



Sikkerhedsnyheder fra FortConsult

Indhold

1. Ændringer fra VISA, MasterCard og PCI Council
2. Nyt om PCI-standarden generelt
3. Præciseringer fra PCI Council
4. Ny vejledning om trådløs sikkerhed
5. Udstederbankernes PCI-udfordringer
6. Stadig flere korttyverier
7. FortConsult på Top 3 i Europa

1. Ændringer fra VISA, MasterCard og PCI Council

Siden sidste nyhedsbrev er der sket en række ændringer, som vil være relevante for forskellige typer virksomheder. Vi gennemgår de væsentligste nedenfor.

1.0 Baggrund:

For de læsere af nyhedsbrevet, der er nye på PCI-området, vil vi lige ridse op, hvordan arbejdsdelingen mellem kortselskaberne og PCI Council er:

Det er PCI Council, der udvikler PCI-standarden baseret på input fra medlemmerne. Medlemmerne tæller både "brugere" af standarden fx banker, supermarkeder og flyselskaber og repræsentanter for kortselskaberne fx VISA, MasterCard, JCB og American Express. Udover at vedligeholde standarden har PCI Council ansvaret for at QSA'erne opfylder de faglige og formelle betingelser, der kræves for at være akkrediteret QSA. Det omfatter også træning af QSA'erne og hjælp til præcisering af fortolkninger af standarden.

PCI Council kan ikke kræve, at bestemte grupper af virksomheder skal overholde PCI-standarden. Det kan kun kortselskaberne.

Kortselskaberne udstikker de overordnede linjer, men det er de enkelte landes indløserbanker, der vælger, i hvilken grad de vil følge kortselskabernes krav til overholdelse af PCI, eller om de eventuelt vil stille mere strikse krav for bestemte virksomheder for at reducere risikoen for korttyveri i det pågældende land. VISA Europa opererer som en selvstændig organisation og styrer selv de compliance-krav, der stilles på det europæiske marked inklusiv at sørge for, at de er målrettet til europæiske forhold. MasterCard styrer alle compliance-krav fra USA og stiller de samme krav i alle verdensdele. Kortselskaberne forsøger i høj grad at koordinere kravene på tværs af selskaber, men det lykkes ikke fuldstændig, og derfor er det ikke altid de samme compliance-krav, der gælder. Almindelige brugere af PCI-standarden vil dog oftest opleve, at deres indløserbank melder et samlet krav ud i overensstemmelse med deres egen udlægning af kravene.

1.1 Ændringer i merchant levels

I løbet af første halvår 2009 har MasterCard ændret deres krav til opfyldelse af PCI for level 2 merchants. Tidligere har level 2 merchants kunnet nøjes med at udføre kvartalsvise PCI-scanninger og selv udfylde et skema med spørgsmål til sikkerheden. Dette krav blev først ændret til, at level 2 merchants også skal have udført en årlig audit af en QSA, og dernæst til at auditen også kan udføres af virksomhedens interne revision, hvis de har deltaget på et PCI-kontrol-kursus. Level 2 merchants omfatter mindre handlende, der har 1-6 millioner transaktioner om året. De vil typisk have færre ressourcer på it-området, og det vil være en meget stor udfordring for dem at skulle igennem en audit. De nye krav har skabt en del debat, da der på betalingsområdet i Europa er mere fokus på at løse de mindre butikkers udfordringer ved hjælp af ny teknologi.

Det er de enkelte indløserbanker, der skal stille det nye krav på vegne af MasterCard, men de fleste europæiske banker er foreløbig afventende og håber at finde en anden løsning.

1.2 Nye krav fra VISA til medlemsbankernes underleverandører

VISA kræver nu, at alle VISA-medlemsbanker fra 1. oktober 2010 kun benytter underleverandører, der er PCI-compliant. Denne compliance skal valideres i henhold til VISA service provider levels. Det betyder, at leverandører med under 300.000 transaktioner årligt kan nøjes med self assessment og scanninger, mens de øvrige skal have en årlig PCI-audit. Da underleverandørers kerneforretning typisk hænger sammen med banktransaktioner – heriblandt kreditkort – finder vi, at det giver god mening at kræve, at sikkerheden valideres årligt. For hvis virksomheder, der har det som deres kerneforretning at behandle kreditkort, ikke skal være PCI-compliant, hvem skal så?

VISA har udmeldt kravet til medlemsbankerne, og så må vi se, hvor hurtigt det bliver stillet videre til tredjeparts-leverandørerne. Det er oplagt, at der for mange af denne type virksomheder er tale om en ret kort frist, og vi hjælper selvfølgelig gerne med rådgivning i den forbindelse, hvis I har behov for det.

1.3 VISA kræver at software-sikkerhedsstandard PA-DSS bliver obligatorisk i hele EU

PA-standarden er – som omtalt i tidligere nyhedsbreve – den nye søsterstandard til PCI-standarden. PA-standarden er gældende for software, der behandler kortdata. Mens PCI-standarden berører virksomheder, der håndterer kreditkorttransaktioner, gælder PA-standarden virksomheder, der udvikler betalingssoftware og kreditkortløsninger, der benyttes i butikker, banker, pengeautomater og e-handel. Hidtil har de virksomheder, der skal leve op til PCI-standarden, selv kunnet vælge, om de ville anvende PA-standarden i samarbejdet med deres underleverandører. I enkelte lande som Sverige og Danmark har indløserbankerne dog allerede i et stykke tid krævet, at point of sale devices og kasse-software skal leve op til PA-standarden. Men nu kræver VISA altså, at man implementerer PA-standarden i hele EU. Alle nye installationer skal bruge løsninger, der er PA-compliant efter 1. juli 2010, og senest 31. december 2012 skal alle merchants (inkl. de små) enten bruge løsninger, der er PA-compliant, eller selv være PCI-compliant (hvor PCI-compliance netop også omfatter selve softwaren).

2. Nyt om PCI-standarden generelt

2.0 Ny PCI-standard ved udgangen af 2010

PCI-standardens livscyklus er sådan, at der kommer en ny standard hvert andet år. Det første år herefter bruger PCI Council på at informere om den nye standard, og i løbet af det efterfølgende år forberedes den næste version. Vi er netop gået ind i et år med forberedelse af en ny standard, og PCI Council udfører i den forbindelse en række aktiviteter.

I løbet af sommeren har de fx forespurgt medlemmerne, brugerne og QSA'erne, hvilke ønsker de har til den næste PCI-standard. Det giver bl.a. os i FortConsult en god mulighed for at påvirke processen,

så vi allerede på dette tidspunkt kan arbejde for at gøre livet lidt lettere for vores kunder. Indtil videre har vi været begrænset af, at vi først kunne forholde os til standarden, når den forelå. Nu får vi lejlighed til at tilpasse udformningen af den efter de praktiske udfordringer, som vi ved, at virksomhederne står med til daglig. For når vi også bliver inddraget i den skabende proces, kan vi selvfølgelig meget bedre forfine vores analyseredskaber.

Derudover har PCI Council sat et arbejde i gang, hvor de ser på, hvilke teknologier der kan hjælpe merchants med at reducere deres risiko, uden at det bliver for omstændeligt eller dyrt for dem. Tanken er, at leverandører af udstyr eller outsourcing-partnere, leverer løsninger, der enten reducerer PCI-scopet fra merchanten, eller endog helt fjerner behovet for PCI. Det vil dog primært være en mulighed for butikker og altså ikke for andre typer af virksomheder, der på nuværende tidspunkt hører ind under PCI-standarden. Flere af de løsninger, der er på bordet, vil ikke fjerne risikoen for korttyveri. Den vil i stedet blive overført til udvikleren af løsningen eller til service-leverandøren.

PCI Council er kun lige begyndt på arbejdet men har analyseret sig frem til en række lovende nye teknologier, som skal analyseres nærmere. Det drejer sig om:

- End-to-end encryption
- Magnetic stripe imaging
- Tokenization
- Virtual terminals

Disse teknologier er udvalgt efter en vurdering af dens tekniske robusthed, af hvor let teknologien er at implementere og vedligeholde hos de enkelte merchants, hvor let den kan integreres med eksisterende indløsningssystemer, og hvor meget ekstra arbejde den giver for service-leverandøren.

Fra et europæisk perspektiv kunne vi godt have ønsket os noget mere. Mange lande har allerede implementeret EMV-chipkort, og så giver magnetic stripe imaging ingen mening. Og end-to-end encryption er allerede implementeret mange steder. Til gengæld ser vi tokenization vinde frem mange steder, og selvom konceptet i sig selv ikke er nyt, betragter vi det som meget lovende. I Europa skal vi således nok forvente en standard, der passer bedre til den teknologi, vi allerede bruger, end én der indeholder banebrydende nye løsninger, der gør det markant lettere at være merchant. Vi håber dog, at dette bliver skridtet, der justerer PCI-standardens krav til risikobilledet hos de mange europæiske virksomheder, der ikke bruger magnetstripe/trackdata men mere avancerede løsninger baseret på EMV.

Vi skal dog understrege, at PCI Council ikke har lagt sig fast på noget endnu, og det kommende års arbejde kan medføre, at de nævnte områder falder bort til fordel for nogle andre. I forhold til det igangværende arbejde hvor der ses på nye teknologier og risk mitigation i bred forstand, har vi en forventning om, at der med den kommende version af PCI-standarden bliver tale om en omfattende opdatering, der vil komme til at påvirke mange. Vi vender tilbage til indholdet af den nye standard, så snart vi ved noget mere.

2.1 På vej mod en mere robust PCI-standard

I FortConsult finder vi, at PCI Council efter at have virket i tre år er ved at finde sine ben, og det viser sig ved, at deres fortolkninger er blevet mere præcise. Det ændrer dog ikke på, at der fortsat vil være punkter, hvor fortolkningerne ændrer sig over tid. Vi kan fx se, at det materiale vi bruger i forbindelse med vores egen uddannelse, har ændret sig ganske betydeligt på en række punkter over tid. Og alene det indikerer jo, at det her er et område i bevægelse. Som professionelle auditorer er det naturligvis en udfordring for os, da vores kunder med rette forventer, at de får en rådgivning de kan regne med holder et stykke tid. Vi har derfor håb om, at PCI Councils seneste, klare udmeldinger vil vise sig mere levedygtige end tidligere.

Siden vi begyndte at lave audits for fire år siden, har vi jævnligt hørt kunder fortælle, at de har oplevet, at forskellige QSA'er har givet forskellige svar på det samme spørgsmål. Det samme har PCI Council mange gange været kritiseret for. Det er netop derfor, at PCI Council nu har lagt sig i selen for at være mere præcise i deres materiale til QSA'erne og for samtidig at følge op på QSA'ernes arbejde (se nedenfor). Fordelen er, at kunderne er betydeligt sikrere på at få det samme svar fra alle QSA'er.

Desværre har denne løsning også en ulempe, nemlig at QSA'erne ikke kan tage individuelle hensyn. En af de væsentligste årsager til, at der har eksisteret forskellige krav, er, at den enkelte QSA'er har kunnet se pragmatisk på problemerne og evalueret risikoen ved hver enkelt kundes set-up. Dermed har vi i høj grad været i stand til at kundeorientere vores arbejde og fokusere på at nedbringe risikoen for korttyverier og taget lidt mindre firkantet på compliance-kravene. Dette spillerum er nu desværre blevet betydeligt mindre.

2.2 Opkvalificeringsprogram for store QSA'er

For yderligere at lette og effektivisere arbejdet med PCI-standarden har PCI Council startet et quality assurance-program, der har til formål at sikre, at QSA'erne fortolker standarden ens overalt. I første omgang inkluderes de største QSA'er, og det betyder, at vi i FortConsult er med i første runde i Europa. I praksis foregår det på den måde, at PCI Councils medarbejdere grundigt gennemgår de rapporter, vi har leveret, evaluerer dem og giver dem karakter. For vores kunder betyder det en ekstra sikkerhed for, at vores arbejde rent faktisk rammer de fortolkninger som PCI Council ønsker, og at vores rådgivning fremadrettet vil være meget lig den, som de andre store QSA'er giver. Som nævnt kan det betyde, at vi ikke i samme grad som hidtil kan tage individuelle hensyn, da der fremover er en meget lille tolerance for, hvad der er tilladt. Samtidig medfører QA-programmet, at alle QSA'er vil skulle bruge betydelig mere tid på at dokumentere det, vi har observeret under vores audit på stedet. I sidste ende betyder det desværre, at kunderne vil komme til at opleve højere priser. Hos FortConsult har vi allerede ændret vores rutiner i forhold til de nye krav, så vi kan begrænse det øgede tidsforbrug mest muligt. Men flere andre QSA'er er enten ophørt eller har markant ændret deres prisstruktur. Vi beklager, at kunderne på flere områder vil blive berørt af det nye QA-program, men vi håber samtidig, at alle vil få fordel af den mere konsistente håndhævelse af standarden på tværs af landegrænser og de enkelte QSA'er.

3. Præciseringer fra PCI Council

3.0 Maskering af kreditkortnumre

Nogle kunder har ønsket at arbejde med en alternativ kortnummermaskering end den gængse i henhold til PCI-standarden, hvor det er de første seks og de sidste fire cifre, der er synlige. Vi har fx skullet tage stilling til, at kunder ville maskere, så de første otte og de sidste 2 cifre var synlige. Ønsket kommer af at kunderne i visse tilfælde har behov for at kunne registrere korttypen, fx i forbindelse med opkrævning af gebyr på udenlandske kort.

PCI Council præciserer, at det ikke er tilladt at bruge alternativ maskering. De er opmærksomme på, at det kan give problemer for en række kunder men kan ikke tillade en opblødning af reglen, da det vil gøre det lettere for hackere at kombinere sig frem til det fulde nummer, hvis de opsnapper de samme transaktioner flere steder med forskellige maskeringer.

3.1 Hvornår skal der laves en penetrationstest?

Pkt. 11.3 i PCI-standarden omhandler penetrationstests, og det angives, at der skal udføres en penetrationstest i forbindelse med alle "afgørende ændringer" ("any significant change"). Spørgsmålet er så, hvad der forstås ved en "afgørende ændring". Her præciserer PCI Council, at der skal foretages penetrationstest i forbindelse med:

- opgradering af operativsystemet
- tilføjelse af undernetværk
- tilføjelse af perimetersystemer som fx en webserver

Fra FortConsult vil vi gerne præcisere, at ikke altid er nødvendigt at gennemføre en fuldstændig penetrationstest i forbindelse med ændringer i set-up'et. Virksomheder vil i nogle tilfælde kunne nøjes med at teste nogle af komponenterne. Det er op til jer selv at vurdere, hvilke områder der er berørt af ændringen og derfor skal testes igen. I tvivlstilfælde bør I teste alt eller tage en drøftelse med os.

Det er vigtigt, at I bider mærke i denne præcisering, da det er et punkt vi fremover vil tjekke, når vi laver audit.

3.2 AI trafik betyder al trafik

Pkt. 11.4 i PCI-standarden handler om brugen af IDS til at monitorere "al trafik" i systemet. Her præciserer PCI Council, at "al trafik" ganske enkelt betyder al trafik. Nogle har spurgt, om man ikke kan nøjes med mindre, men det er ikke tilfældet. For nogle virksomheder betyder det, at der lige nu ikke overvåges tilstrækkeligt mange systemer, da nogle udelukkende har fokuseret på internet-vendte systemer. Vi anbefaler, at I undersøger, om alle systemer i PCI-scopet er med i IDS-overvågningen. Det samme gælder punkt 11.5 vedrørende file integrity monitoring. Også her skal alle systemer i PCI-scopet inkluderes.

3.3 Medarbejderne har pligt til at kende sikkerhedspolitikken

Pkt. 12.6.2 i PCI-standarden foreskriver, at alle medarbejdere én gang om året skal bekræfte, at de har gjort sig bekendt med virksomhedens sikkerhedspolitik. Det er et punkt mange overser, og derfor vil vi minde om, at det skal man altså sørge for. Samtidig minder vi om, at alle medarbejdere ifølge 12.6.1.b skal deltage i security awareness training én gang om året.

4. Ny vejledning om trådløs sikkerhed

Der er kommet en ny vejledning fra PCI Council, der grundigt og letforståeligt fortæller om sikkerhedsproblemer i forbindelse med trådløse forbindelser. Det er et glimrende dokument, som vi varmt kan anbefale. Mange virksomheder oplever, at trådløs sikkerhed for alvor er kommet på dagsordenen, og mange er usikre på, hvad det betyder for netop deres set-up. Vi er endog af og til ude for, at virksomhederne slet ikke er klar over, at der er trådløse forbindelser i deres PCI-scope.

Under alle omstændigheder er det en god idé at få gennemgået set-up'et med henblik på at etablere optimal trådløs sikkerhed og i den forbindelse selvfølgelig også at få undersøgt, om man rent faktisk lever op til PCI-standarden. PCI Councils dokument er meget omfattende, og I er velkomne til at kontakte os, hvis I har behov for rådgivning i den forbindelse. En af vores erfarne PCI-konsulenter, Warren Platt, er ikke kun QSA'er men også specialist i trådløs sikkerhed og tilknyttet SANS Institute som mentor på Wireless-uddannelsen. Warren er i øvrigt én ud af kun seks eksperter på verdensplan, der har opnået den fornemme guldcertificering inden for trådløs sikkerhed GIAC-GSNA.

PCI Councils vejledning finder I på:

https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

5. Udstederbankernes PCI-udfordringer

Udstederbankerne i Europa har traditionelt ikke beskæftiget sig meget med PCI, selvom de er et centralt led i kredittorkæden. VISA og MasterCard har formodentlig forventet, at udstederbankernes sikkerhed var i orden og har derfor ikke gjort meget for at følge op på deres aftaler med udstederbankerne på sikkerhedsområdet. De har henholdt sig til de aftaler, de har indgået og ikke gjort ret meget mere end det.

Efterhånden som PCI er blevet implementeret i alle de andre led, er antallet af virksomheder, der opbevarer kredittorkortdata, blevet kraftigt reduceret, og derfor er der kommet øget fokus på udstederbankerne som det svage led i kæden. Problemet med udstederbankerne er, at de ofte har mange kortdata liggende, og at de anvendes i flere af bankernes interne afdelinger, i rådgivningen, i marketing, osv. I mange tilfælde har bankerne outsourcet deres it, og dermed er det umiddelbare

ansvar for beskyttelse af kortdata flyttet væk fra den daglige omgang med data, og det kan gøre sikkerheden noget diffus. Selvom kortdata beskyttes et andet sted i elektronisk form, er der jo ikke noget i vejen for, at en medarbejder fx kan have printet noget ud og har det liggende et eller andet sted. Bankerne vil også typisk have et samarbejde med underleverandører, der har adgang til kortdata eller systemer med kortdata.

I FortConsult har vi betydelig erfaring med udstederbankernes udfordring på PCI-området. Vi har bl.a. hjulpet flere af de største banker i Skandinavien og en lang række europæiske bankers driftscentre med at leve op til PCI-standarden, og vi kan derfor give nogle gode råd om, hvad I med fordel kan gøre her og nu, hvis I er en udstederbank.

Her er tre tommelfingerregler:

- Start tidligt. Identificer så hurtigt som muligt, hvor langt I er fra PCI-standarden, så I har god tid til at implementere tiltagene og kan indpasse dem i den daglige drift. Jeres it-afdeling bør være opmærksom på PCI i planlægningen og opstarten af alle nye projekter, så I ikke senere skal til at lave det hele om. I kan fx sørge for, at nye applikationer følger PCI- eller PA-standarden. Når medarbejderne skal have nye bærbare computere, vil maskinerne således allerede være tilpasset standarden.

- Få klassificeret de kortdata, I håndterer, og skab opmærksomhed omkring sikkerheden blandt medarbejderne. Måske er jeres medarbejdere ikke tilstrækkeligt opmærksomme på, at det er følsomme data, de har med at gøre, og hvordan de skal håndteres.

- Hvis det er relevant, så sørg for, at PCI er på dagsordenen i kontakten med jeres underleverandører.

- Endelig er det en god idé at sørge for, at ejerskabet til PCI ligger i forretningsdelen af virksomheden og ikke i it-afdelingen. PCI-problemstillingerne omfatter jeres virksomheds aktiviteter bredt og er ikke kun it-relaterede. Faktisk ligger mange af problemerne gemt i den berømte "menneskelige faktor".

PCI Council har annonceret, at de inden længe vil udsende et notat om udstederbankerne og PCI. Så snart det foreligger, vender vi tilbage til sagen.

6. Stadig flere korttyverier

Problemet med tyveri af kreditkort er stadig stigende. Efter historierne i medierne at dømme kan det umiddelbart se ud som om, at det er langt værre i USA end her i Europa, men da virksomhederne i USA i modsætning til i Europa ifølge lovgivningen er forpligtet til at offentliggøre alle korttyverier, bliver billedet let noget fortegnet.

Derfor blev det da også bemærket, da det her i foråret kom frem, at det var lykkedes hackere at bryde ind i bookingsystemet hos et hotel i Ebeltoft og stjæle kortdata fra systemet. Sagen som sådan var ikke noget særligt, for det sker jævnligt, men det specielle var, at den blev offentligt kendt. Det var et godt eksempel på et sted, hvor de ikke havde været fokuseret på PCI, og derfor var særdeles udsat. Havde hotellet levet op til PCI-standarden, havde hackerne ikke kunnet operere på den måde, de gjorde.

Her i Skandinavien har der været mest opmærksomhed omkring tyveri via hæveautomater, og den trafik er desværre også fortsat et stort problem. Det indikerer, at behovet for fokus på PCI bestemt ikke er blevet mindre. Især ikke hvad angår de dele af systemerne, som man måske ikke tænker på i første omgang. I Skandinavien er de fleste tyverier foregået som fysiske angreb, hvor man har installeret en lille skimmer enhed på ATM'en. Nedenfor et link til en amerikansk sag, der minder om de skandinaviske. Bemærk, hvor kreative angriberne har været.

http://www.youtube.com/watch?v=m3qK46L2b_c

PCI-standarden skal primært sikre, at kortdata ikke stjæles, mens de er i virksomhedens varetægt. Nedenfor er et link til en sag fra Østeuropa med et ATM-angreb, der sandsynligvis kunne have været undgået, hvis systemerne havde levet op til PCI-standarden.

http://news.cnet.com/8301-1009_3-10257277-83.html?tag=mncol

7. FortConsult på Top 3 i Europa

Til sidst en nyhed fra de interne linjer. På VISA's seneste liste over certificerede service providers indtager FortConsult nu tredjepladsen over den QSA, der har auditeret flest. Allerede i 2004 blev FortConsult som det første og eneste it-sikkerhedsfirma i Skandinavien godkendt af VISA og MasterCard til at foretage sikkerhedsscanninger og i 2005 fulgte vores godkendelse til at udføre audits. På det grundlag har vi kunnet udvide vores kundeportefølge til hele Europa.

En af årsagerne til vores vækst er uden tvivl vores mangeårige erfaring fra at have løst en lang række PCI-opgaver, at vi sidder samlet i ét kontor i København og har let ved at dele viden og erfaring - både blandt vores sikkerhedsekspertes men også på tværs af vores forskellige specialer. For jer indebærer det, at I altid kan få opdateret og relevant rådgivning om også meget specifikke PCI-problemstillinger, så I ikke risikerer at igangsætte projekter, som senere viser sig at være utilstrækkelige eller uhensigtsmæssige.

Med venlig hilsen

Lars Syberg
PCI Product Manager
FortConsult A/S



FORTCONSULT

Klar besked om it-sikkerhed

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