TOPCERTIFIER
www.topcertifier.com

SERVICEMETOD
PCI DSS

Betalkortsindustrins datasäkerhetsstandard.

TOPCERTIFIER
www.topcertifier.com

INTRODUKTION PCI DSS

TOPCertifier presenterar en förenklad PCI DSS Gap Analysis Checklist som hjälper dig att identifiera områden där din organisation kan behöva förbättringar för att följa PCI DSS (Payment Card Industry Data Security Standard) krav. Denna checklista erbjuder en grundläggande ramverk för att utvärdera din anpassning till PCI DSS och fungerar som ett första steg i bedöma din efterlevnad.

AVSNITT 1: DATASÄKERHET

- är betalkortsdata korrekt krypterad under överföring och lagring
- Är känsliga autentiseringsdata, såsom CVV-nummer, inte lagrade efter auktorisering
- finns det en policy för att säkra kortinnehavarens data och känsliga autentiseringsdata

AVSNITT 2: SÄKERHET FÖR NÄTVERK OCH BRANDVÄGGS

- Ses nätverkskonfigurationer och brandväggsregler regelbundet över och uppdateras
- finns det ett nätverksdiagram som illustrerar flödet av korthållardata
- Finns säkerhetspolicyer och rutiner på plats för att säkra nätverksinfrastruktur

AVSNITT 3: ÅTKOMSTKONTROLL

- Är användarnas åtkomstbehörigheter begränsade baserat på företagets behov att veta
- är multifaktorautentisering implementerad för fjärråtkomst till nätverket
- Avaktiveras användarkonton omedelbart vid uppsägning eller rolländringar

AVSNITT 4: HANTERING AV SÅRBARHET

- Används säkerhetskorrigeringar omedelbart för att åtgärda sårbarheter
- finns det en process för sårbarhetsskanning och penetrationstestning
- Är kritiska säkerhetskorrigeringar granskade och prioriterade utifrån risk

AVSNITT 5: SÄKERHETSPOLICIER OCH PROCEDURER

- Är omfattande säkerhetspolicyer och -procedurer dokumenterade och sprids
- finns det ett utbildningsprogram för säkerhetsmedvetenhet för anställda
- Säkerhetspolicyer granskas och uppdateras vid behov

AVSNITT 6: ÖVERVAKNING OCH LOGGNING

- Säkerhetshändelser och loggar granskas och övervakas regelbundet
- finns det en process för att utföra realtidsvarning för misstänkta aktiviteter
- Finns rutiner för incidenthantering och rapportering

AVSNITT 7: SVAR

- finns det en incidentresponsplan som beskriver steg för att åtgärda säkerhetsincidenter
- Är anställda utbildade i hur man känner igen och rapporterar säkerhetsincidenter
- finns det en dokumenterad process för analys och förbättring efter incidenten

AVSNITT 8: FYSISK SÄKERHET

- Finns fysiska åtkomstkontroller på plats för att förhindra obehörig åtkomst till kortinnehavarens data
- är tillgång till säkra områden begränsat och övervakat
- Förs videoövervakning och besöksloggar för känsliga områden

AVSNITT 9: TREDJEPARTS TJÄNSTELEVERANTÖRER

- Är tredjepartsleverantörer bedömda för PCI DSS-kompatibilitet
- Finns skriftliga avtal med tjänsteleverantörer för att säkerställa kortinnehavarens dataskydd
- Finns det en process för att övervaka och utvärdera tredjeparts säkerhetspraxis

Observera att denna checklista ger en översikt på hög nivå, och det är viktigt att utföra en grundlig analys specifik för din organisations processer och sammanhang. Dessutom är det rekommenderas att samarbeta med PCI DSS-experter eller konsulter för att genomföra en omfattande gapanalys för din organisation.