Koden for sikker datajournalistikk

Norsk Redaktørforenings teknologiskvadron

Høsten 2020

Illustrasjon: Øyvind Hovland

En veileder for redaktører som vil ta ut hele potensialet i journalistikken, men samtidig føle seg trygge på digitalt kildevern og datajournalistikk.

NORSK
REDAKTØRFORENING

Innhold

1 Innledning: Jobb trygt

Teknologi gir fantastiske muligheter for å utvikle journalistikken som fag. Vi kan kommunisere med kilder og publikum hvor som helst i verden. Store datamengder gir oss muligheten til å studere sammenhenger og oppdage kritikkverdige forhold på måter som ikke var mulig tidligere. Presentasjon av databasert journalistikk kan gi helt nye fortellerformer og formidle sammenhenger på måter som gjør det lettere å forstå komplekse spørsmål.

Samtidig gjør teknologi oss sårbare. Det er fort gjort å klikke på en lenke eller åpne et vedlegg vi ikke burde og dermed åpne datasystemene for inntrengere. Vi kan avsløre en hemmelig kildes identitet ved å være sleppehendte med mobilen. Vi kan glemme tofaktor-autentisering som sikrer at de som publiserer innhold på nettstedet vårt, faktisk jobber hos oss.

Redaktørens ansvar, derimot, er uendret. Vær varsom-plakaten pålegger oss å verne om redaksjonens evne til å drive fri, uavhengig journalistikk. Vi skal verne om kildene våre og sikre at upublisert materiale ikke kommer på avveie. Og vi skal vise saklighet og omtanke i alle deler av den journalistiske arbeidsprosessen.

Det er vi redaktører som har ansvar for å lage en god sikkerhetskultur. Ingen systemer eller teknologiske løsninger gjør oss hundre prosent trygge. Vi er avhengig av menneskene som opererer systemene. Det første steget for å få på plass en sikkerhetskultur er å erkjenne at alle kan bli rammet av en hendelse – enten det er datainnbrudd eller en kilde som blir avslørt på grunn av ubevisst bruk av digitale verktøy.

Den enkeltes kunnskap, adferd og holdninger til informasjonssikkerhet er en del av sikkerhetskulturen. Digital sikkerhet er ikke noe som kan løses av en IT-ansvarlig alene, men av alle som håndterer informasjon i et mediehus og alle som har tilgang til mediehusets digitale løsninger og infrastruktur.

Kunnskap og bevisstgjøring er bærebjelker i en god sikkerhetskultur. Gjør digital sikkerhet til et tema for redaksjonen, i ledermøter, på allmøter, på intranettet og i annen kommunikasjon ut til hele organisasjonen. Lag gjerne interne, konkrete kjøreregler rundt passordbruk, mobilbruk eller kildekontakt og gi dette oppmerksomhet.

Vær nysgjerrig og spør om hvordan reportere og mellomledere lagrer informasjon eller hvordan de bruker mobiltelefonen i ulike situasjoner. En god sikkerhetskultur handler ikke bare om å beskytte sensitiv informasjon i store journalistiske prosjekter, men ofte om helt alminnelige problemstillinger som bruk av mobil og e-post i kontakt med kilder som har krav på kildevern.

Vi må vite nok om teknologiens muligheter og begrensninger til å gi gode råd og ta smarte valg. Det er utgangspunktet for denne veilederen. Forhåpentligvis kan vi avmystifisere teknologi og datajournalistikk litt, og vise at det å lede vei gjennom nye redaksjonelle utfordringer faktisk ikke krever doktorgrad i kunstig intelligens. Det krever bare at vi tenker litt, og at vi allierer oss med gode hjelpere på IT-siden der vår egen kunnskap setter begrensninger.

Men å etablere en god sikkerhetskultur fordrer at vi redaktører går foran. Vi må gjøre sikkerhet og sjekklister til noe vi lever etter og praktiserer i det daglige, ikke redusere det til et policy-dokument vi kun tar fram når noe har gått galt. Redaktøren må stille spørsmål, sikre at redaksjonen har den riktige kompetansen og kunnskapen til å ta gode valg, og unngå å selv gjøre alvorlige blundere som setter kildevern eller sikkerhet på unødvendig sterke prøver.

Åpenhet er viktig - også når det gjelder sikkerhet rundt journalistikken. Det betyr selvsagt ikke at vi skal avsløre kildene våre og dele informasjon som gjør oss sårbare for datainnbrudd. Men det er viktig at vi informerer potensielle kilder om trygge måter å ta kontakt med oss på og viser at vi tar sikkerhet på alvor. Vi må også begrense antall personer i redaksjonen som har tilgang til dataene i de mest sensitive sakene, men overdrevent hemmelighold rundt konkrete prosjekter kan også skade arbeidsmiljøet internt.

Denne veilederen er et bidrag til alle som vil komme igang med tryggere rutiner når det gjelder datajournalistikk og kildevern. Vi håper den både kan hjelpe redaktører som trenger starthjelp og de som bare vil sjekke av om rutinene de allerede har etablert er gode nok. Veilederen er utarbeidet av redaktørforeningens teknologiskvadron som i dette prosjektet, i tillegg til redaktører, også er utvidet med dyktige IT-folk i flere mediehus. Målet er at veilederen skal være dynamisk og at særlig oversikten over verktøy skal oppdateres jevnlig.

Ta kontakt på rkn@nored.no dersom du har forslag til endringer. Tusen takk til alle dere som har bidratt underveis til dette dugnadsprosjektet!

Veilederen er utarbeidet av:

Ingeborg Volan	*Dagens Næringsliv*
Espen Andersen	*Kommunal Rapport*
Christer S. Johnsen	*Adresseavisen*
Anniken Hjertholm	*TV 2*
Vibeke Reigstad	*TV 2*
Faste Dyrnes	*Adresseavisen*
Gaute Mjøen	*NHST*
Marius Tetlie	*NRK*
Frank Gander	*NRK*
Øyvind Bye Skille	*Faktisk*
Pål Nedregotten	*Amedia*
Øyvind Brenne	*VG*
Arne Jensen	*Norsk Redaktørforening*
Reidun Kjelling Nybø	*Norsk Redaktørforening*

2 Generelt nettvett

Generelle sikkerhetsråd for alle som bruker teknologi i hverdagen:

- Husk at kriminelle som angriper tekniske løsninger i de fleste tilfeller vil måtte lure deg som bruker for å kunne lykkes. Klikk ikke på lenker eller vedlegg du ikke er trygg på. Vær særlig oppmerksom dersom du mottar e-post, SMS og telefoner som prøver å fremkalle følelse av frykt, hastverk eller fristelser.
- Sørg for at din datamaskin og mobil til enhver tid er oppdatert.
- Bruk kun programvare som er nødvendig for å gjennomføre arbeidet, og unngå nedlastning og installasjon av uautorisert programvare.
- Beskytt alltid tilgang til datamaskin og mobiltelefon. Vær spesielt oppmerksom hvis du deler nettverk med andre på samme sted. Unngå bruk av åpne/ukrypterte nett - i mange tilfeller kan mobilnett være tryggere å bruke.
- Unngå bruk av jobb-e-post til brukernavn på private tjenester og omvendt.
- Tenk over hva du deler i sosiale medier. Forvent at alle kan se informasjonen du deler, både om jobb og privatliv.
- Vurder nøye hvilken kanal du benytter ved kildekontakt, kommunikasjon og informasjonsutveksling. Konfidensiell og sensitiv informasjon krever ekstra forsiktighet samt sikkerhetstiltak som kryptering og passordbeskyttelse (se egne råd for håndtering av «skarpe saker» senere i denne veilederen).
- Meld alltid fra til IT-support om mistenkelige hendelser
- Sjekk om din konto kan ha vært utsatt for et databrudd. Bruk f.eks. tjenesten *haveibeenpwned.com*. Et treff her indikerer at noen kan ha informasjon om kontoen din, og at passord du har brukt derfor kan være kjent av uvedkommende. Hvis du får treff: Bytt passord på alle tjenester der det aktuelle brukernavnet/passordet har vært i bruk.

Råd for passord

- Gi aldri fra deg brukerkonto, passord, persondata eller konfidensiell informasjon.
- Velg ulike passord på ulike tjenester og lag lange passord som er vanskelig å gjette for andre. Bruk gjerne setninger eller passordhåndteringsprogrammer som f.eks.1Password eller Lastpass.

- Aktiver alltid to-faktor innlogging dersom mulig. Da vil du ved innlogging benytte noe du har (f.eks. mobil) eller noe du er (f.eks. fingeravtrykk), i tillegg til det du vet (f.eks. et passord).
- Må du ha en huskeliste, skriv ned hint på papir og beskytt dokumentet som et verdipapir.
- Endre alltid oppstarts- og standardpassord på nye produkter og tjenester.

3 Risikonivåer

Upublisert materiale skal sikres mot at utenforstående får tilgang til det ved et uhell eller gjennom datainnbrudd. Hvor omfattende forholdsregler man tar for å unngå det avhenger av materialets natur og antatt risiko ved en eventuell lekkasje.

Litt forenklet kan man si at en feilsendt e-post med sakslisten for neste dags avis antakelig får færre alvorlige konsekvenser enn om det hadde vært svar-e-posten din til en anonym varsler som har risikert mye ved å kontakte deg.

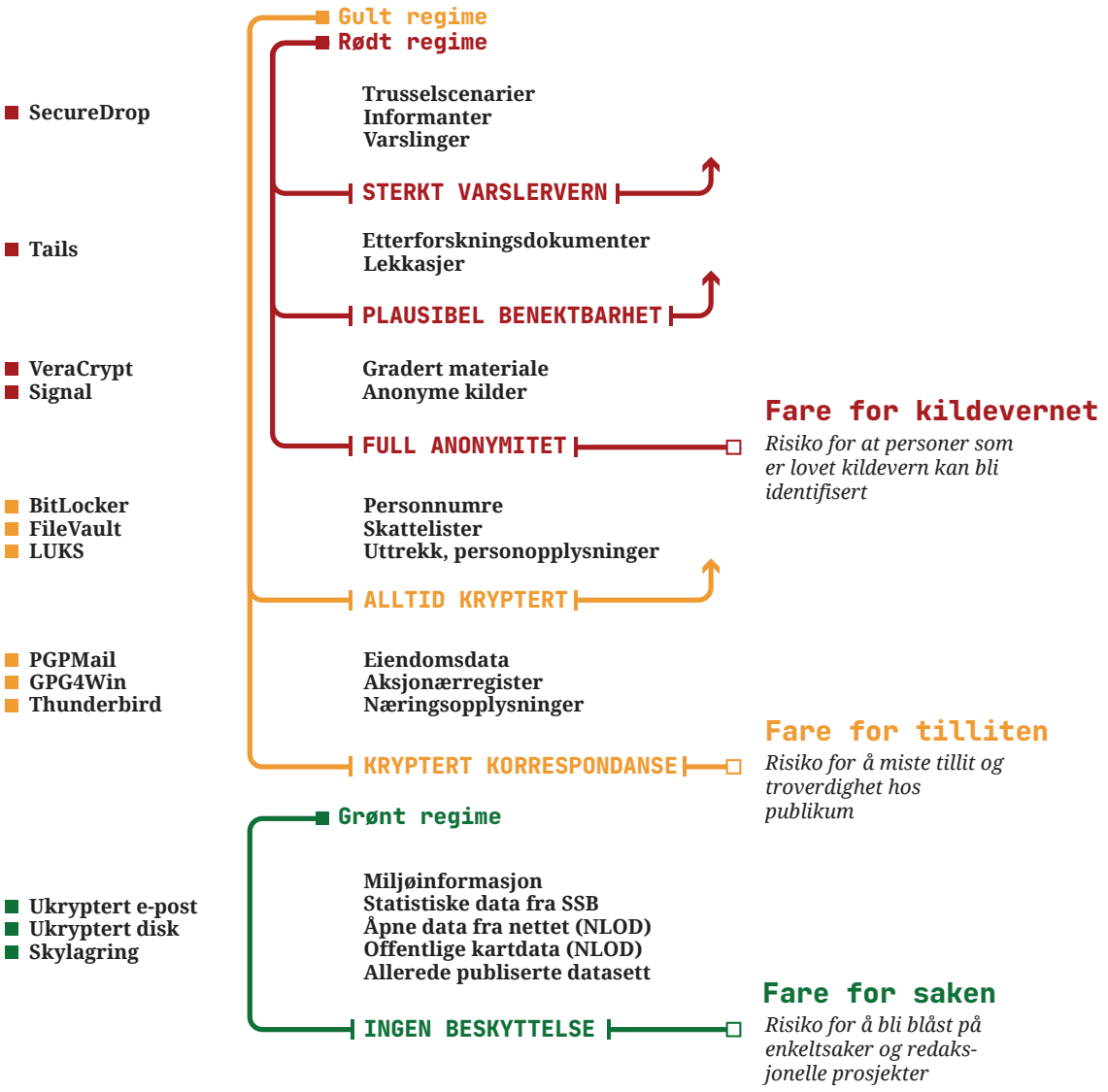
Vi har satt opp tre sikkerhetsnivåer eller *regimer* som gir en pekepinn mot hvilke tiltak som kan være aktuelle for ulike scenarier.

- **Rødt regime** - når en lekkasje av upublisert materiale truer kildevernet, eller setter mennesker i fare.
- **Gult regime** - når en lekkasje av upublisert materiale først og fremst truer tilliten og troverdigheten til pressen, og/eller fører til innstramminger i tilgangen på offentlige data.
- **Grønt regime** - når en lekkasje av upublisert materiale ikke har alvorlige konsekvenser, selv om de eventuelt kan avsløre for utenforstående hvilke redaksjonelle saker som er under arbeid.

Figur 1 er en forenkling. Den gjør en grovinndeling som hverken er uttømmende eller kategorisk. Ingen saker er like. Sikkerheten må alltid vurderes individuelt og fortløpende for hvert prosjekt redaksjonen går i gang med.

Venstre kolonne i figur 1 viser et lite utvalg applikasjoner som typisk er i bruk for å kryptere materiale eller anonymisere kommunikasjon på de ulike nivåene. Det finnes mange andre dataprogrammer som kan brukes til samme formål.

En forsvarlig sikring av upublisert materiale handler likevel om mer enn bare å bruke riktig type sikkerhetsprogramvare. Den avhenger også av at hver medarbeider opptrer konsekvent i sin etterlevelse av sikkerhetrutinene. Redaksjonsledelsens rolle er å skape en dypere forståelse for hvorfor god sikring av visse typer upublisert materiale er nødvendig, og at dette krever høy grad av disiplin.



Figur 1: *Skjematisk fremstilling av hvordan ulike scenarier kan plasseres inn i et av tre sikkerhetsregimer. Kolonnen til venstre gir eksempler på verktøy som kan være relevante for hvert regime.*

3.1 Fare for saken

Grønt regime

Ingen beskyttelse av data utover ordinær pålogging. Statistikk og offentlige data som er tilgjengelig for enhver er eksempler på data som faller inn under grønt regime. Husk at en lekkasje likevel kan ha skadepotensiale, fordi den gir uvedkommende kunnskaper om hvilke redaksjonelle prosjekter som er under arbeid.

Det finnes materiale som er av en slik natur at det ikke er knyttet vesentlig risiko til eventuelle lekkasjer. Dette kan dreie seg om offentlige og allment tilgjengelige datasett — slik som de som fritt kan lastes ned fra *data.norge.no* eller *ssb.no*.

NB! At dokumenter og datasett er offentlige, betyr *ikke* at det automatisk hører inn under grønt regime.

Offentlige datasett kan fortsatt inneholde for eksempel persondata, injurierende og inkriminerende opplysninger og andre saksopplysninger som gjør at datafilene absolutt hører hjemme i gult regime så lenge de ikke er publisert i sammenheng med redaksjonelle prosjekter.

Eksempler på dette er dommer fra domstol.no eller lønnsoversikter fra det offentlige.

Videre skal man være klar over sammenhengen journalistikken vår setter offentlige og "grønne" data inn i. En offentlig liste over byggesaker, lastet ned fra kommunens åpne hjemmesider, kan fort havne i gult regime når vi kobler den mot vernemyndighetenes like offentlige oversikt over fredede og verneverdige bygninger. Derfor kan det hende at en samling datasett bør beskyttes ekstra, selv om hvert enkelt datasett er offentlig og allerede åpent tilgjengelig på nettet.

Husk at enhver datalekkasje — selv de som er ganske "ufarlige" — er skadelig for tilliten til mediene. Publikum kan få inntrykk av at vi slurver med datasikkerheten, og hvordan er det da med kildevernet? Hovedbudskapet er derfor: *Hold deg i gult regime som en hovedregel.*

3.2 Fare for tilliten

Gult regime

E-post kryptert, fulldiskkryptering påskrudd. Som oftest det mest fornuftige nivået å legge seg på for de fleste normale situasjoner. Datasett med offentlige opplysninger som kan knyttes til enkeltpersoner er eksempler på materiale som hører inn under gult regime.

I gult regime legger vi oss på et sikkerhetsnivå som primært retter seg mot å forhindre at upublisert materiale kommer på avveie. Her befatter vi oss mest med *kryptering* og ikke med *anonymisering*.

For de fleste praktiske formål, er dette et fornuftig nivå å legge seg på i det daglige, fordi tilfredsstillende sikkerhet kan oppnås uten for store praktiske ulemper.

Følgende verktøy er relevante for gult regime:

- **Fulldiskkryptering** (BitLocker/FileVault/LUKS) for å sikre alle data på disken *(se side 20)*
- **E-post-kryptering** (PGPMail/GPG4Win/Thunderbird) for å kryptere e-postmeldinger *(se side 19)*

3.3 Fare for kildevernet

Rødt regime

Når kildevernet gjør seg gjeldende, holder det ikke bare å kryptere innholdet i kritisk korrespondanse. Man må man også ta hensyn til behovet for *anonymisering* av selve kommunikasjonen med kilden. Unngå sporbare kanaler som alminnelig e-post og telefon/SMS. Velg anonymiserte kommunikasjonverktøy som *Signal* og anonymiseringsnettverket *Tor*.

Rødt regime er hovedsakelig forbeholdt saker der det kan tenkes at noen aktivt går inn for å finne identiteten til kilder som er lovet anonymitet. I et slikt scenario er ikke kryptering alene tilstrekkelig. Dette gjelder også opplysninger som setter andre mennesker i fare, uavhengig av om de opptrer som kilder eller ikke.

Metadata, som personers navn, IP-adresse, lokasjon, e-postadresse, bruker-id og lignende, må skjules for å avskjære ressurssterke aktører fra å avdekke kilders identitet fra serverlogger eller overvåkningsdata.

De samme verktøyene som er aktuelle for gult regime, er også aktuelle for rødt regime. I tillegg er følgende verktøy viktige:

- **SecureDrop** for sterkt varslervern *(se side 20)*
- **Tails** for å skjule spor *(se side 21)*
- **VeraCrypt** for kryptering av filer og disker *(se side 23)*
- **Signal** for å kommunisere sikkert med kilder *(se side 21)*

4 Digital kildevernplakat

Noe av det viktigste vi gjør i journalistikken er å verne om kilder som gir oss fortrolig informasjon. Dette er en stadig mer krevende oppgave som gjør at vi må ta andre forholdsregler enn tidligere. Her er noen råd og retningslinjer som kan implementeres for et bedre digitalt kildevern i redaksjonen:

- Husk at våre kilder kan bli utsatt for kildejakt fra flere ulike hold. Partnere, arbeidsgiver og politiet kan med enkle grep få innsyn i en kildes telelogg.
- Ved bruk av vanlig telefon og SMS er det mulig for uvedkommende å få oversikt over hvem kilden har hatt kontakt med. Bruk heller apper, som Whatsapp eller Signal. Dette gjør det mye vanskeligere for arbeidsgivere og andre privatpersoner å få innsyn i kommunikasjonen. Vurder å bruke appen Signal i sensitive saker. Signal lagrer i praksis ingen metadata, som gjør det vanskelig selv for statlige aktører å få innsyn i kommunikasjonen. Vurder også å slette innholdet i den elektroniske dialogen med ekstra sensitive kilder fortløpende, dersom dette ikke står i strid med redaksjonens dokumentasjonsbehov.
- Sjekk med den IT-ansvarlige i virksomheten om det er mulig å kryptere pc-en og e-postløsningen for å høyne sikkerheten rundt kildekommunikasjon og upublisert materiale.
- Vær varsom med å følge fortrolige kilder på sosiale medier som Twitter og Facebook, med mindre det en naturlig del av et større kildenettverk.
- Husk at apper kan spore din posisjon, og videreformidle dette til uvedkommende. Vær kritisk når du gir ulike apper tilgang til stedstjenester. I sensitive kildemøter bør du vurdere å legge igjen telefonen hjemme eller på kontoret (men ikke skru den av).
- Sensitivt kildemateriale kan ofte være vannmerket og modifisert på ulike måter som kan avsløre identiteten til kilden. Vær varsom ved publisering av bilder, dokumenter og annet dokumentasjonsmateriale du har fått fra fortrolige kilder.
- Det er ditt ansvar å sørge for at dokumentasjonsmateriale er tilstrekkelig sikret og utilgjengelig for uvedkommende. Snakk med “IT-guruer” i redaksjonen, i virksomheten eller i nettverket ditt, om hvilke krypteringsløsninger som egner seg.
- Det er redaksjonsledelsen som har ansvar for at journalistene i redaksjonen kjenner til kildevernplakaten, og behandler fortrolige kilder i tråd med disse rådene/retningslinjene.

5 Kom trygt i gang!

Sjekkliste til redaktører som vil starte med datajournalistikk

Mange av de viktigste journalistiske sakene de siste årene har kommet gjennom avansert databehandling og analyse - det vi gjerne kaller datajournalistikk. Å systematisere og analysere data ved hjelp av kode er et utrolig nyttig journalistisk verktøy. Det er heller ikke så vanskelig som mange tror.

Men før dere starter med datajournalistikk, er det lurt å tenke gjennom hvilke ressurser og verktøy dere trenger for å overholde Vær Varsom-plakatens bestemmelser om kildevern og beskyttelse av upublisert materiale.

Kildearbeid på nettet er både teknisk,juridisk og etisk litt annerledes enn mer tradisjonelt kildearbeid. En stor del av datajournalistikk handler om å selv innhente informasjon - altså webscraping. Webscraping er kopiering av tekst, bilder, HTML og annen data som finnes på nett, med hensikt å samle informasjon. Det finnes mange metoder for webscraping, både manuelle,automatiske og ved bruk av ulike verktøy.

Det er viktig å huske på at selv om noe er teknisk mulig, må man alltid foreta grundige journalistiske og etiske vurderinger rundt metode, som både inkluderer risikovurdering med tanke på omdømme, redaktøransvar,samt juridiske forhold.

Husk: Det forskjell på å få tilgang til data som andre har skaffet seg ulovlig, og det å selv skaffe seg data ulovlig.

4 faser

Det er fire faser i arbeidet med datajournalistikk du trenger å tenke på. Hver av fasene har sine egne mulige sikkerhetsutfordringer — men ingen av dem er umulige å overkomme.

Et godt samarbeid med IT-avdelingen eller en IT-supportfunksjon kan være nyttig. Hvis bedriften har tilgang til slike ressurspersoner, er det lurt å prate med dem før dere starter med å behandle data journalistisk.

Fase 1: Hvordan skaffer vi data?

Data til journalistisk bearbeidelse kan skaffes på mange måter. Noen prosesser er enkle og ufarlige, f.eks. å koble seg opp mot offentlige API-er som leverer data. Men noen typer datainnhenting kan innebære risiko vi kan prøve å unngå.

- Gjør en kildesjekk av kilden for data. Er det en troverdig kilde, og er det sannsynlig at personen eller institusjonen faktisk har tilgang til de dataene de sier de har?
- Vær særlig forsiktig dersom dere skal laste ned data fra det mørke net-

tet, fra en torrent-lenke eller f.eks. som en zippet fil som kan gjemme andre filer inni seg. Bruk en blank datamaskin som ikke er koblet til det vanlige nettet på jobben hvis du laster ned eller åpner data fra en kilde du er usikker på. Da reduserer du sjansen for at minnepinnen eller kilden kan inneholde skadelig programvare. Skulle noe gå galt, har det bare gått ut over den ene maskinen.

- Hvis noen i journalistisk arbeid skal laste ned hemmelige eller ulovlige data, eller data fra en kilde dere helst ikke vil at skal spore aktiviteten deres av ulike grunner – bruk VPN-tjeneste eller TOR-browser for å anonymisere din nettrafikk overfor kilden.

Fase 2: Hvordan lagrer, systematiserer og analyserer vi data?

Lagring av data – særlig personopplysninger – har en del lovkrav knyttet til seg. Derfor er det viktig å ha et bevisst forhold til hvilke løsninger dere bruker for å lagre og analysere data. I tillegg er det viktig å tenke på kildevern og begrense innsyn til prosjektene fra ikke-journalister og utenforstående.

- Vær sikker på at dere lagrer dataene på en tjeneste som oppbevarer dem godt, at du vet hvor data lagres fysisk og at du har en databehandleravtale hvis dere bruker en tredjepartstjeneste. Hvis mulig, bruk de tjenestene og leverandørene bedriften bruker fra før – da er sannsynligheten høyere for at IT-støtte finnes for det du trenger. Sørg også for god dokumentasjon av oppsettet og for at mer enn én person skjønner hvordan databasen og systemene virker. På den måten sikrer du at dere kan fortsette med datajournalistikk også hvis en nøkkelperson er på ferie.
- Lag interne regler for overføring og kommunikasjon om dataene. Klargjør hvilke løsninger som er godkjente data som er mer sensitive.
- Det er redaktørens ansvar å avgjøre hvem som får titte inn i redaksjonens data. Pass på at redaksjonelle data lagres uavhengig av andre bedriftsdata, og med begrenset innsyn også fra IT-avdelingen. Det kan for eksempel opprettes et eget serverområde for datajournalistiske prosesser der kun noen få IT-folk har innsyn. Ha også nøye kontroll med hvem i redaksjonen som har tilgang, og hvem som kan åpne for tilganger til nye brukere.
- Husk at datalagring koster penger. Hvis du ikke betaler noe for tjenesten, betaler du vanligvis med data. Det anbefales ikke som løsning for datajournalistikk.
- Bruk alltid tjenester som tilbyr identifisering av brukeren med tofaktorautentisering.

- Vurder om arbeidet med dataene i research-fasen innebærer at de er tilgjengelige hele tiden eller ikke. Om de bare trenger å være tilgjengelige når spesifikke personer jobber med dem kan det vurderes å legge dem nedlåst og kryptert (encrypted at rest). Dataene må da låses opp med krypteringsnøkkel/passord hver gang det skal jobbes med dem.
- Vurder å lage mindre sensitive versjoner av datasettene til aktivt arbeid om sensitive deler ikke er nødvendige for undersøkelsene. F.eks. kan det lages en egen ID-nøkkel for unike personer som erstatter fullt fødselsnummer på 11-siffer.
- Hvis dere bruker lokal lagring, og ikke skytjenester, pass på at det er mulig å skalere de løsningene dere velger for lagring dersom dere oppdager at datajournalistikk funker for dere.
- Ikke bruk minnepinner, ekstern harddisk eller egen PC som eneste lagring av datasett. Hvis slike fysiske lagringsenheter skal brukes på noe tidspunkt i den journalistiske arbeidsprosessen, sørg for at enheten beskyttes med kryptering og tilgangskontroll – du vil unngå at det blir skandale hvis noen mister minnepinnen sin.

Fase 3: Trygg presentasjon

Ved publisering gjøres det kjent for hele verden hvilke data redaksjonen har jobbet med. Ta en vurdering av sikkerheten knyttet til både research/bearbeidelse og presentasjon basert på eventuelle trusler etter publisering.

- Hvis data skal brukes direkte i presentasjonen med en database i bakkant, minimer dataene både i databasen og presentasjonen til bare det som faktisk skal offentliggjøres. Husk at data i basen kan bli eksponert selv om de ikke er aktivt vist frem i den redaksjonelle presentasjonen. Vurder også om å gjøre dataene mer unøyaktige er aktuelt.
- Vær oppmerksom på eventuelle muligheter for enumerering av databasene – at teknisk kyndige kan gjette seg fram til større deler av basen ved å lete i nøkler/id-er. Om brukerne ikke skal kunne finne alle dataene sammen kan dere unngå dette ved å ikke bruke løpende eller identifiserbare nøkler i løsningen.
- Hvis data skal være tilgjengelig i en tjeneste for leserne/brukerne, bør disse dataene være lagret atskilt fra øvrige data. Slik unngår du å gi eventuelle hackere en enkel inngangsport i alle datasett og databaser.
- Hvis du skal ha en databasert tjeneste ut mot publikum, tenk på teknisk ytelse og hvilke kostnader som kan påløpe på lagringstjenesten hvis den utsettes for høy trafikk. Du vil helst unngå at tjenesten din kneler ved lansering.

Fase 4: Arkivering og sletting

Ha et bevisst forhold til hvor lenge det er nødvendig å oppbevare dataene du har tilgang til. Enkelte datasett vil du ha for alltid, andre er det naturlig å slette når evt. bruksområdet er borte eller foreldelsesfrist for søksmål er over. Datalagring koster penger, og i henhold til GDPR skal persondata som ikke lenger er i bruk, slettes. Dessuten finnes det alltid en risiko for at uvedkommende kommer inn i data, også data som ikke er i bruk.

Arkivering kan innebære å redusere tilgjengeligheten av dataene. Dette kan i noen tilfeller øke sikkerheten ved at hvilke data som er eksponert mot mulige trusler reduseres. For eksempel kan data fjernes fra aktive arbeids-/produksjonssystemer. Det er ofte ikke nok å trykke «delete» for at data faktisk skal forsvinne.

- Skytjenester håndterer det meste på godt vis hvis du sletter dataene dine – men sjekk hvor lang tid det tar før sletting faktisk finner sted hos eksterne leverandører
- Lokale lagringsenheter som PC, harddisk eller minnepinne kan det være nødvendig å overskrive for at data faktisk skal være helt slettet.

6 Skarpe saker

Noen saker krever ekstra varsomhet. Her får du råd om hvordan du håndterer særlig sensitiv informasjon.

Allerede når du får "Panama Papers i innboksen" må du ha gjort noen valg som sikrer at kilder kan henvende seg til redaksjonen på en trygg måte. Her kan du bruke risikomodellen i kapittel 3 og i tillegg sørge for å være åpen utad om at det er mulig å kontakte redaksjonen via trygge kanaler.

Overordnet er det viktig at redaksjonene har tatt forholdsregler *før* slikt materiale mottas, og er bevisst på at trusselaktører allerede kan sitte og forsøke å overvåke det redaksjonen gjør.

6.1 Når du mottar svært sensitiv informasjon:

1. Stans! All kommunikasjon om innholdet skal skje gjennom krypterte kanaler.

   - Eksempel på kryptert kanal kan være appen Signal (se side 21)
   - Jobb ut fra tanken om at uvedkommende ønsker å se og høre alt du gjør fremover, også via andre i din nærhet.

2. Hvis sensitive opplysninger er mottatt i digital form, vær svært varsom med hvor du åpner materialet. Ikke gå til nærmeste maskin eller telefon, tenk deg om!

3. Gjør en vurdering av hvor sensitivt materialet kan være. Jo mer sensitivt, desto strengere sikkerhetstiltak.

   Svært sensitivt materiale bør åpnes på en "blank" PC — en maskin som aldri har vært, eller er, koblet til internett. Etabler strenge regler i redaksjonen for videre arbeid:

   - Ikke ha mobiltelefoner og lignende enheter i nærheten av denne datamaskinen.
   - Begrens hvem som har tilgang til både materialet og datamaskinen.
   - Tenk nøye på hvor du plasserer maskinen – og hvem som kan komme i nærheten av den.
   - Gjør en nøye vurdering av hvilke verktøy og programvare som skal benyttes i det videre arbeidet, og hvilke opplysninger som overføres hit.

4. Lag en forenklet trusselmodell:
    - Hvilke opplysninger har vi og hvem er de verdifulle/skadelige for?
    - Hva er konsekvensen av at opplysningene kommer på avveie?
    - Hva i materialet kan avsløre kilden?
    - Hvem kan finne på å angripe oss som følge av denne dataen, og hvordan kan angrepene komme? (Hacking, menneskelig påvirkning, osv)

7 Aktuelle verktøy

Her følger en liste over tjenester, systemer og applikasjoner som er relevant for å sikre upublisert materiale og ivareta det digitale kildevernet. Listen er ikke uttømmende, men omfatter mange av de vanligste og mest velprøvde verktøyene for å beskytte digitale dokumenter og kommunikasjonslinjer.

Verktøyene er rangert i alfabetisk rekkefølge.

7.1 E-post-kryptering

Thunderbird, GPG Suite (OS X), GPG4Win (Windows) er eksempler på noen programmer/tilleggsprogrammer som gjør det mulig å kryptere e-postmeldinger.

Ferske versjoner av den gratis e-postklienten Thunderbird har innebygget støtte for kryptering.[1] Thunderbird kan installeres i Windows, OS X og Linux.

For dem som foretrekker å bruke standardprogrammene Outlook eller macOS Mail, finnes det gode løsninger. Pakkene GPG4Win/GpgOL for MS Windows og GPG Suite/GPGMail for Mac OS X er ment å skulle fungere sammen med eksisterende e-postprogrammer. Når disse tilleggsprogrammene installeres, utvider de grensesnittet i e-postprogrammet med knapper og menyvalg knyttet til kryptering og signering av e-poster.

- **OS X:** Thunderbird el. (macOS Mail $\Longleftrightarrow$ GPG) Suite/GPGMail
- **Windows:** Thunderbird el. (Microsoft Outlook $\Longleftrightarrow$ GPG4Win/GpgOL)
- **Linux:** Thunderbird

E-postkryptering er ikke trivielt. Blant annet krypteres ikke hvem som kommuniserer med hverandre (til og fra) og emnefelt som standard – noe man må være obs på i bruken. For kritisk kommunikasjon med kilder og lignende er det viktig at brukeren beholder kontrollen med prosessen gjennom en grunnleggende forståelse av prinsippene. Generelt er det grunn til å være på vakt mot programmer som prøver å forenkle prosessen for mye.

Det kan også finnes sårbarheter som gjør tilleggsprogrammer mindre pålitelige enn alt-i-ett-pakker som Thunderbird.

[1] Versjoner før Thunderbird 78 kunne bruke tillegsprogramvaren Enigmail for å få støtte for e-post-kryptering.

7.2 Fulldiskkryptering

BitLocker (Windows), FileVault (OS X) og LUKS (Linux) er eksempler på løsninger som enkelt kan tas i bruk for å sikre innholdet på hele (eller deler av) harddisken.

I Windows og OS X er det enkelt å aktivere fulldiskkryptering, slik at ikke noe av innholdet på harddisken kan lese av utenforstående. Dette gjelder selv om en angriper tar harddisken ut av maskinen for å hente ut innholdet.

Tilsvarende dette har noen Linux-distribusjoner, som Ubuntu, innebygd funksjonalitet for å kryptere hjemmeområdet. Dokumenter og andre filer som ligger i brukerens egen mappe vil dermed være utilgjengelig for alle som ikke har passordet.

Fulldiskkryptering er den mest effektive måten å beskytte innholdet i datamaskinen på. Men husk: Det finnes ingen annen måte å låse opp en kryptert disk på enn ved å bruke passordet. Glemmer du passordet, kan du skyte en hvit pinn etter dataene på disken. Flere av løsningene sikrer dataene som hovedregel bare når maskinen er avslått. Så det kan være lurt å slå av maskinen når den ikke brukes, er med på bussen eller legges igjen på hotellrommet.

7.3 SecureDrop

Varslerportalen SecureDrop har vært i bruk av flere av de største medieorganisasjonene i en årrekke. SecureDrop er et komplekst serverrigg som krever to separate maskiner og en dedikert brannmur. Systemet opererer over Tor-nettverket for å sikre brukernes anonymitet så godt det lar seg gjøre. Systemet er tett integrert mot *Tails* (se side 21).

Sikkerheten i systemet hviler ikke bare på kryptografiske algoritmer og protokoller. Den avhenger også av at mediebedriften oppfyller en rekke krav rettet mot egen webserver-konfigurasjon, så vel som mot journalistene som skal håndtere materialet som kommer inn.

Det hjelper for eksempel lite med en anonym varslingstjeneste, hvis webserveren logger IP-adressene til potensielle varslere som besøker informasjonssiden for tjenesten.

Til syvende og sist er det redaktøren som har ansvaret for at sikkerhetsregimet blir fulgt, slik at kildene får den beskyttelsen de er lovet.

SecureDrop vedlikeholdes av Freedom of the Press Foundation, en amerikansk, ideell organisasjon som kjemper for ytrings- og trykkefrihet.

Du kan lese mer om løsningen på https://securedrop.org.

7.4 Signal

Kommunikasjon med kilder undergitt kildevern bør anonymiseres. Signal er en meldingsapplikasjon som ende-til-ende-krypterer både samtaler og tekstmeldinger.

Signal hverken kan eller vil registrere hvem du kommuniserer med. Det finnes med andre ord ingen sentral aktivitetslogg som en tredjepart kan skaffe seg tilgang til for å drive kildejakt. Hvem som kommuniserer, og hva de kommuniserer om, er dermed svært vanskelig å avsløre for utenforstående.

Signal finnes for Android, iPhone og iPad. I tillegg foreligger den som desktopversjon til Windows, OS X og Linux.

NB! Desktopvarianten av Signal har fått kritikk for å være mindre sikker enn mobilversjonene. Dette henger sammen med valg av underliggende teknologi.[2] Ha dette i bakhodet når du tar applikasjonen i bruk, unngå eventuelt å bruke desktopversjonen til den mest kritiske kommunikasjonen.

Signal kan lastes ned fra *https://signal.org*

7.5 Tails

Fordi du ikke har full kontroll på datalagringen i moderne operativsystemer, er PC-en din uegnet til å håndtere det mest sensitive kildematerialet. Selv når du har slettet eller kryptert den hemmelige rapporten ingen skulle vite at du hadde, finnes det stort sett alltid spor etter den andre steder på harddisken.

Tails er akronym for *The Amnesic Incognito Live System*. Det er et komplett operativsystem som ikke skal installeres på maskinen. I stedet startes Tails fra en ekstern lagringsenhet — som oftest en minnepinne. Systemet regnes for å være svært sikkert. Når tails avsluttes, forsvinner alle spor etter hva du har drevet med.[3] Harddisken forblir urørt, all interaksjon skjer mot minnepinnen.

Til sammenligning sprer Windows, OS X og til dels Linux backupkopier, historikk, loggfiler, søkeindekser og andre metadata rundt om på maskinen. I tillegg har enkeltprogrammer egne steder hvor de bakgrunnslagrer informasjon om filer og operasjoner.

[2] Desktopversjonen av Signal bruker et programvarebibliotek som kan ha sårbarheter. Se https://github.com/signalapp/Signal-Desktop/issues/1635

[3] Dette gjelder så lenge brukeren ikke har aktivert såkalt persistent lagring. Når persistens er aktivert, vil brukeren kunne lagre data på et kryptert område av minnepinnen.

Selv om fulldiskkryptering forhindrer harddiskanalyse ved å stenge tilgangen til disken, eksisterer dataene like fullt dersom motparten skaffer seg tilgang til passordet eller manipulere deg til å låse opp disken.

Derfor er Tails en av de beste løsningene for helt å unngå problemstillingen når du har dokumenter som kan føre til etterforskning og beslag av datautstyr.

Tails bruker Tor-nettverket for å anonymisere brukeren og beskytte hen mot overvåkning og sensur. I et av de lekkede NSA-dokumentene fra Edward Snowden, ble sikkerheten i Tails betegnet som "katastrofal". Vel å merke i en etterretningsorganisasjons øyne. NSA regner Tails for å være blant applikasjonene som er aller vanskeligst å knekke.

Varslingstjenesten SecureDrop (se side 20) bruker Tails i stor utstrekning.

Tails kan lastes ned fra *https://tails.boum.org*.

7.6 Tor

Tor, eller *Tor-nettverket*, er den mest utbredte løsningen for anonymisering av internettbrukere. Tor har fått et dårlig rykte fordi det ofte trekkes frem i forbindelse med kriminelle aktiviteter. Men systemet brukes også av journalister, varslere, politiske aktivister, politietterforskere og andre som av ulike årsaker kan ha behov for å være anonyme på internett.

Tor består av en spesialtilpasset nettleser og et nettverk av datamaskiner eller *noder* som jobber sammen for å beskytte brukernes identitet.

Når du bruker Tor-nettleseren for å nå en bestemt nettside, går forespørselen fra din maskin via tre noder, før den når frem til nettsiden. Tor-nettleseren krypterer informasjonen som hver av nodene trenger og pakker dem sammen lagvis som i en løk som må skrelles i riktig rekkefølge. Herav navnet "Tor", som står for *The Onion Router*. Prinsippet er som følger:

1. Den første noden — den såkalte *inngangsnoden* — skreller det øverste laget av løken og ser da adressen til neste node i kjeden. Inngangsnoden vet din IP-adresse, og også hvor resten av løken skal videre, men den aner ikke hvilken nettside du vil besøke, eller noe av innholdet i kommunikasjonen. Dette ligger skjult lengre inne i løken.

2. Den midterste noden skreller av et nytt lag og finner adressen til neste node i kjeden. Men den aner ikke din IP-adresse, ettersom den ligger igjen hos den første noden. Hvilken nettside du vil besøke aner den heller ikke, siden denne informasjonen ligger enda lenger inne i løken, som den blindt sender videre til den neste, tredje, noden.

3. Den tredje noden — den såkalte *utgangsnoden* — skreller av det siste laget, og ser dermed hvilken nettside du vil besøke, og gjør forespørselen for deg. Men den har ingen mulighet til å se hvor denne forespørselen opprinnelig kommer fra.

4. Når utgangsnoden har fått respons fra nettsiden du ville besøke, krypterer den svaret slik at bare Tor-nettleseren din kan åpne det. Alt sammen sendes så samme vei tilbake igjen.

Husk at Tor ikke er kryptering! Eieren av utgangsnoden kan se alt du gjør over nettverket dersom du er inne på usikre nettsider. Som ellers er det derfor viktig aldri å utveksle sensitiv informasjon med nettsider som ikke bruker sikker tilkobling!

7.7 VeraCrypt

For fulldiskkryptering av eksterne disker og minnepinner har programmet VeraCrypt med tiden blitt en anerkjent løsning. VeraCrypt er basert på åpen kildekode, og er en videreføring av forgjengeren *TrueCrypt*, som ble avviklet som prosjekt i 2014, da utviklerne trakk seg ut og advarte sterkt mot at programmet ikke lenger er sikkert å bruke. De utdypet ikke hvorfor, men noen av binærfilene som lå ute for nedlasting var blitt manipulert.[4]

VeraCrypt regnes imidlertid som sikkert å bruke, selv om programmet bruker mye av kildekoden fra TrueCrypt. Koden er grundig evaluert av sikkerhetseksperter, som ikke fant noen alvorlige sårbarheter eller feil.

VeraCrypt har funksjonalitet som i teorien kan gi deg såkalt *plausibel benektbarhet*. Programmet kan opprette *doble volumer* på harddisken, der et ytre volum gjemmer et indre, skjult volum.

De ekte dokumentene ligger godt beskyttet i det skjulte volumet, med et hemmelig passord. Det ytre volumet inneholder annen og mindre hemmelig informasjon som er kryptert med et annet passord. Dette siste passordet kan du gi fra deg uten fare for originalmaterialet.

VeraCrypt kan lastes ned fra *https://www.veracrypt.fr/en/Home.html*

[4] https://www.theregister.com/2014/05/28/truecrypt_hack/

8 Råd til it-ansvarlige i mediehus

Mediebedrifter ligner på andre bedrifter, men har noen særegenheter knyttet til journalistikk og sikkerhet. Her er noen råd til deg som er IT-ansvarlig i en mediebedrift.

- Tenk igjennom trusselnivået for din bedrift. Omtaler dere kontroversielle temaer? Driver dere med undersøkende journalistikk? Beskyttelsen bør være i tråd med trusselnivået.
- Lytt til journalistene og avklar hvilke behov de har for beskyttelse av sine data og hvilke verktøy de bruker.
- Foreslå gjerne nye verktøy eller løsninger som de kan bruke, men hør på tilbakemeldingene.
- Det bør tilpasses en «lekegrind» der man kan holde på med ting som ikke bør gjøres i et normalt regime. Betingelser for bruk må være at det er et reelt behov og ikke bare «jeg liker ikke å jobbe i det normale regimet her» uten at journalisten nødvendigvis må redegjøre veldig mye.
- Hjelp til med å få satt opp trygge og gode miljøer, men respekter likevel at IT-avdelingen ikke bør ha tilgang til disse miljøene.
- Følg opp at miljøene som er satt opp, brukes. Hvis de ikke brukes - finn ut hva som er årsaken.
- Vær rask med å reinstallere evt. kompromittert utstyr ved behov.
- Ha tilgjengelig eget utstyr som kan brukes ved reise til f.eks høyrisikoland. Sørg for å reinstallere dette straks journalisten er tilbake fra reisen.
- Sett opp to-faktor på all innlogging hvor det er mulig.
- IT-avdelingen bør sette seg inn i digitalt kildevern, journalistunntaket i personvernloven og gjøre seg kjent med Vær Varsom-plakaten.
- IT-avdelingen må gi sikkerhetstips til redaksjonen og informere om relevante sikkerhetsproblemstilinger.
- Det er viktig å ha etablert avtaler og kontaktpunkter på forhånd som kan hjelpe deg i en krise. Det er for sent å tenke på dette når det smeller. (Politiet, NSM, Datatilsynet, NorCERT, evt. leverandører av Incident Respons-tjenester, andre mediebedrifter, medienettverk)

- Det bør finnes gode beredskapsplaner som det er øvd på i IT-avdelingen. Alle ansatte må som en del av dette vite hvor man skal henvende seg for å melde fra om mistenkelige og uønskede hendelser.