Säkra kortinformationen

Visa och Mastercard har enats om en säkerhetsstandard, Payment Card Industry, PCI Data Security Standard, som också American Express, Diners Club och JCB har anslutit sig till. PCI säkerhetsstandard beskriver hur kortnummer och annan transaktionsinformation ska hanteras och gäller såväl vid betalningar där kortet är fysiskt inblandat som vid telefonorder och handel på internet.

Vad är syftet med PCI?

Syftet med PCI är att säkerställa att alla som hanterar kortinformation gör det på ett sådant sätt att obehöriga inte kommer åt informationen. Du har ansvar för att ditt företags kort- och kundinformation inte hamnar i orätta händer.

PCI säkerhetsstandard gäller för alla som hanterar, samlar in, lagrar och överför kortinformation. Fysiska dokument och elektronisk media (till exempel kvitton, transaktionsloggar och transaktionsrapporter) som innehåller kortinformation ska lagras på en säker plats, som endast behöriga personer har tillgång till.

Vad innebär detta för ditt företag?

Du behöver:

- undvika att lagra kortinformation eller annan känslig information
- säkerställa att kortinformation som lagras är krypterad
- säkerställa att den fullständiga kortinformationen i kortets magnetspår eller chip samt kortets säkerhetskod (de tre sista siffrorna som är tryckta i signaturfältet) inte lagras efter avslutad kortbetalning*
- säkerställa att kortnummer alltid trunkeras, det vill säga aldrig trycks i sin helhet på kvitton eller annat tryckt media*
- radera kortinformation som inte används
- säkerställa att teknisk service genomförs på ett sätt så att kortinformation inte hamnar i orätta händer
- behörighetsskydda tillgången till kortinformation med användaridentiteter och lösenord
- säkerställa att utgivna behörigheter inte sprids till obehöriga
- säkerställa att användandet av behörigheter kan spåras
- säkerställa de interna rutinerna för att undvika insiderbrott eller externa intrång i systemet
- installera och underhålla säkerhetsprogramvara och skydda systemet mot datavirus
- regelbundet genomföra tester av säkerhetssystemet
- utbilda och ge instruktioner till behörig personal som har tillgång till den tekniska utrustningens lösenord.

*Krav du ska ställa på den tekniska utrustningen.

Hur berörs ditt företag av PCI?

För att bedöma vilka åtgärder som ska genomföras har Visa och Mastercard tagit fram olika utvärderingsmetoder. Av tabellen nedan framgår vilka företag som ska använda de olika metoderna och hur frekvent utvärderingarna bör genomföras.

Nivå	Kriterier	Granskning på plats (On-site Audit)	Självgranskning (Self Assessment)	Extern nätverksscanning
1	Säljföretag med mer än 6 miljoner korttransaktioner från Visa eller mer än 6 miljoner korttransaktioner från Mastercard, per år	Årligen	Inget krav	Kvartalsvis
2	Säljföretag med mellan 1 - 6 miljoner korttransaktioner från Visa eller mellan 1- 6 miljoner korttransaktioner från Mastercard, per år	Årligen	Inget krav	Kvartalsvis
3	Säljföretag inom e-handel med mellan 20 000 och 1 miljoner korttransaktioner från Visa eller mellan 20 000 och 1 miljoner korttransaktioner från Mastercard, per år	Inget krav	Årligen	Kvartalsvis
4	Övriga säljföretag	Inget krav	Rekommenderas årligen	Rekommenderas årligen

Inom Nivå 4 finns företag, som till följd av sin branschtillhörighet, ska genomgå en certifiering. Berörda företag kommer att kontaktas av Swedbank.

Vad innebär utvärderingsmetoderna?

- Granskning på plats – företaget anlitar en revisor, som har godkänts** av Mastercard och Visa. Revisorn genomför en granskning av säkerhetsrutiner samt hantering och lagring av transaktionsinformation, på plats.
- Självgranskning – består av ett formulär som företaget fyller i.
- Extern nätverksscanning - verktyg från godkänd leverantör (Approved Scanning Vendor) skannar externa IP-adresser för att upptäcka eventuella säkerhetsbrister i datornätverk.

** En förteckning över de företag som är godkända av Visa och Mastercard, samt vilka länder de är verksamma i, hittar du på www.pcisecuritystandards.org.

Vill du veta mer om PCI? Läs vidare på www.pcisecuritystandards.org