CHECKLIST CYBERSÉCURITÉ

1. *Données sensibles*

a. Données clients

- Inclut les noms, adresses, numéros de téléphone, emails, coordonnées bancaires, et historiques d'achats.
- Leur fuite peut entraîner des violations du RGPD, des poursuites judiciaires et une perte de confiance des clients.
- Mesures de sécurité :
    - Chiffrement des données stockées.
    - Mise en place d'un accès restreint basé sur les rôles.
    - Suppression des données obsolètes.

b. Données des employés

- Données personnelles (nom, adresse, numéro de sécurité sociale), fiches de paie, et contrats.
- Les employés peuvent être victimes de vol d'identité ou d'ingénierie sociale.
- Mesures de sécurité :
    - Stockage dans des systèmes sécurisés, avec un accès limité au service RH.
    - Chiffrement des fichiers sensibles.

c. Données financières

- Comptes bancaires, factures, transactions, budgets.
- Une fuite ou une modification peut provoquer des pertes financières ou des fraudes.

- Mesures de sécurité :
    - Utilisation de logiciels comptables sécurisés.
    - Surveillance en temps réel des transactions.

d. Propriété intellectuelle

- Designs, brevets, stratégies commerciales, algorithmes.
- Leur perte peut donner un avantage à un concurrent ou endommager la compétitivité.
- Mesures de sécurité :
    - Cloisonnement des projets sensibles.
    - Utilisation de systèmes de gestion des droits numériques.

e. Données des partenaires/fournisseurs

- Contrats, informations financières, données d'entreprise partagées.
- Une attaque sur ces données peut affecter les relations commerciales.
- Mesures de sécurité :
    - Mise en place de contrats de confidentialité.
    - Limitation des accès partagés.

2. Comptes utilisateurs

a. Comptes administrateurs

- Comptes dotés de droits étendus pour gérer les systèmes et données critiques.
- Ils offrent un contrôle total et sont une cible de choix pour les cyberattaques.

- Mesures de sécurité :
    - Utilisation de l'authentification multifactorielle (MFA).
    - Audit régulier des connexions.

b. Comptes de messagerie

- Emails professionnels utilisés pour les communications internes et externes.
- Ils sont souvent la porte d'entrée pour le phishing.
- Mesures de sécurité :
    - Filtrage des emails suspects.
    - Sensibilisation des utilisateurs.

c. Accès cloud

- Stockage de fichiers et données dans des services comme Google Drive ou Microsoft OneDrive.
- Une mauvaise configuration peut exposer des données sensibles.
- Mesures de sécurité :
    - Surveillance des permissions.
    - Restriction des partages externes.

d. Applications SaaS

- Logiciels comme CRM (ex. : Salesforce), ERP, outils RH.
- Leur accès peut compromettre des processus métiers critiques.
- Mesures de sécurité :
    - Journalisation des activités.
    - Restriction des accès par fonction.

3. Systèmes informatiques et réseaux

a. Serveurs

- Machines hébergeant les données et applications internes.
- Une compromission peut paralyser toute l'entreprise.
- Mesures de sécurité :
  - Pare-feu dédié.
  - Sauvegardes régulières.

b. Postes de travail

- Ordinateurs et autres terminaux des employés.
- Chaque appareil peut devenir un point d'entrée.
- Mesures de sécurité :
  - Antivirus à jour.
  - Chiffrement des disques.

c. Appareils mobiles

- Smartphones et tablettes connectés aux systèmes de l'entreprise.
- Ils sont plus vulnérables en raison de leur mobilité.
- Mesures de sécurité :
  - Verrouillage par mot de passe.
  - Effacement à distance.

d. Réseaux internes

- Réseaux Wi-Fi ou câblés de l'entreprise.
- Une intrusion peut exposer l'ensemble des systèmes.

- Mesures de sécurité :
    - Segmentation des réseaux.
    - Surveillance active.

e. Pare-feu et routeurs

- Équipements protégeant le réseau.
- Une mauvaise configuration peut ouvrir des brèches.
- Mesures de sécurité :
    - Mise à jour régulière du firmware.
    - Suppression des mots de passe par défaut.

4. Logiciels et applications

a. Systèmes d'exploitation

- Les logiciels fondamentaux comme Windows, macOS, Linux.
- Une faille non corrigée peut être exploitée pour accéder à l'ensemble des données et applications.
- Mesures de sécurité :
    - Activer les mises à jour automatiques.
    - Limiter les droits administratifs aux besoins essentiels.

b. Applications métiers

- Logiciels spécialisés (ex. : logiciels de gestion, ERP, CRM).
- Une compromission peut perturber les opérations clés.
- Mesures de sécurité :
    - Contrôle des accès basé sur les rôles.

- Sauvegardes des configurations critiques.

c. Plugins et extensions

- Modules complémentaires ajoutés aux CMS, navigateurs ou outils logiciels.
- Souvent mal contrôlés, ils peuvent introduire des vulnérabilités.
- Mesures de sécurité :
  - Installer uniquement les extensions indispensables provenant de sources fiables.
  - Vérifier régulièrement les mises à jour.

d. Outils collaboratifs

- Logiciels comme Teams, Slack, Zoom qui facilitent le travail en équipe.
- Une fuite d'information peut entraîner des pertes stratégiques.
- Mesures de sécurité :
  - Contrôle des droits d'accès et suppression des utilisateurs inactifs.
  - Activation des journaux d'audit pour surveiller les activités.

5. Matériel physique

a. Ordinateurs et serveurs

- Matériel informatique contenant des données sensibles ou critiques.
- Leur accès physique peut compromettre les systèmes.
- Mesures de sécurité :
  - Verrous physiques pour les serveurs.

- Utilisation de chiffrement complet des disques.

b. Clés USB et disques durs externes

- Supports de stockage portables contenant des données professionnelles.
- Ils sont facilement perdus ou volés.
- Mesures de sécurité :
  - Chiffrement des données sur les supports.
  - Politique interdisant l'utilisation de supports non approuvés.

c. Photocopieurs et imprimantes connectées

- Matériel souvent négligé, mais connecté aux réseaux internes.
- Ces appareils peuvent être piratés pour accéder aux documents ou au réseau.
- Mesures de sécurité :
  - Modifier les mots de passe par défaut.
  - Effacer les mémoires internes régulièrement.

d. Caméras de surveillance

- Systèmes de vidéosurveillance connectés.
- Elles peuvent être utilisées pour espionner ou accéder au réseau.
- Mesures de sécurité :
  - Utilisation de VPN pour les connexions externes.
  - Mises à jour régulières des firmwares.

6. Emails et communications

a. Boîtes email professionnelles

- Emails utilisés pour les échanges internes et avec les clients.
- Cible principale des attaques par phishing.
- Mesures de sécurité :
  - Filtrage des emails frauduleux.
  - Authentification multifactorielle.

b. Plateformes de messagerie instantanée

- Applications comme WhatsApp, Teams ou Slack.
- Risques de fuite d'information ou d'accès non autorisé.
- Mesures de sécurité :
  - Formation des utilisateurs.
  - Surveillance des canaux externes.

c. Systèmes VoIP

- Téléphonie utilisant Internet.
- Vulnérabilité aux attaques par déni de service (DDoS) ou espionnage.
- Mesures de sécurité :
  - Chiffrement des communications.
  - Configurations réseau robustes.

7. Sauvegardes

a. Sauvegardes locales

- Stockage sur disques durs externes ou serveurs internes.
- Un accès non autorisé peut compromettre l'intégrité des données.
- Mesures de sécurité :
    - Stocker dans des lieux sécurisés (armoires fermées).
    - Rotation régulière des supports.

b. Sauvegardes cloud

- Copies des données stockées sur des plateformes dématérialisées.
- Les données restent accessibles en cas de sinistre local.
- Mesures de sécurité :
    - Utiliser des fournisseurs conformes au RGPD.
    - Activer le chiffrement des données.

c. Snapshots système

- Copies instantanées des systèmes à un moment donné.
- Permet une récupération rapide après une attaque.
- Mesures de sécurité :
    - Stocker des snapshots hors site.
    - Automatiser leur création.

8. Accès physiques

a. Bureaux et salles serveurs

- Lieux où sont stockés les systèmes critiques.
- Empêche les intrusions physiques.
- Mesures de sécurité :
  - Accès par badge ou code.
  - Surveillance vidéo.

b. Armoires sécurisées

- Espaces de rangement pour documents physiques sensibles.
- Réduit les risques de vol ou d'accès non autorisé.
- Mesures de sécurité :
  - Serrures à combinaison.
  - Limitation des clés à des personnes autorisées.

9. Fournisseurs tiers et partenaires

a. Prestataires IT

- Entreprises qui gèrent ou interviennent sur les systèmes informatiques.
- Une attaque sur leurs systèmes peut affecter votre entreprise.
- Mesures de sécurité :
  - Exiger des certifications (ex. : ISO 27001).
  - Limiter les accès à vos systèmes.

b. Sous-traitants

- Partenaires ayant un accès limité à vos données.
- Leur négligence peut compromettre vos systèmes.
- Mesures de sécurité :
  - Clauses spécifiques dans les contrats.
  - Audits réguliers.

c. Fournisseurs SaaS ou cloud

- Services hébergés pour des applications comme CRM ou stockage.
- Ils stockent des données sensibles.
- Mesures de sécurité :
  - Analyse des politiques de sécurité des fournisseurs.
  - Vérification de leur conformité légale.

10. *Processus organisationnels*

a. Plans de gestion des accès

- Règles définissant qui peut accéder à quoi.
- Réduit les risques d'accès non autorisé.
- Mesures de sécurité :
    - Utilisation de politiques de moindre privilège.
    - Révision régulière des accès.

b. Protocoles de réponse aux incidents

- Ensemble d'actions à réaliser en cas de cyberincident.
- Limite les impacts d'une attaque.
- Mesures de sécurité :
    - Simulations régulières.
    - Documentation accessible et claire.

c. Programmes de sensibilisation

- Formations pour apprendre les bonnes pratiques.
- L'erreur humaine est un vecteur majeur des cyberattaques.
- Mesures de sécurité :
    - Formation initiale obligatoire pour chaque employé.
    - Tests réguliers (ex. : phishing simulé).