|  |  |  |  |
| --- | --- | --- | --- |
| Réflexion 7 – Sécuriser les échanges | | | |
| Durée : 20’ | Homme avec un remplissage unipuis Groupe d’hommes avec un remplissage uni | Une image contenant symbole, Bleu électrique, Police, Graphique  Le contenu généré par l’IA peut être incorrect. | Source |

**Travail à faire**

**Après avoir lu le document, répondez aux questions suivantes :**

1. Qu’est-ce que le "shadow IT" et pourquoi représente-t-il un risque pour la sécurité des messageries en entreprise ?
2. Citez deux types de cybermenaces pouvant transiter par la messagerie et expliquez leurs conséquences.
3. Quelles fonctionnalités une messagerie professionnelle doit-elle offrir pour garantir la confidentialité et la conformité des échanges ?
4. Pourquoi la sensibilisation des collaborateurs est-elle aussi importante que les outils techniques pour assurer la sécurité des communications ?

**Doc.  La sécurité des messageries : un enjeu stratégique pour les entreprises**

1. **Des outils indispensables… mais vulnérables**

Les messageries instantanées sont devenues essentielles dans les entreprises : elles permettent une communication rapide, le travail en équipe et le partage de documents.

Mais cette accessibilité cache des risques de sécurité importants. Chaque message, lien ou pièce jointe peut représenter une faille si l’entreprise n’a pas mis en place de mesures de protection efficaces.

1. **Des menaces bien réelles**

**• Phishing et fichiers malveillants**

Le phishing consiste à usurper l’identité d’un contact pour piéger les utilisateurs. Les messages contiennent souvent des liens frauduleux ou des pièces jointes infectées qui permettent d’installer des logiciels espions ou de bloquer les systèmes informatiques.

**• Shadow IT : l’informatique incontrôlée**

L’usage d’applications personnelles comme WhatsApp ou Telegram à des fins professionnelles expose l’entreprise à des risques juridiques, car ces outils échappent au contrôle de la DSI et ne garantissent ni confidentialité ni conformité au RGPD.

1. **Confidentialité, traçabilité et conformité**

Une messagerie professionnelle doit garantir :

* Le chiffrement des échanges
* L’archivage sécurisé
* La gestion des droits d’accès
* La possibilité de supprimer les données sur demande

Ces fonctions sont indispensables pour répondre aux exigences de sécurité et aux obligations légales.

1. **Les solutions à adopter**

**• Des outils sécurisés et conformes**

Des plateformes comme Microsoft 365, Slack Enterprise ou Google Workspace assurent un haut niveau de sécurité et de conformité réglementaire.

**• La formation des utilisateurs**

Les collaborateurs doivent être formés aux bons réflexes numériques : repérer les mails suspects, sécuriser leurs mots de passe, activer la double authentification, signaler les anomalies.

**• Une politique de cybersécurité claire**

Une charte d’utilisation des outils numériques permet de définir les règles, de prévenir les risques et d’impliquer tous les services.

1. **Une responsabilité partagée**

La sécurité des messageries concerne toute l’entreprise. Elle repose sur une combinaison d’outils fiables, de bonnes pratiques humaines et d’une culture numérique solide.

Face à des menaces toujours plus sophistiquées, seule une approche globale peut garantir la protection des données et la continuité de l’activité.

**Réponses**

1. Qu’est-ce que le "shadow IT" et pourquoi représente-t-il un risque pour la sécurité des messageries en entreprise ?
2. Citez deux types de cybermenaces pouvant transiter par la messagerie et expliquez leurs conséquences.
3. Quelles fonctionnalités une messagerie professionnelle doit-elle offrir pour garantir la confidentialité et la conformité des échanges ?
4. Pourquoi la sensibilisation des collaborateurs est-elle aussi importante que les outils techniques pour assurer la sécurité des communications ?