Rådet for Digital Sikkerhed

Velkommen til nyhedsbrev fra Rådet for Digital Sikkerhed, april 2025

Alarmklokker med besindighed

Henning Mortensen og Anne Dorte Bach, Rådets formandskab

Alarmberedskabet har indfundet sig. I slipstrømmen af den geopolitiske situation, toldmure og handelskrig ulmer bekymringen i forhold til Danmarks og Europas digitale infrastruktur. Vi skal både steppe op i forhold til mulige cyberangreb og overveje om vores afhængighed af digitale tjenesteydelser fra USA i sig selv kan udvikle sig til en alvorlig udfordring.

Digital suverænitet

Afhængigheden af amerikansk teknologi har vi kendt til i mange år, og det gælder hele teknologistakken – hardware, netværk, storage og applikationer. Man kan mene, at vi har været naive; men omvendt har Danmark og mange europæiske lande taget digitaliseringen til sig og benyttet de funktionelle og effektive tjenester, som hovedsageligt er udviklet af amerikanske leverandører, og som har været og er til gavn for erhvervslivet og velfærdssamfundet. Og vi har frem til for nylig udviklet løsningerne i samklang med de europæiske regler for cybersikkerhed og persondatabeskyttelse og ikke mindst de europæiske værdier, som er udtrykt EU's charter om grundlæggende rettigheder.

De seneste måneders kommunikation på tværs af Atlanten har imidlertid ikke været helt fin i kanten. Situationens alvor understreges af Jacob Herbst, formand for regeringens cybersikkerhedsråd og medlem af Rådet for Digital Sikkerheds bestyrelse, der for nylig udtalte, at vi ikke kan *"... udelukke, at der kan ske en optrapning: At handelskrigen breder sig til det digitale. Sandsynligheden er ganske lille, fordi det vil være et gigantisk amerikansk selvmål. Men konsekvenserne vil være kæmpestore for det danske samfund. Derfor er det en betydelig risiko, som vi er nødt til at planlægge efter"* (Politiken, 6. april 2025).

I Europa har vi åbnet skufferne til digitale investeringer navnlig inden for cloudteknologi, kunstig intelligens og digital autentifikation. Rådet for Digital Sikkerhed hilser EU's initiativer velkommen. De er perspektivrige ved at have fokus rettet mod at styrke og udvikle de bærende elementer i den europæiske digitale infrastruktur med europæiske løsninger. Der er ikke tale om at smide de amerikanske aktører ud af det digitale Europa, men om at skabe nye præmisser for det transatlantiske samarbejde. Man kan læse mere om nogle af de europæiske initiativer i en kronik om digital suverænitet af Rådets sekretariatschef, Claus Hjorth fra marts.

Udviklingen henimod større digital suverænitet i Europa suppleres af en række tiltag, hvor EU sætter fokus på forskellige aspekter af sikkerhed, modstandskraft og beredskab, hvor følgende aktuelle initiativer kan fremhæves: European internal security strategy, Whitepaper for European defence og EU Preparedness Union

Strategy. Endelig bør det nævnes, at EU's initiativ om European Democracy Shield i øjeblikket er i høring med frist sidst i maj 2025.

Cybersikkerhed
På cybersikkerhedsområdet følger vi udviklingen i det generelle trusselsbillede. Senest har Styrelsen for Samfundssikkerhed (SAMSIK) i marts 2025 hævet trusselsniveauet for cyberspionage mod telesektoren fra middel til høj. Netop cyberspionage vurderes at indgå i forberedelsen af destruktive cyberangreb. De digitale risici understreges i det Nationale Risikobillede 2025 som blev offentliggjort 10. april. Under overskriften 'Danmark står over for det mest alvorlige risiko- og trusselsbillede i årtier' fremhæver Beredskabsministeren Torsten Schack Petersen: " *Vores samfunds basale funktioner skal kunne fungere – også hvis der sker cyberangreb mod vores kritiske infrastruktur..."*

Rådet for Digital Sikkerhed deltager aktivt i at styrke Danmarks cybersikkerhed. I øjeblikket varetager Rådet formandskabet for et offentligt-privat samarbejde om de helt basale sikkerhedsanbefalinger til Danmarks små- og mellemstore virksomheder. Nøglen til at skabe klarhed om, hvad små virksomheder med få midler kan gøre for at højne sikkerhedsniveauet, er, at myndigheder, brancheorganisationer, forsikringsbranchen og ikke mindst eksperter er enige om det helt grundlæggende og taler det samme sprog. Samarbejdet finder sted i regi af Cybersikkerhedspagten i samarbejde med SAMSIK. Rådets formand er også aktiv i den arbejdsgruppe, som giver bidrag til udformningen af vejledningerne til NIS2, hvor det bl.a. er Rådets formål at sikre, at vejledningerne bliver praktisk operationelle og kan anvendes i tilknytning til kendte standarder.

Folketingets behandling af NIS2-loven er i gang og ventes afsluttet inden sommer. Rådet følger arbejdet tæt og har her i starten af april afholdt et medlemsmøde med Ministeriet for Samfundssikkerhed og Beredskab om sigtelinjerne for den endelige lov samt ikke mindst de vejledninger, der er undervejs. Rådets medlemskredsen har modtaget et resume af mødet med ministeriet.

Ændring af PET-loven
Regeringens forslag til ændring af loven om Politiets Efterretningstjeneste (PET-loven), som ventes fremsat i denne Folketingssamling med ikrafttræden til juli 2025, har skabt stor debat. Lovforslaget vil fastsætte regler for PET's behandling af 'større sammenhængende datasæt' fra offentligt tilgængelige kilder, den offentlige forvaltning og registre fra udenlandske myndigheder. Udover at skabe et tydeligt lovgrundlag for PET's databehandling af de store datasæt, vil PET få mulighed for at foretage såkaldt 'ikke personrettede behandlinger' i datasættene. Ifølge Justitsministeriet pressemeddelelse vil de nye muligheder for PET *"... være afgørende for at opdage potentielle terror-, sabotage- og eller spionagetrusler i tide"*.

I Politiken den 31. marts peger Pernille Boye Koch, Institut for Menneskerettigheder på, at der er tale om et paradigmeskift i den måde PET hidtil har arbejdet på, hvor man uden konkret mistanke kan lave meget præcise profileringer af folk. Instituttet *"... efterlyser en markant stærkere retssikkerhedsgaranti for borgerne i lovforslaget i form af eksempelvis en uafhængig juridisk instans til at vurdere de datakilder, som PET vil analysere, samt en transparens for borgerne i, hvordan de bliver overvåget". S*ynspunktet er afspejlet i Institut for Menneskerettigheders høringssvar af 6. marts 2025, som blev præsenteret af instiuttets chefjurist Mikkel Lindberg Laursen for Rådets bestyrelse sidst i marts. Bestyrelsen tilsluttede sig hovedlinjerne i instituttets høringssvar.

Alarmberedskab kræver besindighed. Den digitale dagsordens tre aktuelle hovedtemaer – digital suverænitet, cybersikkerhed og privatlivsbeskyttelse – kan ikke klares med kvikke fix. Investering og udvikling kræver viden og dialog både for at handle strategisk klogt og for ikke at tabe de europæiske værdier af sigte. Rådet for Digital Sikkerhed er et godt netværk til at bygge bro mellem myndigheder, forskningen og erhvervslivet fra både arbejdsgivere og arbejdstagere. Vi kan kun opfordre til, at man melder sig under fanen.

Vil du være med til at fremme et trygt og frit digitalt samfund?

Bliv medlem af Rådet for Digital Sikkerhed. Se her hvordan og følg Rådet på LinkedIn, hvor vi jævnligt opdaterer nyheder, informerer om Rådets arbejde og kommende projekter!

Rådet for Digital Sikkerhed