Bilag 1

It-sikkerhed på tværs af grænser.

Anbefalinger fra en arbejdsgruppe under Teknologrådet.

Arbejdsgruppen

- Carsten Stenstrøm
  - Teknologisikkerhedschef i DR (tidligere Danske Bank).
- Christian Wernberg-Tougaard
  - Director i Unisys, medlem af ENISA's rådgivende ekspertudvalg vedrørende "Awareness Raising"
- Preben Andersen
  - Chefkonsulent i Uni-C, leder af DK-CERT.
- Morten Storm Petersen (ikke tilstede)
  - Signaturgruppen A/S (tidligere TDC).
- Brian Birkvald (ikke tilstede)
  - Security Principal & Manager i IBM's Security Group.
- Lars Neupart
  - Adm. direktør for Neupart A/S.

Ønsket besked til borgere:

- Du kan trygt bruge nettet og informationsteknologien – i dag og i fremtiden

Situationen i dag

- It-relateret kriminalitet er et reelt og stigende problem.
- Hele verden er digitalt forbundet - på tværs af landegrænser.
- I takt med at flere og flere dele af vores samfund digitaliseres rykker kriminaliteten over også over i den digitale verden.
- Kriminelle udnytter teknologien med fordel.
- Internationale problemer kræver internationale løsninger.
- Forudsætning for ønsket tryghed: Politiske initiativer til hævelse af sikkerhedsniveau.
- Gruppen har nogle konkrete forslag til handling. Fordele:
  - Danske borgere får mere tryghed
  - Sikkerhed giver fordele for Danmarks muligheder i den globaliserede verden

Politiske løsninger

1. Lav en EU mærkningsordning, som gør det lettere for forbrugere at vælge de sikre produkter.
2. Stil krav til it-forhandlere om at levere produkter der trygt kan anvendes ved ibrugtagning.
3. Lav krav til producenter om at følge en international standard om sikkerhedsopdatering
4. Oplysning skal gøre borgere opmærksomme på deres muligheder for trygt at bruge teknologien
5. Indfør et EU-borgerservice-pas.
6. Politiets kompetancer øges
7. Politiets internationale muligheder forbedres
8. Offentlig sektors indkøbskraft i EU skal give sikkerhed

It-sikkerhed på tværs af grænser - Præsentation af arbejdsgruppens anbefalinger

Papir til brug til mødet i udvalget 22. marts 2007

Ønsket besked til borgere: Du kan trygt bruge nettet og informationsteknologien – i dag og i fremtiden

Der er en forudsætning for denne tryghed : Politisk handling – vi har nogle konkrete forslag.

Alle eksperter er enige om at it-relateret kriminalitet er et reelt og stigende problem. I takt med at flere og flere dele af vores samfund digitaliseres rykker kriminaliteten over også over i den digitale verden. Kriminelle udnytter teknologien til at begå deres kriminalitet, og har allerede nu en klar fordel af at hele verden er digital forbundet på tværs af landegrænser.

Gruppen, som bl.a. består af de tilstedeværende eksperter, har udarbejdede konkrete løsningsforslag til de problemområder, der er beskrevet i Teknologirådets rapport. Bemærk at det er internationale problemer, som har betydning for Danmark, men som kræver internationale løsninger. Følges anbefalingerne, vil danske borgere få mere tryghed og Danmark vil klare sig bedre i den globaliserede verden.

Løsningsforslag:	Hvad kan vores politikere gøre?
1. Mærkningsordning for produkter der sælges i EU skal gøre det lettere for forbrugere at vælge de sikre produkter. Inspireret af energimærkning for hårde hvidevarer og international crashtest mærkning for biler.	**Etablere en mærkningsordning for sikre it-produkter.** Uden mærkning af it-produkter er det som forbruger alt for svært at skelne mellem sikre og usikre produkter. Man vil derfor være tilbøjelig til at vælge det billigste, der også ofte er det mindst sikre. Det kunne være en opgave for Forbrugerministeriet at nedsætte en arbejdsgruppe, bestående af producenter, eksperter, brancheorganisationer og forbrugere, der kan udarbejde et forslag til en fælles EU-mærkningsordning for sikre it-produkter. Ministeriet kunne herefter arbejde for ordningens gennemførsel på europæisk plan og gå i dialog med WTO for også at udvikle en global mærkningsordning.
2. Krav til it-forhandlere om at levere produkter der trygt kan anvendes ved ibrugtagning.	**Stille lovkrav til sikkerhedsopdatering ved salg af it-produkter.** Mange produkter (computere, mobiltelefoner mm – alle produkter med netværksopkobling) sælges i dag uden den nyeste sikkerhedsopdatering, fordi forhandlere ikke er forpligtet hertil. Det betyder, at nyt it-udstyr allerede fra købet kan være behæftet med alvorlige sikkerhedsbrister. En rimelig løsning kunne være, at forhandlerne ved lov forpligtes til at sikkerhedsopdatere produktet umiddelbart før det overleveres til kunden. Det kunne rent praktisk gennemføres på den måde, at it-leverandører – altså "producenterne" - etablerer en standard for automatisk opdatering af alle programmer via internettet, så forhandleren relativt ubesværet kan opdatere. Der kan nedsættes et tværministerielt udvalg (med deltagelse af Videnskabsministeriet og Økonomi- og Erhvervsministeriet) med det kommissorium at arbejde for indførelse af lovkravet til forhandlerne på EU-niveau

3. Krav om at producenter følger en international standard for automatisk sikkerhedsopdatering – dette gør det muligt for forhandlerne at leve op til kravene til dem.	**Automatiske sikkerhedsopdateringer** vil kunne lukke hovedparten af de sikkerhedshuller i software som it-kriminelle benytter sig af. Derfor bør der etableres en åben standard for automatiske sikkerhedsopdateringer som softwareproducenter kan bruge – for alle program-pakker. Standarden skal teknisk udformes så den muliggør automatisk sikkerhedsopdateringer af brugerens computer uden deres accept. Automatikken bør dog ikke gælde for andre former for opdateringer og programudvidelser. Videnskabsministeriet kunne tage initiativ til udarbejdelsen af en fælles europæisk opdateringsstandard i samarbejde med branchen og de offentlige myndigheder. For at have en reel effekt, skulle det gøres lovpligtigt for softwareproducenter på det europæiske marked at benytte denne standard for opdatering af deres produkter.
4. Oplysning skal gøre borgere opmærksomme på deres muligheder for trygt at bruge teknologien	**Skabe øget oplysning omkring it-sikkerhed og fremme en fælles it-sikkerhedskultur.** En forbedring af it-sikkerheden forudsætter, at it-brugerne har tilstrækkelig viden samt at der opbygges en større bevidsthed om sikker brug af it. I den sammenhæng spiller uddannelsesinstitutionerne en nøglerolle. Undervisningsministeriet kunne derfor undersøge, hvordan it-sikkerhed i højere grad kan indgå i læreruddannelser og integreres i undervisningen, fx ved mindre kurser i folkeskolen, hvor eksterne specialister underviser. Erfaringer kan med fordel udveksles på tværs af EU, men oplysningsarbejdet er primært en national opgave.
5. EU-borgerservice-pas. Et pas siger hvem jeg er.	**Skabe sikker identifikation gennem udvikling af et EU BorgerServicePas.** Sikker identifikation er en grundlæggende forudsætning for, at borgerne trygt kan handle og udveksle personlige oplysninger på internettet med myndigheder og andre. Nuværende identifikationsmekanismer vil ikke være tilstrækkelige i en fremtid, hvor dette i stigende grad foregår på tværs af landegrænser, da de forskellige landes it-arkitekturer ikke er taler sammen på dette område. Det kræver en fælleseuropæisk indsats at gøre de nationale it-arkitekturer i stand til at tale sammen. Målet for indsatsen kunne være udviklingen af et "EU BorgerServicePas" med flere forskellige funktioner, selvom det afgørende ikke er den fysiske identifikationsmekanisme, men netop den bagvedliggende struktur/arkitektur. Et første skridt kunne være at få fastsat nogle politisk bestemte kravsspecifikationer til en ny, sikker identifikation – fx via et udvalg af centrale aktører på området. Initiativet kunne være forankret i Videnskabsministeriet, der kunne gøre en indsats for at sikre den nødvendige interoperabilitet på tværs af EU's landegrænser.

6. Politiets ressurcer og viden	**Politiet mangler kompetencer** til at kunne håndtere den voksende it-kriminalitet og der er for mange eksempler på, at anmeldere af it-kriminalitet må gå forgæves. Dygtige politifolk der arbejder med it-sikkerhed søger (eller hentes) ofte hen i det private erhvervsliv. Problemet kan ikke løses uden at tilføre området flere ressourcer og Justitsministeriet kunne med fordel arbejde for en markant forøgelse af politiets videns- og kompetenceniveau, bl.a. gennem uddannelse af flere specialister på forskellige it-kriminalitetsområder indenfor politiet. En national indsats er dog ikke tilstrækkelig, og Justitsministeriet kunne med fordel opfordre Europol til at iværksætte en fælleseuropæisk, uddannelsesmæssig indsats.
7. Politi -internationalt samarbejde	**Forbedre det internationale politiarbejde**. Stort set al it-kriminalitet overskrider landegrænser og kan derfor kun bekæmpes gennem internationalt samarbejde. De eksisterende samarbejdsaftaler synes imidlertid ikke at fungere efter hensigten og mange kriminelle bliver derfor ikke pågrebet. Justitsministeriet kunne med fordel undersøge, hvordan samarbejdet kan forbedres. En løsning kunne være at udbygge ENISA, som er EU's agentur for it-sikkerhed, til at stå for koordinering og håndhævelse af internationalt politisamarbejde. Justitsministeriet kunne desuden undersøge mulighederne for, at ENISA suppleres med et tilsvarende organ i FN-regi, og arbejde for at få G8 til at sætte fokus på internationalt samarbejde om it-kriminalitet. (Eksempel: Netbankers problemer, der lige så godt kunne have ramt digital signatur)
8. Offentlig sektors indkøbskraft i EU skal udnyttes	**Gøre it-sikkerhed til en parameter i offentlige udbud.** En stigende del af vores forvaltning og kritiske infrastruktur er it-baseret. Alligevel stilles der kun lave krav til it-sikkerhed, når nye opgaver sendes i offentlig udbud. Det er en mangel nu hvor så mange dele af samfundet er forbundet via it. En sikkerhedsbrist et sted nemt kan få konsekvenser et andet. Problemet kan løses ved at indføre nogle højere EU-udbudskrav. Til at udarbejde disse krav og arbejde for deres implementering i EU, kunne der i Danmark oprettes en Digital Sikkerhedstaskforce. Den kunne også få til opgave at højne kravene til it-sikkerhed ved mindre offentlige indkøb, der ikke sendes i udbud i EU. (eksempel EPJ, og DS484/ISO27001 i kontrakter)

Det er arbejdsgruppens opfattelse at disse og rapportens øvrige forslag tilsammen vil kunne medføre en kraftig forbedring af it-sikkerheden.