

## Projektbeskrivelse

### Brugernes it-sikkerhed

De enkelte it-brugeres uhensigtsmæssige adfærd og manglende viden om tekniske sikkerhedsløsninger (firewall, virusfiltre, sikkerhedsopdateringer mm.) udgør en trussel for den generelle sikkerhed på nettet. I hjemmet kan det give gener for brugeren selv. Virus, phishing og hacking kan eksempelvis føre til kompromittering af personlige oplysninger, identitetstyveri, systemnedbrud og direkte økonomisk tab. Men også for andre kan det medføre gener. Brugers computer kan f.eks. bruges som mellemlid ved berigelseskriminalitet og angreb på andres computere, hjemmesider mm. Har brugeren eksempelvis hjemmearbejdsplads, kan uhensigtsmæssig adfærd i hjemmet også give problemer på arbejdspladsen og føre til kompromittering af andres personlige oplysninger, systemnedbrud, tyveri af intellektuelle rettigheder og fortrolige forretningsdata og deraf afledt økonomisk tab for arbejdspladsen.

I mange sammenhænge efterlyser man fra IT-Branchen, fra finanssektoren, fra industrien og fra myndighederne en højnelse af vidensniveauet blandt brugerne (øget "awareness") og der peges på initiativer, der kan øge kendskabet til og forståelsen af it-sikkerhed, samt på initiativer, der kan ændre brugernes adfærd. Meget tyder dog på, at man med dette fokus på den enkelte brugers ansvar ikke i tilstrækkelig grad er i stand til at højne det generelle sikkerhedsniveau og at der er et stigende behov for at fjerne en del af ansvaret for sikkerhedshåndteringen fra den enkelte bruger gennem eksempelvis regulering, koordinering og automatisering af indsatsen.

Der er lavet flere undersøgelser af borgernes adfærd og kendskab til it-sikkerhed, men lige så interessant er deres egen holdning til selve håndteringen af sikkerheden. Der findes ingen danske undersøgelser, der systematisk adresserer dette spørgsmål, men indirekte svar i flere brugerundersøgelser giver det ensartede indtryk, at den menige danskers holdning er, at sikkerhed ikke er noget, som man ønsker at tænke for meget på. Det er svært at holde sig opdateret og vide, hvordan man bør agere og sikkerheden skal helst bare være i orden, uden at man selv skal gøre noget. Er den ikke det, reagerer folk typisk med bekymring og undlader at udnytte deres muligheder på nettet.

Man kan på dette grundlag konstatere, at eksperter/beslutningstagere og brugere i en vis udstrækning har modstridende opfattelser af, hvor ansvaret for sikkerheden bør placeres. Der er flere aktører på it-sikkerhedsområdet, der beskæftiger sig med initiativer til kampagner, gode råd og uddannelse af brugerne og det er selvfølgelig en nødvendighed at højne vidensniveauet. Men selvom sådanne initiativer nok hjælper en smule på det generelle sikkerhedsniveau må man spørge, om de kan stå alene, når man nu ved, at folk synes, at det er både svært og uinteressant at beskæftige sig med sikkerhed. Man kan endvidere spørge, om det er rimeligt, at ansvaret for it-sikkerhed hviler på den enkelte i den grad, det på nuværende tidspunkt er tilfældet?

I enkeltstående tilfælde, såsom danske ISPers scanning af emails for virus og spam, kan der ses en udvikling, der fjerner en mindre del af ansvaret for sikkerhedshåndteringen fra den enkelte bruger. Og der stilles fra forskelligt hold forslag om løsninger, der yderligere kan fjerne noget af ansvaret fra de enkelte brugere. Det debatteres løbende, hvorvidt det er rimeligt, at de enkelte brugere alene skal bære ansvaret for eksempelvis konsekvenserne af usikker software og hardware (phishing, identitetstyveri, alm. hacking mm.) og der er en spirende enighed blandt økonomer på området om, at sådan en ansvarsfordeling bør betragtes som en decideret markedsfejl, og at det rettelig burde påhvile producenterne at sikre produkterne bedre. Andre sikkerhedsløsninger, der kan aflaste brugerne for ansvaret, er

eksempelvis bedre identifikationsmekanismer, mærkningsordninger, øget provider- og leverandøransvarlighed, certificeringsordninger, forbedring af politiets indsats mm.

Der findes så vidt vides intet systematisk overblik over hvilke løsninger, man med brugernes hensyn i tankerne kunne forestille sig at implementere. Løsninger, der kan gøre livet lettere for den enkelte bruger, fjerne en del af ansvarsbyrden og løfte det generelle sikkerhedsniveau.

### **Projektidé**

Der er behov for en mere systematisk gennemgang af løsninger på brugernes sikkerhedsproblemer – dels fordi det vil lette livet for brugerne og dels fordi det vil højne det generelle sikkerhedsniveau.

Projektets idé er derfor at lave en gennemgang af og komme med anbefalinger til sådanne løsninger. Gennemgangen kan med fordel inddrage resultater fra tidligere Teknologirådsprojekter. Gennemgangen skal rumme en vurdering af hvad det er, der hhv. hindrer og tilskynder en given løsning og den skal pege på de mulige løsningers respektive fordele og ulemper. En vurdering indenfor følgende it-sikkerhedsrelaterede områder kunne være af interesse

- Driftssikkerhed/systemnedbrud (huller i software og hardware, virus)
- It-kriminalitet (berigelseskriminalitet gennem phishing, hacking og identitetstyveri, tyveri af intellektuelle rettigheder og fortrolige firmadata)
- Privacybeskyttelse (misbrug og lemfældig håndtering af personlige oplysninger)

For at sikre sig, at de løsninger, der peges på, også er de mest relevante i forhold til brugernes ønsker og adfærd, vil projektet inddrage brugerne i vurderingen af fordele og ulemper ved de forskellige løsningsforslag. Sikkerhedsløsninger, der fjerner ansvar fra den enkelte bruger, vil indebære en række trade-offs, der kan være værdibaserede og kontroversielle, som f.eks.:

- Øgede krav til ISP'ers kontrol af emails kan være i modstrid med demokratiske værdier og ønsker om privacy,
- Større producentansvar kan give dyrere produkter og virke hæmmende for produktudviklingen,
- Større automatisering af sikkerhedsløsninger kan give brugerne mindre mulighed for selv at designe deres egne løsninger.

Det er et væsentligt fokus for projektet at få belyst sådanne værdibaserede trade-offs med udgangspunkt i konkrete løsningsforslag.

### **Formål**

At skabe debat om it-sikkerhed set fra brugernes perspektiv. Projektet skal bidrage til den fremtidige udformning af holdbare it-sikkerhedsløsninger ved at pege på løsninger, der matcher brugernes ønsker, evner og holdninger.

### **Målgruppe og formidling**

Projektets væsentligste målgrupper er danske politikere, embedsmænd, it-udviklere og andre centrale aktører indenfor it-sikkerhedsområdet.

Projektets hjemmeside vil løbende orientere om projektet og forskellige aktører vil blive involveret gennem workshop/udvidede arbejdsgruppemøder.

Når rapporten offentliggøres, vil der blive taget kontakt til pressen, både nyhedsmedier og specielle medier som særligt dækker det it-politiske område. Den vil blive offentliggjort på et

åbent møde mellem arbejdsgruppen og de it-politiske ordførere for Folketingets partier (hvis de vil).

Et engelsk resumé af rapporten vil blive udarbejdet og resultaterne evt. formidlet til EU-parlamentet gennem det europæiske teknologivurderingsorgan STOA.

Resultater fra projektet vil desuden blive formidlet i følgende medier, som Teknologirådet betjener sig af som standard:

Teknonyt:

Teknologirådets elektroniske nyhedsbrev med korte nyheder annoncerer aktiviteter i alle Teknologirådets projekter for en kreds af abonnenter.

Fra rådet til tinget:

Nyhedsbrevet til Folketinget, pressen mfl. udsendes når projektet afsluttes med en opsummering af de vigtigste problemstillinger.

TeknologiDebat:

Det er muligt at sætte fokus på ”Borgernes it-sikkerhed” i TeknologiDebat når projektet er godt i gang.

www.tekno.dk:

Projekthjemmeside med kort præsentation af projektet oprettes fra start. Opdateres løbende ved milepæle i projektet.

**Metode**

Der nedsættes en arbejdsgruppe med it-sikkerhedsekspertter, adfærdsspecialister m.fl. I den første fase af projektet får arbejdsgruppen til opgave at lave et overblik over mulige løsninger, der kan reducere brugernes ansvar for sikkerhedshåndteringen – samt over disse løsningers fordele og ulemper. Overblikket – der skal fungere som oplæg til et efterfølgende interviewmøde - henter inspiration i resultater fra tidligere projekter, workshops og rapporter. De mulige trade-offs drøftes på arbejdsgruppemøder – evt. med deltagelse af indkaldte eksperter. Så vidt muligt foretages en risikovurdering, der tager højde for såvel de enkelte brugeres som det samlede samfunds interesse.

De mulige løsninger samt de implicerede trade-offs præsenteres for og drøftes med almindelige brugere på et interviewmøde med deltagelse af ca. 25 almindelige brugere. Projektledelsen i Teknologirådet er ansvarlig for afholdelsen af dette interviewmøde og resultaterne derfra vil udgøre et selvstændigt delprodukt.

I projektets sidste fase inddrages arbejdsgruppen igen med den opgave – på baggrund af resultaterne fra interviewmødet – at drage sine egne konklusioner og komme med anbefalinger til fremtidige sikkerhedsløsninger. Overblikket, en analyse af resultaterne fra interviewmødet samt arbejdsgruppens konklusioner og anbefalinger præsenteres afslutningsvist i en samlet rapport.

**Arbejdsgruppens sammensætning**

- Jakob Illeborg Pagter, Alexandra Instituttet
- Susanne Karstoft, Juridisk Institut, Århus Universitet
- Birgitte Mikkelsen, Finansrådets it-sikkerhedsgruppe
- Nicholai Kramer Pfeiffer, Cybercity
- Per Tejs Knudsen, cBrain

- Steffen Stripp, Dansk Metal

**Tidsplan**

Marts 07: Research, planlægning af projektforløb og sammensætning af arbejdsgruppe

Maj - Juni 07: 1. arbejdsgruppemøde og udarbejdelse af overblik

September 07: Færdiggørelse af spørgeskema

November 07: Interviewmøde

December 07: Analyse af resultater

Januar 08: Færdiggørelse af rapport med anbefalinger

Februar 08: Offentliggørelse af rapporten