

# Analyse EBIOS

Entreprise Fictive : MedCare Solutions

ChatGPT

## 1. Contexte et Objectifs de Sécurité

Contexte général de l'entreprise :

MedCare Solutions développe et implémente des solutions technologiques pour le secteur de la santé. L'entreprise gère des systèmes de gestion des dossiers médicaux électroniques (DME), de télémédecine, de suivi à distance des patients et de gestion des stocks médicaux. Ces solutions permettent d'optimiser les processus hospitaliers, d'améliorer la qualité des soins et de faciliter l'accès aux soins. Les solutions proposées collectent et traitent des données sensibles et doivent respecter des normes strictes en matière de confidentialité, intégrité et disponibilité des données de santé, conformément au RGPD. Objectifs de sécurité :

- Confidentialité des données : Assurer la protection des données de santé des patients et leur confidentialité dans toutes les étapes de leur traitement.
- Intégrité des données : Garantir que les données médicales, notamment les informations concernant les traitements et les prescriptions, ne soient ni altérées ni corrompues.
- Disponibilité des systèmes : Assurer la disponibilité continue des systèmes de gestion des DME, de télémédecine et de gestion des stocks médicaux pour éviter tout dysfonctionnement pouvant affecter les soins aux patients.
- Conformité réglementaire : Respecter toutes les exigences légales, notamment en matière de protection des données personnelles (RGPD, loi de santé).
- Sécurisation des communications : Assurer la sécurité des communications entre les différents acteurs du système de santé (patients, médecins, hôpitaux, laboratoires).

## 2. Identification des Actifs à Protéger

Les actifs à protéger dans le cadre de l'analyse EBIOS sont les suivants :

- Données sensibles des patients : Informations personnelles, historiques médicaux, prescriptions, résultats d'examen, et données collectées lors des consultations à distance.
- Systèmes d'information (SI) : Les serveurs, applications logicielles (DME, gestion des stocks, télémédecine) et bases de données utilisés pour stocker et gérer les informations des patients.
- Équipements médicaux connectés : Dispositifs médicaux utilisés pour la télémédecine et le suivi des patients à domicile, qui génèrent et transmettent des données médicales.
- Réseaux de communication : Les réseaux utilisés pour échanger des données entre les professionnels de santé, les patients et les systèmes internes.
- Plateformes logicielles : Les logiciels développés par MedCare Solutions pour la gestion des dossiers médicaux, la gestion des stocks, et la télémédecine.

### 3. Identification des Menaces

Voici les menaces principales auxquelles MedCare Solutions pourrait être confrontée :

- Fuites de données :
  - Risque de divulgation non autorisée des données personnelles de santé des patients (via un piratage, une erreur humaine, ou une mauvaise gestion des accès).
- Accès non autorisés aux systèmes :
  - Tentatives de piratage ou d'accès frauduleux aux systèmes de gestion des DME, entraînant une compromission des informations sensibles des patients.
- Altération ou suppression des données :
  - Risque que des informations médicales soient altérées ou supprimées accidentellement ou malicieusement, entraînant des erreurs dans les traitements médicaux.
- Interruption des services :
  - Perturbations dans la disponibilité des services de télémédecine, de gestion des stocks médicaux ou d'accès aux dossiers médicaux électroniques en raison de défaillances techniques ou d'attaques par déni de service (DoS).
- Attaques sur les équipements médicaux connectés :
  - Les dispositifs médicaux connectés utilisés pour le suivi à distance des patients peuvent être la cible d'attaques malveillantes, compromettant l'intégrité des données ou perturbant le bon fonctionnement des appareils.
- Non-conformité réglementaire :
  - Risques liés à l'incapacité de se conformer aux exigences du RGPD ou à d'autres réglementations sur la protection des données personnelles, notamment en raison de lacunes dans la gestion des données ou de l'absence de formation adéquate du personnel.

### 4. Identification des Vulnérabilités

Les vulnérabilités potentielles dans le système de MedCare Solutions peuvent inclure :

- Faiblesses dans la gestion des identifiants et mots de passe :
  - Manque de politiques strictes pour la gestion des accès, comme des mots de passe trop faibles ou un manque de mécanismes d'authentification forte (2FA).
- Systèmes obsolètes :
  - Utilisation de logiciels ou de matériels non mis à jour régulièrement, exposant l'entreprise à des vulnérabilités bien connues que des attaquants peuvent exploiter.
- Erreurs humaines :
  - Les erreurs humaines, telles qu'une mauvaise gestion des permissions ou un envoi accidentel de données sensibles à la mauvaise personne, peuvent entraîner une fuite ou une altération des données.
- Infrastructures non sécurisées :

- Les réseaux de communication (en particulier ceux utilisés pour la télémédecine) peuvent être insuffisamment sécurisés, exposant les échanges de données à des attaques de type « man-in-the-middle » (MITM) ou à des interceptions.
- Absence de plan de continuité d'activité (PCA) :
  - Manque de procédures claires pour assurer la reprise rapide des services en cas d'incident majeur (panne technique, cyberattaque, etc.).
- Absence de surveillance continue :
  - Manque de systèmes de détection d'intrusion et de surveillance continue des activités sur les réseaux et les systèmes, ce qui pourrait permettre à des attaques de passer inaperçues pendant un certain temps.

## 5. Évaluation des Risques

Scénarios de risques identifiés :

- Vol ou divulgation de données sensibles des patients :
  - Probabilité : Élevée
  - Impact : Très élevé (perte de confiance des patients, sanctions légales, atteinte à la réputation)
  - Niveau de risque : Très élevé
- Altération des données médicales :
  - Probabilité : Moyenne
  - Impact : Très élevé (erreurs médicales, risques pour la santé des patients)
  - Niveau de risque : Élevé
- Interruption des services de gestion des soins :
  - Probabilité : Moyenne
  - Impact : Élevé (difficulté d'accès aux informations médicales, retard dans la prise en charge des patients)
  - Niveau de risque : Moyen à élevé
- Non-conformité au RGPD :
  - Probabilité : Moyenne
  - Impact : Élevé (sanctions, amendes, perte de confiance)
  - Niveau de risque : Moyen à élevé
- Attaque sur les équipements médicaux connectés :
  - Probabilité : Moyenne
  - Impact : Très élevé (compromission de la sécurité des patients, défaillance des dispositifs médicaux)
  - Niveau de risque : Très élevé

## 6. Traitement des Risques

Pour chaque risque identifié, voici les actions à mettre en place pour réduire la probabilité ou l'impact :

- Pour la fuite de données sensibles :
  - Implémentation de l'authentification multi-facteurs (2FA) pour accéder aux systèmes.
  - Cryptage des données à la fois en transit et au repos.
  - Mise en place de politiques strictes d'accès basées sur les rôles et une gestion centralisée des permissions.
- Pour l'altération des données médicales :
  - Mise en place d'un système de journalisation des accès et des modifications des données.
  - Contrôles réguliers de l'intégrité des données et mises à jour des logiciels pour éviter les vulnérabilités.
- Pour l'interruption des services :
  - Développement d'un plan de continuité des activités (PCA) avec des solutions de redondance.
  - Mise en place de systèmes de détection d'incidents et d'une gestion rapide des incidents.
- Pour la non-conformité au RGPD :
  - Formation continue des employés sur le RGPD et les bonnes pratiques en matière de protection des données personnelles.
  - Audits réguliers pour s'assurer de la conformité continue.
- Pour l'attaque des équipements médicaux :
  - Sécurisation des équipements avec des protocoles de communication chiffrés et des mises à jour régulières des logiciels embarqués dans les dispositifs médicaux.
  - Surveillance continue des réseaux et des systèmes des équipements médicaux.

## Conclusion

L'analyse EBIOS pour MedCare Solutions révèle des risques importants liés à la gestion des données sensibles, aux interruptions de services et à la conformité réglementaire. Cependant, en mettant en œuvre les actions de sécurité et de gestion des risques appropriées, l'entreprise peut minimiser ces menaces et assurer la sécurité et la confidentialité des données des patients tout en offrant des services de qualité.