



Kontrollera att du uppfyller PCI DSS-kraven så minskar du risken

– både för dig och dina kunder!

Checklista

Bindande krav på verksamhetens hantering av kortinformation.

PCI DSS är ett omfattande regelverk som ska säkerställa att kortinformation hanteras säkert i alla led. Många av kraven handlar om IT-miljön, men höga krav ställs också på säljföretagens hantering i den dagliga verksamheten. Det handlar om hur du hanterar kvittokopior, elektroniska media, lösenord till betalterminalen, behörigheter m.m. Nedan hittar du en sammanställning över några av de viktigaste grundläggande PCI DSS-kraven som Visa och MasterCard för närvarande har definierat och som ditt företag i sitt inlösenavtal med Euroline har förbundit sig att följa.

Testa säkerheten i din verksamhet.

Om du inte kan svara JA på samtliga punkter betyder det att det finns brister som du snarast bör åtgärda. Det är alltid du som har ansvaret för hanteringen av kortdata i din verksamhet, både den fysiskt och digitalt lagrade informationen.

1. Dokument med kortnummer och media som hanterar kortinformation.

Ja Nej

Förvarar ni alla pappers- och elektroniska media med kortinformation på ett säkert sätt (t ex inlåst), där endast behöriga har tillgång till dem? (Sådan media är datorer, elektronisk media, nätverks- och kommunikationshårdvara, tele- kommunikationsledningar, papperskvitton, pappersrapporter och fax.)

Håller du strikt kontroll över förvaringen av och åtkomst till media som innehåller kortinformation?

Förstör du media med kortinformation när det inte längre behövs för verksamheten?

2. Interna rutiner och handlingsprogram.

Har all personal som hanterar bokföring och administration, inklusive kassapersonalen, fått information om vilket ansvar de har för kortinformation och vilka rutiner som gäller?

Är tillgången till datorutrustning och kortinformation begränsad till de personer vars arbete kräver detta?

Specificerar säkerhetspolicys och rutiner klart och tydligt vilket ansvar anställda, leverantörer och uppdragstagare har vad gäller informations-säkerhet?

Har ni upprättat incidentplaner och eskaleringsrutiner och förankrat dessa i verksamheten för att säkerställa en effektiv och lämplig hantering i alla uppkomna situationer?

Ja **Nej**

Finns det ett formellt säkerhetsutbildningsprogram för att lära alla anställda vikten av datasäkerhet vid hantering av betalkort?

3. Externa leverantörer.

Finns följande krav i kontraktet när företaget tecknar avtal med tjänsteleverantör som tar del av företagets kortinformation?

- Att leverantören av tjänsten efterlever kortindustrins datasäkerhetsstandard PCI DSS?
- Att leverantören ansvarar för säkerheten kring den kortinformation som leverantören förvarar?

4. Hantering av din betalterminal.

Är betalterminalen placerad så att du kan ansvara för att obehöriga inte kan manipulera den?

Har företaget rutiner för att hantera betalterminalens lösenord som innebär att:

- enbart behörig personal har tillgång till lösenorden?
- lösenorden förvaras säkert, så att de inte kan komma i orätta händer?
- all personal med tillgång till ett lösenord har fått utbildning och instruktioner om att inte lämna ut det till någon?
- lösenord byts med jämna mellanrum och att ett lösenord som du misstänker har lämnats ut till någon obehörig omedelbart byts ut?

Försäkrar du dig om att innehållet i företagets tekniska utrustning inte blir åtkomligt för någon obehörig i samband med service?

Försäkrar du dig om att inga kortnummer finns lagrade i er tekniska utrustning vid "skrotning" eller försäljning?

Ser du till att teknisk service via extern inloggning endast sker efter det att du har godkänt uppkoppling, och att utloggning sker efter genomförd service?

Fortsättning på nästa sida ►

Kontakta oss om du vill ha hjälp eller råd.

Vill du ha hjälp med testet eller råd kring hur du bäst anpassar verksamheten till kraven i PCI DSS är du välkommen att kontakta vår Företagsservice på telefon 08-14 69 14 eller via e-post: euoline@seb.se

forts.

5. Hantering av data för autentisering och auktorisation.

Ja Nej

Uppfyller företagets alla system följande krav vad gäller lagring av känslig data för autentisering?

- Ser ni till att inte lagra all auktorisationsdata som ni får ut från kortets magnetspår, chip eller på annat ställe?

(För att minimera risken ska ni bara lagra de dataelement som är nödvändiga för verksamheten. Normalt räcker det att lagra: kontohavarens namn, kortnummer, utgångsdatum och servicekod.)

- Är du säker på att auktorisationsdata aldrig lagras efter slutförd auktorisation, inte ens på loggar? (Det gäller även krypterad information.)

- Kan du garantera att ni inte lagrar säkerhetskoden (CVV2/ CVC2), som används för att verifiera transaktioner där kortet inte är närvarande vid köptillfället (card-not-present)?

- Ser du till att ni inte lagrar personligt identifieringsnummer (PIN) eller krypterat PIN block?

- Finns policys, procedurer och rutiner för att förhindra att okrypterade kortnummer skickas via e-post?

PCI DSS

För att ytterligare höja säkerhetsnivån i de globala betalningssystemen har kortindustrin enats om en gemensam säkerhetsstandard. Standarden heter Payment Card Industry Data Security Standard (PCI DSS) och omfattar samtliga kortnätverk. Det innebär att alla; sälj företag, inlösare och andra som lagrar eller överför kortinformation, måste uppfylla kraven i PCI DSS för att skydda de internationella betalningssystemen. Att inte uppfylla kraven medför stora finansiella risker och i förlängningen förlorad rätt att ta emot kort som betalningsmedel.

EUROLINE[®]



VISA

