# HTTPS-BRUK I NORGE

EN UNDERSØKELSE AV HVORDAN OFFENTLIGE ETATER BRUKER SIKRE TILKOBLINGER FOR SINE NETTJENESTER

Metoderapport til SKUP

# PROSJEKTFAKTA

**Prosjektets tittel / beskrivelse:**
HTTPS-bruk i Norge – en undersøkelse av hvordan offentlige etater bruker sikre tilkoblinger for sine nettjenester
**Dato for metoderapport:** 13. januar 2017
**Journalister:** Øyvind Bye Skille
**Redaksjon:** Digital undersøkende redaksjon – NRK Dokumentar og samfunn

# PUBLISERINGSLISTE

30. mars 2016: Ba om bombetips på sårbar nettside
https://www.nrk.no/dokumentar/1.12859753
30. mars 2016: Slik gjør du livet litt surere for nettsvindlere
https://www.nrk.no/dokumentar/1.12866173
30. mars 2016: Usikkert nett
https://www.nrk.no/dokumentar/xl/usikkert-nett-1.12854582
31. mars 2016: Offentlige nettsteder bakpå også innen andre sikkerhetsstandarder
https://www.nrk.no/dokumentar/1.12865594
31. mars 2016: Difi vil vurdere nye anbefalinger
https://www.nrk.no/dokumentar/1.12857676
11. mai 2016: Offentlige nettsteder kan brukes til å svindle eller angripe deg
https://www.nrk.no/dokumentar/1.12937902
12. mai 2016: Over 50 nettsteder fikset etter NRK-saker
https://www.nrk.no/dokumentar/1.12939125
10. juni 2016: Vil kreve sikrere offentlige nettsteder
https://www.nrk.no/dokumentar/1.12988202
16. desember 2016: Ny standard for sikrere offentlige nettsider
https://www.nrk.no/dokumentar/ny-standard-for-sikrere-offentlige-nettsider-1.13279370

**Interaktiv oversikt:**
12. mai 2016: HTTPS-status Norge
https://nrkbeta.no/https-norge/

**Metodesaker:**
30. mars 2016: Slik undersøkte NRK offentlige nettsteder
https://nrkbeta.no/2016/03/30/slik-undersokte-nrk-offentlige-nettsteder/
11. mai 2016: HTTPS-status i Norge – oversikten
https://nrkbeta.no/2016/05/11/https-status-i-norge-oversikten/

INNHOLDSFORTEGNELSE

# HOVEDFUNN

De aller fleste stoler på og har tillit til offentlige etater i Norge. Få tenker over om systemene til kommunen eller staten er sikre nok når de sender informasjon digitalt i stedet for med gammeldagse papirbrev.

Men noen har kanskje fått med seg at de skal se etter hengelåsen i adressefeltet ved besøk i nettbanken. Hengelåsen symboliserer at oppkoblingen er sikker og gjøres med kryptering – en HTTPS-oppkobling.

NRK har kartlagt nesten 10 000 aktive nettsidedomener eid av det offentlige i Norge for bruk av nettopp slik sikker tilkobling, HTTPS.

NRKs undersøkelser viste at en veldig lav andel av nettsteder eid av det offentlige i Norge bruker sikker tilkobling over HTTPS – noe som kan sette innbyggerne som brukere av slike nettjenester i fare. Informasjonen som sendes over nettet kan være svært sensitiv som helseopplysninger eller sikkerhetsmessig problematisk som tips til politiet om at noen bygger en bombe.

Flere ekspertorganer og rådgivere for offentlige etater anbefaler bruk av slike sikre HTTPS-tilkoblinger, men ingen hadde noen oversikt over i hvor stor grad de offentlige nettstedene faktisk brukte HTTPS. I flere andre land er dette allerede påbudt eller i ferd med å bli satt som krav.

NRKs gjennomgang av over 11 000 domener var derfor første gang dette ble sjekket systematisk.

Gjennomgangen viste også at mange av de som hadde forsøkt å sette opp HTTPS hadde betydelige mangler i oppsettet sitt. Noe som gjorde at de var sårbare for kjente sikkerhetsfeil.

NRKs saker har ført til at et stort antall nettjenester blitt rettet opp slik at de ikke lenger er sårbare for kjente sikkerhetsfeil.

Justisdepartementet tok etter at NRKs saker initiativ til å få vurdert om Norge også burde ha krav om sikre HTTPS-tilkoblinger for offentlige nettsteder. Nasjonal sikkerhetsmyndighet (NSM) som fikk utredningsoppdraget anbefalte i en rapport at dette burde innføres. I desember ble det kjent at HTTPS for nettsteder ligger an til å komme inn som en IT-standard for det offentlige i Norge.

NRK har fortsatt med sporingen av hvor utbredt HTTPS er med en jevnlig oppdatert interaktiv oversikt, og utviklingen har gått sakte mot flere offentlige nettsteder med støtte.

# IDEEN

Det hele startet med en interesse for datasikkerhet og sikker digital kommunikasjon.

Over flere år har jeg brukt kryptert e-post, men utvekslingen av krypteringsnøkler har alltid vært en utfordring. Dermed gjorde jeg etter å ha lest ulike råd et forsøk på å få på plass sikker og kryptert tilkobling (HTTPS) på min personlige nettside. Jeg satte opp en egen webserver, konfigurerte den på egenhånd og lærte mye underveis.

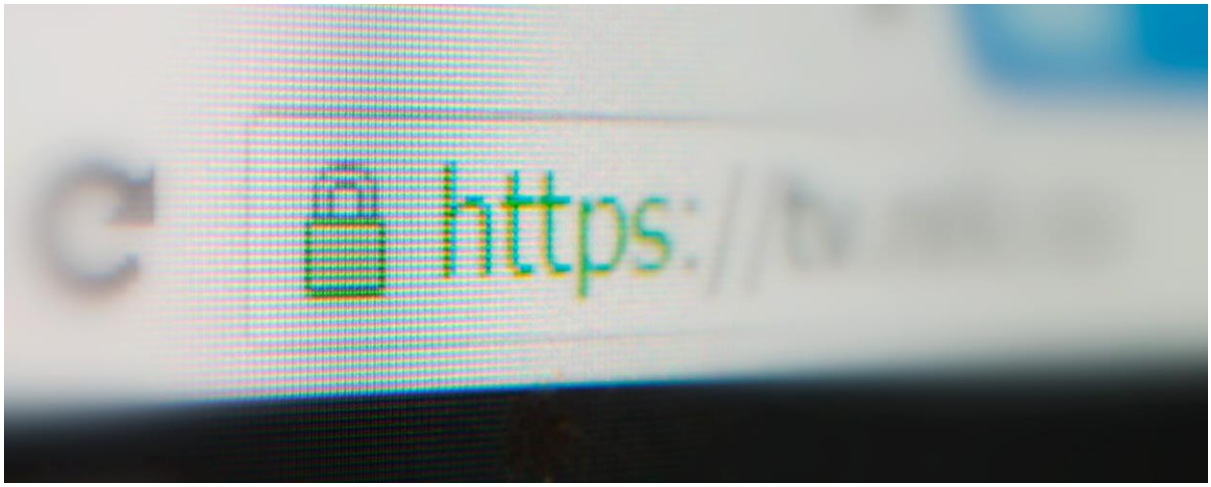
I prosessen leste jeg på nettet om hva som var anbefalt oppsett. Jeg kom også over testsiden SSL Labs. En tjeneste som tester hvordan webservere er satt opp ved å simulere at den kobler seg til som mange forskjellige typer datamaskiner, mobiler og programvarepakker. Testen gir en bokstavkarakter på skalaen fra A (best) til F (stryk). Karakteren sier noe om hvor langt unna et anbefalt oppsett den testede siden virker å være.

Etter å ha testet meg selv, og lært en del underveis i prosessen, ble det som journalist fristende å bruke samme test på andre. Jeg tok derfor først noen stikkprøver blant norske nettsteder, og da spesielt sider drevet av offentlige etater. Litt overraskende fant jeg at flere nettsteder drevet av det offentlige hadde satt opp HTTPS, men likevel fikk strykkarakter og bokstaven F i testen hos SSL Labs.

Videre undersøkelser viste at testen var ganske anerkjent. Både det norske Direktoratet for forvaltning og IKT (Difi) og Det hvite hus anbefalte og brukte testen.

Jeg snakket så med noen fagfolk innen datasikkerhet om det jeg hadde funnet. Tilbakemeldingene jeg fikk ga inntrykk av at noen få eksempler på enkeltsider med dårlige oppsett ble smått i den store sammenhengen for de som jobbet med alvorlig nettkriminalitet og trusler mot kritiske systemer.

**Spørsmålet ble derfor: Hvordan kan jeg finne ut om dette bare er noen få råtne epler?**



# PROBLEMSTILLING

Med bakgrunn i de små eksperimentene og stikkprøvene hadde jeg funnet ut at det fantes eksempler på offisielle nettsider til store norske offentlige etater som fikk stryk i testen fra SSL Labs.

Den sentrale hypotesen ble derfor at mange offentlige virksomheter hang etter innen moderne nettsikkerhet for sine tjenester på nett.

For å finne ut om dette stemte i et større bilde kom det opp flere spørsmål som måtte besvares:

- **Hva finnes av offentlige nettsteder eller nettjenester?**
- **Finnes det noen oversikt over disse?**
- **Hvordan kan mange slike nettsteder sjekkes effektivt?**
- **Hva forteller det oss om et nettsted ikke har HTTPS?**
- **Hva forteller det oss om et nettsted har HTTPS, men får stryk i testen for oppsett?**
- **Hvordan er resultatene sammenlignet med andre land?**

Vi ønsket også å tilgjengeliggjøre begrepet HTTPS for den vanlige leser. I tillegg var det et mål å gi dem et innblikk i våre journalistiske undersøkelser.

# METODE

## Skaffe oversikt over offentlige nettsteder

Jeg ønsket altså å teste et større utvalg nettsteder eid av det offentlige i Norge.
Først tok jeg derfor kontakt med Direktoratet for forvaltning og IKT (Difi) og spurte om de hadde en liste over offentlige nettsteder siden de selv anbefalte testen, og drev med vurdering av nettsteder og nettjenester. Svaret var at de ikke hadde noen fullstendig oversikt liggende.

NRK måtte dermed gå til andre kilder.

Jeg visste fra før at de aller fleste .no-domener er koblet til virksomheter registrert i Brønnøysundregistrene.

Jeg valgte derfor å gå til dataene i Enhetsregisteret, og hentet ut alle registrerte virksomheter under sektorkodene 6100 – Stats- og trygdeforvaltning, 6500 – Kommuneforvaltningen, 1100 – Statens forretningsdrift, 3900 – Statlige låneinstitutter mv.

Fra registeret klarte jeg da å filtrere ut de relevante virksomhetene med organisasjonsnummer og annen relevant informasjon. Deretter kunne jeg laste ned datasettet som regneark-vennlig fil. Ei fil med rundt 2 500 virksomheter.

Listen inneholdt alle kommuner, fylkeskommuner, departementer og statlige direktorater. Samtidig inneholdt den også mange mindre organer som f.eks. mindre kommunale foretak eller kirkelige sogn.

| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | **ORGNR** | **DOMENENAVN** | **DNSSEC** | | | | |
| 692 | 874761222 | helsefremmendearbeid.no | Usignert | | | | |
| 693 | 874761222 | hefa.no | Signert | | | | |
| 694 | 874761222 | friskfaktorer.no | Usignert | | | | |
| 695 | 874761222 | xn--arbeidsmiljovervking-c0b6 | Signert | | | | |
| 696 | 874761222 | arbeidshelsen.no | Signert | | | | |
| 697 | 874761532 | okoepost.no | Signert | | | | |
| 698 | 874761532 | okokrim.no | Signert | | | | |

**Nøkkel:** Nøkkelen for å klare å lage oversikten over offentlig eide domener var å bruke organisasjonsnummeret fra Enhetsregisteret som nøkkel siden dette nummeret fantes både i domeneregisteret og der.

## Oppslag basert på organisasjonsnummer

Siden jeg visste at domeneregisteret hos Norid inneholdt et felt for organisasjonsnummer for å vise hvem som eier domenet hadde jeg et håp om at ei kjøring i en database kunne hjelpe oss.

Jeg tok derfor kontakt med Norid som forvalter registeret over .no-domener[1], og spurte:

> «Jeg vurderer å gjøre en undersøkelse som journalist rundt bruken av kryptering (https/tls) på offentlige nettsteder i Norge.
>
> I den sammenheng hadde det vært veldig fint om Norid kunne vært behjelpelige med å gjøre en direkte spørring i databasen over domeneeierskap (whois) basert på en liste organisasjonsnummer jeg kan gi dere. Er dette mulig?»

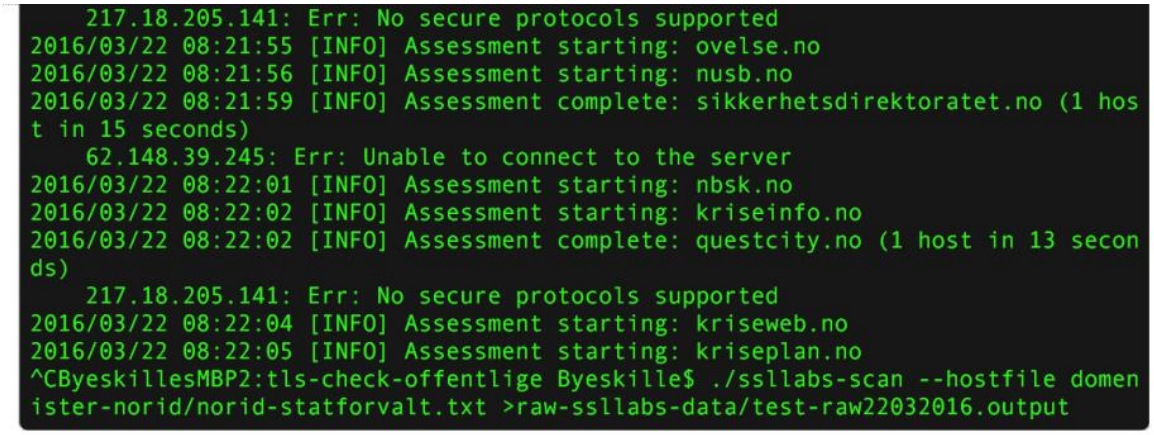
Etter litt fram og tilbake var svaret ja.

Jeg sendte over ei Excel-fil med rundt 2 500 organisasjonsnummer. Tilbake fikk jeg ei Excel-fil med 11 344 domener og hvilket organisasjonsnummer i vår oversikt det tilhørte. Norid hadde også lagt med info om domenet var signert med den nye sikkerhetsstandarden DNSSEC.

Med denne informasjonen kunne jeg enkelt sammenstille våre data fra Brønnøysundregistrene og Norid i et databaseprogram siden de hadde organisasjonsnumrene felles.

I tillegg til informasjonen fra Norid fikk jeg hentet ut informasjon om alle domener under .kommune.no/.herad.no fra KS og om .dep.no/.stat.no fra DSS siden de ikke ligger i Norids base. Jeg hentet også ut noen stikkprøver fra domener under .mil.no ved å lete på Google etter kjente adresser for søkemotoren. Alt dette ble slått sammen og beriket med data fra Enhetsregisteret i en Access-database. Til slutt satt jeg igjen med ei liste på 11 926 domener. Det er ikke en offisiell eller fullstendig liste over norske offentlig eide domener, men et ganske bredt og omfattende utvalg.

[1] Alle kan sjekke hvem som eier et .no-domene hos Norid via noe som kalles whois: https://www.norid.no/no/domenenavnbaser/whois/




**Kommandolinje-løsning:** En slik kommando ble kjørt fra kommandolinjen for å sjekke mange tusen domener, og deretter lagre resultatet til ei fil.

## Automatisert sjekk – hjemmelaget løsning

Som nevnt hadde jeg allerede brukt den enkle testen på SSL Labs for å sjekke meg selv og noen få enkelteksempler.

Denne testen består av ei nettside der man fyller ut hvilket nettsted man vil teste, og svaret kommer på siden vist med grafikk og tekst. Dette gjør det i seg selv ikke mulig å teste mange nettsteder fordi det da ville innebære uoverkommelig stor tidsbruk med manuell tasting og lagring av resultater.

Jeg startet derfor research rundt hvordan SSL Labs egentlig gjør testene sine. Da fant jeg ut at siden har et eget API. Et tilkoblingspunkt som svarer på programmatiske forespørsler. Dette gjør at det er mulig å skrive dataprogram som gjør den samme sjekken som den enkle nettsiden tilbyr, og som også kan lagre resultatet til filer.

SSL Labs har selv laget et veldig enkelt slikt program. En API-klient kalt ssllabs-scan som må kjøres fra kommandolinjen.

Ved hjelp av dette lille programmet kunne jeg dermed sende inn ei fil i programmet med liste over domenenavn jeg vil ha sjekket, og lagre resultatet etterpå. Dette var veldig nyttig og gjorde det mulig å automatisere testingen.

Det var likevel fortsatt et par hindre på veien.

**Det første hinderet var at testingen tok lang tid**. Maskinen vår måtte så stå i mange timer og gjennomføre tester. Om testen ble avbrutt underveis fikk programmet ikke lagret resultatene og alt som var gjort så langt gikk rett i søpla. Dermed måtte jeg dele opp listen på over 11 000 domener i flere biter for å unngå å miste for mye om internett-oppkoblingen var ustabil eller andre ting påvirket testen.

**Det andre hinderet var at testresultatene kom ut som store mengder rådata** på formen JSON med informasjon om både karakter, hvilke teknologier som hvert enkelt nettsted bruker og eventuelle kjente svakheter.

JSON-formatet er ikke akkurat det vanligste å forholde seg til for en menig journalist som egentlig ikke er datautvikler. Dermed var det litt vanskelig å telle opp hvor mange som hadde HTTPS og om de hadde riktig oppsett.

Slik ser f.eks. bare starten av JSON-rådataene ut for ett domene:

```
{
      "ipAddress": "188.166.11.188",
      "serverName": "byeskille.no-ams3",
      "statusMessage": "Ready",
      "grade": "A+",
      "gradeTrustIgnored": "A+",
      "hasWarnings": false,
      "isExceptional": true,
      "progress": 100,
      "duration": 119114,
```

Slike informasjon fikk jeg ut tusenvis på tusenvis av linjer av.

Jeg måtte derfor finne en måte å håndtere disse dataene på.

I arbeidet med å finne informasjon om API-et til SSL Labs kom jeg over en blogg fra en som jobbet som systemadministrator, og som selv hadde skrevet et skript for å følge med endringer i karakter fra SSL Labs for sine egne servere. Skriptet var laget slik at han dyttet inn disse rå-JSON-dataene og fikk ut ei linje per domene i ei tekstfil med det aller mest nødvendige (blant annet karakteren).

### ssllabs-scan på kommandolinjen

Skanningen ble gjort med følgende kommando i programmet ssllabs-scan:

```
./ssllabs-scan –
hostfile
domenelistefil.txt
>resultater/resultater-
raw22032016.output
```

**hostfile** henviser til ei liste lagret med ett domene per linje.

**>** Deretter sendes resultatet fra programmet inn i ei fil

Dette skriptet skrevet i kodespråket python virket lovende fordi det laget filer som lignet litt på csv-filer – kommaseparerte filer som enkelt kan åpnes i databaseprogrammer eller i Excel.

Jeg valgte derfor å ta utgangspunkt i dette skriptet, skrive det litt om og tilpasse det til min bruk[2] slik at det faktisk laget csv-filer for meg av den store mengden JSON-data.

Dermed fikk jeg i praksis store regneark-filer som inneholdt data for hvert domene om SSL Labs klarte å koble seg til med HTTPS, karakteren nettstedet ble gitt og informasjon om helt konkrete sikkerhetssårbarheter.

Alt sammen ble så igjen lastet inn i databaseprogrammet Access for viderebehandling. Der kunne jeg telle opp de ulike kategoriene og hvilke resultater de hadde fått.

**Resultatet var:**
Jeg startet med 11 926 domener i testen. 1 982 av domenene hadde i testperioden den 9. og 10. mars ingen aktiv webserver, og de er derfor ikke tatt med i opptellingen av HTTPS-bruk.

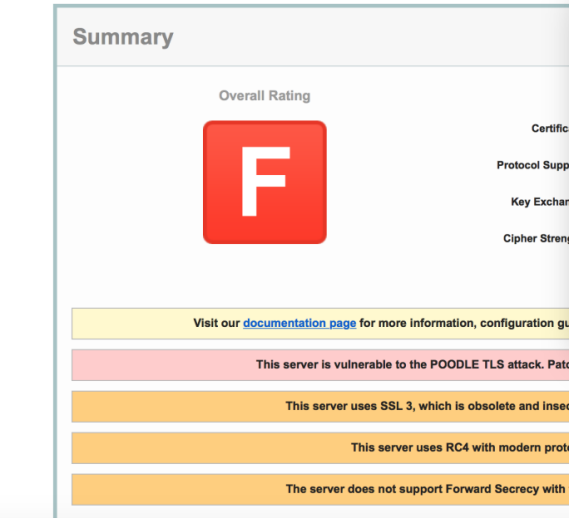
**Bare 422 av 9 944 aktive domener eid av det offentlige hadde fungerende https/tls – tilsvarer 4,2%**

Av disse 4,2 prosentene som faktisk har HTTPS fikk:

- 180 karakteren A/A-/A+ (42,7 %)
- 55 har karakteren B (13 %)
- 72 har karakteren C (17 %)
- 102 får karakteren F = stryk (24,2 %)

I tillegg har noen fått anmerkning for problemer med sertifikat-tillit, men ellers greit oppsett.

Blant nettstedene som fikk stryk i testen var det også enkelte sider som tilhørte etater de aller fleste skulle tro hadde sikkerheten på stell. F.eks. fant NRK feil knyttet til Forsvarets e-postsystemer og tipsmottak hos det norske politiet.




**Stryk-karakter:** Slik framstilles et nettsted på SSL Labs med strykkarakteren F.

Med utgangspunkt i denne gjennomgangen ble de første sakene laget. Vi intervjuet ulike eksperter om mangelen på sikker HTTPS for offentlige nettjenester, og jeg valgte å konfrontere noen etater/virksomheter som enkelt-eksempler for de som ikke klarte å holde oppdatert et godt og sikkert oppsett for sine nettsider med HTTPS.

Etisk sett var det problematisk å vise fram detaljer for den enkelte nettside som kunne ha sikkerhetssvakheter uten at de hadde fått mulighet til å rette opp. Derfor kunne jeg ikke vise fram mer enn disse få eksemplene som både fikk varsel slik at de kunne teknisk rydde opp, og som fikk svare i sakene våre.

[2] Her er min utgave av skriptet: https://gist.github.com/byeskille/397dd1d19661343f8fc3

Jeg ville likevel gå videre slik at det kom enda bedre fram hva som lå i de mange tusen testene.

## Den store oversikten

I arbeidet med de første sakene kom jeg over at det i USA er bestemt fra Det hvite hus at alle føderale etater og virksomheter skal ha nettjenestene sine på sikre HTTPS-tilkoblinger.

For å følge opp innføringen av dette kravet har myndighetene i USA derfor laget en egen nettside som jevnlig følger utviklingen for hvilke som har fått lagt inn støtte, og hvor stor andel av nettjenestene som ennå mangler.

Slik presenterer amerikanerne selv sin oversikt:
**Pulse**
**How federal government domains are meeting best practices on the web.**

Da jeg skrev de første sakene lå føderale myndigheter i USA på 40 prosent, mot Norges 4,2 prosent.

Da jeg så på disse oversiktssidene på https://pulse.cio.gov/ oppdaget jeg noe spennende helt nederst:
Built **in the open** as a collaboration between 18F and the Office of Government-wide Policy at the General Services Administration.

Hele løsningen var basert på åpen kildekode. Så et klikk unna lå hele systemet på Github for både å teste for HTTPS i USA og vise fram resultatene.

Tanken var raskt da: Kan ikke vi i NRK klare å bruke denne koden og lage vår egen versjon? Her er jo mye av grovarbeidet gjort selv om det må gjøres en del tilpasninger for bruk i Norge.

Det var ikke satt av noen dedikert utvikler på prosjektet, men jeg luftet tanken med noen kollegaer som var utviklere. De sa at det vel skulle la seg gjøre, men at det ikke var tid der og da.

Selv om jeg ikke selv er utvikler, eller har noen utdannelse eller spesielle kurs i koding, valgte jeg likevel å begynne å se på det på egenhånd.

Det ble sendt av gårde en e-post til en av de amerikanske utviklerne:

> As I see the Pulse solution are built entirely in the open I started considering to make a clone to track the Norwegian government sites. How much code would have to be changed if I try it as an experiment?

Svaret var at det nok kunne være litt jobb, men at det skulle la seg gjøre. For han visste at en tysker hadde laget en versjon for Tyskland.

## Hjelpen fra Tyskland

Jeg tok derfor en titt på den tyske versjonen – https.jetzt! Et navn som rett og slett oversatt til norsk betyr https.nå!

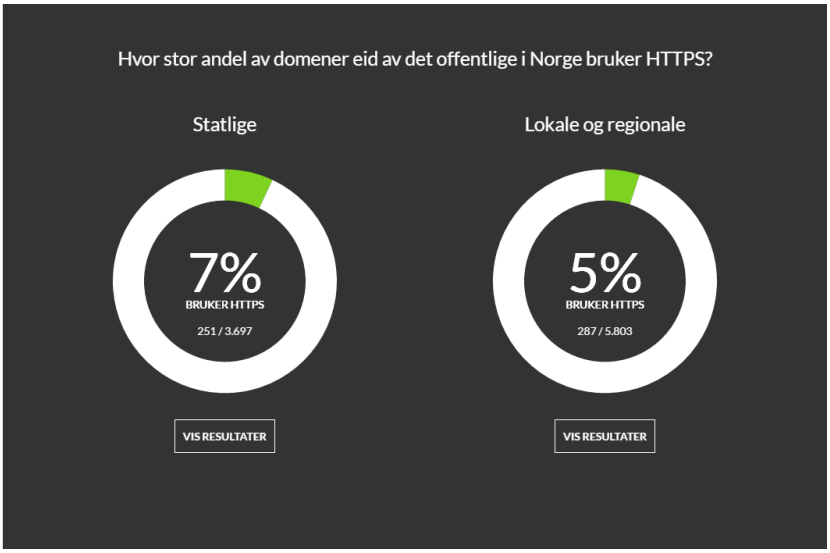
Den tyske utgaven viste seg å være mer rendyrket i den retningen vi var ute etter. Dermed valgte jeg å lage en klone eller fork som det visst heter i programmeringsverdenen.

Etter en liten stund stod jeg dog fast med en del uforståelige feilmeldinger.

Mannen bak den tyske utgaven, Maximilian Richt / @robbi5, var veldig hyggelig og hjelpsom på e-post. Så med litt hjelp til å komme over en del mystiske feilmeldinger var jeg på god vei igjen.

Til tross for en del kunnskapshull har jeg klart å lage en norsk versjon ved å tilpasse våre datasett noe og tilpasse koden for løsningen noe.

Så til slutt klarte jeg å lage en stor interaktiv oversikt over alle de tusenvis av domenene vi hadde testet.




Oversikten kalte vi **HTTPS-status Norge**
https://nrkbeta.no/https-norge/

I oversikten valgte vi etter etiske vurderinger å bare publisere om nettsteder har HTTPS – og dermed ikke legge ut informasjon om sårbarhet for kjente sikkerhetssvakheter.

Etter publisering har vi valgt å holde oversikten jevnlig oppdatert – slik tilsvarende oversikt holdes oppdatert i USA og Tyskland. Vi har derfor gjort nye skanninger av nettsider omtrent én gang i måneden det siste halve året.

NRK har da kunnet se at det sakte, men sikkert blir mer utbredt med HTTPS også i Norge:

- mai 2016: ca 5%
- august 2016: 5,7%
- september 2016: 5,9%
- november 2016: 7,4%
- desember 2016: 8,5%
- januar 2017: 8,9%

Koden for hele vår versjon av løsningen ligger også ute åpent på Github:
https://github.com/byeskille/pulse

Å lage denne oversikten hadde ikke vært mulig uten den åpne kildekoden lagt ut på nettet av 18F/GSA og @robbi5, eller hyggelige mennesker som orker svare på noen spørsmål på e-post.

## Tester også for andre teknologier

Siden arbeidet med å samle og sammenstille data for å skape en oversikt over hvilke domener som er eid av det offentlige allerede var gjort valgte vi å utnytte grunnarbeidet også til andre tester.

Vi fikk derfor i samarbeid med kilder gjennomført tester for andre nett-teknologier som påvirker sikkerheten, f.eks. DNSSEC, security headers og sårbare javascript.

Heller ikke her var alt i sin skjønneste orden for de offentlige nettstedene, og vi lagde et par mindre saker.

# KILDEARBEID OG KILDEKRITIKK

## Ekspertkilder vurderer våre undersøkelser

Sentralt i arbeidet med prosjektet var også å knytte til oss en del fagfolk som kunne vurdere undersøkelsene NRK gjorde.

Allerede tidlig ble det klart at enkelteksempler på feil oppsett av HTTPS, som f.eks. strykkarakter i SSL Labs-testen, ikke nødvendigvis overrasket fagfolkene.

Fagfolkene var mye mer opptatt av den generelle mangelen på HTTPS blant nettjenester.

Dette gjorde at det ble ekstra aktuelt å gjøre den store undersøkelsen for å prøve å dokumentere hvordan det egentlig står til for nettsteder eid av offentlige etater og virksomheter.

## Kontakt med de som hadde feil i systemene sine

Et annet moment som var med på å påvirke hvordan vi håndterte saken var at fagfolk var svært opptatt av at ingen etater eller virksomheter måtte få hengt ut direkte sikkerhetsfeil uten at feilene var rettet, eller i alle fall at de det gjaldt hadde fått god anledning til å rette opp.

Vi valgte derfor å kontakte alle vi skulle bruke som eksempler i god tid.

Virksomhetene/etatene fikk vite hva NRK hadde funnet ut, hvordan vi hadde funnet det ut og hvordan vi så for oss å omtale det. Sammen med informasjonen fikk de også utkast til noen sentrale spørsmål.

Alle de som ble brukt som eksempler i første runde med publisering tok henvendelsen fra NRK veldig seriøst. Det ble stort sett svart raskt med beskjed om at de nå tok dette videre internt med fagfolk innen data, og at de måtte avvente å svare på spørsmål til de hadde fått tilbakemelding fra fagfolkene.

Deretter var det flere som etter svært kort tid hadde fått rettet opp de tekniske svakhetene.

Forsvaret som hadde utdaterte oppsett av en nettportal for lesing av e-post utenfor det vanlige nettverket i Forsvaret valgte faktisk å ta ned hele e-postløsningen i flere døgn, kort tid etter å ha fått henvendelse fra NRK.

Jeg fikk som journalist også svar på mine spørsmål.

Siden litt av målet med dette prosjektet var å bidra litt positivt, fant jeg ut at jeg ville prøve noe nytt.

Jeg valgte å si fra til absolutt alle de som i vår test hadde kommet ut med konkrete feil i oppsettet av HTTPS – selv om de ikke ble nevnt i noen av sakene.

Det ble derfor laget over 100 e-poster med informasjon om at domene de eide hadde fått karakteren F i testen fra SSL Labs, hva dette betød og hvor de kunne finne mer informasjon.

Disse e-postene sendte jeg så ut samtidig som sakene gikk ut på nrk.no.

En slik framgangsmåte gjorde at jeg var noe nervøs på reaksjonen. Ville NRK få en haug med sure svar om at vi holdt på med noe vi ikke hadde greie på? Jeg ble derfor litt overrasket da det i stedet trillet inn takkebrev etter takkebrev. Både ledere i kommuner og fagfolk i IT-avdelinger var tydelig veldig takknemlige for at vi sa fra slik at de kunne se på noe de selv kanskje ikke var klar over.

## Kontakt med myndighetene

Ansvaret for dårlig IT-sikkerhet ved nettsteder eid av det offentlige er bredt og vidt fordelt. Domene i listen jeg laget tilhører alt fra departementer, direktorater og statlige sykehus til små kommuner eller til og med kirkelige menigheter.

Dette gjør at det til en viss grad er vanskelig å finne ett naturlig kontaktpunkt som kan svare i journalistikken.

Vi valgte her å legge fokuset på Direktoratet for forvaltning og IKT (Difi) siden de lager og forvalter standarder og krav til norske offentlige virksomheter for datasystemer[3]. Hvis Norge skulle få et lignende krav som i USA var det stor sannsynlighet for at de ville bli involvert.

Difi svarte i de første sakene og uttrykte at de nok helst hadde sett bedre resultat i denne typen tester, men at de egentlig mener kravene satt til offentlige etater og virksomheter for hvordan de skal drive sine nettsteder og nettjenester er gode nok. De ville dog vurdere dem for framtiden.[4]

Det vakte likevel også litt oppsikt blant noen av fagfolkene vi hadde snakket med, da en avdelingsdirektør i Difi sa dette til NRK:
– Det er ikke er noe poeng med HTTPS der det ikke er nødvendig. Det gjør det både dyrt og vanskeligere.

[3] IT-standarder for offentlig sektor – https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder
[4] Etter publisering av NRKs undersøkelser har Difi publisert en tabell med informasjon om at de har gjort en egen lignende test, men da bare av 64 nettjenester https://kvalitet.difi.no/artikkel/2015/11/32-tjenester-med-sensitiv-informasjon-er-kryptert

Blant annet var en annen offentlig myndighet med rådgiveransvar for IT-sikkerhet, Nasjonal sikkerhetsmyndighet, tydelige på at de helst så HTTPS brukt så bredt som mulig på internett.

At ansvaret for IT-sikkerhet i det offentlige var bredt fordelt oppdaget vi også da vi etter en stund fikk tips fra en av kildene vi hadde snakket med underveis.

Justisdepartementet hadde visst tatt tak i saken etter våre første saker. Ved å søke innsyn i dokumenter fra Offentlig Elektronisk Postjournal (OEP) fant vi ut at fagavdelingen i departementet i et brev[5] med henvisning til NRKs saker hadde bedt Nasjonal sikkerhetsmyndighet (NSM) utrede et krav om HTTPS for alle offentlige nettsteder i Norge.

Denne utredningen fra NSM endte med en tydelig anbefaling om at HTTPS burde innføres i Norge som IT-standard på samme måte som de hadde i USA. I desember ble det også klart at Difi nå ligger an til å ta inn teknologien som en standard[6] for all offentlig IT i Norge i den så kalte Referansekatalogen[7].

## Kildekritikk knyttet til datagrunnlaget

Siden denne sjekken aldri var gjort før fantes det heller ikke noen oversikt over hvilke nettsteder det offentlige driver i Norge.

NRK måtte derfor lage vår egen.

Dette måtte vi også ta med i den kildekritiske vurderingen.
For hadde vi egentlig fått et representativt svar med våre tester?
Var dette faktisk de offentlige nettstedene i Norge?

Vi måtte være kildekritiske til datagrunnlaget, og slik vi vurderte det var dette så langt det var mulig å komme med den informasjonen vi har.

Praktisk talt alle domenene vi har tatt med er faktisk offisielt registrert på en offentlig etat eller virksomhet i Norge. Samtidig kan vi ikke si at vi har fått med absolutt alle. Blant annet har vi ikke sjekket for domener registrert i de internasjonale domeneregistrene, men bare .no-domener.

Det kan også sies at datagrunnlaget er veldig bredt. Listen inneholder alt fra Statsministerens kontor til menigheten i et lite sted i Nord-Norge. Dette har vi valgt å være åpne om, og vi har også skilt mellom statlige og lokale/regionale virksomheter da vi laget vår interaktive og søkbare oversikt.

[5] Brev fra Justisdepartementet – oppdrag til NSM sikker tilkobling HTTPS
[6] https://www.nrk.no/dokumentar/ny-standard-for-sikrere-offentlige-nettsider-1.13279370
[7] https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/referansekatalogen

## Åpenhet om metode

Et annet valg vi tok knyttet til kildekritikk var å være veldig åpne om metodene bak undersøkelsen.

Vi har i to bloggposter på NRKbeta[8] beskrevet hvordan undersøkelsene er gjennomført, hvilke verktøy vi har brukt og hva som er grunnlaget.

Dette gjorde vi fordi vi mener det er viktig at eventuelle feil kan bli påpekt, også av publikum. Det sitter mange kunnskapsrike lesere der ute som gjerne bidrar, og vi har fra tidligere god erfaring med slik åpenhet.

Siden det her også ble skapt datakode, basert på allerede åpent delt datakode, har vi valgt å dele også NRKs datakode. Dette gjør at andre kan bygge videre på vårt arbeid, og at med kunnskap kan bidra med eventuelle rettelser også til datakoden.

# UTFORDRINGER

De største utfordringene var nok at hele prosjektet ble gjort av en journalist som egentlig ikke er utvikler.

Dermed ble det en del knoting med kode og uforståelige feil ved kjøringer.

Underveis har læringskurven vært svært bratt. Alt fra å kunne kjøre en test av mange hundre domener i slengen fra en kommandolinje, til å forstå hva som egentlig er problemet med at en webserver ikke er oppdatert og er sårbar for den så kalte Heartbleed-sårbarheten.

Men med tid, tålmodighet og litt hjelp fra hyggelige kolleger med litt mer teknisk bakgrunn kom vi i mål.

[8] NRKbeta er NRKs sandkasse for teknologi og nye medier, både et lite redaksjonelt miljø for eksperimentering og et publiseringssted for mer teknologifokusert innhold

# KONSEKVENSER

NRKs saker førte i første omgang til økt fokus på nettsikkerhet.

Blant de rundt 100 som fikk beskjed fra NRK om at de hadde et HTTPS-oppsett med strykkarakter hadde over halvparten rettet opp rundt en måned etter.

Andelen offentlige nettsteder med HTTPS har økt sakte, men sikkert. Ved første test lå den på i overkant av 4 prosent. I begynnelsen av januar 2017 hadde dette økt til nesten 9 prosent. NRK fortsetter å oppdaterer oversikten på https://nrkbeta.no/https-norge/ månedlig.

Justis- og beredskapsdepartementet fikk en vurdering fra Nasjonal sikkerhetsmyndighet der det klart og tydelig ble anbefalt å innføre et krav om at alle offentlige nettjenester skal ha HTTPS.

Departementet har nå anbefalingen fra NSM til vurdering, og saken er enn så lenge «under behandling».

I desember ble det også klart at Difi nå ligger an til å ta inn teknologien som en IT-standard i Norge i den så kalte Referansekatalogen. Dermed kan det bli lignende krav som i USA.

Fagfolkene som jobber med innføring av HTTPS for alle føderale organer i USA bruker nå Norge som eksempel på et land som kanskje også innfører liknende krav[9] i sine presentasjoner på konferanser og i møter internt i forvaltningen hvor de viser til NRKs saker som referanse.

# TAKK TIL

Det redaksjonelle miljøet i NRK Dokumentar og samfunn, og da Digital undersøkende redaksjon spesielt, fortjener en stor takk. Et godt samarbeidsklima og hjelp fra gode kolleger er viktig for å dra i land litt uvanlige prosjekter. I dette prosjektet skal spesielt Ellen Borge Kristoffersen og Ståle Hansen takkes for bidrag som var viktige inn mot publisering.

Jeg må også takke for god støtte og bistand fra de som faktisk kan datakode i NRK, utviklerne. Selv om det ikke ble satt av tid til det fikk jeg viktig hjelp fra kollega Stian Lund Johansen underveis da jeg egentlig satt ganske så fast inne i python-koden. Takk for at jeg får lov til å plage dere i Digital historieutvikling innimellom.

Også Henrik Lied i NRKbeta fortjener en takk for støtte og hjelp i innspurten mot publisering av den interaktive oversikten.

[9] https://www.usenix.org/sites/default/files/conference/protected-files/security16_slides_mill.pdf#page=113