Sikre kortoplysninger

Visa og Mastercard har en fælles sikkerhedsstandard, Payment Card Industry - Data Security Standard, PCI-DSS, som også American Express, Diners Club og JCB har tilsluttet sig. PCI-standarden beskriver, hvordan kortnummer og andre transaktions-oplysninger skal håndteres og gælder såvel ved betalinger, hvor kortet er fysisk involveret, som ved telefonordre og e-handel.

Berører PCI-standarden jer?

Formålet med PCI er at sikre, at alle, som håndterer kortoplysninger, gør det på en måde, så uvedkommende ikke får adgang til oplysningerne. I har ansvaret for, at virksomhedens kort- og kundeinformation ikke havner i de forkerte hænder.

PCI-standarden bygger på Visa-programmet Account Information Security, AIS, og Mastercards program Site Data Protection, SDP. PCI sikkerhedsstandard vedrører for alle, som håndterer, indsamler, lagrer og overfører kortoplysninger. Fysiske dokumenter og elektroniske medier (f.eks. kvitteringer, transaktionslogger og transaktionsrapporter), som indeholder kortoplysninger, skal opbevares et sikkert sted, som kun autoriserede personer har adgang til.

Det betyder, at jeres virksomhed skal:

Du behöver:

- undgå at opbevare kortoplysninger eller anden følsom information
- sikre, at kortoplysninger, som gemmes, er krypterede
- sikre, at de fuldstændige kortoplysninger i kortets magnetspor eller chip samt kortets kontrolkode (de tre sidste cifre, som er trykt i signaturfeltet) ikke gemmes efter afsluttet kortbetaling*
- sikre, at kortnummeret altid trunkeres, det vil sige aldrig bliver trykt i sin helhed på kvitteringen eller andet trykt medie*
- slette kortoplysninger, som ikke bruges
- sikre, at der udføres teknisk service på en sådan måde, at kortoplysninger ikke havner i de forkerte hænder
- beskytte adgangen til kortoplysninger med brugernavn og adgangskode
- sikre, at tildelte adgange ikke overdrages til uautoriserede personer
- sikre, at brugen af adgange kan spores
- sikre de interne rutiner for at undgå insiderfor brydelser eller ekstern indtrængen i systemet
- installere og vedligeholde sikkerhedsprogrammer og beskytte systemet mod datavirus
- foretage regelmæssige tests af sikkerhedssystemet
- Uddanne og give instruktioner til det ansvarlige personale som har adgang til det tekniske udstyrs adgangskoder.

* Krav I skal stille til det tekniske udstyr.

Hvordan berøres jeres virksomhed?

For at bedømme hvilke foranstaltninger der skal gennemføres, har Visa og Mastercard udviklet forskellige vurderingsmetoder. Af tabellen nedenfor fremgår det, hvilke virksomheder som skal benytte de forskellige metoder, og hvor ofte vurderingerne skal foretages.

Niveau	Kriterier	Kontrol på stedet (On-Site Audit)	Intern kontrol (Self-Assessment)	Ekstern netværks-scanning (Network Security Scan)
1	Virksomheder med mere end 6 millioner korttransaktioner pr. år, Visa eller Mastercard	Årligt	Ingen krav	Kvartalsvis
2	Virksomheder med mellem 1 og 6 millioner korttransaktioner pr. år, Visa eller Mastercard	Årligt	Ingen krav	Kvartalsvis
3	Virksomheder inden for e-handel med mellem 20.000 og 1 million korttransaktioner pr. år, Visa eller Mastercard	Ingen krav	Årligt	Kvartalsvis
4	Øvrige virksomheder	Ingen krav	Anbefales årligt	Anbefales årligt

På Niveau 4 er der virksomheder, som på grund af deres branche skal igennem en certificering.
Berørte virksomheder bliver kontaktet af Swedbank Pay.

Hvad indebærer vurderingsmetoderne?

- Kontrol på stedet – virksomheden benytter en kontrollant, som er certificeret** af Mastercard og Visa. Kontrollanten gennemfører en undersøgelse af virksomhedens sikkerhedsrutiner samt håndtering og lagring af transaktionsinformation.
- Intern kontrol – består af en formular, som virksomheden udfylder.
- Ekstern netværksscanning – værktøj fra godkendt leverandør som scanner eksterne IP-adresser for at opfange eventuelle sikkerhedsbrister i datanetværket.

** I finder en fortegnelse over de virksomheder, som er godkendt af Visa og Mastercard, på www.pcisecuritystandards.org. Af listen fremgår det i hvilke lande selskaberne er aktive i.

Vil I vide mere om PCI? Læs videre på www.pcisecuritystandards.org