REMISSVAR

It-driftsutredningens slutbetänkande

”Säker och kostnadseffektiv IT-drift – förslag till varaktiga former för samordnad statlig IT-drift” (SOU 2021:97)

Solna 2022-03-21

Infrastrukturdepartementet, enheten för samhällets digitalisering
i.remissvar@regeringskansliet.se
i.esd.remisser@regeringskansliet.se

Blue Safespring AB
Smidesvägen 12, 171 41 Solna
www.safespring.com

Tel: +46 (0)8-551 073 70
info@safespring.com
Number of pages: 6

Yttrande: ert diarienummer I2021/03265

Safespring med branschkollegorna Binero och City Networks tackar för möjligheten att få komma med våra synpunkter. Utredningen har gjort ett mycket omfattande och ambitiöst arbete och vi delar flera av de slutsatser och rekommendationer som ni har kommit fram till. Sedan utredningen publicerades så har det geopolitiska läget förändrats väsentligt. Det ändrar inget i sak för utredningen men belyser ytterligare vikten av suveräna, säkra och robusta IT tjänster.

Det finns IT system som staten absolut lämpar sig bäst för att driva. Vårt svar adresserar inte dessa specialsystem i första hand utan myndigheters behov av innovativa, standardiserade IT system och tjänster för att fortsätta digitalisera och utveckla verksamheten. Våra övergripande synpunkter kan sammanfattas som följer:

- **DET SAKNAS MARKNADSLOGIK** i den finansieringslösning som föreslås av utredningen. Även om fyra myndigheter utses till ”tjänsteleverantörer” finns en överhängande risk att myndigheternas uppdrag som IT-driftsansvariga sammanblandas med myndigheternas övriga uppdrag. I skarpt läge kommer sannolikt kärnverksamheten prioriteras före rollen att vara tjänsteleverantör..

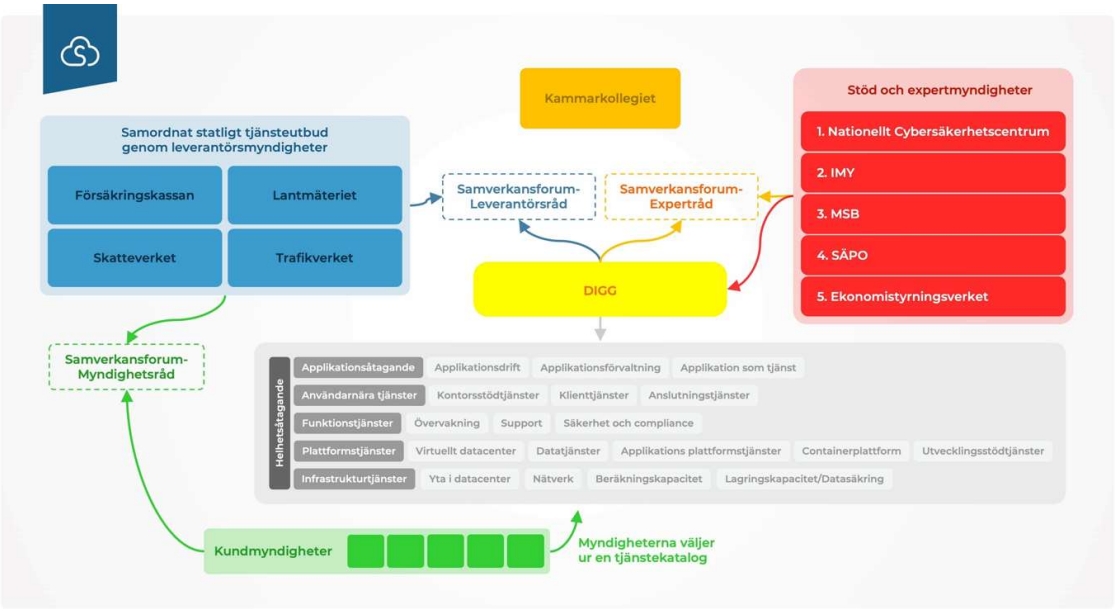
- **VAL AV ÖPPNA INFRASTRUKTURER** och öppna standarder för att motverka inlåsningseffekter är redan utrett (SOU 2007:47). Det framgår inte av utredningen om ni tillvaratagit den informationen.

- **IT-DRIFT VID MYNDIGHETER ÄR LIKA MYCKET NÄRINGSPOLITIK** som myndighetspolitik. Vi efterlyser hållbara lösningar som stödjer marknaden.

- **VI EFTERLYSER VERTIKAL SEGMENTERING AV MARKNADEN** som låter kommersiella aktörer ta hand om ”kärnverksamhet” på varje marknadsnivå, i kombination med tydliga direktiv åt myndigheter som Kammarkollegiet, Upphandlingsmyndigheten och Konkurrensverket att motverka inlåsning i varje marknadsled.

- **DEN SAMORDNANDE MYNDIGHETEN** bör fungera som en central samlingspunkt för råd om informationsklassning, informationskartläggning, dataskyddsklausuler, incidentrapporteringsmallar, och dylikt. I dagsläget är det framför allt regelverket kring faktiska data som spridits ut på många nivåer (nationell, europeisk, personlig, statlig, civilt, försvars, och så vidare). Vi utvecklar dessa tankar nedan.

Inledningsvis illustrerar vi vår övergripande förståelse av utredningens förslag. Sedan följer ett avsnitt om den marknadslogik vi verkar inom som tillhandahållare av just driftstjänster för IT-system. Avslutningsvis ger vi ett antal internationella exempel på cybersäkerhetskoordinering (Storbritannien och Nederländerna) som vi tror kan bidra till regeringens vidare arbete på området.



Källa: Ovan illustration är vår tolkning av bilder ifrån utredningens bild 5.1, samt 11.1.

Marknadsmodellen

Vad vi förstår av utredningens förslag ska fyra centralt placerade myndigheter, Skatteverket, Trafikverket, Försäkringskassan och Lantmäteriet, bli IT-driftsansvariga åt andra myndigheter. Dessa fyra myndigheter ska kunna ta betalt för IT-drift av andra myndigheter, och förväntas med hjälp av DIGG samordna med och implementera råd från ett antal kringliggande myndigheter som har ansvar för informations- och kvalitetsgranskning (markerade 1–5 i bilden).

DIGG ska sedan även samordna med tredjeparter som ovanpå de fyra IT-driftsmyndigheternas infrastruktur kan bygga tjänster som riktas mot var och en av kund-myndigheterna. Därutöver också samordna råd och koordinering från det stora antal myndigheter som idag har tillsynsansvar för olika aspekter av informations- och kvalitetsgranskningsregelverk.

Utifrån våra erfarenheter av IT-drift är detta ett icke ambitiöst förslag som riskerar att ge kund-myndigheterna otillräckliga eller undermåliga möjligheter både till effektiv IT-drift och specialiserade tredjepartstjänster. En av anledningarna till att många myndigheter de senare åren velat satsa på molntjänster är att en renodling av driftsuppdraget är det som skapar bäst förutsättningar för pålitliga, stabila och säkra system. Att vissa av de lösningar som utforskats för att uppnå dessa fördelar haft andra nackdelar, exempelvis att de behäftats med interoperabilitetsproblem, inlåsningseffekter och oklarhet kring rättsliga faktorer, ska inte ses som skäl att avfärda privata tjänsteleverantörer, utan som indikation på att de tjänsteleverantörer myndigheterna tidigare i första hand vänt sig till inte levererar sådana tjänster myndigheterna behöver.

Att sprida ut ansvaret för centraliserad IT-drift på fyra myndigheter kan vara utmanande: fyra olika IT-driftssystem ska införlivas i fyra olika administrativa myndighetskulturer, och som varje år behöver tilldelas uppmärksamhet i fyra olika myndighetsuppdrag som utfärdas av (möjligen) fyra olika departement. Vi saknar också en genomlysning av de praktiska förutsättningarna för ”samordning”: DIGG kommer inte kunna styra tillsynsmyndigheternas uppdrag och verksamhet, så hur ska DIGG kunna skapa rätt förutsättningar för samordning och sammanhållning?

Vi tror att det är viktigt att regeringen vågar visa ledarskap i sina ambitioner för en svensk IT-infrastrukturen. I det här fallet kan det innebära att regeringen bör avvika från starka viljor på centralt placerade myndigheter som försvarar sitt eget IT-driftsterritorium.
På 1990-talet lyckades Sverige bli ett framstående IT-land till följd av ett antal strategiska beslut som rörde infrastruktur. Dels gjorde regeringen det enkelt för anställda att få datorer hemma, dels skapades incitament för investeringar i nätverk. I kombination med europeiska regelverk för liberalisering av telekommarknaden kunde Sverige snabbt bygga upp en bred bas av kompetens inom nätverksteknologi, IT-säkerhet och webbhosting som vi i egenskap av privat molnleverantör gynnas av än idag.

Många av de satsningar som gjordes på 1980- och 90-talen skapade utrymme för privata tjänsteleverantörer att ta plats på nya marknader, och eftersom slutkonsumenterna också var uppkopplade kunde marknaderna snabbt växa. Digitaliseringen av dåvarande Televerkets växlar hjälpte exempelvis Ericsson att bli en av de dominerande mobilnätleverantörerna, en plats de har kvar idag. **Idag har svensk molnindustri liknande möjligheter**, men företag växer sig i regel inte starka om de inte har en stark hemmamarknad. Vi menar bestämt att svenska regeringen, om den ändå ska reformera de nuvarande formerna för IT-drift bland statliga myndigheter, bör ta sådana industripolitiska aspekter i beaktande. Då bör regeringen öppna för privat konkurrens av just basinfrastrukturdrift, och får på köpet tjänsteleverantörer som inte har målkonflikter.

Inte heller i datoriseringens barndom förväntade sig staten bygga och drifta samtliga IT-system själva (se ex. SOU 1973:6). Snarare förstod regeringen att de statliga förvaltningarna skulle vara beroende av privata tjänsteleverantörer och skapade en uppsättning nya regler för dessa omständigheter (SOU 1972:47 med flera). Vid planering av infrastruktur bör regeringen även ta i beaktande humankapital: för att vara i spetsen av kompetens på driftssäkerhet och IT-system behöver en normal IT-arbetare ofta kunna tillskansa sig varierande erfarenheter under ett yrkesliv. Då passar privata anställningsformer bättre än myndighetsjobb. En genomlysning av innevarande inköp av konsulttjänster vid myndigheter i utredningen hade kunnat ge regeringen bättre inblick i hur kunskapsöverförseln mellan det offentliga och privata sker idag.

Vi föreslår att utredningen tar med följande synpunkter i sitt beaktande:

- Vi vill se ett fortsatt fokus på öppna standarder (SOU 2007:47), samt öppna API:er, som uppdateras för ny teknologi. Privata tjänsteleverantörer är inte i sig ett problem, utan det är först när inlåsningseffekter uppstår som myndigheterna hamnar i problem.

- Med vertikal segmentering av marknaden för IT-tjänster för myndigheter menar vi i princip en syn på själva marknadsstrukturen som motsvarar de vita lådorna benämnda ”Potentiella IT-driftstjänster” i bilden på s. 3. Var och en av de vita lådorna bör ses som en egen tjänstemarknad (vilket medför att det även finns naturliga horisontella segmenteringar). På dessa marknader kan myndigheterna införskaffa tjänster från en privat leverantör eller av myndigheten själv. Det viktiga är hur man garanterar interoperabilitet mellan de olika marknaderna och leverantörerna, samt skapar konkurrens inom ramen för varje låda.

- Det saknas ett samverkansforum med den privata sektorn.

- Vi stödjer att Kammarkollegiet får uppgiften att upphandla ramavtal. Det är viktigt att samordningen tillvaratar ovan nämnda vertikala segmentering. Ramavtal(en) skulle kunna ses som en tjänstekatalog eller marknadsplats

I förlängningen kan dock regeringen behöva fundera på om man ville göra mer övergripande förändringar i hur databaserade affärsmodeller används på myndigheter (jämför diskussionen om

öppna myndighetsdata, SOU 2020:55) och om förändringar av dessa affärsmodeller också kan bidra till en säkrare och mer effektiv IT-drift.

Samordning av tillsyn

Vi ser en större potential i att samordna tillsynsorgan för informationslagstiftning utifrån kund-myndigheternas perspektiv, än i att samordna tjänstekataloger från tjänsteleverantörsmyndigheter med tillsynsmyndigheter.

Eftersom den svenska säkerhetsskyddslagstiftningen är skriven så att varje verksamhet själv måste bedöma om den har samhällsviktig eller säkerhetskänslig information, och därför också bedöma vilka IT-gränssnitt som kan vara lämpliga givet den egna bedömningen, kommer det dock vara svårt att samordna mer än de allmänna riktlinjer som befintliga tillsynsorgan producerar.

Det kan innefatta riktlinjer för incidentrapporter, vägledningar för styrsystem, informationssäkerhetsrutiner, och dylikt, som ofta kommer från flera myndigheter samtidigt och utifrån olika perspektiv. En sådan samordning skulle också kunna ge tredjepartsleverantörer som vill leverera specialiserade tjänster till kund-myndigheter en naturlig portal att stämma av de olika kraven som ställs i svensk och europeisk lagstiftning.

Internationellt: Cybersäkerhetscentrum

Idag är ansvaret för svensk cybersäkerhet utspritt på flera myndigheter. Samordningsformerna man tidigare arbetat med för att skapa samförstånd mellan dessa institutioner har inte lett till uppenbart positiva resultat. Vi tror att regeringen i stället för ytterligare samordning i det abstrakta bör sätta konkreta mål.

DIGG kan ges i uppdrag att samla befintliga riktlinjer. Men ett svenskt nationellt cybersäkerhetscentrum enligt brittisk modell kan också hjälpa myndigheterna och privat sektor att få ett bättre grepp om säkerhetsfrågorna.

Storbritannien

NCSC är den publika grenen av GCHQ (Storbritanniens motsvarighet till FRA) och sammanför myndigheter, privata företag och underrättelse- samt säkerhetstjänster i en enda statlig organisation. NCSC har en egen ”GD” och egen finansiering (ca 5 miljarder SEK/år enligt en presentation på Cyberförsvarsdagen 2020, https://soff.se/event/cyberforsvarsdagen-2020/). I Storbritannien leder bokstavligen NCSC landets proaktiva cyberförsvar genom framgångsrika och välfinansierade initiativ. Vidare borde man inspireras av NCSCs framgångsrika samarbete med akademin och forskningen där framförallt CyBOK (https://www.ncsc.gov.uk/section/education-skills/cybok) bör lyftas fram. Dessutom bedriver NCSC ett tätt samarbete med såväl privat näringsliv som universiteten, i syfte att säkra upp nuvarande och framtida jobb inom Storbritannien.

Nederländerna

I Nederländerna lades grunden för det nationella cybersäkerhetsrådet redan 2011. Dels sattes det upp tydliga mål på regeringsnivån för vad cybersäkerhetsarbetet skulle leda till:

- "arbete som innefattar både privata och offentliga aktörer",

- "genomförande av risk-och sårbarhetsanalyser",
- "bättre motståndskraft mot driftsstörningar",
- "bättre svarskapacitet vid driftsstörningar",
- "bättre uppföljning av IT-brottslighet",
- "stimulering av forskning och utbildning",

Dels gavs det tydliga mandat till tidigare GOVCERT att delta vid utvecklingen av implementerande åtgärder. Resultatet har blivit att cybersäkerhetsrådet nu är en samlingsplats för olika aktörer som dels respekterar varandra, dels respekterar forumet där de samverkar. Den politiska nivån har lyckats skapa en plattform där aktörerna möts, i stället för att konkurrera.

Källa: https://www.vno-ncw.nl/sites/default/files/downloadables_vno/de-nationale-cyber-security-strategie.pdf

För Safespring, Binero och City Networks

Fredric Wallsten VD Safespring	Charlotte Darth VD Binero	Johan Cristiansen City Networks

Rådgivare: Amelia Andersdotter