TEKNOLOGI-RÅDET

Idékatalog med rådata fra workshop om IT-sikkerhed

Arrangeret af Teknologirådet

19. april 2006

Forord

Dette idékatalog er resultatet af en workshop afholdt af Teknologirådet den 19. april 2006, hvor en bred kreds af aktører indenfor IT-sikkerhed identificerede de største IT-sikkerhedsmæssige problemer i Danmark. De 35 deltagere har også peget på løsningsforslag og på hvem, der kan løse problemerne. Der er ikke tale om færdige og gennemarbejdede resultater, men om forskellige idéer, forslag, kommentarer til og diskussioner af den nuværende it-sikkerhedssituation i Danmark.
Workshoppen forløb som en kombination af brainstorm, gruppearbejde og afstemninger - og deltagerne arbejdede en del af tiden på bærbare PC'er i systemet "GroupSystems". Det gav dem mulighed for anonymt at bidrage med egne ideer og for at kommentere andres. Alle input samt afstemningsresultaterne er dokumenteret uredigeret i dette idékatalog. Det betyder, at evt. sproglige ukorrektheder og faktuelle fejl ikke er rettet og at de enkelte deltagere ikke hver især kan tages til indtægt for alle udsagn i kataloget. Der er tale om ubearbejdede rådata, der kan tjene som inspiration for fremtidige initiativer på IT-sikkerhedsområdet i Danmark.

Workshoppen faldt i tre overordnede blokke:

1) Fase 1: En brainstorm i plenum hvor alle deltagere kom med deres bud på forskellige it-sikkerhedsmæssige problemer, og placerede dem i 6 hovedkategorier, der på forhånd var defineret af arrangørerne. Brainstormen sluttede med en afstemning

2) Fase 2: Gruppearbejde, hvor deltagerne arbejde med løsningsforslag til de højest prioriterede problemer. Alle deltagere fik efterfølgende mulighed for at komme med løsningsforslag til alle de problemer, der blev identificeret i fase 1

3) Fase 3: Uafhængigt af arbejdet i Fase 1 og 2 kom hver gruppe med deres bud på dét initiativ, der bedst kan fremme IT-sikkerheden i Danmark. Deltagerne fordelte afslutningsvis deres stemmer mellem de 7 initiativer.

Teknologirådet
April 2006

Workshoppen blev faciliteret af Lars Ginnerup, LG Facilitation og Christian Høy-Petersen, Ementor Consulting

Indhold

Fase 1: Brainstorming og prioritering af problemer **4**

Prioritering af problemerne **37**

Fase 2: Bearbejdning af de højest prioriterede problemer i hver kategori **42**

Fase 3: Hvad er vigtigst at gå i gang med NU? **66**

Evaluering af workshoppen **68**

Program **71**

Deltagerliste **72**

Fase 1: Brainstorming og prioritering af problemer

Følgende er resultatet af den indledende brainstorm, hvor deltagerne indtastede deres bud på de væsentligste IT-sikkerhedsproblemer under 6 hovedkategorier, der på forhånd var defineret af arrangørerne. Hvert problem har en hovedoverskrift, hvorunder såvel den oprindelige forfatter som de øvrige deltagere har haft mulighed for at kommentere og uddybe problemstillingen. Problemerne præsenteres her i den rækkefølge, der blev resultatet af den efterfølgende afstemning. Det skal bemærkes, at flere af hovedoverskrifterne – og især kommentarerne - har karakter af løsningsforslag, selvom der i denne fase af workshoppen hovedsageligt blev arbejdet med problemformuleringer. En oversigt over samtlige identificerede problemer kan ses under overskriften "Prioritering af problemerne" på side 34.

1. Regulering og standarder

1.1 Standardisering af it-sikkerhed på tværs af samfundet

For at kunne vurdere it-sikkerhedsniveauet på tværs af organisationer og ikke mindst i forholdet til samarbejdspartnere er det vigtigt at tale samme "sprog" dvs. anvende samme eller sammenlignelige standarder i beskrivelse af it-sikkerhed.

Det statslige system har påbegyndt dette ved at kræve at alle statslige institutioner anvender samme standard for it-sikkerhedsprocesser, DS484:2005.

Denne version er direkte sammenlignelig med ISO17799:2005.

En form for certificering kan være nødvendig hvis roller skal kunne bæres fra et IT-miljø til et andet. F.eks. sygehusdata der skal accesses af en kommunal sygeplejerske.

DS484:2005 bør være et krav for samtlige offentlige myndigheder.

Standarder skal være enkle og forståelige for menigmand ellers henvises til en fælles ubekendt referenceramme

Der mangler et niveauopdelt sæt spilleregler. Der bør kunne kræves væsentligt mere af professionelle brugere end af privatpersoner (som til gengæld har brug for mere hjælp).

Kort! DS484 bør erstattes med ISO27001 da vi i en globaliseret verden ikke kan få nok effekt af en lokal dansk efterligning af en international sikkerhedsstandard.

1.2 ISP´erne gør ikke nok for sikkerheden

ISP´erne har i dag gjort meget for at dæmme op for spamproblemet. Men stort set alle andre områder er goldt land.

"Almindelige mennesker" har ingen reel chance for at sætte sig ind i sikkerhed i forbindelse med deres internetforbindelser. De fleste i dag ved, at de bør have et antivirus-program og en firewall. Men de færreste kan finde ud af at konfigurere og opdatere disse. ISP´erne gør meget lidt for at afhjælpe dette problem - og når de gør, er det i form af dyre tilkøbspakker. Dette på trods af, at den manglende sikkerhed ofte går ud over mange andre abonnenter hos samme ISP.

Ofte bliver hele ip-ranges spærret i andre netværk pga. bot-nets o.lign. (medfører fx spam fra ip-adresser). Dette betyder at helt legitim kommunikation fra helt uskyldige firmaer og private spærres pga. andres problemer.

Der findes ingen mærkningsordninger eller standarder for ISP´ernes sikkerhedsniveau.

Man kan sætte krav til at ISP'er rettet mod private (eller alle ISP'er?) altid har mindst en sikkerhedsløsning. Det kunne være en filtreret forbindelse med e-mail via ISP'ens mail server - de store ISP'er har denne løsning og det skulle være et

valg man foretager når man køber en forbindelse, gerne med sikkerhedspakken som standardløsningen. NB: det er ikke en opfordring til generel filtrering af internetforbindelser - men et specifikt produkt, der kan vælges fra

ISP'erne ejer netværket og linierne - det er ikke deres ansvar at sikre systemerne i enderne.

Kunderne erkender ikke at udstyr, der skal på Internettet, skal hærdes - først

Alle og enhver kan nedsætte sig som ISP eller webhotel, og det gør at prisen på disse services ofte bliver den største konkurrenceparameter, fordi de dårligste ISP/webhoteller sælger "for billigt" - blandt andet fordi de ignorerer sikkerhed.

Der er forskel på situationen med privatpersoners og professionelles brug af Internettet. De professionelle brugere bør selv kunne klare en del af de sikkerhedsmæssige risici, hvorimod privatbrugerne har behov for at kunne få bistand fra bl.a. ISP'ere - og gerne som default.

Hvem skal betegnes som ISPér?

der er tre parter der har et ansvar: isp'ere, sw-producenter, og brugere. (brugere inkluderer private og virksomheder/stat/region/kommune

Kodeks for ISPer bør udbygges

ISP'er bør tilbyde kunder en filtrering så de kan få adgang til enten dele af Internettet eller bestemte typer www sites (horisontalt eller vertikalt)

1.3 · Mangel på politisk fokus

Internettet er anarkistisk og ikke tilstrækkeligt politisk reguleret. Der mangler politisk fokus og ansvar for it-sikkerhed.

Hvad er den politiske løsning? Der er masser af politisk fokus men afmagt ift. at overskue, hvad der skal gøres

IT-sikkerhed bør være den enkeltes ansvar

Det er ikke nok at individualisere problemet - derved har mna givet op.

Anarkisme er ok men udbyderne skal enten underlægges eget kodeks eller rammekrav

IT-sikkerhed skal deles op i Content providers og ISP'er

Politisk styring giver flere problemer end de løser Det bliver en ørkesløs privacy-debat

1.4 Kontrollerbar sikkerhed skal indgå som et krav i offentlige udbud af kritisk national infrastruktur

I forbindelse med privatisering af infrastruktur så som el, tele og vand har der været fokus på at sikre konkurrence mellem udbydere. Konsekvensen har været, at sikkerhed naturligt ikke alle steder er vægtet tilstrækkeligt på trods af at samfundet er afhængig af tjenesterne.

Et eksempel herpå er teleselskabernes GSM netværk, hvor der f.eks. ikke er stillet krav til continuety i forbindelse med uddeling af licenser.

Ved udlicitering bør det offentlige derfor stille målbare krav til sikkerheden. Krav der er målbare og kan verificeres af 3. part.

Er det en løsning "blot" at kræve ds484 eller iso27001 certificering af leverandører?

Der skal arbejdes på en praktisk løsning for kontrollerbarhed, ellers ender det som det tidligere Registertilsyn med anmeldelsesordninger, som ikke giver sikkerhed men kun administrativt bøvl.

Hmm, det kan vel være lige så slemt når det er offentligt styret.

På samme måde som Finanstilsynet kræver af banker, at andre end banken selv skal sige god for regnskabet, er det vel ikke urimeligt at bede om, at andre end virksomheden selv vurderer sikkerheden op mod en standard.

1.5 Tryghed for borgeren i tilfælde af misbrug af dennes digitale signatur (el. andet digitalt identifikationsmiddel)

Vejen til at sikre at "digitaliseringen" virkelig får udbredelse er:

1) at der er gode digitale service-ydelser at hente på nettet.

2) at borgeren føler sig tryg ved at bruge disse.

Så længe ydelserne er upersonlige og uden mulighed for tab for brugeren er der ikke noget problem.

Men hvis borgeren risikerer

- tab af fortrolighed omkring sine væsentlige personlige data

- tab ifm. misbrug af identifikationsmiddel

- tab ifm. identitetstyveri (evt. udenfor den digitale verden) baseret på lækkede informationer i den digitale verden.

så forbliver en stor brøkdel af befolkningen utrygge og tager ikke del i digitaliseringen.

Løsning: Gode sikkerhedsforanstaltninger PLUS tryghedsskabende lovgivning

Eksisterernde løsning via OCES er utilstrækkelig og kan ikke i privat-regi konkurrere med finansverdenens net-ID, som benyttes af flere millioner danskere.

Det er til skade for borgernes sikkerhed m.v. at der ikke er etableret een løsning på området. Offentlige institutioner kræver brug af OCES, og finansverdenen kræver brug af net-ID. Hvad i alverden skal borgerne vælge!

1.6 Balance mellem effektiv offentlig administration og borgerens retsikkerhed eller tryghed ved det offentliges behandling af personlige data

Persondata-loven skal naturligvis overholdes, men hvordan opnår borgeren en følelse af tryghed for at det faktisk sker.

Borgeren kan i kraft af sin digitale signatur få både adgang til og ansvar for korretheden af egne data, som opbevares i det offentlige.

Data, som det offentlige er ibesiddelse af om den enkelte borger, bør kunne bruges "frit men under ansvar" af hele den offentlige forvaltning.

Man data må naturligvis kun anvendes til legitime formål.

Er et af virkemidlerne til at gøre borgeren tryg, at der er klare sanktioner, som faktisk tages i anvendelse, hvis medarbejdere i det offentlige misbruger persondata

Det varer ganske afgjort længe før den fornødne sikkerhed for at data bruges korrekt og kun til specifikke formål kommer på plads. Det forudsætter en hel anden holdning til sikkerhed.

De fleste borgere har ikke en jordisk chance for at vurdere / tjekke om deres data misbruges

Datatilsynet, som har til opgave at føre tilsyn med persondataloven, har meget begrænsede ressourcer

...og indsigt i praktiske løsninger!

Når man

Når det offentlige laver kontrolkørsler og "fanger" nogle der har opnået illegale fordele af en eller anden ordning så er det godt. Det viser det offentlige som en effektiv størrelse der holder orden på borgernes skattepenge. Men det siger næsten sig selv, at hver gang man laver en kontrol, så er der nogle uskyldige der bliver kontrollerede. Spørgsmålet er i høj grad hvad der er "ligitime formål". Hvis kontrollerer og fanger nogle, så er det ligitimt, men hvis vi kontrollerer og ikke fanger nogen, så er de illigitimt?

Der kunne være en data ansvarlig udvnævnt på hver virksomhed / offentlig institution -> tilsyn og information

Persondataloven er en lov der tjener sit eget formål. Borgerne skal have ret over sine egne data. JF Biblioteksagen hvor meddelelser om bøger til afhentning pludselig er et "kæmpe" problem.

Der er et utal af skræmmehistorier om, hvorledes den offentlige forvaltning sjusker med sikkerheden og brugen af persondata. Her skal sanktioner ind !

Borgernes retssikkerhed skal sikres i takt med de nye teknologiske muligheder/nedbrydningen af de "data siloerne"

Men hvordan gøres dette?

Så længe økonomier vægter højere i det offentliges løsninger, end sikkerhed og beskyttelse af borgerne, så bliver der ikke beskyttelse agf borgerne.

Løsningerne findes, men spares væk i udbudene.

Store krav til IT Sikkerheds hos det offentlige vil være med til at skabe vækst i DK, på sammen måde som vindmøller på energiområdet skabte nye industrier og vækst.

1.7 Fællesoffentlige standarder og politikker på tværs af organsisationer

Hvis digital forvaltning skal give mening skal data udveksles på tværs af institutioner/organisationer. Hvis der ikke sker en koordinering af sikkerhedspolitikker og -procedurer, skal der udvikles et virvar af bilaterale aftaler mht. politikker for udveksling af data.

Derfor er der brug for en central koordinering af brugerstyring, -adgang og sikkerhedspolitik på tvær af den offentlige sektor.

Enig men det kræver et politisk fokus som ikke findes og næppe kommer i nær fremtid. Det er ikke nok med sikerhedsråd, -paneler mv. og en sjat penge på 10 mio. Alle rapporterne ender som hyldesucceser og bliver hurtigt forældede.

Offentlige og private skal i højere grad ses som en helhed.

1.8 Lovgivning om ansvar i forbindelse med manglende IT-sikkerhed

Dette vil svare til regler om beskyttelse mod smittespredning og miljøpåvirkning.

Nemlig, manglende IT-sikkerhed medfører ofte betydelige økonomiske eksternaliteter, som således påfører udenforstående udgifter, som de ikke kompenseres for. Aktørerne bør derfor gennem lovgivning gives incitamenter til at tænke disse eksternaliteter med i deres beregninger for, om en given aktivitet skal gennemføres. Den store udfordring er selvsagt at finde ud, hvorledes en sådan lovgivning skal formuleres for at virke efter hensigten. Det har man imidlertid kunne klare på andre områder, så det må også kunne lade sig gøre indenfor IT. Der burde i Danmark forskes, arbejdes og eksperimenteres mere med sådan lovgivning.

Der bygges i dag i vid udstrækning på den regeldannelse, som fremkommer i forbindelse med sagsafgørelser ved domstolene. Det er for trægt. Og i øvrigt er der forskel på afgørelser ved hhv. Vestre og Østre Landsret.

Det skaber usikkerhed for såvel borgere som virksomheder/det offentlige.

1.9 Behov for en langt stærkere tilstedeværelse af danske normer og bidrag til standardisering

Her er det vigtigt at det offentlige ikke definerer egne standarder, men følger Standardiseringsorganernes anbefalinger.

Vi får alt for nemt en "lokal" dansk sikkerhedsløsning.

Globaliseringen medfører krav om fælles standarder. Man kender ikke DS484 i udlandet selvom den er kompatibel.

Det burde stå klart, at danske standarder kun er en nødløsning dersom der ikke findes internationale standarder. Krav om at standarder altid skal være åbne og internationale.

1.10 Offentlige IT-indkøb bør tilstræbe fælles åbne standarder men ellers modarbejde monokultur indenfor kode og platforme

Det er helt enkelt uforsvarligt, at en virksomheds, en offentlig institutions eller hele den danske IT infrastruktur er bygget op omkring lukket kode, der ejes af en enkel stor udenlandsk virksomhed. Det er uhensigtsmæssigt fra en økonomisk vinkel, idet monopoler altid tager højere priser etc., og det er farligt ud fra en sikkerhedsmæssig synsvinkel, idet lukkede, enstrengede systemer er betydeligt mere sårbare end mangfoldige og åbne systemer.

"monokultur" kan være et problem men der er ikke enighed om, at open source giver bedre sikkerhed eller er billigere i drift.

1.11 Lovgivningen skal sikre distribution af kontrol og risiko

Lovgivningen i dag koncentrerer risiko og skaber kontrol og overvågning uden sikkerhed.

De kriminelle kan ALT hvad Staten kan.

Det er nemmere at skabe regler for professionelle (virksomheder og offentlige institutioner). Men for private brugere (borgerne) er det en mangelvare at have "noget ordentligt" at læne sig op af.

1.12 Opret et egentligt Internet Politi

Overvågning og aktioner sker alt for sporadisk (case styret) frem for efter en egentlig plan.

Der er behov for et Net Politi med beføjelser til at lukke servere og forbindelser med øjebliks varsel.

Vi skal passe på her!!! BSA har jo allerede fået etableret et "privat politikorps" (Antipiratgruppen), som kan trænge ind - selv hos borgerne. Det er ikke fremmende for et vidensamfund!

Men et korps i offentligt regi, som har klare spilleregler og er under offentligt opsyn mangler.

Lande og organisationer der ikke følger spillereglerne skal kunne lukkes ude så alm. brugere beskyttes mest muligt mod de lovløses hærgen.

Man skal ikke flytte magten til politiet - det giver en meget stor retsusikkerhed. Noget andet er at specialuddannet politi er nødvendigt.

Enig i "mere specialuddannet politi". Brug pengene på det i stedet for den dyre nyttesløse terror-logning

Det er måske et godt forslag - hvis man kunne afgøre kriterierne for lukning ...

Bits of freedom i Holland oprettede nogle falske sider med noget frit materiale, skrevet af en hollandsk forfatter og så gammelt at det frit måtte kopieres.

Derefter bad de fra falske adresser, hotmail adresse om at materialet blev fjernet

Det lykkedes ofte at få ISP'er til at fjerne selv indlysende frit materiale - så hvad med diskutabelt materiale?

1.13 Internationale krav

I USA har SOX-lovgivningen øget fokus på risici.

I EU har man via det "moderniserede" 8. selskabsdirektiv sat fokus på revisorerne og stillet krav. Men der er ikke kommet andet end 2 hensigtserklæringen omkring Corporate Governance (de er allerede indarbejdet i det danske regelsæt for børsnoterede virksomheder).

Der mangler europæisk fokus på området vedrørende risici - og det lider vi nok lidt under.

1.14 Terrorpakken skaber kriminalitet

Det er et grundliggende problem af Terrorpakkens krav om aflytning (bagdøre) og konstant identifkikation ikke indeholder nogen holdbar sikkerhedsforståelse

a) De kriminelle kan altid beskytte deres kommunikation og arbejder nu trådløst for helt at omgå centrale infrastruktur

b) Bagdøre og usikrede logdata skaber nye angrebspunkter for kommercielle og kriminelle tiltag.

c) krav om Identifikation skaber identitetstyveri

d) Reglerne forhindrer nødvendige sikkerhedstiltag for at sikre kommercielle transaktioner og digital forvaltning

Helt enig og ideen med at lave lovgivning for terror som en specificeret kriminalitet er ikke god. Hvad er terror? Nogle generelle regler der giver mulighed for at opklare og forhindre kriminalitet - herunder it-kriminalitet - er mere hensigtsmæssigt

1.15 · Man går og opfinder den dybe tallerken

Der mangler fælles retningslinjer og standarder for it-sikkerhed.

Der findes en overflod af IT-sikkerhedsstandarder også danske i form af DS484 m.fl.

Der mangler standarder som kan anvendes af små og mellemstore firmaer. DS484 er for kompliceret og for krævende

DS484 er for national. Internationale standarder bør fremmes så man ikke genopfinder internationale standarder i national regi

Muhammed-krisen har klart vist, at Danmark ikke bør benytte "landsby"-betragtninger men bør fokusere mere internationalt. Så enig i, at vi skal orientere os i retning mod internationale standarder!

Internationale retningslinjer må ikke bære præg af nypuritanske holdninger, men primært fokusere på tilgængelighed og værn mod uønsket trafik.

1.16 Standardiseret it-sikkerhed i private virksomheder går trægt

it-sikkerhed er ikke absolut, og behov synes meget individuelt. det er svært for mange at indføre fx ds484

Behov for en letvægtsudgave som er rettet mod private virksomheder. AWARENESS

samme situation i offentlige virksomheder

I både offentlige og private virksomheder bør IT-sikkerhed awareness opprioriteres, derved vil borgerne, som jo er ansatte blive opdateret til også at kunne magte it-sikkerheden i hjemmet

Utilstrækkelig uddannelse øger behovet for standardisering. Imidlertid findes allerede gode standarder - men ikke nok markedsføring.

IT-sikkerhed skal starte i grundskolen. Det er en kulturholdning der skal til.

1.17 Sikkerhed - modent problem?

IT-sikkerhed starter og stopper ikke med IT. Det første spørgsmål er derfor hvordan vi afgrænser problematikken uden at udelukke væsentlige faktorer. Dernæst er vi nødt til at tænke i hvilke kilder der er til IT ikke-sikkerhed samt hvad der er risikoskabende design, systemløsninger, etc..... og adfærd.

Endvidere er det et spørgsmål hvilke sikkerhedsproblemer der er "modne" i betydningen veldefinerede, velbeskrevne og med velkendte metoder til beskyttelse. Dette spørgsmål skal ses i lyset af hvad der er "stabiliseret" således at der er eller kan opnås et sikkerhedsniveau som kan beskrives. Sikkerhedsniveau er et udtryk for en skala af risiko faktorer er kendte og løsninger findes, hvorfor problemet er hvilket trade-off der er mellem risikominimering og omkostninger ved forholdsregler.

IT sikkerhed skal angribes som et spørgsmål om såvel modenheden af et sikkerhedsproblem i betydningen dets stabilitets og løsningsmuligheder, som et spørgsmål om sikkerhedsniveau idet den ultimative "100% sikkerhed" er et farligt ideal at arbejde med - total kontrol kan slå tilbage og blive til en større sikkerhedsrisiko, hvis det utænkelige alligevel sker og eet svigt optræder og dermed risikerer hele systemets sikkerhed.

Hvis ikke 100% sikkerhed så må man arbejde med "begrænset sikkerhed" såvel hvad angår sikkerhedsniveau men også hvad angår sikkerhedsomfang.

Sidstnævnte er et spørgsmål om containment, om at kunne fastholde en problematik indenfor nogle systemer, dvs. sikre at et sikkerhedsproblem forbliver "lokalt".

Modenhed af et problem skal inddrages før fastsættelse af standarder for løsningsrammen. Modenhed og stabilitet følges ad således at reproducerbarhed og andre egenskaber muliggør en systematisk problembearbejdning som grundlag for opstilling af reguleringer.

Sikkerhed skal tænkes ind i løsninger ikke som add on. Vi er ikke kommet ret langt de sidste 25 år.

IT sikkerhed til forskel fra almen sikkerhed skal lægge vægt på dets dynamiske karakter der udspringer af digitalisering og digitale teknologiers "virale" egenskaber. Sikkerhed på IT området er i høj grad problemet om "spredningsfaktoren" og "acceleratorfaktoren" som hver for sig gør et uinddæmmet sikkerhedsproblem uoverskueligt i sine konsekvenser.

IT sikkerhed handler derfor i særdeleshed om "containment" - altså at designe og udvikle systemer og netværk hvor der er indbygget omfattende "containment".

Modenhed af IT sikkerhed er derfor meget nært knyttet til i hvilken grad der er skabt "containment" som forhindrer og begrænser de digitale teknologiers virale egenskaber.

Tidshorisonten i modenhed af IT sikkerhed er ikke kun et spørgsmål om at lade en teknologi modnes - det er også at udnytte vidne om sikkerhedsproblemer til at udforme - proaktivt - såvel proces som produktstandarder der kan give grundlag for certificering af applikationer således at slutbruger har et markedssignal for hvilke applikationer der lever op til hvilke sikkerhedsniveau og kan vælge et produkt svarende til det ønskede (relevante) sikkerhedsniveau.

Ligesom vi har kørekort til bil kunne der indføres kørekort til udarbejdelse af applikationer der har interface til internettet etc.

Effekten af en certificeringsmulighed for applikationer og anden software vil give den mindre kyndige slutbruger et værktøj i hånden uden selv at skulle være ekspert.

Sikkerhedsstandarder burde behandles på samme måde som andre sikkerhedsstandarder - fx kan man tænke i en sikkerhedsorganisation i alle virksomheder og organisationer med mere end x ansatte skal afholde sikkerhedskurser for at påvirke slutbrugeres risikoadfærd ved at lære slutbruger om hvad der er sikkerhedsrisici i deres brug af IT. En årlig "øvelse" - et fingeret angreb udefra, en kriminel handling indefra fra en medarbejders side, etc. kan danne grundlag for en "realistisk" test af organisationens beredskab samt træning af medarbejdere ved at gennemarbejde erfaringen fra øvelsen.

Omkostninger til en sådan sikkerhedsøvelse skulle være et pålæg (regulering) efter revisorinspektion eller revisorpåtegning, opfølgning på tidligere problemer, etc. Kort sagt er sikkerhed ikke et individuelt problem alene men en kollektiv risiko som skal håndteres med en blanding af såvel kollektive, organisatoriske som personrettede tiltag.

Virksomhedsorienterede certificeringer fx ds484 el. tilsvarende, giver værdi. produktcertificeringer fx common criteria, er ikke det papir værd de er skrevet på. det er processen rundt om produktet der vejer tungt

1.18 Internettet skal reguleres FN/ILO

Katastrofe! FN formår ikke at regulere noget der bevæger sig med den hastighed som teknologier bag nettet og forretningsmodeller på nettet bevæger sig med. Skal diverse lande med et ganske begrænset demokrati eller en alternativ demokratiforståelse i forhold til den vestlige være bestemmende for hvordan nettet reguleres over hele verden?

En noget syret betragtning - især set i lyset af den enorme anvendelse af Internettet af både virksomheder, offentlige institutioner og privatpersoner.

Der er tale om grænseoverskridende kommunikation. Vi ønsker vel kun at kunne komme efter "forbryderne" - og ikke skabe et overvågningssamfund.

Spørgsmålet må være, om vi mangler regulering/standarder vedrørende de værktøjer, som benyttes i forbindelse med Internettet - ikke selve nettet.

Internettet skal ikke reguleres. Internettet og dets givne facetter skal beherskes

Man skal ikke regulere noget der ikke er et problem.

Internettet er ikke et særligt retsområde, det er underlagt de samme love som verden i øvrigt.

Men der mangler mulighed for retsforfølgning på tværs af landegrænser (vi er ikke kommet meget videre, selvom det er mange år siden The Cuckoo's Egg så dagens lys).

1.19 Åbne standarder bør indgå i alle offentlige IT-løsninger

Åbne standarder skal kun anvendes hvis det giver mening. Det skal ses i sammenhæng. Support er en væsentlig del af dette.

IT-sikkerhed skal altid være et punkt i offentlige projekter - opfattet bredt.

Der skal spørges ind til IT-sikkerhed i ansættelse, der skal uddannes i IT-sikkerhed, der skal efterspørges IT-sikkerhed når man vælger outsourcing leverandører.

Hvis det altid er med som et specifikt punkt vil det give anledning til spørgsmål og man overvejer det i det mindste.

Så bliver det indimellem et fravalg men andre gange vil man huske det og få gjort noget

IT-sikkerhed mangler i "kravspecifikationer"

1.20 Persondatalovgivningen er forældet

Hvem er det et problem for? Borgerne? Det offentlige?

Alle - fordi det skaber kriminalitet

Vi kan ikke beskytte centrale data - vi er nødt til at antage at kriminelle og andre når helt ned til data.

Samtykke har udvikler sig til afpresning - et valg mellem services uden sikkerhed eller sikkerhed uden service. Dermed skaber samtykke et loose-loose problem.

Digital Forvaltning har så mange undtagelser, at man ikke kan sige at persondataloven begrænser staten.

Persondatalovgivningen er dermed blevet en illusion, der dels bruges som undskyldning for ikke at tænke sikkerhed og samtidig egentlig ekspropriation af borgernes data.

Vend problemstillingen på hovedet og giv borgeren ret til egne data - og pligt at holde dem opdatyeret. Til gengæld må det offentlige overholde krav til beskyttelse af data og til uopfordret at give borgeren en oversigt over brug af hans data med jævne mellemrum.

Formynderiet skal ophøre. jf biblioteksagen hvor kunder ikke ukrypteret må få afhentningsmeddelelser.

1.21 Mangel på lovgivning til bekæmpelse af IT-kriminalitet

Der mangler politiske tiltag til at give mulighed for at efterforske IT-kriminalitet - lettere adgang til oplysninger fra ISPér mv.

Det skal holdes op mod beskyttelse af privatlivets fred og den personlige integritet

1.22 Danmark er alt for dårligt forberedt på kraftigt voksende it-kriminalitet

1.23 Datatilsynet - udbygning - flere ressourcer ?

Med det nuværende personale vil der gå 7 år mellem hvert uanmeldt besøg fra Datatilsynet til en offentlig myndighed. Hvem sagde Fødevarekontrollen?

1.24 Skal der i det hele taget være en standard for it-sikkerhed?

Er it-sikkerhed ikke en del af noget "mere"?

Er it-sikkerhed ikke på lige fod med andre emner i den nuværende standard? Følgende forhold har som fagområde en bredere dækning end it-sikkerhed:

- business continuity

- fysisk sikkerhed

- compliance

- behandling af hændelser

Hvordan styres it-sikkehed på tværs af samarbejdende virksomheder og organisationer, hvor it-anvendelsen sker "på kryds og tværs"? Kan man godtgøre at it-sikkerheden er dækkende og tilstrækkelig, hvis man ser isoleret på én virksomheds tilrettelæggelse?

En minimumsstandard for datasikkerhed i alle offentlige systemer bør være et krav. I den private sektor kan man måske forestille sig de udbyggede kvalitetsmærker også indeholder en højere standard for sikkerhed af køberes/brugeres data.

1.25 IT kriminalitet internt i virksomheden

Undersøgelser peger på at de fleste sikkerhedsbrist skabes af medarbejdere i virksomheder og organisationer (80% er nævnt).

Derfor bør IT sikkerhed sættes på dagsordnen som et økonomisk risikoproblem af betydning for virksomhedens markedsværdi (ser her bort fra ikke børsnoterede virksomheder).

Hvis problemet er et medarbejderproblem kan det ses ud fra kriminologisk forskning, hvor der lægges vægt på at (IT) kriminalitet opstår som følge af en række beslutninger og for hver af disse er der en mulighed for at gribe ind, tilrettelægge forebyggelse etc. hvis man forstår disse processer. Hvis IT kriminalitet skal bekæmpes skal vi derfor koble kriminalitetsviden til IT og omvendt!

1.26 Mindre firmaer skal hjælpes til at klare it-sikkerheden

Mindre firmaer har ikke en chance for at klare alle it-sikkerhedsproblemerne selv hvis de ønsker at udnyttet den nyeste teknologi.

Krav fra det offentlige sammen med støtte til eks. at outsource de fleste it-sikkerhedsopgaver.

1.27 · For milde straffe

Vi straffer ikke IT-kriminelle hårdt nok.

Det afhænger af, hvad der menes med it-kriminelle.

Et problem har været accepten af it-kriminialitet og ikke så meget straffene. Men hvis man selv med en straf kan få et godt job som sikkerhedschef, så blåstempler man kriminaliteten. Det kan næsten ingen straffe hamle op med.

Der mangler definition på "IT-krimminelle"; om it er midlet eller målet

internationalt set har der været flere domme i de seneste par år

IT kriminelle er en misvisende terminologi. Vi taler jo heller ikke om telefon kriminelle eller tændstik kriminelle (brandpåsættere)

Straffen i dag for f.eks. ophavsretlige krænkelser på Internet, der også falder under betegnelsen IT-kriminalitet, er alt for drakonisk. En person på 15 år, der foretager ulovlige kopieringer af musikfiler, straffes hårdere økonomisk etc. end en tyveknægt, der stjæler et fjernsyn fra en butik.

Helt enig - det er helt ude af propotioner. Både den strafferetige konsekvens og den økonomiske. Det kan give 6 års fængsel at piratkopiere og politiet kan uden konsekvens gå ind i private hjem og beslaglægge computere, hvis de blot siger, at de mener der er piratkopiering

Når vi har et retssystem, som straffer "hackere" - indbrud i IT-systemer med fodboldtræning (andre sociale eksperimenter) har vi efter min overbevisning for milde domme.

1.28 Manglende lovgivning indenfor tab af data

Der er ingen konsekvens for tab af kunders data, private data. Det betyder at der ikke er et incitament til at beskytte disse tilstrækkeligt. Californien har lovgivning der kræver at personer hvis data er mistet bliver gjort opmærksomme på dette. Det giver en økonomisk byrde for lemfældig omgang med andres data.

Forslag er at alle hvis data er offentligjort/mistet skal informeres indenfor 4 uger, samt at der skal udsendes information (pressemeddelelse) omkring problemet, løsningen og tiltag til at sikre mod lignende hændelser i fremtiden

Situationer relateret til tab af data reguleres almindeligvis via kontraktforhandlinger, fx i forbindelse med outsourcing.

Det er svært at etablere specifikke regler for tab af data uden samtidig at foretage en form for kategorisering. Ikke alle data er lige væsentlige og/eller følsomme.

Men retssager på området har vist behov for en form for regelgivning.

Måske skal det ikke ligefrem være påbudt at udsende pressemeddelelser om sådanne "nedbrud", men der bør i langt højere grad end i dag være åbenhed om sådanne problemer.

Hvis du skal informere kunderne vil det være til din fordel at sende pressemeddelelse ud for at undgå rygter tror jeg :-)

Åbenhed er godt, men det må altid være en individuel vurdering. Principper bør dog udarbejdes.

Man skulle måske heller fokusere på om en given service ikke fungerer tilfredsstillende

1.29 Revision af love indenfor terrorbekæmpelse og logning

De nuværende love er ikke praktisk anvendelige og hæmmer udviklingen. Det vil på langt sigt stoppe udbredelsen af hurtigere forbindelser, vil gøre Danmark til et uland som ikke er attraktivt for virksomheder.

Taler vi om den "nye" terrorbekendtgørelse?

Ja, det var den jeg tænkte på - men hele glidebanen mod en drømmeverden a la minority report filmen.

Utopi for politiet er at de kan finde ud af alt, fordi alt er logget.

I praksis vil det give informationsoverflow og intet reelt vil blive opdaget.

Problemet er, at man laver høstakken større, men så er nålen netop ikke nemmere at finde.

Start med at finde metoder til at finde nåle, før man prøver at finde den i den største høstak.

Terrorbekæmpelse skal hænge sammen med mål og midler.

Wassenaar (begrænsning af udførelse af kryptosoftware) var en skandale. Kryptering kan altid skaffes af kriminelle.

Regler for Identity resolution der sikrer godkendelse i Sikkerhedspolitisk Udvalg - så det ikke benyttes til andre formål end netop terrorbeskyttelse og -forebyggelse bør være en del af terrorpakken.

1.30 Behov for et SIKKERT internet parallelt med det USIKRE

Der er behov for et sikkert internet hvor alle servere, applikationer og brugere authentificeres. Et nyt og forbedret net kendetegnet ved kvalitet - kvalitet af identitet af kommunikerende partere - kvalitet af information.

Internettet i dag er det VILDE VESTEN og det er nu på tide at skabe lov og orden. Den nuværende tilstand skaber utryghed og mistillid.

Jeg tror ikke en parallelt internet har nogen vej frem. I stedet bør der satser på at udvikle yderligere sikkerhedsprotokoller til det eksisterende internet.

Internet skal fortsat i sin kerne være "dumt" og "usikkert". Sikkerheden må skabes ude i endepunkterne. Hvis man gør selve netværket for "intelligent" ved for eksempel at ændre ved transportprotokollerne, risikerer vi at få mere ukontrollerbar overvågning, centralisering, ustabiltet etc. En sådan top-down tilgang vil være imod alle andre tendenser i retning af distribueret intelligens og decentralisering indenfor netværk og systemer.

Der vil altid være vilde vesten steder på internet, ligesom det altid er dag, nat og morgen et eller andet sted på internet. Tror det var tyskland der forsøgte at gøre det ulovligt at se porno på internet om dagen - i Tyskland.

Man må erkende at internet er verdensomspændende, og at det formentlig vil opfatte meget "censur" og regulering som en fejl og route udenom.

Det tror ingen på.

1.31 Revision af aftalelovgivning

Virksomheder indgår i dag mange aftaler via e-mail og i fremtiden via VoIP, instant messaging - altså medier uden sikkerhed, sporbarhed eller uafviselighed. Aftalelovgivning skal tage højde for disse nye metoder til aftaleindgåelse og det skal gerne udmøntes i vejledninger til virksomheder, hvordan man sikrer sig bedst muligt.

Såfremt dette ikke udføres vil mange virksomheder stå med tvister omkring aftaler og risikere at komme i problemer. Både som leverandør og aftager.

god ide med vejledninger, men hvorfor er sporbarhed, uafviselighed, sikkerhed dårligere i email, voip, IM i forhold til traditionelle aftale dokumenter?

fordi du let kan forfalske en e-mail og skal du underbygge at du har sendt den skal du have fat i internetudbydere osv. osv. - det er sværere at godtgøre uden signatur.

Jeg bruger selv PGP til at kryptere og signere mails.

Giv mig din e-mail og jeg skal sende dig en ordre på 1000 stykker et eller andet - sendt fra anders@andeby.dk :-)

Problemet har ikke været så stort i praksis - det kan også ske med telefon bestilling eller fax - og sådan set også et brev med en ordreseddel.

Der er ikke behov for lovgivning, men for at hver enkelt virksomhed får klare rutiner for hvorledes bestilling og ordrebekræftelse skal håndteres.

2. Systemudvikling

2.1 · Diffust ansvar

Med Open Source er ansvaret for it-sikkerheden svært at placere.

Ansvaret er generelt også uklart placeret i udviklingssituationer. Ofte er der slet ikke taget stilling til, hvem der er ansvarlig for sikkerhedsforhold.

Behov for såvel kvalitetssikring som klarhed på ønsket/krævet sikkerhedsniveau - under udvikling men lige så vigtigt i vedligeholdelsesfasen.

Vi skal sikre at der stilles krav til leverandørerne omkring sikkerhed i systemerne.

En række leverandører har gennem en årrække fokuseret mere på funktionalitet end på sikkerhed. Denne prioritering må ændres.

Forsikring bør indgå som en væsentlig komponent i forbindelse med ansvar for manglende IT-sikkerhed. Såfremt forsikringsselskaber bliver i stand til i et konkurrencedygtigt marked at vurdere risici i forbindelse med IT-løsninger, vil den part, der via lovgivningen er pålagt ansvaret for den manglende IT-sikkerhed, kunne indkalkulere denne udgift i det samlede regnestykke for aktiviteten ved at betale en forsikringspræmie.

2.2 Manglende sammentænkning mellem it-arkitektur og sikkerhed

Der mangler alt for ofte en stærk sammentænkning mellem it-arkitektur og sikkerhed i it-løsninger, store som små.

Sikkerhed ses ofte som noget der "puttes" på til sidst og ikke noget der medtænkes fra starten af et udviklingsprojekt. En af mange årsager er at kravstillere ikke er gode nok til at stille krav til indbygning af en sikkerhedsarkitektur i den overordnede IT arkitekturmodel.

2.3 Én sikker elektronisk ID,- skridt for skridt

På godt og ondt har Danmark haft nytteværdi af CPR nummeret som tillader sammenbygning af tjenester på en sikker måde. På samme måde må vi fremkalde en elektronisk identitet som vi på sigt kan enes om og også fokusere vore kræfter på at gøre sikrest og bedst mulig. Nytteværdien vil være uovertruffen for Danmark.

Vi mangler "situationsbestemt ledelse" på området. OCES og net-ID konkurrerer og efterlader borgere og virksomheder på "herrens mark".

CPR-systemet er sikkerhedsmæssigt forældet !

Men vi kan bruge en god rod-identifikation til at bygge multi-identitet og dermed isolering af data i specifikke sammenhænge på.

Tag som udgangspunkt at du KUN skal bruge Digital Signatur til at skabe nye nøgler

Husk at sondre mellem:

en ID, som er et "navn" i den elektroniske verden, ligesom "Peter" eller "Hans", (men bare bedre fordi det er entydigt),

en autentificeret (entydigt identificeret) bruger i en on-line aktivitet eller en digital signatur på et dokument.

Hvis det er det sidste, så husk altid at medtænke at sikkerhed har en grænse, at det kan gå galt og så skal der også være en god løsning på problemerne.

Biometri må danne grundlag for en erstatning af CPR-systemmet

biometriske produkter i dag er ikke sikre. Husk din fysikundervisning i gymnasiet.

Der er fejlmargen indenfor DNA, fingeraftryk og andre biometriske metoder.

Hvad vil vi acceptere af fejlmargen og hvordan angriber vi den biometriske løsning - biometri er ikke løsningen

2.4 Sikre systemer "out of the box"

Det er et grundlæggende problem at de almindelige standardsystemer kræver en sikkerhedsekspert at gøre sikre før de kan bruges fornuftigt.

Eller måske har de ikke tilstrækkelig viden til være opmærksom på behovet!

Og at specielt private ikke er indstillede på at betale for en ekspert.

2.5 · Dårlig uddannelse

Systemudviklere m.fl. er utilstrækkeligt uddannede i it-sikkerhed.

Der mangler uddannelsesforløb med fokus på sikker programmering

Der mangler gennemgående i hele uddannelsessystemet en fokuseret uddannelse i IT-sikkerhed på forskellige niveauer

Her bør der fokuseres på allerede etablerede uddannelser og certificeringer. Der findes CISA-, CISM- og CISSP certificeringer og ESL-uddannelsen. Tidligere (for et par år siden) blev der på samme lokation som vi er i dag holdt en høring, hvor der blev givet håndslag fra både Århus og København (Universiteter) om at indarbejde sikkerhedsmoduler i ingeniør/master-uddannelserne.

Vi skal også have sikkerhedsmoduler indarbejdet i erhvervsuddannelserne og KVU-uddannelserne indenfor IT

Alle IT-proffessionelle skal som en del af deres uddannelsesforløb gennemgå en anerkendt IT-sikkerhedscertificering - med forskellige delelementer afhængig af uddannelsen.

Ansvaret for at udvikle en international anerkendt IT-sikkerhedscertificering kunne henhøre under ENISA - og i DK: Videnskabsministeriet.

Ansvaret for at implementere IT-sikkerhedscertificeringen henhører under arbejdsmarkedets parter og Undervisningsministeriet

Der er mangel på sikkerhedskyndige i markedet og da det tager meget lang tid at blive ekspert på området er der behov for målrettede uddannelsesforløb.

Man behøver ikke blive ekspert, hvis man blot starter med at ændre sin holdning til det - kommer meget ved logisk tankevirksomhed.

Er det en god ide at bruge "tuborg" som kodeord på virksomhedens centrale server, nej - det er det faktisk ikke. Det er problemet i dag, niveauet er for lavt generelt

2.6 Sikkerhed koster - og der er ingen der er villige til at betale hvad det koster - fordi de ikke kender konsekvenserne

Jeg plejer at sige at god kvalitet er ofte mere sikkert. Et stabilt produkt indeholder sjældnere de grimme brølere som giver anledning til sikkerhedsproblemer.

Problemet som jeg tror du formulerer er at folk antager at sikkerhed koster, og det er et problem for udviklere som derfor ikke får lov til det.

Risiko-analyser/-vurderinger bør være et must for virksomhederne/de offentlige institutioner. Manglende fokus herpå medvirker til at "begrave" fokus på sikkerhedsområdet.

2.7 organiseret økonomisk kriminalitet

Identitetstyveri bliver en stærkt voksende form for kriminalitet også i Danmark

Vi kender annonce-hajerne som lokker medarbejdere til at købe Fup-varer i sommerferien. I fremtiden vil tung økonomisk kriminalitet være en guldgrube. Hvorfor gå efter småsvindel hvis man kan "tappe" en virksomheds elektroniske ordresystem, så man selv kan "godkende" fakturaer og attestere udbetalinger. Denne hackning kan/vil også foregå med hjælp fra "insiders" og vil være vanskelig at skelne fra valide transaktioner gjort intelligent.

Globalisering medfører en uddelegering af rettigheder som forstærker denne problematik. Hvilken loyalitet har medarbejderen i Brasilien?

Afpresning er en meget velfungerende global mekanisme.

Manglende sporbarhed er et problem - svindlerne findes sjældent. Der er behov for effektiv opklaring.

2.8 Brugervenlighed vs. sikkerhed

Brugervenlighed er ikke bare at det er "nemt at bruge". Brugervenlighed er også at det er nemt at bruge sikkert!

For meget software går på kompromis med dette.

Standardsystemer mangler opdeling imellem spørgetransaktioner/funktioner og opdaterende transaktioner/funktioner.

2.9 Web-udvikleres it-sikkerhedskultur og viden er ofte utilstrækkelig

Dette problem er meget udbredt og går fra enkeltpersoners websteder, webhoteller og til websystemer der benyttes i den nationale IT infrastruktur - alle websteder idag i Danmark.

Jeg sporer endog en meget lille interesse blandt selv dygtige udviklere til at dygtiggøre sig indenfor sikkerhed. Det opfattes ofte som et lille appendix til det egentlige arbejde og ikke som en integral part af arbejdet som udvikler.

2.10 Sikkerhed i den Serviceorienterede arkitektur - et upåagtet problem?

I en serviceorienteret arkitektur kan mange aktører bidrage med dele af en samlet sagsbehandling/problemløsning. Det bør være en forudsætning for at stille services til rådighed, at sikkerheden følger en fælles fastlagt, høj standard for autorisation (rolle/brugerstyret) samt kryptering på behørigt niveau. Uden dette vil SOA blive en illusion.

Udvikling inden for dette område tager ikke i tilstrækkelig grad hensyn til brugen af eksisterende (internationalt anerkendte) standarder.

2.11 For lidt fokus på rettigheder

Manglende fokus på muligheden for videreudvikling og fortsat drift hvor der ikke bruges open source

2.12 Systemansvar for IT produkter

Gælder lovgivning om systemansvar for IT produkter? Hardware er omfattet men hvad med software? Skal der laves en særlig lovgivning som indbefatter et sikkerhedsansvar således at det er ansvarspådragende ikke at overvåge og forbedre et fejlende produkt indenfor "rimelige" tidsrammer, og for kommunikations og transmissionssoftware at kræve automatisk fejlmeddelelse og sikkerhedsopdaterings udsendelse til alle brugere - det findes men kunne sættes endnu mere i faste rammer.

2.13 · Manglende offentlighed

Udviklingen af ny software sker i en lukket proces og softwaren er ofte leverandørejet. Derfor har offentligheden ikke mulighed for at

forholde sig kritisk til udvikling af it-systemer, hvilket går ud over sikkerheden.

I det offentliges kritiske it-sikkerhedssystemer bør der måske stilles krav om åbning af kildekoden. Vi har fx i USA set eksempler på hullet software brugt til elektroniske valg (Diebold?).

2.14 Ministerierne laver hver deres sikkerhedsløsning.

De enkelte ministerier kræver forskellige sikkerhedsløsninger i deres systemer.

Disse er langt fra alle særligt gode, og den enkelte bruger bliver forvirret - blive utryg - laver fejl og kompromittere således sikkerheden.

Og kommunerne der skal bruge de forskellige ministeriers web-portaler skal håndtere mange forskellige sikkerhedsprocedurer når medarbejderne skal accesse forskellige sites. Det er dyrt og besværlig og koster tid.

Der mangler fokus på internationale standarder.

2.15 Er it-sikkerheden til stadighed ok i systemer, som udvikles af en serviceprovider?

Eksemplet kan være at mange kommuner opfatter, at IT sikkerhed er deres IT-providers problem, når de blot har forskrifterne i orden for deres intranwrt og PC'ere. Det er den samlede problemløsning 'fra jord til bord' - der skal sikres, ikke blot input og output delen

Virksomheden/kommunen/institutionen har ansvaret for sikkerheden, uanset løsningerne tilvejebringes via outsourcing m.v. Imidlertid har mange svært ved at leve op til dette ansvar og havner i en klemme med stærk afhængighed af leverandøren.

Er aftalegrundlaget tilstrækkeligt til at sikre, at "ejeren" til stadighed har styr på og overblik over it-sikkerheden i såvel generelle som specifikke applikationer?

- tilstrækkelig styr på databaseadministratorer?

- tilstrækkelig logningsoplysninger?

- følges der tilstrækkeligt op på bruger og deres autorisationer?

Er risikovurderingen for systemet opdateret med et dækkende trussels- og afdækningsbillede? Har systemejeren godkendt risikovurderinger, herunder eventuelle restrisici?

Kan man overhovedet bedømme sikkerhedsniveauet før et incident, hvis man ikke har adgang til kildekoden.

2.16 Enterprise Arkitektur og hermed risikovurdering og sikkerhedsløsninger - ikke IT-arkitektur - skal være ledelsens ansvar

3. Teknik og infrastruktur

3.1 Email - få det nu fikset!

Utroligt så meget brugerne må finde sig i når det gælder email! Markedsaktørerne lapper og piller og klistrer men der er stadig ikke en udvikling som peger imod en udbredt anerkendt troværdig, fortrolig og stærkt identificeret email løsning til afløsning for det der blev opfundet i 1980'erne.

Enig! utroligt at Internettets gamle protokoller stadig benyttes, - således at vi anvender kommunikationsprotokoller der ikke er designet med sikkerhed som en del af helheden.

Og ISP´erme tilbyder over en kam stort set ikke kryptering af e-mailforbindelser. En katastrofal mangel, der meget let kan rettes op på.

Større sikkerhedskrav til ISPer - enig omkring krypteringskrav - og kravene kan godt udvides

Det er teknisk muligt at sikre sine e-mails i dag men det kræver den store ingeniøreksamen og det er blokerende for den brede anvendelse.

Mail leverandørerne gør det på hver deres måde - som sjældent er bruger venlig eller logisk. Behov for standardisering som inkluderer brugervenlig sikkerhed.

Ingen protokol, hvor troværdig, fortrolig og identificeret den end er kan gøre noget ved spam-problemet uden at der er mulighed for international håndhævelse. Få det på plads først. SPAM-problemet i DK er begrænset - ikke fordi vi har en bedre protokol, men fordi vi har håndhævelse.

M.h.t. virus vil en tilpas kompromiteret maskine stadig kunne skabe problemer med en anden protokol.

3.2 Digital Authentikering

Biometri må IKKE bruges til Digital Authentikering

Biometri skaber Identitetstyveri og Omvendt Bevisbyrde i retssager

Biometri blokerer for borgernes sikkerhed

Identifikation flytter kontrollen væk fra borgerne og placerer altid magten hos en anden

Hvordan forhindrer vi kriminelle i at misbruge biometriske sensorer?

Det bliver alt for nemt at aflytte/spore f.eks. politikere, sårbare personer og borgere

Digital Signatur er ikke sikker nok

Behovet og nødvendigheden skal være mere klar. Hvad er risikoen for at et dokument opsnappes sammenholdt med muligheden for at stjæle fra postkassen eller fra firmaets papirkurv.

Ja - den er absolut ALT for svær.

En stor del af det offentlige Danmark, og efterhånden også mange private, bruger efterhånden den digitale signatur til identifikation. Dette gør den digitale signatur "missionskritisk" i forhold til hele udviklingen af informationssamfundet.

Den manglende sikkerhed i form af et "fysisk led" gør signaturen meget usikker. Er en cracker inde på en pc, kan samme cracker også fuldstændigt overtage den digitale signatur.

Problemet affærdiges ofte med, at det selvfølgelig ikke er retsligt bindende, at en digital signatur er blevet misbrugt. Men det er en meget reel risiko, at vi i praksis kommer til at se en slags omvendt bevisbyrde i den slags sager.

Når - og jeg mener NÅR - de første sager om misbrug opstår, vil vi risikere at se en voldsom nedgang i tilliden til digital signatur. Og dermed en nedgang i tilliden til informationssamfundet som helhed.

En central Signatur KAN ikke sikres - CA er ikke trustworthy, men risikoskabende.

Pointen er ikke at vi ikke skal have digitale nøgler, men at (gen)brugen af identificerende nøgler ødelægger sikkerhed

Det handler mere om balancen mellem teknisk sikkerhed og brugerens evne til at anvende løsningen.

Vi kan gøre den digitale signatur så sikker, at borgerne ikke kan anvende den - så vil de omgå sikkerheden og resultatet er en lavere sikkerhed.

Signaturen må vokse med nytteværdien. Sikkerheden må vokse i takt med at investeringen kan retfærdiggøres. Men standarderne må fastholdes, så vi skaber en fortløbende rejse.

Certifikatet til den digitale signaturer sikrer en identifikation af hvem folk er - men vi skal også have en mulighed for at kunne graduere hvad man har adgang til - forskellige niveauer. Vi mangler kort sagt attributter på identiteter, der muliggør en identificering af prokura.

3.3 Et fælles nøglekort for den offentlige sektor og finanssektoren bremses af manglende politisk samtænkning

Tænker man i sektororienterede sikkerhedsløsninger får man stærkt varierende sikkerhedsniveau, besværlige og ikke-brugervenlige forskelligartede IT-løsninger og en manglende mulighed for at høste udbyttet af digitalisering overalt i samfundet..

Eksempel: Sygesikringskortet skal erstattes, Tinglysningssystemet efterspørger bærbar digital signatur, EU ønsker biometriske pas, udbredelsen af OCES certifikaterne synes at have stagneret alt imens bankernes net-løsninger får flere kunder. Tænk det sammen, gør noget radikalt og lad alle få glæde af en fælles dansk infrastruktur, der bringer niveauet op på kvalificerede europæiske digitale certifikater.

Man skal huske at et sådant nøglekort ikke kun udpeger en person, men en aktør dvs. en fysiks person som er tilknyttet en organisation: Arbejdspladsen, idrætsforeningen, sin familie etc. Hvis man tænker denne tanke videre så vil man på sigt få en lang række identiteter (organisation * systemer) hvis man ikke samorder så mange som muligt af disse.

Men husk at privacy også er et issue.

3.4 Terror mod infrastruktur

Samfundets infrastruktur styres af IT. El, telefoni, varme, finans, Internet, TV etc. Med terror-motivationen opstår der nye "rationaler" som ikke nødvendigvis er vægtet i selskabernes tidligere risikovurderinger. "Hvem kunne have interesse i det?"- vurderingen vendes på hovedet.

Ganske enig. Problemet er at der ikke i forbindelse med udlicitering af kritisk infrastruktur stilles krav til sikkerheden af det offentlige. Se i øvrigt under Regulering og Standard for samme emne

Enig - her har vi et meget alvorligt samfundsmæssigt problem. Se blot hvad der skete da København var uden strøm 4 timer.

3.5 Der fokuseres for meget på identifikation af personer, og for lidt på hvilken rolle personen spiller i interaktionen med et system

Der er meget offentligt diskussion om hvorvidt en given metode til at identificere personer er tilstrækkeligt sikker, men der fokuseres ikke på den anden halvdel af problemet - nemlig hvad vil man tillade personen at udføre.

Dette er selvfølgeligt ikke et problem i meget simple systemer, men efterhånden som flere processer digitaliseres, er det et stadigt stigende problem at der mangler sikre metoder til tildeling af rettigheder.

Der mangler også en overvågning af, at rettigheder også overholdes. Ofte er det nødvendigt at give tekniske adgang til mere, end man har juridisk adgang til.

Vigtigt at adskille identifikation og autorisation som to forskellige problematikker. Identifikation kan standardiseres vældig godt imens autorisation er meget kontekst afhængigt og en opgave for data ejeren decentralt.

3.6 Løsninger er for komplicerede at bruge

Digital signatur anvendes meget lidt i erhvervslivet - det vælges simpelthen ikke til fordi det er for besværligt.

Der bør være løsninger der er så lette at alle bruger dem

3.7 Der mangler en standard for sikring af privatejet kritisk national infrastruktur

Ligeledes et problem at mange nye teknologier tages i brug tidligt uden gode vejledninger i sikkerheden.

VoIP - der burde være en dansk udgave af NIST vejledning SP800-58 "sikkerhed i VoIP netværk"

- vi har set problemet med 802.11 trådløse netværk, hvor personfølsomme data har været tilgængelige.

Det offentlige kunne gå i front og lave vejledningerne og håbe at virksomhederne ligeledes vil benytte disse.

Sikkerheden i privatejet kritisk national infrastruktur er ikke et konkurrenceparameter og derfor overladt til hvad operatørerne synes er "godt nok". Der ses i udlandet en trend til at sammenkoble de komplekse systemer og at kunne monitorere flere systemer med færre ressourcer. Ved flere samtidige hændelser i sammenkoblede systemer er det sandsynligt, at operatørerne ikke kan overskue situationen og handler uhensigtsmæssigt. Når der er stærke transnationale krav til f.eks. flyveledere og airtraffic control, hvorfor skal man så ikke have det på kritisk national infrastruktur?

3.8 Manglende it-sikkerhed skaber ganske store socioøkonomiske udfordringer - som bliver større og større for hvert eneste år !

Borgere og virksomheder er i stigende grad afhængige af tilstedeværelsen af internettet - mere og mere forretningskommunikation går via IP / messenger / videokonferencer/ telekonferencer - og for borgerne er e-handel i stigende grad ved at afløse traditionel detailhandel.

Denne interdependens af en sårbar kanal vil de kommende år blive endnu mere forstærket idet man må forvente at nogle mega-trends udvikling betyder endnu mere digital kommunikation. Samtidig bliver det offentlige også sårbarer idet såvel betalinger som henvendelser vil formodes tilvejebragt digitalt.

De to megatrends som ligger ligefor er: IP-ficeringen af alt fra køleskabe til varmemålere, telefoner, TV etc. samt RFID-teknologiens digitalisering af en analog verden.

Konklusionen er, at der vil de kommende år være mere og mere konsekvens af manglende it-sikkerhed.

3.9 Behov for at IT-sikkerhed er tilgodeset i nye teknologier

Ny teknologi introduceres med børnesygdomme som allerede er løst i tidligere teknologier

3.10 "DRM" kompromiterer borgernes sikkerhed

Det grundliggende princip i DRM er at ville kontrollere (i hvert fald dele af) den software brugerne anvender. Hvis brugeren ikke har grund til at tillægge DRM-leverandøren trust (og det er sjældent tilfældet) vil brugerens sikkerhed kompromiteres. SONY leverede for nyligt et klart eksempel på dette.

3.11 virus, virus, virus, virus, virus, Trojanske heste og andre skadevoldende programmer

Trojanske heste som trænger ind via fejl i browser el. andet software vil danne grundlag for kriminel aktivitet

Spyware er i dag ikke alene et problem i forhold til kriminalitet. Også i forhold til performance, som man ofte ser gå drastisk ned på inficerede maskiner.

3.12 · Kritisk software står pivåben

Sendmail og Windows er fulde af huller.

Det meste software er fyldt med sikkerhedsproblemer og det lader til at selvom dette har været kendt i mere end 20 år kommer der hele tiden nye udviklere som ikke tænker på sikkerhed

Problemet (i det omfang det eksisterer) forstærkes når det kombineres med en software-monokultur på et område.

Det er derfor nødvendigt med åbne standarder i infrastrukturen for at muliggøre en heterogen infrastruktur, hvor man ikke er bundet til bestemte usikre produkter.

3.13 Et Borgerkort er IKKE et Identifikationskort

Et Borgerkort har til formål at sikre borgerens kontrol med hendes MANGE digital nøgler, som skal kunne holde forskellige sammenhænge (kontekst) adskilt.

I modsætning til et National Id kort, som er en sikkerheds-destruerende og centraliserende overvågningsteknologi.

Ordet Borgerkort er ikke klart defineret.

Det kan indeholde en nøgle, som borgeren kan bruge til at identificere sig elektronisk, så vedkommende kan få adgang til at kigge det offentlige over skulderen.

Men det kan ligeledes bruges til at spore borgerens bevægelser på nettet.

Det er vi menneskers valg hvorledes teknologi anvendes - det er ikke teknologien der er problemet.

Det bør stå klar, at det der skal investeres i er et borgerservicekort - som muliggør sikker autentificering sammenholdt med lokaliserede multiidentitet - det skal principielt afløse samtlige andre offentlige identifikationskort/papirer.

Så derfor: Brug begrebet nøglekort i stedet for

Det offentlige bør som i England tage lead på dette projekt og sikre, at vi har den fornødne infrastruktur til at skabe grobunden for de mangeartede services som et nøglekort vil føre med sig.

Hvad er de sikkerhedsmæssige aspekter hvis man mister sit borgerkort/nøglekort

Den engelske løsning destruerer værdi!

3.14 SPIM - et fremtidigt problem ved VoIP.

Der er ingen grund til at tro, at vi ikke vil komme til at opleve spam via ip-telefoni i de kommende år efterhånden som teknologien vinder indpas. I USA så man i mange år (og til dels stadigvæk) et gigantisk antal automatiserede opkaldstjenester, der bl.a. pga. de lave eller ikke eksisterende lokale takster på telefonnettet, satte maskiner til at ringe folk op med båndoptagelser med reklamer (og nogle gange rent svindel). De samme betingelser for misbrug ligger indbygget i VoIP-teknologien, hvor man gratis eller til meget få penge kan ringe folk op.

VoIP bruges i dag af både private og virksomheder og udbredelsen ser ud til at vokse eksponentielt. Vi risikerer at komme til at stå med samme massive problemer, som spam i dag udgør i forbindelse med mails. Men uden de samme muligheder for filtrering.

Vi har for en gangs skyld muligheden for at tage fat på et problem INDEN det antager store dimensioner.

Mange tele udbydere af vekslende kvalitet gør det særdeles vanskeligt at styre området. God grobund for svindel.

3.15 En global verden giver globale udfordringer

Outsourcing er kommet for at blive - eller er det ? Hvad når man ikke kan garantere at bærebølgen til Bangalore er sikker - eller ikke tilgængelig - hvad så ?

Derfor er sårbarhed / kritikalitet af it-infrastrukturen ikke bare et dansk problem - men et europæisk/globalt...

'Safe Harbour' kræver international kontrolkommission - på linie med atomenergikommissionen

3.16 Der mangler reel end-to-end sikkerhed

Der bruges meget tid på at sikre pc og borgeren mod trusler, men når en transaktion eller opdatering først når den første server, så sendes data ofte på såkaldte "sikre net", hvis eneste sikkerhedsfunktionalitet er at de er direkte tilkoblet internettet! Det betyder at der er mange teknikere som har adgang til fortrolig oplysninger, og muligheder for hackere til at få adgang til informationer.

I dag sendes betalinger, cpr oplysninger etc. ukrypteret på disse net som er defineret sikre, det kan ikke være tilstrækkeligt

3.17 Trusted Computing fører til fjernkontrol af borgerne - typisk udenlandsk og kommercielt betinget

Tankegangen om at eksterne skal kunne kontrollere sikkerheden på din computer er livsfarlig. Det betyder f.eks. at man senere kan "downgrade" systemet med indbygget spyware og trojanske heste, som du ikke har mulighed for at detektere

"Trusted" computing, forhindrer borgene i selv at vælge deres sikkerhed bl.a. i form af indirekte påtvunget software.

Der vil være tale om mere sikkerhed for producenten af computeren, men mindre sikkerhed for borgeren. I praksis vil den "personlige computer" ikke længere være personlig, men noget du "låner" af producenten under vedkommendes (evt. indirekte) kontrol.

Trusted computing kan være en tredjepart certificering af produkter. Der er ikke tale om mere kontrol end den der allerede findes fra de forskellige leverandører. Trusted computing er da et must. Spørgsmålet er snarere hvordan man bedst opnår det? Hvem skal være garant for trust?

Næppe staten

3.18 · Nettet er outdated

Internettet er grundlæggende ikke gearet til nutidens trusselsbillede (mobile enheder, åben tillidsstruktur).

Internet tilbyder grundlaget for kommunikation, det er ikke en del af opgaven at tage sig af truslerne - der er ingen ejer. En af grundideerne er at nettet er "dumt" mens enhederne er dem der er komplekse. Ansvar, politik osv. er noget som man må lægge ovenpå.

3.19 Perimeter sikkerhed fejlet

Server sikkerhed fejler i stadigt større omfang, fordi man fokuserer på at beskytter mod tredjeparter i stedet for at indbygge sikkerhed.

Centrale databaser har ingen sikkerhed - kriminelle kan altid tilgå disse, hvad enten angribere er interne, kriminelle, kommercielle, sociale, institutionelle eller blot fejl

Det fuldt integrerede informationssamfund er dybt sårbart, hvis man ikke indtænker sikkerhed i bunden og antager at perimetersikkerhed fejler.

3.20 Dårlige passwords giver mange problemer

Er der nogle teknologier på vej der reelt og indenfor en overskuelig tidshorisont kan mindske problemer som følge af brugeres dårlige password-adfærd?

Fælles offentlig brugerstyring bør være et krav

En løsning på de mange passwords - ingen kan huske dem og det giver nogle sikkerhedsbrister

3.21 Teknologien skal anvendes til at skabe den sikkerhed som den almindelige bruger ikke kan forstå

Vi kan ikke forvente at alle forstår sikkerhed, eller interesserer sig for det.

Burgeren må kunne forvente at løsningerne, der sælges er sikre, på samme måde, som biler ikke sælges uden sikkerhedsudstyr.

Men der skal stadigt være en "brugsvejledning/ undervisning" i hvorledes man skal begå sig for ikke at få problemer.

3.22 Fællesoffentlig brugerstyring

Kræver en samtænkning af den digitale signatur på tværs af sektorerne - både banksektoren og den offentlige sektor må samarbejde uden at det betyder omkostninger for borgerne. Genvinsten ligger i effektivisering, undgået dobbeltarbejdet og mulighed for at forhøje sikkerhedsniveau.

Hvorfor kun offentlig?

Fællesoffentlig brugerstyring muliggør - ved brug af åbne standarder - at borgerne - såfremt de kan identificere sig - kan få adgang til data lagret i fællesoffentligt regi - i realiteten kunne borgerne ved hjælp af en udvidet E-boks gives adgang til at lagre data på det fælles offentlige datalager - hovedansvaret for sikkerheden ville så påhvile det offentlige - men ville ikke afskære private virksomheder i at benytte samme løsning - med evt. cvr.nr. som identitet.

en central løsning vil øge risiko

En central løsning kræver særlig beskyttelse, ja; men en stor underskov af decentrale løsninger stiller store krav til at mange har tilstrækkelig indsigt i hvorledes løsninger sikres, og den er der stadigt for få af. Så i praksis vil den centrale løsning være mere sikker, på trods af manglerne.

3.23 Bagdøre udnyttes af kriminelle

Statens krav om kontrol med borgerne udnyttes af kriminelle.

Se f.eks. Grækenland, hvor Premierministeren og 100 andre topfolk blev aflyttet af det indbyggede aflytningsudstyr.

De kriminelle bruger systemer uden bagdøre, så det ramme kun de lovlydige borgere, legitime transaktioner og dumme kriminelle

Regel: Ingen bagdøre til systemerne

3.24 Kriminelle vil angribe almindelige pc'er i stadigt større omfang

3.25 Identifikation der baserer sig på at brugers pc er sikker kan blive undermineret

3.26 Dynamisk Sikkerhedsstyring

Problemet er at one-size-fits alle er destruktiv i næsten alle sammenhænge

Vi skal bruge MANGE forskellige sikkerhedsmodeller og nøgler, der kan tilpasses kontekst

3.27 IT-sikkerhed ved biometri/rfid og andre nye teknologier

En enkelt biometrisk indikator vil tiltrække forsøg på omgåelse. (eks: Iris-scanning kan overføres til kontaktlinse) - kun kombinationer kan anbefales.

3.28 Transparens skaber sårbarhed

Tendensen mod konstant identifikation og overvågning svækker ofrene uden at forhindre de kriminelle i at beskytte sig.

Hele tankegangen om at devices og personer har EN identitet er sikkerhedsdestruktiv og hovedkilden til mange afledte sikkerhedsproblemer

Man kan ikke skjule sig i transaktioner med den offentlige sektor - det giver hverken mening eller rationale. Pseudonymitet kan anvendes i en mellemfase, hvor man scanner stor datamængder - og kun ved positiv identifikation af problem kan identiteten afsløres.

Sikkerhedsmæssigt er der ikke stor forskel mellem én og flere identiteter. Datamining udvisker forskellen.

Mange transaktioner vil have behov for autentificering, altså det modsatte af anonymitet

3.29 Automatisk opdatering af programmer

Hvad har Microsoft lige adgang til og i øvrigt andre leverandører - når der automatisk opdateres

ms behøver vel ikke meget data for at et program kan se at et andet program skal opdateres

Automatisk opdatering giver fri adgang til computeren

3.30 dårlig backup kultur - mange tager for sjældent backup

Hvilket måske skyldes for dyre og for besværlige backup-løsninger.

3.31 Er behandling af it-sikkerhedshændelser/-alarmer dækkende og betryggende?

Har virksomhederne overblik over kriterierne for alle relevante hændelser og alarmer?

Er Overvågningen af alle relevante hændelser og alarmer sat i system, ligesom for fysisk sikkerhed og "almindelig problem management"?

de fleste hændelser opdages ikke

3.32 seks ud af 10 offentlige virksomheder har ikke opdateret it-beredskab (ifølge Dansk Statistik)

3.33 Fiberinfrastrukturen bør integreres

De forskellige offentlige myndigheder benytter forskellige leverandører til deres infrastruktur- det betyder at to virksomheder/offentlige myndigheder "fragter data" - som de reelt skal udveksle med hinanden - i samme fiberkabel parallelt med hinanden til en udbyder.

Hvorefter udbyderen sender svardata retur i den selvsamme infrastruktur.

3.34 Ingen servicer-side Single Signon

Server-side single signon fører til Single point of trust failure, som kan udnyttes af kriminelle.

Single Signon er per definition et client-side tiltag

3.35 Konvergens og nye bærbare applikationer skaber nye sikkerhedsproblemer

4. Viden og adfærd

4.1 Almindelige brugere lades i stikken

De almindelige brugere/borgere lades i stikken med usikker teknologi, som de gøres mere og mere afhængige af.

Det er urealistisk at alle brugere skal blive eksperter på softwareopdateringer og sikkerhed.

Der er en del utryghed ved at bruge internettet pga. den alm. brugers angst for at egne data ikke er sikre nok.

Det for vanskeligt at opretholde en sikker adgang til og brug af internettet for almindelige brugere

Den almindelige bruger (private husstande) har ikke forudsætningerne for at håndtere sikkerhed. Hacking, virus mv. giver enorm tidsspilde og de stadig kraftigere private computere kan bruges destruktivt af 3. part

En forbedret og løbende uddannelse af især unge kan over tid sikkert løfte niveauet, men aldrig tilstrækkeligt.

Det må derfor være en opgave for samfundet, serviceudbydere og professionelle aktører i markedet.

Der bør stilles krav om at alle pc'ere der sælges til slutbrugere leveres med færdiginstalleret sikkerhedssoftware og -indstillinger som automatisk sikrer en regelmæssig opdatering af de nødvendige komponenter via internettet.

It-sikkerhed forklares ikke på den almindelige brugers sprog

4.2 IT sikkerhedshjælp til små og mellemstore virksomheder vil fremme globalisering og innovation

Vidensdeling over landegrænser bliver et uomgængeligt krav. De små og mellemstore virksomheder har behov for adgang til kompetence og (open Source) systemer, der kan højne sikkerheden og beskytte virksomhedens intellektuelle rettigheder så vidensdeling med autoriserede partnere kan finde sted. Uden sikker viden bliver mulighederne ikke udnyttet og vi forpasser chancen for vækst.

SMVere er - som indenfor andre områder - en it-hvidplet. Det gælder også sikkerhedsområdet. Special treatment is needed

de små virksomheder ser ikke deres behov

4.3 Hvorfor tænker Digital Forvaltning aldrig sikkerhed?

Digital Forvaltning er totalt centralistisk og gør borgerne transparente overfor kriminelle og staten. Samtidig ser vi en stigende tendens til at Staten derefter "sælger" borgernes data = Ekspropriation

Digital forvaltning handler om effektivisering! Når borgere og politikere insisterer på et stadigt voksende antal af mere komplekse velfærdsydelser, stiger kravene til effektive IT-systemer, der dels kan (bidrage) til at levere ydelserne, og dels kontrollere at der ikke "snydes" i uacceptabelt omfang. Det ser ud til at vi gerne vil have alle mulige ydelser, men vi vil ikke kontrolleres! Men uden kontrol vil efterspørgslen efter ydelserne vokse til en ufinansierbar størrelse. Er kontrollen ikke den pris borgerne må betale for de komplekse velfærdsydelser?

4.4 IT-sikkerhed i hjemmet

Utilstrækkelig fokus på de involverede risici - særligt vedr. brugen af Internettet - medfører kæmpe-potentiale for at benytte privates computere som zombier til brug for bl.a. DDOS-angreb, etablering af phishing sites etc.

Der mangler totalt en erkendelse af, at man som privat bruger ikke er færdig med sine investeringer, når man har købt sin pc, OS og evt. office-suite. Køber man en bil, er man godt klar over, at man engang imellem skal til mekanikeren og punge ud. Køber man en pc, er det for de fleste utænkeligt, at man skal betale for konsulenthjælp - og da slet ikke i for-

bindelse med sikkerhed. Det betyder at en stor del af den danske it-sikkerhed er bundet op på hjælp fra den tilfældige fætter/søn/nabo eller lignende, som den dag havde tid og lyst til at hjælpe med at installere et AV-program.

4.5 Hvor går den menige dansker hen og får viden om hvordan han beskytter sin PC'er?

De fleste er overladt til Microsofts automatiske opdateringsprogrammer og går derfor glip af megen anden kilde til information.

Her mangler vi krav til leverandører af pc'er m.v. til at have fokus på sikkerhed i forbindelse med de komponenter, som de "langer over disken".

Vi kan ikke hvile på laurbærrene her - og bare tro, at leverandørerne tager ansvar. Men det er alligevel de muligheder, som menigmand har.

Det kunne være en opgave for Videnskabsministeriet at udvikle en letforståelig "Pixi-bog" + website hvor folk fik viden om IT-sikkerhed på den private PC

Dette er stort set tilvejebragt i regi af ITEK og IT-Branchen som en udløber af Netsikker.nu 2005

Vi har i PROSA forsøgt det samme med websitet 1984.dk. Og med overraskende store besøgstal til følge.

Det kan ikke være meningen at den alm. brugere skal sætte sig ind i alt dette. Det har de simpelthen ikke forudsætningerne til at gøre.

Brugernes basale behov overses.

Brugerne ønsker ikke generelt at forstå hvordan løsninger omkring it-sikkerhed virker, de vil bare have sikkerheden leveret som en naturlig service de kan have tillid til fra deres leverandører. Det skal være meget lettere at være en "naiv" og "uvidende" bruger af internettet - branchen har svigtet ved at fokusere på tekniske løsninger i stedet for brugevenlighed.

4.6 Der skal fokuseres på vigtige problemer og der skal være proportionalitet mellem problemets alvorlighed og løsningerne

Der er mange virksomheder der ikke i tilstrækkelig grad anser deres systemer for værende forretningskritiske og derfor ikke sikrer dem tilstrækkeligt.

Problem at der ikke sættes ressourcer af til sikring af vitale dele af infrastrukturen, hverken i små eller store virksomheder - ej heller i den centrale infrastruktur

4.7 · Svært at skelne mellem store og små problemer

Der er svært for brugeren at skelne store og reelle problemer fra ubetydelige eller fiktive problemer, bl.a. i kraft af

sensationshistorier i medierne.

Der mangler noget klar underbygget formidling af problemets karakter og omfang

4.8 It-sikkerhed skal gøres lettere at forstå

Alt for ofte forklares it-sikkerhedsmæssige spørgsmål på en teknisk måde, den almindelige bruger ikke har nogen forudsætninger for at forstå

Der kan bl.a. bruges eksempler fra dagligdagen for at gøre sikkerhedsspørgsmål mere forståelige

4.9 Børn og Unge lærer ikke om behovet for sikkerhed.

Der bør indgå mere undervisning i folkeskolen omkring sikkerhed på Internettet.

det er i dag udbredt blandt unde at de deler dere adgangskoder med deres venner / og nogle gange fjender.

Kulturen er at hvis den er hemmelig, så er man ikke rigtig med i fællesskabet.

4.10 Kompromiterede hjemme-computere

Der står for mange kompromiterede computere rundt om i hjemmene og der er for lidt at gøre ved det.

Alm. brugere har ikke indsigten til at at håndtere et indbrud på deres maskine, hverken via virus, orme, eller direkte hacking og reinstallation med en passende opgradering er sjældent en mulighed.

Mere konsekvent sortering af hvilke kunder, ISPerne ønsker. Hvis brugeren ikke vil sikre sig, ophører aftalen. Evt. udveksling af oplysninger mellem ISPérne om "dårlige" Internetbrugere

4.11 Hvem certificerer sikkerhedsløsninger?

I stil med IT-Borger mangler vi en oversigt der på opdateret, autoritativ måde kan fortælle menigmand, hvad der kan bruges

der findes ingen reelt værdiskabende produkt/løsningscertificeringer

Problemet er vel også at sikkerhed ikke bare kan ses isoleret i en løsning, men at implementering og anvendelse er helt centrale for det reelle sikkerhedsniveau. På løsningsniveau kan man kun sige at der er mulighed for at etablere et højt sikkerhedsniveau

4.12 Det Offentlige, undervisningssektoren og de private virksomheder har berøring med de fleste borgere i Danmark

Derfor bør kravet om øget fokus på IT-sikkerhed håndhæves på alle niveauer - ved en fælles indsats vil Danmark kunne opklassificeres både med hensyn til IT-sikkerhed og brug af digitale løsninger

4.13 · Sikkerhedssoftware er for svært at bruge

Det er besværligt at færdes sikkert. Antivirus, firewalls m.v. er for kompliceret for den almindelige bruger.

Sikkerhed bør ikke overlades til "sikkerhedssoftware". Sikkerhed bør tænkes ind i alt software.

"Sikkerhedssoftware" som antivirus og firewalls giver ofte brugerne en falsk fornemmelse af sikkerhed.

Det er ikke et spørgsmål om, at sikkerhedsSW er svært at bruge - det er et spørgsmål om virksomhederne, de offentlige institutioner og privatpersoner har nok fokus på områderne til at være villige til at anskaffe de rigtige løsninger. Har man besvær med at få SW'en til at køre korrekt, er der en række leverandører, som gerne stiller op for "ussel mammon".

Awareness og fokus på medarbejdere/personer mangler klart en plads i højeste prioritet.

4.14 Vi mangler forskning i hvordan hr. og fru Hansen opfatter IT-sikkerhed

En analyse af hvordan trusselsbilledet opleves i græsrodshøjde vil være et godt udgangspunkt for en pædagogisk indsats - og måske for udvikling af mere pædagogiske sikkerhedssystemer.

det er nemt nok: Hansen synes det er svært

sikkerhedssystemer udvikles primært i udlandet

4.15 Jo højere lønramme, jo større risikoadfærd indenfor IT-sikkerhed

I det offentlige er man ved at udbrede DS-484 og få et fornuftigt sikkerhedssetup. Dette vil med sikkerhed blive undermineret af topledelsen, der vil kræve trådløs ukrypteret synkronisering af mail med pda'en i bilen, hvis det er det som skal til for at det kan gå hurtigt nok med synkroniseringen.

4.16 Trust = Accept af risiko i kontekst - Identifikation skaber DISTRUST

Der er et grundliggende problem omkring det at tage Tillid for givet og sætte lighedstegn mellem Identifikation og trust.

Alle agenter er riskoaverse og ingen har naturlig tillid til andre.

Det drejer sig altid om opfattelsen af risiko (som per definition ikke er perfekt) i forhold til den værdi, der opfattes.

Tilsyneladende ikke rationel adfærd - dækker over manglende viden om risiko.

Identifikation skaber altid risiko fordi det fjerner personens kontrol med situationen

4.17 Hvor mange folketingsmedlemmer er bekendt med problemet om IT sikkerhed?

4.18 · Lemming effekten

Brugerne åbner e-mail, som de ved er/kan være farlige.

4.19 "Unsafe at any speed" - for Internetanvendelse

Bilerne blev ikke sikkerhedsmæssigt forbedret af fabrikanterne, før der kom et folkeligt pres, så som med bogen "Unsafe at Any speed" af Ralf Nader.

5. Kommunikation og vidensdeling

5.1 Oplysning på linie med folkesundhed eller trafiksikkerhed

Sikkerhedsproblematikken bliver behandlet som et teknisk randdisciplin for specialister. Se det i stedet som trafiksikkerhed eller folkesundhed

Der bruges ikke nok midler på oplysende aktiviteter om it-sikkerhed til befolkningen og/eller udvalgte målgrupper

Trafiksikkerhedssammenligningen er god, for de fleste mennesker vil ikke tænke over, at de skal til mekanikeren og betale for at få repareret deres bremser af sikkerhedsmæssige årsager. Men de fleste vægrer sig ved at skulle betale en konsulent for at installere og vedligeholde sikkerhedsprogrammer på en privat pc

5.2 Borgerne er interesserede i at være sikre - men ikke i sikkerhed

Borgerne er meget interesserede i at være sikre.

Alle undersøgelser viser imidlertid, at borgerne ikke er interesseret i den tekniske sikkerhed - det er noget de bare forventer fungerer uden at de skal tage ret meget stilling til det.

Og internet brugerne gider ikke bruge masser af timer blot på at få sikkerhedssystemerne til at virke - leverandørerne (af udstyr og internetforbindelser) skal bare sørge for at det virker. De store ISP'ers SPAM og antivirusfiltre er derfor det bedste sikkerhedstiltag i mange år

Der skal stilles større krav (lægges pres) på producenterne af hardware, således at sikkerhed af systemet er en del af fx. opsætningen. Fx. ved trådløst net skal de almindelige sikkerhedsbetragtninger være sat på forhånd og promptes brugeren

Præcist derfor må borgerne have hjælp af professionelle som kan påtage sig ansvar og tillid (og leve af det på den ene eller den anden måde).

Det koster ikke noget, at ignorere sikkerheden i dag for den gennemsnitlige private bruger. Højst en smule irritation over nogle mistede dokumenter. Men som kommentaren ofte lyder: "Jeg har jo ikke noget, der er så vigtigt".

5.3 Uddannelser indenfor IT-sikkerhed mangler på universiteter og andre steder

Uddannelse i sikkerhed er mange steder begrænset til kryptering og algoritmer.

Meget lidt om sikre protokoller, yderst lidt omkring god programmering, intet om backup, intet om drift af systemer. Der mangler uddannelseselementer med fokus på:

sikker programmering

systemadministration som fag - professionel drift af it-systemer

it-sikkerhedsledelse, evt. som en del af handelsskoler?

Man skal tidligt promovere "code of ethics", eksempelvis med udgangspunkt i CISSP ethics, SAGE "system administrators' code of ethics"

IT-sikkerhedsundervisning med certificering skal implementeres i alle IT-uddannelser, uanset om det er på EUD, KVU, MVU eller LVU niveau

5.4 Holdningsændring omkring IT-sikkerhedshændelser

Vi skal have gjort op med den tendens til at virksomheder er flove over at have været udsat for IT-sikkerhedsmæssige hændelser, kun på den måde kan vi lære af hinandens "dyrekøbte" erfaringer.

En løsning kunne være at virksomhederne som en del af årsregnskabet skal oplyse om antal IT-sikkerhedsmæssige hændelser, samt hændelsernes art og årsag. Dette kan hjælpe med til at afmystificere IT-sikkerhedsmæssige hændelser, og derved skabe større åbenhed om disse.

5.5 Databeskyttelse - borgernes sikkerhed for egne data

Små og mellemstore virksomheder der samarbejder med udlandet, og derfor også deler data med disse, har brug for viden om databeskyttelse. Det er min påstand at person data ikke håndteres på en betryggende måde i mange små og mellemstore virksomheder samt at myndighederne ikke har de ressourcer de har brug for, for at kunne gøre en reel forskel fx ifm. information, kontrol etc.

5.6 · Manglende involvering af medarbejderne

Ledelsen involverer ikke medarbejderne i deres IT-sikkerhed - og sikkerheds-politik bliver derfor en halvhjertet eftertanke.

Sikkerhed i virksomhederne er et spørgsmål for teknikere

Den manglende forankring hos ledelsen hænger ofte sammen med den økonomiske udgift ved indførelse af bedre sikkerhed

Ledelsen ved for lidt om sikkerhed.

Den største udfordring for it-chefen og den sikkerhedsansvarlige er ansattes brug af mailprogrammer og regulering/understøttelse af de ansattes adfærd i en sikkerhedsmæssig fornuftig retning.

Nej - jeg er uenig. Den største udfordring er efterhånden blevet de ansattes brug af en browser. Spyware kommer denne vej ind uden eller med meget begrænset interaktion fra brugerne

Har man ikke i en virksomhed fastlagt en sikkerhedspolitik ved den enkelte ansatte ikke så nemt om han/hun gør noget forkert.

Sikkerhedspolitikken er selvfølgelig vital som fundament, men etableringen af en "fin" sikkerhedspolitik er ikke nok. Brugerne (og ledelsen) bliver ikke konsekvent "tvunget" til at fokus på sikkerhed.

Sikkerhedspoltikken fastlægges ofte først når der er sket skader.

5.7 SPAM-problemet

SPAM kan bekæmpes effektivt ved retlige sanktioner imod misbrugere af kommmunikationsmidler og en god håndhævelse., men der mangler politisk initiativ til skabelse internationale åbne standarder, der kan befordre håndhævelsen bedre end den eksisterende basale SMTP samt internationalt samarbejde i håndhævelsen.

Der er fremskridt i SPAM bekæmpelsen i en række lande hvor der er fokus på lovgivning og retshåndhævelse - men desværre er problemet internationalt. SPAM afsenderne har blot flyttet afsender-systemerne videre til lande som endnu ikke

har samme lovgivning og håndhævelse. Der er behov for et internationalt regelsæt på området - og for sanktioner (afkobling/filtre?) overfor de lande som ikke griber ind,

De gode spamfiltre er blevet rigtigt gode. Men desværre ser vi nu en tendens i retning af, at legitme afsendere af massemails skal til at betale for godkendelse. Se fx sagerne om AOL og Yahoo. Dette vil grundlæggende være en bombe under e-mail som vi kender det i dag og skal bekæmpes

5.8 Der er brug for noget andet en "Netsikker.nu" - folkeoplysning på alle leder og kanter

Lad netsikker.nu - udbrede sig til virksomhederne også - således at der er sammenhæng mellem folkeoplysning

ENISA planlægger i 2007 at lave en fælles europæisk netsikkerhed dag - spørgsmålet er, om dette vil være nok til at skabe den fornødne awareness? Tvivler herpå, da NIS er noget som man skal tænke på hverdag hver time...

Sikkerhed er noget man gør, god sikkerhed kommer fra langsigtede initiativer.

En dag er således ikke nok, det skal være en holdningsændring, men gerne mere materiale som www.stophacking.dk - men integreret i undervisningen

Der skal sættes ind allerede i skolen - eller tidligere - med oplysning om sikkerhed, hvis vi skal gøres os håb om at skabe en egentlig it-sikkerhedskultur. Og det tager år...

Klart at folkeskolen bør være et opdrejningspunkt - derfor undrer det, at der ikke er systematisk "it-sikkerheds" undervisning i skolerne - der er fast undervisning og kampagner finansieret af det offentlige omkring trafiksikkerhed og omkring andre af livets mere udfordrende sider --- men it-sikkerhed?

5.9 · ISP'erne sover i timen

ISP'erne er for dårlige til at koordinere indsatsen. Der samarbejdes for lidt når der sker store angreb (fx. ormeangreb på bestemte porte).

5.10 Rapportering til ledelsen på deres præmisser

Hvad er aktuelle informationer for ledelsen? Valg af terminologi? Eksempelvis:

- Styringsmæssige forhold (politikker og retningslinier)?

- Risikovurderinger/-betragtninger?

- Kritiske hændelser?

- Resultater af complianceaktiviteter?

5.11 Pressen ønsker kun skandaler - ingen information

Delvist rigtigt - det er markant vanskeligere at komme igennem med negative historier frem for positive. Det der er behov for er uddannelse af journalister til at se de gode historier i it-sikkerhed.

man kan ikke styre journalistikken - selv uddannelse vil ikke ændre holdningen til "de gode historier"

Uddannelse i it-sikkerhed for brugere af internettet bør ske allerede i folkeskolen. På den måde vil sider af en sikkeradfærd vokse sig frem i befolkningen.

Ja - allerede i folkeskolen. Men ikke som et fag - som noget, der hel tiden skal tænkes ind og være der som en naturlig del af brugen af en pc. Lærernes uddannelsesniveau på dette område er dog rystende ringe. Selv hos dem med det pædagogiske pc-kørekort.

Enig. Journalister har da aldrig arbejdet for 'folkeoplysning'. I stedet bør det være andre gruppers opgave, at forme it-sikkerhedsstoffet, så det er mere interessant at vinkle for journalister

Pressen er én af grundene til at kløften gøres dybere imellem folk som kan vurdere en problemstilling og forholde sig til den og folk som må følge flokinstinktet og "trække i den mentale nødbremse". På sigt er det et problem for samfundet, hvis opinionen styres af følelser frem for af fakta.

Sikkerhedsspecialisterne har en stor opgave i at kommunikere budskaber på pædagogisk og meget let forståelig måde - så journalisterne (og læserne) kan få størst mulig udbytte.

5.12 Åbenhed overfor interessenter (kunder, samarbejdspartnere, investorer)

Hvor åben kan man være omkring it-sikkerhedsstyringen overfor de forskellige interessenter? Hvad forventer de forskellige modtagere:

- investorer?

- kunder?

- samarbejdspartnere?

Hvad skal der stå om it-sikkerhedsstyring i årsberetningen?

Skal virksomhedens it-risikoprofil offentliggøres? Svarende til oplysninger om fx markedsrisiko?

Er det muligt at være åben og ærlig omkring aktuelle sikkerhedsforanstaltninger og hændelser?

5.13 Et flertal af almindelige brugere er ikke specielt interesseret i sikkerhed

Desværre ikke - men hvordan kan vi få dem til at forstå, at de bør være det...

Sikkerhed skal gøres forståeligt for den almindelige bruger - også førend uheldet er ude

5.14 Manglende IT sikkerhed hæmmer SMV'ernes vækst.

Det kræver stadigt stor IT viden at anvende IT erhvervsmæssigt (og privat); men for en lille virksomhed er det fatalt at blive ramt.

Dette gælder hvad enten det er et hackerangreb eller et nedbrud.

Ofte er man dog bevidst om problemet, men nedprioriterer det af ressourcemæssige grunde.

Organisationerne bør hjælpe deres medlemmer med fagspecifikke løsninger - selvfølgelig udviklet ud fra krav om åbne standarder, SOA osv.

IT-sikkerhed kunne implementeres i projekter om. f.eks. e-business, som mange SMV´ere stadig ikke er kommet i gang med.

SMV står i mange henseender i samme situationer som den almindelige borger, når det gælder manglende viden om it-sikkerhed. For de SMV har det blot nogle endnu større konsekvenser

Eller det bliver nedprioteret pga. manglende viden: hvis man har en firewall og noget antivirus så er den potte vel ude! Men at serverne står i et hjørne i receptionen og at leverandøren ringer ind via et modem regnes ikke som et sikkerhedsproblem

5.15 Ulven kommer effekt er farlig

Det er vigtigt at sikkerhedsproblemer er relevante og aktuelle, så det bliver taget alvorligt.

Men dog noget man er nødt til at leve med da pressen altid vil have denne dagsorden

5.16 · Hackerne er snu

Hackere og andre angribere er bedre til at dele viden end ofrene.

Hackere er ikke per definition snu, men det er for let at hacke

Der skal udbredes mere information om hacking generelt, vi skal lære folk at hacke tidligt i uddannelsessystemet.

Give afløb for det, samt lære folk hvordan de dernæst beskytter sig!

Samtidig en holdningsændring at hacking er hærværk/tyveri - de fleste unge opfatter det som leg og drengestreger.

5.17 Borgerne er interesseret i sikkerhed

De fleste borgere er interesseret i sikkerhed og møder den også i større eller mindre grad på deres arbejdsplads.

Hvis man på arbejdspladsen fokuserede mere på digitale løsninger ville dette forøge fokus på sikkerhed og dermed være medvirkende til øget brug af selvbetjeningsløsninger

6. Overordnede principper

6.1 Terrorpakken og borgernes retssikkerhed

Dette tema viser hvor galt det kan gå i debatten. Det er for let at opstille skræmmebilleder, der endda hjælper til at holde på den politiske magt. Bl.a. fordi sikkerhed kan gøres til en meget simpel sag, der kan forstås af enhver, uagtet at det reelle indhold er noget andet.

Proportionalitet efterlyses inden for denne problemstilling

Der er fare for en eklatant tilsidesættelse af borgernes retssikkerhed

Politikerne "gør noget" for folket - Sikkerheds/pricacy folket - snakker om "spøgelser", som folk ikke kan se.

Politikerne gør IKKE noget for folket. De har fundet ud af, at der er stemmer i, at fremmane skræmmebilleder, som man efterfølgende kan vise sig handlekraftig i forhold til. I de tidligere øststater var der meget lidt kriminalitet. Men det kan og må ikke være en vej for det danske samfund

Endvidere er det MEGET lidt sandsynligt, at de foreslåede overvågningsmuligheder i forbindelse med logning rent faktisk vil give en effekt. Der er ganske enkelt for mange huller i reguleringen. Og skal disse huller udfyldes, er vi i sandhed ikke længere bare "på vej" mod en politistat.

Ja... et eksempel er jo åbne WiFi ap. Hvem logger "terroristen", der holder på en villavej?

Retssikkerheden er der mange der kigger på, men vi tænker mere på bremserne end på speederen. Det hæmmer udviklingen. Mere fokus på konkrete problemer.

6.2 privatlivsbeskyttelse

Opstilles ofte som modsætning til sikkerhed

Hovedparten af danskere har intet imod overvågning, når det kan medvirke til bekæmpelse af kriminalitet eller frygt. Der mangler dog politisk vilje.

Politisk vilje til hvad? mere overvågning?.. overvågning er en afmagtsstrategi / symptomstrategi, og med meget lidt dokumenteret effekt

Mange danskere, der efter sigende har det ok med overvågning, kan ikke gennemskue hvad de forholder sig til. Overvågning er ikke 0 eller 1 men en gradvis udvikling, der - hvis vi pludselige kommer for langt - kan have uoverstigelige konsekvenser

Et demokrati er kendetegnet ved, at der er grænser for statsmagtens indtrængen i det private.. hvis politiets hensyn overtrumfer alt andet.. ja så er vi en politistat

Sikkerhed har også et følelsesbetonet element. Hvis man pludselig stiger af følelsesmæssige grunde, er det også et sikkerhedsmæssigt problem

6.3 Stadig mere IT-kriminalitet er økonomisk motiveret

For få år siden var meget IT-kriminalitet baseret på at vise at det var muligt - at lave en orm/virus eller bryde ind i et system.

Men f.eks. spam er et tegn på at de samme teknologiske problemer nu bruges at nogle få (20-40) men slagkraftige organisationer til at tjene penge. Udsendelsen af spam er proportional med modtagernes købekraft og en væsentlig del er derfor målrettet den vestlige verden og specielt USA.

Denne udvikling er farlig da indtægten fra disse aktiviteter vil muliggøre og inspirere nye og kraftige angreb.

6.4 Hvordan skal ansvaret for it-sikkerhed placeres?

Hvordan placeres ansvaret for it-sikkerhed optimalt i virksomheden?

Placering af sikkerhedsansvar - hvis virksomheder/organisationer ikke får den øverste ledelses opbakning, så har man et kæmpeproblem

Fx ansvar for it-sikkerheden mht:

- tilrettelæggelse (politikker, retningslinier, risikovurderinger=

- teknik

- administration

- opfølgning og kontrol, herunder behandling af hændelser

Operationel risikostyring omfatter menneskelige fejl, procesfejl, systemfejl og udefra kommende hændelser. Er it-sikkerhedsstyring ikke blot en del af dette fagområde?

Bør ansvaret for tilrettelæggelse (ikke udførelse) af it-sikkerhed organisatorisk placeres sammen med fysisk sikkerhed, business continuity, compliance, herunder løbende kontrol og opfølgning?

Det er ledelsens ansvar at sørge for at IT-sikkerhed implementeres. Ledelsen skal ikke nødvendigvis være aktiv i udførslen

Fører en centralistisk sikkerhed til mindre awareness hos de aktuelle brugere? Bevirker det på lang sigt en fremmedgørelse over for sikkerhedsproblemer hos den enkelte ansatte

6.5 Hvordan sikres borgerne indsigt i hvilke oplysninger det offentlige har og hvad de bruges til

6.6 Brug for holistisk tænkning

Et problem er, at man ikke tænker holistisk nok når man tænker sikkerhed - derfor vil de kriminelle altid vinde. Dem der designer løsningerne tænker ikke over: Social engineering, intern chikane (ie. på grund af ophørt arbejdsforhold) etc. Og den der tænker fysisk sikkerhed tænker ikke over logisk sikkerhed ... etc.

Derfor er der brug for langt mere holistisk tænkning...

Især fordi løsningerne på sikkerhedsproblemer altid kræver en række forskellige aktører skal samarbejde - ofte på en måde de ikke er vandt til

Start med at tænke Identifikation = Sikkerhedsrisiko og primært -trussel

a) Vi kan ikke identificere sikkert (aldrig)

b) Selv hvis vi kunne ville det føre til et ikke-demokratisk samfund.

Hvor kommer det ikke-demokratiske ind henne? Det er ikke Angola som vi lever i?

6.7 Hvordan identificerer borgerne sig elektronisk på en entydig og sikker måde?

Identifikation er ikke målet, fordi det ødelægger kontekst og dermed skaber risiko for sekundær kriminalitet.

Det reelle problem er hvordan sikrer man at det kan fastslås hvem brugeren er og i hvilken rolle han deltager - det er forskellige muligheder man skal give en ansat, en familie mor, og en foreningskasser

6.8 Der er behov for standardiserede benchmark af it-sikkerhed på tværs af EU

Hvordan er de enkelte landes it-sikkerhedsmæssige udfordringer håndteret - og vil det være muligt at se hvor de gode vs de dårlige lande befinder sig - tør vi stole på en betalingsgateway der står i Italien velvidende at man ikke ved hvordan deres praksis er med hensyn til sikkerhed af personoplysninger etc...

6.9 Manglende standardisering på åbne standarder betyder øget sikkerhedsrisiko for den offentlige sektor

6.10 Der mangler ofte mulighed for at få en bekræftelse ved selvbetjeningssystemer

Ved selvbetjeningssystemer - både telefoni og internet baserede - er der ofte ikke mulighed for at få en bekræftelse på at en inddatering er modtaget. Det betyder at hvis man f.eks. har indrapporteret el-forbrug ikke kan bevise at man har foretaget indrapporteringen, og kan blive pålagt et gebyr etc.

Dette er et problem for den enkelte borgers retssikkerhed, som vedkommende ikke selv har mulighed for at påvirke.

6.11 Der bør etableres et landsdækkende videoovervågningsnetværk for proaktivt hindre kriminalitet og terror

Stop så med al den terrorsnak. Lige fra den amerikanske præsiden til vores egen justitsminister tales der om ´terror rundt om hvert et hjørne'. Den retorik og politiske dagsorden er syg, gavner terroristerne og er i sig selv en betydelig sikkerhedsmæssige udfordring.

Hørt !

Ikke enig - erfaringerne fra London og Madrid taler for sig selv - det er alene mennesker som er bange for retssamfundet som vil føle sig truet af øget overvågning.

åh det gamle "rent mel i posen" argument.. det er grundlæggende ved et retssamfund at borgere kan leve frit, og kun overvåges hvis der er konkret mistanke..

hvor går grænsen ellers.. politiet kan få adgang til alt kommunikation, just in case.. og til vores hjem... for vi har jo ikke noget at skjule..

Selv hvis vi fratrækker snakken om overvågning, kan terror ikke bekæmpes af den vej. Jo mere vi snakker om det som en 'alvorlig fare' jo mere farligt bliver det reelt. Der skal benyttes helt andre midler, der bl.a. handler om dialog, sameksistens og ændret samhandel. Alt andet er symptombehandling

og så godt gammeldags politiarbejde

Videoovervågning KAN ikke sikres

6.12 Opsamling af biometriske data kan ikke sikres

Det skaber ID theft, som både underminerer systemet og personens sikkerhed.

Samtidig underminerer det datasikkerheden, fordi det fratager borgeren muligheden for selv-beskyttelse.

Spørgsmålet er, om det er nødvendigt at opsamle biometriske data andet steds end i det enkelte borgerservicekort??

Man må erkende at biometriske data ligesom et password blot er en streng af data, som kan opsamles og efterlignes.

På samme måde som man har indsat en aflytningsenhed i en dk-kort automat, kan man indsætte en aftlytningsenhed i en biometrisk skanner og herved opfange disse data. I de fleste tilgængelige løsninger kan dette ovenikøbet gøres via f.eks. bagdørsprogrammer. Og så står man med det virkelige problem - man kan skifte password og man kan få spærret sit certifikat - man vi har vel ikke løst til at få udskiftet iris eller fingeraftryk

Basalt set et biometri en niche løsning og ikke et bredt svar på identifikationsproblemet

6.13 Open Metropolis er vejen frem

Det gamle sikkerhedsparadigme "Walled Gardens" eller Feudal Sikkerhed byggende på Identifikation og overvågning skaber kun illusionen af sikkerhed mod kriminelle, mens det gradvist øger sikkerhedsrisici og går det nemmere for kriminelle at angribe systemerne.

I stedet peger sikkerhedsforskningen i EU-regi på Open Metropolis, dvs. at låse data til kontekst, hvorefter de kan deles med væsentlige mindre sikkerhedsrisiko.

Et vigtigt punkt er forståelsen af at sikkerheden ligger i hvordan man kan holde involverede parter ansvarlige for deres misbrug samtidig med at det beskytter borgerne mod angreb

6.14 Hvem er udvikleren i Indien loyal overfor?

I Danmark har vi en homogen kultur og en udviklet samfundsstruktur som vi støtter vore risikovurderinger på. Igennem globalisering uddelegerer vi også vores kontrol,- dette indgår ikke i de business cases som udgør beslutningsgrundlaget. Organiseret kriminalitet skal bare finde kædens svageste led,- hvorhenne i verden det nu findes.

6.15 Mangler vi en positivliste for IT-løsninger der SKAL kunne samkøres?

Her tænkes ikke så meget på almindelige administrative systemer men på de systemer, der skal kunne bringes til at fungere sammen i katastrofesituationer. Dette kan man kalde IT sikkerhed med en universalnøgle. Brandvæsen, politi, private virksomheders alarmsystemer, Securitas, skibstransport ... Dette løses ikke ved et (forældet) Tetranet, men ved indførelse f.eks. af krav til åbne standarder for adressebøger, så løsningerne i den aktuelle situation faktisk KAN tale med hinanden. Det sker ikke i dag. At Seest-ulykken ikke fik større konsekvenser er et mirakel.

6.16 I hvilket land gemmer de værste IT kriminelle sig for tiden?

Verden er en meget sammensat størrelse. Vi snakker om en global landsby, men Muhammed tegningerne illustrerede vel at vi ikke altid forstår hinanden fuldt ud :-)

IT kriminalitet er verdensomspændende, - hvordan får vi hævet standarden over hele verden?

6.17 Sikkerhed er ikke en endimensional størrelse

For meget sikkerhedsdebat tager udgangspunkt i en forsimplet tilgang til sikkerhed.

Man glemmer at det ikke giver mening at snakke "sikkerhed" uden at definere for hvem og imod hvilken trussel.

For mange tiltag resulterer derfor i "mere sikkerhed" for nogle enkelte, men "mindre sikkerhed" for mange.

6.18 Om at løfte i flok

Et af de største problemer med IT Sikkerhed i virksomheder er af få organisationen modnet så den understøtter en "risk-management" tilgang.

Ud over rammer (scope) for ønsket sikkerhed er en væsentligt parameter at få opbygget en organisation der understøtter sikkerheden fra de øverste strategiske beslutninger (Nørby udvalget) til implementering og kontrol.

Løsning! En ud af mange løsninger er til stadighed organisationsarbejde og evne til at trænge igennem i organisationen. IT sikkerhed handler i sidste ende om "business risk management" .

Et bud kan være at have en Business risk & security director der evner at bringe de nødvendige temaer på banen og argumentere for ressourcer

Risk-management fører sommetider til risk-avoidance altså en foreliggende tilstand. Der er behov for at kigge på de positive efter af risk (e.g. first move) for at få en sund forretning. Selv i risk-management er der behov for gambling

6.19 Walled Gardens er ikke holdbar

Hvordan defineres perimeter?

Walled gardens er tankegangen om at vi via adgangskontrol og firewalls kan beskytte data efter de er opsamlet. Det er en ikke holdbar filosofi

6.20 Videoovervågning af offentlige pladser medfører behov for privacy-regulering

Kan videoovervågning virke terroristhæmmende eller er det blot et middel til efterfølgende af dokumentere forløbet?

Prioritering af problemerne

Følgende er resultatet af den afstemning, der fandt sted umiddelbart efter den ovenfor dokumenterede brainstorm for at prioritere de væsentligste problemer. Hver deltager havde to stemmer indenfor hver hovedkategori, og kunne maksimalt bruge een stemme pr. problem. 33 deltagere deltog i afstemningen.

1. Regulering og standarder	
Problemer	Total
1.1 Standardisering af it-sikkerhed på tværs af samfundet	11
1.2 ISP´erne gør ikke nok for sikkerheden	6
1.3 · Mangel på politisk fokus	5
1.4 Kontrollerbar sikkerhed skal indgå som et krav i offentlige udbud af kritisk national infrastruktur	5
1.5 Tryghed for borgeren i tilfælde af misbrug af dennes digitale signatur (el. andet digitalt identifikationsmiddel)	5
1.6 Balance mellem effektiv offentlig administration og borgerens retssikkerhed eller tryghed ved det offentliges behandling af personlige data	4
1.7 Fællesoffentlige standarder og politikker på tværs af organisationer	3
1.8 Lovgivning om ansvar i forbindelse med manglende IT-sikkerhed	3
1.9 Behov for en langt stærkere tilstedeværelse af danske normer og bidrag til standardisering	2
1.10 Offentlige IT-indkøb bør tilstræbe fælles åbne standarder men ellers modarbejde monokultur indenfor kode og platforme	2
1.11 Lovgivningen skal sikre distribution af kontrol og risiko	2
1.12 Opret et egentligt Internet Politi	2
1.13 Internationale krav	2
1.14 Terrorpakken skaber kriminalitet	2
1.15 · Man går og opfinder den dybe tallerken	1
1.16 Standardiseret it-sikkerhed i private virksomheder går trægt	1
1.17 Sikkerhed - modent problem?	1
1.18 Internettet skal reguleres FN/ILO	1
1.19 Åbne standarder bør indgå i alle offentlige IT-løsninger	1
1.20 Persondatalovgivningen er forældet	1
1.21 Mangel til lovgivning til bekæmpelse af IT-kriminalitet	1
1.22 Danmark er alt for dårligt forberedt på kraftigt voksende it-kriminalitet	1
1.23 Datatilsynet - udbygning - flere ressourcer ?	1
1.24 Skal der i det hele taget være en standard for it-sikkerhed?	1
1.25 IT kriminalitet internt i virksomheden	1
1.26 Mindre firmaer skal hjælpes til at klare it-sikkerheden	1
1.27 · For milde straffe	0
1.28 Manglende lovgivning indenfor tab af data	0
1.29 Revision af love indenfor terrorbekæmpelse og logning	0
1.30 Behov for et SIKKERT internet parallelt med det USIKRE	0
1.31 Revision af aftalelovgivning	0

2. Systemudvikling	
Problemer	Total
2.1 · Diffust ansvar	8
2.2 Manglende sammentænkning mellem it-arkitektur og sikkerhed	8
2.3 Én sikker elektronisk ID,- skridt for skridt	8
2.4 Sikre systemer "out of the box"	5
2.5 · Dårlig uddannelse	4
2.6 Sikkerhed koster - og der er ingen der er villige til at betale hvad det koster - fordi de ikke kender konsekvenserne	4
2.7 organiseret økonomisk kriminalitet	4
2.8 Brugervenlighed vs. sikkerhed	4
2.9 Web-udvikleres it-sikkerhedskultur og viden er ofte utilstrækkelig	3
2.10 Sikkerhed i den Serviceorienterede arkitektur - et upåagtet problem?	3
2.11 For lidt fokus på rettigheder	3
2.12 Systemansvar for IT produkter	2
2.13 · Manglende offentlighed	1
2.14 Ministerierne laver hver deres sikkerhedsløsning.	1
2.15 Er it-sikkerheden til stadighed ok i systemer, som udvikles af en serviceprovider?	1
2.16 Enterprise Arkitektur og hermed risikovurdering og sikkerhedsløsninger - ikke IT-arkitektur - skal være ledelsens ansvar	0
3. Teknik og infrastruktur	
Problemer	Total
3.1 Email - få det nu fikset!	5
3.2 Digital Authentikering	5
3.3 Et fælles nøglekort for den offentlige sektor og finanssektoren bremses af manglende politisk samtænkning	4
3.4 Terror mod infrastruktur	4
3.5 Der fokuseres for meget på identifikation af personer, og for lidt på hvilken rolle personen spiller i interaktionen med et system	4
3.6 Løsninger er for komplicerede at bruge	4
3.7 Der mangler en standard for sikring af privatejet kritisk national infrastruktur	4
3.8 Manglende it-sikkerhed skaber ganske store socioøkonomiske udfordringer - som bliver større og større for hvert eneste år!	3
3.9 Behov for at IT-sikkerhed er tilgodeset i nye teknologier	3
3.10 "DRM" kompromiterer borgernes sikkerhed	3
3.11 virus, virus, virus, virus, virus, Trojanske heste og andre skadevoldende programmer	3
3.12 · Kritisk software står pivåben	2
3.13 Et Borgerkort er IKKE et Identifikationskort	2
3.14 SPIM - et fremtidigt problem ved VoIP.	2

3.15 En global verden giver globale udfordringer	2
3.16 Der mangler reel end-to-end sikkerhed	2
3.17 Trusted Computing fører til fjernkontrol af borgerne - typisk udenlandsk og kommercielt betinget	2
3.18 · Nettet er outdated	1
3.19 Perimeter sikkerhed fejlet	1
3.20 Dårlige passwords giver mange problemer	1
3.21 Teknologien skal anvendes til at skabe den sikkerhed som den almindelige bruger ikke kan forstå	1
3.22 Fællesoffentlig brugerstyring	1
3.23 Bagdøre udnyttes af kriminelle	1
3.24 Kriminelle vil angribe almindelige pc'er i stadigt større omfang	1
3.25 Identifikation der baserer sig på at brugers pc er sikker kan blive undermineret	1
3.26 Dynamisk Sikkerhedsstyring	1
3.27 IT-sikkerhed ved biometri/rfid og andre nye teknologier	0
3.28 Transparens skaber sårbarhed	0
3.29 Automatisk opdatering af programmer	0
3.30 Dårlig backup kultur - mange tager for sjældent backup	0
3.31 Er behandling af it-sikkerhedshændelser/-alarmer dækkende og betryggende?	0
3.32 Seks ud af 10 offentlige virksomheder har ikke opdateret it-beredskab (ifølge Danmarks Statistik)	0
3.33 Fiberinfrastrukturen bør integreres	0
3.34 Ingen servicer-side Single Signon	0
3.35 Konvergens og nye bærbare applikationer skaber nye sikkerhedsproblemer	0
4. Viden og adfærd	
Problemer	Total
4.1 Almindelige brugere lades i stikken	10
4.2 IT sikkerhedshjælp til små og mellemstore virksomheder vil fremme globalisering og innovation	10
4.3 Hvorfor tænker Digital Forvaltning aldrig sikkerhed?	7
4.4 IT-sikkerhed i hjemmet	6
4.5 Hvor går den menige dansker hen og får viden om hvordan han beskytter sin PC'er?	6
4.6 Der skal fokuseres på vigtige problemer og der skal være proportionalitet mellem problemets alvorlighed og løsningerne	4
4.7 · Svært at skelne mellem store og små problemer	3
4.8 It-sikkerhed skal gøres lettere at forstå	3
4.9 Børn og Unge lærer ikke om behovet for sikkerhed.	3
4.10 Kompromiterede hjemme-computere	3
4.11 Hvem certificerer sikkerhedsløsninger?	2
4.12 Det Offentlige, undervisningssektoren og de private virksomheder har berøring med de fleste borgere i Danmark	2
4.13 · Sikkerhedssoftware er for svært at bruge	1
4.14 Vi mangler forskning i hvordan hr. og fru Hansen opfatter IT-sikkerhed	1
4.15 Jo højere lønramme, jo større risikoadfærd indenfor IT-sikkerhed	1
4.16 Trust = Accept af risiko i kontekst - Identifikation skaber DISTRUST	1

4.17 Hvor mange folketingsmedlemmer er bekendt med problemet om IT sikkerhed?	1
4.18 · Lemming effekten	0
4.19 "Unsafe at any speed" - for Internetanvendelse	0

5. Kommunikation og vidensdeling

Problemer	Total
5.1 Oplysning på linie med folkesundhed eller trafiksikkerhed	13
5.2 Borgerne er interesserede i at være sikre - men ikke i sikkerhed	7
5.3 Uddannelser indenfor IT-sikkerhed mangler på universiteter og andre steder	7
5.4 Holdningsændring omkring IT-sikkerhedshændelser	6
5.5 Databeskyttelse - borgernes sikkerhed for egne data	5
5.6 · Manglende involvering af medarbejderne	4
5.7 SPAM-problemet	4
5.8 Der er brug for noget andet end "Netsikker.nu" - folkeoplysning på alle leder og kanter	4
5.9 · ISP'erne sover i timen	3
5.10 Rapportering til ledelsen på deres præmisser	3
5.11 Pressen ønsker kun skandaler - ingen information	3
5.12 Åbenhed overfor interessenter (kunder, samarbejdspartnere, investorer)	2
5.13 Et flertal af almindelige brugere er ikke specielt interesseret i sikkerhed	2
5.14 Manglende IT sikkerhed hæmmer SMV'ernes vækst.	1
5.15 Ulven kommer effekt er farlig	1
5.16 · Hackerne er snu	0
5.17 Borgerne er interesserede i sikkerhed	0

6. Overordnede principper

Problemer	Total
6.1 Terrorpakken og borgernes retssikkerhed	10
6.2 Privatlivsbeskyttelse	9
6.3 Stadigt mere IT-kriminalitet er økonomisk motiveret	8
6.4 Hvordan skal ansvaret for it-sikkerhed placeres?	7
6.5 Hvordan sikres borgerne indsigt i hvilke oplysninger det offentlige har og hvad de bruges til	5
6.6 Brug for holistisk tænkning	4
6.7 Hvordan identificerer borgerne sig elektronisk på en entydig og sikker måde?	4
6.8 Der er behov for standardiserede benchmark af it-sikkerhed på tværs af EU	3
6.9 Manglende standardisering på åbne standarder betyder øget sikkerhedsrisiko for den offentlige sektor	3
6.10 Der mangler ofte mulighed for at få en bekræftelse ved selvbetjeningssystemer	2
6.11 Der bør etableres et landsdækkende videoovervågningsnetværk for proaktivt hindre kriminalitet og terror	2
6.12 Opsamling af biometriske data kan ikke sikres	2
6.13 Open Metropolis er vejen frem	2

6.14 Hvem er udvikleren i Indien loyal overfor?	1
6.15 Mangler vi en positivliste for IT-løsninger der SKAL kunne samkøres?	1
6.16 I hvilket land gemmer de værste IT kriminelle sig for tiden?	1
6.17 Sikkerhed er ikke en endimensional størrelse	1
6.18 Om at løfte i flok	0
6.19 Walled Gardens er ikke holdbar	0
6.20 Videoovervågning af offentlige pladser medfører behov for privacy-regulering	0

Fase 2: Bearbejdning af de højest prioriterede problemer i hver kategori

I denne fase blev deltagerne fordelt i grupper, der hver især havde til opgave at uddybe og komme med løsningsforslag til de problemer, der blev højest prioriteret i fase 1. De problemer, der landede på første, anden og tredjepladsen efter afstemningen gik videre til Fase 2, og delte tredjepladser er årsagen til, at der ikke er lige mange problemer under hver kategori.

Deltagerne blev bedt om at svare på følgende:

- Beskriv problemet så præcist som muligt!
- Hvad kan en løsning være?
- Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt!)?
- Hvordan hænger problemet evt. sammen med andre problemer, som har været behandlet i dag?

Nedenstående er resultatet af gruppearbejdet samt kommentarer fra de øvrige deltagere. For hvert af de prioriterede problemer gentages først den oprindelige problembeskrivelse og kommentarer fra brainstormen i Fase 1. Derefter følger bearbejdningen gennem gruppearbejde samt kommentarer fra de øvrige deltagere. Ikke alle grupper nåede at bearbejde alle spørgsmål.

1. REGULERING OG STANDARDER

1.1 Standardisering af it-sikkerhed på tværs af samfundet (11 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

For at kunne vurdere it-sikkerhedsniveauet på tværs af organisationer og ikke mindst i forholdet til samarbejdspartnere er det vigtigt at tale samme "sprog" dvs. anvende samme eller sammenlignelige standarder i beskrivelse af it-sikkerhed.

Det statslige system har påbegyndt dette ved at kræve at alle statslige institutioner anvender samme standard for it-sikkerhedsprocesser, DS484:2005.

Denne version er direkte sammenlignelig med ISO17799:2005.

En form for certificering kan være nødvendig hvis roller skal kunne bæres fra et IT-miljø til et andet. F.eks. sygehusdata der skal accesses af en kommunal sygeplejerske.

DS484:2005 bør være et krav for samtlige offentlige myndigheder.

Standarder skal være enkle og forståelige for menigmand ellers henvises til en fælles ubekendt referenceramme

Der mangler et niveauopdelt sæt spilleregler. Der bør kunne kræves væsentligt mere af professionelle brugere end af privatpersoner (som til gengæld har brug for mere hjælp).

Kort! DS484 bør erstattes med ISO27001 da vi i en globaliseret verden ikke kan få nok effekt af en lokal dansk efterligning af en international sikkerhedsstandard.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

1.1.1 Beskriv problemet så præcist som muligt

Vi mangler level of trust

Arbejde ikke med lukkede standarder

Problemet er at vi fokuserer på centrale løsninger og f.eks. er de 5 første prioriteter på listen problemer der adresserer statsløsninger og ikke tager udgangspunkt i brugere og borgere.

Beskrivelse af et standardiseret sprog

Problemet er at der ikke er en ensartet standard - internationalt

Problemet er at der hersker anarki på området

Standardisering giver et framework for hvad man skal rette sig efter og ikke mindst kan ens samarbejdspartner se, hvad man lever op til. Men det kræver et sign-af at man også lever op til standarden

1.1.2 Hvad kan en løsning være?

Vedkende sig en standard som alle kan bakke op om og så den er teknologiuafhængig - åben for flere modeller.

Arbejde for at udvikle paradigmer for sikkerhed som kan danne grundlag for et overblik over de særlige sikkerhedsproblemet knyttet til fx web services som er ved at udvikle sig til et vækstområde.

Åbne Standarder må være en forudsætning for alle løsninger i den offentlige sektor. Omkostningerne ved fortsat at basere sig på Microsoft standarder for digitale dokumentformater, regneark og ikke mindst A/D (directories) kan vise sig sikkerhedsmæssigt at være meget store. Der findes for alle områder i dag velafprøvede standarder, der ikke ejes af et enkelt firma og som derfor kan behandles sikkerhedsmæssigt forsvarligt, krypteres, sendes etc.

Virksomheder, stat, regioner, kommuner skal stille krav til deres it-driftsleverandører om efterlevelse af ISO27001. Den er international og anerkendt, og på trods af enkelte uhensigtsmæssigheder er den bedst bud på en standard alle burde kræves at følge.

At sikre at standarden er af international karakter så danske virksomheder ikke kun tilgodeser nationale krav men også øger sin konkurrenceevne i forholdet til udenlandske kunder.

At IT og telestyrelsen / økonomistyrelsen udarbejder sammenhænge mellem den nationale sikkerhedsstandard DS484 og udenlandske standarder således at nationale krav kan tilgodeses via en international standard.

Benytte internationalt godkendte standarder og regelværk. ISO27001, ISF's Standard of Good Practice for Information Security, COBIT + få verificeret, at man lever op til de standarder, som man påberåber sig at overholde.

Regulere at Borgerne EJER egne data og at reguleringen skal indrettes så de kan opretholde denne kontrol via Identity management

1.1.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Den offentlige sektor er på vej med DS484. Statens institutioner er ved at implementere og når strukturreformen er gennemført vil kommunerne påbegynde implementeringen af DS484. Nogle kommuner er allerede i gang, resten kommer i løbet af de næste år.

Man kan forstille sig at kravene fra den offentlige sektor til leverandører vil indeholde krav om IT-sikkerhed svarende til den offentlige institutions egen sikkerhed. Dette vil over tid bidrage til at skabe fælles standarder i både privat og offentlig sektor. Fælles standarder skal tage højde for, at der er behov for forskellige sikkerhedsniveauer i forskellige institutioner/virksomheder og for forskellige ydelser. Derfor er kravet om standardisering af IT-sikkerhed på tværs af samfundet måske lige rigeligt bombastisk.

IT og telestyrelsen

Økonomistyrelsen

1.2 ISP´erne gør ikke nok for sikkerheden (6 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

ISP´erne har i dag gjort meget for at dæmme op for spamproblemet. Men stort set alle andre områder er goldt land.

"Almindelige mennesker" har ingen reel chance for at sætte sig ind i sikkerhed i forbindelse med deres internetforbindelser. De fleste i dag ved, at de bør have et antivirus-program og en firewall. Men de færreste kan finde ud af at konfigurere og opdatere disse. ISP´erne gør meget lidt for at afhjælpe dette problem - og når de gør, er det i form af dyre tilkøbspakker. Dette på trods af, at den manglende sikkerhed ofte går ud over mange andre abonnenter hos samme ISP.

Ofte bliver hele ip-ranges spærret i andre netværk pga. bot-nets o.lign. (medfører fx spam fra ip-adresser). Dette betyder at helt legitim kommunikation fra helt uskyldige firmaer og private spærres pga. andres problemer.

Der findes ingen mærkningsordninger eller standarder for ISP´ernes sikkerhedsniveau.

Man kan sætte krav til at ISP'er rettet mod private (eller alle ISP'er?) altid har mindst en sikkerhedsløsning. Det kunne være en filtreret forbindelse med e-mail via ISP'ens mail server - de store ISP'er har denne løsning og det skulle være et valg man foretager når man køber en forbindelse, gerne med sikkerhedspakken som standardløsningen. NB: det er ikke en opfordring til generel filtrering af internetforbindelser - men et specifikt produkt, der kan vælges fra

ISP'erne ejer netværket og linierne - det er ikke deres ansvar at sikre systemerne i enderne.

Kunderne erkender ikke at udstyr, der skal på Internettet, skal hærdes - først

Alle og enhver kan nedsætte sig som ISP eller webhotel, og det gør at prisen på disse services ofte bliver den største konkurrenceparameter, fordi de dårligste ISP/webhoteller sælger "for billigt" - blandt andet fordi de ignorerer sikkerhed.

Der er forskel på situationen med privatpersoners og professionelles brug af Internettet. De professionelle brugere bør selv kunne klare en del af de sikkerhedsmæssige risici, hvorimod privatbrugerne har behov for at kunne få bistand fra bl.a. ISP'ere - og gerne som default.

Hvem skal betegnes som ISPér?

der er tre parter der har et ansvar: isp'ere, sw-producenter, og brugere. (brugere inkluderer private og virksomheder/stat/region/kommune

Kodeks for ISP'er bør udbygges

ISP'er bør tilbyde kunder en filtrering så de kan få adgang til enten dele af Internettet eller bestemte typer www sites (horisontalt eller vertikalt)

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

1.2.1 Beskriv problemet så præcist som muligt

Det er for nemt at afsende spammails og da folk ikke er gode nok til selv at opbygge sikkerhed og kender til løsningen, så privatbrugere skal isp'erne give værktøjer, sikkerhedspakke, have et ansvar, mens hos professionelle brugere gælder der andre forhold.

Vi kan ikke filtrere os ud af problemet.

1.2.2 Hvad kan en løsning være?

ISP-ere kan IKKE løse sikkerhedsproblemer - de kan højst stille sikkerhedsværktøjer til rådighed.

Overvågning og filtrering er uholdbart som tilgang til sikkerhed

1.2.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

1.3 · Mangel på politisk fokus (5 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Internettet er anarkistisk og ikke tilstrækkeligt politisk reguleret. Der mangler politisk fokus og ansvar for it-sikkerhed.

Hvad er den politiske løsning ? der er masser af politisk fokus men afmagt ift. at overskue hvad der skal gøres

IT-sikkerhed bør være den enkeltes ansvar

Det er ikke nok at individualisere problemet - derved har mna givet op.

Anarkisme er ok men udbyderne skal enten under eget kodeks eller rammekrav

IT-sikkerhed skal deles op i Content providers og ISP'er

Politisk styring giver flere problemer ind de løser Det bliver en ørkesløs privacy-debat

Der mangler politisk fokus på efterforskningsmulighederne for politiet og midler til dette.

Der mangler politisk fokus på alvorligheden ved fx. terror eller alvorlig kriminalitet på Internettet og ved anvendelse af dette. Der skal gå noget galt, før "de" vågner op

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

1.3.1 Beskriv problemet så præcist som muligt

Er problemet ikke, at det skal politikerne heller ikke? Vi ser med antiterrorloven, at det er svært at detaillovgive på dette felt, så det skal politikerne holde sig fra.

Et it-sikkerhedsråd skal rådgive, oplyse og skabe awareness - men at forvente det samme for politikerne og ikke mindst at de skal være i løsningsmode er urealistisk

1.3.2 Hvad kan en løsning være?

1.3.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

1.4 Kontrollerbar sikkerhed skal indgå som et krav i offentlige udbud af kritisk national infrastruktur (5 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

I forbindelse med privatisering af infrastruktur så som el, tele og vand har der været fokus på at sikre konkurrence mellem udbydere. Konsekvensen har været, at sikkerhed naturligt ikke alle steder er vægtet tilstrækkeligt på trods af at samfundet er afhængig af tjenesterne.

Et eksempel herpå er teleselskabernes GSM netværk, hvor der f.eks. ikke er stillet krav til continuety i forbindelse med uddeling af licenser.

Ved udlicitering bør det offentlige derfor stille målbare krav til sikkerheden. Krav der er målbare og kan verificeres af 3. part.

Er det en løsning "blot" at kræve ds484 eller iso27001 certificering af leverandører?

Der skal arbejdes på en praktisk løsning for kontrollerbarhed, ellers ender det som det tidligere Registertilsyn med anmeldelsesordninger, som ikke giver sikkerhed men kun administrativt bøvl.

Hmm, det kan vel være lige så slemt når det er offentligt styret.

På samme måde som Finanstilsynet kræver af banker, at andre end banken selv skal sige god for regnskabet, er det vel ikke urimeligt at bede om, at andre end virksomheden selv vurderer sikkerheden op mod en standard.

Der skal være meget mere styring på de private virksomheder, som løser IT-forhold for stat og kommune. De skal afkræves garanti for kvalitet og sikkerhed af data.

Der skal samtidig føres til stadighed tilsyn med dem.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

1.4.1 Beskriv problemet så præcist som muligt

1.4.2 Hvad kan en løsning være?

Når en ydelse sættes i udbud skal der være krav til overholdelse af et vist sikkerhedsniveau og krav til beredskab og continuity.

Opfyldelse af krav skal kunne verificeres og kontrolleres.

Fællesoffentligt autentificeringscenter, f.eks. baseret på erfaringer fra sundhed.dk, der synes at fungere udmærket.

Udvikling af compliancekrav dokumenteret fra anerkendte testlaboratorier af specifikke system sammenkoblinger, etc.

Kravet til sikkerhedsniveau skal forankres i staten

En del af VTU's IT Arkitektur bør udvides til at omfatte et ledelsesmæssigt krav til enterprise arkitekturen og dokumentation af overholdelse af en fælles, offentlig og høj IT sikkerhed.

Meget vigtigt at udbuddet ikke blokeret innovation inden for sikkerhed. Typiske offentlige projekter destruerer sikkerhed og fokuserer kun på overvågning og kontrol af borgerne - hensyn til tillid og forebyggelse af sikkerhedsbrud fejler

1.4.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Beredskabsstyrelsen er i gang med at sikre, at udvalgte kritiske sektorer i samfundet kan videreføre deres kritiske samfundsfunktioner, selvom der skulle forekommer hændelser, der har betydelig indflydelse på sektorens funktion. Der er allerede nedsat grupper pr. sektor til at vurdere en række trusler, og sikre en vis robusthed, så SAMFUNDET kan fortsætte. Der er tale om et SEKTORANSVARSPRINCIP.

1.5 Tryghed for borgeren i tilfælde af misbrug af dennes digitale signatur (el. andet digitalt identifikationsmiddel) (5 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Vejen til at sikre at "digitaliseringen" virkelig får udbredelse er:

1) at der er gode digitale service-ydelser at hente på nettet.

2) at borgeren føler sig tryg ved at bruge disse.

Så længe ydelserne er upersonlige og uden mulighed for tab for brugeren er der ikke noget problem.

Men hvis borgeren risikerer

- tab af fortrolighed omkring sine væsentlige personlige data

- tab ifm. misbrug af identifikationsmiddel

- tab ifm. identitetstyveri (evt. udenfor den digitale verden) baseret på lækkede informationer i den digitale verden.

så forbliver en stor brøkdel af befolkningen utrygge og tager ikke del i digitaliseringen.

Løsning: Gode sikkerhedsforanstaltninger PLUS tryghedsskabende lovgivning

Eksisterernde løsning via OCES er utilstrækkelig og kan ikke i privat-regi konkurrere med finansverdenens net-ID, som benyttes af flere millioner danskere.

Det er til skade for borgernes sikkerhed m.v. at der ikke er etableret een løsning på området. Offentlige institutioner kræver brug af OCES, og finansverdenen kræver brug af net-ID. Hvad i alverden skal borgerne vælge!

Borgerne vil ikke tage sikkerhed alvorligt, når der ikke sættes en evt. konsekvens på.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

1.5.1 Beskriv problemet så præcist som muligt

Vi mangler en kvalificeret digital signatur for borgerne. Folk mangler at se behovet for digital signatur. Hvad er f.eks. straffen ved tyveri af dig sig. - det ved du ikke som ejer af en dig. sig.

Skadesfriholdelse a la Dankortmodellen for brugerne.

Lovgivningsmagt skal regulere det.

Hvad er en kvalificeret digital signatur?

Måske er det ikke så vigtigt med en kvalificeret digital signatur. Anvendelsen vil over tid sikre at den er troværdig. Men identitetstyveri skal begrænses.

Skadesfriholdelse er vanskelig omkring signaturen, idet det ikke er økonomiske transaktioner men dataadgang vi taler om. Vi skal stræbe efter at signaturen bliver den samlede mekanisme folk foretrækker og så modne løsningen i takt med behovet. Første barriere er ren convenience.

1.5.2 Hvad kan en løsning være?

Sikre at borgerne kan handle og kommunikere på måder, hvor de beholder kontrollen.

Dvs. med kontekstspecifikke nøgler, men UDEN at identificere sig, så data ikke kan misbruges sekundært

Det kræver også mulighed for efterspring af eventuelt misbrug, så her har vi brug for tilstrækkelig logning + muligheder for at anvende logningen.

Sørge for at hænge misbrugere ud på en offentlig hjemmeside til skræk og advarsel (kan måske være for bastant, men fx Datatilsynet og Finanstilsynet gør det for virksomheder).

1.5.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

2. SYSTEMUDVIKLING

2.1 · Diffust ansvar (8 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Med Open Source er ansvaret for it-sikkerheden svært at placere.

Ansvaret er generelt også uklart placeret i udviklingssituationer. Ofte er der slet ikke taget stilling til, hvem der er ansvarlig for sikkerhedsforhold.

Behov for såvel kvalitetssikring som klarhed på ønsket/krævet sikkerhedsniveau - under udvikling men lige så vigtigt i vedligeholdelsesfasen.

Vi skal sikre at der stilles krav til leverandørerne omkring sikkerhed i systemerne.

En række leverandører har gennem en årrække fokuseret mere på funktionalitet end på sikkerhed. Denne prioritering må ændres.

Forsikring bør indgå som en væsentlig komponent i forbindelse med ansvar for manglende IT-sikkerhed. Såfremt forsikringsselskaber bliver i stand til i et konkurrencedygtigt marked at vurdere risici i forbindelse med IT-løsninger, vil den part, der via lovgivningen er pålagt ansvaret for den manglende IT-sikkerhed, kunne indkalkulere denne udgift i det samlede regnestykke for aktiviteten ved at betale en forsikringspræmie.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

2.1.1 Beskriv problemet så præcist som muligt

God systemudvikling - fra vugge til grav - er ikke noget som man lærer i dag

I gamle dage skulle man kende systemet og teknologien – i dag er viden specialiseret og der er ikke holistisk helhed.

Uddannelsen af it-arkitekter er mangelfuld

Aftestning af løsninger er ikke så optimal som de kunne være.

At ændre i designfasen koster faktor 1 - at ændre i programmeringsfasen koster faktor 10 - mens at ændre i testfasen koster i faktor 100

Der er tab af kompetence (på web-områderne er der ej heller opbygget disse)

Vedligehold og certificering er en udfordring

Open source - er analogt

Open source og udviklingsstandarder er ikke naturligt forenelige

Kan den påstand uddybes?

Læs evt. producing open source bogen, www.producingoss.com, der er intet i vejen for at Open Source udvikling kan udvikles i et firma, af et firma, men kildeteksten så gives bort ....

open source er licensen - software kan udvikles som man har lyst

"Uddannelsen er mangelfuld" står der. Men hvor stor en del af problemet skyldes at man rundt om i virksomhederne har ekspertisen, men nedprioriterer sikkerhed til "mindre stressede perioder"? (som sjældent kommer)

2.1.2 Hvad kan en løsning være?

Hæve kravene - webudvikler certificering (specielt med fokus på sikkerhed?).

At skabe en it-arkitektur uddannelse - skal have elementer med som rummer kompleksiteten af det at lave sikre it-løsninger.

Det er vigtigt at binde teknologi, ricisi, økonomi og jura som en del af uddannelsen.

Lave et paradigme for et "risiko-regnskab" eller sikkerheds-regnskab ...

Dette kan kombineres med øvelser af hændelser ---

Liability skal placeres hvor beslutningerne tages.

Kontrollen skal dirigeres til dem, som har risiko (decentralt, distribueret, opdelt) = Borgerne/Brugerne

Skabe certifikater der kan signalere compliance med sikkerhedsstandarder og som "nemt" kan anvendes af beslutningstager ved systemanskaffelse.

2.1.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Leverandørerne, virksomheder og slutbrugere skal efterspørger

Sikkerheds deklarationer på SW - certificering af SW er næppe vejen frem.

Er det nu rigtigt ? en CMM certificeret virksomhed må alt andet lige levere et produkt, hvor der er større overensstemmelse mellem kravsspec. og produkt end en ikke CMM certificeret virksomhed

CMMI er ikke en sikkerhedsmæssig standard, men en standard der retter sig imod kvaliteten i systemudviklingen. Måske kunne den kombineres med COBIT, som også bygger på Key Point Indikators og Maturity Models.

2.1.4 Hvordan hænger problemet evt. sammen med andre problemer som har været behandlet i dag?

Standarder og rammer er forudsætningen for effektiv og troværdig sikkerhed

2.2 Manglende sammentænkning mellem it-arkitektur og sikkerhed (8 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Der mangler alt for ofte en stærk sammentænkning mellem it-arkitektur og sikkerhed i it-løsninger, store som små.

Sikkerhed ses ofte som noget der "puttes" på til sidst og ikke noget der medtænkes fra starten af et udviklingsprojekt. En af mange årsager er at kravstillere ikke er gode nok til at stille krav til indbygning af en sikkerhedsarkitektur i den overordnede IT arkitekturmodel.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

2.2.1 Beskriv problemet så præcist som muligt

SP er behandlet under 2.1.1.1-4

2.1.1- 2.1.4 :-))

2.2.2 Hvad kan en løsning være?

it-arkitektur skal dokumenteres og fremstilles, så beslutningstagere kan forstå og gennemskue arkitekturen, herunder den sikkerhedsmæssige del af denne. Paralleller til den fysiske arkitektur/sikkerhed kan evt. bruges med fordel.

2.2.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Veluddannede it-arkitekter, som ikke alene taler et teknikspro g.

2.3 Én sikker elektronisk ID,- skridt for skridt (8 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

På godt og ondt har Danmark haft nytteværdi af CPR nummeret som tillader sammenbygning af tjenester på en sikker måde. På samme måde må vi fremkalde en elektronisk identitet som vi på sigt kan enes om og også fokusere vore kræfter på at gøre sikrest og bedst mulig. Nytteværdien vil være uovertruffen for Danmark.

Vi mangler "situationsbestemt ledelse" på området. OCES og net-ID konkurrerer og efterlader borgere og virksomheder på "herrens mark".

CPR-systemet er sikkerhedsmæssigt forældet !

Men vi kan bruge en god rod-identifikation til at bygge multi-identitet og dermed isolering af data i specifikke sammenhænge på.

Tag som udgangspunkt at du KUN skal bruge Digital Signatur til at skabe nye nøgler

Husk at sondre mellem:

en ID, som er et "navn" i den elektroniske verden, ligesom "Peter" eller "Hans", (men bare bedre fordi det er entydigt),

en autentificeret (entydigt identificeret) bruger i en on-line aktivitet eller en digital signatur på et dokument.

Hvis det er det sidste, så husk altid at medtænke at sikkerhed har en grænse, at det kan gå galt og så skal der også være en god løsning på problemerne.

Biometri må danne grundlag for en erstatning af CPR-systemmet

biometriske produkter i dag er ikke sikre. Husk din fysikundervisning i gymnasiet.

Der er fejlmargen indenfor DNA, fingeraftryk og andre biometriske metoder.

Hvad vil vi acceptere af fejlmargen og hvordan angriber vi den biometriske løsning - biometri er ikke løsningen.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

2.3.1 Beskriv problemet så præcist som muligt

Der er brug for kontekst afhængig identitet (rolle begreber).

Eklektronisk id er en hønen og ægget diskussion. I dag bliver det forderet ud fra effektivitet, men der bør fokuseres på anvendelse til brede formål og sikkerhed som her følger med

2.3.2 Hvad kan en løsning være?

At forestillingen om en og kun en sikker elektronisk identitet bliver skrottet helt!

Indførelsen af digital signatur baseret på en løsning med kvalificerede certifikater.

Man må ALDRIG genbruge nøgler, dvs. forslaget er skrevet uden forståelse for sikkerhed

2.3.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Bankerne kan bidrage

3. TEKNIK OG INFRASTRUKTUR

3.1 Email - få det nu fikset! (5 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Utroligt så meget brugerne må finde sig i når det gælder email! Markedsaktørerne lapper og piller og klistrer men der er stadig ikke en udvikling som peger imod en udbredt anerkendt troværdig, fortrolig og stærkt identificeret email løsning til afløsning for det der blev opfundet i 1980'erne.

Enig! utroligt at Internettets gamle protokoller stadig benyttes, - således at vi anvender kommunikationsprotokoller der ikke er designet med sikkerhed som en del af helheden.

Og ISP´erme tilbyder over en kam stort set ikke kryptering af e-mailforbindelser. En katastrofal mangel, der meget let kan rettes op på.

Større sikkerhedskrav til ISPer - enig omkring krypteringskrav - og kravene kan godt udvides

Det er teknisk muligt at sikre sine e-mails i dag men det kræver den store ingeniøreksamen og det er blokerende for den brede anvendelse.

Mail leverandørerne gør det på hver deres måde - som sjældent er bruger venlig eller logisk. Behov for standardisering som inkluderer brugervenlig sikkerhed.

Ingen protokol, hvor troværdig, fortrolig og identificeret den end er kan gøre noget ved spam-problemet uden at der er mulighed for international håndhævelse. Få det på plads først. SPAM-problemet i DK er begrænset - ikke fordi vi har en bedre protokol, men fordi vi har håndhævelse.

M.h.t. virus vil en tilpas kompromiteret maskine stadig kunne skabe problemer med en anden protokol.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

3.1.1 Beskriv problemet så præcist som muligt

E-mails er (uden digital signatur) usikre. Afsender kan ikke identificeres, de kan hackes, de kan ændres undervejs, de er ikke uafviselige. Det giver usikker kommunikation og mulighed for SPAM fra tredjepart.

E-mails er ikke krypterede på forbindelse fra mailserveren til brugeren (POP3 - IMAP), dvs. password kan opfanges undervejs på f.eks. trådløse netværk.

3.1.2 Hvad kan en løsning være?

Løsningen findes i et vist omfang i form af PKI (digital signatur). I DK findes en national løsning.

Internationale regler for anvendelse af emails, kryptering, spam m.m. så der kan skabes sikkerhed over nationale grænser. Det betyder at det er muligt at forfølge spammere over grænser.

POP3/IMAP problematikken er gældende for alle miljøer hvori der anvendes ukrypterede netværk (mange kontorer, hoteller, byrum osv.). Udbyderne kan uden væsentlige problemer tilbyde en sikker løsning, og de fleste mailklienter kan håndtere krypteringsløsninger.

Løser ingenting fordi angribere bare krypterer deres kommunikation til dig med din nøgle !!!

- Selv med min bedste vilje forstår jeg ikke den kommentar ???

Alle e-mail programmer kan sætte et flueben for at få krypteret POP3 og IMAP, selv en Nokia mobiltelefon

- Ja - men hvis din udbyder ikke tilbyder løsningen, så hjælper det jo ikke meget. Vi taler om en krypteret FORBINDELSE - ikke kryptering af mails. Det er en anden (og ligeså relevant) problemstilling.

fortrolig email opnås kun ved kryptering til modtager direkte fra egen mailklient. Ellers skal du have tillid til netværksoperatører etc.

Der er tale om behov for to former af beskyttelse. Den ene vedrører fortrolighed, og her ville en mulig løsning være kryptering. Den anden vedrører uafviselighed og bevis for levering, og her kommer bl.a. digital signatur (PKI-løsning) på banen.

Desuden skal mail både krypteres og signeres for at det giver beskyttelse mod alle former for trusler, og dette skal ske end-2-end.

Signatur på emails hjælper med til at sortere mails i kvalitet og potentielt spam, på samme måde som breve og adresseløse forsendelser signalerer noget i postkassen.

Signatur kan også hjælpe brugerne med at skelne mellem phishing og troværdige virksomheder, som forsøger at kommunikere med sine kunder via. email. (Dette er jo næsten ved at blive umuliggjort i dag).

Modtagerstyret kommunikation og specifikke emailadresser ville meget hurtigt kunne reducere spamproblemerne uafhængigt af udlandet.

Man skal passe på med ikke at fokusere for meget på protokollens (SMTPs) alder og begrænsninger. Der kan laves ganske små modifikationer (som f.eks. SPF), der vil gøre det nemmere at slå ned på spam. Det vigtigste er stadig at der er en international håndhævelse på linie med den danske og konsekvens overfor dem, der spammer.

3.1.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Kryptering til slutmodtager af e-mail kan løses ved at udbyderne tilbyder/presses til at levere produktet.

Sikkerheden vedr. send/modtag e-mail kan dels løses nationalt (digital signatur) men skal også håndteres internationalt i FN eller andetsteds.

3.2 Digital Authentikering (5 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Biometri må IKKE bruges til Digital Authentikering

Biometri skaber Identitetstyveri og Omvendt Bevisbyrde i retssager

Biometri blokerer for borgernes sikkerhed

Identifikation flytter kontrollen væk fra borgerne og placerer altid magten hos en anden

Hvordan forhindrer vi kriminelle i at misbruge biometriske sensorer?

Det bliver alt for nemt at aflytte/spore f.eks. politikere, sårbare personer og borgere

Digital Signatur er ikke sikker nok

Behovet og nødvendigheden skal være mere klar. Hvad er risikoen for at et dokument opsnappes sammenholdt med muligheden for at stjæle fra postkassen eller fra firmaets papirkurv.

Ja - den er absolut ALT for svær.

En stor del af det offentlige Danmark, og efterhånden også mange private, bruger efterhånden den digitale signatur til identifikation. Dette gør den digitale signatur "missionskritisk" i forhold til hele udviklingen af informationssamfundet.

Den manglende sikkerhed i form af et "fysisk led" gør signaturen meget usikker. Er en cracker inde på en pc, kan samme cracker også fuldstændigt overtage den digitale signatur.

Problemet affærdiges ofte med, at det selvfølgelig ikke er retsligt bindende, at en digital signatur er blevet misbrugt. Men det er en meget reel risiko, at vi i praksis kommer til at se en slags omvendt bevisbyrde i den slags sager.

Når - og jeg mener NÅR - de første sager om misbrug opstår, vil vi risikere at se en voldsom nedgang i tilliden til digital signatur. Og dermed en nedgang i tilliden til informationssamfundet som helhed.

En central Signatur KAN ikke sikres - CA er ikke trustworthy, men risikoskabende.

Pointen er ikke at vi ikke skal have digitale nøgler, men at (gen)brugen af identificerende nøgler ødelægger sikkerhed

Det handler mere om balancen mellem teknisk sikkerhed og brugerens evne til at anvende løsningen.

Vi kan gøre den digitale signatur så sikker, at borgerne ikke kan anvende den - så vil de omgå sikkerheden og resultatet er en lavere sikkerhed.

Signaturen må vokse med nytteværdien. Sikkerheden må vokse i takt med at investeringen kan retfærdiggøres. Men standarderne må fastholdes, så vi skaber en fortløbende rejse.

Certifikatet til den digitale signaturer sikrer en identifikation af hvem folk er - men vi skal også have en mulighed for at kunne graduere hvad man har adgang til - forskellige niveauer. Vi mangler kort sagt attributter på identiteter, der muliggør en identificering af prokura.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

3.2.1 Beskriv problemet så præcist som muligt

En stjålet signatur kan ikke skelnes fra en ikke-stjålet signatur! Der er ingen skrifteksperter der kan afgøre ægtheden. Det kan betyde at det er den "uskyldige" der skal bevise at han IKKE har anvendt sin signatur.

Det samme gælder biometriske signaturer.

Biometri kan altid spoofes og kan ikke revokes - skaber identitetstyveri og alvorlige problemer for borgeren med at genskabe sin identitet

En pragmatisk løsning er at basere sig på kombination af udstedt (klassificeret) signatur, og en eller flere biometriske kendetegn. Proportionalitet i autentificeringskravet med det, som skal beskyttes er en forudsætning. Bedøvet anvendelse af højeste sikkerhedsniveau for ligegyldige ting giver dårlig brugeropmærksomhed

3.2.2 Hvad kan en løsning være?

Den venter vi på?

Et borgerkort uafhængigt af staten og channel providerrs kontrolleret af borgeren,

dvs. instant revokable (i tilfælde af tab/tyveri)

styring, opbygning og vedlighedelse af mutiple identiteter,

on-card biometri som device passwords - selvfølgelig IKKE nogen former for biometri i authentificering vs. eksterne parter

på tværs af kommunikationskanaler, så ingen gatekeepere tager ejerskab af borgerne

En klassificeret signatur skal kun bruges som rodidentitet til at lave nye nøgler, men ikke til eksternt brug

3.2.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

3.3 Et fælles nøglekort for den offentlige sektor og finanssektoren bremses af manglende politisk samtænkning (4 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Tænker man i sektororienterede sikkerhedsløsninger får man stærkt varierende sikkerhedsniveau, besværlige og ikke-brugervenlige forskelligartede IT-løsninger og en manglende mulighed for at høste udbyttet af digitalisering overalt i samfundet..

Eksempel: Sygesikringskortet skal erstattes, Tinglysningssystemet efterspørger bærbar digital signatur, EU ønsker biometriske pas, udbredelsen af OCES certifikaterne synes at have stagneret alt imens bankernes net-løsninger får flere kunder. Tænk det sammen, gør noget radikalt og lad alle få glæde af en fælles dansk infrastruktur, der bringer niveauet op på kvalificerede europæiske digitale certifikater.

Man skal huske at et sådant nøglekort ikke kun udpeger en person, men en aktør dvs. en fysiks person som er tilknyttet en organisation: Arbejdspladsen, idrætsforeningen, sin familie etc. Hvis man tænker denne tanke videre så vil man på sigt få en lang række identiteter (organisation * systemer) hvis man ikke samorder så mange som muligt af disse.

Men husk at privacy også er et issue.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

3.3.1 Beskriv problemet så præcist som muligt

Borgerne skal have flere forskellige elektroniske ID'er afhængig af hvilken service (privat eller offentlig de efterspørger.

Sikkerhedskravene er forskellige i forskellige organisationer! Har de så behov for samme sikkerhedsløsning? Er det trygt for borgeren at det er samme nøgle der skal anvendes på hospitalet og i videokiosken?

Vil øge problemerne med sikkerhed overfor misbrug (tyveri). Hvis et kort stjæles er der adgang til data i mange virksomheder. Hvis banker og det offentlige får en fælles digital løsning, vil den også blive anvendt af mange andre virksomheder. Lige som sygesikringskort der anvendes både hos lægen, på biblioteket og i videokiosken.

Vi kan ikke bruge one-size fits all !!! En løsning skal understøtte forskellige modeller.

Det plejer dog ellers at være god sikkerhedstilgang at fokusere sine kræfter om få mekanismer, som man til gengæld kan sikre en høj kvalitet af, i stedet for mange usikre?

Hvor det ikke er muligt at lave en business case for at indføre smart cards for f.eks. kørekort, kunne det absolut gennemføres for sygesikringskort, pas, lånerkort, kørekort, evt. i kombination med nøgler til private korttyper (bank, forsikring, parkering etc.)

3.3.2 Hvad kan en løsning være?

Er en løsning ønskværdig?

Et fælles nøglekort mellem banksektoren og den offentlige sektor gør det muligt at kombinere flere identiteter og en ensartet, brugervenlig sikkerhedsstruktur.

Vi har en gylden mulighed for at kombinere det nye sygesikringskort (et smart card) med efterfølgeren til OCES, som gør at nøglen bliver bærbar og dermed også kan anvendes f.eks. til løsning af Tinglysningsopgaven,

Nej, man har jo heller ikke et benzinkort der kan anvendes på alle tankstationer.

Nej, men det ville være smart

Hvis ikke nøglekortet indtænkes i en større sammenhæng, går vi glip af en lang række muligheder for forbedring af IT sikkerheden og for indføring af nye, sikre løsninger, der tilgodeser behovet for mere effektivitet og bedre borgerstyring.

Hvis dataloven omformuleres til et mere tidssvarende sprog - således at borgerne kan gennemskue den og få overblik over hvilke oplysninger der er lagret om vedkommende -

Samtidig med at man benytter de forskellige spor i magnetstriben på borgerkortet til forskellige ydelser vil den enkelte borger måske se mildere på indførelse af Borgerkortet - de har jo i dag adskillige kort til både det ene og det andet

Man skal huske at en sådan digital identitet ikke kun udpeger den fysiske person, men den fysiske person i en given sammenhæng - det kunne f.eks. være som privat person eller som ansat i en virksomhed. Det vil derfor ikke være muligt at give en personen en digital identitet til alle sammenhænge, men en identitet som kan anvendes til alle formål i en sammenhæng.

3.3.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Staten kan igennem sine udbud og sine tjenester sætte standarden på området.

3.4 Terror mod infrastruktur (4 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Samfundets infrastruktur styres af IT. El, telefoni, varme, finans, Internet, TV etc. Med terror-motivationen opstår der nye "rationaler" som ikke nødvendigvis er vægtet i selskabernes tidligere risikovurderinger. "Hvem kunne have interesse i det?" - vurderingen vendes på hovedet.

Ganske enig. Problemet er at der ikke i forbindelse med udlicitering af kritisk infrastruktur stilles krav til sikkerheden af det offentlige. Se i øvrigt under Regulering og Standard for samme emne

Enig - her har vi et meget alvorligt samfundsmæssigt problem. Se blot hvad der skete da København var uden strøm 4 timer.

Der skal mere fokus også politisk på dette problem. Det er nu uheldigvis sådan, at ulykkerne skal ske, før øjnene bliver åbnet.

Det kan nok uheldigvis ske, at Danmark vil blive alvorligt ramt af en sådan form for terror - for den danske mentalitet siger nu, at det sker ikke for os....

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

3.4.1 Beskriv problemet så præcist som muligt

Infrastrukturen er fysisk sårbar overfor diverse uforudsete begivenheder (terror).

3.4.2 Hvad kan en løsning være?

3.4.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

3.5 Der fokuseres for meget på identifikation af personer, og for lidt på hvilken rolle personen spiller i interaktionen med et system (4 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Der er meget offentligt diskussion om hvorvidt en given metode til at identificere personer er tilstrækkeligt sikker, men der fokuseres ikke på den anden halvdel af problemet - nemlig hvad vil man tillade personen at udføre.

Dette er selvfølgeligt ikke et problem i meget simple systemer, men efterhånden som flere processer digitaliseres, er det et stadigt stigende problem at der mangler sikre metoder til tildeling af rettigheder.

Der mangler også en overvågning af, at rettigheder også overholdes. Ofte er det nødvendigt at give tekniske adgang til mere, end man har juridisk adgang til.

Vigtigt at adskille identifikation og autorisation som to forskellige problematikker. Identifikation kan standardiseres vældig godt imens autorisation er meget kontekst afhængigt og en opgave for data ejeren decentralt.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

3.5.1 Beskriv problemet så præcist som muligt

3.5.2 Hvad kan en løsning være?

Undgå snakken om sikkerhed som om det er en fiks løsning - sikkerhed er altid relativt til kontekst og derfor et afvejningsproblem mellem risici og omkostninger.

Vi kan logisk designe identiteter med privatlivsfremmende teknologier, så hensyn til alle stakeholders risikohåndtering indbygges.

Sporbarhed og ansvarlighed er selvfølgelig en del af sikkerhedsproblemet, som skal kunne håndteres på forskellige måder

Det er vigtigt at se en identitet som noget, der dynamisk konstrueres til kontekst., dvs. starter og forbliver ikke-identificeret

3.5.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

3.6 Løsninger er for komplicerede at bruge (4 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Digital signatur anvendes meget lidt i erhvervslivet - det vælges simpelthen ikke til fordi det er for besværligt.

Der bør være løsninger der er så lette at alle bruger dem

Gruppen nåede ikke at bearbejde problemet

3.7 Der mangler en standard for sikring af privatejet kritisk national infrastruktur (4 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Ligeledes et problem at mange nye teknologier tages i brug tidligt uden gode vejledninger i sikkerheden.

VoIP - der burde være en dansk udgave af NIST vejledning SP800-58 "sikkerhed i VoIP netværk"

- vi har set problemet med 802.11 trådløse netværk, hvor personfølsomme data har været tilgængelige.

Det offentlige kunne gå i front og lave vejledningerne og håbe at virksomhederne ligeledes vil benytte disse.

Sikkerheden i privatejet kritisk national infrastruktur er ikke et konkurrenceparameter og derfor overladt til hvad operatørerne synes er "godt nok". Der ses i udlandet en trend til at sammenkoble de komplekse systemer og at kunne monitorere flere systemer med færre ressourcer. Ved flere samtidige hændelser i sammenkoblede systemer er det sandsynligt, at operatørerne ikke kan overskue situationen og handler uhensigtsmæssigt. Når der er stærke transnationale krav til f.eks. flyveledere og airtraffic control, hvorfor skal man så ikke have det på kritisk national infrastruktur?

Gruppen nåede ikke at bearbejde problemet

4. VIDEN OG ADFÆRD

4.1 Almindelige brugere lades i stikken (10 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

De almindelige brugere/borgere lades i stikken med usikker teknologi, som de gøres mere og mere afhængige af.

Det er urealistisk at alle brugere skal blive eksperter på softwareopdateringer og sikkerhed.

Der er en del utryghed ved at bruge internettet pga. den alm. brugers angst for at egne data ikke er sikre nok.

Det for vanskeligt at opretholde en sikker adgang til og brug af internettet for almindelige brugere

Den almindelige bruger (private husstande) har ikke forudsætningerne for at håndtere sikkerhed. Hacking, virus mv. giver enorm tidsspilde og de stadig kraftigere private computere kan bruges destruktivt af 3. part

En forbedret og løbende uddannelse af især unge kan over tid sikkert løfte niveauet, men aldrig tilstrækkeligt.

Det må derfor være en opgave for samfundet, serviceudbydere og professionelle aktører i markedet.

Der bør stilles krav om at alle pc'ere der sælges til slutbrugere leveres med færdiginstalleret sikkerhedssoftware og -indstillinger som automatisk sikrer en regelmæssig opdatering af de nødvendige komponenter via internettet.

It-sikkerhed forklares ikke på den almindelige brugers sprog

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

4.1.1 Beskriv problemet så præcist som muligt

Den gennemsnitlige bruger har svært ved at overskue, hvad der skal til for at opnå rimelig sikkerhed på egen pc.

Resultatet er at hjemme-pc'er er for dårligt beskyttede og dermed i for høj grad er sårbare overfor misbrug.

Google som eksempel:

Hver gang en bruger går online og søger via Google udleverer IP-addressen automatisk profilinformation direkte i en amerikansk kontrolleret database. Det skaber dermed profilering af hver enkelt EU-borger og virksomhed uden sikkerhed eller regulering. Kobles IP-adressen via en transaktion med kontaktinformation har profilen dermed fået navn og adresse m.m.

Det er et infrastrukturproblem, idet teknologien bør designes så man ikke genbruger IP-adresser og anden kontaktinformation.

Problemet KRÆVER både teknologi og andre elementer

Borgerne har ikke værktøjer til at styre sin sikkerhed og data i forbindelse med digital transaktioner

Man antager at borgerne er ligeglade eller ikke rationelle i deres adfærd.

En mere brugbar forklaringsmodel er at brugeren kun agerer i forhold til den risiko, de opfatter.

Men at de stadig er risikoaverse og dermed rationelle givet den viden, infrastruktur og værktøjer, de har til rådighed.

Hvis mennesker er usikre og ikke forstår teknologi, så reagerer de ikke med at brokke sig, men ved at stå af.

Dvs. dårlig sikkerhed slår via læring over i modstand mod at deltage i den digitale verden.

God sikkerhed slår via læring over i Demand-pull og brugerdreven innovation i den digitale verden.

Ja, brugere agerer i forhold til den opfattede risiko. Men hvis den opfattede risiko, som tilfældet oftest er, er at brugeren kan miste nogle ubetydelige dokumenter, så hjælper det ikke meget. Brugere kan måske nok bibringes en forståelse for, at deres adfærd kan påvirke andre negativt, men jeg tvivler på, at det vil ændre ret meget når det kommer til at skulle betale. Og det er jo nok det, der skal til.

4.1.2 Hvad kan en løsning være?

Lad den kloge "svigersøn" tage sig af sagen - eller en af de mange andre servicevirksomheder

Større aktører bør bidrage med awareness/sikkerhedsinformationer (ISP'er, Banker, Det offentlige,.....)

Den usikre bruger bør søge hjælp evt. mod betaling.

Ofte kan ISP'er tilbyde en vis grad af hjælp.

Lovgivning:

Skal ISP'er tvinges til at tilbyde sikkerhedspakke?

De skal betale. De kloge svigersønner har jo tydeligvis hidtil ikke gjort et voldsomt godt job.

Multi-Identity Management med brugeren i fokus.

Cliient-side Single Signon, men kun specifikke nøgler og adresser på nettet.

Systemer skal laves med udgangspunkt i den kompetente borger

Hvis borgerne ikke kan/vil/må håndtere sin egen sikkerhed kan man arbejde med lokal delegering

Borgerkort med MANGE nøgler i stedet for et Identifikationskort

Oplysningskampagner kan hjælpe med at gøre den "almindelige" bruger opmærksom på risici og mulige forholdsregler til imødegå disse risici. Bl.a. gøre opmærksom på den enkelte persons sårbarheder med relation til brug af IT, og hvor nemt det dels er at udstille sig selv (og sin mangel på sikkerhed) - dels at beskytte sig, hvis man blot tænker sig en smule om.

Men husk at det ikke kun er den enkelte bruger, der udsætter sig selv for risiko. De udsætter også alle andre på nettet for risiko (bot-nets, spam osv.)

Forbrugerbeskyttelse burde være ensbetydende med at en PC eller en anden enhed (PDA) leveres med et sikkerhedssystem der er "rimeligt, relevant og aktiveret" således at den ukyndige borger kan anvende udstyr uden basalt at skulle sætte sig ind i sikkerhed. Samtidig burde der ligge en "forbrugerinformation" om de mest grundlæggende retningslinjer for fornuftig ("sikker") og etisk ("ansvarlig") digital adfærd.

En normal borger har ret beset kun nogle få behov der rammes af lovløsheden på internettet: informationssøgning, download af filer og udveksling af mails. Teknisk set må det være muligt at lave hw/sw der kan sikre en opdeling i den usikre verden (hvor man vil være anonym) og en sikker verden med bedst mulig autentifikation.

Man kunne forestille sig "sikre" programmer der er certificerede og kun afvikles fra sikret memory (sikker browser, sikker e-mail program).

4.1.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

se forrige

4.1.4 Hvordan hænger problemet evt. sammen med andre problemer som har været behandlet i dag?

Der er relation til:

IT-kriminalitet mod hjemmebrugers pc,

som dels kan rette sig mod bruger selv,

dels kan medføre, at pc'en kan misbruges til angreb mod andre

4.2 IT sikkerhedshjælp til små og mellemstore virksomheder vil fremme globalisering og innovation (10 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Vidensdeling over landegrænser bliver et uomgængeligt krav. De små og mellemstore virksomheder har behov for adgang til kompetence og (open Source) systemer, der kan højne sikkerheden og beskytte virksomhedens intellektuelle rettigheder så vidensdeling med autoriserede partnere kan finde sted. Uden sikker viden bliver mulighederne ikke udnyttet og vi forpasser chancen for vækst.

SMVere er - som indenfor andre områder - en it-hvidplet. Det gælder også sikkerhedsområdet. Special treatment is needed

de små virksomheder ser ikke deres behov

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

4.2.1 Beskriv problemet så præcist som muligt

Mindre virksomheder som er vidensbaserede (og har informationsaktiv, der kunne stjæles), kan være sårbare hvis de ikke beskytter sig.

4.2.2 Hvad kan en løsning være?

Under iværksætter støtteordninger kunne awareness omkring risici samt løsningsmuligheder tilbydes.

SMV'ere ser nok kun deres behov hvis de ser en økonomisk/forretningsmæssig gevinst ved it-sikkerhed.

SME skal behandles ligesom forbrugere – dvs. at der skal være sikkerhedsniveau indbygget i den nøglefærdige løsning – evt. certificeret til at modsvare et standarddefineret sikkerhedsniveau.

4.2.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Erhvervsministeriet

eller andre offentlige organer

4.3 Hvorfor tænker Digital Forvaltning aldrig sikkerhed? (7 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Digital Forvaltning er totalt centralistisk og gør borgerne transparente overfor kriminelle og staten. Samtidig ser vi en stigende tendens til at Staten derefter "sælger" borgernes data = Ekspropriation

Digital forvaltning handler om effektivisering! Når borgere og politikere insisterer på et stadigt voksende antal af mere komplekse velfærdsydelser, stiger kravene til effektive IT-systemer, der dels kan (bidrage) til at levere ydelserne, og dels kontrollere at der ikke "snydes" i uacceptabelt omfang. Det ser ud til at vi gerne vil have alle mulige ydelser, men vi vil ikke kontrolleres! Men uden kontrol vil efterspørgslen efter ydelserne vokse til en ufinansierbar størrelse. Er kontrollen ikke den pris borgerne må betale for de komplekse velfærdsydelser?

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

4.3.1 Beskriv problemet så præcist som muligt

Digital Forvaltning har lagt vægt på effektivitet.

- form af øget samkøring, overgang fra papir til digitale systemer, og færre krav til samtykke

men har ikke i samme opfang haft fokus på awareness omkring korrekt anvendelse, adgangskontrol, ansvarsfastlæggelse, opfølgningsprocedurer samt sanktioner i tilfælde af misbrug.

Digital Forvaltning tager online Identifikation for givet, hvorved hensynet til sikkerheden forsvinder.

Man arbejder ikke med specifik og differentierede adgange.

Betragter Det Offentlige Borgerne som undersåtter eller som borgere ?

Man vil have meget komplekse løsninger og man vil ikke have at andre snyder!!! Det kræver en ganske omfattende kontrol af borgerne at sikre at ingen snyder. Vi kan godt undvære kontrollen, men så vil der være flere der snyder, og det gider vi ikke betale til! Hvis ydelserne var simple, ville der ikke være behov for omfattende kontrolforanstaltninger. Eksempelvis børnetilskud ydes per hoved efter alder (på barnet) uanset bopæl, indkomst, uddannelse eller køn. Sådan er det ikke med kontanthjælp, boligydelser/sikring, varmetilskud, førtidspension osv.

4.3.2 Hvad kan en løsning være?

Øget fokus på awareness omkring korrekt anvendelse, adgangskontrol,

ansvarsfastlæggelse, opfølgningsprocedurer samt sanktioner i tilfælde af misbrug.

Digital forvaltning tænker meget i sikkerhed!

Digital forvaltning skal ikke bygge sikkerhed op om en elektronisk identitet men baseres på en rollemodel med identiteter der svarer til kontekst og ikke kan anvendes i andre (hvilket øger sikkerhed imod misbrug ved tyveri, aflytning, etc.)

4.3.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Dataejer / Systemejer skal sikre at kontrollerne er på plads.

Implementeringen af DS484:2005 bør sikre at det proceduremæssigt anbefalede er med i fokus.

Kræver også en holdningsændring - data har værdi og skal passes på.

Justitsministeriet eller Videnskabsministeriet skal tage fornødent initiativ.

5. KOMMUNIKATION OG VIDENSDELING

5.1 Oplysning på linie med folkesundhed eller trafiksikkerhed (13 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Sikkerhedsproblematikken bliver behandlet som et teknisk randdisciplin for specialister. Se det i stedet som trafiksikkerhed eller folkesundhed

Der bruges ikke nok midler på oplysende aktiviteter om it-sikkerhed til befolkningen og/eller udvalgte målgrupper

Trafiksikkerhedssammenligningen er god, for de fleste mennesker vil ikke tænke over, at de skal til mekanikeren og betale for at få repareret deres bremser af sikkerhedsmæssige årsager. Men de fleste vægrer sig ved at skulle betale en konsulent for at installere og vedligeholde sikkerhedsprogrammer på en privat pc.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

5.1.1 Beskriv problemet så præcist som muligt

Netsikker.nu har ikke gennemslagskraft, da der ikke er politisk interesse og midler. Ulykkescenarierne skal gøres klare. Men problemet kan heller ikke sidestilles med så livs- og velfærdstruende fare som sundhed og trafik.

5.1.2 Hvad kan en løsning være?

Undervisningsinstitutioner, offentlige og private virksomhed skal være fora for uddannelse i basal og dagligdags IT-sikkerhed med konkurrencer, tests og præmier. Der skal være meget gulerod og kun lidt stok. IT-sikkerhedsuddannelse skal sidestilles med kurser i førstehjælp og trafiksikkerhed.

Derudover bør der sigtes mod egentlig folkeoplysning - hvorfor anvendes OBS! spots ikke til at skabe awareness omkring it-sikkerhed?

Der er i andre lande (fx Frankrig) en journalistisk tillægsuddannelse (eller modul) hvor it-sikkerhed indgår.

Sæt Anja Philip til at lave et program i TV om IT sikkerhed - og om IT forbrydelser i den efterfølgende sendetime. Så skal I se!

Sæt Mads Mikkelsen til at lave et program i TV om IT sikkerhed - og om IT forbrydelser i den efterfølgende sendetime. Så skal I se!

Kampagner i fx TV, hvor der vises "skræk-scenarier" a lá de, som har kørt vedrørende usikker omgang med fyrværkeri (fx Troels Trier).

5.1.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Lærere, repræsentanter fra fag- og arbejdsgiverforening samt private eller offentlige undervisningskonsulenter skal videregive informationen. Materiale og økonomiske midler skal stilles til rådighed fra det offentlige. Undervisning med eksamen skal være obligatorisk.

5.1.4 Hvordan hænger problemet evt. sammen med andre problemer som har været behandlet i dag?

Sammenhængen er, at IT-sikkerhed forudsætter brugerinvolvering, og hvis ikke viden om IT-sikkerhed blandt almindelige brugere forøges, løses IT-sikkerhedsproblemet ikke.

5.2 Borgerne er interesserede i at være sikre - men ikke i sikkerhed (7 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Borgerne er meget interesserede i at være sikre.

Alle undersøgelser viser imidlertid, at borgerne ikke er interesseret i den tekniske sikkerhed - det er noget de bare forventer fungerer uden at de skal tage ret meget stilling til det.

Og internet brugerne gider ikke bruge masser af timer blot på at få sikkerhedssystemerne til at virke - leverandørerne (af udstyr og internetforbindelser) skal bare sørge for at det virker. De store ISP'ers SPAM og antivirusfiltre er derfor det bedste sikkerhedstiltag i mange år

Der skal stilles større krav (lægges pres) på producenterne af hardware, således at sikkerhed af systemet er en del af fx. opsætningen. Fx. ved trådløst net skal de almindelige sikkerhedsbetragtninger være sat på forhånd og promptes brugeren

Præcist derfor må borgerne have hjælp af professionelle som kan påtage sig ansvar og tillid (og leve af det på den ene eller den anden måde).

Det koster ikke noget, at ignorere sikkerheden i dag for den gennemsnitlige private bruger. Højst en smule irritation over nogle mistede dokumenter. Men som kommentaren ofte lyder: "Jeg har jo ikke noget, der er så vigtigt".

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

5.2.1 Beskriv problemet så præcist som muligt

Alle vil gerne leve sikkert, men sikkerhed er et trade-off overfor omkostninger ved at opnå sikkerhed. Der skal investeres tid og penge i blive sikker, herunder uddannelse og software. Der er opportunity cost: Mere sikkerhed kan betyde mindre bevægelighed og færre mulighed. Almindelige kan ikke overskue dette trade-off, eller måske kan de, og deres vurdering er, at IT-sikkerheden ikke er det værd!

5.2.2 Hvad kan en løsning være?

Hvis folk skal interesse sig for IT-sikkerhed, skal omkostningerne ved manglende IT-sikkerhed anskueliggøres. Hvad koster det mig eller andre, at jeg eller andre ikke er IT-sikre. Måske skal der lovgives, således at et økonomisk ansvar for manglende IT-sikkerhed lettere kan ifaldes og opgøres.

Nemlig - it-sikkerhed (eller mangel herpå) vil om føje år være langt større end i dag - og overstige de samfundsmæssige udgifter ved fx trafikulykker - set som TCO for samfundet - men der er næppe ikke lig på bordet - med mindre man fortænker en kæde af hændelser...

Analogien med trafik- og sundhedssikkerheden er glimrende. Selvom brud på IT-sikkerheden ikke direkte medfører dødsfald (generelt set - for i udlandet mener man jo konkret at kunne påvise, at en hacket patientjournal var skyld i, at en patient døde ved fejlbehandling!!!), så kan de medføre direkte økonomiske uhensigtsmæssigheder, ligesom "e-brugere" (berettiget eller uberettiget) kan blive beskyldt for ulovlig, uhæderlig eller anden optræden.

5.2.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Hvis folk skal interesse sig for IT-sikkerhed, skal omkostningerne ved manglende IT-sikkerhed anskueliggøres. Hvad koster det mig eller andre, at jeg eller andre ikke er IT-sikre. Måske skal der lovgives, således at et økonomisk ansvar for manglende IT-sikkerhed lettere kan ifaldes og opgøres.

5.3 Uddannelser indenfor IT-sikkerhed mangler på universiteter og andre steder (7 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Uddannelse i sikkerhed er mange steder begrænset til kryptering og algoritmer.

Meget lidt om sikre protokoller, yderst lidt omkring god programmering, intet om backup, intet om drift af systemer. Der mangler uddannelseselementer med fokus på:

sikker programmering

systemadministration som fag - professionel drift af it-systemer

it-sikkerhedsledelse, evt. som en del af handelsskoler?

Man skal tidligt promovere "code of ethics", eksempelvis med udgangspunkt i CISSP ethics, SAGE "system administrators' code of ethics"

IT-sikkerhedsundervisning med certificering skal implementeres i alle IT-uddannelser, uanset om det er på EUD, KVU, MVU eller LVU niveau

Mangler uddannelse indenfor design af multi-stakeholder sikkerhed.

Det bliver altid noget ensidigt navle-centreret

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

5.3.1 Beskriv problemet så præcist som muligt

Der er behov for, at IT-sikkerhed generelt bliver inkorporeret med varierende omfang i forskellige videregående uddannelser, idet IT-sikkerhed skal forstås både fra en bruger-, forretnings- og strategisk vinkel.

Danmark bør satse på IT-sikkerhedsforskning både på det rent tekniske område men også indenfor for brugervenlighed og sociale aspekter i forbindelse med anvendelse.

IT-sikkerhedsundervisning skal ikke kun indarbejdes på de videregående IT-uddannelser - men på alle IT-uddannelser! IT-sikkerheden er nemlig ikke stærkere end det svageste led!

5.3.2 Hvad kan en løsning være?

Der bør etableres en specialeret IT-sikkerhedsudddannelse på højere niveau, hvis indhold må udvikles i samarbejde mellem private og offentlige virksomheder. Uddannelsen kan eventuelt etableres som led i et internationalt samarbejde.

IT-sikkerhed må som begreb og område indtænkes i alle videregående uddannelser i variende omfang, idet alle uddannede i vidt omfang i deres fremtidige virke vil interagere med IT. Beslutningen skal implementeres af undervisnings- og videnskabsministeriet med de fornødne midler efter et klart politisk diktat.

Det ville være logisk at knytte en CISA- eller CISM-certificering som et element, idet en sådan certificering er anerkendt både i DK og internationalt. I Holland har man med stor succes indarbejdet CISA som en del af universitetsuddannelsen.

5.3.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Lærere og andre undervisere som sætter sig og laver kursusmateriale med fokus på sikkerhed. Det kunne eksempelvis skrives ind i bekendtgørelser at sikkerhed skal dækkes.

6. OVERORDNEDE PRINCIPPER

6.1 Terrorpakken og borgernes retssikkerhed (10 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Dette tema viser hvor galt det kan gå i debatten. Det er for let at opstille skræmmebilleder, der endda hjælper til at holde på den politiske magt. Bl.a. fordi sikkerhed kan gøres til en meget simpel sag, der kan forstås af enhver, uagtet at det reelle indhold er noget andet.

Proportionalitet efterlyses inden for denne problemstilling

Der er fare for en eklatant tilsidesættelse af borgernes retssikkerhed

Politikerne "gør noget" for folket - Sikkerheds/pricacy folket - snakker om "spøgelser", som folk ikke kan se.

Politikerne gør IKKE noget for folket. De har fundet ud af, at der er stemmer i, at fremmane skræmmebilleder, som man efterfølgende kan vise sig handlekraftig i forhold til. I de tidligere øststater var der meget lidt kriminalitet. Men det kan og må ikke være en vej for det danske samfund

Endvidere er det MEGET lidt sandsynligt, at de foreslåede overvågningsmuligheder i forbindelse med logning rent faktisk vil give en effekt. Der er ganske enkelt for mange huller i reguleringen. Og skal disse huller udfyldes, er vi i sandhed ikke længere bare "på vej" mod en politistat.

Ja... et eksempel er jo åbne WiFi ap. Hvem logger "terroristen", der holder på en villavej?

Retssikkerheden er der mange der kigger på, men vi tænker mere på bremserne end på speederen. Det hæmmer udviklingen. Mere fokus på konkrete problemer.

Terrorpakkens krav om bagdøre og konstant identifikation blokerer for nødvendige sikkerhedsløsninger

Der er ikke krav i lovgivningen vedr. terrorbekæmpelse om bagdøre. Hvilke "nødvendige" løsninger skulle der lægges hindringer i vejen for?

Kravet om at aflytning skal indbygges forudsætter bagdøre!

Forebyggende sikkerhed umuliggøres af kravet om centralt overvågning og sporing - for at kunne spore og aflytte.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

6.1.1 Beskriv problemet så præcist som muligt

Terrorpakkens formål er at forebygge/efterforske terrorangreb ved at opspore mønstre i kommunikation og handlinger i kommunikationsinfrastrukturen.

Problemet er trefold:

* Politisk er der kritik af at terrorpakken krænker retssikkerheden og privatlivets fred

* Teknisk stilles der spørgsmålstegn ved om foranstaltningerne vil have den ønskede effekt.

* Praktisk kan det være dyrt i forhold til det faktiske udbytte. Penge, der evt. ville kunne være brugt bedre.

Det vil være svært at forhindre huller i overvågningen, der betyder at egentlige terrorister relativt nemt kan omgå logningen.

Løbet er kørt - de kriminelle kan SAGTENS beskytte (anonymisere og kryptere) deres kommunikation.

F.eks. Mixnet er kendte og udbredte. De bliver nu 100% trådløse, dvs. uafhængige af centrale gateways, hvor kommunikationen kan styres.

Terrorpakken rammer de lovlydige borgere og virksomheder - men kun de dumme kriminelle, der ville være fanget alligevel

Flere af terrorpakkens forslag gør det muligt at efterforske på oplysninger, som idag ikke er tilgængelige.

Der skal fastsættes præcist, hvad der fx. skal logges og hvor længe - samt ikke mindst hvem der er dækket af lovgivningen

6.1.2 Hvad kan en løsning være?

Man bør overveje at bruge pengene på mere målrettede løsninger i stedet. F.eks. generelt flere ressourcer til målrettet efterforskning i IT-kriminalitet.

Overvågning af flypassagerer, secure traffic lanes (containertrafik for at undgå atombomber i havnen), sikring af sårbar IT infrastruktur etc. i stedet for

Mulighed for i "nødsituationer" at give myndighederne mulighed for at få adgang til data, som er krypteret. Vil kræve en form for "autoriseret bagdør", men må være i samfundets interesse - forudsat myndighedernes brug overvåges og rapporteres.

Man må som udgangspunkt have tillid til, at politiet kun anvender disse efterforskningsmetoder, når det er aktuelt, ligesom de anvendes efter reglerne.

Der er jo i forvejen tillid til politiets arbejde, og man må sige, at der er meget få sager, hvor der kan sættes finger på efterforskningen.

Tillid kan ændre sig. Een sag er een for mange. Siden Per Stig Møller har der været en skepsis for hvad der foregår, og det er blandt for at gøre borgerne trygge, at man må forlange sporbarhed i anvendelse af efterforskning.

Det handler ikke om tillid. Hvor der er magt, skal der også være tilsyn med denne magt.

Der er generelt meget lidt information om sikkerhedstjenesten i Danmark. Mere information ift. antallet af konkrete overvågninger, statistik for tilsagn / afslag af retskendelser osv.

Anonymous resoulution er en metode, der kan anvendes i forbindelse med udvidede Identity Match søgesystemer. Først når der er match mellem den anonyme borger og et antal belastende forhold/transaktioner, kan anonymiteten hæves, evt. efter dommerkendelse. Metoder eksisterer altså uden at det går uden over borgernes retssikkerhed. Og metoder som denne kan faktisk både dokumenteres og offentliggøres på forlangende.

det hjælper heller ikke at man flytter ressourcer til endnu mere lukkede fora, tænk PET

Der er RIGELIGT med sager hvor betroede medarbejdere af nysgerrighed er gået ind på oplysninger som de ikke havde lov til - hvor mange penge skulle der så til for at de gjorde det ellers?

Terrorbeskyttelse handler mere om udbredt samfundsinformation om "god adfærd" så den enkelte borger bidrager hver på sit sted til en fornuftig - og ikke en "hysterisk" - overvågningstænkning og forholdsregler.

6.1.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Politikerne skal tage den rigtige beslutning i tættere samarbejde med interessenter for at sikre en praktisk realistisk løsning.

6.1.4 Hvordan hænger problemet evt. sammen med andre problemer som har været behandlet i dag?

Det hænger sammen med borgenes retssikkerhed og privatlivsbeskyttelse.

6.2 privatlivsbeskyttelse (9 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

Opstilles ofte som modsætning til sikkerhed

Hovedparten af danskere har intet imod overvågning, når det kan medvirke til bekæmpelse af kriminalitet eller frygt. Der mangler dog politisk vilje.

Politisk vilje til hvad? mere overvågning?.. overvågning er en afmagtsstrategi / symptomstrategi, og med meget lidt dokumenteret effekt

Mange danskere, der efter sigende har det ok med overvågning, kan ikke gennemskue hvad de forholder sig til. Overvågning er ikke 0 eller 1 men en gradvis udvikling, der - hvis vi pludselige kommer for langt - kan have uoverstigelige konsekvenser

Et demokrati er kendetegnet ved, at der er grænser for statsmagtens indtrængen i det private.. hvis politiets hensyn overtrumfer alt andet.. ja så er vi en politistat

Sikkerhed har også et følelsesbetonet element. Hvis man pludselig stiger af følelsesmæssige grunde, er det også et sikkerhedsmæssigt problem.

Overvågning er falsk sikkerhed, som ØGER sikkerhedsproblemerne og reducerer trygheden.

Hr, og fru Danmark har generelt intet imod øget overvågning, når de kan se et formål med det.

Det skal politisk gøres klart, hvad overvågningen skal medvirke til.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

6.2.1 Beskriv problemet så præcist som muligt

Emnet beskriver problemerne omkring overvågning, men privatlivsbeskyttelse indeholder også flere ting, som f.eks. identitetstyveri og misbrug af personlige data.

Der er brug for forbedret lovgivning i forhold til borgernes ret til at vide hvem, der har data om dem og hvad det bruges til. Det skal være gennemskueligt for borgerne.

Der er mange scenarier i vores hverdag, hvor der tilknyttes identiteter, hvor det ikke er nødvendigt.

6.2.2 Hvad kan en løsning være?

Løsningerne er på dette meget store område er hovedsageligt politiske og juridiske.

I de enkelte praktiske scenarier kan der dog være konkrete tekniske løsninger, der kan forbedre forholdene.

Krav om IT Governance (sv. til f.erk.s Sarbanne-Oxley) - Policy bestemt IT sikkerhed skal gennemgås af virksomhedernes revisorer og fremgå med bemærkninger, hvis sikkerheden er mangelfuld.

Skærpet tilsyn og sanktion ved brud på persondatabeskyttelse.

Indbygge persondatabeskyttelsen i tekniske løsninger.

Man skal næppe undervurdere de tekniske løsninger, som er under udvikling. En teknisk løsning, som indebærer en logning af alle de som har haft adgang til ens egne personlige data vil uden tvivl stoppe mange forsøg på at luske sig til data, som ikke skal bruges i en egentlig sagsbehandling. Dette forekommer at være en relativ simpel måde at tage et stort skridt m for at sikre den enkelte borger, at vedkommendes data ikke eksponeres mere end hvad der er nødvendigt.

Privacy impact assesment som et standardelement i systemudvikling.

Holdningsændring, ikke mindst i den offentlige forvaltning. Uddannelse af medarbejdere.

6.2.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

6.3 Stadigt mere IT-kriminalitet er økonomisk motiveret (8 stemmer)

Oprindelig problembeskrivelse og kommentarer fra Fase 1:

For få år siden var meget IT-kriminalitet baseret på at vise at det var muligt - at lave en orm/virus eller bryde ind i et system.

Men f.eks. spam er et tegn på at de samme teknologiske problemer nu bruges at nogle få (20-40) men slagkraftige organisationer til at tjene penge. Udsendelsen af spam er proportional med modtagernes købekraft og en væsentlig del er derfor målrettet den vestlige verden og specielt USA.

Denne udvikling er farlig da indtægten fra disse aktiviteter vil muliggøre og inspirere nye og kraftige angreb.

Herefter følger bearbejdning af problemet gennem gruppearbejde samt kommentarer fra de øvrige deltagere:

6.3.1 Beskriv problemet så præcist som muligt

Alle dele af samfundet bruger IT mere og mere. Det gør økonomisk kriminalitet også. Det kan dog blive nemmere at udføre pga. de generelle problemer med IT-sikkerhed.

Andre IT-sikkerhedsproblemer (som f.eks. identity theft) er derfor medvirkende til øget økonomisk kriminalitet.

Voksende Identifikation gør ofrene sårbare og tvinger de kriminelle til Identity Theft, dvs. det fremtvinger nemmere og sikrere kriminalitet.

6.3.2 Hvad kan en løsning være?

Løsningen på "økonomisk kriminalitet" som sådan er at løse de sikkerhedsproblemer, der gør det muligt.

Ansvaret er fordelt mellem både leverandører, ISP'erne og brugere og man kommer ikke uden om uddannelse.

Økonomisk motiveret kriminalitet behøver ikke at være økonomisk kriminalitet!

SPAM er et godt eksempel herpå - Her bør der skabes en større international indsats for at ramme de firmaer som anveder dette medie som reklame platform.

Der er behov for at se IT-kriminalitet som en "helt almindelig" kriminalitetsform, og ikke som noget særligt.

Mere intelligent overvågning hos ISP'erne og værktøjer til hurtig sporing af synderne og rapportering af hændelser til "politiet".

6.3.3 Hvem kan realistisk set bidrage til at løse problemet og hvordan (så konkret som muligt)?

Fase 3: Hvad er vigtigst at gå i gang med NU?

I denne fase udvalgte deltagerne de syv initiativer, som de mente kan gavne IT-sikkerheden i Danmark mest. Der var ikke tid i denne fase til en nærmere beskrivelse af initiativerne og de skal derfor betragtes som syv hurtige bud fra deltagerne. Deltagerne stemte efterfølgende ved hver især at rangordne initiativerne. Hver deltagers førsteplads gav 7 point, andenpladsen 6 point osv. 23 deltog i afstemningen.

Rangordning

113 point	1. 5 gode råd til borgerne
104 point	2. Smartcardløsning til den digitale signatur
104 point	3. Sygesikringskort med chip
98 point	4. Udvikle bedre IT-sikkerhedsstandarder
93 point	5. Brugerkampagne for børn og barnlige sjæle
76 point	6. Systemadministration som fag og faggruppe
56 point	7. Lovkrav om DS484 i Staten

Initiativer med beskrivelser

1. 5 gode råd til borgerne

Hvad skal der ske?: 5 gode råd til borgerne om it-sikkerhed, hvad kan man selv gøre?

Hvem skal være ansvarlig?: Videnskabsministeriet

Hvilke(t) problem(er) løser det?: Det giver både folk viden - og skaber forøget opmærksomhed om problemet

2. Smartcardløsning til den digitale signatur

Man bør udnytte lejligheden, når sygesikringskortet skal udskiftes, til at indføre en smartcardløsning for den digitalsignatur i overensstemmelse med kvalificerede EU-certifikater. Evt. i et samarbejde med banksektoren.

3. Sygesikringskort med chip

Der er ved at være kritisk masse på anvendelsesområder for digital signatur. Selvom man ikke kan lave den endelige løsning grydeklar for sygesikringskortet kunne man sætte en chip på og "sætte fyrtårnet op".

Ansvarlige: Amtsrådsforeningen, VTU, Digital Taskforce.

Hvilket problem løses: Mobilitet og sikkerhed øges og sårbarheden overfor en usikker PC platform mindskes.

4. Udvikle bedre IT-sikkerhedsstandarder

Fra dansk side skal vi medvirke til at skabe en fælles IT-sikkerhedsmæssig standard med borgernes IT-sikkerhed i centrum. Man skal samtidig være villig til at ofre de økonomiske ressourcer i en sådan standard, men skal samtidig også være bevidste om at en øget IT-sikkerhedsbaseret IT-infrastruktur kan udmøntes i eksportydelser.

Videnskabsministeriet og Erhvervs- og Økonomiministeriet - ministerierne skal bruge de internationale samarbejdsfora til at fremme idéen.

Sikrer at de moderne teknologier kan anvendes og give det fulde udbytte

5. Brugerkampagne for børn og barnlige sjæle

Uddannelse i brugersikkerhed som "dannelseselement" der indgår i den almindelige undervisning i skoler o.l.

En top-X liste der kort beskriver de allervigtigste IT-sikkerhedsmæssige forhold for den private brugere! Og den skal kommunikeres ud til børn og barnlige sjæle. Via Bubber og og Sigurds Bjørne time

6. Systemadministration som fag og faggruppe

Initiativ indenfor system administration

Vi ønsker at der iværksættes initiativer indenfor system administration til anerkendelse som et selvstændigt fag med tilhørende uddannelser og certificeringer.

7. Lovkrav om DS484 i Staten

Ingen uddybende kommentarer

Evaluering af workshoppen

Evalueringsresultater

1. Positive kommentarer

1. Fint at bruge et system med så mange taleglade (og lytte-svage) deltagere.

2. Masser af input -. mange gode kommentarer og en god dialog

3. Udmærket afvikling af gruppesystemet. Kunne godt bruge en større vekselvirkning mellem eget arbejde og gruppearbejde i løbet af formiddagen.

4. Dejlig koncentreret proces i løbet af formiddagen

Første del af eftermiddagen ligeledes

5. hurtig generering af meget information

6. Godt at samle så mange eksperter.

Positivt at få lejlighed til at drøfte emnet bredt.

7. Godt forløb indenfor den afsatte tid

8. God interaktion, mange spændende emner er blevet berørt.

God spredning af deltagere

9. Meget flot fremmøde,- mange havde prioriteret at være med.

10. Brainstorming processen i formiddag tror jeg skabte mange gode ideer der efterfølgende kan benyttes som input

11. En dag med mange ideer -

12. Det var en strålende ide. God måde at køre "debatten" på. Jeg havde aldrig set systemet før, men det virkede strålende.

13. Stor aktivitet - muligheder for alle

14. Der er i dette fora viden til at forbedre sikkerheden, dvs. målgruppen er ok til formålet. Det har været interessant at udveksle information og viden

15. Spændende proces - mange gode indlæg

16. Godt at få samlet snakken

17. Et glimrende initiativ med denne workshop.

God blanding mellem teknik og gruppe-"terapi".

En god og bred sammensætning af deltagerne.

18. Nemt at bruge systemet. Godt initiativ

2. Negative kommentarer

1. Der var en del overlap - også til sidst - som måske kunne have været handlet af og slået sammen. Det er ikke sikkert det betyder så meget i det samlede billede, men det gør det lidt svært at overskue om prioriteringen er rigtig.

2. Formiddagens session var for lang og gav for få seriøse resultater på de sidste kategorier af de 6 temaer der var udvalgt som struktur.

Kunne med fordel have kogt ned til tre overordnede temaer som hver havde haft en egen- og en gruppesession knyttet sammen inden man arbejdede videre.

3. For kort tid til fremlæggelse af gruppearbejdet fra første del af eftermiddagen.

4. for meget spredt fægtning.. kommer ikke langt nok

5. Emnet er for bredt til en helt åben diskusion.

Der skulle have været lagt flere spor, f.eks. i form af oplæg, som kunne styre emneområderne ind. Selvom det ville være styrende.

6. Der var næsten for mange som kunne kommentere på det samme område i formiddagssessionen - meget svært at overskue - burde måske have været delt op i en indsamlingsfase i grupper og en fælles kommentar og afstemningsfase

7. Resultatet af gruppearbejdet var ikke overvældende - jeg tror at debatterne havde mere substans end det rapporterede. Måske et procesproblem.

For lidt tid på at pege på det ene endelige og ultimative initiativ - resultatet var derefter.

8. men meget få nye praktisk anvendelige tiltag

9. for lidt nyt

for rodet proces

- bedre med at så nogle tanker og så arbejde med dem

flere møder med færre deltagere

10. Mange af punkterne går igen i flere afstøbninger

11. ALT for lidt tid.

Der står vel en del redigeringsarbejde tilbage før mange af kommentarerne er operationelle. Det er et stort spørgsmål om dette vil ske - eller om det havde været en bedre ide, at I selv gjorde det.

12. Formen med elektronisk afstemning har ikke været god. Der har været for mange forslag at skulle tage stilling til og Rådet bude have taget sig tid til en grundig redigering af forslagene efter første runde.

Der er ikke værdi for deltagerne i denne proces

13. Processen har ikke virket. Forslagene er decideret dårlige og specielt et smartcard med digital signatur vil være direkte negativ for sikkerheden

14. Der kan være en fare for at feltet bliver noget udvandet når der er så mange forskellige vinkler på hvad IT sikkerhed indbefatter

15. Lidt lang eftermiddag

16. Ikke nogen.

17. For lidt tid til at sætte sig ind i de mange indspark i forhold til tiden til at lave dem.

Der kommer mange emner og påstande op, der kun overfladisk er tænkt over og som kræver en langt dybere diskussion for at få fælles overblik over problemstillingen og konsekvenserne på. Der er således stor fare for forkerte løsninger.

3. Hvad virker interessant, men kunne/burde været gjort anderledes?

1. IT sikkerhed trænger til en klar opdeling i nogle hovedkategorier således at det bliver håndterbart.

2. Sidste punkt på eftermiddagen burde have været en videre evaluering af gruppearbejdet samt en prioritering af de fremlagte emner

3. Fint at samles i grupper, men grupperne kunne være sammensat i forhold til de interesser som folk har.

4. Strukturering og sammenstilling af alle guldkornene bør kunne gøres bedre - kræver nok manuel bearbejdning og dermed tid.

5. Hvis en mindre faggruppe havde udpeget en håndfuld problemområder på forhånd, kunne deltagerne måske havde valgt sig ind i en gruppe i stedet for at havne i områder som de ikke nødvendigvis "brænder" for. Det kunne give lidt mere dybde.

6. Gruppernes konklusioner burde have fået lov til at stå alene - der var alt for mange partsindlæg der blev tilføjet som mudrede billedet af det konkluderende arbejde, grupperne havde brugt lang tid på at nå frem til

7. Vi kunne have haft mere tid til drøftelser hvis alle på forhånd havde indtastet deres forslag.

8. Udvælgelsen af ideer, men formen var ikke god

9. Godt at konfrontere forskellige synspunkter, men der manglede tid og struktur til at fremkomme med nuancerede svar og forslag

10. Rigtigt godt initiativ

11. mere strukturering på eftermiddagen

12. Hvis administratoren havde haft større mulighed for at konsolidere overlappende svar fra formiddagens session, så vi havde fået et endnu bedre grundlag for gruppearbejdet.

4. Alt i alt: Samlet vurdering af dagen

(1=laveste vurdering, 10=højeste vurdering)

Resultatspredning

Choices	Count
1	0
2	1
3	1
4	3
5	3
6	0
7	1
8	8
9	5
10	0

Gennemsnit *6.73*

Afgivne stemmer *22*

Program

8:45 **Kaffe og rundstykke**

9:15 **Velkomst og introduktion til workshoppens formål**
Velkomst, v/ Bjørn Bedsted, Teknologirådet.
Præsentation v/ Line Gulløv Lundh, Videnskabsministeriet.
Introduktion til dagsordenen og metoden v/ Lars Ginnerup, proceskonsulent.

9:50 **Fase 1: IT-sikkerhedsmæssige problemer**
Deltagerne brainstormer på deres bud på de vigtigste IT-sikkerhedsmæssige problemer, og placerer dem under følgende overskrifter:

1. Regulering og standarder
2. Systemudvikling
3. Infrastruktur
4. Viden og adfærd
5. Kommunikation og vidensdeling
6. Andet

Undervejs er der mulighed for at kommentere egne og andres forslag.
Afstemning: Prioritering af problemer.

12:00 **Frokost**

13:00 **Fase 2: Handlinger og løsninger**
Gruppearbejde: Uddybning og af problemer, samt udvikling af løsningsforslag.
Individuel kommentering af løsningsforslag.

15:45 **Fase 3: Afslutning**
Gruppearbejde: Identificering af vigtigste løsningsforslag.
Afstemning: Prioritering af løsningsforslag.

16:30 **Tak for i dag**
Teknologirådet byder på et glas vin.

Deltagerliste

Bent Poulsen	Værdipapircentralen A/S
Carsten Stenstrøm	Danske Bank
Christian Wernberg-Tougaard	Unisys Nordic
Ellen Svenning	Ringe kommune
Flemming Faber	IT- og Telestyrelsen
Freddie Drewsen	Forsvarets Forskningstjeneste
Hanne Bender	Bender von Haller Dragsted
Henrik Lund Kramshøj	Security6.net
Jacob Øst Hansen	Nordea
Jakob Illeborg Pagter	Alexandra Instituttet A/S
Jesper Svarre	PROSA
Martin Povelsen	PriceWaterhouseCoopers
Jørn Guldberg	KMD A/S
Lars Neupart	Neupart A/S
Leif Limkilde Bloch	HK/Privat
Leo Moesgaard	IBM Danmark A/S
Line Gulløv Lundh	Ministeriet for Videnskab, Teknologi og Udvikling
Martin von Haller Grønbæk	Advokatfirmaet von Haller
Michael Hald	Kommunernes Landsforening
Mogens Kühn Pedersen	Handelshøjskolen i København
Morten Storm Petersen	TDC A/S
Niels Mortensen	Fyns Amt
Ole Hvidkjær	Danmarks Nationalbank
Ole Stilund Jeppesen	FTF
Peter Mogensen	Digital Forbruger Danmark
Peter Ussing	PROSA
Rikke Frank Jørgensen	Danske Institut for menneskerettigheder
Sten Sørensen	Rigspolitiet
Stephan Engberg	Priway Aps
Søren Duus Østergaard	IBM Danmark A/S
Thomas Byberg-Hansen	CSC Danmark A/S
Thomas Eriksen	Dansk IT
Thomas Kristmar	Rigspolitiet
Tommy Petersen	Novell Danmark A/S
Torben Andresen Lindhardt	Dansk Metal
Ben Hope	Teknologirådet
Bjørn Bedsted	Teknologirådet
Janus Sandsgaard	Teknologirådet
Lars Ginnerup	Proceskonsulent, LG Facilitation