



# StayInTouch

– sikkerhedsnyheder fra FortConsult

## Indhold i nyhedsbrev for august 2010

1. Forskellige tilgange til sikkerhedstest
2. FortConsult bryder igennem internationalt
3. PCI-nyheder
4. FortConsult støtter Rådet for Større IT-Sikkerhed
5. Nyansatte i FortConsult
6. Nye referencekunder i FortConsult

Du kan tilmelde dig vores elektroniske nyhedsbrev på [www.fortconsult.net](http://www.fortconsult.net)

**FORTCONSULT**

*Klar besked om it-sikkerhed*

# 1. Forskellige tilgange til sikkerhedstest

## - og hvad vi kan lære af hinanden

*Af Ulf Munkedal, adm. direktør i FortConsult*

Det er for mange virksomheder blevet en sund, naturlig disciplin at sikkerhedsteste deres it-systemer med jævne mellemrum, og hver gang der udvikles ét nyt system eller foretages større ændringer i det. Det samme gælder i nogen grad for de virksomheder, som udvikler produkter eller it-løsninger med henblik på videresalg. Hvor naturligt det er blevet at få sikkerhedstestet afhænger nemlig i mange tilfælde af, hvilken type virksomhed man er, og hvilket udbytte man opnår ved at teste på kort sigt.

### Forskellige virksomhedskategorier med forskellige testbehov

I det følgende gennemgår jeg de forskellige kategorier af virksomheder, der får udført sikkerhedstests og sammenligner dem for at se, hvilke konklusioner vi kan drage af forskelle og fællesnævner med henblik af at lære fra de forskellige verdener.

#### **Producenterne**

Overordnet set er det sådan, at producenterne typisk vælger at sikkerhedsteste deres produkter, før de lanceres på markedet, fordi det reducerer omkostningerne ved at rette huller i produktet. En gylden hovedregel siger nemlig, at det er billigere, jo tidligere i processen man retter en sikkerhedsfejl. Producenten er desuden opmærksom på, at de minimerer risikoen for utilfredse kunder og dårlig omtale, hvis der opdages alvorlige sikkerhedsbrister i produktet, efter at det er frigivet. Det er dog det omkostningsmæssige, der normalt vejer tungest for producenterne.

#### **Løsningsleverandørerne**

Løsningsleverandører vælger typisk at sikkerhedsteste deres it-løsninger for at sikre tilfredse kunder og undgå imagetab og eventuelle sagsanlæg. Her er det igen et spørgsmål om, at jo tidligere det sker i udviklingsforløbet jo bedre, og det skal absolut foregå, inden løsningen sættes i produktion, da utilfredse kunder og imagetab er de tungestvejende årsager til, at det kan betale sig for løsningsleverandører at sikkerhedsteste.

#### **Virksomheder i øvrigt (slutkunderne)**

Virksomheder i øvrigt vælger typisk at sikkerhedsteste deres it-systemer for at finde sikkerhedshullerne, før andre kan risikere at udnytte dem, og det kan medføre imagetab, brud på fortroligheden, korruption af data og/eller utilgængelighed. Alt sammen situationer, der kan resultere i uoverskuelige forretningsmæssige konsekvenser for virksomheden.

De fleste sådanne virksomheder vælger at få udført løbende sikkerhedstests som en slags abonnementsordning, hvor alle it-systemerne bliver testet med jævne mellemrum og testresultaterne sammenlignet med henblik på at måle det generelle sikkerhedsniveau. Herudover vælger en del virksomheder i stigende grad at teste deres systemer, hver gang de omkonfigurerer, patcher op, eller der opstår nye, alvorlige sårbarheder.

#### **Konklusion**

Ifølge FortConsults erfaringer er det som oftest slutkunderne, der er mest opmærksomme på fordelene ved at få sikkerhedstestet, det er i stigende grad løsningsleverandørerne, men kun i få tilfælde producenterne. Det burde praktisk set være i den omvendte rækkefølge, da det på den måde er muligt at finde sårbarheder, inden slutkunderne risikerer at miste data.

### Forskellige testmetoder

Hvad enten man tester et produkt eller en løsning, er der en lang række fællesnævner for, hvad der giver en god sikkerhedstest. Det er dog sådan i praksis, at de tre ovenfor nævnte kategorier af virksomheder med behov for at sikkerhedsteste får udført tests med helt forskelligt fokus og udbytte af testen.

Her er en kort beskrivelse af de tre typer testmetoder:

### **Producenternes testmetode**

Producenterne benytter som regel en produkttester til at finde fejl i komponenterne herunder forhåbentlig også sikkerhedsfejl. Det bliver oftest udført af producenternes egen testafdeling, eksterne produkttestere eller eksterne penetrationstestere. De skal teste for at finde producentfejl - altså udviklingsfejl i den enkelte komponent - eller kompatibilitetsfejl - det vil sige fejl, når komponenterne sættes sammen.

Produkttesternes styrke er, at de traditionelt set er vant til at arbejde efter en stærk testmetodik og struktur. Derfor er de som regel meget stærke på metodik- og struktursiden, og de kan som oftest præsentere dokumentation for, at de har lavet et udførligt stykke testarbejde.

Svagheden er, at de ikke har fokus på sikkerhedstests og dermed ikke kan vide sig sikre på, at de har kompetencer til at få fat i alle alvorlige sikkerhedshuller, eller at de rent faktisk kommer hele vejen rundt, selvom de tester efter en struktureret metodik.

### **Løsningsleverandørernes testmetode**

Løsningsleverandørerne benytter løsningsstestere til at finde fejl i en sammensat løsning. Det er også muligt, at de tester for sikkerhedsfejl, hvis det er en del af "accepttesten", som er aftalt med slutkunden. Sikkerhedstestene bliver udført af enten en tekniker hos løsningsleverandøren, teknikere hos slutkunden eller eksterne penetrationstestere. De skal teste for at finde producentfejl, kompatibilitetsfejl, designfejl, løsningsleverandørfejl og konfigurationsfejl. Producentfejl er udviklingsfejl i den enkelte komponent, kompatibilitetsfejl er fejl, der opstår, når komponenterne sættes sammen, designfejl er fejl i måden, designet er bygget på, løsningsleverandørfejl er fejl i leverandørens kode, mens konfigurationsfejl er fejl i opsætningen/konfigurationen.

Løsningsstesternes styrke er, at de har et teknisk overblik over slutkundens løsning. De forstår løsningen, og hvad den skal kunne. Svagheden er, at de ikke har kompetence inden for eller fokus på sikkerhedstests og dermed ikke kan sikre, at de får fat i alle alvorlige sikkerhedshuller, eller at de kommer hele vejen rundt

### **Virksomhedernes metode**

Virksomheder i øvrigt - det vil sige slutkunderne - benytter penetrationstestere til at finde sårbarheder i deres it-systemer. De har fokus på sikkerhed og intet andet. Sikkerhedstestene bliver udført af virksomhedernes interne sikkerhedsafdelinger, testafdelinger eller eksterne penetrationstestere.

Der skal testes for at finde producentfejl, kompatibilitetsfejl, designfejl, løsningsleverandørfejl, konfigurationsfejl og vedligeholdelsesfejl – det vil sige fejl i virksomhedens vedligeholdelse af systemet.

Penetrationstesterne har stor sikkerhedsteknisk indsigt. De er højt specialiserede og kan ikke benyttes til særligt meget andet ud over forskellige typer sikkerhedstests og opgaver i øvrigt, som kræver såkaldt sårbarhedseksperise - det vil sige viden om forskellige sårbarheder, hvordan de opstår, hvordan de kan udnyttes af hackere og orme, og hvordan man som virksomhed kan beskytte sig mod dem.

## **Hvad kan de tre virksomhedskategorier lære af hinanden?**

Hver af de tre virksomhedstyper har styrker, som er vigtige elementer i enhver god sikkerhedstest, som både skal indeholde:

- Testudførelse tidligst muligt i udviklingsforløbet
- Stærk testmetodik/struktur
- Teknisk overblik over produktet eller løsningen
- Stor sikkerhedsteknisk indsigt

Det bedste ville være, at alle ovenstående punkter var opfyldt i enhver sikkerhedstest. I det følgende vil jeg gennemgå de to øverste, som jeg mener, kræver en nærmere forklaring for at forstå, hvorfor de er så vigtige.

### **Testudførelse tidligst muligt i udviklingsforløbet**

Både for producenterne og løsningsleverandørerne gælder det, at det er vigtigt at bygge sikkerhed ind tidligst muligt i udviklingsprocessen - og ikke kun til sidst lige før eller lige efter, at løsningen eller produktet er blevet frigivet. De elementer, der er vigtigst, når man bygger sikkerhed ind i sin udviklingsmodel er efter vores erfaringer såkaldte secure coding-tjeklister, som fx sikrer, at der sker input-validering af alt input og såkaldte source code-inspektioner - det vil sige sikkerhedstests, som er med til at sikre, at sikkerheden løbende bliver tjekket undervejs i udviklingsforløbet.

Som nævnt er det en god ide at give udviklerne tjeklister, der angiver nogle principper, som de skal arbejde efter. Det behøver ikke være omfattende tjeklister - evt. blot en side. Tjeklisten skal give en ramme lige fra start til slut. Inkluder fx secure code-inspektioner i tjeklisten, hvor udviklerne tjekker hinanden for at kvalitetssikre. Det giver et godt awareness-niveau.

Producenterne og løsningsleverandørerne er i stigende grad blevet opmærksomme på de fordele, som de opnår ved at teste tidligst muligt. For slutkunderne er det ikke et indgroet fænomen, og kun enkelte virksomheder, der udvikler sine egne løsninger eller køber it-løsninger hos løsningsleverandører, er opmærksomme på at udføre eller forlange, at der arbejdes efter secure coding-tjeklister, og at der udføres source code-inspektioner. Det er selvfølgelig muligt for disse virksomheder at få gennemgået source-koden i en it-løsning for sikkerhedsfejl, efter at de har købt it-løsningen og sat den i produktion, men de bør også overveje at stille præcise krav til deres it-løsningsleverandører. Det vil i høj grad spare dem selv for omkostninger og besvær.

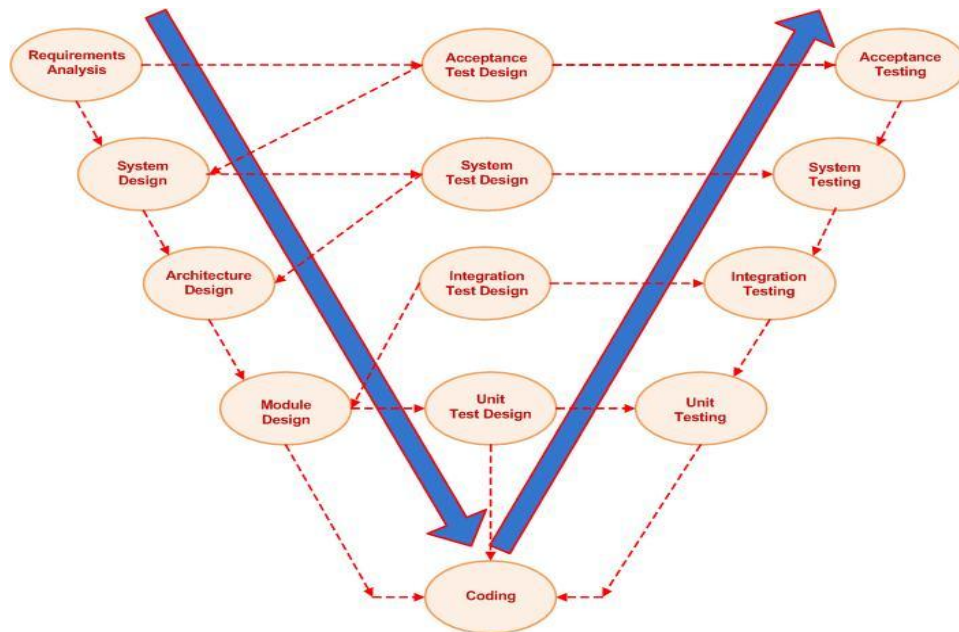
### **Stærk testmetodik/struktur**

Ud over at foretage sikkerhedsreviews og sikkerhedstests så tidligt i forløbet som muligt, er det vigtigt med en stram struktur, når man tester. Sikkerhedstests kræver ganske enkelt en detaljeret og struktureret testplan for at sikre, at testen bliver systematisk, og at man ikke glemmer noget. Dette er helt essentielt, da en sikkerhedstest kan risikere at give en falsk tryghed, hvis den ikke omfatter hele kæden, og der derfor kan være svage led i hele kæden, som ikke bliver tjekket. Testplanen muliggør desuden en struktureret tilgang, hvor kreativiteten og de manuelle tests kan få frit spil inden for en struktureret ramme, hvor testeren ikke behøver at skulle tænke på, om han kommer hele vejen rundt men kan give kreativiteten frit spil.

En god testplan skal indeholde test-scenarier, test-cases og pass/failed-kriterier. Fra almindelige testplaner kender vi test-scenarier eller "use-cases". I en sikkerhedstest skal man vende det på hovedet og bygge "misuse-cases" eller "attack-scenarier". For at kunne skrive gode "misuse-cases" er det blandt andet vigtigt at have en testbaggrund og en stærk forståelse af gængse angrebsmetodikker og sårbarheder. Derudover skal testere også have en sikkerhedsbaggrund, der giver en forståelse og respekt for en struktureret test.

En typisk penetrationstest er ikke nødvendigvis særlig struktureret. Derfor er det en rigtig god ide at indføre - eller stille krav om en klar struktur og testplan hvis man bruger en ekstern tester. Mange tests på markedet i dag er nemlig såkaldte "rent a hacker"-tests, hvor sikkerhedstesten udelukkende beror på penetrationstesterens egne kompetencer, og der ligger meget begrænsede eller ligefrem ikke nogen testplaner bag.

En stærk testmetodik kan illustreres i figur 1, hvor det kan ses, at der løbende igennem de faser, der udvikles i, bliver verificeret, at det man gør, er okay. Det er en klassisk model, som trænger til opdatering, men den illustrerer konceptet om, at man skal teste tidligt i forløbet og følge en strukturel tilgang.



**Figur 1: Den klassiske v-udviklingsmodel**

Det er desuden en rigtig god idé at benytte et test management-system for at holde styr på oplysningerne om testen. Hvis I tester med automatiske værktøjer kan det til tider være tilstrækkeligt at benytte det management-system, som er indbygget i værktøjet, men ellers findes der blandt andet Quality Center, som er et udmærket test management-værktøj, selvom det ikke er målrettet mod sikkerhed.

## Hvilket sikkerhedsniveau skal man vælge?

Sidst men ikke mindst handler det også om, at man fra starten har gjort sig klart, hvilket sikkerhedsniveau man ønsker at ligge på, så man kan sikre sig, at man kan forholde sig til testresultaterne, og hvad de betyder for éns virksomhed.

De løbende sikkerhedstests skal nemlig verificere det sikkerhedsniveau, man som virksomhed har besluttet helt fra starten, at man ville bygge ind i produktet eller løsningen. Forud for testen skal det derfor besluttes:

- Hvornår er det sikkert nok?
- Hvilken model vil man bruge til at blive enige om, hvor højt et sikkerhedsniveau man ønsker?

Se fx FortConsults model med trusselsniveauer i figur 2, hvor man definerer sit ønskede sikkerhedsniveau set i forhold til trusselsbilledet dvs. man afvejer risikoen og vurderer den i forhold til ens sikkerhedsmæssige ambitionsniveau.

### Model til at bestemme det ønskede sikkerhedsniveau

- Niveau 1: Tilfældige/elementære angreb?
  - o Kan modstå: Orme og amatørhackere
  - o Typisk testmetodik: Værktøjskørsler
- Niveau 2: Målrettede angreb?
  - o Kan modstå: Dygtige og vedholdende hackere samt politisk motiverede hackere
  - o Typisk testmetodik: Manuelle test udført efter test-cases suppleret med kreative tests
- Niveau 3: Målrettede angreb med insider-viden?
  - o Kan modstå: Tidligere medarbejdere, kunder, organiseret kriminalitet, samarbejdspartnere, industrispionage og efterretningsvæsener
  - o Typisk testmetodik: Skræddersyede "misuse-cases" og testplaner suppleret med kreative tests

**Figur 2: FortConsults model over trusselsniveauer**

Niveau 1 er amatørhackere, som googler på nettet og finder værktøjer. De er ikke særlig vedholdende eller grundige i deres tilgang, og det er heller ikke svært at gardere sig imod dem. Det kan klares ved at køre nogle standard-værktøjer. Hvis man derudover vil sikre sig på niveau 2, så tager man også højde for de målrettede angreb. Hackerne er dygtigere og mere vedholdende - de giver ikke op med det samme. Det kan foregå over en længere periode og også ved manuelle testmetodikker. På niveau 3 har vi at gøre med en ekstra dimension af insider-viden, hvor hackeren fx kender koden. Det kræver, at der laves skræddersyede misuse-cases til den enkelte virksomhed.

En niveau 1-test kan alle gå i gang med forholdsvis hurtigt og simpelt. På niveau 2 og 3 kræves der organisatorisk indsigt, struktureret tilgang og en dyb forståelse for sikkerhed. Her kan det være en god idé at alliere sig med dygtige penetrationstestere med betydelig sårbarhedserfaring og en struktureret tilgang til at teste. Kun på den måde kan det lade sig gøre at komme hele vejen rundt og finde alle de alvorlige sikkerhedshuller, som kan udgøre en risiko for, at ens virksomhed bliver hacket og får stjålet, slettet eller ændret sine data. Jeg kan ikke fremhæve stærkt nok, hvor vigtigt det er at have en struktureret tilgang til at sikkerhedsteste, lige gyldigt om man er producent, løsningsleverandør eller slutkunde. Og der er ingen tvivl om, at de rendyrkede penetrationstestere, som typisk er dygtige men ustrukturerede kan forbedre deres testresultater ved at lære af producenterne avancerede testmetodikker.

## 2. FortConsult bryder igennem internationalt

**Danske tests af it-sikkerhed går som varmt brød i udlandet. FortConsults internationale salg voksede med 70 procent fra 2008 til 2009, og virksomheden har nu fået fodfæste i Sverige, Norge, Island og Portugal. Det første FortConsult-kontor i Europa forventes at være en realitet inden for en overskuelig fremtid.**

Fra et beskedent kontor på Nørrebro formår Danmarks største firma inden for sikkerhedstest og kreditkort-sikkerhed at sælge sine ydelser til nogle af Europas mest sikkerhedsbevidste virksomheder deriblandt de allerstørste finansielle virksomheder. Portugal, Norge, Sverige og Island er indtil nu de mest succesfulde markeder uden for Danmark, og FortConsult satser på at sælge fra Nørrebro til 17 forskellige lande.

-Vi er stolte og glade for, at vi bliver så positivt modtaget i udlandet. Vi ser det som et solidt bevis på, at vores penetrationstest og ydelser til finanssektoren holder et højt internationalt niveau, siger adm. direktør Ulf Munkedal fra FortConsult, som på kort tid har opnået en position som en af de tre største virksomheder inden for penetrationstest og kreditkortsikkerhed i Europa.

FortConsults internationale salg voksede med 70 procent fra 2008 til 2009, og i de første fem måneder i år har FortConsult allerede solgt lige så meget til udlandet som i hele 2009.

FortConsult er i forvejen markedsledende i Danmark med en kundekreds bestående af nogle af de største virksomheder og den finansielle sektor. Derfor er internationalisering den logiske vej til vækst for FortConsult.

Selv om vi kommer fra en beskeden dansk baggrund, har vi sat os det mål at blive den foretrukne leverandør af sikkerhedstest i hele Europa, siger Ulf Munkedal. Vi har lagt en plan for at teste 17 markeder over 12 måneder, og ind til videre går det klart over forventning. Ulf Munkedal forudser, at FortConsult åbner kontorer eller indgår partnerskaber i flere europæiske lande i løbet af de kommende 24 måneder.

### **Vækst på top- og bundlinje**

FortConsult har generelt ikke nogen problemer relateret til krisen, og virksomheden fremlægger sit bedste regnskab nogensinde. Sikkerhedsfirmaet kom ud af 2009 med en omsætning på 26,9 millioner kroner, hvilket er en vækst på 30 procent i forhold til 2008. Overskuddet før skat blev på 4,0 millioner kroner på trods af de kraftige investeringer i internationaliseringen, hvilket Ulf Munkedal betegner som "tilfredsstillende".

I april måned indgik FortConsult en verdensomspændende aftale med IKEA, som ønskede en sikkerhedspartner til at auditere kreditkortsikkerheden på globalt plan. I Tyskland valgte Siemens FortConsult som ekstern leverandør af sikkerhedstests på webapplikationer hos Siemens selskaber i en

række lande i Europa. Det skete efter en nøje gennemgang og godkendelse af FortConsults test-metoder af Siemens' egen CERT-organisation i Tyskland. Herudover er Nordea og British American Tobacco betydelige internationale kunder.

### **Hackere i den gode sags tjeneste**

FortConsult beskæftiger en række konsulenter, som agerer hackere i den gode sags tjeneste. Kunderne er typisk store virksomheder, der hyrer det danske firma til at forsøge hacke sig ind i it-installationen udefra. FortConsults konsulenter kombinerer hackerens ekvilibristiske metoder med en struktureret og gennemprøvet tilgang, så kunderne får et grundigt og objektivt produkt, når de trækker på sikkerhedstests fra FortConsult. FortConsults 30 medarbejdere inkluderer sikkerhedstest-eksperter fra Danmark, Sverige, Holland, Belgien, Sydafrika og Grækenland.

FortConsult – i mio. kr.	2009	2008
Bruttofortjeneste	22,5	17,1
Resultat primær drift	3,8	1,8
Resultat før skat	4,0	1,4
Årets resultat	2,9	1,0
Antal medarbejdere primo	27	24

## **3. PCI-nyheder**

*Af Lars Syberg, PCI-produktchef i FortConsult*

### **1. Amerikansk PCI-lov indvarsler nye tider i Europa**

I dag er der ingen specifik lovgivning på PCI-området i Danmark. Vi har kun PCI-standarden, som ikke er en lov, men en frivillig aftale mellem to parter, som er underkastet de almindelige aftaleretlige regler. Sådan har det hidtil også været i USA, men her er der nu lovregler om kreditkortsikkerhed på vej, og den tendens vil formentlig også brede sig til EU og Danmark i fremtiden. Blandt andet er der med sikkerhed lovregler om datalækage på vej i Europa.

#### **De amerikanske regler**

De nye amerikanske lovregler betyder, at man nu har valgt at inkludere regler om beskyttelse af kreditkort i lovgivningen i Nevada, Minnesota og senest Washington, og det er sandsynligt, at flere stater vil følge trop.

Den nyeste lov i Washington trådte i kraft 1. juli 2010 og medfører, at amerikanske virksomheder nu er tvunget til at overholde bestemte regler på kreditkortområdet. Formålet med loven er, at en udstederbank skal have mulighed for at få kompensation for udgifter til udstedelse af nye kort, hvis en butik med mere end 6 mio. transaktioner eller kortprocesser mister kortdata, fordi dataene ikke var ordentligt beskyttet. I Nevada har man i stedet valgt gennem lovgivningen at kræve, at erhvervslivet skal overholde PCI-standarden.

#### **Hvad kommer det til at betyde for EU?**

I EU er der naturligvis stor interesse for, om der ligesom i USA vil blive indarbejdet PCI-lignende krav på nationalt eller europæisk niveau. Står det til kreditkortselskaberne, ser man helst, at der ikke indføres lovgivning. Her foretrækker man, at man selv kan formulere og styre reglerne. Og for tiden er der da heller ikke tegn på, at vi får lovgivning om beskyttelse af kreditkort foreløbig. Omvendt har Europa generelt haft tradition for at bygge forbrugerbeskyttelse ind i lovgivningen, og derfor vil vi alligevel i en nær fremtid se flere nye love, som berører betalingssikkerhed, i EU-regi.

I forbindelse med SEPA-direktivet, der primært vil blive implementeret i Euro-landene, vil der eksempelvis blive indført et krav om, at betalinger skal ske med chipkort, allerede i år. Desværre siger EU-reglerne intet om, hvilke sanktioner der vil være, hvis kravet om chipbetaling ikke efterleves.

## **Regler om datalækage på vej i EU**

Når det gælder forbrugerbeskyttelse i forbindelse med datalækage, har man allerede i dag lovregler på området i USA. Reglerne betyder, at hvis man mister data, så har man pligt til at stå offentligt frem og redegøre for datatabet.

Lignende regler er også på vej ind i EU-lovgivningen, og Storbritannien har eksempelvis allerede nu indført sanktionsmuligheder i forbindelse med datatab i lovgivningen.

Siden 6. april i år har Information Commissioner's Office (ICO) fx haft bemyndigelse til at udskrive bøder og give påbud ved datatab. Bøderne kan i dag være på op til 500.000 pund i modsætning til før 6. april, hvor de var på maksimalt 6.000 pund. Reglerne blev indført efter en skandale, hvor toldmyndighederne mistede oplysninger om 25 mio. briter, fordi oplysninger lå på en cd, som gik tabt i posten.

Marks & Spencer fik eksempelvis også et påbud om at kryptere alle deres bærbare computere, efter at de havde mistet oplysninger om 26.000 ansatte, fordi en medarbejder fik stjålet sin computer.

I modsætning til de amerikanske regler kræver de britiske regler dog ikke, at man skal offentliggøre alle hændelser om datatab.

På EU-plan er den såkaldte Digital Agenda også på vej. Den har syv hovedinitiativer, som betyder, at der snart vil blive indført regler om, at internetudbydere skal offentliggøre hændelser, hvor de taber personfølsomme data. Reglerne vil formentlig senere blive bredt ud, så de kommer til at omfatte andre typer af virksomheder.

## **Reglerne vil styrke kreditkortsikkerheden i EU og Danmark**

I forhold til kreditkortsikkerheden i EU og Danmark er det FortConsults vurdering, at de kommende EU-lovregler vil være en klar styrkelse.

For det første vil det gavne både virksomheder og forbrugere, fordi vi får øget gennemsigtigheden, når vi begynder at få mere information om omfanget af datatab i Europa, hvis virksomhederne i højere grad tvinges til at stå frem. Det vil gøre det langt tydeligere for virksomhederne, hvorfor det er så vigtigt at have styr på kreditkortsikkerheden.

Samtidig vil reglerne skabe et langt mere håndgribeligt incitament blandt virksomhederne til at beskytte dataene bedst muligt, fordi det vil skade deres omdømme, hvis et datatab tvinger dem til at stå offentligt frem, og de samtidig risikerer økonomiske sanktioner.

## **2. Chipkortet på vej til at ændre PCI-standarden**

Chipkortet er så småt ved at erstatte kort med magnetstribe i USA, og det er samtidig PCI Councils intention, at PCI-standarden skal tilpasses chipkort. Det er godt nyt for Danmark og resten af Europa, hvor man længe har efterlyst en ændring af PCI-standarden, fordi chipkortet her er langt mere udbredt end kort med magnetstribe.

### **PCI-standarden tager udgangspunkt i kort med magnetstribe**

PCI-standarden, som vi bruger i Europa, herunder Danmark, er som bekendt fra USA. Derfor tager standarden også udgangspunkt i, at den skal beskytte kreditkort med magnetstribe, fordi det stadig er den korttype, der er langt mest udbredt i USA.

PCI-standarden har uden tvivl sin berettigelse pga. det store antal kortnumre, der bliver kopieret og misbrugt over hele verden. I flere årtier har det været muligt at kopiere en magnetstribe fra et kort og derefter lægge indholdet ned på et andet kort. Det er dog først inden for de seneste fem-ti år, at de kriminelle for alvor har fået fokus på svindel vha. teknologi og internettet, fordi alle betalingssystemer nu direkte eller indirekte er forbundet til internettet. PCI Council har derfor siden 2004 fokuseret på at udvikle PCI-standarden, så kortnumrene bliver beskyttet under opbevaring og ved betaling.

### **Chipkortet er et skridt tættere på sikker teknologi**

I Danmark og resten af Europa er vi imidlertid overvejende gået væk fra kreditkort med magnetstribe og over til de langt mere sikre chipkort (EMV). Men fordi vi bruger den samme PCI-standard som USA, skal vi alligevel overholde de samme 240 sikkerhedspunkter som amerikanske virksomheder, fordi reglerne ikke tager højde for, at de europæiske kort er langt mere sikre.

Det betyder, at PCI-standarden reelt ikke matcher de europæiske forhold, som det er i dag, fordi den ikke tager højde for den højere sikkerhed i chipkort.

For mens PCI-standarden i virkeligheden er designet til at skabe sikkerhed omkring en usikker teknologi – nemlig kreditkort med magnetstribe – har vi i Europa valgt at gå i retning af, at vi i stedet hellere vil have en teknologi, som grundlæggende er sikker, i form af chipkort.

Konsekvensen er, at mange af de kontroller, der er i PCI-standarden i dag, bliver mindre vigtige i Europa, set ud fra et sikkerhedssynspunkt. De bliver dermed reduceret til en slags compliance-tjek.

Derfor har der fra mange fronter længe været et ønske om, at USA skal indføre EMV-kort, så de kan højne sikkerhedsniveauet, og så PCI-standarden samtidig kan blive moderniseret og komme til at matche det europæiske sikkerhedsniveau.

### **Fordelene ved EMV**

Fordelen ved EMV er helt overordnet, at det indeholder en lille computer, som er involveret i selve transaktionen. Kortet indeholder et digitalt id, som kortet bruger til at bevise sin autenticitet som en del af transaktionen. I de nyere kort er sikkerheden forbedret ved at bruge Dynamic Data Authentication (DDA), som tilføjer en "random challenge/response" til autorisationsprocessen.

Processen foregår ved, at terminalen sender transaktionsinformation og et tilfældigt tal til chipkortet. Chippen bruger en intern privat nøgle til at generere en unik digital signatur til den specifikke transaktion. Chippens transaktionssignatur bliver tjekket vha. en offentlig nøgle af terminalen og netværket som en del af autorisationsprocessen. Det er kun en uforfalsket chip, der kan levere en gyldig signatur på grundlag af de data, den får, og derfor bekræfter DDA-processen, at kortet er både ægte og til stede. Det er chippen i kortet, der beregner responsen internt, så de vigtige informationer forlader ikke chippen, og derfor kan informationerne ikke bare kopieres, som det er tilfældet med et kort med magnetstribe.

EMV har igennem mange år været et robust værn imod angreb, og teknologien anses stadig for at være relativt sikker i dag. I europæisk perspektiv er det dog et problem, at vores kort stadig skal være udstyret med magnetstribe, så de også kan bruges uden for EU. Magnetstriben kan nemlig kopieres og bruges til at lave kortkopier, der kan misbruges i udlandet. Det betyder bl.a., at PCI-reglerne tvinger en stor udgift ned over mange virksomheder, fordi der på den måde sker korttyverier fra de usikre magnettribesystemer (og gennem e-handel).

FortConsult har udført mange audits gennem de seneste seks år. Hovedparten har fundet sted i Europa, men vi har også lavet en del i USA, Kina, Rusland, Canada og flere andre steder uden for Europa. Vores erfaring viser klart, at EMV markant begrænser muligheden for at stjæle data.

Derfor ser vi meget positivt på, at der i USA er tegn på, at man ønsker at benytte EMV, og at det PCI Councils intention, at de i den kommende version af PCI-standarden vil prøve at tilpasse reglerne til chipkortet – selvom vi endnu ikke ved hvordan. Det vil nemlig gavne både de danske og de øvrige virksomheder, der har implementeret EMV, fordi man med chipkortet tager fat ved problemets rod: at magnettribeteknologien grundlæggende er for usikker.

### **WalMart vælger chipkortet**

I USA har bl.a. supermarkedskæden WalMart for nylig indført betaling med chipkort og pinkode for at øge sikkerheden. Al WalMarts hardware er allerede klar til at benytte EMV-teknologien, og de arbejder i øjeblikket på at færdiggøre softwaren.

Ellen Richey, chief enterprise risk officer hos Visa, USA, har bl.a. kommenteret problemstillingen i USA. I den forbindelse sagde hun, at det ikke er et spørgsmål om, hvorvidt USA skal eller ikke skal gå over til chip,

men i stedet et spørgsmål om hvornår og hvordan. Samtidig har Richey sagt, at Visa mener, at chipteknologien øger sikkerheden og gør det både nemmere og hurtigere at handle for både kunder og virksomheder, og at Visa derfor støtter teknologien 100 pct.

Der er dog stadig lang vej endnu, før chipkortet er den dominerende kreditkorttype i USA, men efterhånden som det vinder indpas, er håbet, at PCI-standarden også vil blive tilpasset den nye og mere sikre virkelighed i USA og dermed også Europa.

Chipkortet løser imidlertid ikke problemet med sikkerheden, når det gælder onlinebetaling, hvor man stadig bruger kortnummeret, udløbsdatoen og evt. kontrolcifrene. Så på det område vil der stadig være de samme udfordringer med at skabe sikkerhed omkring oplysningerne, men også her bliver der arbejdet på nye og mere sikre løsninger – men det ligger noget længere ude i fremtiden.

### **3. Ny standard for PCI-scanninger ændrer processen**

Jeres ASV (Approved Scanning Vendor) vil fremover begynde at stille nogle andre spørgsmål og gøre nogle andre ting, end I er vant til, når I skal have lavet PCI-scanninger. Det skyldes, at PCI Council har ændret reglerne i den del af PCI-standarden, som har med scanning at gøre. Det stiller nye krav til ASV'ernes ydelser.

#### **ASV'en skal involveres mere i processen**

De nye regler ændrer ikke voldsomt meget på typen af scanning. Der er stadig tale om en scanning, der overordnet set skal afsløre sårbarheder med nogen fokus på webapplikationer, men processen omkring scanningen er blevet grundlæggende ændret.

Selvom det hele tiden har været hensigten med PCI-scanningsreglerne, at ASV'en skal hjælpe kunden med scanningen, har de hidtidige regler reelt gjort det muligt, at en virksomhed selv kan stå for hele processen omkring en ASV-scanning. Det har betydet, at en ASV i virkeligheden blot har kunnet nøjes med at stille et webinterface til rådighed for sine kunder, som så via selvbetjening har kunnet indtaste informationer og IP-adresser og køre scanningen på egen hånd.

Problemet med den fremgangsmåde er, at en del PCI-scanninger er blevet udført forkert, fordi ASV'en ikke har kontrolleret, at de informationer, kunden indtaster i webinterfacet, også er de korrekte og nødvendige informationer. Den gamle løsning har dermed givet mulighed for betjeningsfejl, fordi ASV'erne i mange tilfælde har fortalt deres kunder, at en scanning kan klares med ganske få klik i et webinterface og intet andet. Dermed er der i princippet ingen garanti for, at virksomheden reelt er sikker, selvom den på papiret består PCI-scanningen, og det kan nemt reducere kontrollen til en slags alibiscanning. Det betyder, at der kan være stor forskel på den sikkerhed, PCI-scanningen skulle give – og som PCI Council har ønsket – og den sikkerhed, som virksomhederne reelt har opnået.

Den form for selvbetjening er en fremgangsmåde, man typisk ser hos de ASV'er, der primært konkurrerer på prisen, og det er en fremgangsmåde, vi hos FortConsult altid har været kritiske over for, og som vi derfor aldrig selv har praktiseret som ASV.

Vi har altid været fortalere for, at ASV'en skal være en aktiv del af processen. Derfor er vi også tilfredse med, at de nye regler i langt højere grad end de gamle regler tydeliggør, at ASV'en skal involveres i scanningsforløbet for i kundens egen interesse at kontrollere, at det reelle sikkerhedsniveau følger PCI-standarden.

#### **Konsekvenserne af de nye regler**

Som køber af en PCI-scanning vil de nye procedurer bl.a. medføre, at jeres ASV fremover skal kontrollere, at de informationer, I indtaster, er korrekte, at scanningen er foregået korrekt, og at scanningsrapporten er retvisende.

De nye regler påpeger desuden specifikt, at ASV'en altid skal dobbelttjekke scanningsresultater, som formodes at indeholde falske positive.

Virksomheden skal selv undersøge de formodede falske positive og forklare, hvorfor det blot er en fejl i scanningsmekanismen og ikke en reel sårbarhed. Det gælder også, hvis man får en falsk positiv to kvartaler i træk uden at have ændret på konfigurationen. Det vil naturligvis gøre processen mere krævende end tidligere, og for mange vil det blive et irritationsmoment. Men ud fra et forsigtighedsprincip mener vi, at skærpelsen giver god mening, fordi noget, der ligner en falsk positiv, af og til faktisk viser sig at være en reel sårbarhed.

### **Mere fokus på webapplikationer**

De nye regler betyder også, at webapplikationstesten er blevet opprioriteret, hvilket vi er særdeles tilfredse med. Området var næsten fuldstændig overset i de gamle regler, selvom de fleste indbrud sker via sårbarheder i webapplikationer. Der er dog stadig langt til en decideret webapplikationstest, men den type test bør virksomhederne også selv udføre i forbindelse med kapitel seks i PCI-standarden. I praksis er der dog mange mindre virksomheder, som ikke får udført kontrollerne under kapitel seks og derfor nøjes med PCI-scanningen (og det vil naturligvis gøre dem noncompliant, at de ikke udfører alle kontroller).

Derudover indeholder reglerne også hjælp til situationer, hvor man bruger IDS/IPS, har outsourcet dele af løsningerne og mange andre situationer, man som kunde kommer ud for i dagligdagen, og som tidligere har været uklart beskrevet.

### **De nye regler løfter sikkerhedsniveauet**

De nye regler har været længe undervejs og er blevet grundigt bearbejdet af mange forskellige interessenter. Det har også været nødvendigt at gennemarbejde dem, da de grundlæggende bygger på en MasterCard-standard, der er næsten 10 år gammel, og som oprindeligt ikke var koblet sammen med PCI-standarden (der er baseret på Visa CISP-standarden).

De gamle PCI-scanninger har efter vores mening ikke givet nævneværdig sikkerhed for de virksomheder, der fik foretaget scanningerne. Men de har som nævnt stadig givet en sikkerhedsgodkendelse på papiret, og i mange mindre virksomheders tilfælde har PCI-scanningen været det eneste, som er blevet foretaget af en ekstern leverandør for at validere, om virksomheden overholder PCI-standarden.

Derfor er de nye procedurer efter FortConsults vurdering et skridt i retning af bedre sikkerhed, fordi de gamle regler ikke i tilstrækkeligt omfang har formået at sikre, at hensigten med PCI Councils regler blev understøttet. Derfor håber vi også, at formuleringerne i de nye regler er klare nok til at luge ud blandt ASV'er i branchen. Nogle ASV'er har nemlig hidtil udnyttet hullerne i det gamle regelsæt til at udbyde discountscanninger, som desværre har været med til at udvande kvaliteten af PCI-scanningerne. Dermed har de ASV'er også været med til at underminere både standarden og i sidste ende også sikkerheden hos kunderne.

De nye regler vil derfor formentlig betyde, at lavprisscanningerne stiger i pris – medmindre det lykkes lavpris-ASV'erne at finde en ny smutvej uden om PCI Councils regler og intentioner. Hos FortConsult forventer vi ikke, at vi ændrer prisen på ASV-scanninger, da vi hele tiden har været involveret i scanningsprocessen for at sikre, at vores kunders scanninger er blevet udført ud fra de korrekte procedurer.

Lige nu er det frivilligt for ASV'erne, om de vil følge de nye eller de gamle regler, men fra 1. september skal ASV'erne følge de nye regler.

## **4. De simple PCI-løsninger er tit bedst og billigst**

Når vi holder indlæg på PCI-konferencer rundt omkring i verden, bliver vi bagefter ofte kontaktet af hardware- og softwareleverandører, der gerne vil have os til at kigge nærmere på deres PCI-sikkerhedsløsninger og anbefale dem til de kunder, vi er QSA (Qualified Security Assessor) for. Det skyldes, at mange af hardware- og softwareleverandørerne har set muligheder på PCI-området, og i mange tilfælde har QSA'ere også en ganske god forretning ud af at sælge løsninger ved siden af at udføre audits. Sammenblandingen af QSA- og leverandørrollen er imidlertid ikke uden problemer, fordi det skaber en tendens til, at kunderne ofte ender med at købe for komplicerede og for store PCI-løsninger, når man sammenligner med deres reelle behov.

Efter vores mening er det vigtigste for en QSA, at de bevarer uafhængigheden, så kunderne altid ved, at de kan stole på de råd, QSA'en giver dem om, hvad de skal ændre i deres sikkerhedssystem for at overholde PCI-standarden. Hvis man ligesom en mekaniker både påpeger problemet og sælger løsningen på samme problem, mister man en del af troværdigheden, og derfor takker vi som regel nej til at samarbejde med dem.

#### **Mange virksomheder forkøber sig i PCI-løsninger**

Som kunde hos en QSA er problemet tit, at man ikke altid er klar over, hvilken løsning der skal til for at overholde PCI-standarden. Derfor ser vi en tendens til, at mange virksomheder kommer til at forkøbe sig i alt for avancerede løsninger på PCI-området. Det skyldes både, at kunderne ikke altid selv har styr på, hvordan de opfylder et konkret krav i PCI-standarden, men også at mange kunder bliver overvældet af de mange funktioner, der typisk er i de store totalløsninger.

Problemet med mange af de avancerede løsninger er, at de bygger på standardsikkerhedsprodukter, der typisk ikke er designet til at imødekomme kravene i PCI-standarden, men som i stedet er lavet til at dække over mange forskellige typer af sikkerhedsbehov. Selvfølgelig kan mange af produkterne justeres, så de lige nøjagtig dækker et bestemt punkt i PCI-standarden, som fx overvågning af logfiler eller id-management. Men vi ser tit, at det kommer bag på en virksomhed, at den avancerede løsning, de har investeret i, faktisk ikke overholder alle PCI-reglerne, men skal suppleres med en eller flere andre løsninger. Det gør det tit svært for virksomhederne at overskue og administrere PCI-løsningerne, og så kan de nemt havne i en situation, hvor deres PCI-løsning aldrig bliver ordentligt implementeret. I mange tilfælde ser vi meget dyre og avancerede løsninger, som ikke er implementeret ordentligt i organisationen og derfor slet ikke fungerer efter hensigten.

Men det behøver faktisk slet ikke at være så svært.

#### **Hjemmelavede løsninger rækker langt**

Mange af vores kunder har udviklet deres egne løsninger, som er simple, og som virker rigtig godt. De bliver godkendt af os som QSA, og så er de desuden typisk meget velintegrerede i virksomhedens øvrige processer og eksisterende software.

Det gælder med andre ord om at finde en løsning, som opfylder de behov, man helt konkret har på PCI-området, og så sørge for at få den løsning implementeret i dagligdagen. Det giver nemlig oftest både den sikreste og billigste løsning og en proces, som gør det nemmest muligt at overholde PCI-standarden.

I næste nyhedsbrev kan du læse mere om den nye PCI-standard, der træder i kraft 1. januar 2011.

## **4. FortConsult støtter Rådet for Større IT-Sikkerhed**

FortConsult har valgt at støtte Rådet for Større IT-Sikkerhed i deres bestræbelser på at forbedre it-sikkerheden i Danmark og internationalt. Rådets primære formål er sikre, at it-brug kan ske sikkert. De vurderer it-sikkerhedstiltag og stræber efter at give uafhængig rådgivning til både politiske institutioner såvel som borgere, virksomheder og den offentlige sektor.

FortConsult har valgt at støtte Rådet og håber derved, at vi kan bidrage til styrkelsen af it-sikkerheden i Danmark.

Du kan læse mere om Rådet for Større IT-Sikkerhed på [www.rfsits.dk](http://www.rfsits.dk)

## 5. Nyansatte i FortConsult

FortConsult A/S har i andet kvartal af 2010 ansat tre nye medarbejdere. Security Consultant Anders Olsen, Business Development Manager Peter T. Hansen og Delivery Assistant Kristina Landsperg har alle sluttet sig til FortConsult for at fremme den fortsatte vækst.

Anders Olsen er ny Security Consultant i FortConsult. Han har arbejdet med it-sikkerhed i mere end 6 år og har de sidste 4 år været ansat som it-sikkerhedschef for den danske hostingvirksomhed EasySpeedy ApS. Før dette var han selvstændig drifts- og sikkerhedskonsulent. Anders' primære ansvarsområde i FortConsult bliver at udføre penetrationstests af vores kunders it-systemer.

Peter T. Hansen har en baggrund inden for it-branchen og kommer fra en stilling som Country Sales Manager i Danmark for den tyske koncern EPLAN, hvor han blandt andet havde ansvaret for salg, markedsføring og kundesupport. Før dette havde Peter salgsledelsesjob i Danmon Danmark A/S og Semco Danmark A/S. Peter skal varetage en fast kundegruppe i FortConsult og samtidig medvirke til at videreudvikle salgsorganisationen, så den danner grobund for FortConsults fremtidige vækst, både nationalt og internationalt.

Kristina Landsperg er ansat i FortConsult som Delivery Assistant og er en del af vores leveringsplanlægningsteam. Du vil derfor møde Kristina, når du skal have planlagt en leverance.

Vi er meget glade for, at de tre nye ansatte har sluttet sig til os, og håber, at I vil få et godt samarbejde.

## 6. Nye referencekunder i FortConsult

Vi byder velkommen til vores nye danske referencekunder: Chempilots, Cimber Air, Dansk Supermarked Gruppen, Region Syddanmark og SKAT.

Vi byder også velkommen til vores nye internationale referencekunder: Bank Petrocommerce (RU), Boss Media (SE), BS/2 (LT), DnB NOR (NO), EDB Business Partner (NO), EDB Card Services (SE), EMIS (AO), ErgoGroup (NO), HZMEDIA LIMITED (RU), IKEA (SE), INPAS (RU), Nurbank (RU), Russian Agricultural Bank (RU), Signicat (NO), Teris (IS), UniCredit Group (RU) og Valitor (IS).

EDB Card Services, Region Syddanmark, Dansk Supermarked Gruppen og Signicat har udtalt sig om vores samarbejde:

### **En professionel og positiv oplevelse**

"FortConsults PCI-auditor var både positiv og konstruktiv, på et højt teknisk niveau og kvalificeret til at rådgive os om tekniske problematikker. Han var detaljeorienteret og effektiv på samme tid og leverede en meget professionel og grundigt forberedt PCI-audit, som både vi og VISA var tilfredse med. Gennem hele processen har vi følt os i gode hænder og er glade for at have indgået en lang 3-årig kontrakt med FortConsult."

*Tommy Johansson, EDB Card Services*

### **Dygtighed og fleksibilitet**

"FortConsult har leveret en rigtig god teknisk sikkerhedsrapport som resultat af vores sikkerhedstest. Præsentationen af rapporten henvendte sig til både teknikere og ledelse og har givet et godt indblik i vores sikkerhed. Topkarakter til sikkerhedskonsulenten - han både brænder for tingene og har evnen til at præsentere testresultaterne og anbefalingerne godt. Vi er meget imponerede. Ydermere har vi sat stor pris på den fleksibilitet, som FortConsult udviste i planlægningen af testen."

*Carsten Frølich, Region Syddanmark*

### **God blanding af tekniske kompetencer, forretningsforståelse og PCI-viden**

Jeg er godt tilfreds med gap-analysen som FortConsult har udført for os. FortConsult leverer en god blanding af tekniske kompetencer, forretningsforståelse og PCI-viden i et sådan projekt. Vi har gennem hele processen følt os trygge og haft en rigtig god dialog med alle de involverede hos FortConsult. Det har betydet, at vi har kunnet holde fokus på de relevante forhold omkring compliance. Jeg kan varmt anbefale samarbejdet med FortConsult til andre."

### **9,5 for god proces og et højt fagligt niveau**

*Allan Fabricius, Dansk Supermarked Gruppen*

Vi har igennem vores samarbejde med FortConsult følt os i trygge hænder igennem hele processen - der har været gode tilbagemeldinger og god information om, hvad der skulle ske. FortConsult har haft godt styr på processen og udvist stor fleksibilitet i at tilpasse leveringstidspunktet til vores behov. Vi er desuden fuldt ud tilfredse med sikkerhedsrapporten, som er veludformet og med et fagligt højt indhold. Vi er vældig positive og giver FortConsult 9,5 på en skala fra 1-10, hvor 10 er højest. "

*Harald Stendal, Signicat*

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