



Test dig selv

Hvor digitalt suveræn er din organisation?

Tekst Timme Bisgaard Munk



En guide til kommunikationsafdelingen

Digital suverænitet lyder som noget, IT-afdelingen skal tage sig af. Det er det også. Men det er samtidig et spørgsmål, der rækker langt ud over serverrum og krypteringsnøgler. Det handler om, hvem der i sidste ende bestemmer over jeres organisation. Hvem der kan lukke for jeres systemer. Hvem der ejer jeres data. Og hvem der kan diktere jeres fremtid.

Det er spørgsmål, kommunikationsafdelingen skal kunne besvare. Ikke fordi I skal konfigurere firewalls, men fordi I skal kunne forklare ledelsen, hvad der er på spil. Fordi I skal kunne fortælle historien om, hvorfor digital suverænitet ikke bare er et teknisk anliggende, men et strategisk, værdimæssigt og i sidste ende politisk spørgsmål.

Denne test hjælper jer med at finde ud af, hvor jeres organisation befinder sig på rejsen mod digital suverænitet. Den er designet til at kunne besvares uden teknisk ekspertise. I skal ikke vide, hvordan en API fungerer. I skal vide, om jeres organisation har overblik, kontrol, og en plan.

Testen er bygget op omkring fem niveauer. Hvert niveau repræsenterer en grad af digital selvbestemmelse. For at placere jer på et niveau, skal I kunne svare ja til alle spørgsmål på det pågældende niveau og alle niveauer under.

Start fra bunden. Vær ærlige. Der er ingen skam i at opdage, at I befinder jer på trin nul. De fleste gør. Skammen ligger i ikke at ville vide det.

Timme Bisgaard Munk er fellow ved Center for Digital Democracy på SDU, hvor han med støtte fra TrygFonden undersøger, hvordan offentlige og private organisationer kan vurdere og håndtere deres digitale afhængigheder.

Projektet tager udgangspunkt i en simpel, men ofte overset erkendelse: De fleste organisationer har i dag dyb afhængighed af en håndfuld amerikanske techgiganter, uden at have et klart billede af, hvad den afhængighed faktisk betyder for deres handlefrihed, datasikkerhed og langsigtede strategiske råderum.

Som del af projektet har Timme udviklet selvevalueringsværktøjer, scenarieøvelser og samtalekort, der skal gøre digital suverænitet til en konkret ledelsesdiskussion fremfor et abstrakt politisk begreb.

En del af disse redskaber er lagt ud her digitalt hos DM til fri og tryk afbenyttelse, så organisationer selv kan tage dem i brug og tilpasse dem til deres egen kontekst.

Værktøjerne er designet til at møde organisationer der, hvor de er, og hjælpe dem med at stille de rigtige spørgsmål til deres egen teknologiske situation. Formålet er ikke at levere færdige svar eller pege på bestemte løsninger. Det er at synliggøre de trade-offs og værdimæssige præmisser, som forskellige strategiske tilvalg og fravalg bygger på. For digital suverænitet er i sidste ende ikke et teknisk spørgsmål. Det er et spørgsmål om, hvilken grad af kontrol og selvbestemmelse en organisation vil acceptere i sin digitale infrastruktur.

Niveau 0

Den digitale søvngænger

Trade-off: I bytter infrastrukturel magt og strategisk handlerum for bekvemmelighed og hurtig adgang til teknologi.

Hvad slår hvad: Bekvemmelighed slår frihedstrang. I har valgt den lette vej og fortrængt prisen.

Værdimæssig position: Utilitaristisk kynisme. I har maksimeret kortsigtet nytte og ignoreret de langsigtede konsekvenser for organisationens autonomi og borgernes rettigheder.

På dette niveau har organisationen ingen reel kontrol over sin digitale infrastruktur. I er 100 procent afhængige af tech-giganternes vilje, teknologi og lovgivning. I har byttet frihed for bekvemmelighed.

Spørgsmål til niveau 0

- 1. Ved I, hvem jeres vigtigste digitale leverandører er?*
Kan I på stående fod nævne de tre til fem vigtigste leverandører, jeres organisation er afhængig af i det daglige? Tænk på e-mail, dokumenthåndtering, kalendersystemer, videomøder, cloud-lagring. Hvis svaret er "det ved IT-afdelingen", er svaret nej.
- 2. Ved I, hvilket land jeres primære leverandører hører hjemme i?*
Er jeres e-mailsystem amerikansk, europæisk eller noget tredje? Hvad med jeres cloud-lagring? Jeres videokonferenceløsning? Det handler ikke om, hvor serverne står, men om hvilket lands lovgivning leverandøren er underlagt.
- 3. Har I nogensinde spurgt, hvad der sker, hvis en leverandør lukker for adgangen?*
Ikke fordi de går konkurs. Men fordi de vælger at gøre det. Eller fordi en regering beordrer dem til det. Har I stillet spørgsmålet? Har I fået et svar?
- 4. Ved I, om jeres data kan tilgås af udenlandske myndigheder?*
Amerikanske virksomheder er underlagt CLOUD Act, som betyder, at amerikanske myndigheder kan kræve adgang til data, uanset hvor i verden de befinder sig. Ved I, om jeres data er omfattet?
- 5. Har ledelsen nogensinde diskuteret digital afhængighed som en strategisk risiko?*
Ikke som et IT-sikkerhedsspørgsmål, men som et strategisk spørgsmål om organisationens handlefrihed og fremtid. Har det været på dagsordenen?

Hvis I svarede ja til alle fem spørgsmål

I har taget det første skridt. I er bevidste om jeres afhængighed. Det betyder ikke, at I har løst problemet, men I har erkendt det. Det er forudsætningen for alt andet.

Hvis I svarede nej til et eller flere spørgsmål

I er digitale søvngængere. Det er ikke en dom. Det er et udgangspunkt. De fleste danske organisationer befinder sig her. Men det betyder, at I har overladt kontrollen over jeres digitale skæbne til andre. I fungerer på nåde af leverandører, der kan ændre vilkårene, hæve priserne eller lukke for adgangen, når det passer dem.

Niveau 1

Den juridiske optimist

Trade-off: I bytter reel fleksibilitet for dokumenteret tryghed og juridisk rygdækning.

Hvad slår hvad: Formalitet slår substans. I har papirerne i orden og forveksler det med kontrol.

Værdimæssig position: Proceduremæssig retfærdighed. I har fokuseret på at følge reglerne og sikre formelle rettigheder, men forvekslet processen med substansen. Kontrakten siger I er beskyttet. Virkeligheden siger noget andet.

På dette niveau har organisationen papirerne i orden. Kontrakter, databehandleraftaler, GDPR-dokumentation. Juridisk set er I dækket ind. Men teknisk er I stadig låst.

Spørgsmål til niveau 1

- 1. Har I databehandleraftaler med alle jeres kritiske leverandører?*
Ikke bare de store. Også de små. Også dem, I glemte, I brugte. Har I styr på, hvem der behandler jeres data, og på hvilke vilkår?
- 2. Ved I, hvad jeres kontrakter faktisk siger om dataejerskab?*
Ikke hvad I tror, de siger. Hvad de faktisk siger. Har I læst dem? Har nogen, der forstår dem, læst dem?
- 3. Har I overblik over, hvilke data der forlader Danmark?*
Og til hvilke lande? Og under hvilken lovgivning? GDPR giver jer rettigheder, men kun hvis I ved, hvad der foregår.
- 4. Kan I dokumentere jeres GDPR-compliance over for Datatilsynet?*
Hvis de bankede på døren i morgen, har I så dokumentationen klar? Eller ville I skulle bruge uger på at samle den?
- 5. Har I en proces for at vurdere nye leverandørers databehandling, før I indgår aftaler?*
Ikke bagefter. Før. Har I en tjekliste, en procedure, en ansvarlig person?

Hvis I svarede ja til alle fem spørgsmål (og alle spørgsmål på niveau 0)

I er juridiske optimister. I har styr på kontrakterne. I kan dokumentere jeres compliance. I har taget ansvar for at vide, hvad der foregår med jeres data.

Men pas på. Jura er ikke det samme som kontrol. Kontrakten siger, I ejer jeres data. Prøv at flytte dem et andet sted hen. Se, hvad det koster. Se, hvor lang tid det tager. Juridisk ejerskab og praktisk kontrol er to forskellige ting.

Niveau 2

Den tekniske pragmatiker

Trade-off: I bytter enkelhed og sømløs integration for datakontrol og krypteringsmagt.

Hvad slår hvad: Kontrol slår komfort. I har erkendt problemet og begyndt at handle, men stoler stadig på systemet.

Værdimæssig position: Oplyst egeninteresse. I har erkendt risikoen og taget skridt til at beskytte jer selv, men endnu ikke fuldt konfronteret spørgsmålet om, hvem der i sidste ende bestemmer. I handler rationelt inden for et system, I ikke kontrollerer.

På dette niveau har organisationen taget konkrete skridt til at beskytte sine data. I har ikke bare papirer, I har kontrol. Men I opererer stadig inden for et system, I ikke selv kontrollerer.

Spørgsmål til niveau 2

1. *Har I klassificeret jeres data efter følsomhed?*

Ved I, hvad der er kronjuvelerne? Hvilke data ville true organisationens eksistens, hvis de kom i de forkerte hænder? Hvilke data kan I leve med at miste kontrollen over?

2. *Ligger jeres mest følsomme data på infrastruktur, I selv kontrollerer?*

Ikke bare på servere i EU. På infrastruktur, hvor I har den tekniske kontrol. Hvor I bestemmer, hvem der har adgang.

3. Ved I, hvem der har den tekniske mulighed for at slukke for jeres systemer?

Ikke hvem der har lov til det ifølge kontrakten. Hvem der teknisk kan gøre det. Er det jer? Eller er det en leverandør et andet sted i verden?

4. *Har I nogensinde testet, om I kan hente jeres data ud af jeres nuværende systemer?*

Ikke i teorien. I praksis. Har I faktisk prøvet at eksportere jeres data og importere dem et andet sted?

5. *Kender I de reelle omkostninger ved at skifte leverandør?*

Ikke hvad leverandøren siger, det koster. Hvad det faktisk koster. I tid. I penge. I tabt funktionalitet. I frustrerede medarbejdere.

Hvis I svarede ja til alle fem spørgsmål (og alle spørgsmål på niveau 0 og 1)

I er tekniske pragmatikere. I har erkendt, at juridisk beskyttelse ikke er nok. I har taget skridt til at opnå reel kontrol over jeres vigtigste data.

Men vær opmærksomme på faren for suverænitets-washing. Det er let at føle sig suveræn, fordi man har taget nogle tekniske skridt. Den virkelige test er hårdere: Kan I faktisk handle uafhængigt, når det gælder? Er jeres data stadig underlagt amerikansk lovgivning gennem CLOUD Act? Jeres krypteringsnøgler hjælper ikke, hvis I ikke kan komme ind ad døren.

Niveau 3

Risiko-realisten

Trade-off: I bytter plug-and-play-løsninger og markedets standardvalg for operationel modstandskraft og leverandøruafhængighed.

Hvad slår hvad: Robusthed slår raffinement. I accepterer ringere brugeroplevelse til gengæld for ægte handlefrihed.

Værdimæssig position: I tager jeres værdier og ansvar alvorligt, men accepterer en kalkuleret risiko med fortsat begrænset afhængighed. I handler ud fra en forpligtelse til forsigtighed og langsigtet ansvarlighed. I accepterer ulemper i dag for at sikre handlefrihed i morgen. Det er ikke idealisme, men praktisk visdom.

På dette niveau har organisationen opnået ægte handlefrihed. I kan flytte jeres systemer. I kan skifte leverandør. Hvis forsyningslinjerne brydes, kan I drifte videre.

Spørgsmål til niveau 3

- 1. Kan I skifte primær cloud-leverandør inden for seks måneder uden at miste kritisk funktionalitet?*
Ikke i teorien. I praksis. Har I en plan, der faktisk kan eksekveres?
Med navngivne ansvarlige, tidslinjer og budgetter?
- 2. Har I testet jeres beredskab ved at simulere et leverandørsvigt?*
Har I gennemført en øvelse, hvor I forestillede jer, at en kritisk leverandør lukkede for adgangen? Ved I, hvad der ville ske? Ved I, hvad I ville gøre?
- 3. Har I interne kompetencer til at vurdere og implementere alternativer til jeres nuværende løsninger?*
Ikke konsulenter. Interne folk. Mennesker, der forstår jeres systemer godt nok til at kunne ændre dem. Eller i det mindste til at kunne stille de rigtige krav til dem, der skal.
- 4. Ligger jeres kronjuveler på infrastruktur, der ikke er underlagt fremmed jurisdiktion?*
Ikke bare i EU. På infrastruktur, der er immun over for CLOUD Act og lignende lovgivning. Europæisk ejede. Europæisk driftede.
- 5. Kan I forklare jeres digitale strategi til ledelsen uden at bruge teknisk jargon?*
Kan I fortælle historien om, hvorfor I har valgt den sværere vej? Hvorfor I accepterer mere bøvl i hverdagen til gengæld for større robusthed? Hvis I ikke kan forklare det, har I ikke forstået det.

Hvis I svarede ja til alle fem spørgsmål (og alle spørgsmål på niveau 0, 1 og 2)

I er risiko-realist. I har opnået ægte handlefrihed. I er ikke prisgivet en enkelt leverandør. I kan træffe beslutninger uden at spørge om lov. Lad os være ærlige om prisen. De europæiske alternativer er ofte ringere. Interfacet er knap så poleret. AI-funktionerne halter et år eller to. Jeres medarbejdere vil klage. Det er prisen for, at I kan træffe beslutninger uden at spørge om lov. At I kan skifte retning, når omstændighederne kræver det. At ingen udefra kan diktere jeres tempo, jeres prioriteter eller jeres fremtid. Den frihed koster noget i daglig komfort. Men alternativet er at opdage, at I slet ikke har noget valg, den dag I virkelig har brug for et.

Dette er det niveau, de fleste organisationer bør sigte efter, fordi det er den mest realistiske løsning på kort sigt.

Niveau 4

Den digitalt suveræne

Trade-off: I bytter adgang til global innovation og hurtig implementering for fuld kontrol over hele teknologistakken.

Hvad slår hvad: Principper slår pragmatisme. I betaler den højeste pris for den rene form for digital selvbestemmelse.

Værdimæssig position: I handler ud fra princippet om, at ægte frihed kræver selvbestemmelse. I nægter at behandle jeres organisation eller borgere som midler til andres mål. Suveræniteten er ikke bare praktisk, det er et moralsk imperativ.

På dette niveau kontrollerer organisationen hele teknologistakken. Hardware, cloud, software, AI-modeller. Alt. Det er det dyreste niveau. Det mest idealistiske. Og for de fleste organisationer: urealistisk.

Spørgsmål til niveau 4

- 1. Kører jeres kritiske systemer på infrastruktur, I selv ejer eller kontrollerer gennem europæiske fællesskaber?*
Ikke lejer. Ejer. Eller kontrollerer gennem andelsmodeller som OS2 eller lignende. Har I den fulde kontrol?
- 2. Bruger I primært open source-software, som I selv kan auditere og modificere?*
Ikke fordi det er billigere. Fordi det giver jer indsigt og kontrol. Kan I se, hvad koden gør? Kan I ændre den, hvis I har brug for det?
- 3. Har I egne specialister til at drifte og vedligeholde jeres infrastruktur?*
Ikke konsulenter. Ansatte. Mennesker, der kender jeres systemer indefra og kan holde dem kørende uden ekstern hjælp.
- 4. Er I immune over for beslutninger truffet af fremmede magter?*
Kan en amerikansk præsident, en kinesisk embedsmand eller en tech-milliardær påvirke jeres drift? Eller er I fuldstændig uafhængige?
- 5. Bidrager I aktivt til at opbygge europæisk digital infrastruktur?*
Ikke bare som brugere. Som bidragsydere. Deler I jeres løsninger? Investerer I i fællesskabet? Hjælper I andre med at opnå det samme?

Hvis I svarede ja til alle fem spørgsmål (og alle spørgsmål på niveau 0, 1, 2 og 3)

I er digitalt suveræn. I har opnået fuld kontrol over jeres digitale skæbne. I er herre i eget hus.

For de fleste organisationer er dette niveau urealistisk. Men nogle må gå forrest. Offentlige institutioner med særligt følsomme data. Kritisk infrastruktur. Organisationer, der af politiske eller strategiske grunde ikke kan acceptere nogen fremmed afhængighed.

Her er data-hierarkiet ikke et prioriteringsværktøj, men en absolut grænse. Ingen kronjuveler forlader organisationens kontrol. Ingen kritiske systemer afhænger af fremmede magters velvilje.

Hvad nu?

Hvordan bruger i testen

Find jeres niveau

Gå tilbage til spørgsmålene. Start fra niveau 0. Svar ærligt. Det niveau, hvor I første gang svarer nej til et spørgsmål, er niveauet under jeres nuværende placering.

Accepter jeres udgangspunkt

Der er ingen skam i at være på niveau 0 eller 1. De fleste er der. Skammen ligger i at blive der, uden at ville vide det.

Beslut jer for jeres ambition

Ikke alle behøver at nå niveau 4. For de fleste er niveau 3 det rigtige mål. Men I skal træffe et bevidst valg om, hvor langt I vil gå, hvorfor, og til hvilken pris.

Tag kommunikationsansvaret

Digital suverænitæt er for vigtig til at overlade til IT-afdelingen alene. Det er kommunikationsafdelingens opgave at oversætte teknisk afhængighed til strategisk risiko. At fortælle historien om, hvad der er på spil. At sikre, at ledelsen forstår, at dette ikke handler om servere og software, men om værdier og fremtid.

Brug kronjuvel-metaforen

Spørg: Hvad er vores kronjuveler? Hvilke data definerer, hvem vi er som organisation? Hvor ligger de? Hvem kontrollerer dem? Det er spørgsmål, alle kan forstå. Og svarene afslører ofte mere, end nogen teknisk audit.

Kommunikationsafdelingens særlige ansvar

Hvorfor skal kommunikationsafdelingen bekymre sig om digital suverænitæt?

Fordi det handler om mere end teknik. Det handler om, hvad teknologi betyder for danske og europæiske værdier. Om hvem der bestemmer over vores data, vores systemer og i sidste ende vores demokratiske institutioner.

IT-afdelingen kan fortælle jer, hvad der er teknisk muligt. Kommunikationsafdelingen skal fortælle organisationen, hvad der er strategisk nødvendigt. I forstår narrativer. I forstår, hvordan man forklarer komplekse spørgsmål til en ledelse, der har travlt med andre ting.

Og I forstår, at kronjuvelerne ikke bare er et teknisk begreb. Det er de data, der definerer, hvem I er som organisation. Dem skal I beskytte.

Rejsen mod digital suverænitæt begynder med en erkendelse. Og erkendelser kræver sin kommunikation.