PROTOCOLE D'URGENCE FACE À UNE CYBERATTAQUE

À l'ère de la digitalisation, la menace des cyberattaques est omniprésente. Toutes les entreprises, des plus petites aux multinationales, peuvent être ciblées. D'après un rapport de l'ENISA daté de 2021, près de 68 % des PME ont subi une cyberattaque, soulignant ainsi l'importance cruciale de la préparation et de la réactivité face à ces menaces.
Face à cette réalité, comprendre comment réagir efficacement lors d'une cyberattaque devient une priorité. Voici comment naviguer dans ces situations difficiles :

Préparation en amont

- **Identification des systèmes.** Dressez un inventaire complet de tous les appareils et systèmes (les serveurs, les ordinateurs de bureau, les ordinateurs portables, les tablettes, les smartphones, etc.) connectés à votre réseau. Cela vous permettra d'avoir une vue d'ensemble de votre infrastructure.
- **Sauvegarde des données.** Assurez-vous d'avoir des copies sécurisées de toutes vos données essentielles. Utilisez des services de sauvegarde en ligne ou des disques durs externes pour garantir la récupération en cas de perte.
- **Protection du réseau.** Mettez en place un pare-feu robuste et assurez-vous que tous vos systèmes et logiciels sont régulièrement mis à jour pour se protéger contre les vulnérabilités.
- **Formation des employés.** Organisez des sessions de formation pour sensibiliser vos employés aux différentes menaces cybernétiques et leur enseigner les bonnes pratiques pour éviter les incidents.
- **Plan de réponse aux incidents.** Élaborez un plan détaillé qui décrit les étapes précises à suivre en cas d'incident de sécurité.

Réaction pendant l'incident

- **Identification.** Soyez vigilant aux signes d'une éventuelle attaque, tels que des :
  - Problèmes de connexion inattendus
  - Modifications non autorisées de fichiers
  - Comportements système anormaux
  - etc.
- **Restez calme.** Même en situation de crise, il est essentiel de garder son sang-froid et de suivre les procédures établies.
- **Informez votre responsable.** Communiquez rapidement avec votre hiérarchie, en fournissant des détails précis sur l'incident.
  - **Soyez précis.** Fournissez des informations concrètes sur ce que vous avez observé, comme les systèmes affectés, les alertes (ou indices) et le moment de la première détection.
  - **Ne cherchez pas de solution.** N'essayez pas de supprimer le logiciel malveillant ou de restaurer les systèmes vous-même, sauf si vous êtes un expert en cybersécurité.
  - **Suivez les instructions.** Une fois que vous avez informé votre responsable, soyez prêt à suivre ses instructions.
  - **Documentez vos actions.** Tenez un journal de vos actions et de tout comportement inhabituel observé.

  Votre promptitude à signaler peut faire une grande différence dans la gestion de la cyberattaque.
- **Contention de l'attaque :** Suivez les étapes suivantes pour gérer et limiter l'impact de l'attaque informatique :
  - **Agissez rapidement** pour limiter l'impact de l'attaque.
  - **Déconnectez les systèmes compromis du réseau** pour éviter la propagation de l'attaque.
  - **Créez des sauvegardes d'urgence avec l'aide d'un professionnel**, si vous n'en disposez pas déjà.

    Les méthodes peuvent inclure :
    - Utilisation d'un service de sauvegarde en ligne (cloud).
    - Stockage de copies de fichiers importants sur un disque dur externe.

  Soyez conscient du risque de sauvegarder des données pendant une attaque.

- **Contactez les experts :** En cas de doute ou de gravité de l'incident, sollicitez l'aide d'experts en cybersécurité. Le Computer Incident Response Center Luxembourg (CIRCL), par exemple, est une ressource précieuse.
  - Tél. : (+352) 247 88444
  - E-mail : info@circl.lu

  Soyez prêt à fournir autant d'informations que possible sur l'incident, y compris :
  - le type d'attaque ;
  - les systèmes touchés ;
  - les données compromises ;
  - les mesures que vous avez prises jusqu'à présent pour contenir l'attaque ;
  - etc.

Il est important de tenir un journal des événements avec toutes les descriptions, les preuves et la chronologie, même si toutes ces informations ne sont pas immédiatement disponibles. Ces informations aideront les professionnels à comprendre la situation et à déterminer les meilleures étapes à suivre.

Activités post-incident

Évaluation de l'attaque. Une fois la menace contenue, prenez le temps d'évaluer l'étendue des dégâts. Identifiez les systèmes touchés et déterminez la nature des données potentiellement compromises. Repérez les indices révélateurs, comme :

- des problèmes de connexion ;
- des modifications de fichiers inexpliquées ;
- des performances de système irrégulières ;
- des alertes de logiciels de sécurité ;
- etc.

- **Notification.** Informez toutes les parties concernées de l'incident, qu'il s'agisse de clients, de partenaires ou d'autorités réglementaires (p.ex. la commission nationale pour la protection des données (CNPD) ou la police).
- **Résolution et restauration.** Travaillez à la remise en état de vos systèmes. Cela peut nécessiter de nettoyer les systèmes infectés ou de restaurer à partir de sauvegardes.
- **Analyse post-incident.** Réfléchissez à ce qui a pu causer l'incident. Identifiez les failles de sécurité, renforcez vos défenses et réévaluez vos procédures actuelles pour éviter de futurs incidents.

Conclusion

La cybersécurité n'est pas seulement une question de technologie, mais aussi de sensibilisation et de préparation. Investir dans des mesures de sécurité robustes, former régulièrement vos employés et avoir un plan d'action clair en cas d'incident sont essentiels. Pour toute assistance ou conseil, le NC3 au Luxembourg est à votre disposition.

Pour plus de détails sur le protocole d'urgence face à une cyberattaque :

CHAMBRE DES MÉTIERS
LUXEMBOURG

Vous avez des questions ?
Vous souhaitez recevoir plus d'informations sur la digitalisation ? Contactez le Service eHandwierk de la Chambre des Métiers :
E-mail : **ehandwierk@cdm.lu**
Tél. : **42 67 67 - 505**