Cybersikkerhed i Danmark for ringe = De tre abers princip

Af John Michael Foley

Dagligt berettes om alvorlige angreb i cyberspace verden over. Danmark er ikke blevet skånet og er blot et af de talrige lande, der rammes i en globaliseret og digitaliseret verden uden grænser.

Men koordinerede reaktioner og handlinger herpå er få og i det store hele udeblevet i Danmark. De tre abers princip (se no evil, hear no evil, talk no evil) forekommer udbredt. Bevares, nogle tiltag er gennemført på operativ-drift niveau (eller ved at blive gennemført), men det er min påstand, at de er for få, for små, for stedmoderagtigt behandlet og ikke koordinerede. Jeg vil senere vende tilbage hertil, men forinden gå lidt mere i dybden med truslerne og cyberangrebene.

Trusler, angreb og sårbarheder

Den digitaliserde verden giver mange fordele, men medaljen har også en bagside. Alt og alle bliver mere sårbart, jo mere vi benytter internettet og anden informations- og kommunikationsteknologi. Sådan er virkeligheden og tiden kan ikke skrues tilbage. I EU's Cybersikkerhedsstrategi fra 2013 står der bl.a.:

"Angrebene kan være tilsigtede eller utilsigtede, og de vokser med alarmerende hast og vil kunne afbryde forsyningen af væsentlige tjenester, som vi tager for givet, f.eks. vand, sundhed, elektricitet eller mobiltjenester. Truslerne kan have forskellig oprindelse — der kan bl.a. være tale om kriminelle angreb, politisk motiverede angreb, terrorangreb eller statsstøttede angreb samt naturkatastrofer og utilsigtede fejl."

I *Sårbarhedsudredningen fra 2004* identificeres fire forhold som afgørende har ændret risikoscenariet:

- Globalisering,
- Teknologisk udvikling (informations- og kommunikationsteknologi (IKT))

- Terror
- Bortfaldet af en direkte militærtrussel med den kolde krigs ophør.

Især de to første udviklingstendenser er blevet markant forstærket siden 2004. I dag baserer store dele af vores samfundsvigtige funktioner sig helt eller delvis på Informations- og kommunikationsteknologi (IKT) uden for national kontrol.

Outsourcing og privatisering

Den stærkt accelererende outsourcing og privatisering af Danmarks samfundsvigtige og kritiske infrastruktur har i stort omfang forbedret angrebsmulighederne og tilsvarende forøget samfundets sårbarhed. Den 19. september meddelte TDC 's direktør f.eks. at den kinesiske mobilproducent Huawei skal levere udstyr til at drive TDC's mobilnetværk i Danmark. Huawei, der af nødvendighed og i et ukendt omfang er knyttet til det kinesiske regime, får dermed direkte adgang til en vigtig del af den samfundsvigtige og kritiske IKT - infrastruktur. Set i sammenhæng med de daglige meddelelser, der løbende tilgår om andre landes overvågning via sociale medier, synes det ekstra påkrævet og aktuelt, at der er nogen der bekymrer sig om og på et strategisk/overordnet/strukturelt niveau tager hånd om Danmarks sikkerhed i cyberspace i en koordineret og gennemtænkt indsats.

Behov for en national strategi

Problemerne, angrebene og udfordringerne eskaleres dag for dag, og burde ses i et større forsvars- og sikkerhedspolitisk perspektiv og kontekst. Forsvaret har jf. forsvarsaftalen af 30. november 2012 en rolle at spille, men opgaverne kan kun løses i et samspil mellem mange andre aktører såvel civile som militære. Et godt sted at begynde ville, i lighed med mange andre lande, være formulering af en national strategi vedrørende cybersikkerhed og kritisk IKT-infrastruktur. Dette er desværre ikke sket endnu til trods for de øgede trusler og de mange alarmerende angreb. I NATO, EU, USA og mange andre lande vi normalt sammenligner os med, er der for længst formuleret tværsektorielle nationale strategier på området. EU har endvidere gentagne gange formelt henstillet til de lande, der endnu ikke har formuleret en national strategi, at man trækker i arbejdstøjet.

Danmark tøver og er igen kommet sent fra start

Alligevel tøver Danmark, hvilket har medført en ukoordineret og ustruktureret tilgang til løsning af de ovenfor nævnte problemer og udfordringer. Det skyldes primært, at de få igangsatte initiativer gennemføres på operativt-driftsniveau i forskellige etater i stedet for strategisk og tværsektorielt i et tæt samarbejde på højt niveau med civile aktører.

Der er mange instanser, både statslige myndigheder og private virksomheder, beskæftiget med cybersikkerhed og beskyttelse af samfundsvigtig kritisk infrastruktur, men det sker i isolerede siloer med stort set vandtætte skotter imellem.

For yderligere at understrege behovet for en koordineret national indsats henvises til, at Danmark, i modsætning til de fleste andre EU lande, ikke deltager i European Cyber Security Month (ECSM), hvor der fokuseres på borgernes internetsikkerhed (eller mangel på samme). Set i lyset af statens tvangsdigitalisering forkommer det særligt graverende og ildevarslende at befolkningen ikke involveres i

vigtige oplysningskampagner, hvor de får muligheder for at blive orienteret og forberedt på de faldgruber og trusler, der findes på internettet og i cyberspace.

For yderligere information om ECSM se linket: www.cybersecuritymonth.eu

Sektoransvarsprincippet som snublesten

I Danmark gælder det ”hellige” sektoransvarsprincip, hvilket betyder, at det enkelte ministerområde har ansvaret for tiltag indenfor eget ressort. Det er langt hen ad vejen er et godt princip, bare ikke i relation til cyberspace og IKT kritisk infrastruktur, der går på tværs af alle sektorer og grænser, og er en forudsætning for (ligesom elektricitet) at sektorerne kan virke internt og interagere eksternt med andre samfundsvigtige funktioner.

I en rapport udarbejdet for Energistyrelsen af Security Lab som er et velrenomeret IT sikkerheds- og rådgivningsfirma står der bla., at man ved infiltration på såkaldte SCADA systemer (Supervisory Control and Data Acqusition) , der bl.a. bruges i forbindelse med trafikstyring, energiforsyning, industrielle processor med farlige stoffer m.v kan rette alvorlige angreb imod bl.a el-, vand og varmeforsyningen i Danmark. Hacking af det iranske atomprojekt skete formodentligt via et SCADA system ved brug af et inficeret USB-stik.

Risikoen

I Beredskabsstyrelsens *Nationale Risiko Billede* anføres cyberangreb endvidere, som værende et blandt de ti centrale risikoscenarier for Danmark På side 50 står der f.eks., at ”*cyberangreb ikke noget nyt fænomen, men cyberangreb kan i dag have større konsekvenser, dels fordi det moderne samfund bliver stadig mere afhængigt af IKT, dels fordi ITK-anvendelsen i stigende grad finder sted i indbyrdes forbundne netværk med enten direkte eller indirekte internetopkobling. Højere grad af integration betyder større kompleksitet og dermed også flere potentielle sårbarheder over for cyberangreb.*

Envidere står der, at ”Cyberangreb har, i de former der er konstateret hidtil, ikke direkte kostet menneskeliv. Cyberangreb kan imidlertid potentielt true en række kritiske samfundsfunktioner, og dermed få afledte konsekvenser for liv, helbred og velfærd. Cyberangreb vurderes således at kunne frembringe ulykker eller andre situationer, der ud over materielle skader også bringer menneskeliv i fare – enten forsætligt eller som utilsigtet sideeffekt. Det kunne fx ske, hvis cyberangreb rammer kritiske IKT-systemer hos politi, redningsberedskab og sundhedsberedskab, eller hvis de rammer visse SCADA systemer, som bruges i forbindelse med trafikstyring, energiforsyning, industrielle processer med farlige stoffer mv.”

I diverse medier omtaltes for nylig et omfattende angreb imod borgernes CPR-numre og persondata afsløret. Angrebet blev ikke opdaget i Danmark, men i Sverige, der venligt fortalte det videre til dansk politi. Først mange måneder senere blev angrebet offentliggjort til den undrende danske befolkning.

Politisk sagsbehandling

Justitsministeren havde svært ved at forklare sig (og henviste til ressourceproblemer og manglende tid) og sendte sagen videre (til hjørnespark) til behandling i en til formålet oprettet gruppe mhp. at komme med en rapport og redegørelse på et senere tidspunkt.

For at demonstrere politisk handlekraft kunne Justitsministeren, få dage efter et indkaldt samråd om CPR-sagen oplyse, at der nu ville blive oprettet en Cybersikkerhedssektion i regi af Politiets Efterretningstjeneste. Et tiltag, der forekommer uigennemtænkt, ukoordineret med øvrige tiltag, ikke ressourcesat, og derfor forventeligt uden større virkning. Sådan klarer man den i politiske kredse.

Det sidste nye er, at man i efteråret 2013 i Folketingets Retsudvalg forbereder en eksperthøring bag nedrullede gardiner og hermetisk lukkede døre, for at afklare, hvad CPR-sagen har medført af skade på den danske befolkning.

Når rapporten fra Retsudvalgets ekspertgruppe (forhåbentlig) på et eller andet tidspunkt offentliggøres, vil det ikke undre, hvis den fritager involverede myndigheder og politikere for et ansvar (håndvaskeprincippet). Dele af den vil sandsynligvis også blive klassificeret, så vigtige passager og oplysninger ikke kommer til offentlighedens kendskab (idet rapporten udarbejdes af Politiets- og Forsvarets Efterretningstjeneste).

Offentlig – Privat – samarbejde nødvendigt

Koordinationen imellem de forskellige civile og militære aktører, der aktivt og 24/7/365 arbejder med bekæmpelse af cyberangreb m.m., skal styrkes ved en koordineret indsats, herunder anvendelse af de eksisterende kapaciteter og instanser under udvikling. Uhensigtsmæssige knobskydninger, der koster rigtig mange penge, har der været for mange af. Løsningen bør være en national sikkerheds- og forsvarspolitisk tilgang, hvor der til at begynde med udarbejdes en samordnet national tværsektoriel strategi for området samt en konkret og struktureret handlingsplan. Umiddelbart forekommer Statsministeriet som værende den rette instans til af lede og koordinere dette arbejde i et tæt samarbejde mellem relevante ministerier og relevante private virksomheder.

For god ordens skyld skal nævnes, at offentlige myndigheder allerede tilbydes opstilling af diverse udstyr, der skal muliggøre tekniske aflæsninger af evt. uhensigtsmæssig trafik centralt. Men det er en driftsmæssig foranstaltning, der langt fra tilgodeser behovet for en national strategisk tilgang og løsning.

Computer Network Operations

I forsvarsaftalen fra 2012 er der afsat betydelige midler (150 mill. årligt) til etablering af såkaldte Computer Network Operations (CNO) kapaciteter. I Forsvarsministeriet har man længe arbejdet med CNO, men er mig bekendt endnu ikke færdig med konkrete bud eller løsninger på, hvordan projektet skal udmøntes i praksis. Også CNO projektet bør ses i en større sikkerhedspolitisk kontekst, og ikke kun snævert i forsvarets regi, og kan ikke træde i steder for en national strategi på tværs af sektorerne.

Der findes som nævnt oven for allerede nogen cyberkapacitet ved bl.a. politiet og forsvaret og der er planlagt yderligere tiltag, f.eks førnævnte cybersektion ved PET og de nævnte kommende CNO kapaciteter i forsvaret. Og der er også stor viden, kapaciteter og ressourcer i mange andre sektorer (f.eks. finanssektoren) og ved private virksomheder og teleoperatører, der ejer det meste af Danmarks kritiske IKT infrastruktur, jf. outsourcing og privatsering nævnt tidligere.

Endvidere er der i EU for ganske nylig oprettet et European Center for Cybercrime (EC3), der har en dansk chef. Hvorfor ikke benytte en god anledning til at få alle initiativer og kapaciteter samt private

virksomheder til at trække på samme hammel? Se bort fra brødnid, siloer og vandtætte skotter, og træk i arbejdstøjet.

Cybersikkerheden i Danmark er (desværre) for ringe

Cybersikkerheden i Danmark er desværre for ringe, og i særlig grad fordi der savnes en overordnet sikkerheds- og forsvarspolitisk tilgang og løsning på de mange udfordringer, som en globaliserede og digitaliserede verden har medført. Specielt er jeg forundret over den fraværende offentlige debat og politikernes ligegyldighed, idet mange anser *"Cyberwarfare" og CNO,* som værende en ny dimension i sikkerhedspolitik og krigsførelse. Nogle, f.eks. Richard A. Clarke og Robert K. Knake, har i bogen "Cyberwar "(fra 2010) endog det synspunkt at "cyberkrigen" allerede er i gang og foregår 24/7/365. På side 41 I bogen "Cyberwar" står der f.eks., at *" Cyberspace is a contested domain, and the fight is on – today."*

John Michael Foley/ Center for Offentlig-Privat IKT-Sikkerhedssamvirke (Resilience & Cyber Security) samt Danmarks repræsentant i EU's Network and Information Security Platform (NIS) med reference til EU's vicepresident Nellie Kroes.