En IT-politik udover det sædvanlige

IT-politisk udspil og arbejdsplan af Niels Callesøe, SF, marts-maj 2019.

En af de store udfordringer vi har i Danmark, er manglen på politikere med indsigt i IT. De mange sager om kuldsejlede digitaliseringsprojekter, tabte persondata og hovsa-lovgivning taler deres tydelige sprog.

I virkeligheden er det ikke så underligt. Det er et komplekst stofområde, med mange faldgruber og stærke lobbyister. Derfor kan det være svært for en folkevalgt med en anden baggrund at skille skidt fra kanel.

Som et første skridt til at rette op vil jeg her kort redegøre for en række helt centrale IT-politiske emner, baseret på en lang karriere indenfor området. Til de folketingsmedlemmer og -kandidater der mangler en IT-politik, siger jeg: Tag min!

Jeg er ganske vist selv folketingskandidat, men jeg vil gerne dele. IT-politik kan meget dårligt være partipolitik, og alle vinder hvis vi løfter den fælles forståelse af området. Så kopier min politik. Byg videre på den. Gør den bedre. Sådan som vi gør i branchen.

Indeks:

En anden dagsorden for udbud af offentlige opgaver

Mange af de følgende punkter hænger sammen, så lad mig starte med en helt grundlæggende ændring vi har stærkt behov for. Rammerne er i nogen grad dikteret af internationale aftaler, men der er stadig meget vi kan gøre anderledes end vi gør nu.

Vi har set, gentagne gange, hvordan den eksisterende udbudsmodel for offentlig IT fører til ekstremt store opgaver der går til ekstremt store leverandører, og hvor den mindste ændring i forudsætninger eller vilkår kan betyde at hele projektet må skrottes, med udgifter i milliard-klassen og enorme forsinkelser til følge. I første række er det oplagt at staten udvider sine egne evner til at kunne eksekvere og implementere mindre IT-opgaver, så ikke alt skal i udbud. Men selv med en sådan enhed, vil mange opgaver stadig skulle varetages af private aktører.

Derfor er det centralt at vi gør op med den nuværende tilgang til IT-udbud, hvor opgaver typisk udbydes som én kæmpestor aftale. I stedet har vi brug for at statens udbud deler opgaver op i mindre enheder og engagerer vækstlaget, i stedet for de internationale mastodonter. Dette kunne enten foregå ved pre-udbud eller ved at etablere en statslig enhed med kompetencerne til opgaven.

Skulle det vise sig at være problematisk i forhold til EU-lovgivning på udbudsområdet, må der findes løsninger på det, og Danmark må arbejde for at få undtagelser eller ændringer af udbudsreglerne. Det er ikke i vores interesse at rigide regler forhindrer os i at vælge de leverandører der er bedst til opgaven, frem for dem der er bedst til rigide regler.

Langt det bedste arbejde, langt de bedste løsninger, laves ikke af de største firmaer, med de største aktiekapitaler. De skabes af de skarpe og internationalt anerkendte, danske leverandører i lille- og mellemstørrelsen. Deres størrelser giver mulighed for at være langt mere fleksible, innovative og omkostningseffektive end de store spillere. Man kan også langt bedre pege på IT-projekter der er blevet en succes, med den type leverandør ved rorpinden.

Til gengæld har mastodonterne et, ret ufortjent, ry for at være mere stabile og sikre, særligt i forhold til at levere support til deres løsninger på længere sigt. Historien med de danske løsninger viser tydeligt at danske projekter har langt større succes når leverandørerne ikke er kæmpestore aktører.

Om det alene skyldes de førnævnte forhold, eller om det også spiller ind at mellemstore virksomheder er langt mere motiverede for at levere kvalitet til en statslig aktør, er ikke til at sige. Men vi skal under alle omstændigheder understøtte det der tydeligvis virker bedst.

Behovet for stabile løsninger der kan vedligeholdes i mange år fremover, er dog reelt nok. Hvilket leder mig til min næste pointe:

Udgangspunktet for dansk IT skal være fri og åben

Absolut den bedste måde at sikre at offentlige systemer er stabile, sikre, relativt fejlfri og kan vedligeholdes af andre end de oprindelige udviklere, er at gøre så meget kode som muligt offentligt tilgængelig som fri og åben software.

Det bør i øvrigt være det naturlige udgangspunkt for alt arbejde der udføres for offentlige midler, at resultatet -- ikke bare produktet -- kommer så mange som muligt til gode. Derfor skal offentlige udbud kræve at der i videst muligt omfang anvendes åbne teknologier, og at kildekoden gøres offentligt tilgængelig. Andre virksomheder og uddannelsesinstitutioner vil kunne drage stor nytte heraf, og samfundsværdien af det offentligt udførte arbejde øges markant.

Naturligvis vil der være systemer eller elementer der af forskellige årsager ikke kan gøres fuldstændigt åbne. Men åbenhed skal være udgangspunktet. Ikke bare for kildekode, men også for design, API og procesbeskrivelse. Selv hvor kildekode eller andre forhold ikke kan gøres offentligt tilgængelige, skal det stadig være et krav at anvende standardiserede og åbne API'er i videst muligt omfang.

Vi skal også sikre at både kode og rettigheder til ethvert offentligt projekt deponeres, så det offentlige kan skifte hvis leverandøren går konkurs eller misligholder kontrakten. I det hele taget skal det altid være sikret at der kan skiftes leverandør(er) på en offentlig IT-løsning, uden at arkitektur, design eller øvrige aftaler skal genopbygges fra bunden.

Endnu mere fokus på offentligt tilgængelige data

På samme måde som kildekode og processer skal være åbne, skal data der indsamles, beregnes eller på anden måde udarbejdes af offentlige institutioner, gøres offentligt tilgængelige hvor det er muligt. Som ovenfor vil det ikke altid kunne lade sig gøre eller være klogt. For eksempel sætter GDPR en række oplagte begrænsninger. Men vi har allerede en god tradition for at gøre mange offentlige data tilgængelige fra Danmarks Statistik, Geodatastyrelsen m.fl., og den praksis skal understøttes og udvides til at omfatte flere datasæt i fremtiden.

Beskyttelse af det digitale privatliv

Efter den snak om åbenhedens fortræffeligheder, er det vigtigt at påpege et område der ikke kræver yderligere åbenhed. Tværtimod. Det drejer sig selvfølgelig om borgernes ret til privatliv og til råderetten over deres egne data. I samme spor som EU, der har begrænset mulighederne for at misbruge data ved at vedtage GDPR, har vi brug for særlig forbrugerbeskyttelse efter danske forhold.

Udgangspunktet for udbud skal være at borgerens ret til at begrænse og godkende brugen af sine egne data bør være beskrevet og sikret i hovedprojektet. Udgangspunktet for politikudvikling skal være, at borgeren har retten til at bestemme over sine egne data, både om borgerens person og borgerens adfærd, så længe den ikke overtræder loven.

Derfor skal vi, hurtigst muligt, tilbagerulle de ulovlige dele af logningsbekendtgørelsen, og vi skal sikre at der altid ligger en dommerkendelse til grund for et indgreb i meddelelseshemmeligheden. Loven om samme skal opdateres til at svare til den moderne tid og tage højde for moderne teknologi. Vi skal absolut ikke mørklægge alle data eller forhindre forskning eller samkørsel, men vi skal sikre, at det kun sker med borgerens informerede samtykke.

Det skal, på samme måde som ovenfor, være et krav at offentlige IT-løsninger gennemgår en uvildig sikkerhedsanalyse der skal sikre at borgernes data holdes hemmelige i det nødvendige omfang, og at leverandøren holdes ansvarlig for at sikkerheden i de leverede systemer lever op til en høj standard. Både hvad angår databeskyttelse og sikring af systemerne mod nedbrud eller angreb fra fremmede magter.

Med samme formål for øje skal der etableres bedre beskyttelse af forskere og andre der undersøger software og systemer for sårbarheder, således at de ikke risikerer at komme i klemme hvis de afslører problemer på ansvarlig vis.

Etablering af IT-Havarikommission

Der bør etableres en IT-Havarikommission. Den skal have til opgave at afdække både om ovennævnte er overholdt og årsagerne til større IT-relaterede hændelser. I tilfælde af omfattende datatab, nedbrud af samfundsmæssigt skadeligt omfang, og når større, offentlige projekter kuldsejler som vi ganske ofte har set de senere år.

Kommissionen skal, ved egen drift og fuldstændig uafhængigt, kunne undersøge de mest

alvorlige af disse sager. Der skal samtidig være pligt til, for offentlige og private aktører, at indberette hændelser af samfundsvæsentlig størrelse, så kommissionen kan tage stilling til om den vil gå ind i en sag.

Ud over at beskrive forløb, og evt. henvise til domstol med henblik på at placere ansvar, skal kommissionen også kunne udarbejde forslag til forbedringer der kan forhindre lignende katastrofer i fremtiden. Kommissionens arbejde og anbefalinger skal, i det omfang det giver mening, gøres offentligt tilgængelige, således at alle kan lære af de største katastrofer. På den måde vil omkostninger til kommissionens arbejde blive langt oversteget af den forventede samfundsmæssige gevinst.

Udover Havarikommissionen skal det overvejes, om den nuværende ombudsmand skal suppleres med en egentlig IT-ombudsmand der kan og skal være forbrugernes vagthund i IT-sager, og som har ret og pligt til at påtale grove tilfælde af uansvarlig omgang med data eller IT-sikkerhed. Ikke som en erstatning for GDPR, men som et supplement.

Absolut ingen eValg eller statslig blockchain

Sidst, men ikke mindst, er det centralt at sikre dødsstødet til et par grundlæggende dårlige ideer der optager politikere og medier verden over langt mere end de har meritter til. Disse koncepter skal skrinlægges og der skal ikke spildes mere tid på at gentage diskussioner som for længst er afgjort.

Den første er eValg. Altså ideen om at folketingsvalg kunne foretages elektronisk, så borgeren ikke behøver møde fysisk frem på valgstedet. Som ekspert i IT-infrastruktur og -sikkerhed kan jeg, med en lang række forskere og mere prominente eksperter i branchen i ryggen, slå fuldstændigt fast at det ikke er en farbar vej for vores demokrati.

Det er fuldstændig centralt at vores valghandlinger er til at forstå for menigmand, og umulige for fremmede eller indre magter at manipulere så der opstår tvivl om resultat eller gyldighed. Disse krav er umulige at opfylde med eksisterende teknologi, og der er ingen tegn på bedring af disse forhold i fremtiden.

Helt så afvisende behøver vi ikke være over for teknologi der optimerer lokalt på valgstederne og sikrer kvittering mv. Men al teknologi, der berører vores valg, skal være 100% åben software, så alle har mulighed for at kigge den demokratiske proces i kortene.

Det andet ubrugelige koncept er blockchain. Langt de fleste af os tænkte det var vældigt spændende dengang det var et nyt koncept. Men det er det ikke længere, og det er nu entydigt at blockchains ikke har løsningen på nogen problemer der ikke kan løses bedre på anden vis.

Samtidig har virtuelle valutaer, som eksempelvis Bitcoin, vist sig at være et udmærket alternativ for kriminelle til hvidvask og afpresning, men ikke rigtig have funktioner for lovlydige borgere.

Måske endnu værre er den store klimapåvirkning af de enorme energimængder der skal til for at opretholde de virtuelle valuta, en international katastrofe. Derfor skal vi ikke blot afvise at bruge blockchains til offentlige opgaver, vi skal også nedsætte en arbejdsgruppe der skal komme med forslag til hvordan vi bedst modvirker det enorme energispild, både i Danmark og i EU-regi.

Etablering af civil digital sikkerhedstjeneste

Det nuværende Center For Cybersikkerhed (CFCS) er et nødvendigt organ i sikring af danske interesser over for udenlandske aktører. Derfor giver det også mening, at det er organiseret under Forsvarets Efterretningstjeneste. Men samtidig har CFCS fået ansvaret for en lang række opgaver der ikke er af militær karakter, og som bør håndteres i det civile system, og med langt større gennemsigtighed end det er muligt under FE.

Derfor skal der etableres en civil digital IT-sikkerhedsfunktion (arbejdstitel: CDS) der skal overtage en række funktioner fra CFCS, og samtidig påtage sig en række nye opgaver der ikke løftes i dag. Først og fremmest med den kongstanke at den primære opgave er at understøtte og uddanne offentlige og private virksomheder og foreninger i IT-sikkerhed, og på den måde styrke Danmarks sikkerhedsstilling. Frivillighed skal være omdrejningspunkt for at løfte det danske bundniveau for sikkerhed, ikke tvungne foranstaltninger.

I den nye form skal CDS opbygge indgående viden om cybersikkerhedstrusler og stille den viden til rådighed i form af offentligt tilgængelige analyser, best practices og målrettet rådgivning og undervisning til virksomheder og institutioner. Målet er ikke at erstatte det velfungerende, private marked for sikkerhedsydelser, men løfte det generelle bundniveau og samtidig åbne organisationernes øjne for informationssikkerhed som central politik. I alt må efterspørgslen efter sikkerhedsydelser forventes at stige, ikke falde, som konsekvens.

Produktansvar på software

En større og større del af vores hverdag baserer sig på computersystemer. Ikke bare de store, dem vi sidder ved, eller kører rundt i. Men i virkeligheden langt mere de små vi ikke tænker så meget over, men hvis antal vokser eksponentielt i disse år. Ure, målere, støvsugere, vaskemaskiner, listen er uendelig. Fælles for dem er at de alle sammen indeholder computere, og disse computere indeholder software.

I princippet er det meget fint. I praksis har det desværre vist sig at meget af den software vores enheder indeholder, er af meget lav kvalitet, hvilket kan medføre en lang række problemer med sikkerhed eller funktioner. Men i modsætning til stort set alle andre produkter på markedet, er selve softwaren ikke omfattet af produktansvar. Det skal laves om.

Det er bydende nødvendigt, at vi begynder at stille krav til software-leverandører om at deres software ikke bare skal være af absolut lavest mulige kvalitet for at få produktet til at køre. Vi skal stille krav om at software skal kunne opdateres hvor det giver mening, og om at kvaliteten lever op til visse standarder. Gør den ikke det, skal produkter kunne tilbagekaldes, såfremt producenten ikke kan eller vil gøre en opdatering tilgængelig, uden beregning.

Den ekstra omkostning som produktansvar vil betyde for producenterne, vil betyde marginalt højere priser på en række produkter. Men på samme måde som andre typer produkter er blevet af markant højere kvalitet, vil effekten være den samme på software, og den samfundsøkonomiske gevinst være enorm. For nogle typer producenter kan man evt. lave open source eller source-escrow-aftaler, eller -krav, således at det sikres at andre kan udvikle på software for produkter hvor producenten ikke længere findes, hvis der er et marked for det.

Dansk kontrol med kritisk IT-infrastruktur

Indtil for nylig har der manglet en vigtig diskussion på Christiansborg om at sikre at den mest centrale infrastruktur bevares under dansk kontrol. Den dagsorden er heldigvis blevet løftet, og et politisk flertal har tilkendegivet at man fra nu af vil arbejde i den retning.

En vigtig pointe er dog at kritisk infrastruktur i høj grad også omfatter IT-systemer og -løsninger der understøtter sundhedsvæsenet, energisektoren mv. Derfor skal vi sørge for at også IT-systemer vurderes med henblik på at komme ind under paraplyen af kritisk infrastruktur, så vi kan sikre at vi beholder den overordnede kontrol på danske hænder.

Det bliver ikke nogen let opgave, for som bekendt er IT-verdenen massivt globaliseret. Når det alligevel er værd at bruge energi på, skyldes det forholdet mellem sandsynligheden for at der kan opstå problemer med løsninger der er kontrolleret uden for dansk rækkevidde, og den meget store potentielle skadevirkning det vil have for vores samfund, hvis de mest centrale systemer lammes i længere tid.

Fin