15 minutes d'avance

Fiche conseil. 06

Comment aborder la cybersécurité ?

Phishing, Ransomware, DDoS, virus, cheval de Troie, ... Ces cyberattaques font maintenant partie des menaces quotidiennes. En 2022, 831 attaques ont été portées à la connaissance de l'ANSSI soit seulement 0,2% du total estimé. La question n'est plus « qui » sont les entreprises touchées, mais « quand » serons-nous attaqués ?

Risques

Quelles que soient les motivations du pirate (défi technologique, vol de données, messages idéologiques, espionnage, vengeance, profit, ...), les impacts pour l'organisme attaqué sont nombreux et peuvent être irréversibles :

1. **Perte de disponibilité** : impossibilité d'accéder aux outils informatiques et donc de maintenir l'activité et les relations.
2. **Perte financière** : pour gérer l'attaque et parfois pour payer une rançon.
3. **Atteinte à l'image** : attaqué, l'organisme dévoile ses « failles » en termes de sécurité.
4. **Atteinte à la protection des données** à caractère personnel : perte de contrôle des données confiées.
5. **Cession définitive d'activité**.

Que dit le RGPD ?

- Principes fondamentaux du RGPD : intégrité et confidentialité
- Art. 32 sur l'obligation d'assurer la sécurité des données personnelles

Le RGPD joue un rôle essentiel dans la lutte contre la cybercriminalité en imposant des normes strictes en matière de protection des données personnelles et en incitant les organisations à renforcer leur sécurité informatique pour se protéger contre les violations de données et autres cyberattaques.

Bonnes pratiques

- Mettre en place des **mesures organisationnelles et techniques** et plus précisément une politique de sécurisation de l'entreprise : protocoles de transfert, sécurisation des postes de travail, des outils mobiles, vidéo-surveillance, gestion des droits d'accès, charte informatique, engagement de confidentialité, politique de classification de l'information, etc.
- Rendre les **engagements contraignants** en les annexant au règlement intérieur ou aux contrats de travail, le cas échéant.
- Programmer des **séances de sensibilisation et de formation** continues auprès de l'ensemble des publics (équipes en poste, stagiaires, bénévoles) en contact avec les outils informatiques et les données gérées par l'organisme.
- Renforcer l'attitude responsable de chacun en diffusant **régulièrement des supports de communication** pratiques et pédagogiques (vidéos, fiches repères, quiz, challenge, etc.) mis à disposition par des institutions de confiance (Cnil, Linc, ANSSI, Cybermalveillance) et en invitant des spécialistes. Bref, faire de la cybersécurité un thème transversal et partagé.
- Souscrire une **assurance « cybercriminalité »** spécifique et adaptée et s'entourer d'un **conseil**.
- En cas de doute et de question, se rapprocher de son DSI ou de son DPO.

Pour aller plus loin

GOUV – La cybersécurité pour les TPE/PME

GOUV – Rapport de la cybermenace en 2022

LINC - Laboratoire d'Innovation Numérique de la Cnil

Cybermalveillance

ANSSI – Passeport de conseils aux voyageurs

ANSSI – hameçonnage infographie (01/2022)

ANSSI – fiche rançongiciel (01/2022)