HackFactorizz

POLITIQUE DE SECURITE
RANSOMWARE PROTECTION SYSTEM

HACKFACTORIZZ
EFREI PARIS
30 AVENUE DE LA REPUBLIQUE
94800 VILLEJUIF

6 JUILLET 2023

HackFactorizz

TABLE DE MATIERE

HackFactorizz

1. Introduction

La cybersécurité est un enjeu majeur de notre époque. Les attaques de ransomware sont devenues une menace significative pour les individus et les organisations, causant souvent des pertes de données importantes et perturbant les opérations quotidiennes.

Notre application anti-ransomware a été conçue pour lutter contre cette menace en offrant une protection efficace et robuste contre les ransomwares. Cette politique de sécurité a été établie pour encadrer et renforcer cette protection, définissant des normes claires de confidentialité, d'intégrité, de disponibilité et de conformité, ainsi que des directives pour le développement sécurisé, la formation et la sensibilisation, et la gestion des incidents.

1.1. Objectif

Cette politique vise à définir les règles et procédures de sécurité qui doivent être mises en œuvre pour protéger l'application anti-ransomware et les données des utilisateurs. Elle vise également à sensibiliser les utilisateurs aux bonnes pratiques de sécurité.

1.2. Champ d’application

Cette politique s'applique à tous les aspects de l'application anti-ransomware, y compris mais sans s'y limiter à la conception, au développement, à la maintenance, au support, et à son utilisation par les utilisateurs et les administrateurs.

1.3. Historique des modifications

Version	Date de modification	Objet de la modification	Auteur
1.0	06/07/2023	Création de la politique de sécurité pour l'application Anti-Ransomware	Michel WU

1.4. Responsibilités

Les responsabilités liées à l'utilisation de l'application anti-ransomware sont partagées entre l'administrateur client et ses collaborateurs. Le tableau ci-dessous fournit une répartition détaillée de ces responsabilités.

Rôles	Responsibilités
Administrateur client	• Il est responsable de l'installation et de la configuration initiale de l'application anti-ransomware. • Il doit surveiller régulièrement l'activité de l'application pour détecter tout comportement suspect ou signe de ransomware. • Il est de la responsabilité de l'administrateur de mettre à jour l'application pour garantir l'efficacité de la protection contre les ransomwares. • Il est responsable de la mise en place et de la gestion des sauvegardes automatiques de données pour prévenir la perte de données en cas d'attaque de ransomware. • En cas d'attaque de ransomware, l'administrateur est responsable de la gestion de l'incident, y compris l'analyse de l'incident, la remédiation et la communication avec les collaborateurs concernés. • En cas d'absence (maladie, vacances, etc.), l'administrateur est toujours responsable. Il doit donc mettre en place un plan de remplacement ou de délégation pour assurer la continuité de la protection.
Collaborateurs	• Ils sont responsables de l'adoption de bonnes pratiques de cybersécurité pour réduire la probabilité d'une attaque de ransomware. • Si un collaborateur remarque une activité suspecte qui pourrait indiquer une attaque de ransomware, il doit le signaler immédiatement à l'administrateur. • En cas d'incident de sécurité, les collaborateurs sont responsables de la coopération avec l'administrateur, y compris le partage des informations nécessaires pour l'analyse de l'incident et le respect des mesures de remédiation définies. • En cas d'absence de l'administrateur, les clients sont responsables du respect du plan de remplacement ou de délégation mis en place par l'administrateur. • Ils doivent suivre les formations et les séances d'information sur la cybersécurité organisée par l'administrateur pour être au courant des dernières menaces et savoir comment les prévenir.

1.5. Définitions générales de la politique

• **Administrateur Client :** Personne ou équipe responsable de la gestion de l'application anti-ransomware pour l'entreprise. Ils sont responsables de la configuration des paramètres, de la surveillance des alertes et de la réponse aux incidents de sécurité.

• **Ransomware** : Un type de logiciel malveillant qui chiffre les fichiers de l'utilisateur, rendant les données inaccessibles jusqu'à ce qu'une rançon soit payée au pirate informatique.

• **Application Anti-Ransomware** : Logiciel utilisé pour protéger les systèmes contre les attaques de ransomware. Il surveille en temps réel l'activité du système, détecte les menaces de ransomware, bloque les fichiers ransomware et alerte les utilisateurs.

• **Collaborateurs** : Dans ce contexte, ce sont les utilisateurs finaux de l'application anti-ransomware. Ils sont responsables de suivre les directives de l'administrateur, de signaler les incidents et d'adopter de bonnes pratiques de cybersécurité.

• **Cybersécurité** : Mesures prises pour protéger un ordinateur, un réseau ou des données contre le vol, les dommages ou l'accès non autorisé.

• **Incident de Sécurité** : Tout événement ayant un impact négatif sur la confidentialité, l'intégrité ou la disponibilité des données ou des systèmes informatiques.

• **Conformité** : L'adhésion aux lois, réglementations, directives et spécifications applicables en matière de cybersécurité.

• **Formation et Sensibilisation** : Processus d'éducation des collaborateurs (clients) sur les menaces à la cybersécurité et sur la manière de les prévenir.

• **Sauvegarde des Données** : Processus de copie des données pour pouvoir les restaurer en cas de perte de données.

• **Tableau de Bord** : Interface utilisateur de l'application qui présente les informations et les contrôles de manière visuelle et facilement accessible.

• **Plan de Remplacement ou de Délégation** : Plan qui définit qui doit assumer les responsabilités de l'administrateur en son absence.

2. POLITIQUE POUR L'ADMINISTRATEUR CLIENT

2.1. Objectif

Assurer une protection maximale contre les menaces de ransomware à travers une utilisation effective et à jour de l'application anti-ransomware.

2.2. Visée

Cette politique vise à guider l'administrateur client à maintenir l'intégrité, la confidentialité et la disponibilité des données en utilisant l'application anti-ransomware.

2.3. Politique

En cas de détection de ransomware, l'administrateur doit suivre les recommandations de réponse à l'incident fournies par l'application.

2.4. Instructions techniques

L'administrateur est chargé de l'installation, de la mise à jour et de la maintenance de l'application anti-ransomware. En cas de détection de ransomware, l'administrateur doit suivre les recommandations de réponse à l'incident fournies par l'application.

2.5. Confidentialité

L'administrateur est responsable de la protection des données de l'entreprise et doit s'assurer que toutes les informations sensibles restent confidentielles.

2.6. Intégrité

L'administrateur doit vérifier régulièrement l'intégrité des sauvegardes et veiller à ce que les données ne soient pas altérées ou perdues lors d'une attaque de ransomware.

2.7. Disponibilité

En cas d'absence de l'administrateur client pour des raisons de santé ou autres, il doit déléguer ses responsabilités à un autre membre de l'équipe de confiance.

2.8. Sécurité

L'accès à l'application doit être sécurisé par un mot de passe fort, qui doit être changé régulièrement. De plus, l'application ne doit être accessible que depuis des appareils sécurisés.

2.9. Formation et sensibilization

L'administrateur doit se tenir à jour sur les dernières menaces de ransomware et les meilleures pratiques de cybersécurité.

2.10. Gestion des accidents

En cas d'incident de sécurité, l'administrateur client doit réagir rapidement en suivant les instructions fournies par l'application, et doit documenter l'incident pour analyse future et amélioration continue.

3. POLITIQUE POUR LES COLLABORATEURS

3.1. Objectif

Maintenir la sécurité des données en se conformant aux directives et aux protocoles établis par l'administrateur client.

3.2. Visée

Cette politique vise à guider les collaborateurs dans leurs interactions avec l'application anti-ransomware et les données sensibles, afin de minimiser les risques de compromission par les ransomwares.

3.3. Politique

Les collaborateurs sont tenus de signaler toute activité suspecte à l'administrateur client immédiatement. Ils doivent également se conformer aux instructions de l'administrateur pour la prévention des ransomwares.

3.4. Instructions techniques

Les collaborateurs ne devraient pas tenter de résoudre eux-mêmes les incidents liés aux ransomwares. Au lieu de cela, ils devraient suivre les procédures d'escalade établies, qui impliquent généralement de signaler l'incident à l'administrateur client.

3.5. Confidentialité

Les collaborateurs doivent veiller à ne pas divulguer d'informations sensibles liées à la sécurité, y compris les détails des protocoles de sécurité ou des incidents, sauf si cela est spécifiquement requis par leur rôle.

3.6. Intégrité

Les collaborateurs doivent s'efforcer de préserver l'intégrité des données en suivant les meilleures pratiques de cybersécurité, comme éviter de cliquer sur des liens suspects ou d'ouvrir des pièces jointes de sources inconnues.

3.7. Disponibilité

Les collaborateurs doivent s'assurer qu'ils ont un accès régulier et fiable à l'application anti-ransomware pour que leur travail ne soit pas interrompu par des problèmes de sécurité.

3.8. Sécurité

Les collaborateurs sont encouragés à maintenir la sécurité de leurs propres systèmes en veillant à l'installation régulière de mises à jour de sécurité et l'utilisation de logiciels antivirus.

3.9. Formation et sensibilisation

Les collaborateurs doivent se tenir informés des dernières menaces de ransomware et des mesures de prévention, telles que mises à jour par l'administrateur client.

3.10. Gestion des accidents

En cas d'incident de sécurité, le collaborateur doit informer immédiatement l'administrateur client et suivre ses instructions pour atténuer et résoudre l'incident.

4. CONFORMITE

L'application sera développée et maintenue conformément à toutes les lois et réglementations pertinentes en matière de protection des données et de sécurité informatique.

5. Conclusion

La sécurité est un élément essentiel de l'application anti-ransomware. Cette politique vise à garantir la protection des informations des utilisateurs et la résilience de l'application face aux menaces de sécurité.

HackFactorizz

HackFactorizz

ACCEPTATION DU PARRAIN

Approuvé par le parrain du projet :

EFREI Paris

Date : 07/07/2023