DIGITAL SÅRBARHET

ÅPENHET, SIKKERHET OG TRUSSELBILDER I EN DIGITAL FORVALTNING

TEMAFLAK

TIL DEBATT

VÅR FELLES STYRKE
- DIN TRYGGHET

Norsk Tjenestemannslag

INNLEDNING

I midten av mai 2017 ble 150 land rammet av løsepengeormen WanaCrypt0r i det som antagelig var verdens mest omfattende angrep til nå. Direktør for Senter for cyber- og informasjonssikkerhet (CCIS) ved NTNU, Sofie Nystrøm, sa til Dagsavisen 16. mai: "Sårbarheten vår er høyere fordi vi bruker teknologi til flere funksjoner i samfunnet. [...] Økonomien vår har gitt oss gode rammevilkår, og derfor var vi mindre utsatt denne gangen, men alle studier tilsier at vi ikke er like flinke på sikkerhet som vi er på å ta i bruk teknologien."

I denne brosjyren setter NTL fokus på digital sårbarhet i forvaltningen. Hvordan skal vi sørge for at behovet for effektivisering ikke går ut over sikkerheten? Er kompetansen på IT-sikkerhet god nok? Hvordan skiller staten seg fra andre aktører i IT-spørsmål? God debatt!

INNHOLD

Hva er digital sårbarhet?

Sårbarhetsutvalget definerte i 2000 sårbarhet som «et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet». Lysneutvalget definerer digital sårbarhet som «sårbarheter som knyttes direkte til IKT--systemer, både logiske og fysiske feil [... og ...] sårbarheter i selve samfunnsfunksjonene som er forårsaket av svikt i IKT-systemer, og ved at svakheter arves av feil i IKT-systemer.»

Digital sårbarhet er altså et samfunnsproblem som øker etter hvert som flere og flere av systemene vi er avhengige av digitaliseres. Dette gjelder såvel offentlige systemer med høy beredskap som dagligdagse ting vi like fullt er avhengige av: strømmåleren, bilen, oppvarmingen i huset, kloakken. I sum kan svikt i i disse systemene skape kaotiske situasjoner i et samfunn.

Vi skal i denne temabrosjyren likevel konsentrere oss om de typene digital sårbarhet som den offentlige forvaltningen er utsatt for, med hovedvekt på sektorer der NTL organiserer. Dette omfatter både sårbarhet som rammer den enkelte og sårbarhet som rammer offentlig tjenesteproduksjon og myndighetsutøvelse.

> *Et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet*

Effektiviseringen er ønsket og forventet, og de forventingene som stilles øker raskt

Statens doble rolle som tjenestetilbyder og myndighetsutøver stiller strenge krav til hvordan informasjon om befolkningen skal kunne brukes.

Balanse mellom sårbarhetshensyn og effektivitetshensyn

En hovedkilde til den bekymringen som kommer til uttrykk om sårbarheten i digitale systemer er asymmetrien mellom feilkilde og konsekvens. Jo flere systemer som er sammenkoblet, jo større er konsekvensen ved en feil i ett av systemene. Kommer én opplysning på avveie vil spørsmålet straks stilles om også alle andre opplysninger i samme system også er eksponert. Blir én funksjon satt ut av spill av en ulykke eller angrep kan det få konsekvenser for andre funksjoner i samme system.

Denne asymmetrien kan ses som prisen vi betaler for de effektiviseringsgevinster vi oppnår ved digitalisering av forvaltningen og i andre sektorer i samfunnet. Sammenstilling og tilgjengeliggjøring av data er en forutsetning for effektiviseringsgevinster ved digitalisering. Samtidig fører sammenstillingen til at en feilkilde kan ha konsekvenser for eller generaliseres for et helt system eller et helt datasett.

Denne effektiviseringen er ønsket og forventet, og de forventingene som stilles øker raskt. Digitale verktøy med ufattelig effektiviseringspotensial utvikles og spres i resten av samfunnet, og normaliseres i kontekster der kravene til datasikkerhet er helt annerledes, eller der deling av egen personinfo er ønskelig fra brukerens synsvinkel. Staten må etterstrebe lignende tilbud og tjenester i eForvaltningen for å tilfredsstille allmenne krav til effektivitet og brukervennlighet og samtidig ivareta de datasikkerhetskrav som gjelder for svært sensitive opplysninger.

Den merverdien som oppstår ved tilsiktet sammenstilling av data er en business-ide i det private næringslivet, særlig blant virksomheter som lever av å generere og selge bruksmønsterdata for markedsføringsformål. Denne merverdien er vanskelig å ta i bruk i det offentlige. Sammenstilling av data kan gi en bedre tilrettelagt tjenestepakke for den enkelte, men assosieres også med overvåkning og misbruk av myndighet. Enkelte typer data er også forbudt å sammenstille.

Statens rolle som dataforvalter er annerledes enn det som er tilfelle i det private. Staten forvalter i mange tilfeller opplysninger som den enkelte gir fra seg ufrivillig etter pålegg i lovverket. Statens doble rolle som tjenestetilbyder og myndighetsutøver stiller strenge krav til hvordan informasjon om befolkningen skal kunne brukes.

NTL mener

NTL mener utvikling og drift av offentlige IKT-tjenester skal organiseres slik at det er underlagt demokratisk styring og kontroll.

Digital sårbarhet i forvaltningen

Den norske forvaltningen har over de siste tiårene digitalisert både grunnregistre, intern samhandling og brukerrettede tjenester, en prosess som gjerne kalles eForvaltning. eForvaltningen er drevet delvis av forventninger fra omverdenen om tilgjengelighet, fleksibilitet og innsyn, og dels av et ønske om effektivisering basert på IKT.

En viktig del av arbeidet med å utvikle effektive og brukervennlige digitale offentlige tjenester har vært satsingen på de såkalte felleskomponentene. Felleskomponentene i eForvaltningen består av en rekke sentrale registre, som folkeregisteret, enhetsregisteret og matrikkelen, verktøy for kommunikasjon mellom den enkelte og det offentlige, som Altinn og digital postkasse, og sist, men ikke minst, felles innlogging og autentisering i ID-porten.

Å samle data i disse felles registrene gjør det enklere både å tilby gode velferdstjenester på tvers av departementssiloene, men også å skjerpe myndighetsutøvelsen, utføre tilsyn og kreve inn skatt. Samtidig øker asymmetrien mellom feilkilde og konsekvens. Til gjengjeld kan arbeidet med å sikre dataene samordnes og prioriteres.

Hvem skal eie og drifte eForvaltningen?

Mange statlige virksomheter har sterke IKT-avdelinger med kompetanse og kapasitet til å utvikle og drifte egne systemer. NTL mener utvikling og drift i egen regi er en forutsetning for en forsvarlig langsiktig systemforvaltning og for muligheten til å tenke strategisk i eForvaltningspolitikken.

Outsourcing av IKT-utvikling gjør staten avhengig av eksterne aktører med andre motiver enn staten selv. Dette innebærer en risiko knyttet til den eksterne partens prioriteringer i en tilspisset situasjon. Sammenbrudd i offentlig tjenester er kritisk, ikke bare når det gjelder beredskapsetatene, men også i systemer knyttet til vannforsyning, kommunikasjon, transport og helsetjenester.

NTL mener utvikling og drift av offentlige IKT-tjenester skal organiseres slik at de er underlagt demokratisk styring og kontroll. Forvaltningen av IKT-systemene må anses som en statlig kjerneoppgave som ikke kan bestemmes av økonomiske beregninger. Staten skal ha oversikt over og eierskap til sin egen digitale struktur og arkitektur.

NTL mener

NTL mener det bør utredes om staten kan drifte sin egen skytjeneste for offentlig virksomhet.

Hvor skal vi lagre offentlige data?

I Nasjonal strategi for bruk av skytjenester peker Kommunal- og moderniseringsdepartementet på endel problematiske sider ved bruk av skytjenester til lagring av personopplysninger. Kontraktene er gjerne standardkontrakter som ikke er tilpasset norsk lovverk, og den nøyaktige lagringsplasseringen spesifiseres ikke tilstrekkelig. Bransjen er ikke underlagt den typen regulering som er nødvendig for å kunne drifte digital infrastruktur på en god måte.

Som et ledd i oppfølgingen av strategien har departementet fått utredet mulighetsrommet for konsolidering av statlige datasentre i en rapport fra Nexia Management Consulting levert i mars 2017. Rapporten anbefaler å klargjøre lovverket om muligheten for samarbeid på tvers av etater, etablere fagfora for koordinering av planer, strategier og kompetanseutveksling, og å gjennomføre av analyse av de eksisterende datasentrene med sikte på standardisering.

NTL mener det bør utredes om staten kan drifte sin egen skytjeneste for offentlig virksomhet og hvilke fordeler og ulemper dette ville føre med seg. Et offentlig datasenter vil kunne tilpasses de behov som finnes i forvaltningen, og eliminere kostnader knyttet til innkjøp av datalagringstjenester fra private aktører. En statlig skytjeneste ville også kunne unngå at data lagres i utlandet og blir tilgjengelig for utenlandsk etterretningstjeneste.

NTL mener

Ved anskaffelser skal det stilles krav om oversikt over hvilke medarbeidere som har tilgang til data.

Trusselbilder mot en digital infrastruktur

Å vurdere den digitale sårbarheten i forvaltningen forutsetter å tegne opp noen mulige trusselbilder.

Trusselbildene kan deles i to typer: utilsiktede og tilsiktede hendelser. Utilsiktede hendelser omfatter rutinesvikt, menneskelige feilvurderinger, tekniske feil, misforståelser og lignende. Tilsiktede hendelser omfatter vinningskriminalitet, terror og elektronisk krigføring.

Trusselbildene kan etter NTLs mening motvirkes av kompetanseheving, klarspråk og tilstrekkelig bemanning og finansiering.

Outsourcing motvirker langsiktighet i forvaltningen av systemer fordi den eksterne parten og staten ikke har samme målsetning

NTL mener

Den beste måten å sikre kompetanse over tid er å ha kompetansen i egne ansattrekker.

Kompetanseheving

Kompetanse er avgjørende for statens evne til å beskytte den digitale infrastrukturen og opprettholde myndighetsutøvelsen og tjenesteleveransen. Et sentralt spørsmål i forvaltningspolitikken er derfor hvordan denne kompetansen skal skaffes og beholdes. Behovet for kompetanse vil trolig øke i takt med at flere og flere offentlige tjenester digitaliseres og samordnes. NTL mener den beste måten å sikre kompetanse over tid er å ha kompetansen hos egne ansatte.

Outsourcing motvirker langsiktighet i forvaltningen av systemer fordi den eksterne parten og staten ikke har samme målsetning med driftsavtalen. Mens statens målsetning er systemets nytteverdi, er leverandørens målsetning å tjene penger.

NTL mener kompetansen om informasjonssikkerhet bør styrkes gjennom noen målrettede tiltak:

- Styrke rekrutteringen av datakrimetterforskere i politiet ved å åpne for økt bruk av sivil arbeidskraft, herunder støtte Politihøgskolens nye etterforskerutdanning åpnet for sivile, som må ansettes som spesialetterforskere, med nødvendige fullmakter for oppgaveløsning.
- Bidra til at overtallige ingeniører i oljesektoren kan omstilles til arbeid innenfor digital sikkerhet.
- Styrke grunnleggende og videregående IKT-utdanning ved å inkorporere dybdekunnskap om sårbarhet innenfor teknologi og personvern.
- Støtte samarbeidsprosjekter mellom etatene og næringslivet for å sikre at det ikke oppstår gråsoner der det er uklart hvem som har ansvar for hvilken teknologi og tjeneste.

Tilstrekkelig bemanning og finansiering

Informasjonssikkerhet er i i stor grad en prioriteringssak. Systematisk arbeid med informasjonssikkerhet er ressurskrevende og krever investeringer i stillinger og systemer. Underbemanning fører til menneskelige feil.

På samme måte er det viktig at arbeidet med informasjonssikkerhet samordnes på tvers av sektorene i samfunnet.

Klarspråk og tilgjengelighet

Sørge for at instrukser skrives på en måte som gjør at enhver som kommer i befatning med informasjonen kan forstå instruksen.

- En grenseoverskridende arena for organisert kriminalitet

Leder i NTL Forsvaret, Tom Rune Klemetsen, er bekymret for Norges evne til å stå imot villede angrep mot den digitale infrastrukturen. - Cyber--kriminalitet er et alvorlig samfunnsproblem; det digitale rom er en grenseoverskridende arena for organisert kriminalitet på mange vis, fra terror til utpressing, med id-tyveri og trakassering, sier Klemetsen.

Sammen med NTLs landsforeninger i Politiet og Direktoratet for sivil beredskap har NTL Forsvaret og Klemetsen bidratt med innspill til NTLs standpunkt i sårbarhetsspørsmålet. Han ivrer for høyere prioritering av datasikkerhet. - Norske myndigheter har løftet datasikkerhet høyt opp på den politiske og utøvende agenda. Spørsmålet er hvor dypt forståelsen stikker og hvor gjennomgripende tiltakene er, sett opp mot sårbarheten og konsekvensene, sier han.

Statens nøkkelrolle

Klemetsen understreker hvor viktig statsforvaltningen er i å legge grunnlaget for digital sikkerhet i det norske samfunnet. Statlige virksomheter

Tom Rune Klemetsen ivrer for høyere politisk prioritering av infosikkerhet.

Hege Fjellberg mener det er behov for harmonisering av nasjonale lovverk om teknologirelaterte forbrytelser.

spiller en viktig rolle i å skape nødvendig trygghet og tillit til kritiske systemer og offentlige løsninger.

Digitaliseringen skaper ifølge Klemetsen mange muligheter som det offentlige har et ansvar for å utnytte. - Tilgangen til offentlige tjenester for alle må bedres, og det tilligger det offentlige et særlig ansvar å sikre at nye digitale tjenester ikke bidrar til å forsterke sosiale og økonomiske forskjeller. Digitalisering må bidra til utjevning, mener Klemetsen.

Etterforsking og personvern

Balansen mellom myndighetsutøvelse og den enkeltes personvern kan være problematisk i etterforskningen. Teletilbydere skal slette informasjon om kontakt mellom mobiltelefoner innen tre uker. I praksis innebærer dette ofte at det ikke lagres slik informasjon. - Dette kan være en utfordring for politiet i arbeidet med å bevise og påtale trakassering og misbruk av bilder på internett, sier Hege Fjellberg i NTL Politiet.

Fjellberg mener det er behov for harmonisering av lovverk internasjonalt for å kunne påtale og straffe kriminalitet begått med, av og mot teknologi. - For å øke rettssikkerheten er det behov for et internasjonalt regelverk. Dette er internasjonale forbrytelser, og vi har behov for internasjonal koordinering på myndighetssiden, sier Fjellberg.

Motstridende hensyn i forvaltningen av elektonisk informasjon

Staten har et ansvar for å ivareta sikkerheten til den informasjonen det offentlige har om den enkelte. I hvilke tilfeller bør det offentlige bruke informasjonen om den enkelte mot dem? Kan de samfunnsmessige konsekvensene være så store at det er riktig å spre opplysninger som i utgangspunktet er konfidensielle? Skal staten ha anledning til å samle informasjon om den enkelte som ikke er nødvendig for lovpålagte oppgaver?

Personvern eller samfunnsvern?

I 2018 trer EUs personvernforordning i kraft. Forordningen generaliserer for hele EU/EØS-området prinsippet om at hensynet til den enkelte går foran hensynet til staten i personvernspørsmål. Det innebærer blant annet at uavhengige parter ikke kan pålegges å utlevere opplysninger om sine kunder eller medlemmer til staten, slik det er tilfelle i mange land utenfor Europa.

Samtidig kan stater ha et legitimt behov for å bruke opplysninger om personer mot dem selv dersom de samme personene utgjør en fare for det fellesskapet staten skal beskytte. Et sterkt personvern beskytter den enkelte, men kan også skjule sporene etter kriminell aktivitet. Amerikanske myndigheter har blant annet kritisert forordningens regler om samtykke og retten til å bli glemt. Det meste av kritikken mot forordningen har imidlertid kommet fra privat næringsliv, som banker, forsikringsselskap og internettjenester, som baserer sin forretning på behandling av personopplysninger.

Staters bruk av personopplysninger til å bekjempe kriminell og fiendtlig aktivitet balanserer på grensen mellom det trygghetsskapende og tillitsvekkende og det autoritære og undertrykkende. Bush-administrasjonens doktrine om forebyggende krig (pre-emptive strikes) mot terrorister basert på mistanke om framtidig aktivitet understøttet av personopplysninger med ukjent opphav er et eksempel på hvordan staters bruk av informasjon kan føre til en politikk som langt overskrider etablerte normer for sivile og politiske rettigheter.

Rettigheter og plikter i forordningen

Forordningen blir del av norsk lov i mai 2018 og sikrer den enkelte fire grunnleggende rettigheter: retten til å bli glemt, retten til å ta med seg sin opplysningsportefølje på tvers av leverandører, retten til å begrense bruken av opplysningene til det formål de ble innhentet for, og retten til å motsette seg profilering og automatiserte avgjørelser på grunnlag av slik profilering. I tillegg stiller forordningen krav til klarspråk i redegjørelser, avtaler og betingelser som har å gjøre med personopplysninger.

EUs personvernforordning trer i kraft 25. mai 2018 og tas inn i norsk lov samme dag.

Virksomheter som behandler personopplysninger får også nye plikter. Alle systemer som nyutvikles skal bygges med personvern som en grunnleggende mekanisme, såkalt innebygd personvern, og ikke bare som et tillegg i rapporteringsfunksjonene. Alle virksomheter skal inkludere personvern i sin risikoanalyse og identifisere personvernfremmende tiltak. Alle offentlige virksomheter og andre som behandler større mengder personopplysninger skal dessuten opprette et personvernombud, som skal jobbe for å styrke virksomhetens kunnskap og kompetanse om personvern.

Digitalt grenseforsvar?

DGF vil gi etterretningstjenesten tilgang til all tele- og datatrafikk som krysser grensen

Lysne II-utvalget leverte i august 2016 rapporten om et digitalt grenseforsvar (DGF), som vil gi etterretningstjenesten tilgang til all tele- og datatrafikk som krysser Norges grenser. Utvalget skriver blant annet at «DGF anses som nødvendig for nasjonens sikkerhet, særlig gjelder dette beskyttelse mot sabotasje og spionasje i det digitale rom. DGF slik utvalget anbefaler gir etterretningsmessig verdi og er teknologisk realiserbart.»

Utvalget peker likevel på betydningen av å begrense muligheten til å bruke opplysninger om enkeltpersoner: «DGF er et potensielt svært personverninngripende virkemiddel, og utvalget kan ikke anbefale innføring av DGF med svakere kontrollmekanismer og tekniske filtre mv. enn det som er beskrevet i rapporten.»

Et sentralt spørsmål i debatten om et digitalt grenseforsvar er hvilke opplysninger som skal kunne brukes, av hvem, og til hva. Grenseforsvaret er i utgangspunktet en militær installasjon og skal kun brukes til å reagere på opplysninger som kan true rikets sikkerhet. Konsekvensen av dette er at de som jobber med å gå gjennom opplysningene som fanges opp kan komme til å måtte la opplysninger om alvorlige forbrytelser passere, noe som fører til at kriminelle kan gå fri, og være belastende for den som jobber med disse oppgavene.

Datatilsynet går mot innføringen av et digitalt grenseforsvar. Til NRK Dagsnytt 13. januar 2017 sier Datatilsynets direktør Bjørn Erik Thon at grenseforsvaret vil gripe uforholdsmessig inn i den enkeltes privatliv ved å tilgjengeliggjøre informasjon om for eksempel hva vi har gjort, hvem vi har kommunisert med, hvilke nettsteder vi har besøkt. «Det er ingen tvil om at et digitalt grense vil være et stort inngrep i personvernet, ettersom de aller fleste mennesker ikke gjør noe galt, og utgjør heller ikke noen trussel mot samfunnet. Det Datatilsynet frykter er at dette kan føre til en såkalt nedkjølende effekt i samfunnet, det vil si at når vi vet at noen kan kikke oss i kortene, så blir vi mer engstelige for å kommunisere og for hvem vi kommuniserer med», ifølge Thon.

NTL mener

NTL mener den enkeltes rett til kontroll over egne personopplysninger er en grunnleggende forutsetning for et åpent samfunn.

Et åpent samfunn?

NTL mener den enkeltes rett til kontroll over egne personopplysninger er en grunnleggende forutsetning for et åpent samfunn. Med kontroll over egne personopplysninger menes ikke at det offentlige ikke under noen omstendigheter skal kunne bruke opplysningene, men at forutsetningene for slik bruk skal være kjent på forhånd, og at informasjon om hvilke opplysninger som tas i bruk til hvilke formål skal være tilgjengelig for den det gjelder.

NTL mener samfunnet er tjent med et mangfold av livsstiler, næringsvirksomhet og politiske meninger, og at bruk av personopplysninger i etterforskning og etterretning kan motvirke den relative friheten som kjennetegner samfunnet i dag. Balansegangen mellom statens operative behov for et datagrunnlag og hensynet til den enkelte må derfor alltid ses i et perspektiv som også omfatter hensynet til et åpent samfunn på lang sikt og ikke bare den enkeltes påviselige umiddelbare interesser.

Norsk
Tjenestemannslag

www.ntl.no