TOPCERTIFIER
www.topcertifier.com

PALVELUMENETELMÄT PCI DSS

Maksukorttialan tietoturvastandardi.

TOPCERTIFIER
www.topcertifier.com

JOHDANTO PCI DSS

TOPCertifier esittelee yksinkertaistetun PCI DSS Gap Analysis -tarkistuslistan, joka auttaa sinua tunnistamaan alueet, joilla organisaatiosi saattaa tarvita parannuksia noudattaakseen PCI DSS (Payment Card Industry Data Security Standard) vaatimukset. Tämä tarkistuslista tarjoaa perustiedot puitteet PCI DSS:n mukautumisen arvioimiseksi ja toimii ensimmäisenä askeleena arvioimalla vaatimustenmukaisuuttasi.

OSA 1: TIETOTURVA

- onko maksukortin tiedot oikein salattu siirron ja tallennuksen aikana
- Ovatko arkaluontoiset todennustiedot, kuten CVV-numerot, tallennetut valtuutuksen jälkeen
- onko olemassa käytäntöä kortinhaltijatietojen ja arkaluonteisten todennustietojen suojaamiseksi

OSA 2: VERKKO JA PALOMUURI TURVALLISUUS

- Tarkistetaanko ja päivitetäänkö verkkokokoonpanot ja palomuurisäännöt säännöllisesti
- onko olemassa verkkokaavio, joka havainnollistaa kortinhaltijatietojen kulkua
- Ovatko tietoturvakäytännöt ja -menettelyt käytössä verkkoinfrastruktuurin turvaamiseksi

OSA 3: PÄÄSYHALLINTA

- Onko käyttäjien käyttöoikeuksia rajoitettu liiketoiminnan tarpeiden perusteella
- on monitekijätodennus toteutettu verkon etäkäyttöä varten
- Poistetaanko käyttäjätilit välittömästi käytöstä poistamisen tai roolin vaihtuessa

OSA 4: HAAVATTOMUUSTEN HALLINTA

- Onko tietoturvakorjaukset asennettu viipymättä haavoittuvuuksien korjaamiseksi
- onko olemassa prosessi haavoittuvuuden skannaamiseksi ja läpäisevyyden testaamiseksi
- Poistetaanko käyttäjätilit välittömästi käytöstä poistamisen tai roolin vaihtuessa

OSA 5: TURVALLISUUSPOLITIIKAT JA MENETTELYT

- Onko kattavat turvallisuuskäytännöt ja -menettelyt dokumentoitu ja levitetty
- onko työntekijöille turvatietoisuuskoulutusohjelma
- Tarkistetaanko ja päivitetäänkö tietoturvakäytännöt tarpeen mukaan

OSA 6: SEURANTA JA KIRJAUS

- Tarkistetaanko ja valvotaanko turvallisuustapahtumat ja lokit säännöllisesti
- onko olemassa prosessi reaaliaikaisten hälytysten suorittamiseksi epäilyttävistä toiminnoista
- Onko vaaratilanteisiin reagointi- ja raportointimenettelyjä luotu

KOHTA 7: TAPAHTUMAN TOIMINTA

- onko olemassa vaaratilanteiden reagointisuunnitelma, jossa esitetään turvavälikohtausten käsittelyvaiheet
- Onko työntekijöitä koulutettu tunnistamaan ja raportoimaan tietoturvahäiriöt
- onko olemassa dokumentoitu prosessi tapahtuman jälkeistä analysointia ja parantamista varten

OSA 8: FYYSINEN TURVALLISUUS

- Onko käytössä fyysisiä kulunvalvontalaitteita, joilla estetään luvaton pääsy kortinhaltijan tietoihin
- pääsyä suojatuille alueille on rajoitettu ja valvottu
- Pidetäänkö herkkien alueiden videovalvontaa ja vierailijalokeja

OSA 9: KOLMANSIEN PALVELUN TARJOAJAT

- Onko kolmannen osapuolen toimittajien PCI DSS -yhteensopivuus arvioitu
- Onko palveluntarjoajien kanssa tehty kirjallisia sopimuksia kortinhaltijoiden tietosuojan varmistamiseksi
- Onko olemassa prosessi kolmannen osapuolen tietoturvakäytäntöjen valvomiseksi ja arvioimiseksi

Huomaa, että tämä tarkistuslista tarjoaa korkean tason yleiskatsauksen, ja on välttämätöntä suorittaa a perusteellinen analyysi organisaatiosi prosesseista ja kontekstista. Lisäksi se on suositellaan vuorovaikutusta PCI DSS -asiantuntijoiden tai konsulttien kanssa suorittaakseen kattavan aukkoanalyysi organisaatiollesi.