NRK Nyheter

Metoderapport SKUP 2017

IT- AVSLØRINGENE i offentlige etater

Av Line Tomter og Anne Cecilie Remen, NRK Nyheter

Innholdsfortegnelse

Innsendere:

Line Tomter, line.tomter@nrk.no, 97150094, Anne Cecilie Remen, anne.cecilie.remen@nrk.no, 90126354

Redaksjon: Økonomi- og politikkredaksjonen, NRK Nyheter, FP 21, 0340 Oslo

1.INNLEDNING. Et spørsmål om tillit

Konkurranseutsetting i det offentlige skal sikre samfunnet gode tjenester til en lavere kostnad. Selv helt sentrale funksjoner som Nødnett og drift av IT-systemer i helsevesenet – som blant annet omfatter helseopplysningene til landets innbyggere - har blitt satt ut til – eller er vedtatt satt ut til - private selskaper med base i utlandet.

Kan vi være sikre på at selskapene som får disse svært viktige og følsomme oppdragene er til å stole på?

Kan vi stole på at norske offentlige foretak med ansvar for vår sikkerhet og vår helse har kompetanse som skal til for å følge opp eksterne IT-leverandører?

Og ikke minst; kan vi stole på at de private aktørene og toppledelsen i offentlige etater sier fra når noe går galt, og gir riktig informasjon når sikkerheten er truet og lover er brutt?

I løpet av dette prosjektet oppdaget og avslørte vi at svaret på alle disse spørsmålene var nei.

2. SLIK STARTET DET. Nyttårstipset

På Sørlandet første uken i januar, 2017. Kuldegradene hadde krøpet nedover og solen skinte over Pollen i Arendal. Vi satt på Sørlandskontoret til NRK for å skrive Skup-rappport.

Vi hadde laget flere saker på hvordan globalisering av IT-bransjen påvirket norsk næringsliv. Mens vi jobbet, kom det inn en mail fra en ukjent person, som skrev:

«Jeg vet ikke hvor mye info dere har om outsourcingen Broadnet har gjort til India? Tech Mahindra har full adgang til å sabotere infrastrukturen og de tok senest ned SDH-nettet i Kirkenes, så det var lite av Nødnett som var operativt i regionen."

Kunne virkelig deler av Nødnett, som spiller en helt sentralt i den norske sikkerhetsberedskapen, ha blitt satt ut av spill fra India?

Dette kunne åpenbart være et viktig tips, og det kom trolig som en direkte følge av akkurat de sakene vi satt og skrev Skup-rapport om – mulige farer ved outsourcing av IT-tjenester. Vi svarte tipseren straks. Arbeidet med Skup-rapporten fikk vente.

Tipseren insisterte på å snakke med oss via krypterte kanaler og lurte på om vi hadde Telegram, en applikasjon som er gratis å laste ned og bruke. Den krypterer samtaler og meldinger slik at det er umulig for arbeidsgiver og teleselskaper å spore hvem man har kontakt med. Vi bekreftet at vi brukte den aktuelle appen.

Mens vi ventet på ny kontakt, begynte vi å sjekke tipset så godt vi kunne.

Vi visste fra før at Broadnet leverer tjenester til sykehusforetakenes kjernenett og at selskapet er en viktig underleverandør til helseforetakene. Selskapet har sitt hovedkvarter på IT Fornebu i Bærum, og er en av Norges dominerende leverandører av fiberbasert datakommunikasjon.

- Tech Mahindra viste seg å være en indisk IT-gigant med over 117 000 ansatte som leverer tjenester verden over.

- SDH er navnet på et internasjonalt digitalt overføringssystem med høy kapasitet.
- Nødnett er navnet på et digitalt kommunikasjonsnett som skal sikre effektiv kommunikasjon for nød- og beredskapstjenester, blant annet politi, brannvesen og redningsetater.
- Nødnett skal også sikre nødetatene og Forsvaret trygg kommunikasjon med sykehus og flere sentrale virksomheter, blant annet kongehuset og Statoil. Nødnett er viktig i ulykker, krisesituasjoner og ved terroraksjoner.

Vi fant ingen offentlig tilgjengelig informasjon om at IT-systemet i Nødnett ble driftet fra utlandet.

Etter noen timer tok kilden igjen kontakt. Personen ga oss ikke navnet sitt, og oppga ikke arbeidssted, men ga umiddelbart et troverdig inntrykk. Det personen sa virket gjennomtenkt.

Påstanden var:
Underleverandørene til Nødnett har satt ut deler av driften til India, i strid med avtaler og lovverk. Deler av Nødnett hadde vært nede – såkalt nedetid – på lillejulaften 2016, og det skyldtes en feil utført i India.

Dette var en oppsiktsvekkende og skremmende påstand.

Et raskt søk ga oss følgende info: Direktoratet for nødkommunikasjon har gitt Motorola Solutions hovedansvar for drift, overvåking og feilretting i Nødnett.

Linjene eies av Staten, Telenor og Broadnet. I 2015 satte Broadnet ut IT-driften av noen av linjene til indiske Tech Mahindra. Men vi fant ingen informasjon om at dette gjaldt Nødnett.

Regnskapstallene til Broadnet viste at selskapet slet med store underskudd. Outsourcing kunne være en måte å kutte kostnader på.

Landets helseforetak er helt avhengige av et sikkert og velfungerende Nødnett. Etter hvert som vi snakket med folk om Nødnett-tipset, opplevde vi at mange ville tipse om oppsiktsvekkende og utrygge IT-forhold ved Helse Sør-Øst. Vi valgte å følge begge sporene.

3. METODER OG KILDEBRUK. Bit for bit i sladdede brev

Tipseren hadde ingen dokumentasjon på at outsourcingen til India var ulovlig. I arbeidet med tidligere saker om IT-sikkerhet hadde vi satt oss inn i sikkerhetsloven, og vår hypotese ble ganske raskt at Nødnett kunne være underlagt denne loven, og at drift fra India kunne være i strid med sikkerhetsloven.

Sikkerhetslovens hensikt er å motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale sikkerhetsinteresser.

Loven skal trygge innbyggernes rettssikkerhet og tilliten til - og kontrollen med - forebyggende sikkerhetstjeneste.

Første steg ble å få klarhet i om Nødnett var regulert av sikkerhetsloven. Det ble en mye mer omfattende prosess enn vi hadde sett for oss, og vi merket fra første stund stor motstand fra de aktuelle private og offentlige aktørene.

Vi søkte etter spor etter Nødnett og sikkerhetsloven i postjournalene til departementene, men fant ingenting – bortsett fra at Direktoratet for samfunnssikkerhet og beredskap (DSB) betegnet Nødnett som kritisk infrastruktur, noe som ble utdypet slik:

«Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner."

Mens vi kjørte hjem fra Sørlandet, tok vi kontakt med Nasjonal sikkerhetsmyndighet (NSM) for å høre om Nødnett var underlagt sikkerhetsloven. Det ville de ikke svare på.

Skuffet måtte vi konstaterte at denne type informasjon om sikkerhetsloven var unntatt offentligheten.

Vi måtte tenke ut nye veier for å få fakta på bordet. Vi håpet på at Nødnett – som sentral infrastruktur - var gjenstand for omfattende saksbehandling og kommunikasjon mellom offentlige etater i Norge.

Selv om etatene kan ha stor aktsomhet for ikke å røpe sensitiv informasjon, ville vi undersøke om ikke deler av puslespillet var å finne i brev og dokumenter der Nødnett ble omtalt.

Vi gikk i gang med søk i postjournalene, og valgte – i første omgang - å begrense søkene til dokumenter til og fra Nasjonal kommunikasjonsmyndighet (Nkom), Direktoratet for samfunnssikkerhet og beredskap (DSB), Justis- og beredskapsdepartementet og Forsvaret.

Vi fikk blant annet innsyn i et brev fra Forsvarsdepartementet til Samferdselsdepartementet, datert den 4. mars 2015. Der kunne vi lese følgende:

"Forsvarsdepartementet tar til etterretning eierskiftet og navneendringen fra BaneTele AS til Broadnet AS, og gjør med dette vedtak med hjemmel i sikkerhetsloven § 2 tredje ledd om at Broadnet AS er omfattet av sikkerhetsloven. "

Begrunnelsen som ble gitt var at Broadnet har kontroll over kritisk infrastruktur.

Det var blink. Vi hadde funnet en liten bit av puslespillet, men det var en viktig en. Nå kunne vi slå fast at Broadnet var underlagt sikkerhetsloven.

Dermed kunne vi gå i gang med jakten på neste brikke: Hadde Broadnet, slik vår kilde påstod, brutt sikkerhetsloven?

Vi søkte og fikk delvis innsyn i Nasjonal kommunikasjonsmyndighets (Nkom) halvårsrapport fra 2016 om sikkerhet og beredskap til Samferdselsdepartementet.

Mye var sladdet, men vi fant en ny viktig brikke i puslespillet: I rapporten fremkom det at Nkom og Nasjonal sikkerhetsmyndighet (NSM), sommeren 2016 hadde gjort tilsyn i Broadnets fysiske installasjoner.

Dermed kunne vi spisse søket i postjournalene ytterligere, og vi fikk delvis innsyn i et brev fra Broadnet til Nasjonal sikkerhetsmyndighet fra desember 2016.

Der ble det referert til at noen avvik var lukket. Det sto ikke hvilke avvik eller om avvikene gjaldt sikkerhetsloven. Vi kontaktet NSM igjen, og igjen ville de ikke svare på spørsmål om det aktuelle tilsynet - deres rolle i dette var, framholdt de, unntatt offentlighet.

Vi visste imidlertid at Nasjonal sikkerhetsmyndighet bare utfører tilsyn angående sikkerhetsloven. Vår hypotese var derfor at avvikene etter alt å dømme handlet om sikkerhetsloven. Det lå også i dagen at Broadnets brev var et svar på en tilsynsrapport.

Siden NSM ikke ville snakke om dette med oss, søkte vi om innsyn i tilsynsrapporten fra Nasjonal kommunikasjonsmyndighet. Og igjen ble sikkerhetsloven brukt til å hindre oss fullt innsyn.

Og igjen opplevde vi at vi likevel fant et par verdifulle brikker til puslespillet. Mellom sladdene på sidene, kunne vi lese følgende om Broadnet:

"Tilsynet avdekket manglende kompetanse på sikkerhetsloven med forskrifter. Særlig innen objektsikkerhet var det mange og alvorlige avvik".

For oss var dette et nytt viktig gjennombrudd: Broadnet hadde ikke fulgt sikkerhetsloven. De manglet endatil kompetanse.

At vi lyktes med bit-for-bit-metoden ga oss selvtillit til å gyve løs videre. Vi hadde for lengst erfart at private aktører og norske myndigheter ga oss så lite som overhodet mulig.

Men så lenge vi fortsatte med målrettede journalsøk, klarte vi sakte men sikkert å øke vår kunnskap og oversikt, basert på den informasjonen som ikke ble sladdet i brevene og dokumentene.

Neste skritt var å lete i postjournalene etter dokumenter til og fra Broadnet og Motorola, hovedleverandøren til Nødnett.

Hos Direktoratet for samfunnssikkerhet og beredskap søkte vi om innsyn i kontrakten mellom Broadnet og Motorola, og igjen fikk vi nei.

Vi klaget, men fikk fortsatt ikke innsyn av – ble vi forklart - hensynet til forretningshemmeligheter, statens forhandlingsposisjon og sikkerhetsloven.

Direktoratet ga oss derimot delvis innsyn i et "clarification document" fra Broadnet til Motorola fra 2015. Her sto det:

"Tech Mahindra Operations will be a combined ON and OFF shore setup, where all activities regulated by the Security laws (i.e. Nødnett) is handled in Norway, from Broadnet "A-rated" locations with authorized resources. • No information related to the complete Nødnett network will be accessible or visible in the off-shore operation."

Vi kunne nå slå fast at Nødnett var underlagt den strenge sikkerhetsloven, og at Nødnett skulle driftes fra Norge av sikkerhetsklarerte og autoriserte medarbeidere.

På denne bakgrunn ville det være svært alvorlig hvis Broadnet hadde outsourcet drif og og gitt IT-arbeidere i India tilgang til Nødnett.

Neste etappe i arbeidet vårt var å finne ut om det faktisk hadde skjedd.

3.1 Kan vi stole på kilden?

Kilden vår hevdet at en IT-ingeniør under arbeid med feilretting på Nødnett, hadde oppdaget uautorisert jobbing på nettet fra India. Men hvorvidt dette var meldt til myndighetene, var usikkert.

Vi fant ingen spor om at hendelsen var innrapportert i postjournalene. Da vi disse første dagene i januar ringte Nasjonal sikkerhetsmyndighet (NSM), Nasjonal kommunikasjonsmyndighet og Direktoratet for nødkommunikasjon avviste alle at det var innrapportert en slik hendelse.

Vi kunne ikke la være å sjekke videre. Utfordringen var: Kunne vi stole på den ansiktsløse kilden? Hvilke motiver hadde vedkommende? Var informasjonen riktig?

Det hender vi bruker anonyme kilder for å få ut vesentlig informasjon som vi ellers ikke ville fått. Men aldri før har vi kommunisert med en fullstendig anonym kilde over så lang tid. Selv om vi ønsket å sjekke tipset, var vi urolige. En anonym kilde kunne være hvem som helst.

Derfor var vi underveis i prosessen bevisste på dette. Vi skulle under ingen omstendighet publisere informasjon fra kilden som ikke var bekreftet på annet hold.

Kilden ville ikke avsløre noe om seg selv, men åpnet seg om sitt motiv: Vedkommende var opprørt over at Nødnetts underleverandører fikk ture frem uten at myndighetene reagerte.

Kilden mente at alle som var avhengige av et sikkert Nødnett måtte få kunnskap om at det ble driftet fra India. Det handlet om at nasjonale interesser sto på spill.

Tilliten vår til kilden fikk tidlig en smell. Det viste seg at den aktuelle datoen for nedetid i Nødnett som kilden hadde oppgitt, var feil.

Når datoen ikke stemte, hvordan kunne vi stole på resten av informasjonen?

Samtidig opplevde vi at samtlige direktører vi var i kontakt med i Broadnet, Motorola og Direktoratet for nødkommunikasjon tilbakeviste at Nødnett var delvis driftet fra India.

Dette skrev info-avdelingen i Direktoratet for nødkommunikasjon den 6.januar 2017, fire dager etter at vi begynte å jobbe med saken:

" Som formidlet tidligere til NRK driftes hele Nødnett og linjene som Nødnett benytter fra Broadnet og Telenor, fra Norge."

Hvis påstanden var riktig, var et helt sentralt premiss i vår hypotese feil.

Den anonyme kilden vår presenterte oss for et alternativt scenario: Direktoratet for nødkommunikasjon, som ble underlagt Direktoratet for samfunnssikkerhet og beredskap i mars 2017, hadde ikke kompetanse, og forsto ikke - eller fulgte ikke med på - hva som skjedde hos underleverandørene.

Fra andre saker vi hadde jobbet med tidligere, visste vi at det er vanskelig å dokumentere hvor IT-systemer driftes fra.

3.2 Trøbbel i Kirkenes

Da vi fikk tipset om Nødnett, tok vi først kontakt med Sør-Varanger kommune hvor Kirkenes ligger, deretter politi, sykehus og ambulansetjenesten i Finnmark. Hadde Nødnett vært nede den 23. desember 2016?

Vi begynte med dette sporet, siden vi regnet med at det ville være enklest å få bekreftet den delen av tipset. Stemte denne detaljen, var det en pekepinn om at resten av tipset kunne være troverdig.

Men vi slet med å få bekreftet at det hadde vært nedetid på Nødnett i Kirkenes. Folk vi snakket med i nødetatene understreket at nettet kan falle ut i perioder, uten at de får beskjed. Heller ikke i Finnmark forøvrig, i Troms eller Nordland hadde det blitt rapportert om problemer i dagene før jul.

Det hadde vært mildvær og ingen store ulykker lille julaften 2016. Ingen ville ha merket om Nødnett hadde falt ut, fikk vi vite.

Hadde primærkilden misforstått? Vi kontaktet både Direktoratet for nødkommunikasjon og Nasjonal Sikkerhetsmyndighet.

Det ble flere telefoner. Vi sjekket i postjournalene om det hadde vært korrespondanse mellom de aktuelle aktørene.

Etter gjentatte henvendelser og krav om innsyn fikk vi til slutt oversikt over utfall i nettet. Den 10. januar skrev Direktoratet for nødkommunikasjon (DNK) til oss i en e-post:

"Vi kan bekrefte at DNK 22. desember mottok varsel fra Motorola om et mulig avvik fra definerte driftsrutiner hos Broadnet."

Direktoratet avsluttet med *"Ytterligere detaljer rundt det konkrete avviket må rettes til Broadnet."*

Kildens påstand om et utfall i Nødnett i Kirkenes var korrekt, men det hadde funnet sted 22. desember, og ikke på lille julaften.

Broadnet ville overfor NRK bare innrømme at det hadde vært et enkeltstående avvik, som skyldtes en menneskelig feil, og nevnte ikke Nødnett med et ord.

Vi fikk senere vite at Motorola den 6. januar ga tilsynsmyndighetene et muntlig varsel om en uautorisert hendelse. India ble ikke nevnt.

Både Motorola og Broadnet ga tilsynsmyndighetene skriftlig varsel først flere døgn etter at NRK hadde gjennomført en omfattende ringerunde, og et par uker etter hendelsen hadde skjedd.

I slutten av januar fikk vi innsyn i Motorolas varsel, der de bekreftet at avviket involverte det indiske selskapet Tech Mahindra og en ansatt i utlandet.

Vi oppsummerte:

- Vi kunne nå dokumentere at Nødnett hadde hatt et utfall, og at det hadde vært en uautorisert tilgang fra utlandet.

- Vi visste også at de private selskapene når de rapporterte forholdet til norske tilsynsmyndigheter, ikke redegjorde for at hendelsen skjedde via en uautorisert tilgang fra India. Det var i strid med avtaler og lovverk.

3.3 Kompetansebygging som metode

Vi var to journalister med samfunnsvitenskapelig utdanning, uten stor teknologisk kompetanse. Det ble tidlig klart for oss at uten kunnskap om IT-systemer, ville det være vanskelig å stille riktige spørsmål og det ville være umulig å tolke påstander fra de involverte selskapene og myndighetene.

For å forstå konsekvensene av den omfattende outsourcings-bølgen innen IT i store norske virksomheter, måtte vi bli minst like gode på IT som maktens direktører.

I dette prosjektet sto vi rett og slett oppe i en kompetanse-fight av dimensjoner.

Vi måtte ha kompetanse på IT for å få respekt og bygge tillit hos kildene.

Vi måtte ha kompetanse på IT for å forstå det voksende og kompliserte kildematerialet.

Og ikke minst; Vi møtte stor motstand fra selskapene og de offentlige etatene. Vi måtte ha like god kompetanse som aktørene for å forstå om de redegjorde sannferdig.

Vi måtte lære oss et begrepsapparat, for å forstå og gjøre oss forstått. Her er noen få faguttrykk, av flere titalls eksempler, som vi lærte oss:

- Transmisjonsnett og -linjer (Linjene som Broadnet eier er med på å binde sammen Nødnetts kjernenett og basestasjoner)
- IT-Infrastruktur (Alt som binder sammen et stort IT-miljø; utstyr, programvare, funksjoner o.l. som gjør tjenester tilgjengelig for brukere)
- Tilgangsstyring (Løsninger som sikrer at kun utvalgte brukere har tilgang, og som logger og sporer hva brukerne gjør)
- Leverandørportal (En sikker linje inn til sykehusene som leverandører benytter. Man kan ikke se om teknikere henter eller endrer informasjon når de først er inne i systemet)

Men det viktigste for oss ble å forstå mer av hvordan IT-systemene ved store virksomheter er bygget opp, hvordan de regulerer tilgangsstyring, og hva IT-arbeidere får adgang til når de har administrative rettigheter.

Vi tilbragte adskillig tid med IT-ingeniører og IT-sikkerhetseksperter for å bedre kompetansen vår. Vi møtte IT-folk, som ikke ville bli sett sammen med NRK-journalister, på bortgjemte cafeer, og studerte tegninger over IT-systemer, brannmurer og tilgangsstyring, IT-arkitektur, databaser og sikkerhet.

I løpet av seks måneder var vi i kontakt med over 130 kilder for å bedre kompetansen vår. Vi møtte kontakter og kilder i Forsvaret, sikkerhetsmyndigheter, politiet, forskere, ulike fagforbund, frittstående konsulenter, jurister, IKT-eksperter, IT-direktører, sikkerhetssjefer, innkjøpere, IT-arkitekter, ledere, leger, medarbeidere i ulike tilsynsorganer og ansatte i Helse Sør-Øst, datagiganten DXC, Broadnet, Motorola, Tech Mahindra og andre selskaper i Norge og India.

Vi deltok også på flere IKT-seminarer og leste fagrapporter.

Når kompetansen vår økte, vokste også kildenes tillit til oss.

Jo mer vi forsto av IT, dess mer var kildene villige til å gi av presis og fortrolig informasjon. De stolte på at vi jobbet seriøst med stoffet, og de ville i økende grad bidra. Vår nyervervede IT-kompetanse ble en døråpner til datanerdene.

Under et kaffe-møte fikk vi ny informasjonen hvordan IT-infrastrukturer er bygget opp.

På et annet møte ble vi orientert om strukturen i det såkalte transmisjonsnettet.

Sammen med brokker av annen informasjon vi fikk, forsto vi at den som sitter på linjene i transmisjonsnettet kan stenge store deler av Nødnett, og at den som styrer drift av linjene kan utføre sabotasje.

Denne kompetansen gjorde det mulig for oss å etterprøve direktørene og selskapenes påstander. Da Direktoratet hevdet at Broadnets leveranse fra India ikke påvirket Nødnett, visste vi at det var feil.

IT-eksperter forklarte oss risikoen ved å innføre ny teknologi som skulle spille sammen med et lappverk av gamle systemer, slik både HSØ og Nødnett hadde gjort. Beskjeden fra kildene våre var: *Gamle svakheter kan forsterkes med nye løsninger.*

Flere av sikkerhetsekspertene vi snakket med understreket hvor viktig det var med systemer som overvåker og logger, og at det blir enda viktigere når en ekstern leverandør overtar driften. Det skulle vise seg at slike systemer var mangelvare i Helse Sør-Øst.

3.4 India-sporet

I et møte i Oslo med noen som kjente systemene fra innsiden, fikk vi vite det *ikke* var mulig å skille mellom driftstilgang av styringssystemer og transmisjonslinjer, slik Broadnet og Direktorat for Nødkommunikasjon hevdet.

Nettet er bygget opp slik at hvis man har tilgang til styringssystemet og kjernenettet, så har man i praksis tilgang til linjene Broadnet leverer til Nødnett.

Det finnes kun to nivåer, enten har du tilgang til alt, eller så har du tilgang til ingenting. Det skyldtes tekniske svakheter i systemene. Dette var vesentlig kunnskap å få. Denne dokumentasjonen viste vi til sikkerhetsfolk som kjenner til hvordan datasystemer er bygget opp.

"Dette er alvorlig," var tilbakemeldingen de ga.

En person som nylig hadde jobbet med tekniske sider ved Nødnett beskrev manglende sporbarhet som et sikkerhetsproblem. Dessuten var systemet for loggføring av hvem som hadde vært inne i systemene dårlig, loggene ble overskrevet – slettet - etter få uker.

Dessuten var det mulig for ansatte i Tech Mahindra å gjøre endringer på komponenter i kjernenettet, uten såkalt brukerautentisering. Det hørtes alvorlig ut.

Og når vi satte denne informasjonen sammen med hva sikkerhetseksperter tidligere hadde fortalt oss om at kjernenettet styrer all trafikken i Nødnett, forsto vi at det var grunn til å frykte for konsekvensene.

Året før hadde vi jobbet med saker om indiske IT-selskaper og kjente allerede teknikere som hadde jobbet for disse selskapene. Vi skulle møte en utenlandsk IT-arbeider med innsyn i Nødnett. Vedkommende trakk seg, men bidro med informasjonen som overbeviste oss om at vi var på rett spor.

Vi satt til slutt med flere oppsiktsvekkende opplysninger:

- Ledelsen i Broadnet lot IT-arbeidere i India ha uautoriserte tilganger og mulighet til å stenge ned vitale deler av Nødnett.
- Det var flytende overganger mellom Broadnet og Tech Mahindras organisasjoner.
- Nettet var bygget slik at det er vanskelig å begrense hva man kan foreta seg når man først har en teknisk tilgang. Vi fikk nye bekreftelse på tekniske svakheter.

I løpet av noen uker lyktes vi ad ulike veier å få tak i dokumentasjon på IT-driften fra India. Vi fikk blant annet innsyn i bedriftsinterne hemmeligheter, blant annet organisasjonskart til selskapene som var ansvarlige for Nødnett. Vi fikk navn på ansatte og ansvarlige ledere, alle

med indisk-klingende navn og med adresse i India. Vi fikk også innsyn i beskrivelsene av arbeidsoppgavene deres.

Dette var avgjørende dokumentasjon. Det var ikke riktig, som både myndigheter og selskaper hadde fortalt oss, at Kirkenes-hendelsen var et engangstilfelle.

IT-systemet til Nødnett var driftet fra India, av personell som ikke var sikkerhetsklarert, slik loven krevde. For å beskytte kildene, publiserte vi på det aktuelle tidspunktet ikke informasjonen. Av samme grunn kan vi ikke være mer spesifikke nå.

Informasjonen ga oss uansett viktig ballast i våre framstøt mot direktørene, og arbeidet med å ettergå deres svar og forklaringer. Omsider innrømmet Direktoratet for nødkommunikasjon at noen i India hadde hatt tilganger de ikke skulle hatt. Direktøren påsto at alt var ordnet opp i. Han hadde full tillit til Broadnet.

Da vi publiserte første sak om Nødnett, den 7. februar, hadde vi ingen åpne kilder på at sikkerhetsloven ble brutt. Likevel valgte vi å slå det fast som et faktum. Vi stolte på det sentrale personer hos myndighetene og forskere på IT-sikkerhet fortalte – og vår egen kompetanse. Direktøren for Nødnett ble satt til side.

PST, som senere etterforsket NRK-avsløringene, slo i november 2017 fast at aktørene, også Direktoratet for nødkommunikasjon, hadde brutt sikkerhetsloven.

3.5 Snikveien til Bulgaria

Mens vi jobbet med Nødnett nevnte flere kilder den planlagte outsourcingen i Helse Sør-Øst. Det handlet også her om tekniske svakheter i IT-systemene. Datoen for tjenesteutsetting i HSØ nærmet seg.

Med nyervervet kompetanse om styringssystemer og tilganger innen Nødnett, fikk vi kontakt med folk som hadde innspill til å følge opp outsourcingen i landets største helseforetak.

Vi fikk beskrevet svakheter i IT-systemene i HSØ som gjorde det teknisk umulig å sette ut infrastrukturen til eksterne uten å gi underleverandøren tilgang til samtlige pasientjournaler til 2, 8 millioner nordmenn.

Vi fikk også se kart over intern dataflyt i systemene, som vi lovet å ikke publisere, men som dokumenterte tekniske svakheter. Vi fikk informasjon om at pasientdatabasen i Helse Sør-Øst var et lappeteppe av gamle systemer fra mange ulike sykehus, som gjorde det vanskelig å overvåke og logge hva som skjer på innsiden av IT-systemet.

Det finnes systemer som overvåker og logger trafikk – hvem som gjør hva innenfor brannmurene – men Helse Sør-Øst, ble vi fortalt manglet slike systemer, som er meget kostbare.

Administrerende direktør i Helse Sør-Øst, Cathrine Lofthus, hadde noen måneder tidligere forsikret Storting og helseminister Bent Høie at all pasientdata skulle bli i Norge, og at utenlandske IT-arbeidere ikke ville få tilgang. Basert på det vi nå visse, framsto uttalelsen som naiv.

Vi fikk høre at det hadde blitt utarbeidet en risikoanalyse om outsourcing til Bulgaria, et halvt år etter styrets vedtak om å outsource. Vi fant merkelig nok ikke spor etter den i postjournalene, men en person hjalp oss ved å gi oss navnet på dokumentet - *Risk assessment, Access to CMO from Bulgaria*.

Dermed fikk vi innvilget innsyn hos Datatilsynet. Rapporten var sterkt sladdet, men påpekte økt risiko ved å outsource til Bulgaria. En risiko verken styret eller ledelsen hadde tatt høyde for da de et halvår før besluttet å sette ut driften til det amerikanske storselskapet DXC (Tidligere Hewlett Packard Enterprise). Kontrakten var verdt 7 milliarder kroner.

En person vi hadde hatt kontakt med over tid fortalte at eksterne IT-arbeidere, blant annet fra Bulgaria, allerede hadde vært på opplæring i HSØs kontorer i Oslo. De skulle ha fått omfattende tilganger, også til servere med pasientopplysninger.

Dette var i strid med alle løfter som var gitt, og det skjedde før outsourcingen var etablert, og uten at forholdsregler og sikkerhetsrutiner var etablert.

Problemet var at vi fortsatt manglet avgjørende dokumentasjon.

3.6 Husmøte med kildene

Outsourcingen ved HSØ skulle skje om noen uker. Dersom påstander om at bulgarere hadde tilgang til pasientinformasjon stemte, var dette viktig å avdekke før den formelle overtakelsen til DXC.

Vi kommuniserte tett med kildene på ulike måter, men vi manet samtidig til forsiktighet, vi ville ikke at noen skulle avsløres.

Ingen måtte benytte jobbtelefon eller arbeidsgivers e-post i kontakt med oss.

Etterhvert oppstod tanken på et stormøte, der målet var å sette sammen flest mulig biter med konkret informasjon. Først smilte vi av tanken. Snart var det likevel alvor og mange meldte at de ville stille.

En ettermiddag dukket en svært kompetent gruppe kilder opp på Marienlyst. De kom parvis, andre alene. Noen hadde gått god for oss. Mange av personene hadde vi aldri sett før eller snakket med. Ingen skrev seg inn under eget navn.

I et møterom på Marienlyst ble det drukket kaffe og Farris og spist sjokolade. Vi formidlet at vi håpet på å få dokumentasjon på hvem som hadde tilganger til IT-systemene, hvor de jobbet og hva de kunne gjøre med tilgangene.

Dynamikken på møtet ble enda bedre enn vi hadde håpet. Når hver og en kom med informasjon innen et gitt område, opplevde alle i rommet at de bare avslørte litt. De opplevde at det var mindre farlig å gi oss detaljer siden det var så mange andre som gjorde det samme. Slik ga hver og en små, men viktige biter av puslespillet.

Vi fikk se lister med navn over utenlandske IT-arbeidere som hadde administrative rettigheter og tilganger til dataservere med pasienthemmeligheter. En nervøs og oppildnet stemning preget møtet.

I løpet av det fire timer lange møtet ble lag på lag med opplysninger avdekket, sentrale personer i Helse Sør-Øst datterselskap Sykehuspartner hadde gitt en rekke utenlandske IT-arbeidere alle tilgangene til hundrevis av servere.

Sykehuspartner er et datterselskap av Helse Sør-Øst, som har ansvar for å drifte sykehusenes IT-systemer.

Selv for de fleste fremmøtte var dette ny informasjon. Folk ble sjokkerte og forbannet.

Det er uvanlig at betrodde ansatte har alle tilgangene, ble vi fortalt. Vi fikk se hvor ofte enkelte av de vel 100 IT-arbeiderne fra en rekke land, også i Asia, hadde vært inne i de mest sensitive datasystemene med tilgang til pasientjournaler. Flere hadde vært pålogget fra andre land, og mange hadde vært inne flere titalls ganger.

IT-arbeiderne hadde mulighet til å kopiere hele databasen med sensitive pasientdata på noen minutter, til å slette og endre data uten å legge igjen et eneste spor.

HSØ hadde lovet politikere, ansatte og pasienter at det eksterne selskapet ikke skulle få tilgang til pasientopplysninger.

Nå hadde vi dokumentasjon på at ledelsen i HSØ hadde brutt disse løftene. All informasjon vi fikk denne kvelden kjentes som avgjørende for prosjektet. Vi kunne nå også dokumentere at teknologidirektøren ved HSØ hadde feilinformert oss da vi intervjuet ham en uke tidligere.

Han hevdet blant annet at utenlandske arbeidere ikke hadde hatt, og ikke skulle få, tilgang til pasient-data. To dager etter at vi publiserte saken, måtte han trekke seg fra stillingen og styrelederververvet i Sykehuspartner.

3.7 Fasit er på LinkedIn

Dagen etter stormøtet gikk vi gjennom listen med over 100 navn som hadde fått tilganger til dataservere med pasientinformasjon. Nå begynte et detektivarbeid for å finne ut hvor disse jobbet og hvilken nasjonalitet de hadde. Vi googlet navnene, vi sjekket LinkedIn og vi brukte Facebook for å sjekke.

Vi kunne peile inn nettverket til folk for å sjekke om de jobbet i for eksempel DXC.

Fordelen med LinkedIn er at de fleste legger ut arbeidsgiver, utdanning og kompetanse, og at profilene er mer åpne enn på Facebook.

På denne måten fant vi ut at HSØ hadde gitt folk med en rekke ulike nasjonaliteter tilganger. Noen av IT-arbeiderne jobbet i India, noen i Malaysia, Bulgaria og Tyskland.

Vi fant også kinesiske navn, som ved søk viste seg å ha tilhold i Malaysia og Australia. Vi fant russiske navn. Noen så til ut å jobbe også andre steder enn DXC – trolig jobbet de for underleverandøren av underleverandøren. Dette var oppsiktsvekkende og i strid med alt ledelsen hadde lovet.

Det var et stort gjennombrudd. Dokumentasjonen vi nå satt på, var sentral i saken vi publiserte den 3. mai. Der innrømmet toppledelsen i Helse Sør-Øst at utenlandske IT-arbeidere fra India og Bulgaria likevel hadde hatt tilgang til sensitive pasient-data.

Saken ble samme dag tema i Stortingets spørretime. HSØ innkalte til ekstraordinært styremøte, og to dager senere begynte det store mannefallet i HSØ med teknologidirektørens avgang.

3.8 Send sikkert tips

For hver artikkel vi publiserte fikk vi nye tips. I reportasjene på NRK.no gjorde vi leserne oppmerksomme på at de kunne sende krypterte tips via “Secure drop”. Det fremkom i faktaboksen at dette er en sikker måte å tipse på der man ikke etterlater digitale spor.

Tjenesten, som en rekke norske medier tilbyr, gjør det mulig å dele filer og opplysninger, og forbli anonym overfor oss journalister.

Vi fikk flere tips på denne måten, som resulterte i gode saker. I mai kunne vi blant annet avsløre at IT-svikten ved Helse Sør-Øst var mye mer omfattende enn vi selv tidligere hadde avdekket:

IT-arbeidere i Malaysia, India og Bulgaria hadde ikke bare hatt tilgang til norske pasientdata, de hadde også hatt tilgang til e-post og hjemmeområdene på jobb-PC-ene til over 70 000 ansatte i Helse-Norge. Dessuten kan langt flere personer enn tidligere kjent hatt tilgang til sensitive pasientopplysninger på 2,8 millioner nordmenn.

4.MOTSTAND

Vi tror ikke vi tidligere har opplevd like intens og omfattende motstand i et journalistisk prosjekt.

De sentrale aktørene, både offentlige eller private, nektet, nesten uten unntak, å stille til intervjuer. Vi forsto etterhvert at aktørene trolig håpet at vi ville gi opp.

Samtidig som de fortalte oss minst mulig, minnet de oss i hver e-post på PFU og Vær Varsom-plakaten.

Resultatet var at vi ikke fikk noe som helst intervju verken med Broadnet, Motorola eller Tech Mahindra før vi publiserte den første Nødnett-saken. Vi fikk bare sitater gjennom mailer.

Vi opplevde gang etter gang at aktørene dyttet sikkerhetsloven foran seg. De hevdet sikkerhetsloven gjorde det vanskelig å besvare spørsmålene våre.

Slik brukte de sikkerhetsloven som en unnskyldning til å nekte oss journalister innsyn, og slik lyktes de lenge å hindre at norsk offentlighet fikk kunnskap om alvorlige mangler og svikt i landets kritiske infrastruktur.

Verken Nasjonal sikkerhetsmyndighet, Nasjonal kommunikasjonsmyndighet og Direktoratet for nødkommunikasjon ville innrømme at det hadde skjedd noe som var ulovlig eller ureglementert.

Direktoratet svarte omsider etter flere dager:

"I Finnmark er det ikke registrert utfall på basestasjoner 22./23. desember. Utfallene var i andre deler av landet. Vi trenger noe tid til å sammenstille informasjon her (...).."

Etter at direktoratet forsto at vi satt på avgjørende informasjon kom de med en ny forklaring: "*IT-arbeiderne i India hadde bare hatt tilgang til ti prosent av Nødnett."*

I postjournalen oppdaget vi at Broadnet klaget til Nasjonal kommunikasjonsmyndighet etter at de hadde gitt oss innsyn i den fullstendige rapporten hvor lovbruddene var beskrevet.

Vi forsto at miljøet er lite. Direktører i Motorola, Broadnet og direktoratet kjente hverandre.

I intervju med NRK hevdet direktør Tor Helge Lyngstøl i Direktoratet for nødkommunikasjon at det var nærmest umulig å kontrollere underleverandørene, og at mye var basert på tillit.

På spørsmål fra oss om han hadde spurt hvor lenge Tech Mahindra hadde hatt tilgang, svarte direktøren nei. Innrømmelsen var viktig for oss og et gjennomslag i jobbingen.

Vi fant det oppsiktsvekkende at Direktoratet som hadde ansvar for at Nødnett faktisk fungerte lot underleverandørene styre nettet uten noen form for tilsyn og kontroll, og at direktoratet selv ikke varslet tilsynsmyndighetene da de første gang hørte om avviket.

Også etter at vi hadde publisert de første sakene, hevdet Direktoratet for nødkommunikasjon at vi kom med feil informasjon og krevde at vi fjernet påstander om at Nødnett ble driftet fra India.

5. DETTE ER NYTT

- NRK avdekket at IT-arbeidere i India i 14 måneder hadde uautorisert tilgang til Nødnett.

- NRK avslørte at ansvarlige norske myndigheter ikke hadde kontroll over hvem som driftet Nødnett, noe som er i strid med loven.

- NRK avdekket at landets største helseforetak, Helse Sør-Øst, ga IT-arbeidere i en rekke land i Asia og Øst--Europa omfattende innsyn i pasientjournaler til 2,8 millioner nordmenn, i strid med lovgivingen.

- NRK avslørte at toppledelsen i Helse Sør-Øst feilinformerte Storting og Helse- og omsorgsdepartementet, ved å opplyse at ingen pasientdata skulle bli tilgjengelig fra utlandet.

- NRK avdekket tekniske svakheter i de viktigste IT-systemene til både Nødnett og Helse Sør-Øst.

- NRK avslørte at Helse Sør-Øst vedtok å konkurranseutsette IT-infrastrukturen uten å vurdere risikoen.

- Direktoratet for nødkommunikasjon lot en underleverandør konkurranseutsette drift av Nødnett til et indisk selskap. Direktoratet og underleverandøren gjennomførte ingen risikovurdering.

6. KONSEKVENSER

NRKs avsløringer fikk store konsekvenser.

Hele styret i Sykehuspartner, som drifter IT-systemene til Helse Sør-Øst, måtte gå av. Administrerende direktør fikk sparken. Teknologidirektøren måtte trekke seg fra stillingen.

Datatilsynet ila sykehusene i Helse Sør-Øst tilsammen 7,2 millioner kroner i bøter for blant annet brudd på personvernloven.

Helse Sør-Øst stoppet den planlagte outsourcingen av IT-driften til utlandet. Den er fortsatt i bero.

I oktober innrømmet helseminister Bent Høie at Helsedepartementet mangler oversikt over IT-sårbarheter i helsevesenet.

Helse Sør-Øst hyret rådgivningsgiganten PWC til å gjennomgå informasjonen lagt fram i NRKs saker. Rapporten var knusende for ledelsen i helseforetaket (og bekreftet NRKs funn).

Nasjonal kommunikasjonsmyndighet gjennomførte et omfattende tilsyn etter NRKs saker. De avdekket ni lovbrudd i Broadnet, som blant annet ble refset for å ha gitt personell i India tilgang til Nødnett. Det kunne tilrettelegge for spionasje og sabotasje mot Nødnett.

PST startet etterforskning av Broadnet og alle aktørene i Nødnett-saken. PST konkluderte med at aktørene hadde brutt sikkerhetsloven. Sakene ble henlagt, fordi hjemlene i sikkerhetsloven var mangelfulle. PST krever endringer i sikkerhetsloven.

Høsten 2017 varslet justisministeren endringer i sikkerhetsloven, som en følge av Nødnett-saken. Statsråden oppfordret sentrale statlige organer til å gjennomgå alle IT-kontrakter.

Forsvarsdepartementet jobber med ny sikkerhetslov, og hjemmel til å ilegge bøter og sanksjoner ligger inne i det nye lovforslaget.

Nasjonal kommunikasjonsmyndighet konkluderte med outsourcingen til utlandet av IT-tjenester for Nødnett, la til rette for spionasje og sabotasje fra India med mulighet til å påvirke tilgjengeligheten i nettet.

I det tidligere Nødnettdirektoratet, som nå er underlagt Direktoratet for samfunnssikkerhet og beredskap, ble direktøren fratatt ansvaret for Nødnett.

OVERSIKT OVER SAKENE

Oversikt over de viktigste sakene i Nødnett og Helse Sør-Øst, på NRK.no, Dagsnytt/Nyhetsmorgen og på TV:

07.02.2017
Driftet nødnettet ulovlig fra India

https://www.nrk.no/norge/driftet-nodnettet-ulovlig-fra-india-1.13358591
https://radio.nrk.no/serie/nyhetsmorgen/NPUB50002717/07-02-2017
-Nødnettsaken er en varslet skandale
https://radio.nrk.no/serie/nyhetslunsj/NPUB44002717/07-02-2017#t=5m22s
Justisministeren: Et alvorlig tillitsbrudd
https://www.nrk.no/norge/justisminister_---alvorlig-tillitsbrudd-at-it-arbeidere-i-india-har-tilgang-til-nodnett-1.13364039
Lysne om nødnett + justisministeren om nødnett
https://radio.nrk.no/serie/nyhetsettermiddag/NPUB51002717/07-02-2017#t=34m33s
https://radio.nrk.no/serie/nyhetsettermiddag/NPUB51002717/07-02-2017
Om AMK, nødnett driftet fra India, Krøvel fra Broadnet om sikkerhet, og nødnettsjef Tor Helge Lyngstøl innrømmer lovbrudd:
https://tv.nrk.no/serie/dagsrevyen/NNFA19020717/07-02-2017
08.02.2017
Nkom: Aktuelt å anmelde nødnett
https://tv.nrk.no/serie/dagsrevyen/NNFA19020817/08-02-2017
10. 02.2017
Broadnet flytter all IT-drift fra India til Norge
https://www.nrk.no/norge/broadnet-flytter-all-it-drift-fra-india-til-norge-1.13371402
PST starter etterforskning i nødnettsaken
https://tv.nrk.no/serie/dagsrevyen/NNFA19021017/10-02-2017#t=7m51s
NSM åpner tilsynssak etter Nødnettskandalen
https://tv.nrk.no/serie/kveldsnytt/NNFA23021017/10-02-2017#t=48s
14.02.2017
IT-arbeidere i India hadde tilgang i 14 måneder
https://www.nrk.no/norge/it-arbeidere-i-india-hadde-nodnett-tilgang-i-14-maneder-1.13377940
Justisministeren er sjokkert over at det tok 14 måneder å oppdage indere i nødnett
https://tv.nrk.no/serie/dagsrevyen/NNFA19021417/14-02-2017#t=5m44s
31.03.2017
Indere har fremdeles tilgang til Nødnettet + politisk reaksjoner
https://radio.nrk.no/serie/nyhetsmorgen/NPUB50006517/31-03-2017
https://www.nrk.no/norge/it-arbeidere-i-india-har-fortsatt-tilgang-til-nodnettet-1.13452434
https://radio.nrk.no/serie/nyhetslunsj/NPUB44006517/31-03-2017#t=19m37s
03.05.2017
Innrømmer at IT-arbeidere i utlandet har hatt tilgang til pasientjournaler
https://www.nrk.no/norge/helse-sor-ost_-innrommer-at-utenlandske-it-arbeidere-har-hatt-tilgang-til-pasientjournaler-1.13478443
Bent Høie om pasientinformasjon
https://radio.nrk.no/serie/dagsnytt/NPUB22010617/03-05-2017#t=32s
Høie anklages for å ha villedet Stortinget:
https://tv.nrk.no/serie/dagsrevyen/NNFA19050317/03-05-2017
04.05.2017
Krever at adm. direktør i Helse Sør-Øst går av:
https://tv.nrk.no/serie/dagsrevyen/NNFA19050417/04-05-2017#t=6m0s
05.05.2017
Vedgår at helseministeren fikk mangelfull informasjon

https://www.nrk.no/norge/helse-sor-ost-vedgar-mangelfull-informasjon-1.13501745
08.05.17
Mener Høie var arrogant da han avviste bekymringsmelder.
https://www.nrk.no/norge/mener-hoie-var-arrogant-da-han-avviste-bekymringsmeldinger-1.13503750
05.05.2017
Bagley trekker seg som styreleder
https://www.nrk.no/norge/bagley-trekker-seg-som-styreleder-i-sykehuspartner-1.13503436
https://tv.nrk.no/serie/dagsrevyen/NNFA19050517/05-05-2017#t=9m2s
09.05.2017
Frykter for feilbehandling etter IT-svikt
https://www.nrk.no/norge/pasientombud-og-lege-frykter-feilbehandling-etter-it-svikt-1.13508332
Krever åpenhet om journalskandalen
https://tv.nrk.no/serie/dagsrevyen/NNFA19050917/09-05-2017
https://tv.nrk.no/serie/kveldsnytt/NNFA23050917/09-05-2017
19.05.2017
Sparket helsetopp får ny direktørjobb i helsevesenet
https://www.nrk.no/norge/fagforbund-kritiske-til-at-sparket-helse-sor-ost-sjef-far-ny-direktorjobb-i-helsevesenet-1.13517166
24.05.2017
Høie kan ikke love at journalskandalen er over
https://www.nrk.no/norge/hoie-kan-ikke-love-at-journalskandalen-er-over-1.13530672
Cathrine Lofthus om at IT-prosjektet settes på vent
https://radio.nrk.no/serie/nyhetslunsj/NPUB44010317/24-05-2017#t=14m13s
IT-ansatte i utlandet får ikke lenger drifte datasystemene i HSØ
https://tv.nrk.no/serie/dagsrevyen/NNFA19052417/24-05-2017
31.05.2017
Skifter ut hele styret i Sykehuspartner
https://www.nrk.no/norge/skifter-ut-hele-styret-i-sykehuspartner-1.13539226
09.06.2017
Toppsjef i Sykehuspartner går fra stillingen
https://www.nrk.no/norge/sykehuspartner-toppsjef-gar-fra-stillingen-1.13552506
14.06.2017
Helseministeren frifinner seg selv
https://www.nrk.no/norge/helseminister-frifinner-seg-selv-i-journalskandalen-1.13557150
26.06.2017
Betrodde medarbeidere holdt tilbake informasjon
https://www.nrk.no/norge/helse-sor-ost_-betrodde-medarbeidere-holdt-tilbake-informasjon-om-risikoen-ved-outsourcing-1.13577233
28.06.2017
Rapporten om pasientjournaler viser omfattende svikt
https://tv.nrk.no/serie/dagsrevyen/NNFA19062817/28-06-2017
-Ledelsen burde stilt spørsmål ved risikoen
https://radio.nrk.no/serie/nyhetsmorgen/NPUB50012417/28-06-2017
Rapporten om pasientjournaler viser omfattende svikt
https://tv.nrk.no/serie/dagsrevyen/NNFA19062817/28-06-2017

Helse Sør-Øst: Outsourcingen stoppes. https://www.nrk.no/norge/helse-sor-ost_-outsourcing-stoppes-1.13578806
29.06.2017
Bent Høie svarer om journalskandalen
https://radio.nrk.no/serie/dagsnytt/NPUB22015517/29-06-2017
26.07.2017
AP vil ha mindre outsourcing av IT-tjenester
https://www.nrk.no/norge/ap-vil-ha-mindre-outsourcing-av-ikt-tjenester-1.13617204
10.08.2017
Frykter at ondsinnede kan utnytte sikkerhetshull i nødnettet. Fortsatt brudd på sikkerhetsloven
https://www.nrk.no/norge/frykter-at-ondsinnende-kan-utnytte-sikkerhetshull-nodnettet-1.13633385
8.09.2017
Tilsynsmyndighet: - Må ha orden i eget hus før man outsourcer
https://www.nrk.no/norge/_-ma-ha-orden-pa-it-i-eget-hus-for-man-outsourcer-1.13646789
09.09.2017
Offisersforbundet: - Vi er bekymret for sikkerheten i nødnettet
https://www.nrk.no/norge/offisersforbundet_-_-vi-er-bekymret-for-sikkerhetshull-i-nodnettet-1.13672231
14.09.2017
Fortsatt IT-uvisshet i Helse Sør-Øst
https://www.nrk.no/norge/fortsatt-it-uvisshet-i-helse-sor-ost-1.13686202
15.09.2017
Lofthus: - Jeg har vært forbannet
https://www.nrk.no/norge/helse-sor-ost_-_-jeg-har-vaert-forbannet-1.13689249
22.09.2017
https://radio.nrk.no/serie/nyhetslunsj/NPUB44019017/22-09-2017#t=1m24s
21.10.2017
https://www.nrk.no/norge/varsler-gebyr_-flere-lovbrudd-i-driften-av-nodnettet-1.13787958
25.10.2017
Vet ikke hvem som har tilgang
https://radio.nrk.no/serie/dagsnytt/NPUB35029817/25-10-2017
https://www.nrk.no/norge/innrommer-mangel-pa-oversikt-over-ikt-sikkerhet-i-helse-sor-ost-1.13748804
27.10.2017
Millionbøter etter outsourcing av sykehus-IT
https://www.nrk.no/norge/millionboter-etter-outsourcing-av-sykehus-it-1.13751516
Helse Sør-Øst. Store millionbøter.
https://tv.nrk.no/serie/dagsrevyen/NNFA19102717/27-10-2017
21.11.2017
Rapport fra Nkom bekrefter tilganger fra India
https://radio.nrk.no/serie/dagsnytt/NPUB21032517/21-11-2017#t=21s
Reaksjoner på rapport om tilganger fra India
https://radio.nrk.no/serie/nyhetsettermiddag/NPUB51023217/21-11-2017#t=27m12s
Tekna kaller Nødnett-vedtak for milepæl
https://radio.nrk.no/serie/nyhetsettermiddag/NPUB51023217/21-11-2017

22.11.2017
PST etterlyser bedre lover for IT-sikkerhet
https://www.nrk.no/norge/pst-ber-politikerne-om-tydeligere-lover-for-it-sikkerhet-1.13788835
PST ber om at Sikkerhetsloven endres
https://www.nrk.no/norge/pst-ber-politikerne-om-tydeligere-lover-for-it-sikkerhet-1.13788835
Nødnett oppfølging, radio
https://radio.nrk.no/serie/nyhetsmorgen/NPUB50022917/22-11-2017#t=1h46m22s
28.11.2017
Justisministeren: - Mangel på risikovurdering i nødnettsaken
https://www.nrk.no/norge/amundsen_-mangel-pa-risikovurdering-i-nodnett-saken-1.13798108
Nødnett, justisministeren vil endre sikkerhetsloven
https://tv.nrk.no/serie/kveldsnytt/NNFA23112817/28-11-2017
30.11.2017
E-helsedirektoratet: - Det er fritt frem for utflagging av IT i helse-Norge
https://www.nrk.no/norge/e-helse_-__det-er-fritt-frem-for-utflagging-av-it-i-helse-norge-1.13802322
Utflagging av e-helsetjenester
https://radio.nrk.no/serie/dagsnytt/NPUB35033417/30-11-2017
12.12.2017
Nødnettselskap avviser at de la til rette for spionasje
https://www.nrk.no/norge/avviser-at-de-la-til-rette-for-spionasje-1.13820832
Samling av nettsaker under tema: Utflagging av IT
https://www.nrk.no/emne/utflagging-av-it-arbeidsplasser-1.12941470