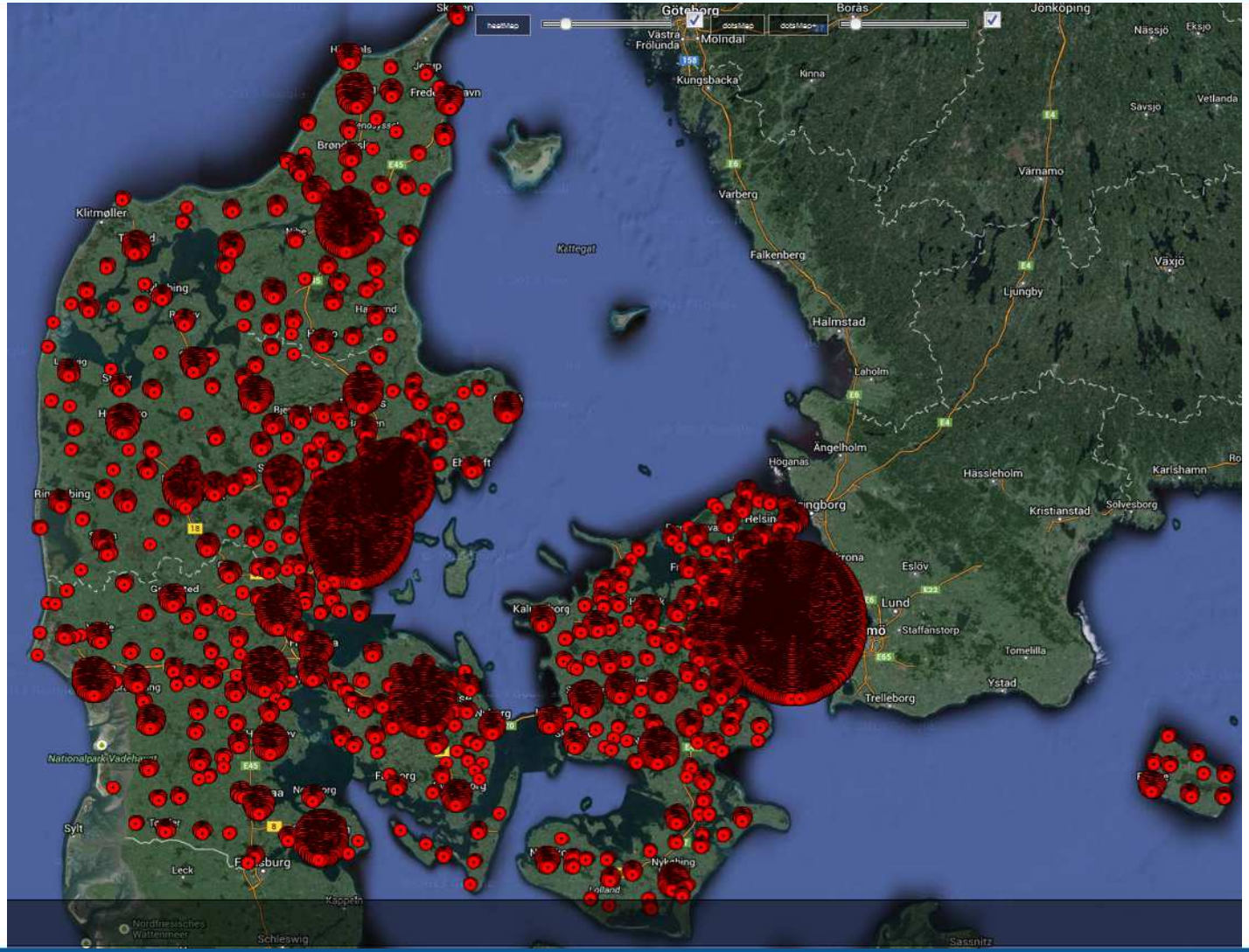
Åben høring, Folketinget

Varetagelse af persondata i det private

Peter Kruse (pkr@csis.dk)
Head of CSIS eCrime and Research & Intelligence Unit

PGP-ID: 0x715FB4BD
Fingerprint: E1A6 7FA1 F11B 4CB5 E79F 1E14 EE9F 9ADB 715F B4BD


Göteborg
Borås
Jönköping
Nässjö
Eksjö
Vetlanda
Savsjö
Värnamo
Växjö
Ljungby
Varberg
Falkenberg
Halmstad
Laholm
Ängelholm
Höganäs
Hässleholm
Karlshamn
Kristianstad
Solvesborg
Eslöv
Lund
Staffanstorp
Tomelilla
Ystad
Trelleborg
Kungsbacka
Kinna
Mölndal
Västra Frölunda
Kattegat
Klitmøller
Sylt
Leck
Schleswig
Sassnitz

Offentlige data i private løsninger

- Det private leverer services og tjenester til det offentlige. Men behandles, transmitteres og opbevares disse data forsvarligt?
- Talrige sager, herunder i særdeleshed CSC hændelsen demonstrerer manglende kontroller fra offentlig side med deres leverandør, ligesom det illustrerer lemfældig omgang med grundlæggende best practise indenfor IT-sikkerhed herunder mangelfuld overvågning og tilsyn med systemer og servere, forældede løsninger og software, svigtende policies og forfejlet sikkerhedsarkitektur anno 2014.
- Private virksomheder har et medansvar i at sikre borgernes data - og generelt offentlige løsninger. Mange data transporteres i det daglige mellem offentlige og private systemer, og potentielt videre ud i skyen. Indlysende skal de data beskyttes mod angreb og overvågning.

Krav til private løsninger og leverandører

- Allerede i projekt fasen skal it-sikkerhedsmæssige aspekter belyses, så løsningerne ikke bare ”virker”, men også er forsvarligt designet og implementeret og sikres vedligeholdelse og opfylder best practise indenfor it-sikkerhed.
- Kontraktligt skal der arbejdes på at forpligte de private leverandører bedre. Det offentlige, som har det egentlige ansvar for borgenes følsomme oplysninger, skal føre tilsyn og kontroller med de private leverandører.
- Private virksomheder skal løbende dokumentere at der foretages revision af en ekstern part. Hos CSIS, med ca. 40 ansatte, er vi f.eks. kontrakteligt forpligtet til at dokumentere vores it-sikkerhedspolitik, compliance, backup procedurer, logning og overvågning, business continuity, fraud, hvidvaskning m.v. Er det ikke rimeligt, at staten og det offentlige, stiller samme krav til deres leverandører og måske særligt med en sådan størrelse og setup som de skal beskytte?
- Der bør implementeres et ISP filter, som blokerer for trafik som afsendes til kendte og veldokumenterede BOTnet servere. Det vil mindske risikoen for datalækager som i dag repræsenterer en betydelig risiko mod bl.a. vores konkurrence evne samt angreb mod kritisk infrastruktur.