Aftenposten

METODERAPPORT:

DATASKANDALEN I

REGJERINGSKVARTALET

Ansvarlig:
Per Anders Johansen
Journalist
Politisk redaksjon
Aftenposten

Biskop Gunnerus gate 14 A
Postboks 1, 0051 Oslo, Norway
T: +4797540345
F:
M: +4797540345
per.anders.johansen@aftenposten.no
www.aftenposten.no

Dataskandalen i regjeringskvartalet

1.INNLEDNING

Ett av mine favorittsøk i postlistene er "Riksrevisjonen" – men de siste fem årene har det vært langt mellom treffene. Et flertall bestående av Ap, Høyre og KrF sørget for at Stortinget skreddersydde paragrafen nr 5 – som i praksis hindrer journalister i å omtale sakene inntil et dokument legges frem for Stortinget. De fleste sakene legges frem en gang i året samtidig, under fremleggelsen av dokument nr 1. Mange store og viktige saker som hadde fortjent mer oppmerksomhet, blir parkert på denne måten. De fleste går i glemmeboken i løpet av noen dager. Akkurat slik som politikerne i Ap og Høyre har ønsket.

Av nærmest gammel vane er vi noen få journalister som fortsatt søker om innsyn Riksrevisjonen, selv om det blir mye avslag. Men avslåtte innsynsbegjæringer er ikke bortkastet – det gir likevel en pekepinn om hva som bør jobbes med, og hva som kommer. Alt kan brukes i et puslespill av enkeltdokumenter, ideer, tips, innspill, artikler og postjournaler.

Aftenposten rettet i høsten 2010 gjennom en serie artikler søkelyset på datasikkerheten i Regjeringskvartalet. Artiklene viste at Regjeringen rett og slett passet for dårlig på sine hemmeligheter – og hvordan datasikkerheten hos statsrådene og deres medarbeidere over flere år hadde vært for dårlig.

Ved hjelp av en kombinasjon av anonyme og åpne kilder, omfattende kildepleie i et lukket og ganske paranoid miljø i og utenfor Norge, samt omfattende graving i postjournalene til en rekke departementer – kunne Aftenposten sette på dagsorden et graveprosjekt rundt et tema som knapt har vært berørt i SKUP-sammenheng, nemlig datateknologi og datasikkerhet.

Saken førte til at direktøren i Departementenes Servicesenter – tidligere Statens Forvaltningstjeneste – gikk av. Det samme gjorde en avdelingsdirektør. Samtidig satt Regjeringen i gang i en granskning i regi av Nasjonal Sikkerhetsmyndighet, som har konkludert med at det er behov for en rekke tiltak for å beskytte Regjeringens hemmeligheter bedre. Rapporten som ble lagt frem før jul er blitt sikkerhetsgradert, og en rekke tiltak er satt i verk.

2. ARTIKLENE

Dette er de viktigste artiklene i serien, som ble publisert fra 19. oktober til 12. desember 2010:

Regjeringen tappet for store mengder data. 19. oktober 2010
Stoltenberg-regjeringen har passet for dårlig på sine hemmeligheter. Da Riksrevisjonen kom for å undersøke forholdene – ble de rett og slet ført bak lyset

Slik sviktet Regjeringens datasikkerhet. 20. oktober 2010
– Har ikke tatt trusselen om dataspionasje alvorlig nok

Eksstatsråd skjulte dårlig datasikkerhet. 21. oktober 2010
I over ett år fikk en rekke statsråder i Stoltenberg-regjeringen og deres medarbeidere ikke vite at det var avdekket meget «kritiske svakheter» i regjeringskvartalets datanett.

Foss – En skandale. 22. oktober 2010. Reagerer kraftig på at store sikkerhetsfeil i datanettet ble holdt skjult for resten av regjeringen

Regjeringen ber om datahjelp. 23. oktober 2010. - NSM skal granske IT-sikkerheten. Rigmor Aasrud henter inn konsulenter.

Frykter kinesisk Nobel-spionasje. 27. oktober 2010.
- Ligner metodene som ble brukt mot Google og Dalai Lama

Slik skulle Nobel- instituttet tappes. 11.november 2009.
- Hacker-mail for å bryte seg inn på direktørens PC.

Mange ble hacket 14.11.2010
- Dataangrep mot Nobelkomiteen får ringvirkninger. Som følge av slett datasikkerheten i Nobel- komiteen, kan over 300 personer og selskaper ha blitt utsatt for dataspionasje

Sikkerhetsloven brytes av Regjeringen 24.11.2010
- Sender fortsatt hemmeligheter på åpent nett. Får varsel om pålegg etter tilsyn

Ut på dato. - Et eldorado for hackere 25.11.2010
Regjeringen bruker dataprogrammer som gikk ut på dato i 2007, noe som er en gave- pakke til hackere og dataspioner. Aftenposten kartla sikkerhetshull i regjeringskvartalet - fra en kafé i Amsterdam.

Nytt dataangrep mot Regjeringen 26.11.2010
- Alarm om dataangrep mot Regjeringskvartalet Trusselnivået hevet i all hemmelighet

Passet hemmeligheter uten klarering 28.11.2010
- Satt på Stoltenbergs internpost uten å være sikkerhetsklarert - En formalitet, mente DSS.

Dataforsvaret er blitt kraftig svekket 1.12.2010
- Nasjonal sikkerhetsmyndighet oppdager færre spionasjeforsøk IT-sikkerhetsfolk livredde for å kritisere

Ikke gjør som Jens - 2.12.2010
- Stoltenberg på Twitter var en «sikkerhetsrisiko»

Går på dagen etter dataskandalen 8.12.2010
- DSS-sjefen er ferdig

Sendte varslingsbrevet til sjefen hennes 12.12.2010
Historien om hvorfor du bør tenke deg om før du blir varsler.

I tillegg legger vi ved artikkelen som førte til at vi fikk det første tipset om å gå videre – artikkelen om Stuxnet 29. august.

3. SLIK STARTET SAKEN

I august hadde jeg et oppslag i Aftenposten om at Stuxnet-viruset for første gang var oppdaget i Norge (vedlegg s. 1 – første artikkel). Stuxnet hadde i løpet av sommerferien blitt et hett tema i fagmiljøer og blant datanerder. Dette var første gang at dataangrep klarte å slå ut industrielle styringssystemer. Saken baserte seg på et tips, og ble bekreftet etter en rask kilderunde (NSM, Telenor, Hafslund, Siemens).

I dag er det stadig flere spor som peker på at Stuxnet var at avansert dataangrep rettet mot de iranske atomanleggene – og spesiallaget av israelske eller amerikanske myndigheter for å knekke sentrifugene som anriker uran. Deretter spredde viruset videre en store deler av verden.

I etterkant av denne saken fikk jeg et anonymt tips. Tipset gikk ut på at jeg burde **grave mer i datasystemene i departementene, og se nærmere på hvordan regjeringen beskytter seg mot datalekkasjer**.

På forhånd visste jeg – etter utallige postlistesøk i OEP – at Riksrevisjonen også jobbet med temaet. Over flere måneder hadde brevene om Riksrevisjonens arbeid informasjonssikkerheten gått frem og tilbake i postlistene– alle unntatt offentlighet. Jeg viste imidlertid fra journalene at arbeidet hadde pågått i nesten et år, og at et utkast til en rapport var sendt på høring.

Vi får mange tips og leserreaksjoner – og som for de fleste andre journalister er jeg nødt til å legge vekk de fleste. Det var imidlertid flere forhold som gjorde tipset interessant:
*Først og fremst ble jeg ganske smigret – og overrasket - da jeg forsto at tipseren hadde lest metoderapporter jeg hadde sendt inn til SKUP, før jeg ble kontaktet. Det vitnet om en systematisk tilnærming.
*Jeg var i utgangspunktet veldig engasjert i temaet, ikke minst fordi overdreven sikkerhet er en av mine største hindringer i arbeidet som journalist. Datasikkerhetsspørsmål holdt på å stoppe hele OEP-prosjektet (elektronisk spørsmål) da personvernombudene i departementene stilte spørsmål ved datasikkerheten. Min tanke var derfor at god datasikkerhet var en forutsetning for å kunne praktisere åpenhet.
*Over flere år hadde jeg opparbeidet meg et visst kildenett innenfor temaet. Mange datasikkerhetsfolk er ofte svært negative til oss journalister – enten er vi kunnskapsløse, eller så er vi en trussel mot selskapet/Rikets sikkerhet. I sikkerhetsmanualen til det britiske forsvarsdepartementet – som Wikileaks lekket for to år siden – ble journalister, kriminelle og terrorister omtalt i samme åndedrag av sikkerhetsekspertene.
*Tipset minnet meg om en artikkel jeg laget sommeren før, som handlet om hvordan flere offentlige nettsider var hacket – og spredde virus til intetanende besøkende. Nettsidene tilhørte Barne- og familiedepartementet. Den gang lovet departementet å bedre sikkerheten. Det var på tide å se hva som hadde skjedd.
*Selv om temaet var ganske tørt og teknisk – databaser, IP-adresser, programvare og – var jeg nysgjerrig på saksfeltet – mente jeg saksområdet hadde et "stor potensiale". Wikileaks-lekkasjene om Afghanistan og Irak hadde preget dagsorden på forsommeren, og stadig flere begynte å få øynene opp for dette fenomenet.

4. MÅLSETNING

Målet var å undersøke hvordan Regjeringens datasikkerhet fungerte. Min hovedhypotese var at departementenes datasikkerhet var for dårlig, at problemene var langt større enn man ville innrømme offentlig - og at det var fare for at informasjon kom på avveie:
- få ut alt som fantes av skriftlig dokumentasjon – tråle de elektroniske postjournalene.
- få ut Riksrevisjon-rapporten på forhånd, slik at jeg visste hva de jobbet med – og hva de eventuelt ikke hadde gjort noe på.
- kartlegge systemene – og skaffe hjelp til å forstå de tekniske løsningene.

Tidsmålet var også klart: Dersom jeg klarte å få hull på saken, ønsket jeg å timeburde første artikkel times mot fremleggelsen av Dokument 1 til Riksrevisjonen. Årsaken var at jeg regnet med at dette kunne bli et av temaene – samt at det ville bli lettere å få drahjelp av andre medier.

5. TIDSPLAN/RESSURSBRUK

Arbeidet med sakene om Regjeringens datasystemer har pågått fra september til desember, hvor av omlag 7 uker på full tid og resten på "deltid" – dvs inne i mellom andre saker og prosjekter.
I forbindelse med oppfølgingen av varsler-saken (12.12.) fikk jeg hjelp av kolleger i politisk redaksjon til oppfølging på nett/papir. Nobel-saken og saken om dataangrepet på regjeringskvartalet samarbeidet med nettreporter Lars Akerhaug (som siden har begynt i VG), som hadde veldige gode kilder på dette stoffet. Dataangrepet på regjeringskvartalet var det han som fanget han opp, og Nobel-sakene var teamwork. Utover det har dette vært et enmannsprosjekt var etter eget valg.

15.9.10- 1.10.10: Research deltid/når det var tid

De første ukene foregikk research parallelt med annen jobbing. Ble bl.a. nødt å følge opp Treholt-saken. De to første ukene foregikk derfor researchen midt oppe i mye annet.

1.10.10-19.10.10: Fulltid research/intervjuer/skriving

Fra 1. oktober var jeg sikker på at dette kom til å bli en sak. Derfra og frem til publisering – med unntak av noen dager med høstferie – var det fulltid og overtidsjobbing.
Dessuten fikk politisk avdeling ansatt to vikarer, slik at det mulig å grave litt mer – og ikke hele tiden måtte hoppe over på diverse løpende saker.

19.10.10-23.10.10 : Publisering

De første tre artiklene var i praksis nesten ferdig fra starten av – men ble justert noe underveis. Hele uken gikk med til skriving og oppfølging.

23.10.10-23.11.10 : Ny research-runde

Etter den første publiseringsrunden fra 19.10 til 23.10, som endte med at Regjeringen lovet tiltak (samt hevdet at dette var "gamle" forhold som nå er rettet opp), begynte en ny research-periode på fulltid for å følge opp flere av ideene og trådene fra første runde, organisere og få på plass samarbeid i utlandet. Under researchen snublet jeg over "Nobel-sakene", som ble skrevet ut umiddelbart.

24.11.10-12.12.10: Publisering/research/publisering

De fleste sakene var ferdig researchet - men ikke skrevet - 24.11. Unntaket var varslersaken o – som ble landet og skrevet de siste ukene.

6. ORGANISERING AV ARBEIDET- SKRIFTLIGE OG MUNTLIGE KILDER

4.1. Dokument-jakten

Arbeidet startet umiddelbart med å søke i journalene og kreve innsyn i alt som berørte temaet i postlistene. Jeg begynte systematisk å be om innsyn i alt jeg kunne komme over av dokumenter knyttet til datasikkerhet og datasystemene i Regjeringen:

-Jeg søkte i første omgang på ”datasikkerhet*”, ”informasjonssikkerhet*”, ”sikkerhet* og data*”.

-Deretter gikk jeg over til å søke på flere av avsenderne/mottagerne som dukket opp på de første søkene: ”Riksrevisjonen”, ”DSS”, ”FAD”, ”Departementenes Servicesenter”, ”NSM/Nasjonal sikkerhetsmyndighet”, ”Koordineringsutvalget for informasjonssikkerhet”/ KIS.

-Neste skritt var på søke på stikkord basert på de første treffene: – for eks ”avvik”, ”Depnet/Dep.net”.

-Deretter gikk jeg over på andre stikkord nevnt journalene, for eks ”ekst

I løpet av den neste uken gikk det av gårde 140 innsynsbegjæringer. 52 prosent av sakene ble unntatt offentlighet. Det dukket opp en rekke interessante dokumentspor – både blant de offentlige og ”hemmeligstemplede” dokumentene. For de som er spesielt interessert, er det mulig å gjøre søkene selv på www.oep.no. Det vil sprenge rammene for en metoderapport å gjennomgå alt, men her noen eksempler:

Eks 1. ”**Forprosjekt - Sikkerhetsgjennomgang av Dep.net U”. Dato:** 08.03.2010

Virksomhet:	Fornyings-, administrasjons- og kirkedepartementet
Sak:	Offentlig anskaffelse - Innkjøp av konsulenttjenester vedr Dep.nett-U
Dokumenttittel:	Forprosjekt - Sikkerhetsgjennomgang av Dep.net U
Saksnummer:	2009/02379
Dokumentnummer:	7
Dokumenttype:	Innkommende
Avsender:	Watchcom Security Group AS
Dokumentdato:	08.03.2010
Journaldato:	09.03.2010
Publisert i OEP:	18.03.2010
Unntaksgrunnlag dokument:	Sikkerhetsloven § 11

Dette hemmeligstemplede dokumentet (sikkerhetsloven par. 11, noe som betyr at dokumenter er sikkerhetsgradert) i postjournalene var en regning fra Watchcom, og vekket interesse umiddelbart. Watchcom kjente jeg godt til – og av journalen var det mulig å slå fast at de var blitt hyret inn for å se på datasikkerheten i Departementenes Servicesenter. Den første sjekke-telefonen gikk derfor til en kilde jeg hadde brukt i flere saker tidligere om datakriminalitet og hacking, nemlig datasikkerhetseksperten Preben Nyløkken i selskapet Watchcom. Responsen var tankevekkende: Nyløkken ville ikke snakke med meg i det hele tatt - ikke en gang ta en kaffe. En så bastant avvisning fra en god og gammel kilde inspirerte til hardere arbeid. Når selv et av Norges største private sikkerhetsselskap blir livredde bare jeg ba om en kaffe, var det god grunn til å gå dypere. Hvorfor ble de hyret inne? Hva hadde de funnet? Hva var problemet?

Eks 2. Melding om avvik

Virksomhet: Departementenes servicesenter

Dataskandalen i regjeringskvartalet

Sak:	Avviksmelding informasjonssikkerhet
Dokumenttittel:	Melding om avvik - MinTid - vedr. tilgang til stemplingsinformasjon - vi ber om snarlig tilbakemelding på at DSS har gjenopprettet normal tilstand
Saksnummer:	2010/00375
Dokumentnummer:	1
Dokumenttype:	Innkommende
Avsender:	Landbruks- og matdepartementet
Dokumentdato:	26.08.2010
Journaldato:	27.08.2010

Dette dokumentet var også overraskende, og antydet at det var problemer med datasikkerheten. Det viste seg at to avdelingsdirektører i Landbruksdepartementet LMD hadde oppdaget at de hadde tilgang til persondata om medarbeidere over hele regjeringskvartalet, for eksempel sykefravær, overtid etc. LMD reagerte kraftig – og forlangte umiddelbart at driftsansvarlig – Departementenes Servicesenter – ryddet opp. Svaret var at det ikke var mulig – med mindre man ville miste brukerrettigheter. Jeg stusset ved hele saken. Hadde de ikke bedre orden i sakene enn dette?

qbe1A59.pdf

Eks 3: Olje- og energidepartementet 2008/00894-016 2008.09.02 Seksjon for/HJO Avsender : Departementenes servicesenter Tittel : Feil og mangler på IT systemene for nyansatte i OED

539492_539399_HO VEDDOKUMENT.PDF

Dokumenter og brev som dette dukket opp flere steder – og tegnet et bilde som tydet på at det rett og slett var mye rot i DSS. Mange av brukerne – dvs enkeltdepartementene – klaget med jevne mellomrom.

Eks. 4. Analyse av ekstern kommunikasjon i Depnett-U
Til Finansdepartementet fra FAD 09/1314 200800247-/JFN 14. mai 2009

Rapport - Analyse av ekstern kommunikasjc

Dette var ett av de viktigste dokumentene som kom frem i postjournal-søkene var knyttet til "analyse av ekstern kommunikasjon". Dokumentene var en del av brevveksling mellom FAD og Finansdepartementet, OED og UD.
Dokumentet refererte til en rapport som DSS hadde bestilt høsten 2007 for "å få et dypere innblikk i risikonivået knyttet til internettrafikken inn til regjeringsfellesskapet".

Dataskandalen i regjeringskvartalet

Rapporten ”avdekket behov for å gjøre noen konkrete tiltak, både umiddelbart, og både på kort og mellomlang sikt” – noe som på byråkratsspråket betyr at det var veldig mye som var galt. Det ble snakket om ”infiserte maskiner”, ”umiddelbar” handling, ”tatt av nett”,”skjermingshensyn” og ”sårbarhet”.
Selve rapporten var klassifisert ”Begrenset” – dvs sikkerhetsgradert – noe som var selvmotsigende. DepnettU var nemlig et dataområde som i utgangspunktet ikke skal brukes til å sende sikkerhetsgradert informasjon.
Det dukket opp brev i flere departementer om denne saken. Ut fra de enkelte dokumente var det mulig å sette sammen deler av innholdet i rapporten. Det viste seg også at den nevnte rapporten hadde vært holdt skjult for de andre departementene av FAD – og dette vakte til dels sterke reaksjoner.

Oppsummering dokument-jakt:
*Dokumentjakten gjennom elektronisk postjournal ga veldig gode resultater. I alle sakene som ble publisert, var dokumentene en avgjørende del av kildegrunnlaget. Unntaket var Nobel-sakene og saken om dataangrepet på regjeringskvartalet, hvor vi basert oss på muntlige kilder.
*Totalt fikk jeg innsyn i ca 70 ulike dokumenter som jeg vurderte som relevante. I tillegg kom massevis av bomskudd, feilbestillinger og saker som viste seg å være helt uinteressante.
*Innsynsbegjæringene ble rettet til følgende etater og departementer: Utenriksdepartementet, Miljødepartementet, Fiskeridepartementet, Samferdselsdepartementet, Fornyings- og administrasjonsdepartementet, Justisdepartementet, Departementenes Servicesenter, Olje- og energidepartementet og Nasjonal Sikkerhetsmyndighet NSM.
*Om lag halvparten av dokumentene ble unntatt offentlighet.
*Jeg ba rutinemessig om innsyn i de samme dokumentene i flere departementer – både hos mottager og avsender – for å få en grundig vurdering fra flere hold. Noen steder fikk jeg innsyn, andre steder var det avslag. Årsaken er at departementene gjør ulike skjønnsmessige vurderinger av hvor grensen for innsyn bør gå. Det har både positive og betenkelige sider. På den ene siden er det bra at departementene gir en uavhengig behandling av innsysbegjæringen. Men samtidig forklarer dette også hvorfor det er så mye hemmelighold i forvaltningen: Offentlighetsloven overlater altfor mye til den enkelte byråkrats skjønn.
*Ved siden av journal-jakten, hentet jeg også ut årsrapporter og tilsynsrapporter fra NSM og DSS.

Men jeg hadde aldri klart å komme så dypt inn – og ikke minst forstå dokumentene – hvis jeg ikke hadde flere andre kilder, noe som er tema for neste kapitel.

4.2. DE MUNTLIGE KILDENE

4.2.1. Åpne kilder

Dette var de viktigste åpne kildene i prosjektet (i tilfeldig rekkefølge):
Næringslivets Sikkerhetsråd (Arne Rød Simonsen).
Telenor Security Operation Center i Arendal TTOC (Leder Frank Stien).
Nasjonal Sikkerhetsmyndighet og NorCERT. (Adm.dir. Kjetil Nilsen, Christophe Birkeland, Kjetil Veire)
Departementenes Servicesenter (Dir. Ivar Gammelmo).
Fornyings- og administrasjonsdepartementet (Statsråd Rigmor Åsrud, info.sjef Frode Jacobsen).
Utenriksdepartementet. Arkivet.
Olje- og energidepartementet. Arkivet.
Justisdepartementet. Info.avdelingen.
Forsvarsdepartementet. Arkivet.
Landbruks- og matdepartementet. Arkivet.
Finansdepartementet.Arkivet.
EDOK-konferansen.
CONFEX-konferansene.
NSMs sikkerhetskonferanse.
Telenors sikkerhetskonferanse (Roadshow)
NORSIS. Norsk Senter for Informasjonssikring.
Tidligere statsråd Heidi Grande Røys og de som tilhørte hennes politiske stab.
Riksrevisjonen (riksrevisor Jørgen Kosmo og ekspedisjonsjefskollegiet).
Direktoratet for IKT og forvaltning.
Politiets data- og materiellltjeneste (Info.sjef Espen Strai).
Udo Galle, talsmann for QCIC. (www.qcic.nl)
Jorid Bodin, tidligere ansatt i DSS.

Bruno Winter, nederlandsk journalist som hjalp meg med å sjekke QCIC.
WOB-seminar i Gent i Belgia og konferansen til den flamske foreningen for undersøkende journalister VVOJ. Her diskuterte jeg datasikkerhetsspørsmål og postjournal-søk med flere journalister, blant annet Phil Myers i BBC
Stortingets kontrollkomite (Anders Anundsen og Per Kristian Foss).

Kommentarer/drøfting av de åpne muntlige kildene
Jeg nevner ikke navn på personene jeg var i kontakt med i alle departementene, rett og slett fordi jeg valgte ikke å referere fra samtalene i artiklene.
Av de åpne kildene vil jeg spesielt kommentere QCIC, Riksrevisjonen, FAD, NSM, Jorid Bodin og DSS.

Nasjonal sikkerhetsmyndighet fortjener ros for måten de valgte å praktisere offentlighetsloven på. Siden NSM ikke er en del av OEP, gjorde jeg en egen "manuell" innsynsrunde i NSM på saker knyttet til tilsyn i departementene og DSS. Selv om innsynsbegjæringene tok lang tid, så var vurderingene saklige og omfattende. I flere saker praktiserte de meroffentlighet på en god måte.
I enkelte saker var det NSM som insisterte på at en sak ikke skulle sikkerhetsgraderes, for eksempel saken om regjeringens postmenn som manglet sikkerhetsklarering.
Men samtidig er det et tankekors at den siste rapporten NSM leverte ved juletider, er sikkerhetsgradert. Det gjør det nesten umulig å sjekke i ettertid om tiltak kommer på plass – det blir til syvende og sist et spørsmål om vi stoler på de som skal ivareta sikkerheten.
Det er likevel grunn til å problematisere om NSM kom for lett unna i denne omgang.

QCIC. Da Regjeringen avfeide saken som gammelt nytt (etter Riksrevisjon-saken og de første tre sakene), bestemte jeg meg for å gjøre min egen analyse – og til det trengte jeg hjelp. Målsetningen var å få "nå"-status på datasikkerheten. Først kontaktet jeg flere kilder i norske datasikkerhetsselskaper, men jeg forsto raskt at det var dødfødt. Ingen ønsket å være med på noe som kunne oppleves som kritikk av deres viktigste kunde – nemlig staten.
I utgangspunktet hadde ikke QCIC noe stort behov for å medvirke. Men vi hadde mailkontakt over lengre tid, og ble til slutt enige om et samarbeide.
Måten vi fikk kontakt med QCIC på, er redegjort for punktet om anonyme kilder.
Jeg gjorde flere forsøk på å sjekke mest mulig om QCIC, og det var en selsom opplevelse. Gruppen/foreningen/sammenslutningen har en offisiell nettside, men der finnes ingen navn. Når søker på QCIC gjennom søkemotorene – og plukker opp "cached"-versjoner – har QCIC vært inne og "fiklet" med resultatet. Du får til svar at "er du ikke klar over at Google blir sponset av CIA?".

Jorid Bodin hadde vi en dialog med før hun bestemte seg for om hun ville stille opp i et åpent intervju i Aftenposten. Jeg mente i utgangspunktet at hennes historie var så viktig at den også kunne fortelles anonymt. Hun valgte å stille opp som åpen kilde for å unngå fokus på spekulasjoner om hvem som varslet, og for å gi saken mer tyngde. Hun ønsket at fokuset skulle være på varselets innhold og hvordan varslersaken ble håndtert etter at hun varslet regjeringsråden. Saken illustrer hvordan FAD, som har ansvar for statlige retningslinjer for håndtering av varslingssaker, selv har håndtert en varslingssak slik at varsleren ble utsatt for gjengeldelse. Hennes historie forklarer etter min mening hvorfor det er så få som ønsker å stå åpent frem om sine erfaringer på innsiden av det norske byråkratiet.

Riksrevisjonen og deres rapport ga de tre første sakene i artikkelserien ekstra tyngde, og det faktum at de arbeidet med saken var en av grunnene til at jeg valgte å sette i gang. De første tre artiklene lente seg mye på Dok.nr. 1 fra Riksrevisjonen. Derfra og ut sto all research "egen", og her klarte Aftenposten å komme langt dypere enn det Stortingets kontrollorgan hadde gjort. Riksrevisjonen som kilde fikk mindre verdi, nettopp fordi det var mulig å avfeie kritikken som "sneen som falt i fjor".
Det har foregått en kildejakt i Riksrevisjonen i etterkant. Årsaken er at Aftenposten fikk tak i deler av Dok.nr. 1 før det ble lagt frem Stortinget. Riksrevisor Jørgen Kosmo fikk "så ørene flagret" i Stortingets kontrollkomite fordi Aftenposten omtalte saken samme dag som rapporten ble lagt frem. Mange av mine kontakter i Riksrevisjonen er redde for å snakke med meg, selv om de ikke gir annen en ren saksinformasjon.

Jeg mener Riksrevisjonen heller burde bekymre seg mer over hvor lett det var for Regjeringen å avveie innholdet i rapporten, blant annet ved å vise til at Riksrevisjonens rapport baserte seg på forhold frem til 31.12.2009. "Riksrevisjonen er opptatt av fortid, vi er opptatt av nå-tid og fremtid", sa statsråd Rigmor Åsrud gjentatte ganger i debattene som fulgte i avis, nett, radio og TV etter Aftenpostens artikler.
Forholdene som Riksrevisjonen pekte på i rapporten burde vært gjort kjent på et mye tidligere tidspunkt, ikke minst med tanke på å få på plass tiltak. I stedet blir kritikkverdige saker som Riksrevisjonen avdekker holdt skjult for offentligheten i måneder og år. Etter min mening er det å undergrave den viktige jobben som Stortingets revisorer gjør i vårt demokrati.

4.2.2. Anonyme kilder

Miljøet av datasikkerhetfolk, konsulenter og tjenestemenn er et allsidige miljø, og er langt mer fargerikt enn deres tekniske og nerdete arbeidsoppgaver skulle tilsi. På den ene siden har den en meget åpenhjertig debatt i sine interne fora – mens utad er mange svært skyggeredde. Rent gjennomgående er mange ganske paranoide – ikke minst fordi de fleste vet nøyaktig hva som er mulig å gjøre ved hjelp av data. I tillegg er det en rekke økonomiske hensyn som stadig virker inn – og gjør at alt som sies offentlig veies opp mot forretningsmessige hensyn.

Underveis i research-arbeidet opparbeidet jeg kontakt med flere kilder på innsiden av dette miljøet i både statsforvaltningen og det private næringslivet– uten dem ville jeg neppe forstått dokumentflommen. Dessuten hjalp de meg med konkrete tips om dokumenter jeg burde lete etter.

En av personene vi hadde kontakt med, fikk hacket sin mobil – uten at vi har klart å dokumentere at det var relatert direkte til denne saken. Saken ble politianmeldt av vedkommende, men i per januar 2011 ligger anmeldelsen fortsatt hos politiet..

De anonyme kildene var så engstelige at de som regel unngikk å bruke sin egen mobiltelefon. De lånte i stedet andre telefoner, eller skaffet seg en egen mobiltelefon for sensitive samtaler. Enkelte ville kun ha kontakt ansikt til ansikt. I slike tilfeller avtale vi møter på litt avsidesliggende steder.

Et gjennomgående trekk var at flere av de anonyme kildene ikke ville ha kontakt på mail – underforstått at det var svært enkelt for deres overordnede å overvåke mailen.

"George Bondegard" og QCIC
"George " er en anonym medarbeider i QCIC med base i Nederland. Jobber med Udo Galle som talsperson. En utrolig dyktig datasikkerhetsekspert, men stor sans for humor og spisse kommentarer. Han har jobbet som datasikkerhetsekspert for en rekke selskaper og organisasjoner.
"George Bondegard" var en av 30-40 personer som tok kontakt med meg etter de første tre sakene. Siden utvekslet vi over 50 mail, og ble enige om å møtes i Amsterdam sammen med Udo Galle og fotograf Olav Olsen.
Amsterdam-turen var et sjansespill – vi visste ikke sikkert hva vi ville finne, og hvordan det ville gå.
"George" hjalp meg med å kartlegge datasystemene og finne frem til inngangsdørene. Han viste hvordan jeg kunne sende meldinger forbi brannmurene for å undersøke hva slags programvare som ble brukt i datasystemene til Regjeringen. I tillegg var det han som bidro

med å lage et datakart over systemene, adressene – og informasjonsstrømmene inn og ut av regjeringskvartalet.
Han gjorde alt gratis – det eneste Aftenposten dekket var lunsj og noen øl.
George Bondegard er nok bare passe fornøyd med undertegnedes innsats – han synes nok vi burde skrevet 50 artikler til. Generelt sett så var det mitt inntrykk at George og hans kolleger mener vi journalister var helt på jorde, overfladiske og svært lette å manipulere – og egentlig ikke verdt å kaste bort tiden på. Jeg er glad for at han gjorde et unntak for meg.
QCIC lever av å selge sine tjenester, samtidig som gruppen også har klare idealistiske mål. De markedsfører seg som en gruppe som liker å avsløre rådyre dataselskaper som selger defekte sikkerhetsløsninger.

"Anonym kilde A ansatt i statsforvaltningen".
Vedkommende hjalp meg med å få tilgang til Riksrevisjonsrapporten, før den ble publisert. Jeg valgte bevisst ikke å referere helt direkte fra rapporten, men i stedet omtale den med egne ord. Da er det vanskeligere å prøve å spore kilden. Formuleringene i de ulike versjonene av Riksrevisjonens dokumenter kan nemlig variere avhengig av hvor man er i prosessen, og hvem dokumentene blir distribuert til.
Ga gode råd om dokumenter jeg burde be om innsyn i, samt forståelse for hvordan dokumentene skulle tolkes.

"Anonym kilde B ansatt i statsforvaltningen".
Ga nyttig bakgrunnsinformasjon om datasikkerhet – og måten arbeidet foregikk på i departementene.

"Anonym kilde ansatt i privat datasikkerhetsselskap".
Ansatte i privat datasikkerhetsselskap som jobber for blant annet oppdragsgivere i staten. Ville mistet jobben på flekken dersom kontakten med Aftenposten ble kjent.
statsforvaltningen.

De er ingen tvil om at de anonyme kildene var en viktig del av dette prosjektet, selv om ingen av kildene er referert i artiklene. Årsaken til at de ønsket å være anonyme, var flere – og høyst legitime. Faren for å miste jobben, reaksjoner fra kolleger, eller rett og slett bli gjenstand for politietterforskning var overhengende. De anonyme kildene hadde underskrevet en taushetsplikt-erklæring, som dessuten la strenge begrensninger på hva de kunne si.

Siden målet var at sakene skulle stå fjellstøtt, var uttalelsene til de anonyme kildene i seg selv lite verdt. Men de hadde svært stor betydning på ett område, nemlig å forstå de tekniske sidene ved alle dokumentene jeg klarte å få innsyn i, samt å fortolke de dokumentene jeg fikk innsyn i. I tillegg fikk jeg svært gode råd om hva slags dokumenter jeg kunne søke på.

Dette er en svært effektiv og renslig metode. For det første unngår den anonyme kilden å bryte taushetsregler. Vedkommende holder seg på riktig side av loven – i tilfelle kontakten med journalisten skulle bli oppdaget.
Dessuten slipper du å bli sittende med mye informasjon som du likevel ikke kan bruke. Det har liten verdi å bruke masse tid på anonyme kilder, hvis du likevel ikke kan sitere innholdet. Dette er en metode som flere på innsiden av statsforvaltningen burde bruke – dersom de ønsker å få satt fokus på kritikkverdige forhold. Den bør rett og slett markedsføres mer.

4.2.3. Annen kildepleie

En viktig del av researchperioden gikk ut på å snoke rundt på datakonferanser. Det er et enormt tilbud av ulike konferanser, og datakonsulenter er åpenbart veldig glade i å dra på seminarer – i likhet med journalister. I løpet av september, oktober og november meldte jeg meg på det jeg kunne finne av seminarer og kurs.
Jeg fikk tid til å få med meg fire konferanser i løpet av research- og arbeidsperioden: i Telenor, i Nasjonal sikkerhetsmyndighet, samt CONFEX og EDOK. Hensikten var å finne kilder, få kontakt med personer som kunne noe om feltet – og rett og slett plukke opp hva som rørte seg i miljøet. Flere av de anonyme – og åpne – kildene kom jeg i kontakt med på seminarene.
Ved to av konferansene (EDOK og CONFEX) ble jeg dessuten også invitert til å holde innlegg. Det var ekstra nyttig, siden jeg dermed kunne være nærmest en del av "klientellet". Dermed fikk jeg også adgang til alle foredrag som ble holdt på seminarene (ca 50 foredragspresentasjoner), som bare var tilgjengelig for deltagerne.

En del av sakene var et direkte resultat av ideer og tanker som kom opp på seminarene – eller uttalelser som kom under foredragene. Dette var ideer som ble "saltet ned", med tanke på senere publisering:
Saken om Stoltenbergs twitring plukket jeg opp på NSMs konferanse i foredraget til Næringslivets sikkerhetsråd.
Saken om Nobel-instituttet kom på NSMs konferanse (i foredraget til NorCERT).

5. UTFORDRINGER UNDERVEIS

5.1. Operasjon "Pågående aktiviteter"

Både DSS og FAD gjorde betydelig anstrengelser på å bagatellisere saken og holde tilbake til informasjon. Alle spørsmål måtte sendes på mail. Eneste unntak var det større intervjuet vi gjorde med statsråd Rigmor Åsrud.

Et eksempel på metodene som ble brukt, er måten man journalførte en del saker. Noen av dokumentene hadde tittelen "Pågående aktiviteter". Dette viste seg å være brev hvor DSS – i forkant av Riksrevisjonens rapport – etablerte et nettverk på tvers av departementene for å håndtere Riksrevisjonen. Jeg vurderte å lage en sak på det – men droppet det fordi Riksrevisjonens sjef Jørgen Kosmo mente det var uproblematisk. – De får holde på. Vi lar oss ikke lure, svarte Kosmo.

5.2. Andre medier

Saken fikk bred omtale og oppslag over alt i norske medier. Det var imidlertid ingen som første å følge opp saken –eller grave videre. Det var med andre ord ingen drahjelp å få.
Dette var dessuten en sak uten advokater – det var ingen talsmenn eller interessegrupper som holdt saken varm– selv om det for så vidt var noen som ville uttale seg. Det førte til at jeg blant annet måtte delta i debatter i Dagsnytt 18 – og forsvare saken.

5.3. Skadebegrensning

En tankevekkende episode – ut over den vanlige og rutinemessige hemmeligholdelsen av dokumenter og forsøk på ta saken ned gjennom pressemeldinger og leserinnlegg– var en episode i forholdet til Stortinget:

Politikere i Stortinget (kontrollkomiteen) ble orientert om den første saken kvelden før den sto på trykk, og uten at Aftenposten hadde hatt kontakt med dem. Dette kom frem da jeg snakket med riksrevisor Jørgen Kosmo etter pressekonferansen da Dokument nr 1 ble lagt frem. Kosmo var irritert på Aftenpostens oppslag – som han vanligvis er når vi skriver om hva Riksrevisjonen oppdager. Han var ekstra opprørt denne gang.
Kosmo fortalte at han ble ringt opp kvelden i forveien fra personer tilknyttet kontrollkomiteen i Stortinget – han ville ikke si hvem – som da var blitt orientert om Aftenpostens oppslag. De var sinna på Kosmo for at Riksrevisjonen lekket saker før Stortinget fikk dokumentene.
Det pussige er at Aftenposten ikke hadde hatt kontakt med noen på Stortinget. De eneste vi kontaktet på forhånd var FAD og DSS, som begge fikk anledning til å kommentere saken og gi tilsvar.
Min teori er at dette var et eksempel på en PR-metode som pressefolk dessverre er lite klar over. PR-apparatet i regjeringskvartalet driver det som kalles "skadebegrensning" – og kontakter ofte kilder i Stortinget før journalisten selv ringer. Tanken er selvfølgelig å presentere sin versjon av saken først – og få politikerne til å besinne seg i sine uttalelser. Da jeg spurte FAD hvem som hadde ringt rundt til politikere på forhånd, var svaret at dette kjente man ikke til.

5.4. Hvem svarer egentlig?

Flere av svarene vi fikk fra DSS og FAD var dessuten problematiske, og påfallende like. Rigmor Åsrud og DSS-direktør Gammelmo brukte mange av de samme formuleringene: – Ja vi har hatt problemer, men dette har vi tatt tak i og ryddet opp i.
En interessant observasjon var at svarbrevene Aftenposten mottok da vi stilte spørsmål til DSS (som måtte foregå på mail), kom i word-dokumenter som var opprettet av informasjonssjef i FAD Frode Jacobsen.

Departementenes Servicesenter fremstilte Aftenpostens artikler som kampanje-journalistikk. For en mektig etat som nesten aldri hadde opplevd et kritisk søkelys, er det lett å forstå at de oppfattet det slik.

Fra mitt ståsted var det nødvendig å holde trøkket over tid, ikke minst fordi DSS i utgangspunktet avviste problemstillingen. Temaet var så tungt, vanskelig og komplisert, at jeg ønsket å samle opp nok ulike artikler til å holde fokuset over lengre tid. Alt måtte kunne dokumenteres gjennom skriftlige kilder.

5.5. Teknikk og presisjon

Et gjennomgående utfordring under hele saken, var å formidle et svært komplisert stoff på en presis og likevel forståelig måte.
I etterkant har det ikke kommet kritikk på noe som helst, ut over et punkt. FAD mente gjengivelsen av tre eksempler på sikkerhetsgraderte saker som ble journalført i offentlig elektronisk postjournal var misvisende (onsdag 24. november)– i den forstand at FAD mente dokumentene ble oppbevart på en forsvarlig og sikker måte. Det er jeg helt uenig i – men departementet fikk komme til orde i to leserinnlegg.
Det er ingen tvil om at sikkerhetsgradert informasjon er blitt sendt over det åpne nettet (DepnettU) - det er dokumenter gjennom flere tilsyn og rapporter - og man kan spørre seg hva som er FADs motivasjon for å late som om det ikke har skjedd.

5.6. Grensene for hacking

Vi vurderte om vi skulle få hackermiljøene til å hente ut eposter til noen av statsrådene, for eksempel statsminister Jens Stoltenberg. Det er ingen tvil om at det ville vært en viktig dokumentasjon. Vi valgte å holde oss på den riktige siden av loven – selv om vi fikk tilbud om å gjøre det.
En del av vurderingen var at vi likevel hadde så mye dokumentasjon, at vi ville klare å sette dagsorden med sakene.
Et annet moment var at det ville koste penger – og dermed ville vi ha finansiert kriminalitet dersom vi hadde takket ja til tilbudet. Dessuten var det usikkert hvor mye det ville koste. Anslaget gikk ut på at det ville ta mellom en dag – og en måned – å hente ut eposten til Stoltenberg.
Et annet moment som ble vurdert underveis, var om sakene våre kunne fungere som "honningkrukker" for hackermiljøene. Her prøvde vi å finne en balanse mellom å være konkret, dokumentere våre funn i artiklene – og samtidig ikke fortelle absolutt alt. En ting vi var forsiktige med, var å bruke de konkrete tekniske adressene på en del følsomme områder i regjeringskvartalets datasystemer. Dessuten kom vi til at en rekke numre, adresser, navn etc likevel ikke ville øke forståelsen for leseren.
For øvrig er det verdt å merke seg en av George Bondegards utsagn: det meste av all hacking baserer seg på åpne kilder som settes sammen i et puslespill. Slik sett har vi journalister og hackere veldig mye tilfelles – og vi journalister har nok mye å lære av hackernes grundige og systematiske tilnærming.

5.7. Hvordan illustrere datakriminalitet?

Det var en gjennomgående utfordring hvordan vi skulle presentere sakene. En egen grafiker ble koblet til saken, og jobbet en uke med de grafiske løsningene.
Vi valgte også å gjøre om på flere artikler – og i stedet presentere innholdet som grafikk. Flere av grafikk-presentasjonene i artikkelserien var basert på det som opprinnelig var ment som selvstendige nyhetsartikler.
Internt var det delte meninger om hvor vellykket det var – men etter min mening gjorde bruken av grafikk at vi klarte å formidle et veldig komplisert materiale for flere.

5.8. Wikileaks

Et lite paradoks til slutt. Den største utfordringen i arbeidet med serien om dårlig datasikkerhet i Regjeringen inntraff på slutten - da Aftenposten fikk Wikileaks i hus. Tre dager før vi publiserte varsler-artikkelen, fikk Aftenposten tilgang deler av den kanskje største offentlige datalekkasjen noensinne – i form av alle de norske Wikileaks-dokumentene. Noen uker senere fikk avisen tak i hele materialet.
Dette har ført til at det fortsatt er flere ideer og saker knyttet til regjeringskvartalets datasystemer som ennå ikke er publisert.

6. AVSLUTNING

Aftenposten dokumenterte gjennom artikkelserien at det som skulle være "det sikreste av det sikre" –Regjeringens datasystemer – hadde alvorlige mangler og hull. Vi viste også at forholdene ikke var blitt rettet opp – til tross for en rekke advarsler internt. Selv etter at Riksrevisjonen leverte sin rapport, klarte ikke DSS å rydde opp.
Ved hjelp av en omfattende gravejobb i postlister – kombinert med tett jobbing i forhold til både åpne og anonyme kilder – ble det dokumentert at datasikkerheten var dårlig og hadde betydelige svakheter.

Saken har fått flere følger:
- DSS-direktør Ivar Gammelmo gikk av, og det samme gjorde avdelingsdirektør Petter Møller, som hadde ansvar for datasikkerhetsområdet. I den interne begrunnelsen ble det sagt at pressekjøret gjorde det umulig å fortsette – og at DSS trengte arbeidsro.
- Artiklene fikk svært omfattende oppfølging, og de fleste av sakene ble sitert bredt, kommentert og gjenstand for ledere, kommentarer og debatter.
- I etterkant har NSM kommet med en sikkerhetsgradert rapport. Innholdet er ikke kjent, men det har kommet frem at NSM påpekte en rekke huller og svakheter i Regjeringens datasystemer – som nå skal rettes på. Dette står i skarp kontrast til det Fornyings- og administrasjonsdepartementet svarte Riksrevisjonen. Da ble det hevdet at tiltak allerede var på plass, eller i ferd med å gjennomføres. Aftenpostens serie dokumenterte at det langt fra var nok.

Dette er viktig å understreke at dette er en sak som ikke er avsluttet. Fra researchen er det fortsatt en rekke ideer som ligger og venter – og som kommer til å bli publisert de neste månedene.

Vedlegg: Artiklene.

Datasikkerhet low.pdf