STRATEGISK CYBERSIKKERHET

6 FORSLAG FOR MER ROBUST DIGITAL SIKKERHET

AV: SIMEN BAKKE

UTSYN – FORUM FOR UTENRIKS OG SIKKERHET

INNLEDNING

Vi lever i en tid med økt sikkerhetspolitisk spenning hvor den digitale teknologien har gjort det enklere å begå kriminalitet og andre samfunnsskadelige handlinger. Den digitale teknologien har også gjort det enklere for kompetente trusselaktører å ta i bruk såkalte hybride virkemidler, slik at samfunnet kan påvirkes og destabiliseres. Digital spionasje, sabotasje, omfattende bruk av skadevare som for eksempel løsepengevirus, samt desinformasjons- og påvirkningskampanjer, kan alle være virkemidler for å skape konflikt, uro og usikkerhet – både i sivilsamfunnet og staten, og dens underliggende virksomheter.

For å stå imot slike koordinerte operasjoner, kreves det et bredt spekter av virkemidler i både stat og sivilsamfunn. Et relevant spørsmål å stille i den forbindelse, er om vi i dag har etablert et bredt nok spekter av virkemidler. Og om vi evner å koordinere oss godt nok – både mellom statens mange aktører og ved inkludering av det øvrige sivilsamfunnet – til at vi vil klare å motstå forsøk på destabilisering utenfra. Det er mye som tyder på at vi har et forbedringspotensiale knyttet til de nevnte temaene, også her i Norge.

Vi har flyttet mange av de viktigste verdiene våre, enten det er økonomi, informasjon, kommunikasjon eller samhandling, over til de digitale plattformene. Sikkerheten har imidlertid ikke fulgt tilsvarende etter, gitt trussel- og sårbarhetsbildet i det digitale domenet. Det digitale domenet skiller seg fundamentalt fra det analoge. Dersom vi skal evne å ivareta samfunnslimet også i det digitale domenet, er vi nødt til å tenke nytt og annerledes om digital sikkerhet og sikring. Vi har flyttet vårt demokratiske samfunn over til digitale plattformer, og nå må vi sikre at også tilliten ivaretas.

Dette fagnotatet er delt i tre. I første del av fagnotatet vil det redegjøres kort for noen hovedtrekk som *skiller* det digitale cyberdomenet fra den analoge, fysiske verden og hvordan dette påvirker sikkerheten vår. Andre del handler om sentrale utviklingstrekk og trusselscenarioer som belyser *hvorfor* vi i dag opplever økende utfordringer knyttet til *sikkerhet* og *sikring* i det digitale domenet. Deretter vil det i del tre diskuteres noen sentrale *virkemidler* for å sikre det digitale samfunnet bedre, og hvordan vi kan *organisere* oss for å skape en mer robust digital sikkerhet. Fagnotatet er derfor inndelt i følgende temaer:

1. Det digitale samfunnet
2. Det digitale trusselbildet
3. Virkemidler for bedre sikkerhet

1. Det digitale samfunnet

For det første forholder ikke komplekse datanettverk og internettet seg til *tid* og *rom* på samme måte som vi mennesker gjør i det analoge samfunnet og i den fysiske verden. Det tar millisekunder å sende informasjon på tvers av kontinenter i den digitale virkeligheten. Dette til tross for at dataene, som i sin enkleste og reneste form kun består av kodene "0" og "1" ("av" eller "på"), transporteres over fysiske kabelforbindelser på tvers av kontinenter. I praksis betyr dette at informasjon kan nå tilnærmet *hvem som helst*, *hvor som helst*, *når som helst*, uten store begrensninger så lenge man er tilkoblet internett.

For det andre kan nettverksoperasjoner *skalere* på en helt annen måte i det digitale domenet, sammenliknet i den fysiske virkeligheten. Det er med andre ord ikke et 1-til-1 forhold mellom antallet mennesker og antallet operasjoner som det samme mennesket kan utføre innen et bestemt tidsrom ved hjelp av datamaskiner. Én datamaskin kan utføre enormt mange operasjoner på svært kort tid. Datamaskiner kan kobles i nettverk med mange flere maskiner, og dermed kan de styres fra én sentral infrastruktur som gjør at ett enkelt menneske kan utføre svært mange operasjoner, *samtidig*. I praksis betyr dette at én enkelt kriminell aktør kan sende ut skadevare som låser ned enormt mange datamaskiner, verden over. Eller at én statlig trusselaktør sprer usann og falsk informasjon som når ut til svært mange personer, på tvers av geografiske grenser, som del av sine påvirkningsoperasjoner.

For det tredje er det utfordrende å verifisere *hvem* som befinner seg på den andre siden av dataskjermen. Vår bruk av digitale teknologier har i lang tid bygget på antakelsen om at man kan stole på hvem som benytter seg av en datamaskin. Dette viser seg å være en feilslått antakelse, som i dag skaper utfordringer for vårt digitale samfunn. Antakelsen om at du kan stole på at personen er den han utgir seg for å være, bygger på tillit. I den fysiske verden har vi mennesker stort sett tillit til hverandre og vi stoler på at vedkommende er den han faktisk utgir seg for å være. Dette er en antakelse som blir vesentlig utfordret når man ikke lengre ser personen på den andre siden av skjermen. Derfor trenger vi autentiserings-mekanismer som verifiserer identitet. Disse mekanismene, enten det er brukernavn, passord, kodebrikker eller ID-kort med elektronisk chip, kan likevel være relativt enkle å utnytte. Fordelen i det digitale domenet er at de fleste elektroniske spor *kan* lagres. Utfordringen de fleste møter i dag er imidlertid evnen til å analysere sporene ettersom datamengdene blir enorme.

For det fjerde er det utfordrende å *regulere* alle sider av de digitale teknologiene med en nasjonal tilnærming ettersom teknologiene i mindre grad forholder seg til nasjonalstatlige grenser. Det vil for eksempel være vanskelig, for ikke å si umulig, for Stortinget å regulere Facebook, Amazon, Twitter, Youtube eller Google. Det må derfor tilstrebes internasjonale samarbeid for regulering av store internasjonale teknologifirmaer og plattformselskaper. For eksempel gjennom FN, EU, WTO og liknende organisasjoner. Det eksisterer imidlertid en rekke områder som likevel *kan* reguleres nasjonalt, herunder sikring og beskyttelse av IKT-systemer. Ett eksempel på dette er sikkerhetsloven som har til hensikt å beskytte informasjonssystemer som er sentrale for ivaretakelsen av nasjonale sikkerhetsinteresser. Sikkerhetsloven regulerer imidlertid kun de virksomhetene som er underlagt loven, slik at det er svært mye informasjon som er verdt å sikre som ikke nødvendigvis er underlagt bestemmelsene i sikkerhetsloven. Personopplysningsloven er et annet eksempel med utgangspunkt i EUs GDPR, men denne loven har til hensikt å ivareta enkeltindividets personvern, ikke det digitale samfunnet og sikkerheten til våre tjenester, i stort.

For det femte er *leverandørkjederisiko* en problemstilling som er svært krevende i det digitale samfunnet. Internettet og de mange nettverkene det består av, er tett sammenvevd og integrerte. Det eksisterer både fysiske og logiske skiller og separasjoner, men kompleksiteten i nettverkene er formidable. Dette fører til at det er svært vanskelig å holde oversikt over den risiko som genereres hos leverandører og underleverandører, og som påvirker den enkelte virksomhet, tjeneste eller et helt samfunnsområde.

Problemstillingen med leverandørkjederisiko kan man gjenkjenne også fra det analoge samfunnet, noe som har blitt aktualisert med den såkalte Bergen Engines-saken. Norske myndigheter var ikke klar over at aktører med tilknytning til Russland, ønsket å kjøpe Rolls-Royce-bedriften som leverer båtmotorer til Etterretningstjenestens "spionskip" Marjata og det norske Sjøforsvaret. I det digitale samfunnet har bruken av det kinesiske selskapet Huawei som leverandør til vestlige telekom-nett, herunder utbygging av 5G-infrastruktur, skapt stor sikkerhetspolitisk debatt. Årsaken til dette er at det vil være tilnærmet umulig for vestlige samfunn og Norge, å helgardere seg mot at Huawei og kinesiske myndigheter legger bakdører inn i telekom-infrastrukturen, som igjen gir mulighet for spionasje eller sabotasje.

2. Det digitale trusselbildet

Utfordringene som er skissert ovenfor finner man også igjen i trusselscenarioene som er beskrevet i denne delen av fagnotatet. Det digitale trusselbildet består i dag av mange ulike trusselaktører og trusselscenarioer. Fire former for trusselscenarioer fremstår likevel som spesielt skadelige, er derfor verdt å trekke frem. Digital spionasje (nettverks-operasjoner), leverandørkjedeangrep, løsepengevirus (ransomware), og digitale påvirkningsoperasjoner.

Trusselscenario 1: Digital spionasje

Datainnbruddene mot Stortinget august 2020 og mars 2021, indikerer at fremmede stater er interessert i informasjon knyttet til våre politiske og folkevalgte organer. Dette har PST og Etterretningstjenesten advart mot i sine trusselvurderinger i lengre tid, og bør dermed ikke komme som en overraskelse på det norske samfunnet. Det som imidlertid ser ut til å ha overrasket mange, er at e-post, som de fleste av oss anser som et trygt sted å lagre informasjon, ikke er å anse som like sikkert som en safe med kodelås. Alle IKT-systemer innehar sårbarheter. Noen av sårbarhetene er relativt enkle å unytte, mens andre ikke engang er kjent for produsenten. Slik som tilfellet var med Microsoft Exchange-sårbarhetene som ble utnyttet ved datainnbruddet mot Stortinget i mars 2021.[1] Dette var såkalte nulldagssårbarheter, som Microsoft ikke var kjent med før de ble utnyttet av trusselaktører.

Selv om sårbarhetene ikke er kjent for leverandøren, betyr ikke dette at det er umulig å sikre seg mot slike trusselscenarioer. Stortingets direktør Marianne Andreassen uttalte etter det nevnte datainnbruddet at Stortinget ikke kunne avverget angrepet, ettersom det var nulldags-sårbarheter som ble utnyttet.[2] Dette er imidlertid en påstand med modifikasjoner. Hvorvidt man klarer å forhindre, avdekke og avverge et forsøk på angrep eller innbrudd, avhenger av *tiltakene* som er implementert. Et godt sikret system med en helhetlig sikkerhetsarkitektur som bidrar til å beskytte data, forhindre urettmessig tilgang, og detektere trusselaktivitet, kan også bidra til å forhindre slike scenarioer som det Stortinget ble utsatt for. Det handler om å begrense en trusselaktørs mulighet til å foreta handlinger, mest mulig.

Når det gjelder datainnbruddet mot Stortinget høsten 2020, viser PST i sin etterforskning at innbruddet trolig kunne vært forhindret, eller i det minste vanskeliggjort, ved bruk av helt grunnleggende sikkerhetstiltak: Sterkere passord, tydeligere skille mellom jobb og privat e-post, og bruk av to-faktor-autentisering på alle internett-eksponerte tjenester. PST skrev videre at "det er sannsynlig at operasjonen er utført av cyberaktøren som i åpne kilder omtales som APT28 og Fancy Bear. Denne aktøren knyttes til Russlands militære etterretningstjeneste GRU".[3] Datainnbruddene mot Stortinget er derfor to ytterst relevante eksempler på at helt sentrale norske virksomheter, som er viktige symbolmål i Norge, kan mangle grunnleggende sikkerhetstiltak. Dette til tross for Stortingets demokratiske viktighet.

Ved begge hendelsene ble det avdekket at e-post fra stortingsrepresentanter var på avveie. Det ble etter offentliggjøring av hendelsen uttalt at det ikke var snakk om sikkerhetsgradert informasjon, beskyttet med hjemmel i sikkerhetsloven. E-poster som sendes til og fra stortingsrepresentanter kan likevel inneholde informasjon som er sensitiv. Benyttet på riktig måte av en kompetent trusselaktør, kan informasjonen likevel medføre

stor skade. Politisk betent informasjon brukt i en strategisk desinformasjons- og påvirknings-kampanje styrt av en fremmed stat, kan ha et skadepotensiale ved offentliggjøring som er større enn spredning av sikkerhetsgradert informasjon. Er informasjonen kontroversiell nok og spres i de riktige kanalene til mange nok mennesker, kan det bidra til å skape splittelse i befolkningen eller det kan påvirke beslutninger i konkrete saker. Nettopp derfor er tilstrekkelig sikring av Stortinget og andre sentrale virksomheters IKT-systemer, avgjørende for å ivareta statens suverenitet.

Med utgangspunkt i de to hendelsene fra Stortinget er det grunn til å stille spørsmål om mangelen på sikringstiltak var innenfor det Stortinget aksepterer av risiko. Dette er lite sannsynlig, gitt at Stortinget er Norges fremste folkevalgte politiske institusjon. Vi kan aldri fjerne all risiko, men den kan reduseres til et akseptabelt nivå. Evnen til å ta stilling til akseptabel risiko, noe virksomheter underlagt sikkerhetsloven er forpliktet til å gjøre, forutsetter at de er i stand til å beskrive, vurdere og håndtere risiko. Uten å kritisere sikkerhetsarbeidet på Stortinget på noe som helst måte, er det grunn til å reflektere over hvorvidt de faktisk har vært i stand til å bedrive risikostyring. Etter mitt syn viser dette noe av utfordringen med at hver enkelt virksomhet selv står ansvarlig for egen sikkerhet og sikring. Vi er nødt til å diskutere om dette er den mest hensiktsmessige måten å skape et robust digitalt samfunn på (noe som vil belyses med forbedringsforslag i siste del av fagnotatet).

Trusselscenario 2: Leverandørkjedeangrep

Leverandørkjedeangrepet mot Solarwinds var en "game-changer" innen cyberangrep- og sikkerhet. Dette scenarioet er også tett knyttet opp mot temaet digital spionasje. Det som i ettertid ser ut til å være aktører som arbeider på vegne av russiske myndigheter, plantet en sårbarhet i programvare-oppdateringene til Orion-plattformen som leveres av Solarwinds. All programvare oppdateres jevnlig for at blant annet sikkerhetshull og andre sårbarheter skal fjernes. Det at trusselaktører planter bakdører og skadelig kode inn i helt legitime og nødvendige oppdateringer, er skadelig for tilliten til oppdateringsregimet. Vi er alle avhengige av å oppdatere program- og maskinvare, for å tette sikkerhetshull.

Svært mange virksomheter benyttet Solarwinds Orion-programvare. Så mange som 18 000 av de 33 000 selskapene som benyttet programvaren, installerte også oppdateringen med sårbarhetene som gav trusselaktøren bakdører for tilgang til deres IKT-systemer.[4] Bare i USA ble det på et tidlig tidspunkt rapportert at over 250 private og offentlige virksomheter var blitt rammet ved at sårbarheten var utnyttet, herunder helt sentrale myndighetsorganer som Department of Defence og Department of Homeland Security.[5] Det interessante å merke seg, er at ikke engang amerikanske sikkerhetsmyndigheter som CISA, den amerikanske utgaven av NSM, var i stand til å avdekke trusselaktørene. Først når trusselaktørene utførte datainnbrudd hos det private sikkerhetsselskapet FireEye ble utnyttelse av sårbarheten avdekket. Dette var når trusselaktøren stjal de avanserte "hacker"-verktøyene til FireEye. Senere var også Microsoft i stand til å detektere og avdekke nettverksoperasjonene da trusselaktørene beveget seg fra bedriftenes datasentre over til Microsoft sine skytjenester.

Sentrale norske institusjoner benyttet også Solarwinds programvare, og var berørt av sårbarheten. Oljefondet, SAS og et tosifret antall kraftselskaper rapporterte at de benyttet programvaren og installerte oppdateringene.[6] Hvorvidt en trusselaktør faktisk utnyttet disse sårbarhetene hos norske offentlige virksomheter, er ikke offentlig kjent. Problemstillingen som illustreres er imidlertid at også norske virksomheter blir berørt av internasjonale forhold, leverandørkjederisiko og den sikkerhetspolitiske spenningen som preger verden for øvrig. Denne gangen var det Solarwinds programvare som var offer for avanserte trusselaktører, og spørsmålet alle stiller seg er; hvem blir den neste?

Leverandørkjederisiko er en enorm utfordring i cyberdomenet. Dette skiller den digitale verden vesentlig fra den analoge. De færreste har tilgang til programvarekode som IKT-systemer kjører på, og dermed fungerer disse i stor grad som "black-boxes". Det betyr at man ikke har mulighet til å inspisere hva programvaren *faktisk* utfører av

operasjoner. Som hendelsen med Solarwinds illustrerer, kan også helt legitim programvare som mange virksomheter er avhengige av, bli utnyttet. Dette har ført til at flere virksomheter og i særdeleshet den amerikanske staten og deres sikkerhetsmyndigheter, nå trekker frem Zero-Trust som et prinsipp som alle IKT-systemer må implementere.[7] Zero-Trust betyr at man ikke skal stole på noen, og at man derfor må verifisere tilgang til data, ressurser og tjenester. Prinsippet innebærer også at man skal forvente at trusselaktører befinner seg innenfor virksomhetens nettverk, og at man dermed må ha evne til å detektere aktivitet.

Samtidig er det verdt å merke seg at dataselskapet IBM tidligere har uttalt at det i gjennomsnitt tar 280 dager før en virksomhet oppdager et data-innbrudd.[8] Dette sier altså noe om hvor utfordrende det for mange virksomheter kan være å avdekke slik aktivitet selv. Videre skriver sikkerhetsselskapet FireEye, som er noen av de fremste på cybersikkerhet, at 53 prosent av alle cyberangrep foregår uten at virksomheten selv merker det, og hele 91 prosent av alle angrep genererer ikke noen alarmer eller varsler hos virksomheten.[9] Dette indikerer altså hvor utfordrende det kan være å sikre IKT-systemer, med mindre man har en gjennomtenkt og helhetlig sikkerhetsarkitektur som bidrar til å beskytte mot, detektere og håndtere angrep.

I etterkant av Solarwinds-angrepet har president Joe Biden lansert en presidentordre for å øke cybersikkerhetstilstanden i det amerikanske samfunnet. Ordren inneholder en rekke helt konkrete sikkerhetstiltak, som skal implementeres innen en kort tidsfrist på 60-180 dager.[10] Presidentordren må sees i lys av både Solarwinds- og Microsoft Exchange-sårbarhetene som rammet det amerikanske samfunnet svært hardt. Dette er noe også Norge bør hente inspirasjon fra, dersom vi ønsker å heve cybersikkerhetstilstanden til et akseptabelt nivå.

Trusselscenario 3: Løsepengevirus (ransomware)

Ransomware er skadevare som krypterer og utilgjengeliggjør data, hvor trusselaktøren presser virksomheten til å utbetale løsepenger for å få tilgang til verktøy som igjen dekrypterer dataene. Løsepengene ønskes som oftest overført i Bitcoin eller annen kryptovaluta som dermed gjør sporing og etterforskning utfordrende. Dersom virksomheten ikke betaler, truer trusselaktøren med å spre dataene offentlig tilgjengelig ut på internett eller ved hjelp av andre kanaler, slik som "DarkWeb". Slike trusselscenarioer *kan* for private virksomheter medføre konkurs. Derfor er tilbøyeligheten til å betale ofte stor, selv om det anbefales at man ikke skal la seg presse. Et nylig eksempel på ransomware er angrepet mot Colonial Pipeline og rørledningsnettet i USA, hvor angrepet stanset drivstofftilførselen. Hendelsen hadde helt reelle konsekvenser for det amerikanske samfunnet, og førte til at bedriften betalte 36 millioner i løsepenger for igjen å få tilgang til egne datasystemer.[11]

For offentlige virksomheter kan ransomware-angrep føre til driftsstans, tap av enorme mengder data og sensitiv informasjon på avveie, samt brudd på personopplysningsloven (persondata på avveie). Løsepengevirus er et trusselscenario med konsekvenser som potensielt er vesentlig mer alvorlig sammenliknet med mange andre digitale trusselscenarioer. Det har forekommet dødsfall som følge av ransomware- angrep i Tyskland, hvor en kvinne måtte transporteres til et annet sykehus fordi universitetssykehuset i Düsseldorf ble rammet av ransomware.[12] Det er foreløpig ikke meldt om dødsfall i Norge, men politiet skriver i sin trusselvurdering for 2021 at "det vurderes som meget sannsynlig at norske virksomheter vil bli utsatt for datainnbrudd med løsepengevirus". Og videre skriver politiet at "det er videre mulig at virksomheter med samfunnskritiske funksjoner vil bli utsatt for datainnbrudd".[13]

Dette betyr at kraft- og vannforsyning, helsevesen, politi, kommuner, og andre sentrale samfunns-funksjoner *kan* bli utsatt for ransomware-angrep. Hvorvidt trusselaktørene vil lykkes med sine operasjoner, vil avhenge av den enkelte virksomhets sikkerhetsarkitektur, tiltak og sikring. Det som imidlertid er verdt å merke seg, er at løsepengevirusene blir mer og mer avanserte, og trusselaktørene blir dyktigere i sine operasjoner. Det er med andre ord vanskeligere å sikre seg, og det har vokst frem et organisert kriminelt marked

for å bestille angrep med bruk av løsepengevirus, såkalt Ransomware as a Service (RaaS).[14]

I Norge har løsepengeviruset som slo ut Østre-Toten kommune i starten av 2021, vist hvor omfattende konsekvensene av et slikt trusselscenario kan være for norske virksomheter. Kommunens digitale tjenester ble lammet og saksbehandlerne i kommunen måtte gå over til penn og papir ettersom tilgangen til informasjon i datasystemene var borte. I tillegg hentet trusselaktørene ut sensitive personopplysninger knyttet til de digitale tjenestene, og disse ble lagt tilgjengelig for nedlasting på "DarkWeb". Dette betyr igjen at hvem som helst, enten fremmede staters trusselaktører eller kriminelle, kan få tilgang til sensitive opplysninger som har blitt hentet ut fra Østre-Toten kommunes databaser.[15] Dette kan også gjelde sensitive person-opplysninger, eksempelvis knyttet til innbyggernes helsetjenester. Hva en trusselaktør vil kunne ønske å benytte slike opplysninger til, kan vi bare spekulere i. Det ligger imidlertid et stort misbrukspotensiale knyttet til slike opplysninger i dagens digitale samfunn.

Trusselscenario 4: Digitale påvirknings- og destabiliseringsoperasjoner

Digitale påvirkningsoperasjoner og desinformasjon er det skrevet mye om de siste årene, og spesielt etter at Trump i 2016 ble valgt til president i USA. Blant annet har det blitt dokumentert at aktører som opererte på vegne av russiske myndigheter benyttet sosiale medier for å spre bestemte budskap egnet for å påvirke utfallet av det demokratiske presidentvalget. Det ble også benyttet splittende retorikk for å sette befolkningsgrupper opp imot hverandre. Trump-supportere mottok negativt ladede budskap om Hillary Clinton, og motsatt; Clinton-supportere mottok negativt ladede budskap om Trump. Spesielt er disse metodene brukt i sosiale medier hvor spredningen av desinformasjon og propaganda kan være veldig effektiv. Risikoen og kostnadene for en aktør som ønsker å påvirke befolkningen ved spredning av desinformasjon i sosiale medier er liten, mens den potensielle gevinsten er stor. Derfor er sosiale medier i dag en egnet kanal for spredning.

Undertegnede har skrevet både fagnotat[16] og artikler[17, 18, 19] om påvirkningsoperasjoner, tidligere. Disse kan leses for utfyllende informasjon om påvirkningsoperasjoner. Det viktigste å merke seg i dette fagnotatet er at trusselscenarioene beskrevet her, er svært relevante også i forbindelse med digitale påvirknings- og destabiliserings-operasjoner. Informasjon som en trusselaktør tilegner seg gjennom digital spionasje, leverandørkjedeangrep eller løsepengevirus, kan alle benyttes til digitale påvirkningsoperasjoner. En kompetent trusselaktør som vet hvilken informasjon de er ute etter – som også vet hvordan denne informasjonen kan brukes strategisk for å påvirke folkemeningen, "stemningen" eller utfallet av en konkret sak – kan få en vesentlig fordel av å benytte fordekte påvirkningsoperasjoner. Eller informasjonen kan benyttes i forbindelse med destabiliseringsoperasjoner.

Sensitiv informasjon enten denne er tilegnet gjennom digital spionasje eller ransomware med uthenting av data, kan for eksempel offentliggjøres i digitale kanaler og spres ved bruk av sosiale medier. Dette kan gjøres utenom de tradisjonelle redaktørstyrte mediene som har en høyere terskel for å publisere informasjon tilegnet ved bruk av ulovlige metoder og kriminalitet, slik tilfellet er med digital spionasje og ransomware. En nyere sak fra Washington DC viser at politiet ble utsatt for løsepengevirus, hvor trusselaktøren presser politiet til å betale for ikke å publisere informasjon fra straffesaker, om informanter eller gjengmedlemmer.[20] Publisering av den nevnte informasjonen kan bidra til å øke konfliktnivået samt destabilisere lokalsamfunn. Dersom det ikke er kriminelle aktører ute etter penger som står bak slike operasjoner, men statlige aktører som ønsker å destabilisere en virksomhet eller et samfunn, vil dette være svært kostnadseffektiv metodebruk.

Utfordringen knyttet til digitale påvirknings- og destabiliseringsoperasjoner er at selv om myndighetene kan forsøke å skadebegrense, vil offentliggjøring og spredning av sensitiv informasjon i seg selv kunne medføre skade. Det er utfordrende for myndigheter eller andre å kontrollere hvordan informasjonen spres, hva den blir benyttet til, eller hvilke skadefølger (konsekvenser) offentliggjøringen har i et samfunn.

Staten kan ha så mange reaktive krisehåndterere og etterforskere som den bare vil, men klarer man ikke være proaktive og *forhindre* innbrudd, angrep, spionasje eller sabotasje, så vil man måtte akseptere at hendelsene vil kunne medføre konsekvenser. Derfor er det desto viktigere å forhindre at sensitiv informasjon kan komme på avveie, gjennom bedre, *forebyggende* sikkerhet.

3. Virkemidler for bedre sikkerhet

Hendelsene beskrevet i *det digitale trusselbildet* gir oss en god indikasjon på hvorfor vi har behov for å få på plass et generelt høyere sikkerhetsnivå i store deler av det norske samfunnet. Datainnbruddene på Stortinget, nulldagssårbarhetene i Solarwinds og Microsoft Exchange, samt løsepengevirusene blant annet mot Østre Toten-kommune, er noen sentrale hendelser fra nyere tid. Disse hendelsene viser hvilke utfordringer vi står overfor når det kommer til å sikre vår felles digitale infrastruktur, i møte med et mer krevende trusselbilde.

I denne delen av fagnotatet vil det listes opp noen mulige løsninger og forbedringsområder på de utfordringene som er skissert ovenfor. Forslagene har til hensikt å forbedre sikkerheten til staten, samfunnet og de mange virksomhetene som den består av, i stort. Enkelte tiltak kan være enklere og mindre tidkrevende å implementere, mens andre krever mer grunnleggende endringer når det gjelder utvikling av felles regelverk og reguleringer.

3.1 En sentralstyrt innsats for å øke cybersikkerhetstilstanden i Norge

Det er verdt å se nærmere på hva det amerikanske samfunnet foretar seg i etterkant av Solarwinds-hendelsene. President Joe Biden har signert en svært ambisiøs presidentordre for å heve cybersikkerhetstilstanden i det amerikanske samfunnet. Ordren gir føringer for iverksettelse av en rekke nødvendige tiltak i myndighetsapparatet, med relativt kort tidsfrist.

Det er verdt å se nærmere på hva det amerikanske samfunnet foretar seg i etterkant av Solarwinds-hendelsene. President Joe Biden har signert en svært ambisiøs presidentordre for å heve cybersikkerhetstilstanden i det amerikanske samfunnet. Ordren gir føringer for iverksettelse av en rekke nødvendige tiltak i myndighetsapparatet, med en tidsfrist som anses som hurtig.[21] Noen av de viktigste tiltakene fra presidentordren som kan være verdt å trekke frem, er:

- Trusselaktivitet skal deles umiddelbart med myndigheter som har ansvar for cybersikkerhet.
- Å benytte moderne skytjenester som kan tilby et høyt sikkerhetsnivå, skal fremskyndes.
- Det skal implementeres en risikobasert sikkerhetsarkitektur med utgangspunkt i Zero-Trust.
- Myndighetene skal tilstrebe mest mulig standardisering for ugraderte systemer som forvaltes av de mange private og offentlige aktørene.
- Ugradert informasjon skal verdivurderes og beskyttes etter skadepotensiale.

Dette er tiltak som er relevante også for Norge, og som ville bidratt til å øke sikkerhetstilstanden i hele samfunnet. Amerikanske myndigheter ser ut til å erkjenne at digital sikkerhet ikke er et tema som de kan overlate til resten av samfunnet, og til hver enkelt virksomhet selv, å avgjøre. Myndighetene må sette minimumskrav og tilrettelegge for at sikkerhetstilstanden kan økes, slik at både staten og samfunnets sikkerhet ivaretas. Spesielt viktig blir dette i en tid der kompetente trusselaktører ønsker å utføre skadelige handlinger.

3.2 Et eget lovverk for IT-sikkerhet i Norge

En konkret og relevant anbefaling fra NOU 2018:14 "IKT-sikkerhet i alle ledd", er å vedta en egen lov for IKT-sikkerhet i det norske samfunnet.[22] En slik lov kan bidra til å gi en *baseline* med minimums-krav alle virksomheter som opererer i Norge må forholde seg til, slik at sikkerhetstilstanden i samfunnet generelt sett, heves. Dagens risikobaserte tilnærming med liten grad av lovregulering og standardisering av krav, fører til stor variasjon i virksomheters risiko- og akseptnivå. Fordelen med å lovregulere IT-sikkerhet er at det i tillegg til å etablere minimumskrav til forvaltning, også kan gjennomføres tilsyn knyttet til etterlevelse av lovverket. Dette vil på sikt bidra til å øke

sikkerhetstilstanden hos underlagte virksomheter. Et slikt lovverk må sees på som et tillegg til de føringer som sikkerhetsloven fastsetter og vil kunne treffe flere virksomheter, og større deler av samfunnet enn hva som er tilfellet for sikkerhetsloven. Detaljene for hva som helt konkret skal reguleres og hvordan, må utredes.

Dagens regulering av IT-sikkerhet er fragmentert hvor en rekke ulike lovverk har bestemmelser relatert til informasjonsbehandling og informasjonssikkerhet. Dette kan føre til uoverensstemmelse mellom lovverk, samt utfordringer knyttet til teknisk utvikling av løsninger som understøtter lovkravene. Det kan være fordelaktig å vurdere en lov for digital informasjonsbehandling mer generelt, hvor IT-sikkerhet er innebygget som én vesentlig del av dette lovverket, fremfor å ha en egen IKT-sikkerhetslov. Poenget er i begge tilfeller å forplikte spesielt offentlige virksomheter, som forvalter data på vegne av fellesskapet, å beskytte informasjonen så godt som mulig. I tilfeller hvor det ikke stilles lovkrav til forvaltningen, kan politikk og andre hensyn ofte gå fremfor det å ivareta god sikkerhet.

Det kan blant annet stilles krav om etablering av styringssystem for informasjonssikkerhet og etterlevelse av rammeverk for beste praksis, slik som NIST-, CIS- eller ISO-rammeverkene. Etablering av styringssystemer og etterlevelse av rammeverk for informasjonssikkerhet, sørger for at alle relevante områder knyttet til forebyggende sikkerhet og informasjonssikkerhet er regulert av den enkelte virksomhet. Tilsynsfunksjonen som kan etableres gjennom et lovverk vil bidra til at ledelsen får økt oppmerksomhet knyttet til IKT-sikkerhet. Det vil alltid være slik at eksterne tilsyn og revisjoner gir oppmerksomhet og ledelsesforankring knyttet til et fagområde, selv om motivasjonen primært bør komme fra virksomheten selv. Et lovverk er bare et hjelpemiddel for å skape forpliktelse og motivasjon.

3.3 En felles digital grunnmur for offentlige og private virksomheter

En eventuell lov må følges opp med konkrete tiltak. Blant annet kan dette gjøres ved å følge NSMs anbefaling om å etablere en "felles digital grunnmur".[23] Større grad av fellesskap i staten og samfunnet knyttet til drift og utvikling av infrastruktur og plattformer, kan bidra til å øke sikkerhetsnivået for mange virksomheter. Ett konkret eksempel på dette fra offentlig forvaltning, er bruken av informasjonssystemer for behandling av sikkerhetsgradert informasjon. Dette er systemer som forvaltes sentralt og som holder et høyt sikkerhetsnivå.

En annen relevant diskusjon er om en "felles digital grunnmur" i Norge skal bestå av skytjenester som driftes av staten selv, eller om det på andre måter skal tilrettelegges for felles infrastruktur og plattformer som kan tilby et generelt høyt sikkerhetsnivå. En felles nasjonal skytjeneste er blant annet noe NSM har tatt til orde for tidligere.[24] Det er liten tvil om at mange aktører i dag velger å benytte seg av skytjenester fra store kommersielle og internasjonale selskaper som Microsoft, Amazon og Google. Dette kan bidra til å øke sikkerhetsnivået for mange virksomheter ettersom de kan utfase utdaterte systemer og annen "teknisk gjeld". Det er samtidig flere problemstillinger knyttet til rettslig regulering, internasjonale forhold og sikkerhetspolitikk, som gjør at skytjenester fra store aktører som de nevnte, også innebærer risiko. En felles tilnærming for staten som helhet knyttet til disse temaene og problemstillingene, ville vært fordelaktig for de mange vurderingene som må gjøres.

Det er imidlertid hevet over enhver tvil at det faktum at hver enkelt virksomhet selv står ansvarlig for å drifte, sikre, vedlikeholde, og oppdatere egne IKT-systemer både er dyrt og krevende. Ikke minst er det kompetansekrevende, noe Norge allerede har et underskudd på hva gjelder IT-sikkerhetsressurser.[25] Ved større grad av samarbeid på tvers av sektorer og virksomheter kan Norge bøte på kompetanseunderskuddet ved å tilrettelegge for mer bruk av felleskomponenter i alle deler av IT-drift og utvikling, der det er mulig.

3.4 Bedre samordning i det forebyggende, risikoreduserende sporet

Staten har de senere årene hatt stort fokus på samordning i det reaktive, hendelseshåndterende

sporet. Spesielt gjelder dette for virksomheter som er nært knyttet opp imot sikkerhets- og etterretningstjenestene. Felles cyber-koordineringssenter (FCKS) er ett eksempel hvor NSM, KRIPOS, PST og Etterretningstjenesten samarbeider og utveksler informasjon fra sine respektive kanaler. Nasjonalt cybersikkerhetssenter (NCSC) er NSMs senter for samarbeid knyttet til forebyggende IKT-sikkerhet og digital hendelseshåndtering.

Det er likevel, fremdeles, slik at hver enkelt virksomhet selv står ansvarlig for å gjennomføre forebyggende tiltak for å sikre egne IKT-systemer, med utgangspunkt i en risikobasert tilnærming. Noe vi blant annet finner igjen fra Sikkerhetsloven av 1. januar 2019.[26] Dette er både tid-, kompetanse- og kostnadskrevende. For å være i stand til å vurdere risiko, må virksomhetene ha oversikt over *verdier*, *trusler* og *sårbarheter*. Verdier og sårbarheter er virksomhetene i god stand til å ha oversikt over selv. Når det gjelder trusselbildet mot hver enkelt virksomhet, kan dette være noe mer utfordrende å holde oversikt over. En av årsakene til dette, er at det kan være vanskelig for hver enkelt virksomhet å ha oversikt over *hvem* og *hvilke aktører* som befinner seg bak et forsøk på innbrudd eller angrep.

Sentrale myndigheter kan ofte være i bedre posisjon til å vurdere hvilke aktører som trolig vil kunne ha interesse av verdier eller annet, knyttet til en bestemt virksomhet eller sektor. For at virksomhetene skal kunne sikres tilstrekkelig og risiko skal kunne reduseres til et akseptabelt nivå, må det tilrettelegges for deling av tilpasset trusseletterretning. NSM, PST og Etterretningstjenesten utgir åpne, ugraderte trusselvurderinger. Disse åpne, ugraderte trusselvurderingene kan ikke betraktes som spesifikke nok til at det gir virksomhetene tilstrekkelige forutsetninger til å vurdere *forsvarlig sikkerhetsnivå* og *akseptabel risiko*. Dette betyr at hver enkelt virksomhet eller sektor selv må etablere større kapabilitet og kapasitet til å utarbeide trusselvurderinger, noe som kan være utfordrende for mange virksomheter. Eller så må staten i større grad tilrettelegge for at dette utføres sentralt, og sørge for distribusjon til de mange virksomhetene og sektorene som skal sikre sine virksomheter.

3.5 Dimensjonerende trusselaktører og -scenarioer for sikringen

Som diskutert ovenfor i tiltak 4, er en sentral problemstilling avgjørelsen om hvilke aktører man skal dimensjonere sikkerheten og sikringen for. Dette omtales ofte som *dimensjonerende trusselaktører*. Vil andre staters etterretnings-tjenester eller aktører som opererer på vegne av disse være interessert i verdiene? Hvis svaret på dette er bekreftende, vil det være behov for å fastsette statlige aktører som dimensjonerende for sikringen. Videre blir spørsmålet hvilke verdier vil de i så tilfelle være interessert i? Dersom vi bruker Stortinget og datainnbruddene mot e-post-kontoene som eksempel, ville det vært relevant å vurdere beskyttelse av e-postserverne mot statlige aktører. Dersom dette var gjort, er det trolig mindre sannsynlig at Stortinget ville akseptert fraværet av grunnleggende sikringstiltak.

Videre vil hva man beslutter som dimensjonerende trusselaktører også ha betydning for hva man anser som et *forsvarlig sikkerhetsnivå*, noe også virksomheter underlagt sikkerhetsloven blir pålagt å forholde seg til. For å være i stand til å vurdere forsvarligheten i sikringen, er man derfor også nødt til å ha et bevisst forhold til trusselbildet.

En måte å imøtekomme denne utfordringen på, er at staten med sine respektive sektordepartementer tar ansvar for å utarbeide *dimensjonerende trusselscenarioer* som utgangspunkt for å vurdere forsvarlig sikkerhetsnivå. På den måten kan virksomhetene underlagt spesifikke sektorer generelt, eller sikkerhetsloven spesielt, benytte scenarioene som er utarbeidet. Da vil behovet for at virksomheten skal ansette eget personell for å bedrive kontinuerlig trusseletterretning, reduseres. Samtidig må den enkelte virksomhet påregne å gjøre noen egne vurderinger, men da med et bedre utgangspunkt.

3.6 Bedre sammenheng mellom proaktive og reaktive aktører og tiltak

Det eksisterer en rekke tiltak for å redusere sårbarhet og bidra til sikkerhet. Noen av tiltakene er *proaktive*, det vil si at de har til hensikt å forhindre skadelige handlinger å inntreffe. Andre er *reaktive*, det vil si at tiltakene har til hensikt å

skadebegrense eller å gjenopprette normaltilstanden etter at en hendelse har inntruffet. Tiltakene er videre fordelt på en rekke ulike aktører i det norske stats-, samfunnssikkerhets- og beredskapslandskapet.

En sentral utfordring knyttet til de *reaktive* virkemidlene i cyberdomenet, er at det er svært vanskelig å etterforske og straffeforfølge lovbrudd. Hendelsene mot Stortinget er således et illustrerende eksempel på hvilke utfordringer som sentrale statlige virksomheter *kan* stå overfor. Aktørene befinner seg utenfor Norge, hvor vi i liten grad har myndighet til å håndheve våre straffebud, tvangsmidler og rettsregler. Dette gjelder også mot mange av de kriminelle aktørene, i den grad det er hensiktsmessig å skille mellom kriminelle og statlige.

Til tross for dette, har vi likevel i Norge hatt stort fokus på de reaktive virkemidlene, slik som for eksempel politiets evne til å etterforske datakriminalitet. Riksrevisjonen ga politiet *sterk kritikk* for etatens arbeid mot datakriminalitet tidligere i 2021.[27] Det er i den forbindelse verdt å reflektere litt over hva som faktisk kan forventes av politiet og andre reaktive aktører i møte med den digitale kriminaliteten. Spesielt gjelder dette i tilknytning til etterforskning og straffeforfølgning av digital kriminalitet. Strafferetten stiller store krav til notoritet og saksbehandlingen generelt. Dette er høyere kvalitetskrav enn hva som for eksempel stilles til etterretningsbasert arbeid. En årsak er naturligvis at etterforskning med påfølgende påtale kan føre til domstolsbehandling og straff, noe som er grunnleggende i en rettsstat.

Den som mistenkes å ha begått et straffbart forhold har derfor krav på rettssikkerhet, noe som til en viss grad garanteres gjennom den rettslige reguleringen av politiets etterforsknings-virksomhet. Samtidig kan digitale etterforskninger medføre et enormt ressursbehov i politiet, dersom etaten skal være i stand til å gjennomføre de etterforskningsskritt som kreves for å sikre tilstrekkelig kvalitet og notoritet i bevisførselen. Derfor må vi gjøre det vanskeligere å begå digital kriminalitet. Vi må sikre våre systemer bedre og vi må etablere bedre samarbeids- mekanismer i Norge på tvers av de mange aktørene og sektorene i landet. Det er behov for mer strategisk tenkning om *hva* vi skal oppnå, *hvordan* og med bruk av *hvilke* virkemidler enn hva det tilrettelegges for i dag. Dette må også involvere de mange private cybersikkerhetsaktørene som er svært kompetente, ressurssterke, og ikke minst fungerer de som pådrivere på mange områder.

Fremfor å ha et enkeltfokus på aktører og enkeltlovverk, må vi i større grad heve blikket å se hvordan de ulike aktørene og samarbeids-mekanismene fungerer i et samspill, for å forhindre høyst relevante trusselscenarioer, slik som løsepengevirus og digital spionasje. Vi må etablere et samfunn med sikring i *dybden* hvor vi forhindrer trusselaktører å få tilgang til våre IKT-systemer og viktigste verdier. Samtidig som vi ivaretar helt grunnleggende demokratiske rettigheter, slik som eksempelvis personvern, kommunikasjonsfrihet og et minimum av overvåkning. Dette kan vi få til ved å skape et mer *robust* samfunn, hvor informasjons- og IKT-sikkerhet er en helt grunnleggende byggestein i alt vi foretar oss.

Vi bygger i dag fremtidens digitale samfunn og vi må gjøre det på en måte som sikrer tilliten mellom oss. Slik vi har hatt det de siste 207 årene, etter at demokratiet ble etablert i 1814.

Fotnoter

1. https://www.stortinget.no/no/Hva-skjer-pa-Stortinget/Nyhetsarkiv/Pressemeldingsarkiv/2020-2021/stortinget-utsatt-for-it-angrep/
2. Ibid.
3. Ibid.
4. https://krebsonsecurity.com/2020/12/solarwinds-hack-could-affect-18k-customers/
5. https://www.nytimes.com/2021/01/02/us/politics/russian-hacking-government.html
6. https://e24.no/teknologi/i/9O6P7l/norske-kraftselskaper-beroert-av-solarwinds-hacking
7. https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2515176/nsa-issues-guidance-on-zero-trust-security-model/
8. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/
9. https://www.fireeye.com/current-threats/annual-threat-report/security-effectiveness-report.html
10. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
11. https://www.digi.no/artikler/colonial-pipeline-betalte-36-millioner-til-hackerne/510304
12. https://www.cw.no/artikkel/hacking/tysk-kvinne-dode-etter-ransomeware-angrep-mot-sykehus
13. https://www.politiet.no/globalassets/04-aktuelt-tall-og-fakta/politiets-trusselvurdering-ptv/2021-02-12-0-ptv-2021.pdf
14. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
15. https://www.ostre-toten.kommune.no/dataangrepet/
16. https://www.prosjektutsyn.no/hvordan-bekjempe-desinformasjon-aktorer-strukturer-og-tiltak/
17. https://www.prosjektutsyn.no/beskyttelse-mot-pavirkningsoperasjoner/
18. https://www.dn.no/innlegg/datasikkerhet/hacking/cyberkriminalitet/innlegg-dataangrep-mot-demokratiet-et-varsel-om-illegitim-valgpavirkning/2-1-867612
19. https://www.nof.no/arkiv/Digitale-pavirkningsoperasjoner
20. https://www.washingtonpost.com/local/public-safety/ransomware-attack-dc-police/2021/05/11/e1cb8600-b295-11eb-ab43-bebddc5a0f65_story.html
21. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
22. https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/
23. https://nsm.no/getfile.php/136165-1612871437/Demo/Dokumenter/Rapporter/Risiko%202021%20hand-out.pdf
24. https://www.digi.no/artikler/norske-myndigheter-ser-pa-mulighetene-for-a-etablere-en-egen-nasjonal-nettsky/500512
25. https://www.ikt-norge.no/wp-content/uploads/2017/12/ikt-norges-kompetanserapport--2015-1-0-1-3-docx.pdf
26. https://lovdata.no/dokument/NL/lov/2018-06-01-24
27. https://www.riksrevisjonen.no/rapporter-mappe/no-2020-2021/undersokelse-av-politiets-innsats-mot-kriminalitet-ved-bruk-av-ikt/

Om forfatteren

SIMEN BAKKE

Bakke har en bred bakgrunn innen sikkerhet og beredskap, både fra Politiet og Forsvaret. Han er senior informasjonssikkerhetsrådgiver i Politiets IKT-tjenester, og har en master i risikostyring og sikkerhetsledelse fra Universitetet i Stavanger. Bakke er også aktiv i den offentlige debatten om disse temaene, og har skrevet en rekke artikler og fagnotater.

UTSYN – FORUM FOR UTENRIKS OG SIKKERHET

Stortorvet 3
0155 Oslo

www.prosjektutsyn.no

post@prosjektutsyn.no