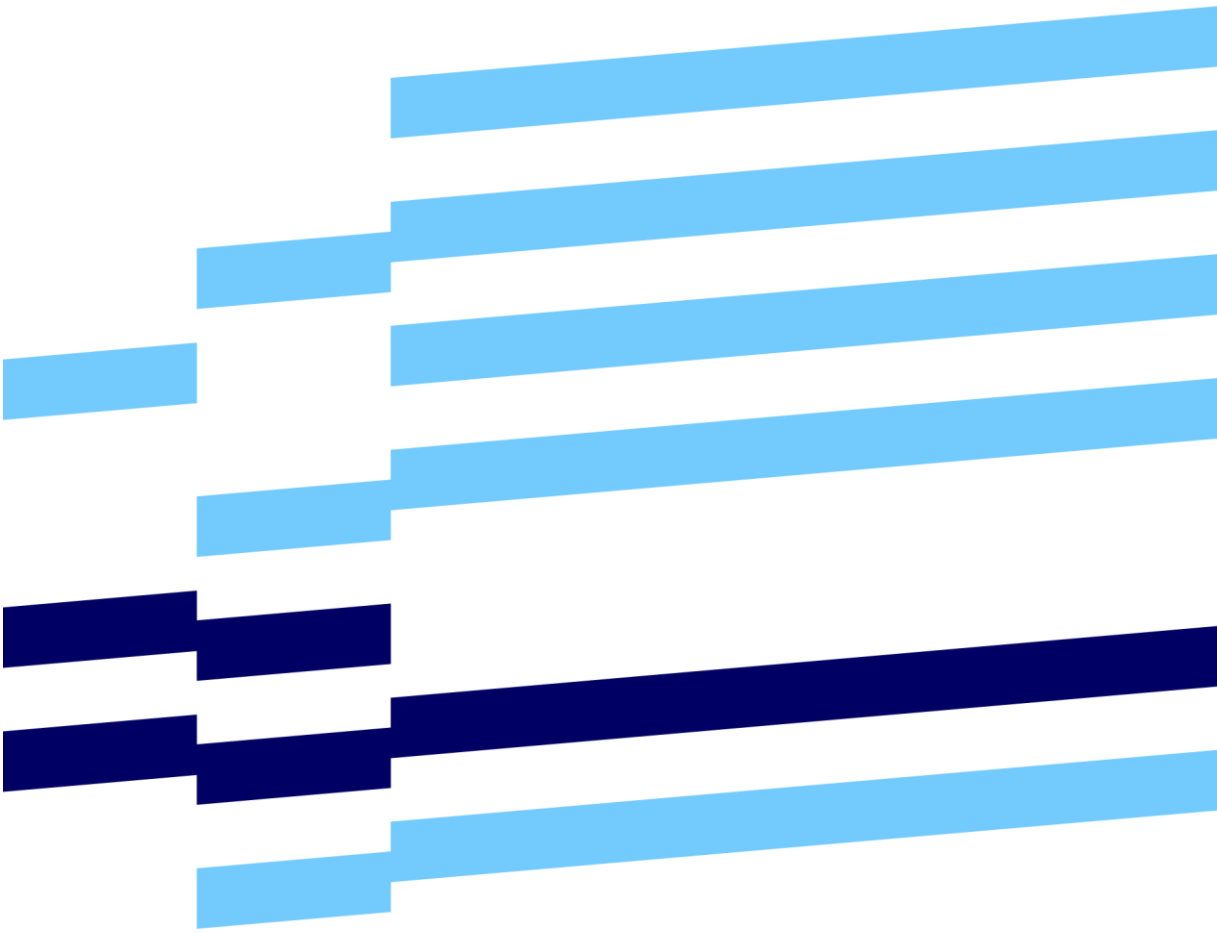
Difi
Direktoratet for
forvaltning og ikt

Utredning av HTTPS som obligatorisk IT-standard i forvaltningen



Innhold

Forord

Kommunal- og moderniseringsdepartementet (KMD) har gitt Direktoratet for forvaltning og ikt (Difi) i oppdrag å utrede konsekvensene av å gjøre HTTPS obligatorisk for nettsteder som leveres av virksomheter i offentlig forvaltning. I dag er bruk av HTTPS en anbefalt forvaltningsstandard i Referansekatalogen for IT-standard[1].

I utredningen har Difi benyttet utredningsinstruksen[2] og de seks sentrale spørsmålene derfra som mal.

Som en del av utredningen sendte Difi ut en spørreundersøkelse til et utvalg statlige og kommunale virksomheter som har innført HTTPS. Her fikk vi innspill på både ressursbruk, kostnader ellers og erfaringer med bruk av HTTPS som er brukt i denne utredningen.

[1] Referansekatalogen for IT-standarder https://www.difi.no/referansekatalogen

[2] Utredningsinstruksen, https://www.regjeringen.no/no/dokumenter/instruks-om-utredning-av-statlige-tiltak-utredningsinstruksen/id2476518/

Sammendrag

Difi anbefaler at den eksisterende anbefalingen i referansekatalogen gjøres obligatorisk og fastsettes i forskrift.

De positive virkningene vurderes som flere og større enn de negative virkningene som i hovedsak knyttes til relativt små kostnader for hver enkelt virksomhet. I en total sammenheng for hele offentlig forvaltning vurderes kostnaden som liten til moderat. De positive virkningene er flere og viktige for både opplevd og faktisk sikkerhet på nettsteder for virksomheter i offentlig forvaltning. Uten bruk av HTTPS vil risikoen for bl.a. uvedkommende innsyn og brudd på personvernforordningen, økonomisk tap, omdømmetap og tap av tillit for virksomheter og offentlig forvaltning være betydelig større enn ved bruk av HTTPS.

I en gjennomført undersøkelse til virksomheter som har innført HTTPS, og i redegjørelser for Standardiseringsrådet, har det ikke kommet frem mange eller vesentlige negative holdninger eller negative erfaringer knyttet til bruk av HTTPS.

En eventuell ikrafttredelse av oppdatert forskrift med HTTPS, inkludert frist for innføring, vil sannsynligvis ta mellom 1-2 år. I løpet av denne tiden er det god grunn til å tro at mange flere offentlige virksomheter uansett vil innføre HTTPS på sine nettsteder som en del av den generelle tekniske utviklingen og oppgradering av systemer/infrastruktur. Med dette er det realistisk å anta at den totale kostnaden for offentlig forvaltning, knyttet spesielt til innføring av HTTPS som obligatorisk standard, vil være mindre enn det man har anslått med de nåværende tall for nettsteder som enda ikke har innført HTTPS.

Null-alternativet, HTTPS som anbefalt standard, gir et svakere signal til offentlig forvaltning om viktigheten av å bruke HTTPS enn om det fastsettes som obligatorisk standard og at det nedfelles i forskrift. Difi forutsetter at utbredelsen av HTTPS på offentlige nettsteder vil øke raskere som en følge av at forskriften om IT-standarder i offentlig forvaltning blir fulgt av alle offentlige virksomheter og HTTPS blir en obligatorisk forvaltningsstandard.

1 Hva er problemet, og hva vil vi oppnå?

Den overordnede utfordringen som gjelder for denne utredningen, er beskrevet i Digitaliseringsstrategi for offentlig sektor 2019-2025[3] fra KMD: *«Digital sikkerhet er en grunnleggende forutsetning for å opprettholde tillit til offentlig sektors IT-systemer og offentlige digitale tjenester. En vellykket digitalisering handler derfor også om å ivareta krav til sikkerhet og den enkeltes personvern på en god måte.»*

Det overordnete målet ved å bruke HTTPS som obligatorisk standard er å bidra til at IT-systemer og digitale tjenester levert av virksomheter i offentlig forvaltning har tilstrekkelig informasjonssikkerhet. Difi har i denne utredningen avgrenset problemet til å redusere risikoen for flere forskjellige sikkerhetsrelaterte hendelser knyttet til overføring av data mellom nettsted (webtjeneste) og nettleser eller andre applikasjoner.

Denne utredningen er også avgrenset til spørsmål om risikohåndteringen av overføring av data til og fra nettsteder (webtjenester) som tilhører virksomheter i offentlig forvaltning eller som brukes til tjenester som leveres av virksomheter i offentlig forvaltning. Dette omfatter både overføring av data mellom nettleser (sluttbruker) og nettsted (webtjener), og overføring av data mellom tjenester (applikasjonsgrensesnitt) som bruker hypertekstoverføringsprotokoll (HTTP).

Sikkerheten i den tekniske løsningen for hver enkelt tjeneste er en problemstilling som faller utenfor denne utredningen.

Nedenfor beskrives sentrale forhold knyttet til overføring av data i offentlig forvaltning.

1.1 Risikobilde og konsekvenser

1.1.1 Risiko knyttet til personvern

Risikoen som ble vurdert som uakseptabel for sikker datakommunikasjon fra offentlige nettsteder da HTTPS først ble anbefalt 12. september 2017, er knyttet til konfidensialitet og muligheten som uvedkommende har til å få innsyn i opplysninger som overføres fra nettsted til bruker, eller fra bruker til nettsted. Dette er en risiko som også må vurderes ved etterlevelse av personvernforordningen. Håndtering av denne risikoen har medført at mange virksomheter har tatt i bruk kryptert overføring (HTTPS) kun for deler av nettstedene de har ansvaret for.

Konsekvenser:

- Virksomheter kan få straffegebyr for brudd på personvernforordningen
- Virksomheten kan få omdømmetap og redusert tillit
- Data på avveie og uberettiget innsyn kan redusere brukeres tillit til offentlig forvaltning

[3] Se kapittel 9 i Digitaliseringsstrategi for offentlig sektor 2019-2025

1.1.2 Endring av data

En risiko, som etter at HTTPS ble vedtatt som anbefalt standard i Referansekatalogen har blitt betydelig høyere, er at uvedkommende endrer data som overføres når den sendes fra et nettsted til brukeren, eller fra brukeren til et nettsted. Dette kan en tredjepart utnytte til å gjennomføre phishing-angrep, hvor den forfalskede informasjonen ser ut som den kommer fra en virksomhet i offentlig forvaltning. Dette kan utnyttes til å angripe brukerens maskin med ondartet programvare.

Konsekvenser:

- Brukere av en tjeneste kan lide økonomisk tap.
- Brukere av en tjeneste kan oppleve konfidensialitetsbrudd for informasjon lagret på egen maskin.
- Virksomheten som har ansvar for tjenesten, kan få omdømmetap og redusert tillit.
- I noen tilfeller kan slike hendelser redusere brukeres tillit til offentlig forvaltning.

1.1.3 Tilgang

En tredje risiko er knyttet til tilgjengelighet. De dominerende produsentene av nettleserprogram har vurdert at nettsteder som ikke bruker kryptering for å sikre overføring av data mellom nettsted og nettleser ved bruk av kommunikasjonsprotokollen HTTPS vil merkes som usikre. Nettlesere har i økende grad begynt å sperre tilgang til nettsted som ikke bruker HTTPS.

Konsekvenser:

- Utilgjengelighet kan få omfattende konsekvenser for viktige samfunnstjenester.
- Virksomheten kan få omdømmetap og redusert tillit.
- Offentlig forvaltning kan få omdømmetap og redusert tillit.

1.1.4 Omfang

NRKbeta har i flere omganger undersøkt hvor stor andel av domener eid av offentlig forvaltning som bruker HTTPS. Siste undersøkelse ble utført i fjerde kvartal 2018. NRKbeta har brukt et utdrag fra det norske registeret for domenenavn (Norid AS) hvor de har identifisert 8.733 domenenavn eid av virksomheter i offentlig forvaltning. Av disse var 3.355 domenenavn registrert av statlige virksomheter. Hvilken dato dette utdraget er foretatt er ikke oppgitt. Målingen til NRKbeta i fjerde kvartal 2018 viste at 33 prosent av domenene hos statlige virksomheter brukte HTTPS og 32 prosent av domenene hos kommuner og fylkeskommuner brukte HTTPS.

Tallene fra Norid AS gir ikke en fullstendig oversikt, ettersom enkelte virksomheter i offentlig forvaltning også har registrert domenenavn i andre registre for domenenavn.

Som grunnlag for å telle domenenavn eid av virksomheter i offentlig forvaltning tok NRKbeta utgangspunkt i domenenavn registrert på organisasjonsnummer med følgende institusjonelle sektorkoder:

- 1110 Statens forretningsdrift

- 3900 Statlige låneinstitutter mv
- 6100 Statsforvaltningen
- 6500 Kommuneforvaltningen

Norid AS har oppgitt følgende tall, på forespørsel fra Difi, for disse fire sektorkodene per 9. september 2019: Totalt 15.874 domener, hvor 6.063 domener er registrert av virksomheter med sektorkodene 1110, 3900 og 6100. 9.811 domenenavn er registrert på sektorkode 6500 Kommuneforvaltningen.

I tillegg til det overnevnte er 8.076 domenenavn som er registrert av virksomheter med følgende institusjonelle sektorkoder:

- 1120 Statlig eide aksjeselskaper mv.
- 1510 Kommunale foretak med ubegrenset ansvar
- 1520 Kommunalt eide aksjeselskaper mv.
- 3100 Norges Bank

1.1.5 Usikkerhet knyttet til bruk og omfang av dagens domenenavn

Hvert av de registrerte domenenavn kan brukes til en eller flere digitale tjenester. Hvert av de registrerte domenenavnene kan også brukes til å etablere underdomener, og hvert av disse underdomenene kan brukes til en eller flere digitale tjenester.

Vi har i dag ingen oversikt over hvor mange domenenavn som hører til hver av kategoriene. Et forhold som kompliserer måling, er at mange domenenavn er satt opp med et nettsted som forteller brukere at domenenavnet ikke er i bruk.

Difi gjennomførte i juni 2019 en spørreundersøkelse hvor et av spørsmålene gjaldt hvor mange nettsteder den aktuelle virksomheten eller kommunen hadde ansvar for. Svarene oppgitt sier at en virksomhet eller kommune kan ha ansvar for alt fra ett nettsted til 150 nettsteder. Dette er i samsvar med stikkprøver tatt fra Norid. Imidlertid er det et begrenset antall virksomheter som er registrert med mer enn 100 domenenavn.

1.2 Hva slags domenenavn vil en obligatorisk bruk av HTTPS omfatte?

I forbindelse med denne utredningen er det hensiktsmessig å dele bruken av domenenavn inn i fire kategorier:

a) Domenenavn som ikke er i bruk (parkerte domener).
b) Domenenavn som kun brukes til andre digitale tjenester enn nettsider.
c) Domenenavn som kun videresender brukere til nettside på et annet domene.
d) Domenenavn som brukes for digitale tjenester som omfatter nettsteder.

Et obligatorisk krav for bruk av HTTPS vil omfatte domenenavn i kategoriene c, d og deler av kategori b som beskrevet over. Når det gjelder domenenavn som kun videresender brukere til en nettside på et annet domene (kategori c) er det som regel snakk om svært enkle tekniske løsninger. Vi tar utgangspunkt i at risikovurderingen i de fleste tilfeller vil gjøre det akseptabelt å benytte enkleste type sertifikater. I færre tilfeller kan det vurderes å bruke

sertifikater med mer funksjonalitet, høyere sikkerhet og som har en høyere kostnad. Det er derfor domenenavn som brukes for digitale tjenester som omfatter nettsteder (kategori d), som vil medføre den vesentligste andelen av kostnader ved dette sikkerhetstiltaket.

Når det gjelder domenenavn som kun brukes til andre digitale tjenester enn nettsider (kategori b) vil det være hensiktsmessig at et obligatorisk krav om bruk av HTTPS gjelder for domenenavn som brukes til tjenester som benytter HTTPS for kommunikasjon mellom for eksempel applikasjoner. Denne utredningen har ikke kartlagt hvor mange domenenavn dette gjelder og hvilke risikovurderinger som bør legges til grunn for valg av sertifikater til disse løsningene.

1.3 Eksisterende anbefaling knyttet til bruk av HTTPS

Referansekatalogen er en oversikt over IT-standarder som er obligatoriske eller anbefalte for offentlig sektor.

Referansekatalogen for IT-standarder har hatt en anbefaling om bruk av HTTPS siden 12. september 2017. En oppdatert vurdering av risikobildet som er kort beskrevet i avsnittene over har medført at anbefalingen om bruk av HTTPS ble oppdatert 26. oktober 2018.

Det samme risikobildet er årsaken til at HTTPS utredes som en aktuell obligatorisk forvaltningsstandard. Et tiltak som skal bidra til at IT-systemer og digitale tjenester levert av virksomheter i offentlig forvaltning har tilstrekkelig informasjonssikkerhet.

2 Hvilke tiltak er relevante for innføring av HTTPS som obligatorisk standard?

Tiltaket som er relevant å gjennomføre og som utredes er å gjøre HTTPS, som i dag er en anbefalt forvaltningsstandard i referansekatalogen, om til en obligatorisk forvaltningsstandard.

Forvaltningsstandarden består av flere tekniske standarder som er fastsatt av Internet Engineering Task Force (IETF) som er en åpen internasjonal organisasjon. HTTPS er en av de tekniske standardene.

Alternativet til ikke å gjøre HTTPS til en obligatorisk standard er null-alternativet, dvs. ikke å gjøre noen endring fra dagens anbefaling, og at HTTPS fortsetter som en anbefalt forvaltningsstandard.

Difi legger til grunn at hastigheten på den tekniske utviklingen fører til at en detaljert regulering av tekniske sikkerhetstiltak raskt blir utdatert. Standarder som har god aksept i markedet og vurderes som stabile teknologier kan være relevante som obligatoriske standarder.

For å underbygge argumentasjonen om å gjøre HTTPS til en obligatorisk forvaltningsstandard tar vi i denne utredningen utgangspunkt i to veiledere publisert av Nasjonal sikkerhetsmyndighet (NSM). Veilederne ble sist oppdatert høsten 2016.

- IT-veiledning for ugraderte systemer nr. 14 (U-14): Sikring av kommunikasjon med TLS[4]
- IT-veiledning for ugraderte systemer nr. 15 (U-15): Hypertext Transport Protocol Secure[5]

Nedenfor gjennomgås de tekniske standardene som forvaltningsstandarden fastsatt av Internet Engineering Task Force (IETF) består av.

2.1 Transport Layer Security (TLS)

Transport Layer Security (TLS) er en kommunikasjonsprotokoll som benytter kryptering. Den er beskrevet i NSMs veileder U-14 og brukes av mange forskjellige tjenester. TLS gir mulighet for bruk av forskjellige krypteringsmekanismer. Som kommunikasjonsprotokoll er TLS relativt stabil og kan brukes i regulatoriske tiltak, men anbefalinger om hvilke krypteringsmekanismer som bør brukes kan raskt endres. Kommunikasjonsprotokollen TLS har stor markedsaksept.

De to eldste versjonene av TLS vil sannsynligvis trekkes tilbake i nær fremtid, og dagens anbefaling i Referansekatalogen gjelder derfor kun TLS versjon 1.2 og versjon 1.3.

[4] Sikring av kommunikasjon med TLS

[5] Hypertext Transport Protocol Secure

2.2 Hypertext Transport Protocol (HTTP)

Denne tekniske standarden er grunnleggende for overføring av data mellom nettsted (tjeneste) og nettleser (bruker), og kan ikke velges bort. Den eldste versjonen det er aktuelt å anbefale, HTTP/1.1 tilbys av så godt som alle nettsteder. Det er denne versjonen som er lagt til grunn for dagens anbefalte forvaltningsstandard. Den nyeste versjonen, HTTP/2, som kom i 2015 støttes av alle de store nettleserprodusentene, og krever i praksis at overføring av data er sikret med TLS. Når det gjelder markedsaksept støtter 4 av 10 nettsteder denne versjonen i dag. HTTP/2 er langt mer effektiv en HTTP/1.1 og det er derfor grunn til å anta at den eldste versjonen gradvis vil bli utfaset. Det er vanskelig å anslå tidshorisonten for når HTTP/1.1 kan tas ut av anbefalinger. En nyere versjon, HTTP/3, er under utvikling og hvilken effekt dette vil ha for utbredelsen av de nye versjonene er usikkert. Det er derfor ikke grunnlag for å foreslå HTTP/2 som en del av en forvaltningsstandard.

2.3 Hypertext Transport Protocol Secure (HTTPS)

Den tekniske standarden som beskriver hvordan den usikrede protokollen HTTP skal sikres ved bruk av TLS heter Hypertext Transport Protocol Secure (HTTPS) og er beskrevet i NSMs veileder U-15[6] kapitlene 1, 2 og 3.1 til 3.3. Oppsummert er HTTPS en sikrere utgave av HTTP som tilbyr autentisering og kryptering av kommunikasjonsprotokollen HTTP.

Når det gjelder markedsaksept legger vi til grunn at mer enn halvparten av alle offentlig tilgjengelige nettsted bruker HTTPS, og trenden er at flere nettsteder tar denne protokollen i bruk. Internasjonal utbredelse av protokollene beskrives mer utfyllende i kapittel 2.7.

2.4 HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) er en enkel teknisk standard som har til formål å instruere nettlesere og apper at et nettsted i fremtiden utelukkende skal kontaktes med bruk av HTTPS. Standarden er beskrevet i NSMs veileder U-15 i kapittel 3.4.

Denne standarden reduserer risikoen for at et mellomledd kan gripe inn i kommunikasjonen mellom nettleser og nettsted for å forsøke å etablere en usikret (ukryptert) forbindelse. Standarden har en lav markedsaksept, men dette kan skyldes at en del virksomheter aksepterer risikoen det medfører å ha et nettsted med innhold som kun delvis er sikret (blandet innhold).

Dersom det skal være obligatorisk å bruke HTTPS er det ikke ønskelig med blandet innhold. I høringen før behandling av forslaget til HTTPS som forvaltningsstandard i Standardiseringsrådet ble det påpekt at det kan være ønskelig å skru av HSTS i perioder man samler statistikk.

---

[6] Hypertext Transport Protocol Secure

2.5 HTTP Public Key Pinning (HPKP)

HTTP Public Key Pinning (HPKP) er en teknisk standard (RFC7469) som binder nettstedet mot et sertifikat. Standarden er omtalt i NSMs veileder U-15 kapittel 3.7, men etter siste revisjon av denne veilederen er det funnet svakheter i løsningen og den støttes ikke lenger av de største nettleserprodusentene. HPKP er derfor ikke en del av gjeldende anbefaling i referansekatalogen.

2.6 Certification Authority Authorization (CAA)

Certification Authority Authorization (CAA) er en teknisk standard (RFC6844) som eier av et domene kan benytte for å angi hvilke sertifikatutstedere som er autorisert til å utstede sertifikater for domenet. Dette reduserer risiko for at sertifikater blir utstedt på feil grunnlag. Sertifikatutstedere som er medlemmer av organisasjonen CA/Browser Forum er forpliktet til å følge denne standarden.

Standarden CAA har fått økende oppmerksomhet etter at standarden HPKP ikke lenger støttes av de største nettleserprodusentene, men den har etter vår vurdering ikke fått tilstrekkelig marksedsaksept til å være aktuell som en del av en obligatorisk forvaltningsstandard.

2.7 Utbredelsen av tiltakene internasjonalt

Internasjonalt er HTTPS allerede vel utprøvd og nedenfor beskrives en kort status på internasjonal utbredelse. Tallene gir grunnlag for god trygghet i de tekniske løsningene.

HTTPS: 56,1 prosent av alle nettsted har HTTPS som standard (77,1 prosent av topp 100.000 rangert av Alexa.com).[7] Her brukes «alle» som en antagelse etter at omkring 10 millioner nettsted er testet. Statistikken er hentet ut 12. november 2019. Mer enn halvparten av nettstedene som er testet bruker HTTPS, og for nettsted som har høyt trafikkvolum er andelen nettsted som bruker HTTPS høyere. Av de 100.000 nettstedene som rangeres med høyest trafikk av Alexa.com bruker tre av fire nettsted HTTPS.

HSTS: 11,5 prosent av alle nettsted bruker HSTS (21,6 prosent av topp 100.000 rangert av Alexa.com).[8] Den lave utbredelsen skyldes antagelig at virksomhetene aksepterer blandet innhold. For nettsted som har høyt trafikkvolum er andelen som bruker HSTS høyere.

HTTP/2: 41,7 prosent av alle nettsted tilbyr HTTP/2 (50 prosent av topp 100.000 rangert av Alexa.com).[9] Fire av ti nettsted er tilgjengelig med protokollen HTTP/2. Det er kun nettsted som bruker HTTPS som tilbyr denne versjonen av HTTP.

---

[7] Kilde: https://w3techs.com/technologies/breakdown/ce-httpsdefault/ranking (dato 12.11.2019)

[8] Kilde: https://w3techs.com/technologies/breakdown/ce-hsts/ranking (dato 12.11.2019)

[9] Kilde: https://w3techs.com/technologies/breakdown/ce-http2/ranking (dato 12.11.2019)

2.7.1 Eksempler på regulering i andre land

De følgende to eksempler er det nyeste og det eldste eksempel på relevant regulering i andre land som gjelder nettsteder tilhørende offentlig sektor vi kjenner til.

Danmark

I Danmark har Styregruppen for den nationale cyber- og informationssikkerhedsstrategi publisert tekniske minimumskrav for statlige myndigheter[10]. Dette omfatter et krav om at all trafikk til hjemmesider skal krypteres og det skal anvendes minst TLS versjon 1.2. Dette vil si at det skal brukes HTTPS. Kravet gjelder fra 1. januar 2020.

USA

I USA ble det gjennom Memorandum M-15-13[11] innført krav om at alle føderale nettsted skal bruke HTTPS med HSTS. Kravet har vært gjeldende fra 31. januar 2016.

3 Hvilke prinsipielle spørsmål reiser tiltaket om å innføre HTTPS som obligatorisk standard?

Vi kan se tre mulige prinsipielle spørsmål som reises i spørsmålet om å innføre HTTPS som obligatorisk standard

1. **Vil HTTPS ta hensyn til personvern og privatlivets fred?** Som beskrevet i kapittel 1.1. anses bruken av HTTPS på nettsteder som bruk av personvernøkende teknologi, og økt personvern er ønskelig. Samtidig vil bruken av HTTPS medføre begrensninger i muligheten til å kommunisere anonymt. For å starte kryptert samband må den ene parten bruke et sertifikat, og det kan i praksis medføre at denne parten ikke kan være anonym. Ettersom det i dette tilfellet dreier seg om virksomheter i offentlig forvaltning, er det imidlertid lite sannsynlig at virksomheter har behov for å være anonyme.

2. **Er det miljøhensyn å ta knyttet til HTTPS?** Kryptering medfører i seg selv energibruk på grunn av økt prosesseringsbehov i systemene som utfører dette. Motvekten er at ny teknologi, i dette tilfellet HTTP/2 som i praksis forutsetter bruk av kryptering, vil gi en innsparing av energibruk som er like stor eller større enn energien som brukes til kryptering.

3. **Vil HTTPS medføre kostnader for sluttbrukeren?** Dette tiltaket medfører ingen nye kostnader for sluttbrukeren. Kostnaden for innføring av HTTPS på offentlige nettsteder vil være hos virksomhetene.

---

[10] Se: https://sikkerdigital.dk/media/10946/tekniske-minimumskrav.pdf (datert 30.09.2019)

[11] Se https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2015/m-15-13.pdf (datert 8. juni 2015)

4 Hva er de positive og negative virkningene av å innføre HTTPS som obligatorisk standard?

4.1 Positive virkninger ved innføring av HTTPS som obligatorisk standard

De positive virkningene av tiltaket med å innføre HTTPS som en obligatorisk standard er:

- Redusert risiko for forskjellige typer sikkerhetshendelser, jf. beskrivelsen i punkt 1.1.
- Virksomhetene som tar i bruk HTTPS vil være forberedt til å ta i bruk den nyeste versjon av standarden for å overføre data mellom nettsteder og nettlesere (HTTP/2).
- Nettstedene etterlever den foreslåtte forvaltningsstandarden ved å unngå de negative virkningene som følger av at nye versjoner av nettlesere forventer at nettstedene bruker HTTPS.

I tillegg vil tiltaket ha flere indirekte effekter, som bl.a.:

- Virksomheter i offentlig forvaltning blir bedre til å teste at nettstedene som de har ansvaret for følger forvaltningsstandarden for sikker overføring av data mellom nettsted og nettleser. Difis spørreundersøkelse knyttet til denne utredningen avdekket at flere virksomheter ikke har testet at nettstedene har etablert HTTPS. Stikkprøver Difi har gjennomført som del av undersøkelser i utredningen viser også at mange nettsteder har forsøkt å etablere sikker overføring av data, men at det er forskjellige typer mangler i etableringen av tiltaket. Den vanligste mangelen gjelder hvordan omdirigering fra HTTP til HTTPS blir utført.
- Tiltaket for sikker overføring av data mellom nettsted og nettleser kan også brukes for kommunikasjon mellom nettsted og applikasjoner, og for sikker kommunikasjon med andre typer utstyr i tingenes internett.
- Hver enkelt virksomhet vil skaffe en god oversikt over hvilke domener man faktisk har registrert og hva de brukes til. En slik oversikt vil være et insentiv til mer effektiv ressursbruk, for eksempel mer kostnadseffektiv drift og endret kost/nytte-vurdering kan også føre til færre nettsteder.

4.2 Negative virkninger ved innføring av HTTPS som obligatorisk standard

Det er ikke identifisert vesentlige negative virkninger av innføring av HTTPS. Kostnader knyttet til nødvendige tilpasninger kan vurderes som en negativ virkning, men disse vurderes som små til moderate. Denne kostnaden er avhengig av teknologivalg og omfang på eksisterende tjenester.

Vi tar utgangspunkt i at nettsteder som tilhører virksomheter i staten allerede er omfattet av den gjeldende anbefalingen i Referansekatalogen for IT-standarder. Disse vil i praksis ikke få

ekstra kostnader som en følge av at anbefalingen blir fastsatt som et obligatorisk krav i en forskrift.

4.2.1 Oppfølging i kommunal sektor

Kostnaden knyttet til kravet om HTTPS som obligatorisk standard vil være størst for kommunale nettsteder. Det er 9.811 domenenavn som er registrert av virksomheter med institusjonell sektorkode 6500 (kommuneforvaltningen). Ved inngangen til 2020 vil det være 356 kommuner i Norge. For å gjøre et estimat av kostnadene knyttet til et obligatorisk krav om bruk av HTTPS, er det nødvendig å vurdere hvor mange nettsteder hver kommune har behov for. Basert på antall kommuner, fylkeskommuner og antall grunnskoler og videregående skoler i landet, vil et anslag på 3000 nettsteder for denne sektoren være tilstrekkelig. Med utgangspunkt i undersøkelsen til NRKbeta legger vi til grunn at en tredjedel av kommunale nettsteder allerede har tatt i bruk HTTPS. Dette antyder behov for å etablere HTTPS på 2000 nettsteder.

4.2.2 Oppfølging i statsforvaltningen

Det er 6.063 domener som er registrert av virksomheter med sektorkodene 1110, 3900 og 6100. Det eksisterer ikke noen samlet oversikt over hvor mange domenenavn som faktisk er i bruk for nettsteder og tjenester. Også for statsforvaltningen må det gjøres et estimat når det gjelder hvor mange nettsteder det samlet er behov for. Hver enkelt virksomhet vil som regel ha et nettsted som representerer virksomheten og noen ganger vil forskjellige underliggende enheter ha sitt eget nettsted. Flere virksomheter har også etablert et antall nettsted for selvstendige tjenester eller aktiviteter. Antall nettsteder i statsforvaltningen vil derfor være større enn antall virksomheter, og antallet vil variere over tid. Vi antar at det kan være 1500 nettsteder i statsforvaltningen og at en tredjedel allerede har tatt i bruk HTTPS. Dette antyder behov for å etablere HTTPS på 1000 nettsteder.

4.2.3 Teknisk tilrettelegging

Kostnadene for teknisk tilrettelegging av et nettsted vil variere. For nyetablerte nettsteder vil tilrettelegging i praksis ikke medføre noen ekstra kostnader når dette kravet er tatt med i anskaffelsen. For eksisterende nettsteder er kostnaden avhengig av den tekniske løsningen som er valgt for det enkelte nettstedet. Tilbakemeldinger Difi har fått i spørreundersøkelsen angir kostnader som varierer fra et par tusen kroner til 50.000 kroner per nettsted. Dersom kostnadene ved å tilpasse nettstedet vurderes som for høye vil et alternativ være å benytte seg av løsninger med mellomtjener, som fortløpende koder om kommunikasjonen fra et usikkert nettsted til å benytte HTTPS. Kostnaden for slike løsninger er avhengig av trafikkvolumet til nettstedet, men kan være en kostnadseffektiv midlertidig løsning fram til virksomheten skal anskaffe en ny løsning for nettsted.

Dersom vi antar at hver kommune i gjennomsnitt har ett nettsted som det vil koste 50.000 å tilpasse for HTTPS anslår vi at kostnad for denne typen tilpasning vil være 20 millioner kroner i kommunesektoren. For statsforvaltningen antar vi at det kan være 100 nettsteder som det vil koste 50.000 å tilpasse, det vil si 5 millioner kroner. Samlet gir det en engangskostnad på 25 millioner kroner.

4.2.4 Sertifikater

Kostnader til drift har en forutsigbar faktor knyttet til sertifikatlisenser. Omfang og kostnad for denne anskaffelsen avhenger av hvilken type sertifikat som skal benyttes, og dette vil avhenge av en risikovurdering for hvert enkelt nettsted. Gjeldende anbefaling fra NSM tilsier at det benyttes sertifikat av høyeste klasse, som også vil medføre det største volumet av sertifikater og de høyeste årlige kostnader. Dersom vi tar utgangspunkt i at det må anskaffes 3.000 sertifikater av den høyeste klassen vil dette gi en årlig utgift på 7,5 millioner kroner.

Det kan også være utgifter knyttet til etablering av rutiner for å sikre at alle tjenester har gyldige sertifikater, men dette er en funksjon som kan automatiseres og dermed er det snakk om en engangsutgift. Selve programvaren eller skriptet som utfører denne kontrollen vil være lik for alle etater og utgiften vil derfor i hovedsak være knyttet til at hver enkelt kommune og hver enkelt virksomhet i statsforvaltningen må legge inn en liste over hvilke domenenavn de til enhver tid har registrert. Vi anslår at dette arbeidet i snitt bør ta mellom ett og to dagsverk og har estimert en etableringskostnad på 7 millioner kroner. Dette er en engangskostnad.

4.2.5 Testing

Et område hvor det er utfordrende å anslå pris er kostnader til testing. Årsaken er at forskjellige tjenester vil ha ulik risikovurdering. For nettsteder med høy risiko kan det være behov for en helhetlig sikkerhetstesting som vil omfatte mange flere tiltak enn HTTPS. For andre nettsteder kan det være tilstrekkelig å gjennomføre en enkel automatisert test for å sjekke at tiltaket virker som beskrevet i standarden. Difis spørreundersøkelse avdekket at virksomheter med høye sikkerhetskrav kan bruke opptil kr.100.000,- per år for sikkerhetstesting av nettsteder, men dette er et arbeid som omfatter langt mer enn å bekrefte at sikkerhetstiltaket HTTPS virker. En test som er avgrenset til å kontrollere at HTTPS er satt opp riktig, og at sertifikatet er gyldig, bør ikke ta mer enn en arbeidstime per nettsted per år, og mindre enn dette dersom virksomheten har mange nettsteder. Kostnaden er ikke en del av denne utredningen ettersom den bør regnes som vanlig teknisk kontroll av nettsteder.

4.2.6 Totale kostnader for innføring av HTTPS som obligatorisk standard

Vårt kostnadsanslag er følgende:

Engangskostnad for å tilrettelegge eksisterende nettsteder for bruk av HTTPS: 25 millioner kr.

Engangskostnad for etablering av rutiner for å kontrollere sertifikater: 7,5 millioner kr.

Årlige kostnader for sertifikater: 7 millioner kr.

4.3 Usikkerhet knyttet til tallgrunnlaget for utredningen

I denne utredningen er det knyttet usikkerhet til estimatet av antall domenenavn som faktisk brukes til nettsteder, og hvor mange domenenavn som brukes til videresending til disse nettstedene. Vi har i denne utredningen gjort anslag basert på stikkprøver.

Det er også usikkerhet knyttet til kostnadsestimat der enkelte nettsted kan ha teknisk gjeld som må utbedres før sikkerhetstiltaket HTTPS kan etableres. Det kan dermed påløpe utgifter til annen type teknisk vedlikehold og oppgraderinger som følge av andre sårbarheter og mangler som avdekkes når man skal etablere HTTPS. Dette er utgifter som ikke kan knyttes direkte til etablering av HTTPS og som ikke omfattes av vårt kostnadsestimat.

Det er heller ikke alle kommuner og virksomheter som har tilstrekkelig god oversikt over sine egne nettsteder og domenenavn. Også dette kan medføre utgifter som ikke kan knyttes direkte til etablering av HTTPS.

5 Hvilket tiltak anbefales, og hvorfor?

Vi anbefaler at den eksisterende anbefalingen i referansekatalogen, gjeldende bruk av HTTPS, gjøres obligatorisk.

Oppsummert vurderes de positive virkningene beskrevet over som flere og større enn de negative virkningene. De positive virkningene er flere og viktige for både opplevd og faktisk sikkerhet for virksomheter i offentlig forvaltning. Kostnaden for hele offentlig forvaltning vurderes som liten til moderat. I hovedsak vil den enkelte virksomhet ha relativt små kostnader.

Uten bruk av HTTPS vil risikoen for bl.a. uvedkommende innsyn og brudd på personvernforordningen, økonomisk tap, omdømmetap og tap av tillit for virksomheter og offentlig forvaltning være betydelig større enn ved bruk av HTTPS.

I en gjennomført spørreundersøkelse til virksomheter som har innført HTTPS og i redegjørelser for Standardiseringsrådet har det ikke blitt belyst vesentlige negative holdninger eller negative erfaringer knyttet til bruk av HTTPS.

Null-alternativet, HTTPS som anbefalt standard, gir et svakere signal til offentlig forvaltning om viktigheten av å bruke HTTPS enn om det fastsettes som obligatorisk og at det nedfelles i forskrift. Difi forutsetter at forskriften om IT-standarder i offentlig forvaltning blir fulgt av alle virksomheter i offentlig forvaltning og at utbredelsen av HTTPS på offentlige nettsteder vil øke raskere og som en følge av at HTTPS blir en obligatorisk forvaltningsstandard.

6 Hva er forutsetningene for en vellykket gjennomføring?

Dersom det gis støtte til HTTPS som en obligatorisk standard må det gjennomføres en prosess for at standarden endres fra anbefalt til obligatorisk standard i forskriften om IT-standarder i offentlig forvaltning. Dette vil antagelig innebære behov for en høring av forslaget til endring i forskriften og Referansekatalogen, i tillegg til høring av forskriftsendringen i ESA/EU før endelig behandling og eventuelt beslutning.

En eventuell ikrafttredelse av oppdatert forskrift med HTTPS, inkludert frist for innføring, vil ta mellom 1-2 år, ut fra antatt saksbehandlingstid. I løpet av denne tiden er det grunn til å anta

at mange flere offentlige virksomheter vil innføre HTTPS på sine nettsteder som en del av den generelle tekniske utviklingen og oppgradering av systemer/infrastruktur. Med dette er det realistisk å anta at den totale kostnaden for offentlig forvaltning, knyttet spesielt til innføring av HTTPS som obligatorisk standard, vil være mindre enn det man har anslått med de nåværende tall for nettsteder som enda ikke har innført HTTPS.

Involvering, støtte og forankring hos sentrale virksomheter er viktig, bl.a. gjennom en behandling av det konkrete forslaget i Arkitektur- og standardiseringsrådet. I en offentlig høring vil også mange offentlige virksomheter gis anledning til å sette seg inn i forslaget og gi innspill.

Forutsetningen for en vellykket gjennomføring av implementeringen hos virksomhetene er at det gis god veiledning i hvordan de tekniske standardene skal brukes, og at det gis god veiledning i testing av at nettsted etterlever den obligatoriske standarden.