



StayInTouch

– sikkerhedsnyheder fra FortConsult

Indhold i nyhedsbrev for april 2009

1. Ny sikkerhedsstandard fra kreditkortselskaberne
2. Slæk ikke på sikkerheden selvom et tyveri virker usandsynligt
3. PCI-nyheder
4. Awareness omkring Side Wide Cross Site Scripting
5. Sikkerhedskonsulent i FortConsult opnår guldcertificering i trådløs sikkerhed
6. Nyansatte i FortConsult

Du kan tilmelde dig vores elektroniske nyhedsbrev på www.fortconsult.net

FORTCONSULT

Klar besked om it-sikkerhed

1. Ny sikkerhedsstandard fra kreditkortselskaberne

Den udbredte PCI-standard har fået en søster-standard ved navn PA (Payment Application), som har til formål at gøre betalingsapplikationer mere sikre. Hermed adresserer kreditkortselskaberne et af de svageste led i PCI-kæden til opnåelse af den nødvendige kortsikkerhed i de mange fysiske så vel som elektroniske butikker.

FortConsult er som den eneste danske virksomhed - ud af 39 på verdensplan - blevet godkendt af kreditkortselskaberne til at teste sikkerheden i betalingssoftware ifølge PA-standarden. Den omfattende investering i blandt andet et nyt testlab ser FortConsult som et naturligt skridt i virksomhedens bestræbelser på at blive førende på PCI-området i Europa.

Kreditkortselskaberne, anført af VISA og MasterCard og deres fælles organisation PCI Council, har lanceret en ny sikkerhedsstandard ved navn PA-standarden, som følger i kølvandet på den meget udbredte søsterstandard, PCI (Payment Card Industry). Mens PCI-standarden berører virksomheder, der håndterer kreditkorttransaktioner, er PA-standarden gældende for virksomheder, der udvikler eller installerer betalingssoftware og dankortløsninger, som benyttes rundt omkring i danske butikker, banker, pengeautomater og e-handelsløsninger.

PCI-standarden blev introduceret i 2004 og er allerede implementeret i stor udstrækning i USA og Europa. I Danmark er adskillige tusind virksomheder i dag berørt af denne standard, deriblandt butikker, banker og betalingsgateways. Nu er turen kommet til PA-standarden, som adresserer et af de svageste led i PCI-kæden: Sikkerheden i butikkernes betalingsapplikationer. De første amerikanske og europæiske virksomheder er i fuld gang med at gøre sig klar til at blive PA-certificeret - heraf en række danske virksomheder som fx integratorer, der udvikler software til kasseapparater og terminalleverandører, som udvikler betalingsterminaler til butikker.

Certificeret som eneste danske virksomhed

Til at hjælpe sig med at rådgive og sige god for sikkerheden i de mange forskellige typer betalingssoftware, som skal leve op til PA-standarden, har kreditkortselskaberne udpeget og certificeret 39 sikkerhedsvirksomheder på verdensplan. FortConsult er den eneste danske virksomhed, som har søgt om og bestået PA-certificeringen. Ulf Munkedal, adm. direktør i FortConsult, udtaler: "Vi er glade for at være de første i Danmark, som kan hjælpe softwareleverandører med at få godkendt deres betalingssoftware, så deres kunder ikke risikerer erstatningssager fra kreditkortselskaberne, hvis softwaren bliver hacket. Det har krævet en betydelig investering for os at blive klar til at kunne sikkerhedsteste betalingssoftware, men vores mangeårige erfaring i at hacke it-systemer og vores fodfæste i den finansielle branche har været en stor hjælp til at komme godt fra start."

Satser på PCI

Ifølge Ulf Munkedal har det været en naturlig beslutning for FortConsult at blive PA-certificeret. "Vi har et erklæret mål om at blive førende på PCI-området i Europa, og at kunne sikkerhedsteste betalingssoftware efter PA-standarden er et must for at få adgang til endnu flere kunder og nye markedssegmenter både i Danmark og i resten af Europa. Vi var blandt de første, der blev certificeret til at udføre kontroller af virksomheders betalingssystemer i henhold til PCI-standarden og har siden vi opnåede certificeringen i 2004 opbygget et lukrativt forretningsområde, som er medvirkende til, at vi får mange henvendelser fra nye kunder i hele Europa," siger Ulf Munkedal.

Teknikerdrøm der går i opfyldelse

FortConsults nye testlab er oppe at køre, og virksomhedens sikkerhedskonsulenter har været igennem et omfattende træningsprogram i USA for at blive klar til at teste de første softwareløsninger. Ulf Munkedal: "Det er meget motiverende for vores teknikere, at de nu også kan

teste "live" kreditkortsystemer, som er koblet til PBS og udenlandske banker i vores nye testlab. At få lov til at hacke en "pengeautomat" er uden tvivl blandt de mest spændende opgaver for en sikkerhedstester i dag."

FortConsult har med sine 26 medarbejdere Danmarks største arbejdsplads for sikkerhedstestere i Skandinavien. Med sin PA-certificering håber sikkerhedsvirksomheden at opnå en yderligere blåstempling af sin hackerekspertise. Ulf Munkedal pointerer: "Der er ingen tvivl om at PCI- og PA-standarden er kommet for at blive, og at kreditkortselskaberne vil gøre meget for at håndhæve, at standarderne bliver fulgt. Eksempelvis har VISA netop offentliggjort en liste over leverandører, der leverer applikationer med utilstrækkelig sikkerhed."

FortConsults PCI-historie

- PCI-certificeret i 2004 til at udføre sikkerhedsskanninger som de første og eneste i Skandinavien.
- PCI-certificeret i 2005 til at udføre audits som de første og eneste i Skandinavien.
- Udvalgt af PBS til at hjælpe danske datacentre med at blive PCI-godkendte pga. vores tidlige PCI-certificering, vores betydelige erfaring på PCI-området og vores store kendskab til den finansielle branche.
- Fast PCI-leverandør til alle danske banker med behov for PCI-assistance.
- Har udført PCI-opgaver for nogle af de største butikskæder i Norden på internationalt plan.
- Er i dag den største PCI-leverandør i Norden og Baltikum. Vi har fx PCI-certificeret over 60 procent af virksomhederne på VISA's liste over godkendte skandinaviske service providers.
- PA-certificeret i 2008 som de første og eneste i Danmark - og blandt de første 14 på verdensplan.

2. Slæk ikke på sikkerheden, selvom et tyveri virker usandsynligt

Røveriet på Antvorskov Kaserne i vinter besvarer det helt centrale spørgsmål omkring sikkerhed. Kan det betale sig at sikre sine værdigenstande, selvom det virker usandsynligt, at nogen kan finde på at stjæle dem? Svaret er selvfølgelig ja, især i de tilfælde, hvor konsekvenserne af et tyveri er meget alvorlige.

Lars Syberg, PCI-produktchef i FortConsult, sammenligner Forsvaret og deres - for kriminelle så attraktive - våben med virksomheder, der håndterer kreditkortdata.

Af Lars Syberg, PCI-produktchef i FortConsult A/S

I vinter lykkedes det for en gruppe kriminelle at stjæle våben svarende til 100 mands udrustning fra Antvorskov Kaserne. Efterfølgende diskuterede både politikere, forsvarsledelsen og de menige det centrale spørgsmål: Kan det virkelig passe, at civile kan troppe op og uden større vanskeligheder tvinge sig adgang til så mange våben?

Røveriet kom bag på mange, selvom det skete på et sted, hvor der findes en stor samling af moderne våben, som kriminelle i Danmark eller udlandet naturligt nok kunne tænkes at være interesserede i. Samtidig var de sikkerhedsmæssige foranstaltninger på kasernen på et sådant niveau, at våbnene ligefrem har været lette at stjæle.

Sammenligning mellem Forsvaret og PCI

Det er efter min mening nærliggende at trække nogle paralleller til vores egen PCI-verden:

- Ifølge Rigspolitiets NEC er det organiserede kriminelle, der står bag. Organiserede kriminelle står også bag de fleste tyverier af kreditkortdata.
- Stjålne kreditkort og våben bruges begge dele til at udføre endnu mere kriminalitet, oftest for at berige de kriminelle.
- Uden at være ekspert i organiseret kriminalitet vil jeg gætte på, at penge står øverst på de kriminelles ønskeliste. Efter penge kommer sandsynligvis forskellige værktøjer, der kan hjælpe med at skaffe penge fx våben. Fra mit arbejde som PCI-produktchef i FortConsult ved jeg, at kreditkortdata ligger inden for top 5 - endnu en parallel mellem våben og kreditkortdata.
- Til gengæld giver kreditkortdata lynhurtigt adgang til penge uden den fysiske risiko, der ligger i at komme i ildkamp med politiet - hvilket man ikke kan sige er tilfældet med våbentyverier.

Høj risiko som blev undervurderet

At ligge inde med dét, som kriminelle jagter allermest, hvad enten det er våben eller kreditkortdata, indebærer naturligvis en stor risiko for, at værdigenstandene bliver stjålet. Faktisk bør man med høj sandsynlighed regne med, at de bliver stjålet på et tidspunkt, hvis sikkerheden ikke er i orden, selvom det forekommer én at være usandsynligt.

I tilfældet med Antvorskov Kaserne kunne Forsvaret efter min mening være ret sikre på, at et tyveri ville finde sted på et tidspunkt. Tilsyneladende valgte de alligevel at reducere sikkerheden på kasernen løbende, og de overvejede efter sigende at outsource den til private ubevæbnede vagter. Dette skete formentlig bevist eller ubevist, fordi der ikke var sket noget alvorligt hidtil, og fordi det for de fleste virker helt utænkeligt, at en kaserne får besøg af bevæbnede mænd, som overmander Forsvarets egne vagter. Men virkeligheden er en anden, har det vist sig med al tydelighed. Forsvaret har nu oplevet, at risikoen er der - og i virkeligheden er den måske endda tiltagende på grund af den stigende organiserede kriminalitet.

På samme måde må vi huske, at det også kan forekomme højest usandsynligt, at kreditkortdata bliver stjålet fra et rimeligt sikret sted.

Forsvarets hændelse får mig til at få lyst til at drage paralleller til sikkerheden ved kreditkortdata:

Sørg for sikkerhed hele vejen rundt

Vi må løbende sørge for, at sikkerheden er i orden hele vejen rundt, når vi har med kreditkort at gøre - også selvom der ikke er sket tyverier hidtil, og man ikke kan forestille sig, at det vil ske i praksis. Især skal vi passe på ikke at sløse med procedurerne. Fx skal vi huske at låse døren hver gang, vi skal løbende tjekke, at alle sikkerhedsmekanismerne stadigvæk fungerer, og vi skal sørge for at kontrollere, hvem vi ansætter. Og så skal vi huske, at det uventede kan ske, og at det måske endda sker ved et voldsomt (elektronisk) angreb, og ikke bare ved at en CD med kreditkortdata uheldigvis bliver tabt et sted.

Det er disse hændelser, som vi får hjælp til at sikre os imod fra PCI-standarder. Den sikrer nemlig, at vi kommer hele vejen rundt, så vi også er parate til det uventede.

Vær opmærksom på truslen indefra

Politiet kom frem til, at røveriet på kasernen blev udført af tidligere soldater, da røverne havde meget præcis viden om, hvilke skabe de skulle have adgang til, hvilke låse der skulle åbnes, og hvilken vagtbemanding der var. Omkring halvdelen af de kreditkorttyverier, der sker, bliver udført af "insidere" - det vil sige nuværende/tidligere medarbejdere, samarbejdspartner eller servicefolk. Igen skal vi huske at adressere disse trusler, når vi beskytter kreditkortdatene.

Husk overvågning

Forsvaret havde ingen spor af røverne. De havde tilsyneladende kun et enkelt videokamera, som overvågede en indgang, som ikke bliver brugt mere. Og ingen blev alarmeret, før røverne var over alle bjerge. Med PCI-standarden skulle vi gerne have tilpas meget overvågning, så vi under og efter et tyveri nøjagtigt kan se, hvad der er sket. Vi kan formentlig ikke sikre alting 100 procent, men hvis vi bliver alarmeret, når der sker noget, har vi i kraft af vores overvågning de bedste forudsætninger for at stoppe de kriminelle hurtigst muligt.

Uden at være ekspert i hvordan våbentyve opfører sig, vil jeg mene, at der er stor sandsynlighed for at de i dagene efter røveriet stadigvæk har befundet sig i Danmark eller i et land tæt på. Når det kommer til stjålne kreditkort, er der imidlertid kun én ting, der er sikkert: Kreditkortdataene findes et eller andet sted på kloden eller muligvis alle steder - i kraft af internettet. Endnu en god grund til at sætte overvågningsløsninger op - både fysisk og elektronisk.

Flere fysiske røverier af kreditkort

De fleste vil nok mene, at det er usandsynligt, at der vil dukke bevæbnede røvere op for at røve vores kreditkortdata. På samme måde som det virkede utopisk at røvere ville gå til angreb på Forsvaret. Virkeligheden er igen en anden: Risikoen og dermed sandsynligheden eksisterer i høj grad, hvad angår kreditkortdata. Vi ser allerede i andre dele af verden, at bevæbnede tyve truer butiksekspedienter til at isætte skimming-chips i butikens kreditkortterminal, så det er desværre muligt, at det kun er et spørgsmål om tid, før det sker i Danmark. Vi kan blot håbe på, at der kommer til at gå lang tid - og i mellemtiden tage de nødvendige forholdsregler for at beskytte os.

3. PCI-nyheder

1. Ny version af PCI-standarden

Den tredje version af PCI-standarden, version 1.2, udkom i oktober 2008 og har været gældende 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 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-rikisico 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-standarden - 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-standarden.

I Sverige er de virksomheder, som skal overholde PA-standarden, 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 spille 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

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.

Målttede 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 målttet 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

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 fik ændringen betydning for mange af vores kunder, som skulle 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-standarden og vender tilbage med næste nyhedsbrev, når vi har relevant nyt at fortælle.

4. Awareness omkring Site Wide Cross Site Scripting

Af Anders H. Salling, it-sikkerhedskonsulent i FortConsult A/S

1. Indledning

Sammen med Peter Österberg, som også er sikkerhedskonsulent i FortConsult, har jeg opdaget en ny måde at udnytte en hackerteknik på, som både webudviklere og sikkerhedsansvarlige skal være opmærksomme på og beskytte sig mod. Det vil jeg skabe awareness om ved at beskrive teknikken her i artiklen. Teknikken har vi valgt at kalde Site Wide Cross Site Scripting (SWXSS) og er en udvidet hackerteknik inden for Cross Site Scripting (XSS).

Hackerteknikken XSS (Cross Site Scripting) ligger i top 10 på OWASPs liste¹ over web-sikkerhed og er derfor vigtig at være opmærksom på. Jeg mener, at der generelt er for lidt fokus på XSS, muligvis fordi det er en sårbarhed, der bliver vist i browseren (og angriber brugeren) og dermed ikke kommer ind på serveren (og angriber virksomheden). Ved XSS har der først og fremmest været fokus på, at det kan udnyttes til at lave "internet-graffiti" eller måske stjæle brugerens cookie. I denne artikel om SWXSS kan du læse om et eksempel på, hvor meget mere det kan udnyttes - ikke blot til at omfatte de sårbare sider - men også efterfølgende sider.

En ekstra dimension

For web-applikationer, der er sårbare over for XSS, er SWXSS en yderligere dimension af sårbarhed at tage højde for. Den begrænsning, der er ved XSS, er ikke længere gældende for SWXSS, da det tilførte script ved brug af SWXSS stadig er brugbart for hackeren, når brugeren forlader den sårbare URL-adresse - dog fungerer SWXSS stadig kun inden for det aktuelle site. Den ekstra dimension ved SWXSS består i, at det tilførte script forbliver i brugerens browser, selv efter at han forlader den sårbare URL, dog betinget af at brugeren klikker sig frem mellem siderne og ikke ændrer i URLen.

Der er god grund til at være opmærksom på SWXSS, da teknikken giver hackere mulighed for at se alle de oplysninger, som brugeren taster ind på sitet. Der skal skabes større awareness omkring problemet og spredes viden om konsekvenserne. Det gælder både på ledelsesniveau og som en teknisk viden hos web-udviklerne.

2. Konsekvenser af et SWXSS-angreb

Det er vigtigt at forholde sig til alvorligheden af de konsekvenser, det kan have, hvis en webside med fortrolige oplysninger bliver udsat for et angreb af enten XSS eller SWXSS. En række eksempler på, hvad en hacker kan foretage sig ved hjælp af SWXSS:

- Industrispionage
- Stjæle personoplysninger som fx
 - o Kreditoplysninger
 - o Passwords
 - o Cookies
- Lave graffiti - ændre websitet
- Bestille varer og handle i andres navn
- Netbanksoplysninger – internationale banker

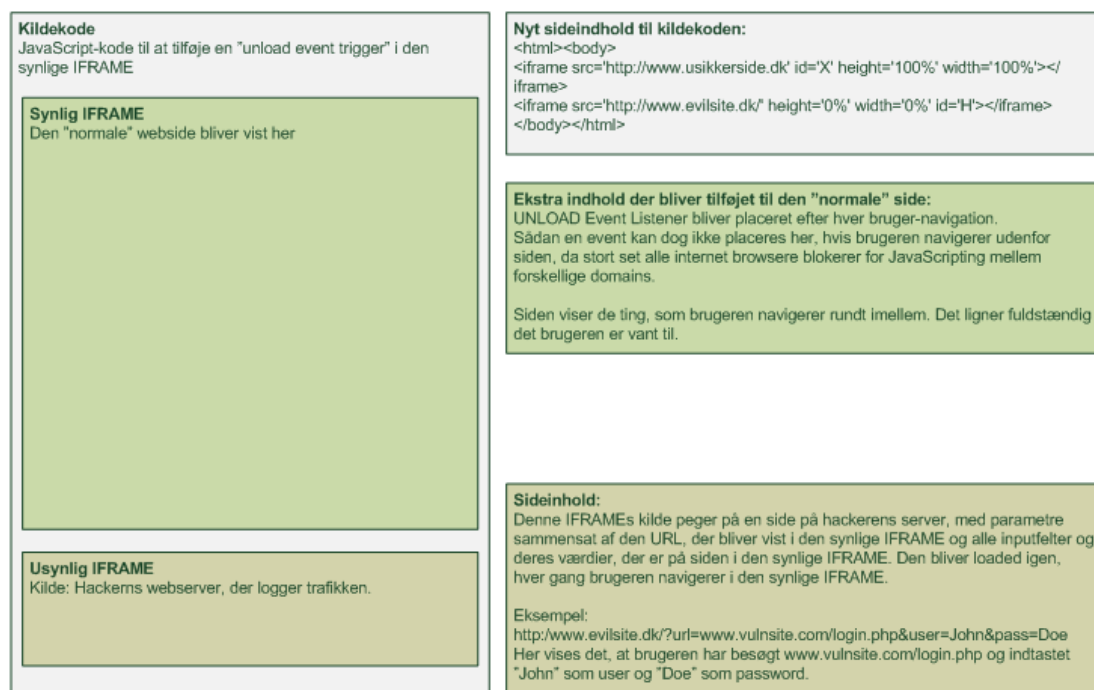
Et eksempel på konsekvenserne af SWXSS kan være, når en kunde logger ind på en web-shop. Brugeren indtaster sit brugernavn og login for at komme ind på siden. Det er oplysninger, som hackeren får adgang til, også selvom det er en SSL session, som normalt sikrer, at udefrakommende ikke kan overvåge trafikken til serveren. Men det stopper ikke her. Hvis brugeren beslutter sig for at gøre et indkøb på hjemmesiden, vil han sidst i forløbet blive bedt om at taste en række oplysninger ind. Det drejer sig om kreditkortoplysninger, som hackeren også får direkte adgang til, inklusiv CC-nummer, CVV-nummer, udløbsdato og eventuelt brugerens fulde navn. Oplysninger som kan bruges til svindel, tyveri og grov udnyttelse af personoplysninger. Alt sammen kan føre til fatale konsekvenser, som websitets virksomhed juridisk hæfter for.

3. Hvordan gør hackeren?

Hackeren bruger en kombination af indsat HTML og JavaScript på et website. HTML-koden er indsat via JavaScript, hvoraf den ene er synlig. Herefter viser hackeren en valgt side, fx forsiden, til brugeren i den synlige IFRAME, og hackeren kan nu lægge et link ind til en side hos sig selv i den usynlige IFRAME. Teknikken gør, at hver gang der bliver navigeret i den synlige IFRAME vha. links eller forms, bliver alle indtastede data fra siden sendt tilbage til hackeren i den usynlige IFRAME.

Hackeren kan load mere JavaScript i den synlige IFRAME fra sin web-server, og på den måde får hackeren alle de informationer, som brugeren indtaster på web-siden hver gang der navigeres på siden.

IFRAMEN er skabt, så den fylder hele skærbilledet i browseren. Derved kan brugeren på ingen måde se, hvad der foregår på den bagvedliggende side og kan derfor ikke have den fjerneste anelse eller mistanke om, at der er andre sider end den synlige, som er aktive.



Figur 1: Visualisering af SWXSS

4. Hvem skal være opmærksom?

Det er både på ledelsesniveau og hos web-udviklerne, at der skal være fokus på problemstillingen og awareness om SWXSS. På ledelsesniveau skal der være awareness omkring hackerteknikken, så der kan udvikles retningslinjer og procedurer for, hvordan man skal håndtere sikkerheden omkring web-applikationer.

Web-udvikleren skal rent praktisk være opmærksom på SWXSS og XSS, da overholdelsen af retningslinjerne for sikkerheden ligger hos udviklerne, og det er afgørende, at de har en teknisk sikkerhedsforståelse.

5. Hvordan beskytter du dig mod SWXSS-angreb?

Det er kun muligt at blive angrebet af SWXSS, hvis web-applikationen allerede har en XSS-sårbarhed, så derfor kan SWXSS afhjælpes på samme måde som XSS. For at skabe det bedste forsvar anbefaler jeg, at man i alt sætter 3 forsvarslinjer op, for på den måde at have det bedste forsvar. SWXSS skal betragtes som en mere alvorlig udgave af XSS med større konsekvenser end det gennemsnitlige XSS-angreb.

De tre forsvarslinjer kan deles op i:

- Input validation
- Output validation
- Frame killing

Input validation

Input validation er en af de bedste og vigtigste metoder, man skal bruge til at beskytte sine web-applikationer mod en række sikkerhedstrusler, inklusiv XSS, SQL injection osv. Der er utallige måder at gøre dette med forskellige resultater til følge. Den bedste måde er at benytte en Positive List, hvor det kun er det forventede input, som tillades at passere. Det er desværre ikke altid muligt at vide, hvad valide input er, og det kan derfor være nødvendigt at bruge en Negative List. Det gøres nemmest ved at filtrere for kendte illegale karakterer og kombinationer.

Output validation

Output validation skal betragtes som det andet forsvar mod XSS- og SWXSS-angreb. Det kan anbefales, at input validation altid suppleres med output validation. Det er nødvendigt af den grund, at input validation kan indeholde fejl, eller at hackeren har fundet en metode til at narre input validations-mekanismerne. Hvis det skulle være tilfældet, er det godt i hvert fald at have et mere forsvar at falde tilbage på.

Output validation bliver brugt til at sikre, at outputtet fra web-applikationen aldrig indeholder karakterer, der kan generere valide tags. Det vil sige HTML, XML osv.

Ønsker du mere information om output validation kan du finde flere oplysninger ved at læse på OWASPs hjemmeside. www.owasp.org

Frame killing

Da SWXSS er mere alvorlig end det gennemsnitlige XSS-angreb, anbefaler jeg yderligere et tredje og sidste forsvar; frame killing.

Frame killing er en teknik, hvor man på sit website kan kontrollere, om siden også bliver vist i en frame eller en IFRAME på en anden usynlig side. Hvis siden er vist i en frame eller en IFRAME, vil et stykke JavaScript kode kunne navigere brugeren hen på den rigtige side, så den bliver vist direkte i stedet for at blive vist via en frame eller en IFRAME.

Det er vigtigt, at første og andet forsvar fungerer optimalt, for hvis det ender med at falde tilbage på frame killing, er der højst sandsynlig andre seriøse sårbarheder på webapplikationen. Frame killing er ikke et sikkerhedsforsvar i klasse med input og output validation, det er mere en teknik til at sikre sig mod, at ens website ikke bliver vist gennem en frame eller IFRAME på andre sider.

6. Muligt at opdage et SWXSS-angreb

Som bruger er der mulighed for at opdage, hvis man er udsat for et SWXSS-angreb. Men det kræver en del teknisk indsigt, som den almindelige bruger ikke kan forventes at have. Her er nogle eksempler på, hvordan man som bruger vil kunne opdage et SWXSS-angreb.

- Hvis brugeren anvender Firefox, er der en mulighed for at opdage et angreb, hvis der er mere end den synlige side. Firefox viser en menu-option, der siger 'This Frame'. Hvis brugeren højre-klikker på browserens dokument, vil brugeren få oplysning om, at der er flere aktive frames. Der vil dog være mange falske positive, da der er mange web-sider, som anvender frames, som vil skabe denne menu-option, selvom der ikke er tale om et SWXSS-angreb.
- Hvis brugeren anvender Internet Explorer, vil det ikke give de samme informationer. Her vil brugeren blot få den normale menu-option; 'View Source'.

7. Sådan beskyttes web-applikationerne

Hvis man som it-ansvarlig leder eller web-udvikler vil beskytte sine web-applikationer bedst muligt imod SWXSS og XSS, vil jeg anbefale, at I sørger for at få udviklet en politik med anvendelse af best practice for udvikling af web-applikationer. I politikken skal følgende punkter være inkluderet:

- Få udviklet retningslinjer og procedurer for de tre forsvarslinjer: Input validation, output validation og frame killing.
- Lav en intern QA ved udvikling af web-applikationer. Det skal være en fast rutine, at få en kollega til at verificere den nyudviklede kode, inden den tages i brug.
- Sørg for, at der bliver lavet en sikkerhedstest af virksomhedens web-applikationer med et fast interval alt efter den enkelte virksomheds behov, og når der sker større ændringer i web-applikationen.
- Husk løbende at opdatere sikkerhedspolitikkerne efter tidens standarder.

8. Nyttige links

<http://ha.ckers.org/xss.html>

<http://www.owasp.org>

Denne artikel er publiceret i Børsens ledeshåndbog om it-sikkerhed og bringes her efter tilladelse fra Børsens Ledeshåndbøger.

5. Sikkerhedskonsulent i FortConsult opnår guldcertificering i trådløs sikkerhed

FortConsult sørger løbende for at videreudvikle sin ekspertise inden for it-sikkerhed og opbygge kompetencer på nye, aktuelle områder. Et af vores fokusområder i øjeblikket er trådløs sikkerhed, og vi glæder os over, at en af vores sikkerhedseksperter har opnået en guldcertificering i trådløs sikkerhed.

Som et led i FortConsults satsning på nye teknologiske områder, hvoraf trådløs sikkerhed er et af dem, sørger vi for løbende at uddanne vores sikkerhedskonsulenter i de nyeste teknologier, inklusive hvordan man bedst sikrer dem. Ønsket om at være i front har senest resulteret i, at Warren Platt, der til daglig arbejder som sikkerhedskonsulent i FortConsult, har opnået en GAWN guldcertificering. GAWN står for GIAC Assessing Wireless Networks og er en GIAC-certificering.

En af verden bedste

Warren Platt er en af de seks, der ud af i alt 373 personer på verdensplan, har opnået guldcertificering inden for trådløs sikkerhed. Certificeringen består af to dele, hvor Warren opnåede en gennemsnitsscore på 90 %. Den første del er en online test, og på den baggrund blev Warren udvalgt som mentor og underviser af SANS Institute til deres kursus i trådløs sikkerhed. Den anden del er et white paper, som er blevet godkendt af SANS Institute.

På forkant med sikkerheden

Det white paper, som udløste guldcertificeringen, omhandler både eksisterende sikkerhedstrusler inden for trådløs sikkerhed så vel som nye sikkerhedstrusler, som er lige rundt om hjørnet. I takt med at virksomheder bliver bedre til at beskytte deres trådløse netværk, opstår der nemlig mere

avancerede hackermetoder, og derfor er det vigtigt hele tiden at være på forkant og tage de allernyeste sikkerhedstrusler med i betragtning.

White paperet beskriver, hvordan man kan forebygge hackernes nye angrebsmetoder og dermed være på forkant med sikkerheden inden for it-sikkerhed. Warren, som til dagligt rådgiver og udfører sikkerhedstest for FortConsults kunder og har mere end 8 års erfaring inden for it-sikkerhed, understreger at de nye angrebsmetoder, som hackerne bruger, ikke kun gælder på det trådløse område, men at de også kan benyttes til traditionelle angreb via internettet.

Hvis du vil vide mere

Hvis du er interesseret i at læse Warrens white paper: "[Wireless at the hospital and the threats they face](#)" kan du downloade det fra vores hjemmeside www.fortconsult.net. Hvis du har spørgsmål eller ønsker mere information om trådløs sikkerhed i det hele taget, er du velkommen til at kontakte Warren Platt ved at skrive en mail til: wp@fortconsult.net

6. Nyansatte i FortConsult

FortConsult A/S har ansat to nye medarbejdere. Det er Senior Security Consultant Tom Van de Wiele og Key Account Manager Henning Bahl Larsen.

Tom Van de Wiele er 28 år og har arbejdet med it-sikkerhed i mere end 7 år. Han kommer fra en stilling som Senior Information Security Consultant hos Verizon Business / Cybertrust. Igennem Toms karriere har han opnået stor erfaring inden for sikkerhedstest, forensic analysis, risk assessment og Scada. Tom er oprindelig fra Belgien, men er nu flyttet til København for at blive en del af FortConsults team af it-sikkerhedskonsulenter.

Henning Bahl Larsen er 57 år og har arbejdet inden for it og it-sikkerhed i mere end 20 år. Han har senest været selvstændig og ejet it-sikkerhedsfirmaet Change Master. Som selvstændig har Henning bl.a. arbejdet med it-beredskabsplaner, it-sikkerhedspolitikker, backup og compliance-løsninger for danske og udenlandske kunder. Henning er en del af FortConsults team af Key Account Managere og skal bidrage til FortConsults fortsatte vækst.

Vi er meget glade for, at både Tom og Henning har sluttet sig til os, og de er begge allerede godt i gang med at servicere vores kunder.

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