En överlevnadsguide för PCI DSS

Sentor förklarar vanliga begrepp och förkortningar

Centrala begrepp

	Betyder	Innebär
AoC	Attestation of Compliance	AoC är en förkortad redogörelse för vad handlare eller SP är granskade och godkända gällande. Skrivs av QSA och kan lämnas till andra organisationer som ett bevis på vad de är godkända för.
PA-DSS	Payment Application Data Security Standard	Annan standard inom PCI som adresserar betalapplikationer (i PED eller PoS)
PCI DSS	Payment Card Industry Data Security Standard	Det regelverk som företag kontrolleras mot. 400 krav och 1200+ kontrollpunkter, även om det är ovanligt att handlare kontrolleras mot samtliga punkter.
RoC	Report on Complaince	Rapport som, i detalj beskriver resultatet av PCI DSS granskningen. Enormt dokument där tomma mallen är på 252 sidor och färdiga resultatet ofta är på 400+ sidor. Fylls i av QSA, lämnas till inlösande bank.
SAQ	Self Assessment Questionaire	SAQer är självdeklarationer baserade på de olika sorters betalflöden som finns. SAQer är riktat mot mindre organisationer. En SAQ får man som handlare av sin inlösande bank.

Roller

	Betyder	Innebär
Acquiring Bank	Inlösande bank	Bank som har förhållandet mellan handlare och inlösen av kundernas betalkort
ASV	Approved Scanning Vendor	Företag som är godkända av PCI SSC för att genomföra externa sårbarhetsscanningar.
Brands	Visa, MasterCard, American Express, JCB och Diners	De varumärken som skapade och styr PCI SSC. Deras roll är även att utkräva böter vid ev. incidenter eller när företag inte uppnår full efterlevnad
Issuer	Utgivare	Den organisation som ger ut korten – kan vara en bank.
Merchant	Handlare	Handlare tar emot betalkort från något av varumärkena, Kan ha han en kombination av kortflöden i butiker, e-handel, restauranger etc.
PSP	Payment Service Provider	En SP som tar emot trafiken från Merchant. Kan ofta ha andra tjänster så som lagring av PAN för att underlätta konverteringsgrad vid köp i e-handel.
QSA	Qualified Security Assessor	En QSA är godkänd av PCI SSC att genomföra PCI DSS på-plats granskningar. Måste arbeta för ett QSA-företag, genomgå årlig certifiering och ha separat ansvarsförsäkring för PCI.
SP	Service Provider	Företag som är direkt inblandade i hantering, lagring eller kommunikation av andras kortdata. Om en SP har en egen AoC så avlastar de handlarens krav. Om SP saknar AoC som omfattas de av handlarens granskning. SP måste inte bara leva upp till sina handlares krav – utan även skydda kortdata mellan olika handlare. Exempel på SP-tjänster på är drift av datahall, nätverk eller brandväggar.

sentor

SSC	Security Standards Council	Organisationen som äger PCI DSS och PA DSS. SCC underhåller, utvecklar, styr, hanteringar utbildning för standarderna.

Tekniska termer

	Betyder	Innebär
CC	Compensating Controls	Kompenserande kontroller är ett begrepp som används när en handlare inte kan leva upp till kravet så som det är utformat. Det kan vara av lagliga, tekniska eller affärsskäl. Man kan då istället införa en CC som: •Möter upp syftet och nivån av kravet i PCI DSS •Ger samma nivå av skydd som kravet i PCI DSS •Ska vara “above and beyond” andra krav •Kompensera för den extra risk som uppstår när man inte lever upp till kravet i PCI DSS
CDE	Cardholder Data Environment	CDE omfattar personal, processer och den teknologi som lagrar, hanterar och sänder CHD eller SAD. Omfattningen av CDE bestämmer hur omfattande granskningen kommer att bli.
CHD	Card Holder Data	Som minst innehåller CDH ett omaskat PAN. Följande ingår i CHD: PAN, Innehavarens namn, service kod samt utgångsdatum. Även SAD räknas som CHD, men dessa får inte lagras.
P2PE	Point to Point Encryption	SAQ för PED där godkänd utrustning inte kan läcka information. Minskar scopet drastiskt. PCI listar godkända produkter, så även Pan Nordic Card Assciation.
PAN	Primary Account Number	Unikt betalkortnummer utgivet med varumärket och utgivarens loggor, kortet kan vara fysiskt eller virtuellt.
PED	Pin Entry Device	Den enhet där du matar in din PIN-kod.
PIN	Personal Identification Number	PIN-koden till kortet, den hemlighet som endast användaren känner till för att styrka sin identifiering med kortet. PIN-kod är naturlig i Sverige, men kontroversiellt i andra länder där det som regelana används bara till bankomater.
PoS	Point of Sale	Kassa på svenska. Hård- och mjukvara som används för att processa betalningar hos handlaren.
SAD	Sensitive Authentication Data	Delmängd av PAN som innehåller extra känslig information. SAD får inte lagras efter att köp är genomfört. •Hela innehållet från magnetkortet/Chip •CVV2 •PIN kod eller PIN-block
SSL	Secure Sockets Layer	Standard för kryptering mellan webbläsare och server för att säkra sekretess och siktighet. Inte längre vad PCI DSS kallar “Strong Encryption”.
TLS	Transport Layer Security	Skapad med målet att ge sekretess och riktighet mellan två applikationer genom en krypterad tunnel. Efterträdare till SSL. Tidigare version av TLS kan inte längre ses “Strong Encryption” enligt PCI DSS.