TOPCERTIFIER
www.topcertifier.com

MÉTHODOLOGIE DE SERVICE PCI DSS

Norme de sécurité des données du secteur des cartes de paiement

TOPCERTIFIER
www.topcertifier.com

INTRODUCTION PCI DSS

TOPCertifier menyajikan Daftar Periksa Analisis Kesenjangan PCI DSS et Disederhanakan pour membantu Anda mengidentifikasinarea di mana organisasi Anda mungkin memerlukan Perbaikan pour la mématuhi PCI DSS (Pembayaran Persyaratan Standar Keamanan Data Industri Kartu). Daftar periksa ini menawarkan hal mendasar kerangka kerja pour l'évaluation Keselarasan Anda dengan PCI DSS et berfungsi sebagai langkah awal menilai kepatuhan Anda.

SECTION 1 : SÉCURITÉ DES DONNÉES

- les données de carte de paiement sont-elles correctement cryptées pendant la transmission et le stockage
- Les données d'authentification sensibles, telles que les numéros CVV, ne sont-elles pas stockées après autorisation
- existe-t-il une politique de sécurisation des données des titulaires de carte et des données d'authentification sensibles

SECTION 2 : SÉCURITÉ DU RÉSEAU ET DU PARE-FEU

- Les configurations réseau et les règles de pare-feu sont-elles régulièrement révisées et mises à jour
- existe-t-il un schéma de réseau illustrant le flux des données des titulaires de carte
- Des politiques et procédures de sécurité sont-elles en place pour sécuriser l'infrastructure réseau

SECTION 3 : CONTRÔLE D'ACCÈS

- Les privilèges d'accès des utilisateurs sont-ils limités en fonction des besoins de l'entreprise
- L'authentification multifacteur est-elle mise en œuvre pour l'accès à distance au réseau
- Les comptes d'utilisateurs sont-ils rapidement désactivés en cas de résiliation ou de changement de rôle

SECTION 4 : GESTION DES VULNÉRABILITÉS

- Les correctifs de sécurité sont-ils appliqués rapidement pour remédier aux vulnérabilités
- existe-t-il un processus d'analyse des vulnérabilités et de tests d'intrusion
- Les correctifs de sécurité critiques sont-ils examinés et hiérarchisés en fonction du risque

SECTION 5 : POLITIQUES ET PROCÉDURES DE SÉCURITÉ

- Les politiques et procédures de sécurité complètes sont-elles documentées et diffusées
- existe-t-il un programme de formation de sensibilisation à la sécurité pour les employés
- Les politiques de sécurité sont-elles examinées et mises à jour si nécessaire

SECTION 6 : SURVEILLANCE ET JOURNALISATION

- Les événements et journaux de sécurité sont-ils régulièrement examinés et surveillés
- existe-t-il un processus pour émettre des alertes en temps réel en cas d'activités suspectes
- Des procédures de réponse aux incidents et de reporting sont-elles établies

SECTION 7 : RÉPONSE AUX INCIDENTS

- existe-t-il un plan de réponse aux incidents décrivant les étapes à suivre pour résoudre les incidents de sécurité
- Les employés sont-ils formés sur la manière de reconnaître et de signaler les incidents de sécurité ?
- existe-t-il un processus documenté pour l'analyse et l'amélioration post-incident

SECTION 8 : SÉCURITÉ PHYSIQUE

- Des contrôles d'accès physiques sont-ils en place pour empêcher tout accès non autorisé aux données des titulaires de carte
- l'accès aux zones sécurisées est-il restreint et surveillé
- La vidéosurveillance et les journaux de visiteurs sont-ils conservés pour les zones sensibles

SECTION 9 : PRESTATAIRES DE SERVICES TIERS

- Les fournisseurs tiers sont-ils évalués pour leur conformité à la norme PCI DSS
- Des accords écrits avec les prestataires de services sont-ils en place pour garantir la protection des données des titulaires de carte
- Existe-t-il un processus de surveillance et d'évaluation des pratiques de sécurité des tiers

Veuillez noter que cette liste de contrôle fournit un aperçu de haut niveau et qu'il est essentiel d'effectuer une analyse approfondie spécifique aux processus et au contexte de votre organisation. De plus, c'est Il est recommandé de collaborer avec des experts ou des consultants PCI DSS pour mener une évaluation complète analyse des écarts pour votre organisation.