

CYBER DETECTION

CYBER SOCIAL

ATELIER – UPE 06 – MERCREDI 17 FEVRIER 2021

Intervenants :

- Fabrice Lavergne ; Chef d'entreprise
- Pierre Gouspy ; Expert en Cybersécurité

LES MENACES INTERNES

- L'accident
- La négligence
- La malveillance

Vos employés sont-ils à la solde de cybercriminels ?

- Ransomware
- Atteinte à l'image de l'entreprise et de ses dirigeants
- Espionnage
- Sabotage

EXEMPLE DU SECTEUR DE LA SANTÉ

- Assurer la pérennité et la continuité de votre activité: soigner vos patients
- La violation de la sécurité des données peut avoir un fort impact sur l'activité

UNE SURVEILLANCE RESPONSABLE

Pour une surveillance responsable des collaborateurs

- avoir un objectif clairement défini et ne pas être utilisé à d'autres fins ;
- être proportionné et adéquat à cet objectif ;
- nécessiter une information préalable des personnes concernées.

⇒ Elaborer et faire signer

- une charte informatique
- Une charte du télétravail

⇒ Respecter le RGPD (règlement général sur la protection des données)

CYBERSOCIAL : la solution

REMONTÉE D'ALERTES EN CAS :

- D'accès aux fichiers et répertoires protégés ainsi qu'aux bases de données et autres progiciels ⁽²⁾
- De suppression et/ou de copie de donnée massives
- De dépassement horaire pour lutter contre les accidents au travail (en dev)
- De connexion hors plages horaires définies pour l'entreprise
- De connexion hors zone géographique définies pour l'entreprise
- De statut « actif / inactif » du collaborateur (en dev)
- D'accès aux sites WEB définis par l'entreprise (au-delà de l'interdiction d'accès aux sites qui sera lui géré par le pare-feu)

NB : toute base de données et autres progiciels peuvent être mis sous surveillance à partir du moment où elle génère des journaux d'évènements (log).

Et toujours...

5 conseils pour lutter contre la cyber-malveillance :

- La sauvegarde des données
- La mise à jour automatique des ordinateurs
- La sécurisation des mots de passe
- L'implication et la formation du personnel
- Disposer d'un outil de contrôle des menaces type **SIEM** (Gestion des événements de sécurité) **comme CyberDetection**

CYBER

DETECTION

WWW.CYBERDETECCION.NET

contact@cyberdetection.net - [+33 \(0\)4 69 96 80 08](tel:+330469968008)