Da kriminelle tok 15.000 innbyggere som gisler og sendte kommunen 30 år tilbake i tid.

DATA-ANGREPET MOT ØSTRE TOTEN

Dette er historien om hvordan Oppland Arbeiderblad arbeidet med det alvorligste dataangrepet som har rammet en norsk kommune.

Metoderapport
Oppland Arbeiderblad

Nominasjon til SKUP-PRISEN 2022

Prosjektnavn: Data-angrepet på Østre Toten

Innsendere:

Sæmund Moshagen

Espen Amundrud Solhaug

Erik H. Sønstelie

Publisert i Oppland Arbeiderblad og Toten Idag fra 9. januar 2021. Arbeidet har fortsatt inn i 2022.

Kontakt:

Erik H. Sønstelie

Oppland Arbeiderblad AS

Øvre Torvgate 26

2815 Gjøvik

E-post: erik.sonstelie@amedia.no

Telefon: 905489877

Takk til:

Tor Arne Brekne, Mina Th. Watz, Trude Dale, Alexander Ranum Nilsen, Hege Lockert, Erik Børresen, Stina Håkensbakken, Belinda Rudshagen Jørdandli, Kjetil Lysengen, Henning Raae Fosslien, Trine Rognli og resten av staben i Oa og i Toten I dag som har bidratt.

Coverbilde: Montasje av fotos fra Oppland Arbeiderblad og NTB/AP.

1.0 Innledning

OA vil nominere sakskomplekset **“dataangrepet på Østre Toten”**, med 80 artikler, podkaster og videoer om det som til nå er det alvorligste hacker-angrepet noen norsk kommune er blitt utsatt for.

Som lokal- og regionavis for Vestoppland og Innlandet har OA rapportert om det som skjedde, om konsekvensene for kommune, folk flest og for næringslivet. OA har underveis i dekningen fått frem nye og egne uavhengige opplysninger om dataangrepet ved hjelp av systematisk bruk av ulike kilder, strukturerte postjournal-søk og ny teknologi som gjorde at avisen kunne bevege seg på det mørke nettet uten å bli sporet.

Nesten alle avisens reportere har vært involvert, men det er Espen Solhaug, Sæmund Moshagen og ansvarlig redaktør Erik H. Sønstelie som har fulgt saken tettest over tid. To av de sakene som har vært mest lest eller snakket om, har vært artiklene**, “Protect your data, amigo”** og **“De slapp data om henne på det mørke nette**t. Sistnevnte artikkel ga en på publiseringstidspunktet unik oversikt over hva slags sensitivt materiale som de kriminelle publiserte om kommunen og dens innbyggere rett før påskehøytiden i 2021. Kommunestyret og innbyggerne i Østre Toten fikk først vel en uke senere en nærmere orientering om de sensitive dataene den kriminelle banden Pysa hadde lekket ut på internett..

Her er en **presentasjon** som kort presenterer prosjektet og dens viktigste problemstillinger.

2.0 Metode

2.1 Hvordan arbeidet kom i gang

Tipset var et resultat av ordinær kildepleie.

Journalist Sæmund Moshagen har hatt ansvar for å dekke Østre Toten i mange år. Denne dagen hadde han fri. Heldigvis ble han oppringt. Litt før kl. 14.30 lørdag 9. januar fikk han vite at kommunen hadde blitt hacket. En pressemelding ville snart komme.

Moshagen både sendte melding og ringte inn til nyhetsdesken. Der fikk nyhetsjeger Tor Arne Brekne og frontsjef Mina Th. Watz snart bekreftet nyheten. Frontsjef Watz fikk ut første sak, satte Tor Arne Brekne og Trude Dale på å finne ut mer - og kontaktet deretter redaktør.

Snart kom flere opplysninger frem. Natt til lørdag 9. januar hadde ukjente, avanserte data-kaprere slått til mot Østre Toten kommune, deres 1300 ansatte og 14821

innbyggere. De hadde kryptert 250 datasystemer. En rekke av kommunens tjenester var lammet eller sterkt berørt. Politi og Nasjonal Sikkerhetsmyndighet var varslet , Det var også satt krisestab. De kriminelle hadde framsatt krav.

2.2 Hvordan arbeidet utviklet seg og ble organisert

OA er ingen stor avis. Som for andre norske lokal og regionaviser er arbeidspresset stort og ressursene begrenset. Men i første fase, helgen da angrepet rammet kommunen, arbeidet frontsjef, nyhetsjeger og en reporter tett og hardt med saken. De utgjorde over 50 prosent av helgebemanningen, sportsvakten inkludert.

Siden det er var få ekstra ressurser tilgjengelig, og sykdom, engasjerte derfor ansvarlig redaktør seg i saken lørdag ettermiddag og kveld. Hans fokus var å gjøre det de andre ikke rakk over. Etter hvert fokuserte han på hvem som kunne stå bak, hva slags spor som fantes og hva som kunne komme til å skje videre. Det gjorde at vi allerede samme helg kunne avsløre hvor myndighetenes spor gikk – mot den internasjonale IT-banden Pysa.

Etter helgen, mandag 11. april, ble det videre arbeidet organisert.

I et eget Google Meet-møte - på grunn av pandemien - ble det bestemt å sette to reportere på å følge opp saken, en fra datteravisen Toten I dag, og en fra hovedredaksjonen med ansvar for Østre Toten kommune i det daglige. Espen Solhaug skulle ta kommunen og konsekvensene lokalt og mot nabokommunene. Sæmund Moshagen skulle arbeide mot politi, sikkerhetsmyndigheter og cyber-miljøene i regionen. Siden ansvarlig redaktør satt med spesielle kilder, og hadde søkt opp opplysninger på det åpne nettet om tidligere angrep den mistenkte banden sto bak, fokuserte han på å forberede en større sak med planlagt publisering senere i uken eller mot helgen. Den som ledet teamet og arbeidet med saken, var nyhetsredaktør. Selv om alle arbeidet med saken, betød det at alle også måtte ta andre oppgaver innimellom.

Man hadde i helgen opprettet en egen chat-kanal for de som arbeidet med dataangrepet. Denne kommunikasjonskanalen ble videreført. For øvrig drøftet man ideer og videre framdrift på morgenmøtet. Det ble også besluttet, slik vi gjør det ved større hendelser og ved gravesaker, å opprette en såkalt saksjournal, en Google Drive-mappe der hver sak, hvert prosjekt, har sin «egen journal». Den er organisert etter en bestemt mal. I mappen logger man alt hva man gjør, samler notater, dokumenter, bilder og deler informasjon. Dette letter arbeidet, dokumenterer det som behøves hvis det blir spørsmål eller strid sene - og en slik mappe er god å ha når man skal lage større nyhetsdokumentarer om en sak som har stor interesse og går over tid.

Den samme organiseringen har vært bevart gjennom prosjektet og til dags dato. For øvrig har store deler av redaksjonen vært involvert i dekningen på en eller annen måte underveis.

Toten I dag og Oppland Arbeiderblad har en redaksjon på 29 redaksjonelle medarbeidere, ledelsen inkludert. Redaksjonen er delt inn i en nyhetsdesk og en dagsorden-avdeling. Mindre, løpende nyhetssaker i forbindelse med dataangrepet er derfor løst av den daglig operative nyhetsdesken. Enkelt-reportasjer har vært overlatt til OAs datteravis Toten I dag, som OA deler stoff med.

2.3 Betydningen av strukturert innsynsynsarbeid

Som en mellomstor lokal- og regionavis har OA og Toten I dag gode systemer på journalsøk og innsyns-arbeid.

Det er aviser som våre helt avhengig av. Mange saker starter som følge av overvåking av postjournalene. Men både det digitale postmottaket, journalsystemet og arkivet, ble lammet av angrepet i Østre Toten. Det rammet formannskap og kommunestyre. Men det rammet også våre reportere.

Vi fikk nytte av innsynsarbeid på statsforvalternivå, fylkesnivå og andre offentlige etater underlag einnsyn. Men det er andre sider enn strukturert innsynsarbeid og overvåking av postjournaler, som har vært viktig for OA i denne saken.

2.4 Verdien av kildepleie og oppfølging

Kildepleie gir alltid resultater. Det ga oss tipset. Det ga oss også saker gjennom resten av prosjektet. I arbeidet kom det til nytte at vi hadde erfarne reportere med stort kildenettverk på saken.

Slik fikk vi raskt frem historien at hjemmetjenestens svarte Ipad-er ikke fungerte etter angrepet. Nå måtte de huske hva pasientene skulle ha av medisiner eller kontakte lege. – Det er som å bli kastet 30 år tilbake i fortiden, sa en av hjemmesykepleierne, tidligere ordfører Guri Bråthen.

Deretter skrev vi om at det i hele kommunen ble kjøpt inn penn, papir og ringpermer. Nå måtte mye arbeid gjøres manuelt, arbeid som normalt tok sekunder, tok nå timer eller dager. Overtidstimene eksploderte. Innleie av vikarer og konsulenter gikk i været. En telefaksmaskin noen fant i kjelleren, ble hentet fram med jubel og tatt i

bruk igjen. Man oppdaget at svar fra sykehusene på pasientprøver ikke kom frem slik de skulle. En stund måtte det gås manuelle brannvakter ved offentlige bygg. Feierne visste ikke hvilke piper de skulle feie. Kommunen klarte ikke å betale regningene sine innen frist. Inkassokravene bygget seg opp. Utsendelsen av eiendomsskatten måtte utsettes. Brev måtte sendes innbyggerne om å huske å sette av nok penger til betaling av avgifter når kommunens systemer var oppe igjen. NAV-brukere måtte søke om støtte på nytt eller fortelle hvor mye de normalt fikk utbetalt. Byggesaker som innbyggere og næringsliv hadde inne, stanset opp. Det samme med mange andre prosesser kommunen var involvert i.

Ved hjelp av godt kildenettverk, og fordi vi fulgte diverse møter på ulike nivå i kommunen, fikk vi stadig nye saker. Som nyheten om uro i de tillitsvalgtes rekker da det ble snakk om å gå gjennom alle ansattes e-poster. Om uro blant de folkevalgte da ledelsen ville legge ned arbeidsplassene i IKT-avdelingen og kjøpe tjenesten utenfra. Om uenighet da det ble spørsmål om kommunen skulle melde seg inn i Nasjonalt senter for informasjonssikkerhet i kommunesektoren.

2.5 Bruk av lukkede kilder

Lukkede kilder for å få bakgrunn og forstå konteksten rundt et sakskompleks man som journalist skal dekke, er viktig, tidvis avgjørende. Det har det vært også i dette arbeidet. Kontakt med kilder som har kompetanse eller arbeider med datasikkerhet kunne i denne saken flere ganger gi OA innsikt og av og til helt avgjørende stikkord - innenfor rammen av kilders taushetsplikt. Det skjedde første kvelden etter angrepet. Ved å lytte godt, se på notatene, og sette de enkelte opplysningene etter en omfattende runde med samtaler på ulike kanaler, sammen som i et puslespill, kunne avisens medarbeider søke seg frem på internett og finne data som bekreftet «hintene». Vi fikk lære at kryptoprogram har kjennetegn, at skadevaren som var brukt i Østre Toten trolig hadde vært brukt i Storbritannia og Frankrike. At banden bak hadde lekket opplysninger ut på nettet nylig. Med det som hjelp fant vi etterhvert gjennom nye søk og samtaler hvilket miljø politi og sikkerhetsmyndigheter mistenkte sto bak angrepet. Alle spor pekte mot det kriminelle nettverket kalt Pysa. Et angrep fra oktober 2020 lammet fortsatt bydelen Hackney i London. Bare dager før angrepet på Østre Toten 9.januar 2021 hadde britisk presse skrevet at sensitive data etter angrepet nå var sluppet ut på nettet. Nettsteder som spesialiserte seg på datasikkerhet og hacking, kunne også fortelle om andre angrep. Vi fant en rapport som det nasjonale senteret for informasjonssikkerhet i Frankrike hadde laget etter angrep i Sør-Frankrike. Disse opplysningene, gjorde at vi snart kunne lage en større nyhetsdokumentar om angrepet og det kriminelle nettverket Pysa man mistenkte sto bak.

Verdien av å bygge tillit og arbeide opp et kildenett går aldri av moten. I en tid hvor e-post, SMS og digital kommunikasjon i stadig større grad preger journalistikkens hverdag, kan det være grunn til å minne om at det er gjennom møter og fysisk samtale mennesker i mellom at tillit oppstår lettest og best. Dette gir også rammene for å lage best mulig journalistikk. Det finnes ofte et rom i saker med stort hemmelighold hvor noen opplysninger kan gis i en samtale, og uten at taushetsplikt brytes – som i sum kan gi deg viktige svar for komme videre.

2.5. Bruk av teknologi for å søke og overvåke det mørke nettet:

Vi hadde fått opplyst at løsepengevirus-aktøren etter all sannsynlighet kom til å slippe data ut på nettet om kravet om løsepenger ikke ble betalt. For en norsk kommune er det selvsagt umulig å betale penger til kriminelle. Norske politikere kan ikke understøtte organisert kriminalitet, bidra til hvitvasking av penger og fore et voksende beist av et samfunnsproblem.

Derfor kom snart spørsmålet. Kan OA og Toten I dag finne gruppens portal og overvåke denne, være der når dataene slippes, for så å kontrollere hva slags data som legges ut og likeså hva kommunen forteller befolkningen? Vi mente at saken hadde offentlighetens interesse, at det også kunne bidra til å øke kunnskapen og årvåkenheten til innbyggerne når de visste hva som ble lekket.

Noen av oss som arbeidet med dataangrepet, har tidligere i andre aviser fått mulighet til å drive undersøkende journalistikk og også lære litt om hvordan man kan arbeide på det mørke nettet. For det er på det såkalte «mørke nettet» at løsepengevirus-nettverkene gjerne slipper dataene de har stjålet fra sine ofre. Vi tok derfor snart kontakt med Amedia support og Amedia Teknologi for å få bistand. Vi forstod at dette ikke kunne være noe soloprosjekt hvor en norsk lokalavis trampet ut i et mørkt univers med kriminelle, spioner, politi og andre krefter. Vi ville rapportere hva vi ønsket å gjøre, slik at vi kunne gjøre det på en forsvarlig måte og ikke kompromittere hverken oss selv, mediehuset eller konsernet avisene våre er en del av. Med rask og effektiv hjelp av Amedia sentralt fikk vi overlevert en helt ny datamaskin (uten forhistorie). Den var utrustet med eget trådløst nettverk. Vi ønsket også en egen VPN-beskyttelse og kryptert nettleser. Med denne maskinen kunne OA surfe anonymt og uidentifiserbart på nettet - uten å kompromittere verken Amedia eller oss selv.

Vi samlet inn alt av opplysninger om løsepengevirus, trusselaktører - og spesielt om skadevaren Pysa og det kriminelle syndikatet som brukte denne programvaren. Vi søkte i sosiale medie-kanaler, i diverse forum og på møteplasser for hackere, dataeksperter og andre interessert i hacking for å finne portalen deres.

Det vi jaktet på var hvor på det mørke nettet portalen, Pysas «leak site», var.

Via et omdiskutert forum, men som kort tid senere ble stengt ned, fikk vi tak i en adresse som skulle angivelig gå til portalen hvor Pysa lekker dokumenter og "shamer" sine "partnere". Det var rett adresse. Men portalen forsvant, lenken «døde». Da andre «hackerinteresserte» også etterlyste den på nettet, laget vi en sak på det og at Europol nylig hadde slått til mot et annet syndikat i Ukraina. Så mistet vi litt motet. Nye nyheter dukket opp. Det krevde oppmerksomhet. Heldigvis var det nok av andre saker å skrive om i kjølvannet av dataangrepet.

Da alarmen gikk, og vi fikk forlydender om at Pysa hadde lekket data fra Østre Toten (i ettertid vet vi at det det var FBI som varslet norsk politi) fra en helt ny adresse, satte vi i gang på nytt. Vi gjorde et nytt intenst forsøk på å finne den nye adressen til gruppen. Endelig lyktes vi: I en tråd i et nytt hackerforum fant vi 30. mars endelig den nye adressen. Utstyrt med den lange raden med sifre, som vi hadde funnet og tatt bilde av, kom vi rett til "hoveddøren til banden". Litt senere fant vi også mappen med dataene fra Østre Toten. Mellom en lang rekke kjente og ukjente navn på universiteter, bedrifter, organisasjoner og internasjonale konsern fant vi også en mappe merket «Østre Toten Voksenopplæring.»

Der lå alt Pysa hadde sluppet på nettet fra data-angrepet 9. januar.

3.6 Bruk av excel/visuell grafikk og video og lyd som dokumentasjon

Vi så av overskriftene at det kunne dreie seg om både «uskyldig» og mer sensitivt materiale i mappen. Det var filnavn som handlet om 110-logger, oppfølgingssamtale-rapporter, beredskapsplaner mm. Før vi avsluttet arbeidet for natten, lagde vi en kort video hvor vi fortalte om saken. Den laget vi med mobiltelefon. Den var tenkt å legges ved nyhetsartikkelen når den var klar. Vi ville først få inn kommentarer fra personer og bedrifter vi hadde funnet og kommunen. Vi ønsket også å snakke med politiet. Tidlig om morgenen ble to reportere satt i verk med dette, Men i samtale på tidlig formiddag med kommunedirektøren i Østre Toten, fortalte han at kommunen var i ferd med å sende ut en pressemelding, Midt i denne samtalen sendte redaktøren redaksjonen beskjed om å få ut videoen som ble laget på natten. Dermed publiserte OA og Toten Idag først. En times tid senere hadde vi klar teksten og kunne også publisere artikkelen om OAs funn. Da var også pressemeldingen fra kommunen kommet.

Påsken var i gang. Hytteferien til redaktøren måtte avbrytes da ektefellen ble beordret på jobb på intensivavdelingen på sykehuset. Dermed ble det god tid til å drive journalistikk. Det ga resultater. Vi gjennomgikk materialet som hadde blitt

sluppet på nettstedet til Pysa. Vi lagde først et excel-ark hvor vi kopierte inn alle filnavnene. Deretter sorterte vi materialet og kategoriserte det. Vi mente at vi ved å gjøre dette kunne danne oss et bilde av hva slags materiale som var sluppet ut, hvor mye det dreide seg om, og at vi dermed kunne gi leserne et godt overblikk over innholdet og omfanget, Materialet omsatte vi i grafikk - ved hjelp av Datawrapper. Dette viste at Pysa bare hadde publisert en liten del av materialet de hadde tatt ut av datasystemene til Østre Toten. Det betød at det kunne bli sluppet mer. Med andre ord: De hadde fortsatt pressmidler mot kommunen,

En del av filnavnene var det umulig å lese innholdet ut av. Derfor startet vi med de filnavnene som ga åpenbare stikkord til oss. Vi fant alle konkrete personer og bedrifter nevnt i filnavnene. Vi sorterte ut filnavn som syntes sensitive – som 110-logger og beredskapsplaner. Målet var å lage en større nyhetsdokumentar som kunne ligge ute i påsken. I sum ble dette OAs “påskekrim” i 2021. Saken ble låst på fronten gjennom påsken og ble både godt lest og solgte abonnement. Vi hadde dessuten noen måneder før gjort et upublisert intervju med en sikkerhetsekspert vi hadde hatt kontakt med tidligere. Intervjuet ble lagt inn i rulleteksten etter at sikkerhetseksperten hadde godkjent sine sitater. Dermed kunne intervjuet berike saken og heve den kvalitetsmessig.

3.0 Spesielle problemstillinger

Ovenfor har vi beskrevet problemstillingen med å gå på det mørke nettet uten å stå i fare for å kompromittere deg selv, mediehuset og konsernet.

Men saken reiste også andre problemstillinger for oss:

3.1 Juss og etikk ved nedlasting av stjålne data

Redaktøren mente at - ut fra det han hadde lest og ut fra egen kunnskap - ikke ville være ulovlig å orientere seg i hva det kaprede materialet inneholdt.

Men å laste ned selve filene ville han likevel gå en ekstra runde på.

En ting var hvorvidt det var lovlig å publisere det stjålne materialet. Selv om man agerte som journalist med et samfunnsoppdrag, burde det gås en ekstra runde, mente han. Et annet spørsmål han var opptatt av, var det presseetiske i at OA publiserte materialet. Ville OA bli angrepet for å bli en aktør i hendelsen? I så fall med hvilken rette? Bidro vi til å øke presset på kommunen eller prisen på materialet om vi publiserte deler av innholdet? Dessuten fryktet han at en nedlasting av det

stjålne materialet også kunne potensielt innebære en risiko for at det kom farlige skadevare eller virus i vårt eget datasystem.

Dette måtte avklares.

Vi søkte på nettet, og fulgte oppfordringen som ofte gis på SKUP-konferanser og andre steder, om å lese metoderapporter. Vi tok kontakt med tidligere Adresseavisen og nå E24-reporter Jonas Alsaker Vikan, som er prisbelønnet for sitt arbeid på det mørke nettet. Han ga oss nyttige tips og råd. Vi innhentet kommentarer fra presseetikk-eksperter både i og utenfor konsernet. I tillegg fikk redaktøren hentet inn en rask juridisk vurdering. På bakgrunn av dette konkluderte vi med at det var "innenfor" å laste ned alt materialet når det er gjort som en del av en “journalistisk virksomhet for å avdekke lovbrudd av samfunnsviktig betydning”.

Vi fikk også avklart at det neppe var farlig å laste ned materialet.

Pysa-portalen var der for å bli lest. Det var forretningsideen. Det var pressmiddelet. Dermed kunne vi se bort fra at det var skadevare i filene vi lastet ned, Dessuten var det neppe farlig med det spesialtilpassede utstyret vi brukte for å laste ned materialet, fikk vi opplyst fra fagfolk vi stolte på.

3.2 Kildevern

I det nedlastede materialet lå det mengder med stjålne data, sensitive opplysninger, materiale som ikke skal på avveie.

Derfor var det også en problemstilling før vi lastet ned selve materialet, hvordan vi skulle oppbevare det for å gjøre det trygt, sikkert og ikke komme på kant med lover og forskrifter.

Dersom du som journalist ikke tar vare på stjålet materiale du har fått i egenskap av rollen din på på en sikker måte, og står i fare for å spre sensitive data, kan du bli straffet for det. Slik er loven kort fortalt. Det endte med at vi lastet materialet ned på en ekstern disk, som vi krypterte, og låste inn et sted ingen uvedkommende har tilgang. Bare en person i mediehuset har tilgang.

Da vi lastet ned alle filene - og så nærmere på hva som skjulte seg bak overskriftene, kom det alvorlige i lekkasjene frem. Her var det data om mennesker som i visse tilfeller var livsfarlige for enkeltindivider om de kom i feil hender. Det var

personsensitive opplysninger om en rekke mennesker, deriblant barn og unge, asylsøkere og flyktninger.

Det ble til nye artikler rett etter påske.

Vi valgte ikke å gå i detalj, men mer generelt beskrive innholdet, for ikke å sette andres liv i fare, røpe noens identitet eller på annen måte begå presseetiske lovbrudd. Trolig kunne vi, om vi hadde hatt flere ressurser, funnet måter som vi presseetisk kunne gått inn i dette materialet på og gjennom enkeltmenneskers historier, bedre belyst alvorligheten i det. Dessverre fant vi ikke det mulig slik situasjonen var.

OAs artikler kom før KPMG og kommunen orienterte de folkevalgte i Østre Toten og ga kommunen sin endelige rapport. KPMGs rapport var selvsagt av et helt annet kaliber enn OAs rapporter. Men ved å ha funnet materialet, gått inn i det, og funnet en måte å omtale det på, mener vi at vi samtidig med vår rapportering klarte å gi et uavhengig og forsøksvis balansert bilde av lekkasjene, lekkasjer som kommunens ledelse risikerte å bli straffet for i ettertid. Dette var vi også i kontakt med Datatilsynet om i påsken, for øvrig, Datatilsynets direktør hadde avbrutt ferien sin for å ta et møte med kommunen.

Opplysningene vi hentet frem, mener vi viser hvor alvorlig det kan være om ikke en kommune klarer å ta vare på de mange og ytterst personlige opplysningene man har om innbyggerne sine. Ettertiden har vist oss at personlige data om samtlige 14.821 innbyggere i Østre Toten ble kompromittert under angrepet. Kommunen mener at det ikke ble lastet ned data om alle, men Datatilsynet skriver at data om alle innbyggere ble kompromittert og at ingen vet i hvilken grad opplysninger er på avveie.

Kommunens ledelse har ifølge Datatilsynet utvist «grov uaktsomhet» før dataangrepet. Kommunen har fått et ovetredelsesgebyr på 4 millioner kroner. Det er den største boten noen norsk kommune er gitt av Datatilsynet. I summen er det hensyntatt at kommunens økonomi før angrepet var anstrengt, at dataangrepet har kostet mye og at kommunen og kommunens ledelse har gjort en god jobb etter angrepet.

3.3. Falske e-post-konti og kjøp av programvare

Siden vi ikke hadde drevet journalistikk på det mørke nettet før, hadde vi frykt for det meste - også for maskinen vi arbeidet på.

Vi stolte ikke helt på at ikke IT-kriminelle kunne spore oss hvis vi la igjen personlige opplysninger på den.

Men for å lese dataene vi hentet ned, måtte vi installerer programvare. Siden den ikke måtte spores til OA eller Amedia, opprettet vi en «falsk» hotmail-konto og alt gikk greit fram til vi måtte oppgi personlige data for å få kjøpt windows office, Adobe osv. Det endte med at vi kjøpte programvare privat med et lite brukt kredittkort, som vi kunne stenge senere. Hva mer IT- og sikkerhetsfaglige dyktige journalistkolleger eller eksperter mener om vår frykt og våre tiltak, har vi ikke sjekket nærmere.

3.4 Redaktørens rolle

Det finnes flere grunner til at en ansvarlig redaktør skal holde avstand til det operative.

Det å ha et kaldt hode som skal kunne se en sak fra et annet sted enn de som står midt i den, er et viktig argument for at redaktør skal være forsiktig med involvere seg i det konkrete journalistiske arbeidet.I en mindre avis med mindre ressurser enn i de større regionale og nasjonale redaksjonene, lar ikke dette seg ikke alltid gjøre. Også redaktøren må av og til trå til når det brenner på dekk. Derfor ser man heller ikke sjelden at skrivende redaktører i mindre medier involverer seg.

For Oppland Arbeiderblad i denne saken var det viktig at redaktøren var klar over fallgruvene som kan ligge i å gå ned i det operative. Det finnes ferske saker fra bransjen som har vist farene ved å bli for operativ. Men det var også viktig at man i OA har en ledergruppe som er klar over utfordringene og hvor det er trygt å si ifra dersom man ser det oppstår problemer. I denne saken hadde nyhetsredaktør, utviklingsredaktør og debattredaktør et ansvar for å lede nyhetsarbeidet med saken. Ansvarlig redaktør hadde en teknisk og digital kunnskap som gjorde det var riktig og viktig at han gikk inn i saken. Han hadde arbeidet med datasikkerhet i Schibsted. Han hadde også arbeidet i flere år i VG med undersøkende og gravende journalistikk. Det var en kompetanse som man ikke kunne unngå å bruke aktivt i saken. Dessuten innebar det en praktisk mulighet for å drive kompetanseoverføring i realtid.

3.5 Rapportering, analyser og kommentarer

Med omfanget dataangrep-saken fikk, var det naturlig at det også ble skrevet en rekke ledere og kommentarartikler. I en stor redaksjon skriver ikke reportere ledere og kommentarer. I en mindre avis hender det, som i denne saken, at redaktør også er reporter. Det er heller ikke uproblematisk slik vi ser det når kommentar- og meningsjournalistikk blandes med reporterarbeid i felt. Men det avgjørende for oss som en mindre avis, er at leseren ser når det er snakk om en mening og når det er

snakk om en artikkel. Redaktøren må være tydelig på hva slags hatt han har på. Innholdet må merkes klart slik at skillet mellom reportasje og kommentar kommer fram. Dessuten settes det ekstra krav til journalistikken som utøves. Redaktøren har ikke råd til å gjøre grove feil.

I forbindelse med dataangrepet mot Østre Toten skrev politisk redaktør/debattredaktør alle lederne. Ansvarlig redaktør skrev noen navngitte analyser, men også noen kommentarer med byline, men tydelig merket “kommentar” og utstyrt med ditto vignettering. Etter at sakens alvor viste seg, har redaktøren også sett det som avisens oppgave å bruke avisens arena til å gi et klart varsko. Som tilskuer på først benk til et dataangrep, har Toten I dag og OA sett det som viktig å bruke kunnskapen til å slå alarm og øke bevisstheten i samfunnet om nødvendigheten om å sette et større fokus på datasikkerhet i norsk kommunesektor.

4.0 Kildevalg/kildekritikk

I arbeidet med dataangrepet på Østre Toten har vi søkt å bruke et bredt spekter av kilder – ut fra det som har vært mulig med avisens ressurser. Det vært brukt lokale kilder, regionale og nasjonale kilder, innenfor både politikk, forvaltning, politi og påtalemyndighet, forsvar og IT-sikkerhet.

Det har tidvis vært bruk av lukkede kilder. Opplysningene fra disse er holdt opp mot andre kilder, muntlige som skriftlige. Vi har i tekst og bildeutvalg tatt forbehold der vi mener vi ikke har kunnet dokumentere 100 prosent alle fakta.

I forbindelse med den første større artikkelen om banden Pysa er det henvist til noen nettsteder vi har vært usikre på soliditeten til. Det er noen av de kriminelle syndikatene som skal lage «fake news» på nettet. I disse tilfellene er det opplyst om og tatt forbehold. De er også supplert med andre kilder.

5.0 Konsekvenser

Konsekvensene av vårt fokus på dataangrepet i Østre Toten kommune er at innbyggerne i Vestoppland har blitt holdt oppdatert på hva som rammet dem.

Det er vår hovedoppgave.

Samfunnet kan mer om datasikkerhet og betydningen av det i dag som følge av OAs artikler. Det er også skjedd mange endringer i datasikkerheten i kommunal sektor i

vårt nedslagsfelt. Men det kan ikke OA ta på seg æren for, utover at vi har gitt angrepet i Østre Toten mye oppmerksomhet og i beste fall har medvirket til endringer. Et eksempel viser dette.

Da kommunestyret i Østre Toten holdt på å si nei til å melde seg inn i kommune-CSIRT, Nasjonalt senter for informasjonssikkerhet i kommunesektoren, skrev OA om saken på kommentarplass. Dagen etter hadde politikerne snudd.

For øvrig er bare 43 kommuner med i kommune-CSIRT. Det viser etter vårt syn at mange kommuner fortsatt lukker øynene. Kommune-CSIRT dekker ifølge ledende sikkerhetsaktører i Norge et behov som ingen andre gir norske kommuner.

Som følge av Oppland Arbeiderblads omtale av dataangrepet, ble det i fjor bestemt at temaet skulle komme opp på den største næringslivskonferansen i Innlandet, Mjøskonferansen. Dessverre ble konferansen avlyst på grunn av pandemien. Men OA har også blitt invitert til en rekke konferanser, arrangement og møter for å snakke både om tematikken og om avisens måte å dekke saken på. Lederne og kommentarene til OA er også plukket opp av andre medier, blant annet Nationen, Kommunal Rapport og Digi.no. Etter at avisen ble invitert til å holde foredrag om saken på Data-Skup, har avisen også fått invitasjoner fra andre mediehus til å presentere hvordan vi arbeidet med saken.

OA ble selv, gjennom dataangrepet mot Amedia 28. desember 2021, rammet av dataangrep, Det underbygger etter vårt syn det vi har skrevet gjentatte ganger. Løsepengevirus er blitt en betydelig samfunnstrussel som ut fra et beredskapsperspektiv bør komme langt høyere på dagsorden. Angrepet kunne blitt langt mer alvorlig om ikke Amedia hadde arbeidet så vidt mye med datasikkerhet de siste årene. Når redaktørstyrte aviser rammes av dataangrep, rammes en av hjørnesteinene i vårt demokratiske samfunnssystemet. Ytringsfriheten kan bli satt i fare. Kildevernet risikerer å bli utsatt. I siste instans rammes den enkelte innbygger ved ikke å få uavhengig informasjon om det som hender i samfunnet,

6. Oppsummert

For en kommune er jobb nr. 1 å gi innbyggerne trygghet. Det lyktes ikke Østre Toten med. Det har OAs dekning av dataangrepet på Østre Toten klart vist. Ikke bare har OA kunnet fortelle at samtlige 14.821 innbyggere fikk kompromittert opplysninger om seg, OA har også som øyenvitne kunne rapportere fra slagmarken hva som skjer konkret og på et menneskelig praktisk plan, når all digital infrastruktur i en kommune går ned.

Vi mener vi gjennom dekningen av saken har vært tidlig ute med å rope et varsko til samfunnet om å heve vår bevissthet og vår beredskap på datasikkerhet. Som vi skrev da vi omtalte KPMGs granskingsrapport: Østre Totens datasikkerhet var svært svak. En årsak er at fokuset for kommunene, som mange andre, er digitalisering og

effektivisering. Sikkerhetsaspektet rundt digitaliseringen gis ikke nok fokus. For øvrig skriver sikkerhetsekspertene i granskingsrapporten at man må være oppmerksom på at Østre Totens datasikkerhet ikke skilte seg ut i norsk sammenheng. Kommunens IT-sikkerhet var på et gjennomsnittsnivå i norsk kommunesektor!

Vi håper det kan ligge læring og erfaringer i det arbeidet vi har nedlagt for andre aviser i det vi har gjort, ikke minst for andre lokalaviser-kolleger. Journalistisk overvåking og rapportering fra det mørke nettet tror vi at andre lokale og regionale aviser også vil stifte bekjentskap med etterhvert. Det er også av stor betydning at de store nasjonale mediehus-redaksjonene overvåker det som skjer der. Lederen for Nasjonal Sikkerhetsmyndighet Lene Nystrøm har fastslått at det er en eksplosiv utvikling på det mørke cyber-universet det er all grunn til å advare mot.

7. Vedlegg

Saker sortert etter dato for publisering - kopier tittel/lenke for å få opp saken

Saknr	Mest lest	Tittel (med lenke)	Byline	Publiseringsdato
1	6	https://www.oa.no/5-35-1259083	Tor Arne Brekne	2021-01-09
2	8	https://www.oa.no/5-35-1259156	Tor Arne Brekne	2021-01-09
3	37	https://www.oa.no/5-35-1259181	Mina Therese Watz	2021-01-09
4	3	https://www.oa.no/5-35-1259233	Mina Therese Watz, Hege Locard	2021-01-09
5	17	https://www.oa.no/5-35-1259433	Trine Rognli	2021-01-10
6	22	https://www.oa.no/5-35-1259718	Hege Locard og Erik Sønstelie	2021-01-10
7	29	https://www.oa.no/5-35-1259450	Trude Dale	2021-01-10
8	42	https://www.oa.no/5-35-1259485	Mina Therese Watz	2021-01-10
9	58	https://www.oa.no/5-35-1259636	Erik Sønstelie	2021-01-10
10	65	https://www.oa.no/5-35-1259713		2021-01-10
11	11	https://www.oa.no/5-35-1259802	Erik Sønstelie	2021-01-11
12	14	https://www.oa.no/5-35-1260119	Tor Arne Brekne	2021-01-11
13	51	https://www.oa.no/5-35-1259836	Kjetil Lysengen	2021-01-11

14	53	https://www.oa.no/5-35-1260212	Erik Sønstelie	2021-01-11
15	66	https://www.totenidag.no/5-109-43566	Espen Amundrud Solhaug, Henning Raae Fosslien	2021-01-11
16	67	https://www.totenidag.no/5-109-43560	Espen Amundrud Solhaug	2021-01-11
17	75	https://www.totenidag.no/5-109-43569	Henning Raae Fosslien	2021-01-11
18	1	https://www.oa.no/5-35-1260273	Erik Sønstelie	2021-01-12
19	30	https://www.oa.no/5-35-1260559	Kjetil Lysengen	2021-01-12
20	36	https://www.oa.no/5-35-1260840	Tor Arne Brekne	2021-01-12
21	52	https://www.oa.no/5-35-1260828	Tor Arne Brekne	2021-01-12
22	79	https://www.totenidag.no/5-109-43608	Espen Amundrud Solhaug	2021-01-12
23	84	https://www.totenidag.no/5-109-43661	Espen Amundrud Solhaug, redaktør Toten Idag	2021-01-12
24	26	https://www.oa.no/5-35-1261355	Sæmund Moshagen	2021-01-13
25	73	https://www.totenidag.no/5-109-43756	Tomas Jevne	2021-01-13
26	48	https://www.oa.no/5-35-1262348	Sæmund Moshagen	2021-01-15
27	64	https://www.oa.no/5-35-1262214	Erik Sønstelie	2021-01-15
28	82	https://www.totenidag.no/5-109-43816	Espen Amundrud Solhaug	2021-01-15
29	60	https://www.oa.no/5-35-1263899	Sæmund Moshagen	2021-01-18
30	56	https://www.oa.no/5-35-1265865	Sæmund Moshagen	2021-01-25
31	76	https://www.totenidag.no/5-109-44652	Belinda Jørandli Rudsengen	2021-02-01
32	68	https://www.totenidag.no/5-109-44697	Belinda Jørandli Rudsengen	2021-02-02
33	81	https://www.totenidag.no/5-109-44519	Espen Amundrud Solhaug	2021-02-03
34	74	https://www.totenidag.no/5-109-44853	Belinda Jørandli Rudsengen	2021-02-05
35	9	https://www.oa.no/5-35-1274439	Sæmund Moshagen	2021-02-07
36	40	https://www.oa.no/5-35-1274667	Trine Rognli	2021-02-08
37	55	https://www.oa.no/5-35-1278614	Stina Håkensbakken	2021-02-12
38	61	https://www.oa.no/5-35-1280408	Erik Sønstelie	2021-02-14
39	78	https://www.totenidag.no/5-109-45442	Espen Amundrud Solhaug	2021-02-18
40	13	https://www.oa.no/5-35-1285787	Sæmund Moshagen	2021-02-24

41	34	https://www.oa.no/5-35-1285216	Sæmund Moshagen	2021-02-24
42	38	https://www.oa.no/5-35-1286428	Erik Sønstelie	2021-02-25
43	5	https://www.oa.no/5-35-1286881	Sæmund Moshagen	2021-03-01
44	57	https://www.oa.no/5-35-1296251	Stina Håkensbakken, Erik H. Sønstelie	2021-03-12
45	71	https://www.totenidag.no/5-109-48801	Tor Arne Brekne, Espen Amundrud Solhaug	2021-03-30
46	87	https://www.totenidag.no/5-109-48805	Espen Amundrud Solhaug, Erik Sønstelie	2021-03-30
47	7	https://www.oa.no/5-35-1306053	Erik Sønstelie, Trude Dale	2021-03-31
48	23	https://www.oa.no/5-35-1305491	Erik Sønstelie	2021-03-31
49	24	https://www.oa.no/5-35-1306028	Trude Dale	2021-03-31
50	69	https://www.totenidag.no/5-109-48897	Erik Sønstelie, Brynjar Eidstuen, Espen Amundrud Solhaug	2021-03-31
51	92	https://www.oa.no/5-35-1305567		2021-03-31
52	2	https://www.oa.no/5-35-1306437	Erik Sønstelie	2021-04-02
53	10	https://www.oa.no/5-35-1307332	Erik Sønstelie	2021-04-03
54	25	https://www.oa.no/5-35-1307825	Erik Sønstelie	2021-04-04
55	43	https://www.oa.no/5-35-1308815	Erik Sønstelie	2021-04-07
56	72	https://www.totenidag.no/5-109-48966	Espen Amundrud Solhaug	2021-04-07
57	90	https://www.totenidag.no/5-109-48960	Espen Amundrud Solhaug	2021-04-07
58	15	https://www.oa.no/5-35-1309491	Erik Sønstelie	2021-04-08
59	62	https://www.oa.no/5-35-1309515	Stina Håkensbakken, debattredaktør	2021-04-08
60	59	https://www.totenidag.no/5-109-48969	Espen Amundrud Solhaug	2021-04-09
61	91	https://www.totenidag.no/5-109-49054	Espen Amundrud Solhaug	2021-04-09
62	33	https://www.oa.no/5-35-1310347	Stina Håkensbakken	2021-04-10
63	4	https://www.oa.no/5-35-1312639	Sæmund Moshagen	2021-04-15
64	39	https://www.oa.no/5-35-1320922	Erik Sønstelie	2021-05-02
65	12	https://www.oa.no/5-35-1323283	Sæmund Moshagen	2021-05-05

66	19	https://www.oa.no/5-35-1341085	Sæmund Moshagen	2021-06-09
67	16	https://www.oa.no/5-35-1347765	Henrik Hornnæss	2021-06-23
68	89	https://www.totenidag.no/5-109-48953	Espen Amundrud Solhaug	2021-07-04
69	21	https://www.oa.no/5-35-1388507	Sæmund Moshagen	2021-08-27
70	47	https://www.oa.no/5-35-1388342	Mina Therese Watz	2021-08-27
71	41	https://www.oa.no/5-35-1408188	Sæmund Moshagen	2021-09-29
72	35	https://www.oa.no/5-35-1420284	Erik Sønstelie	2021-10-19
73	70	https://www.totenidag.no/5-109-58039	Henning Raae Fosslien, Hanna Reppen Kvikstad, Kristin Horni, Espen Amundrud Solhaug	2021-10-19
74	80	https://www.totenidag.no/5-109-58100	Espen Amundrud Solhaug, Erik Sønstelie	2021-10-19
75	45	https://www.oa.no/5-35-1420400	Erik Sønstelie, Espen Amundrud Solhaug	2021-10-20
76	44	https://www.oa.no/5-35-1421302	Martin Grime	2021-10-21
77	83	https://www.totenidag.no/5-109-58703	Espen Amundrud Solhaug	2021-10-30
78	85	https://www.totenidag.no/5-109-59081	Espen Amundrud Solhaug	2021-11-05
79	18	https://www.oa.no/5-35-1445991	Martin Grime	2021-12-06
80	46	https://www.oa.no/5-35-1446620	Trude Dale	2021-12-06
81	86	https://www.totenidag.no/5-109-61567	Espen Amundrud Solhaug	2021-12-08
82	20	https://www.oa.no/5-35-1450332	Erik Sønstelie	2021-12-14
83	77	https://www.totenidag.no/5-109-62050	Henning Raae Fosslien	2021-12-17
84	31	https://www.oa.no/5-35-1455777	Hanna Reppen Kvikstad	2021-12-23
85	32	https://www.oa.no/5-35-1458382	Stian Andrè Lund	2021-12-28
86	63	https://www.oa.no/5-35-1458254	Erik Sønstelie	2021-12-28
87	28	https://www.oa.no/5-35-1458921	Erik Børresen	2021-12-29
88	88	https://www.oa.no/5-35-1459079	Bjørn Ivar Bergerud	2021-12-29
89	50	https://www.oa.no/5-35-1461394	Henning Gulbrandsen	2022-01-03
90	27	https://www.oa.no/5-35-1466304	Erik Sønstelie	2022-01-11

Lenker til noen av de mest sentrale sakene.

Den første nyheten

Kriseledelse samler seg, hjelp tilkalles

Den første saken om hvem som kunne stå bak

Den første kommentaren

De første konsekvensene: - Helt surrealistisk

Om hvordan de slo til: Protect your system, Amigo

Flyktninger rammet

Sakkyndige rapporter om enkeltpersoner og deres hjelpebehov

Siste: Fremmed stat kan stå bak

Datatilsynet: Personopplysninger om alle kommunens innbyggere ble kompromittert

Avisenes artikler om dataangrepet er i sin helhet samlet på denne, denne og denne taggen.

OA Podkaster om dataangrepet

OA Podden - Lederen for Nasjonalt senter for IT-sikkerhet i kommune-Norge 15.01-2021

OA Podden - intervju ordføreren og med Kripos-sjefen om dataangrepet 12.2.2021

OA Podden Også Lunner kommune ble forsøkt angrepet 12.3. 2021

OA Podden - Dataangrepet blir dyrt 09.04.2021

To av OA videoer/streams om dataangrepet

Pressekonferansen et døgn etter angrepet 10.01.21

Her er de stjålne dataene fra Østre Data - OA fant de på det mørke nettet 31.03.21

Oslo 17.01.2022 Erik Sønstelie