



# PCI-nyhedsbrev

## - januar 2009

### 1. Ny version af PCI-standarden

Den tredje version af PCI-standarden, version 1.2, udkom i oktober 2008 og skal følges fra den 1. januar 2009.

I version 2.1 er der foretaget en række ændringer, som I skal være opmærksomme på. De væsentligste ændringer er beskrevet nedenfor, men det er vigtigt, at I selv læser den nye version grundigt igennem for at finde ud af, hvad der især er relevant for netop jeres virksomhed.

#### **Bredere formulerede krav**

Ændringerne i PCI-standarden reflekterer for de flestes vedkommende, at kravene i standarden er blevet formuleret bredere. Det gælder især formuleringer af konkrete tekniske specifikationer, som er blevet udtrykt i mere generelle vendinger for at give plads til, at PCI-standarden kan følge den teknologiske udvikling, uden at PCI Council behøver at udgive en ny opdatering, hver gang der opstår en teknologisk ændring.

Fx inkluderer PCI-standarden ikke længere en specifik liste med de 10 vigtigste sårbarheder i webapplikationer baseret på OWASP's prioriterede liste. I stedet for henviser standarden nu til OWASP's liste over de største web-sårbarheder, og PCI Council behøver derfor ikke opdatere PCI-standarden, hver gang der sker en ændring eller omprioritering af sårbarhederne hos OWASP.

Ændringerne betyder, at det er vigtigt, at I løbende holder jer opdateret med hensyn til nye teknologier og sikkerhedstrusler, så I kan vælge de nødvendige tiltag på de rigtige tidspunkter.

Nedenfor giver vi en række eksempler på ændringerne i PCI-standardens version 1.2.

#### **Firewall-review**

Ifølge den nye version 1.2 er det ikke længere et krav, at man skal uføre firewall-review hvert kvartal. Det er nu ændret til hvert halve år.

#### **Wireless**

Virksomheder, som benytter wireless-teknologi baseret på den gamle WEP-protokol, skal sørge for at udskifte deres udstyr inden den 30. juni 2010. Hvis I installerer nye trådløse enheder efter

31. marts 2009, skal I være opmærksomme på, at disse installationer ikke må være med WEP-protokol men skal følge den nyere WPA-protokol i stedet for.

Denne ændring skyldes, at krypteringen i WEP-protokollen ikke er implementeret sikkert nok. WEP-protokollen har længe været anset som usikker, men PCI Council har alligevel tilladt den af hensyn til de mange gamle WEP-baserede trådløse terminaler, som har været i omløb.

Ændringen er især relevant for butikker med håndholdte terminaler, hvor en del af udstyret er baseret på WEP.

### **Antivirussoftware**

I PCI-standardens version 1.2 er kravet til antivirussoftware blevet udtrykt i mere generelle termer. Det betyder eksempelvis, at den tidligere nævnte undtagelse for Unix-systemerne ikke længere eksisterer. PCI Council fremtidssikrer dermed PCI-standarden, så de ikke behøver at udgive en ændring, i tilfælde af at hackerne begynder at udvikle virus til UNIX-systemer.

Antivirussoftware skal nu også fange ondsindet (malicious) kode. Derfor anbefaler vi, at I undersøger, om den version af antivirussoftware, som I benytter, opsnapper dette. I kan generelt ikke regne med, at alt antivirussoftware inkluderer funktioner til at fange ondsindet kode.

### **Patching**

Baseret på den nye version af PCI-standarden kan I nu benytte en tilgangsvinkel til patchning, som er baseret på de reelle risici. Nu skal I nemlig vurdere sårbarheder og patches i forhold til jeres egen situation frem for at skulle opdatere alle høj-risiko sårbarheder inden for 1 måned - inklusive de sårbarheder, der ikke er kritiske for jeres konkrete setup.

### **Backup-løsninger**

Det er blevet præciseret, at virksomheder, der har backup-løsninger hosted ude i byen, skal besøge deres leverandør minimum en gang om året for at sikre sig, at backup-løsningen er sikker.

### **IDS-systemer**

I den tidligere version af PCI-standarden skulle IDS-systemet monitorere al trafik. I den nye version er PCI-kravet blevet præciseret, således at systemet kun skal overvåge al trafik inden for de it-miljøer, som håndterer kortdata.

Ovenstående er blot nogle af de ændringer, som er beskrevet i den nye PCI-standard version 1.2. FortConsult anbefaler derfor, at I læser hele den nye version af PCI-standarden for at finde ud af, hvad den betyder for jeres virksomhed.

## **2. PA-standard - ny søster til PCI**

I maj 2008 lancerede PCI Council den nye PA-DSS-standard, som henvender sig til virksomheder, der udvikler eller installerer betalingsløsninger. I Danmark indbefatter det udviklere og integratorer af kasseapparatløsninger og terminalleverandører af kreditkortterminaler. Disse virksomheder har allerede modtaget brev fra PBS om, at de skal overholde sikkerhedskravene i PA-standard.

I Sverige er de virksomheder, som skal overholde PA-standard, blevet informeret af Pannordic om de præcise sikkerhedskrav på tilsvarende vis. Vi forventer, at øvrige lande vil følge trop, fordi VISA i USA har meldt klart ud, at al software skal være PA-godkendt.

### **Nemmere at stille krav**

PA-standarden er blevet udviklet med formålet at gøre det nemmere for de virksomheder, som køber betalingsløsninger - primært butikker - at kommunikere med sine leverandører og stille krav til sikkerheden i deres applikationer, så butikkerne selv kan blive PCI-godkendte. Med PA-standarden har softwareleverandørerne nu fået et konkret værktøj til finde ud af, hvordan de skal gøre deres applikationer sikre – og dermed opfylde kravet fra butikkerne.

### **Skab overblik som det første**

Hvis I udvikler software med kreditkort i, råder vi jer til at danne jer et overblik over PA-standarden, og hvad der kræves af ændringer i jeres virksomhed hurtigst muligt. Det giver jer mulighed for at samkøre handlingsplanen for at blive PA-godkendt med jeres udviklingsplaner og derved undgå at spilde unødigt udviklingstid på at producere software, som ikke opfylder PA-kravene og dermed ikke er fremtidssikret.

### **Eneste dansker**

FortConsult er som den eneste danske virksomhed certificeret af kreditkortselskaberne til at tjekke og auditere sikkerheden på deres vegne i de dankortløsninger, som er underlagt PA-standarden. På verdensplan er 18 virksomheder godkendt til at udføre PA-audits.

I kan læse meget mere om PA-standarden, og hvad man skal gøre for at opfylde den her:  
[http://www.fortconsult.net/pci/softwareudviklere\\_pa.php](http://www.fortconsult.net/pci/softwareudviklere_pa.php)

## **3. Interne PCI-penetrationstest**

De nye PCI-krav til interne penetrationstest blev udgivet i foråret 2008 og trådte i kraft med det samme. Formålet med interne PCI-penetrationstest er at afprøve i praksis, om alle bestemmelserne i PCI-standarden er implementeret korrekt, og om det er muligt for uvedkommende at stjæle kreditkortdata.

Interne penetrationstest udføres på samme måde, som når en hacker angriber en virksomhed for at stjæle kortdata, efter at han fysisk er trængt ind i virksomheden. Eller på samme måde som en almindelig medarbejder uden adgang til kortdata kunne tænkes at forsøge at bryde igennem virksomhedens forsvarsværker for at stjæle kreditkortinformationer.

### **Testen skal godkendes**

Alle virksomheder, der er omfattet af PCI-standarden, skal have udført en intern penetrationstest i forbindelse med en PCI-audit. Som en del af den audit, FortConsult udfører, kontrollerer vi, om testen er udført, og om den opfylder kravene fra PCI Council.

### **Uvildighed er et krav**

Da PCI-standarden stiller krav om, at man ikke må teste sit eget arbejde, skal interne PCI-penetrationstest udføres af en uvildig person. Som virksomhed kan man derfor enten vælge at udføre testene selv - vel at mærke af en person som ikke først har været involveret i at konfigurere virksomhedens sikkerhedsløsninger - eller få et sikkerhedsfirma til at gøre det. Der er som udgangspunkt ikke noget i vejen med at gøre det selv, men man skal i så fald være opmærksom på, at PCI Council stiller høje krav til selve testen og til kompetenceniveauet hos den person, der skal udføre den.

For at få sin egen sikkerhedstest godkendt skal man kunne dokumentere, hvad man har testet, hvorfor og hvordan på en måde, der er tilstrækkeligt uddybet til, at dokumentationen kan læses af udenforstående. Når FortConsult udfører auditen, skal vi med andre ord kunne opnå en præcis forståelse for testen og en opfattelse af, at den er udført tilpas grundigt til, at vi kan stå inde for den over for PCI Council.

### **Målrettede test**

Det er vigtigt, at man sammensætter sin test baseret på den uddybende dokumentation, der allerede findes, så man sikrer sig, at man får testet dét, der er mest kritisk for ens virksomhed. Den eksisterende dokumentation omfatter blandt andet risikovurderingen af ens virksomhed, resultaterne af de interne scanninger og overblikket over PCI-scopet.

Når vi eksempelvis udfører interne PCI-penetrationstest i FortConsult, skræddersyr vi en tests indhold til hver enkelt virksomhed, ved at vi allerførst sætter os ind i den eksisterende dokumentation, og i hvordan en hacker vil kunne angribe den pågældende virksomhed. Det medfører, at testen i praksis kommer til at fokusere på virksomhedens største risici for reelt at blive hacket og få stjålet kreditkortdata i modsætning til at dække hele PCI-standarden bredt og medtage områder, som er irrelevante eller svære at udnytte.

Virksomheden, der bliver testet, får på denne måde en både målrettet og praktisk test - hvor vi undersøger, hvad der rent faktisk kan lade sig gøre - og på den måde være sikker i praksis, frem for "blot" at følge PCI-standarden.

### **Nyt om den eksterne PCI-penetrationstest**

Der er også kommet nye krav til den eksterne penetrationstest, hvor det nu er blevet mere klart, hvad man skal gøre. I praksis er der ingen ændringer for de virksomheder, der får udført penetrationstesten af FortConsult.

Ændringerne i kravene til både de eksterne og interne penetrationstest er præciseret i PCI Councils clarification letter:

[https://www.pcisecuritystandards.org/pdfs/infosupp\\_11\\_3\\_penetration\\_testing.pdf](https://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf)

Hvis I har yderligere spørgsmål om de nye krav til interne og eksterne penetrationstest, er I velkomne til at kontakte os.

## **4. Nyt self assessment-skema (SAQ)**

I starten af 2008 udkom en ny og forbedret version af self assessment-skemaet (SAQ). Skemaet er relevant for virksomheder, der skal følge PCI-standarden, men som ikke har krav om at skulle have udført en audit.

Fra starten af 2009 vil ændringen få betydning for mange af vores kunder, som skal til at benytte den nye version af spørgeskemaet fra og med det nye år.

### **Mere konkrete formuleringer**

Den oprindelige version af SAQ'en - version 1.0 - var meget overordnet, og mange virksomheder kunne med god samvittighed svare ja til de fleste spørgsmål i skemaet uden først at læse PCI-standarden, som det var meningen. I den nyeste version - version 1.2 - er spørgsmålene imidlertid formuleret mere konkret, og det indebærer, at det bliver mere tydeligt, hvis der er nogle forhold, som man ikke overholder eller nogle områder, som man bliver nødt til at undersøge nærmere, inden man kan besvare spørgsmålene.

I praksis har der hidtil været mange virksomheder, som fejlagtigt har angivet, at de overholder PCI-standarden. Når de begynder at benytte det nye skema, vil det hurtigt blive synligt, hvad de mangler.

### **Sikkerhedsmæssigt ansvar**

Selvom jeres virksomhed ikke skal kontrolleres, og I blot skal udfylde SAQ'en, skal I være opmærksomme på, at I har et stort ansvar. Såfremt I bliver hacket, og I ikke reelt opfylder hele PCI-standarden, vil I kunne risikere at komme til at dække de beløb, der er svindlet for på de kortnumre, der bliver stjålet. Baseret på erfaringer fra tidligere svindelnumre svarer

erstatningen, som I skal betale, til 1.000 Euro pr. kortnummer, og herudover skal I betale en bøde.

Vi hjælper jer gerne med at udfylde SAQ'en, hvis I vil være sikre på at få gjort det rigtigt.

## 5. Afklaring af typiske misforståelser

Når FortConsults PCI-sikkerhedskonsulenter auditerer og tester for vores kunder, oplever de to typiske misforståelser, som vi gerne vil bidrage med at afklare i det følgende:

### Misforståelse 1:

"Hvis vi ikke gemmer kortdata, skal vi ikke overholde PCI-standarden."

### Afklaring 1:

Selvom man ikke opbevarer kortdata, skal man stadigvæk følge hele PCI-standarden, men det praktiske arbejde med at overholde standarden er i mange tilfælde nemmere.

Det er selvfølgelig nemmest for en hacker at hacke sig ind i kortdatabaser med store mængder data samlet på ét sted. Men en hacker kan også stjæle data ved at opsamle kreditkortdata, hver gang der bliver processeret et kort. Det foregår blot over en længere periode. I sådanne tilfælde installerer hackeren fx et program, der kopierer hvert kortnummer til en server på internettet. Programmet installeres så tæt på kilden, at nummeret kan opfanges ukrypteret.

Hackerne er i øvrigt i langt større grad begyndt at benytte den sidstnævnte metode, da mange virksomheder ikke længere opbevarer kortdata i større mængder af sikkerhedsmæssige årsager.

### Vær klar over scopet

Det er vigtigt, at man er klar over sin virksomheds scope - det vil sige, hvilke systemer PCI-standarden gælder for - både hvad angår systemer, som opbevarer og/eller processerer og/eller transmitterer kreditkortdata, og hvad angår alle andre systemer, der befinder sig på det samme netværkssegment. Betegnelsen "systemer" dækker bredt fra servere og arbejdsstationer til firewalls, routere og andre netværksenheder – og ikke mindst kreditkortterminaler.

For mange butikker betyder det, at alle deres computere i hele butikskæden er omfattet af PCI-standarden - ikke kun en enkelt kasseløsning.

### Misforståelse 2:

"Trådløst netværk er forbudt hos os, så vi behøver ikke at udføre en trådløs test."

### Afklaring 2:

Selvom man ikke benytter trådløse løsninger, skal man stadig udføre en trådløs test.

Krav 11.1 i PCI-standarden er gældende for alle og handler om, at man skal udføre en trådløs test en gang i kvartalet. Det gælder også, selvom man ikke har trådløst udstyr, og selvom udstyret ikke er koblet sammen med systemer, der opbevarer kreditkortdata.

### Undersøgelse for trådløse access-punkter

Hensigten med den trådløse test er at undersøge, om der er nogle oversete trådløse access-punkter, som fx er opstået som resultat af en fejlkonfiguration af en bærbar pc eller en printer. Herudover har testen til formål at belyse, om hackere eller medarbejdere har sat trådløse access-punkter op, som virksomheden ikke kender noget til.

I den nye version af PCI-standarden - version 1.2 - er der inkluderet en ændring til punkt 11.1, der drejer sig om, hvilke testmetoder der er acceptable. Det er nu også tilladt at benytte trådløse IDS-systemer frem for at teste, men da trådløse IDS-systemer er omstændelige at konfigurere og typisk kræver mange trådløse access-punkter for at kunne dække hele virksomhedens PCI-scope, bliver det hurtigt en dyr løsning. I praksis giver det derfor fortsat mest mening at udføre en trådløs test, hvor man manuelt går rundt og tjekker alle lokationer med trådløst testudstyr.

Har I spørgsmål eller kommentarer, er I meget velkomne til at kontakte os. Vi følger hele tiden udviklingen i PCI- og PA-standarderne og vender tilbage med næste nyhedsbrev, når vi har relevant nyt at fortælle.



**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](http://www.fortconsult.net)