Projet ISO 27005 & EBIOS-RM

Sujet : Microsoft Teams 

Rédigé par :

Rabab SOLEIMAN

Redwane ZAGHOUINI

Mohamed Anouar BOUACHOUR

Sous la supervision de :

M. Fawzi GEDEON

Clause 7 : Établissement du contexte

1. Choix de la méthode d'analyse des risques :

Pour notre projet sur Microsoft Teams, nous avons opté pour la méthode EBIOS pour l'analyse des risques. Cette méthode, largement utilisée en France et développée par l'ANSSI, se distingue par son approche structurée pour identifier, évaluer et traiter les risques liés à la sécurité de l'information. EBIOS nous permet de définir clairement les besoins de sécurité spécifiques à notre projet Teams, d'analyser les menaces potentielles et les vulnérabilités, et d'évaluer les impacts sur la confidentialité, l'intégrité et la disponibilité des données. Cela nous permettra de mettre en place des mesures de sécurité efficaces et adaptées, en alignement avec nos objectifs organisationnels et les standards locaux de sécurité.

2. Définir le contexte et les objectifs du projet

- **Contexte** : Le contexte de cette analyse de risque pour Microsoft Teams possède un cadre incluant la politique de sécurité, les procédures de gestion des incidents, et l'implication des parties prenantes. Les critères d'évaluation des risques se basent sur l'identification des actifs critiques, des menaces et des vulnérabilités. Le périmètre couvre les contextes externe (réglementations, impact économique) et interne (structure organisationnelle, infrastructure informatique). Un inventaire des actifs (utilisateurs, données, infrastructures) et leurs interactions est réalisé. La méthode EBIOS permet d'enrichir et d'améliorer cette analyse de risques.

- **Objectifs** : Assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations échangées et stockées sur Microsoft Teams, ainsi que minimiser les risques associés à son utilisation.

3. Définir le domaine d'application et des limites

- ***(Domaine d'application** : Microsoft Teams, y compris les messages, fichiers, appels, et intégrations avec d'autres services Microsoft 365.*
- ***Limites** : Les périphériques utilisateurs (ordinateur, smartphones) sont considérés hors du périmètre direct, mais leurs impacts seront pris en compte indirectement. Les services et applications externes intégrés à Teams, autres que Microsoft 365, sont également hors du périmètre.)*

- **1. Domaine d'Application**

  1.1 Objectifs Stratégiques Commerciaux, Stratégies et Politiques

- **Objectifs Stratégiques** : Améliorer la collaboration et la communication entre les équipes, faciliter le partage de documents et la gestion de projets à travers une plateforme centralisée.
- **Stratégies et Politiques** : Utiliser Microsoft Teams comme plateforme principale pour la communication interne et la collaboration. La politique de sécurité de l'information doit garantir la protection des données échangées sur Teams conformément aux normes de sécurité de l'organisation.

1.2 Processus Métier

- **Identification des Processus Métier** : Microsoft Teams est utilisé pour :
  - La gestion des réunions internes et externes.
  - La collaboration sur des documents partagés.
  - La communication instantanée entre membres de l'organisation.
  - La gestion des projets et des tâches via les fonctionnalités intégrées.

1.3 Fonctions et Structure de l'Organisme

- **Fonctions** : Teams est utilisé par tous les départements pour la communication et la collaboration, y compris la direction, les équipes opérationnelles, les ressources humaines, et le support technique.
- **Structure** : Microsoft Teams est intégré dans la structure organisationnelle avec des équipes dédiées et des canaux pour chaque département ou projet.

1.4 Politique de Sécurité de l'Information

- **Politique de Sécurité** : La politique de sécurité de l'information spécifie les exigences pour la gestion des accès, la protection des données, et la surveillance des activités sur Microsoft Teams. Les utilisateurs doivent respecter les bonnes pratiques en matière de sécurité, comme l'utilisation de mots de passe robustes et la gestion appropriée des autorisations.

1.5 Actifs Informationnels

- **Actifs Informationnels** :
  - **Données échangées** : Messages, fichiers, enregistrements de réunions.
  - **Documents stockés** : Tous les fichiers et documents partagés via Teams.

- **Informations de profil** : Données personnelles et professionnelles des utilisateurs.

1.6 Localisations et Caractéristiques Géographiques

- **Localisations** : Utilisation de Microsoft Teams à partir de divers sites géographiques de l'organisation, y compris bureaux régionaux et télétravail.
- **Caractéristiques Géographiques** : Évaluer l'impact potentiel des différentes régions en termes de réglementation locale sur la sécurité des données.

1.7 Contraintes Affectant l'Organisme

- **Contraintes** :
  - **Réglementations Locales** : Respect des lois et règlements locaux concernant la protection des données personnelles.
  - **Budget** : Limitation des ressources pour l'implémentation de mesures de sécurité supplémentaires.
  - **Technologie** : Dépendance à l'infrastructure Microsoft Teams fournie par Microsoft, avec ses propres limites techniques.

1.8 Attentes des Parties Prenantes

- **Parties Prenantes** : Les utilisateurs internes, les administrateurs IT, les équipes de sécurité, et les gestionnaires doivent avoir des attentes claires en matière de disponibilité, de confidentialité et de sécurité des données échangées sur Teams.

1.9 Environnement Socioculturel

- **Environnement Socioculturel** : La diversité culturelle des utilisateurs peut influencer les préférences et les comportements en matière de communication et de collaboration. Des ajustements dans l'utilisation de Teams peuvent être nécessaires pour répondre à ces diverses attentes culturelles.

1.10 Interfaces

- **Interfaces** :
  - **Systèmes Internes** : Intégration avec d'autres outils de productivité comme SharePoint, OneDrive, et Outlook.

        - **Systèmes Externes** : Connexions potentielles avec des partenaires externes via Teams, nécessitant des contrôles de sécurité supplémentaires.

- 2. Limites du Domaine d'Application

2.1 Justification des Exclusions

- **Exclusions** :
    - Les systèmes de communication non intégrés à Teams, tels que les plateformes de messagerie personnelle ou des outils de collaboration tiers non approuvés.
    - Les données non stockées ou échangées via Teams, telles que les informations qui sont exclusivement gérées en dehors de la plateforme.

2.2 Contraintes Spécifiques

- **Contraintes Techniques** :
    - Limitations imposées par la plateforme Teams concernant le stockage de données, la gestion des accès et les capacités de surveillance.
    - Dépendance à l'infrastructure cloud de Microsoft, avec les politiques et les contrôles de sécurité propres à Microsoft.
- **Contraintes Budgétaires** :
    - Limitation des fonds disponibles pour les investissements supplémentaires en sécurité, tels que les outils de surveillance avancés ou les mesures de protection supplémentaires.
- **Contraintes Organisationnelles** :
    - La structure organisationnelle peut influencer la mise en œuvre des politiques de sécurité, avec des défis potentiels pour uniformiser les pratiques à travers divers départements.

2.3 Contraintes Fonctionnelles et Méthodologiques

- **Fonctionnelles** :
    - La nécessité de garantir la disponibilité continue de Teams, avec des mesures de résilience et de continuité des activités en cas de défaillance.
    - La capacité à gérer les flux de travail et les processus métier de manière sécurisée et efficace sur la plateforme.
- **Méthodologiques** :

        - Utilisation des meilleures pratiques de gestion des risques en sécurité de l'information adaptées au contexte de Teams, avec une attention particulière à la gestion des accès et la protection des données.

2.4 Contraintes Environnementales

- **Environnementales** :
    - Impact des risques naturels ou géographiques sur l'accès et l'utilisation de Microsoft Teams, tels que les interruptions de service causées par des événements climatiques extrêmes.

4. Définir les rôles et responsabilités de chacun

- **RSSI** (Responsable Sécurité des Systèmes d'Information) : Supervise le projet de sécurité pour Microsoft Teams et assure l'intégrité globale des mesures de sécurité.
- **Administrateur Teams** : Gestion des configurations et paramètres de sécurité de Teams selon les politiques établies.
- **Utilisateurs finaux** : Adhésion aux politiques de sécurité, sensibilisation et formation.
- **DSI** (Directeur des Systèmes d'Information) : Support et validation des mesures de sécurité.
- **Équipe de Support Technique :** Fournit un support technique aux utilisateurs et assure la maintenance des outils de sécurité liés à Teams.
- **Responsables de la Conformité :** Veillent à la conformité avec les réglementations et réalisent des audits réguliers des pratiques de sécurité.

5. Définir les critères et échelles

- **Besoins de sécurité (DICP)** : Critères définis incluant la confidentialité des communications, l'intégrité des données partagées, la disponibilité du service Teams, et la protection contre les accès non autorisés.
    - **Disponibilité** : 1 (Faible) à 5 (Critique)
    - **Intégrité** : 1 (Faible) à 5 (Critique)
    - **Confidentialité** : 1 (Faible) à 5 (Critique)
    - **Preuve** : 1 (Faible) à 5 (Critique)

- **Vraisemblance d'un scénario** : Évaluation basée sur la probabilité de scénarios de risques spécifiques pouvant affecter Teams.
    - 1 (Très improbable) à 5 (Très probable)

- **Évaluation des conséquences d'un scénario** : Échelle définie pour mesurer les impacts potentiels sur l'organisation, tels que la perte de données critiques, les interruptions de service et les conséquences financières.
    - 1 (Insignifiant) à 5 (Catastrophique)

6. Définir la matrice d'évaluation des scénarios risques

	VRAISEMBLANCE d'un scénario d'incident					
IMPACT sur l'activité		Très improbable	Rare	Occasionnel	Probable	Très probable
	Catastrophique	Modéré	Modéré	Élevé	Très élevé	Critique
	Elevé	Faible	Modéré	Élevé	Très élevé	Très élevé
	Modérée	Faible	Modéré	Modéré	Élevé	Très élevé
	Mineur	Faible	Faible	Modéré	Modéré	Élevé
	Insignifiant	Faible	Faible	Modéré	Modéré	Élevé

7. Définir les critères d'acceptation des risques

- **Largement acceptable** : 1 - 4 (Vert)
- **Acceptable** : 5 – 10 (Jaune)
- **Tolérable avec surveillance** : 11 - 15 (Orange)
- **Inacceptable** : 16 – 24 (Rouge)
- **Critique** : 25 (Bordeaux)

Pour la Clause 8, nous allons suivre les étapes fournies pour une analyse détaillée des risques de Microsoft Teams. Nous allons créer un fichier Excel avec les trois onglets suivants : **Actifs**, **Mesures de sécurité existantes**, et **Analyse de risques**. Voici les détails pour chaque section :

Clause 8 : Appréciation des risques

8. Identifier les actifs primordiaux

1. **Données utilisateurs**
    - **Description** : Informations personnelles, messages, fichiers partagés, calendriers, et autres données sensibles partagées via Teams.
    - **Responsable** : Administrateur de la plateforme et responsables de la protection des données.
    - **Besoin DIC** :
        - **Disponibilité (D)** : Très élevée, car les utilisateurs doivent pouvoir accéder aux données à tout moment.
        - **Intégrité (I)** : Élevée, les données ne doivent pas être altérées ou corrompues.
        - **Confidentialité (C)** : Très élevée, car les données peuvent contenir des informations sensibles et confidentielles.
    - **Type** : Immatériel.

2. **Serveurs et infrastructures cloud**
    - **Description** : Serveurs hébergeant les services de Microsoft Teams, y compris les serveurs de bases de données, serveurs d'application, etc.
    - **Responsable** : Équipe IT de Microsoft Azure.
    - **Besoin DIC** :
        - **Disponibilité (D)** : Très élevée, car les services doivent être accessibles en permanence.
        - **Intégrité (I)** : Élevée, les serveurs doivent fonctionner correctement sans altération non autorisée.
        - **Confidentialité (C)** : Modérée, car les infrastructures peuvent contenir des données sensibles.
    - **Type** : Matériel et logiciel.

3. **Applications et services de support**
    - **Description** : Les applications intégrées (ex : SharePoint, OneDrive) et services (ex : authentification, gestion des identités) qui permettent le bon fonctionnement de Teams.
    - **Responsable** : Départements responsables des applications intégrées et services support.
    - **Besoin DIC** :
        - **Disponibilité (D)** : Élevée, car ces services supportent les fonctionnalités principales de Teams.
        - **Intégrité (I)** : Élevée.
        - **Confidentialité (C)** : Modérée à élevée.
    - **Type** : Logiciel.

9. Identifier les actifs en support

1. **Réseaux de communication**
   - **Description** : Réseaux LAN, WAN, et Internet qui assurent la connectivité des utilisateurs avec les serveurs de Microsoft Teams.
   - **Responsable** : Administrateurs réseau et fournisseurs de services Internet.
   - **Besoin DIC** :
     - **Disponibilité (D)** : Élevée.
     - **Intégrité (I)** : Modérée.
     - **Confidentialité (C)** : Modérée.
   - **Type** : Matériel.

2. **Outils de surveillance et de gestion de la sécurité**
   - **Description** : Solutions de monitoring, antivirus, systèmes de détection d'intrusion, etc.
   - **Responsable** : Équipe de sécurité informatique.
   - **Besoin DIC** :
     - **Disponibilité (D)** : Modérée.
     - **Intégrité (I)** : Élevée.
     - **Confidentialité (C)** : Modérée.
   - **Type** : Logiciel.

3. **Support client et documentation**
   - **Description** : Équipe de support client, guides d'utilisation, documentation technique.
   - **Responsable** : Équipe de support technique et documentation.
   - **Besoin DIC** :
     - **Disponibilité (D)** : Modérée.
     - **Intégrité (I)** : Modérée.
     - **Confidentialité (C)** : Faible.
   - **Type** : Humain et immatériel.

10. Identifier les mesures de sécurité existantes (ISO 27002, NIST SECURITY, CIS Controls)

Contrôle	Réf ISO 27002	Réf ISO 27005	Réf NIST Security	Réf CIS Controls	Description	C	I	D

Gestion de la confidentialité des données utilisateur	8.2.3	9.2.1	AC-17, SC-12	13, 14	Chiffrement des données en transit et au repos	X	X	X
Protection des accès utilisateurs	9.2.1	9.3.3	IA-2, AC-2	4, 5	Authentification multifactorielle (MFA) pour les utilisateurs	X	X	
Surveillance et audit des activités	12.4.1	10.2.1	AU-6, SI-4	6, 7	Monitoring des activités et audit des accès	X	X	
Sauvegarde des données	12.3.1	10.5.1	CP-9	10	Sauvegardes régulières et vérification des restaurations	X	X	X
Gestion des incidents de sécurité	16.1.1	11.2.3	IR-4	19	Processus de réponse et gestion des incidents	X	X	X
Gestion des accès privilégiés	9.2.3	9.3.4	AC-6, AC-5	5, 16	Contrôle strict des accès privilégiés avec journaux d'audit	X	X	
Sensibilisation et formation à la sécurité	7.2.2	9.4.1	AT-2, PM-13	17	Programmes de formation réguliers pour les utilisateurs et le personnel	X	X	
Protection contre les logiciels malveillants	12.2.1	10.4.1	SI-3, SI-7	8	Solutions antivirus et anti-malware, scans réguliers	X	X	
Gestion des correctifs de sécurité	12.6.1	10.3.2	SI-2, CM-3	7	Application régulière des correctifs de sécurité sur les systèmes et logiciels	X	X	X

11. Identifier les menaces pesant sur le système étudié

Utilisation de catalogues de menaces comme l'annexe C de la norme ISO 27005:2011 ou des CERT pour identifier les menaces pertinentes pour Microsoft Teams.

Menaces

- **Accès non autorisé** : Tentative d'accès sans autorisation aux données utilisateurs.
    - Actif ciblé : Données utilisateurs, serveurs, infrastructures cloud

- **Logiciels malveillants (malware)** : Introduction de logiciels malveillants dans le système via des pièces jointes ou des liens.
    - Actif ciblé : Serveurs, infrastructures cloud, réseaux de communication

- **Exploitation des vulnérabilités** : Utilisation des failles logicielles pour compromettre le système.
    - Actif ciblé : Applications et services de support

- **Intrusion physique** : Accès non autorisé aux installations physiques hébergeant les serveurs.
    - Actif ciblé : Serveurs, infrastructures cloud

- **Attaque DDoS :** Attaques visant à rendre les services inaccessibles en les surchargeant.
    - Actif ciblé : Serveurs, infrastructures cloud

- **Piratage de compte utilisateur** : Accès non autorisé à un compte utilisateur en contournant les mesures de sécurité.
    - Actif ciblé : Données utilisateurs

- **Fuite de données par phishing** : Tentatives de tromper les utilisateurs pour qu'ils divulguent des informations sensibles.
    - Actif ciblé : Données utilisateurs

12. Identifier les vulnérabilités du système étudié

Analyse des vulnérabilités spécifiques à l'infrastructure, le logiciel et le réseau de Microsoft Teams.

Vulnérabilités

- Authentification faible : Utilisation de mots de passe simples ou d'authentification unique sans sécurité supplémentaire.
    - Actif ciblé : Comptes utilisateurs, données sensibles

- Absence de chiffrement de bout en bout : Communications non chiffrées de manière à ce que seul l'expéditeur et le destinataire puissent lire les messages.
    - Actif ciblé : Communications (messages, appels, fichiers)

- Configuration incorrecte des serveurs : Mauvaise configuration des paramètres de sécurité des serveurs.
    - Actif ciblé : Serveurs, infrastructures cloud

- Absence de segmentation réseau : Réseaux non segmentés permettant une propagation facile des attaques.
    - Actif ciblé : Réseaux de communication

- Faible sensibilisation des utilisateurs : Manque de formation et de sensibilisation à la sécurité chez les utilisateurs.
    - Actif ciblé : Données utilisateurs

- Failles dans les API utilisées : Vulnérabilités dans les API intégrées avec Microsoft Teams.
    - Actif ciblé : Applications et services de support

- Utilisation de mots de passe faibles : Utilisation de mots de passe simples ou réutilisés par les utilisateurs
    - Actif ciblé : Données utilisateurs

- Logiciels non mis à jour : Non application des correctifs de sécurité.
    - Actif ciblé : Applications, services de support

13. Identifier les scénarios de risque (Evènements redoutés sur le CID de l'actif)

Événements redoutés sur le CID (Confidentialité, Intégrité, Disponibilité) des actifs primordiaux.

Scénarios de Risque

- Accès non autorisé via mot de passe faible : Un attaquant obtient un accès non autorisé aux données utilisateur en exploitant un mot de passe faible.
    - Actif concerné : Actif concerné

- Divulgation de conversations : Une partie non autorisée accède aux conversations privées des utilisateurs, compromettant la confidentialité des discussions.
    - Actif concerné : Communications (messages, appels)

- Propagation de malware via pièce jointe : Un utilisateur reçoit une pièce jointe infectée, entraînant l'introduction de malware dans le système.
    - Actif concerné : Serveurs, infrastructures cloud

- Altération de fichiers partagés : Un attaquant modifie les fichiers partagés au sein de Microsoft Teams, entraînant la corruption des données ou la diffusion d'informations erronées.
  - Actif concerné : Fichiers partagés, documents

- Phishing aboutissant à un vol d'identité : Un utilisateur se fait tromper par une tentative de phishing et divulgue ses informations d'identification.
  - Actif concerné : Données utilisateurs

- Attaque DDoS rendant le service inopérant : Une attaque par déni de service distribué (DDoS) surcharge les serveurs, rendant Microsoft Teams inaccessible.
  - Actif concerné : Serveurs, infrastructures cloud

- Exploitation d'une vulnérabilité dans une API : Un attaquant exploite une vulnérabilité dans une API intégrée pour obtenir un accès non autorisé ou voler des données.
  - Actif concerné : Applications et services de support

- Intrusion physique dans les installations des serveurs : Un individu non autorisé accède physiquement aux installations où sont hébergés les serveurs de Microsoft Teams.
  - Actif concerné : Serveurs, infrastructures cloud

14. Estimer les impacts des scénarios (Utilisez les échelles)

Utilisation des échelles définies pour évaluer les impacts de chaque scénario de risque.

Impacts des Scénarios

- Accès non autorisé via mot de passe faible : Impact Modéré
- Propagation de malware via pièce jointe : Impact Élevé
- Phishing aboutissant à un vol d'identité : Impact Élevé
- Attaque DDoS rendant le service inopérant : Impact Élevé
- Exploitation d'une vulnérabilité dans une API : Impact Modéré
- Altération de fichiers partagés : Impact Élevé
- Intrusion physique dans les installations des serveurs : Impact Catastrophique
- Divulgation de conversations : Impact Élevé

15. Estimer la probabilité des scénarios

Utilisation des échelles définies pour évaluer la probabilité de chaque scénario de risque.

Probabilités des scénarios

- Accès non autorisé via mot de passe faible : Probabilité Probable
- Propagation de malware via pièce jointe : Probabilité Occasionnel
- Phishing aboutissant à un vol d'identité : Probabilité Probable
- Attaque DDoS rendant le service inopérant : Probabilité Occasionnel
- Exploitation d'une vulnérabilité dans une API : Probabilité Occasionnel
- Altération de fichiers partagés : Probabilité Rare
- Intrusion physique dans les installations des serveurs : Probabilité Très improbable
- Divulgation de conversations : Probabilité Occasionnel

16. Estimer les niveaux de risque des scénarios

Calcul du niveau de risque initial en multipliant la probabilité par l'impact.

(Sur le fichier Excel)

Clause 9 : Traitement des risques

17. Sélection des options de traitement : Acceptation, Réduction, Refus, Transfert

- **Accès non autorisé via mot de passe faible**
  - **Option de traitement : Réduction**
    - Renforcer les politiques de mot de passe (exigences de complexité, durée de validité) et mettre en œuvre une authentification multi-facteurs (MFA).

  Justification : La réduction des risques est appropriée ici car elle permet de sécuriser les comptes utilisateur contre l'accès non autorisé en améliorant les politiques de mot de passe et en ajoutant une couche de sécurité supplémentaire avec la MFA. Ces mesures sont efficaces pour réduire la probabilité de succès d'une attaque par mot de passe faible.

- **Propagation de malware via pièce jointe**
  - **Option de traitement : Transfert**
    - Mettre en place des solutions antivirus, des filtrages de pièces jointes et former les utilisateurs à reconnaître et éviter les pièces jointes suspectes.

  Justification : Si une solution de sécurité tierce (comme un service de filtrage des pièces jointes et de détection de malware) est utilisée pour protéger contre les menaces de malware, cela peut être une forme de transfert de risque. Le fournisseur

de sécurité gère la détection et la prévention des malware, réduisant ainsi le fardeau sur les ressources internes de l'organisation.

- **Phishing aboutissant à un vol d'identité**
  - **Option de traitement : Réduction**
    - Sensibiliser les utilisateurs aux techniques de phishing et mettre en place des filtres anti-phishing.

Justification : La réduction des risques est efficace pour limiter les chances qu'un utilisateur soit victime de phishing en utilisant des outils de détection et en éduquant les utilisateurs. Ces mesures aident à prévenir les attaques de phishing et à réduire l'impact potentiel.

- **Attaque DDoS rendant le service inopérant**
  - **Option de traitement : Transfert**
    - Utiliser des services de protection contre les attaques DDoS et mettre en place des mécanismes de détection ou utiliser des services de mitigation DDoS fournis par des fournisseurs spécialisés.

Justification : Les attaques DDoS peuvent causer des perturbations majeures et sont souvent gérées plus efficacement par des fournisseurs spécialisés dans la mitigation des DDoS. Ces fournisseurs disposent de l'infrastructure et de l'expertise nécessaires pour gérer et atténuer les attaques de manière plus efficace que ce qu'une organisation interne pourrait mettre en place. Transférer ce risque à des experts en sécurité DDoS est généralement plus économique et pratique que de développer une solution interne.

- **Exploitation d'une vulnérabilité dans une API**
  - **Option de traitement : Réduction**
    - Mettre en œuvre des correctifs de sécurité, réaliser des tests de sécurité et des audits réguliers des API sans oublier de surveiller les vulnérabilités des API.

Justification : Réduire les risques par l'application de correctifs et l'audit des API est une approche efficace pour sécuriser les interfaces et prévenir l'exploitation des vulnérabilités. Ces pratiques permettent de maintenir les API sécurisées contre les menaces potentielles.

- **Altération de fichiers partagés**
  - **Option de traitement : Acceptation**

        - Utiliser des contrôles d'accès rigoureux, surveiller les activités sur les fichiers partagés et utiliser des solutions de sauvegarde régulières.

Justification : Si des contrôles d'accès et des sauvegardes régulières sont déjà en place et que les risques d'altération de fichiers sont faibles ou bien gérés, l'acceptation des risques résiduels peut être une option. Cela pourrait être pertinent si les coûts ou l'effort pour des mesures supplémentaires sont jugés élevés par rapport aux impacts potentiels.

- **Intrusion physique dans les installations des serveurs**
    - **Option de traitement : Refus**
        - Renforcer les mesures de sécurité physique et des procédures de sécurité, comme les contrôles d'accès et la surveillance vidéo.

Justification : Si l'infrastructure physique est située dans une zone à risque élevé et qu'il est économiquement ou techniquement difficile de renforcer la sécurité physique à un niveau acceptable, il pourrait être plus approprié de déplacer les serveurs dans un environnement plus sécurisé ou de revoir la localisation des installations pour éviter complètement le risque. Le refus peut également impliquer une reconfiguration ou un changement des pratiques pour éviter la nécessité de sécuriser des installations à haut risque.

- **Divulgation de conversations**
    - **Option de traitement : Réduction**
        - Mettre en œuvre des protocoles de chiffrement de bout en bout pour les communications et contrôler les accès et les autorisations aux communications sensibles.

Justification : La réduction des risques est appropriée en protégeant les communications avec le chiffrement de bout en bout, ce qui garantit que seules les parties autorisées peuvent accéder aux conversations. Cela protège la confidentialité des échanges et réduit le risque de divulgation non autorisée.

18. Sélection des mesures de réduction des risques avec l'annexe A de la norme ISO 27001

1. Accès non autorisé via mot de passe faible

Annexe A de la norme ISO 27001

- **A.9.1.1** (Gestion des accès utilisateurs) : Définir et mettre en œuvre une politique de gestion des droits d'accès qui inclut la gestion des mots de passe.
- **A.9.2.1** (Gestion des droits d'accès utilisateur) : Les droits d'accès doivent être accordés sur la base du besoin d'en connaître et doivent être régulièrement revus.
- **A.9.2.2** (Gestion des mots de passe) : Les politiques doivent inclure des exigences pour les mots de passe, comme la longueur minimale, la complexité, et le changement périodique des mots de passe.
- **A.9.2.4** (Authentification) : L'utilisation d'authentification multifactorielle pour des accès critiques est recommandée.

Norme ISO 27002

- **9.2.1** (Gestion des identités et des accès) : Développer et maintenir des politiques de gestion des identités et des accès, y compris les mots de passe et l'authentification multifactorielle.
- **9.2.3** (Authentification forte) : Assurer que des mécanismes d'authentification forte sont utilisés pour protéger les accès aux systèmes sensibles.
- **9.2.5** (Gestion des mots de passe) : Appliquer des règles de gestion des mots de passe robustes, y compris des exigences de complexité et de durée de validité.

Mesures techniques et organisationnelles

- **Exigences de mot de passe** : Imposer des politiques de complexité des mots de passe (longueur, caractères spéciaux, majuscules, minuscules) et leur expiration régulière.
- **Authentification multifactorielle (MFA)** : Intégrer MFA pour ajouter une couche de sécurité supplémentaire au processus d'authentification.

2. Propagation de malware via pièce jointe

Annexe A de la norme ISO 27001

- **A.12.2.1** (Défense contre les logiciels malveillants) : Installer et maintenir des solutions antivirus et anti-malware pour détecter et prévenir les infections par logiciels malveillants.
- **A.12.3.1** (Sauvegarde) : Assurer la sauvegarde régulière des données pour minimiser les impacts en cas de contamination par malware.

Norme ISO 27002

- **12.2.1** (Défense contre les logiciels malveillants) : Mettre en œuvre des solutions antivirus à jour, ainsi que des solutions de filtrage des pièces jointes et des contenus.
- **12.4.1** (Filtrage des emails) : Déployer des technologies pour filtrer les pièces jointes et les liens contenus dans les e-mails pour détecter les menaces potentielles.

Mesures techniques et organisationnelles

- **Solutions antivirus et anti-malware** : Installer des logiciels de sécurité sur tous les systèmes pour détecter et éliminer les menaces.
- **Filtrage des pièces jointes** : Utiliser des systèmes de filtrage pour examiner les pièces jointes des e-mails et bloquer celles suspectes.
- **Formation des utilisateurs** : Éduquer les employés à reconnaître les pièces jointes suspectes et les comportements sûrs en matière de sécurité informatique.

3. Phishing aboutissant à un vol d'identité

Annexe A de la norme ISO 27001

- **A.7.2.2** (Sensibilisation et formation) : Assurer que les employés reçoivent une formation continue sur les menaces de sécurité, y compris le phishing.
- **A.13.2.1** (Gestion de la sécurité des communications) : Utiliser des solutions de sécurité pour protéger contre les attaques de phishing et les tentatives de fraude.

Norme ISO 27002

- **7.2.2** (Formation et sensibilisation à la sécurité) : Mettre en place des programmes de formation pour sensibiliser les employés aux risques de phishing.
- **13.1.1** (Sécurisation des communications) : Déployer des solutions de filtrage anti-phishing et des technologies de détection pour protéger contre les e-mails de phishing.

Mesures techniques et organisationnelles

- **Formation anti-phishing** : Développer des programmes de formation réguliers pour aider les utilisateurs à identifier et à éviter les tentatives de phishing.
- **Filtres anti-phishing** : Utiliser des solutions logicielles pour bloquer les e-mails de phishing et détecter les URL malveillantes.

4. Attaque DDoS rendant le service inopérant

Annexe A de la norme ISO 27001

- **A.13.1.2** (Protection contre les menaces externes) : Mettre en place des mesures pour protéger les systèmes contre les menaces externes, telles que les attaques DDoS.
- **A.13.2.1** (Gestion de la sécurité des réseaux) : Déployer des solutions de sécurité pour assurer la disponibilité des services en cas d'attaque.

Norme ISO 27002

- **13.2.1** (Sécurisation des réseaux et des communications) : Utiliser des solutions de mitigation DDoS et des services spécialisés pour protéger les réseaux contre les attaques par déni de service distribué.
- **13.2.3** (Gestion des incidents) : Mettre en place des mécanismes pour détecter et répondre aux attaques DDoS.

Mesures techniques et organisationnelles

- **Services de protection DDoS** : Engager des fournisseurs spécialisés pour la mitigation des attaques DDoS et la protection des infrastructures.
- **Surveillance et réponse aux incidents** : Mettre en place des outils pour détecter les attaques DDoS et réagir rapidement pour atténuer leur impact.

5. Exploitation d'une vulnérabilité dans une API

Annexe A de la norme ISO 27001

- **A.14.2.1** (Sécurité des applications et des systèmes) : Mettre en œuvre des contrôles de sécurité pour les applications, y compris les API, pour protéger contre les vulnérabilités.
- **A.14.2.2** (Gestion des vulnérabilités des applications) : Assurer la gestion continue des vulnérabilités des applications en appliquant des correctifs et en réalisant des tests réguliers.

Norme ISO 27002

- **14.2.2** (Gestion des vulnérabilités) : Appliquer des correctifs de sécurité pour combler les vulnérabilités connues dans les API et autres applications.
- **14.2.4** (Tests de sécurité) : Réaliser des tests de pénétration et des audits réguliers pour identifier les vulnérabilités des API et les corriger.

Mesures techniques et organisationnelles

- **Application de correctifs** : Mettre en œuvre des correctifs de sécurité dès qu'ils sont disponibles pour réduire les risques liés aux vulnérabilités des API.
- **Tests de sécurité** : Effectuer des tests de sécurité réguliers pour identifier et corriger les vulnérabilités des API.

6. Altération de fichiers partagés

Annexe A de la norme ISO 27001

- **A.9.1.2** (Contrôle d'accès aux informations et aux actifs) : Définir et appliquer des contrôles d'accès stricts pour protéger les fichiers partagés contre les altérations non autorisées.
- **A.12.3.1** (Sauvegarde) : Assurer la sauvegarde régulière des fichiers partagés pour permettre la restauration en cas d'altération.

Norme ISO 27002

- **9.1.2** (Contrôles d'accès) : Implémenter des contrôles d'accès aux fichiers partagés pour prévenir l'accès et les modifications non autorisées.
- **12.3.1** (Sauvegarde) : Utiliser des solutions de sauvegarde régulières pour protéger les fichiers contre l'altération et les pertes de données.

Mesures techniques et organisationnelles

- **Contrôles d'accès** : Mettre en place des contrôles d'accès rigoureux pour limiter l'accès aux fichiers partagés aux utilisateurs autorisés.
- **Sauvegardes régulières** : Effectuer des sauvegardes régulières et automatisées des fichiers partagés pour permettre la restauration en cas de modification ou de perte.

7. Intrusion physique dans les installations des serveurs

Annexe A de la norme ISO 27001

- **A.11.1.1** (Zones sécurisées) : Mettre en place des mesures pour protéger les zones sécurisées contre les accès non autorisés.
- **A.11.2.1** (Contrôles d'accès physique) : Utiliser des systèmes de contrôle d'accès physique et des dispositifs de surveillance pour sécuriser les installations des serveurs.

Norme ISO 27002

- **11.1.1** (Sécurité physique) : Mettre en œuvre des contrôles d'accès et des mesures de sécurité physique pour protéger les installations de serveur.
- **11.1.2** (Sécurisation des zones) : Appliquer des procédures de sécurité pour protéger les zones où les équipements critiques sont situés.

Mesures techniques et organisationnelles

- **Contrôles d'accès physique** : Installer des systèmes de contrôle d'accès, tels que des badges, des cartes magnétiques, et des systèmes biométriques pour limiter l'accès aux zones sensibles.
- **Surveillance vidéo** : Mettre en place des systèmes de surveillance vidéo pour détecter et enregistrer les accès non autorisés.

8. Divulgation de conversations

Annexe A de la norme ISO 27001

- **A.10.1.1** (Contrôle des communications) : Assurer la protection des informations en transit pour prévenir la divulgation non autorisée.
- **A.10.1.2** (Chiffrement des informations) : Mettre en œuvre des protocoles de chiffrement pour protéger les communications et les informations sensibles.

Norme ISO 27002

- **10.1.1** (Protection des informations en transit) : Utiliser le chiffrement pour protéger les communications contre l'interception et la divulgation non autorisée.
- **10.1.2** (Gestion des clés de chiffrement) : Assurer une gestion sécurisée des clés de chiffrement utilisées pour protéger les communications.

Mesures techniques et organisationnelles

- **Chiffrement des communications** : Utiliser des protocoles de chiffrement robustes pour sécuriser les conversations et les échanges d’informations.
- **Contrôles d'accès aux informations** : Assurer que seules les personnes autorisées ont accès aux informations sensibles en mettant en place des contrôles d'accès rigoureux.

Clause 10 : Acceptation des risques

Acceptation formelle des risques (RSSI, DSI ou DG)

Communication et Indicateurs (Comité de direction)

19. Rappeler le contexte et les objectifs

20. Communiquer sur la cartographie des risques

21. Mettre en évidence les risques les plus critique

Clause 10 : Acceptation formelle des risques, Communication et Indicateurs

19. Rappeler le contexte et les objectifs

Dans le contexte actuel de gestion de la sécurité de l'information, il est essentiel de mettre en place des mécanismes efficaces pour identifier, évaluer et traiter les risques de sécurité. L'objectif principal de cette démarche est de protéger les actifs informationnels de l'organisation contre les menaces potentielles et de garantir la confidentialité, l'intégrité et la disponibilité des informations.

Les risques identifiés couvrent une variété de menaces, allant des accès non autorisés et des attaques de phishing aux intrusions physiques et aux divulgations non autorisées de communications. La gestion de ces risques permet non seulement de renforcer la posture de sécurité de l'organisation, mais aussi de se conformer aux exigences réglementaires et aux meilleures pratiques de l'industrie, telles que la norme ISO 27001.

20. Communiquer sur la cartographie des risques

Scénarios de Risque

1. Accès non autorisé via mot de passe faible (R1)
2. Propagation de malware via pièce jointe (R2)
3. Phishing aboutissant à un vol d'identité (R3)
4. Attaque DDoS rendant le service inopérant (R4)
5. Exploitation d'une vulnérabilité dans une API (R5)
6. Altération de fichiers partagés (R6)
7. Intrusion physique dans les installations des serveurs (R7)
8. Divulgation de conversations (R8)

La cartographie des risques a été élaborée pour identifier et évaluer les différentes menaces pesant sur les actifs informationnels de l'organisation. Voici un aperçu des risques identifiés et des options de traitement choisies :

- **Accès non autorisé via mot de passe faible** : Réduction par le renforcement des politiques de mot de passe et la mise en œuvre de l'authentification multi-facteurs (MFA).
- **Propagation de malware via pièce jointe** : Transfert en utilisant des solutions antivirus et des filtres de pièces jointes, ainsi que la formation des utilisateurs.
- **Phishing aboutissant à un vol d'identité** : Réduction par la sensibilisation des utilisateurs et la mise en place de filtres anti-phishing.
- **Attaque DDoS rendant le service inopérant** : Transfert en engageant des fournisseurs spécialisés dans la mitigation des attaques DDoS.
- **Exploitation d'une vulnérabilité dans une API** : Réduction par l'application de correctifs de sécurité et la réalisation de tests réguliers.
- **Altération de fichiers partagés** : Acceptation en utilisant des contrôles d'accès rigoureux et des sauvegardes régulières.
- **Intrusion physique dans les installations des serveurs** : Refus par le renforcement des mesures de sécurité physique.
- **Divulgation de conversations** : Réduction par l'utilisation de protocoles de chiffrement de bout en bout.

Interprétation

Avant Mesure :

- **Critique (16)** : Propagation de malware via pièce jointe (R2), Phishing aboutissant à un vol d'identité (R3), Attaque DDoS rendant le service inopérant (R4), Altération de fichiers partagés (R6), Divulgation de conversations (R8) sont identifiés comme des risques majeurs avec une probabilité "Occasionnel" et un impact "Élevé".
- **Majeur (12)** : Accès non autorisé via mot de passe faible (R1) et Exploitation d'une vulnérabilité dans une API (R5) sont classés comme des risques majeurs avec des probabilités "Probable" et "Occasionnel" respectivement.
- **Important (8)** : Intrusion physique dans les installations des serveurs (R7) est classée comme importante avec une probabilité "Très improbable".

Après Mesure :

- Les mesures de réduction ont permis de diminuer la criticité de plusieurs risques. La propagation de malware (R2), le phishing (R3), les attaques DDoS (R4), et l'altération de fichiers (R6) ont été réduits à un niveau de risque modéré ou inférieur.
- L'accès non autorisé via mot de passe faible (R1) et l'exploitation des vulnérabilités dans les API (R5) sont maintenant considérés comme ayant un risque modéré après les mesures de gestion et d'audit.

- L'intrusion physique dans les installations des serveurs (R7) reste un risque important nécessitant des mesures continues de surveillance.
- La divulgation de conversations (R8) a été réduite à un niveau de risque mineur grâce au chiffrement de bout en bout et aux contrôles d'accès renforcés.

21. Mettre en évidence les risques les plus critiques

Risques Critiques Avant Mesure

Avant la mise en place des mesures de réduction, les risques suivants étaient identifiés comme les plus critiques :

1. **Propagation de malware via pièce jointe (R3)**
   - Impact : Élevé
   - Probabilité : Occasionnel
   - Niveau de Risque Initial : Majeur (12)
   - Description : Introduction de logiciels malveillants dans le système via des pièces jointes ou des liens, entraînant des infections et perturbations majeures.
2. **Phishing aboutissant à un vol d'identité (R5)**
   - Impact : Élevé
   - Probabilité : Probable
   - Niveau de Risque Initial : Majeur (12)
   - Description : Tentatives de tromper les utilisateurs pour qu'ils divulguent des informations sensibles, conduisant à des vols d'identité et des accès non autorisés.
3. **Attaque DDoS rendant le service inopérant (R6)**
   - Impact : Élevé
   - Probabilité : Occasionnel
   - Niveau de Risque Initial : Majeur (12)
   - Description : Attaques visant à rendre les services inaccessibles en surchargeant les serveurs, perturbant gravement la disponibilité des services.
4. **Altération de fichiers partagés (R4)**
   - Impact : Élevé
   - Probabilité : Rare
   - Niveau de Risque Initial : Majeur (12)
   - Description : Modification non autorisée des fichiers partagés au sein de Microsoft Teams, entraînant la corruption des données ou la diffusion d'informations erronées.
5. **Divulgation de conversations (R2)**
   - Impact : Élevé
   - Probabilité : Occasionnel
   - Niveau de Risque Initial : Majeur (12)

- Description : Accès non autorisé aux conversations privées des utilisateurs, compromettant la confidentialité des discussions.

6. **Intrusion physique dans les installations des serveurs (R8)**
   - Impact : Catastrophique
   - Probabilité : Très improbable
   - Niveau de Risque Initial : Critique (16)
   - Description : Accès non autorisé aux installations physiques hébergeant les serveurs, menaçant gravement la sécurité des infrastructures cloud.

Risques Critiques Après Mesure

Après la mise en place des mesures de réduction, les risques les plus critiques ont été atténués, mais certains restent significatifs :

1. **Propagation de malware via pièce jointe (R3)**
   - Impact : Moyen
   - Probabilité : Rare
   - Niveau de Risque Résiduel : Modéré (4)
   - Description : Solutions antivirus et politiques de sécurité strictes ont atténué le risque, mais la vigilance est de mise.
2. **Phishing aboutissant à un vol d'identité (R5)**
   - Impact : Moyen
   - Probabilité : Rare
   - Niveau de Risque Résiduel : Modéré (4)
   - Description : Sensibilisation des utilisateurs et filtres anti-phishing ont réduit le risque, mais des mesures de surveillance supplémentaires sont nécessaires.
3. **Attaque DDoS rendant le service inopérant (R6)**
   - Impact : Moyen
   - Probabilité : Rare
   - Niveau de Risque Résiduel : Modéré (4)
   - Description : Services de mitigation DDoS et pare-feu de nouvelle génération ont réduit le risque, mais il reste un risque résiduel nécessitant une préparation continue.
4. **Altération de fichiers partagés (R4)**
   - Impact : Moyen
   - Probabilité : Rare
   - Niveau de Risque Résiduel : Modéré (4)
   - Description : Contrôles d'accès rigoureux et surveillance des activités sur les fichiers partagés ont atténué le risque, mais la vigilance est de mise.
5. **Divulgation de conversations (R2)**
   - Impact : Moyen
   - Probabilité : Rare
   - Niveau de Risque Résiduel : Modéré (4)

- Description : Protocoles de chiffrement de bout en bout pour les communications et contrôles d'accès ont réduit le risque, mais nécessitent une surveillance continue.

6. **Intrusion physique dans les installations des serveurs (R8)**
    - Impact : Moyen
    - Probabilité : Très rare
    - Niveau de Risque Résiduel : Mineur (2)
    - Description : Contrôles d'accès physiques renforcés et surveillance accrue ont réduit le risque, mais une vigilance constante est requise.

Ces risques critiques nécessitent une attention particulière et des ressources adéquates pour leur traitement. La mise en œuvre des mesures de sécurité appropriées et la formation continue des utilisateurs sont essentielles pour minimiser les impacts potentiels sur l'organisation.