work Safe - Protégez votre entreprise contre les cybermenaces

Téléphone : +32 (0)2 123 456 78

E-mail : info@uworksafe.online

Site web : https://uworksafe.online

UWORKSAFE.ONLINE

6. Notifier les Autorités Compétentes

- **Commission de la protection de la vie privée (CPVP)**
  - Site web : www.autoriteprotectiondonnees.be
- **Service de police spécialisé en cybercriminalité**
  - Numéro d'urgence : 101
  - Point de contact : https://pointdecontact.belgique.be/meldpunt/fr/bienvenue
  - Si vous êtes victime d'une cyberattaque, nous vous conseillons de déposer plainte auprès de la police locale.

Délais de notification en vigueur :

RGPD	Notification dans les 72 heures à l'Agence de protection des données		
NIS2	Une alerte précoce doit être donnée dans les 24 heures « après avoir pris connaissance de l'incident ».	Cette alerte sera suivie d'une notification complète dans les 72 heures, qui devra inclure une évaluation initiale de l'incident.	Un rapport final devra être présenté dans un délai d'un mois à compter de la notification de l'incident.
DORA	Obligation de signaler aux autorités compétentes les incidents significatifs qui pourraient impacter la résilience numérique ou perturber les services financiers. La notification doit être effectuée rapidement, souvent dans un délai de 72 heures.		

7. Réviser et Améliorer les Mesures de Sécurité

- Mettez à jour vos systèmes et logiciels de sécurité.
- **Planifiez une formation en cybersécurité pour vos employés.**

Note : Ce guide est destiné à vous assister en cas de cyberattaque.
Il ne remplace pas les conseils personnalisés d'un expert en cybersécurité.