|  |
| --- |
| Réflexion 1 – Identifier l’origine de risques informatiques |
| **Durée** : 20’ | *Homme avec un remplissage uniouDeux hommes avec un remplissage uni* | **Source** |

**Travail à faire**

Après avoir lu le document, répondez aux question suivantes :

1. Quelles sont les principales conséquences d’une cyberattaque ?
2. Pourquoi est-il important de former le personnel aux risques informatique ?
3. Pourquoi faut il mettre à jour régulièrement les logiciels et les pilotes informatiques ?
4. Pourquoi l’entreprise doit veiller à respecter la RGPD par exemple ?

**Doc.  Les risques informatiques et numériques**

Les risques informatiques et numériques peuvent avoir un impact significatif sur les entreprises, tant sur le plan financier que sur le plan opérationnel. Il est donc important pour elles de mettre en place des mesures de sécurité pour se protéger. En mettant en place ces mesures, les entreprises peuvent réduire le risque de subir des dommages dus à des cyberattaques, des erreurs humaines, des pannes matérielles ou des changements technologiques.

Les principaux risques informatiques et numériques d'une entreprise sont les suivants :

* **Les cyberattaques** sont les menaces les plus graves pour les entreprises. Elles entraînent des pertes de données, des interruptions d'activité, des dommages à la réputation et des pertes financières.

Elles peuvent prendre de nombreuses formes :

* les **virus** qui altèrent des fichiers ou le fonctionnement des ordinateurs ;
* les **ransomwares** qui cryptent les données et rendent le système informatique inutilisable tant qu’une ranson n(a pas été payée ;
* les **attaques par déni de service (DDoS)** qui submergent les serveurs d'une entreprise et bloque ou perturbe les opérations ;
* **l'espionnage industriel et les logiciels espion**s qui s’approprient des informations confidentielles, etc.
* **Les erreurs humaines** sont également une source importante de risques informatiques, notamment lorsque les salariés sont mal formés. Les employés peuvent commettre des erreurs suivantes :
	+ la **perte ou la destruction de données** à l’occasion de travaux courant sur les fichiers ou bases de données ;
	+ la **divulgation d'informations** sensibles tel que l’identifiant ou le mot de passe noté sur un post-it ;
	+ la **configuration incorrecte** des systèmes informatiques qui n’ont pas fait l’objet d’une mise à jour régulières ;
	+ **l’ouverture inappropriée d’un fichier** avec une pièce jointe contenant un virus ou un ransomware qui infecte et bloque le serveur. Le Phishing et Ingénierie Sociale sont souvent utilisés pour tromper les employés et obtenir un accès non autorisé.
* **Les pannes et problèmes matériels** peuvent également entraîner des pertes de données ou des interruptions d'activité. Elles peuvent être causées par des facteurs tels que
	+ des **catastrophes naturelles**, des **accidents ou des défauts de fabrication** ;
	+ les **retards de mises à jour de Sécurité** peuvent rendre les systèmes vulnérables aux nouvelles menaces. Elles concernent les antivirus, les pilotes matériels et logiciels et les logiciels eux même. Ces éléments peuvent contenir des failles logicielles qui sont exploitées par les hackeurs.
	+ **Les changements technologiques** peuvent également présenter des risques. L’entreprises doit s'assurer que son système informatique est compatible avec les nouvelles technologies.
* **La non-conformité aux lois et réglementations** en matière de protection des données peut entraîner des sanctions pénales et financières et affecter la réputation de l'entreprise. C’est notamment le cas si l’entreprise ne respecte pas la RGPD.

Voici quelques mesures de sécurité que les entreprises peuvent mettre en place pour se protéger contre les risques informatiques et numériques :

* installer un logiciel antivirus et anti-malware ;
* former les employés aux bonnes pratiques de sécurité informatique ;
* mettre en place une politique de sécurité informatique ;
* effectuer des sauvegardes régulières des données ;
* gérer les accès aux systèmes informatiques ;
* surveiller les systèmes informatiques pour détecter les activités suspectes.

**Réponses**

1. Quelles sont les principales conséquences d’une cyberattaque ?
2. Pourquoi est-il important de former le personnel aux risques informatique ?
3. Pourquoi faut-il mettre à jour régulièrement les logiciels et les pilotes informatiques ?
4. Pourquoi l’entreprise doit veiller à respecter la RGPD par exemple ?