

PCI DSS er en forkortelse for Payment Card Industry - Data Security Standard.

Standarden er lavet af "Payment Card Industry". PCI DSS Gruppen blev stiftet af nogle af de store kreditkort virksomheder heriblandt Visa, MasterCard og American Express med det formål at lave en ensartet høj sikkerhed omkring elektronisk betaling, således at manglende sikkerhed ikke ville undergrave tilliden til online betaling.

Standarden omfatter en række krav til sikkerheden, herunder udformning af politikker og procedurer, netværksarkitektur, software design og en række andre foranstaltninger. Yderlig information kan hentes her: <https://www.pcisecuritystandards.org>

Hvem gælder den for?

Alle virksomhederne der modtager online betalinger via betalingskort er omfattet af standarden: "PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted". Det betyder i praksis, at alle virksomheder der behandler, opbevarer eller transmitterer betalingskort-oplysninger skal efterleve PCI DSS. Ifølge standarden gælder det også for virksomheder, der har indgået en service-aftale med en formidler af f.eks. online transaktioner til betaling i en e-handels butik.

Hvor meget skal kontrolleres

Det er mængden af kortdata der bestemmer hvilket niveau af kontrol der skal foretages. Har man eksempelvis flere end 20.000 kreditkort transaktioner om året er man omfattet af reglen omkring kvartårige penetrationstests. Disse test skal gennemføres af en "Approved Scanning Vendor" (ASV). Har man færre transaktioner, er det stadigvæk et krav fra VISA og MasterCard, at man skal overholde sikkerhedskravene, men de udfører ikke kontrol med det.

Konsekvensen af manglende PCI DSS efterlevelse, kan medføre at selskaberne bag PCI, jævner deres aftaler, fjerner en butiks mulighed for at modtage betaling med blandt andre VISA og Mastercard.

Efterlevelse af PCI DSS standarden

Ezenta er certificeret ASV og kan hjælpe alle der er underlagt PCI DSSs krav omkring de kvartårige penetrations tests. For at sikre mindst mulige driftsforstyrrelser og andre u hensigtsmæssigheder tilrettelægger en konsulent fra Ezenta A/S i

samarbejde med den netværks- eller sikkerhedsansvarlige gennemførelse af penetrationstesten.

Der indsamles relevant information og netværket dokumenteres med udgangspunkt i den nærværende aftale. Herefter aftales der præcist hvilke komponenter/elementer i netværket der skal testes og hvornår de pågældende test udføres. Disse informationer samles og indgår i en projektplan som Ezenta udfærdiger.

Der udføres en lang række systematiske angreb på installationen. Resultatet af scanningen afleveres i en overskuelig rapport, der giver en status på individuelle komponenters sikkerhedsniveau herunder identifikation af kendte sårbarheder.

Rapporten besvarer blandt andet:

- Om man er PCI compliant
- Hvilke sårbarheder er fundet i systemet?
- Hvor alvorlige er de?
- Hvordan kan man rette op på dem?

Rapporten der udarbejdes på engelsk og indeholder et ledelses resumé bestående af en kort opsummering og konklusion. Denne vedlægges en detaljeret teknisk specifikation der kan benyttes til at lukke evt. identificerede sikkerhedshuller på en nem og overskuelig måde.

Rapporten klassificerer de identificerede sårbarheder, således at der er mulighed for at fokusere på at løse de sikkerhedsopgaver, der giver det største udbytte.

Ezenta
Approved Scanning Vendors
Certificate Number
3889-01-02