

I er velkomne til at kontakte os for at høre om mulighederne, inkl. hvordan I evt. selv kan tjekke sikkerheden ved brug af et effektivt skanningsværktøj.

*Se i øvrigt PCI Councils beskrivelse af, hvad der kræves for at blive compliant:
https://www.pcisecuritystandards.org/pdfs/infosupp_6_6_applicationfirewalls_codereviews.pdf*

3: Lancering af PA-DSS-standarden

PCI Council har lanceret PA-DSS-standarden i april 2008. Denne standard er en separat PCI-standard, som skal overholdes af firmaer, som udvikler programmer til håndtering af kreditkortdata. Den gælder kun for firmaer, som udvikler programmer med henblik på videresalg - ikke hvis de kun udvikler til eget brug.

PA-DSS-standarden bygger på VISA's tidligere PABP-standard, som PCI Council har overtaget og opdateret. Standarden er i store træk en delmængde af PCI-DSS-standarden, og indeholder kun de dele der har med applikationsudvikling at gøre. Alle elementer vedrørende drift er fjernet. Med andre ord bliver dét, der før var en best practice guideline til at udvikle en sikker applikation (nemlig PABP-standarden) nu til et krav, der skal overholdes.

I praksis bliver det sådan, at virksomheder med programmer til håndtering af kreditkortdata vil blive annonceret på PCI Councils hjemmeside, når de har opnået en certificering efter PA-DSS-standarden. Virksomheder, der arbejder med kreditkort, må fremover kun benytte applikationer og versioner fra de virksomheder, som er at finde på godkendelseslisten.

En godkendelse varer i 2 år, eller indtil der lanceres en ny version af standarden.

Kravet er allerede trådt i kraft i Sverige, og vi forventer, at kravet vil blive kommunikeret til de berørte virksomheder i Danmark i løbet af det kommende kvartal.

PCI Council publicerer alle godkendte applikationer på deres website: [Link](#)

4: Underleverandører SKAL være PCI-godkendte

Det er vigtigt, at I er opmærksomme på, at det er jeres ansvar, at jeres underleverandører opfylder PCI-standarden. Ifølge PCI-standarden skal I nemlig sikre jer, at hele jeres løsning er PCI-godkendt, også selvom dele af den er outsourcet til andre. Derfor skal I være opmærksomme på alle de samarbejdspartnere og underleverandører, der har adgang til jeres kortdata, som fx eksterne it-leverandører, servicefirmaer og managed hosting-firmaer.

I de kontrakter, I har tegnet med underleverandører, bør I derfor sørge for at inkludere et krav om, at underleverandørerne skal være PCI-godkendte, og at de selv er ansvarlige for at sikre, at dét, de leverer, ikke bliver hacket. Hvis det alligevel skulle ske, bør jeres aftale sikre jer, at I kan sende eventuelle bøder og erstatningskrav videre til underleverandørerne.

NB: Statistikkerne viser, at halvdelen af de korttyverier, der sker på verdensplan, er forårsaget af underleverandører – enten pga. manglende sikkerhed, eller fordi deres medarbejdere svindler.

5: Ny version af PCI-standarden er på vej

Til oktober 2008 udkommer den nye version af PCI-standarden fra PCI Council. Vi kender endnu ikke hele indholdet, men vi kan generelt informere om at:

- der kommer enkelte nye krav
- det kommer primært tydeligere formuleringer
- der bliver ryddet op i krav, der overlapper hinanden
- der kommer ekstra beskrivelser af hvordan PCI-scoping skal foretages

FortConsult får henover sommeren den nye standard til gennemlæsning for at give feedback til PCI Council. Vi forventer derfor, at vi kan fortælle meget mere efter sommerferien og ser frem til at holde jer underrettede om udviklingen.

Spørgsmål

Vi håber, at ovenstående informationer vil være en hjælp i jeres bestræbelser på at blive klar til den næste PCI-certificering. Har I spørgsmål, er I som altid velkomne til at kontakte mig på telefon 7020 7525 eller e-mail ls@fortconsult.net



FORTCONSULT

Klar besked om it-sikkerhed

FortConsult ApS Tel +45 7020 7525
Tranevej 16 - 18 Fax +45 7020 7526
DK-2400 Copenhagen NV www.fortconsult.net