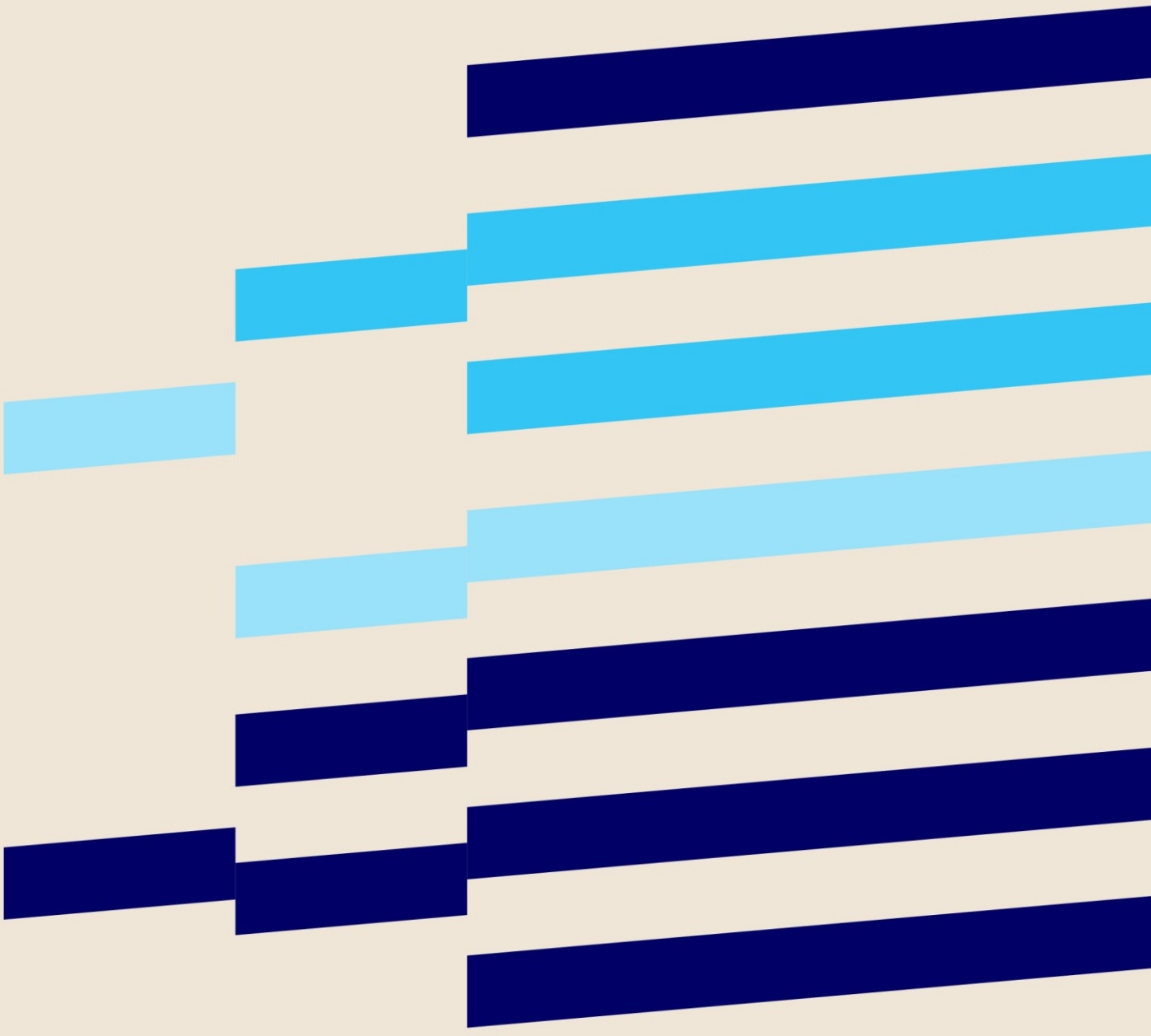
Difi
Direktoratet for
forvaltning og ikt

Difi-notat
2018:4

ISSN 1892-1728

Standarder for sikker informasjonsutveksling på Internett

Konsekvenser og anbefalinger



Forord

God informasjonssikkerhet er grunnleggende for at offentlig sektor skal kunne innovere og digitalisere på en effektiv og sikker måte, som gir tillit. God informasjonssikkerhet fordrer alt fra god internkontroll og risikohåndtering på overordnet nivå til rett bruk av tekniske standarder i tilknytning til de digitale løsningene en virksomhet benytter.

Direktoratet for forvaltning og ikt har på oppdrag fra Kommunal- og moderniserings-departementet vurdert tekniske standarder for sikker informasjonsutveksling på Internett.

Vi vil takke Nasjonal kommunikasjonsmyndighet, Uninett Norid og Nasjonal sikkerhets-myndighet for deres samarbeid. Videre vil vi takke for alle som har bidratt med høringssvar på standardene, og for de råd vi har fått av Standardiseringsrådet.

Difi står ansvarlig for innholdet i notatet. Seksjonssjef Øyvind Grinde har vært prosjektansvarlig og Petter Andreas Strøm har vært prosjektleder.

Oslo, 15.10.2018

Grete Orderud

avdelingsdirektør

Innhold

Sammendrag og konklusjon

Difi har utredet bruk av standarder som tekniske tiltak mot uønsket trafikk på Internett. Vi har i dette arbeidet hatt en dialog med Nasjonal kommunikasjonsmyndighet (Nkom), Nasjonal sikkerhetsmyndighet (NSM) og Uninett Norid for å avgrense problemstillingen og gjøre en første vurdering av enkelte standarder.

Det er ulike former for uønsket trafikk på Internett, herunder uønsket e-post, avlytting eller endring av data under overføring, angrep mot sårbare tjenester og omdirigering av trafikk. Vi har i dette arbeidet fokusert på uønsket e-post og avlytting eller endring av data under overføring. Innenfor disse områdene har vi identifisert fire problemstillinger som aktuelle for å bruke standarder som sikkerhetstiltak:

1. Sikker kommunikasjon mellom bruker og nettsted
2. Transportsikring av e-post
3. Tiltak for å motvirke falske avsendere av e-post
4. Tiltak for bedre sikring av domenenavnsystemet

I denne forbindelse har vi blant annet sett nærmere på standardene HTTPS, DANE, DMARC og DNSSEC.

Difi anbefaler at standarden for sikker kommunikasjon mellom bruker og nettsted (HTTPS) bør utredes som en obligatorisk standard for virksomheter i offentlig sektor. Dette er en moden og stabil standard, og utviklingen på markedet for nettlesere gjør at det kan oppstå negative konsekvenser for virksomheter som ikke bruker standarden ettersom flere nettlesere gir advarsler dersom brukere besøker nettsteder som ikke bruker sikker kommunikasjon.

Difi har vurdert at de tre øvrige standardene som representerer tekniske tiltak mot uønsket trafikk ikke bør fastsettes som obligatoriske tiltak på nåværende tidspunkt. For hver av standardene har dette litt forskjellige begrunnelser, men generelt er det ønskelig å få erfaringsdata fra bruk av standardene før en vurdering om de bør fastsettes som obligatoriske.

Ved ferdigstilling av dette notatet har Standardiseringsrådet behandlet tre av fire forslag og gitt råd om å fastsette disse med status som anbefalt. Behandlingen av det siste forslaget (DANE) er, etter forslag fra Difi, utsatt til neste møte i Standardiseringsrådet. Standardiseringsrådet har videre anbefalt at en av standardene, HTTPS, bør utredes videre som en obligatorisk standard.

Ved å fastsette standardene som anbefalte, vil tiltakene bli tatt i bruk og raskt bidra til bedre informasjonssikkerhet. Årets sikkerhetsmåned vil bli brukt til å informere om at standardene er anbefalt.

Difi har også sett på muligheter for forsterkende tiltak. Disse er:

- Etablering av selvbetjeningsløsning for å sjekke etterlevelse av standarder. Denne kan også benyttes til å ta ut sentral statistikk.
- Videreutvikle norge.no for å gi bedre overs over offentlige digitale tjenester

- Bruk av sertifikat knyttet til HTTPS for å opprettholde høy tillit til tjenestene. Dette kan f.eks. følges opp gjennom føring i digitaliseringsrundskrivet

Difi har ikke utredet de økonomiske og administrative konsekvensene av de forsterkende tiltakene. Dette må bli en del av beslutningsgrunnlaget før eventuell igangsettelse.

1 Innledning

1.1 Om oppdraget

I supplerende tildelingsbrev nummer to fikk Difi følgende oppdrag: «Difi bes også om å bidra til utredning av konsekvenser av et eventuelt pålegg om bruk av enkelte standarder for sikker informasjonsutveksling på internett, i samarbeid med relevante myndigheter som Nkom og NSM. Utredningen skal foreligge innen 15. oktober 2018. KMD i samarbeid med SD vil bistå med nærmere presisering av oppdraget» Oppdraget ble først beskrevet som tekniske tiltak mot uønsket trafikk på Internett, og deretter presisert i supplerende tildelingsbrev med teksten nevnt ovenfor.

1.1.1 Avgrensning og presisering av oppdraget

Samferdselsdepartementet, Kommunal- og moderniseringsdepartementet (KMD), Nkom og Difi diskuterte retning for arbeidet i et innledende møte. I møtet ble det fra departementenes side uttrykt en klar forventning om at arbeidet skulle lede til faktiske resultater og ikke bare en utredning. Vi fulgte opp med arbeidsmøter med Nkom, Uninett Norid, NSM og Difi hvor vi gjorde et utvalg av standarder for sikker informasjonsutveksling på Internett som det var naturlig å gå videre med. Disse ble presentert for KMD som ikke hadde noen merknader til utvalget av standarder. For å gi resultater utover et dokument, ble arbeid med Standardiseringsrådet og Referansekatalogen for IT-standarder pekt ut som et prioritert arbeidsområde i prosjektet.

1.2 Avgrensning og utdyping av problemstilling

1.2.1 Hva er uønsket trafikk på Internett?

Begrepet uønsket trafikk på Internett favner bredt og kan oppfattes som flertydig ettersom forskjellige virksomheter og brukere kan ha ulik oppfatning av hva som er ønsket trafikk. Det er likevel viktig å forbedre brukeres muligheter til å håndtere uønsket trafikk, for å bidra til et tryggere og mer effektivt digitalt samfunn. I dette kapittelet gir vi en kort bekrivelse av forskjellige former for uønsket trafikk på Internett og noen eksempler på risiko som forbindes med hver av disse.

Uønsket e-post

Uønsket e-post kan være reklame, forsøk på forskjellige former for bedrageri, eller forsøk på å få mottager til å åpne vedlegg med skadevare eller klikke på lenker som er knyttet til skadevare. Dette er en trussel som kalles nettfisking[1]. En ukjent andel av slike e-postmeldinger har forfalsket avsenderadresse[2].

Mørketallsundersøkelsen 2018[3] viser en kraftig vekst i «Phishing eller andre manipuleringsangrep» sammenlignet med 2016.[4] Mørketallsundersøkelsen uttaler videre at «den vanligste metode i målrettede angrep er bruk av infiserte e-postmeldinger (phishing

[1] Nettfisking omtales ofte som «phishing».

[2] Forfalsket avsenderadresse omtales også som «spoofing».

[3] Mørketallsundersøkelsen 2018, side 14. https://www.nsr-org.no/moerketall/

[4] Se figur 7 på side 15 i Mørketallsundersøkelsen 2018.

eller nettfiske)». NSMs rapport Risiko 2018[5] fremhever at det har vært en nedgang i antall tilfeller av kompromittering som følge av målrettet nettfisking[6]. «NSM anbefaler sterkt at virksomheter fortsatt fokuserer på epostsikkerhet da nettfiske fortsatt er en angrepsteknikk som kan skade virksomheten i stor grad.»[7]

Avlytting eller endring av data under overføring

En trussel som er nært beslektet med uønsket e-post er at en e-postmelding blir endret underveis mellom avsender og mottager, det vil si et såkalt mellommannsangrep. En trussel mot e-post er at uvedkommende kan lese eller endre meldingen når den er på vei gjennom Internett. En melding som endres kan brukes til å gjennomføre bedrageri eller et dataangrep.

En tilsvarende trussel gjelder kommunikasjonen mellom brukerens nettleser og forskjellige nettsteder. Selv om brukerens dialog med nettstedet ikke omfatter opplysninger hvor konfidensialitet er viktig, kan en trusselaktør utnytte tilliten brukeren har til nettstedet og endre eller legge til opplysninger som kan brukes til å gjennomføre et dataangrep. Et eksempel kan være at en trusselaktør legger inn programvare som utnytter brukerens maskin til å utvinne kryptovaluta.[8]

Difi vurderer endring av data under overføring til brukeren som en risiko som krever særlig oppmerksomhet ettersom konsekvensen ofte rammer brukeren,[9] mens det er eier av nettsted som må gjennomføre sikkerhetstiltak for å redusere denne risikoen. Enkelte leverandører av nettlesere vurderer trusselen som så alvorlig at nettleseren gir advarsel om nettsteder som ikke bruker sikker overføring av data.

Angrep mot sårbarheter i tjenester

En mye omtalt type angrep på digitale tjenester, er tjenestenektangrep[10] som ofte gjennomføres ved å sende store mengder trafikk mot tjenesten som angripes.

En annen type uønsket trafikk på Internett, er forsøk på å finne og utnytte forskjellige sårbarheter i utstyr som er koblet til Internett. Her er det som kalles tingenes internett[11] («Internet of Things» eller IoT) en stor utfordring som vil kreve oppmerksomhet i tiden fremover, og hvor det arbeides med å utvikle standarder for bedre sikkerhet.

Omdirigering av trafikk

En utfordring som er nært knyttet til uønsket trafikk på Internett, er at trafikken kan omdirigeres til feil destinasjon.

---

[5] https://nsm.stat.no/publikasjoner/rapporter/rapport-om-sikkerhetstilstanden/

[6] Målrettet nettfisking omtales ofte som «spearphishng».

[7] Mørketallsundersøkelsen 2018, side 42.

[8] «Illegitim graving etter kryptovaluta (såkalt kryptojacking) øker sterkt.» Mørketallsundersåkelsen 2018, side 42.

[9] «Flere virksomheter og enkeltpersoner benytter krypteringsløsninger for å beskytte lagrede data og digital kommunikasjon. NSM forventer at trusselaktører oftere vil angripe de endepunktene som behandler de ukrypterte dataene» NSMs IKT-risikobilde 2018, side 10. https://nsm.stat.no/publikasjoner/rapporter/helhetlig-ikt-risikobilde/

[10] Tjenestenekt kalles i denne sammenhengen også «Denial of Service».

[11] Tingenes internett omtales ofte som «Internet of Things» eller IoT.

En form for omdirigering skjer dersom systemet som opplyser om adressen til hver eneste navngitt tjeneste på Internett, domenenavnsystemet, blir manipulert. Dette kan føre til at en bruker kontakter en forfalsket tjeneste, eller at all kommunikasjon mellom tjenesten og brukeren går via et mellomledd som kan avlytte og endre innholdet av det som kommuniseres. Det er derfor ønskelig å styrke integriteten i domenenavnsystemet.

Omdirigering kan også gjøres på andre måter slik at store mengder trafikk dirigeres til feil del av Internett. Internett er et nettverk av nettverk og det er sårbarheter i mekanismene som skal styre trafikken mellom nettverkene.

1.2.2 Avgrensing

Innenfor den begrensede rammen for arbeidet som beskrives i dette notatet har vi ikke behandlet angrep mot sårbarhet i tjenester eller omdirigering av trafikk utover manipulering av domenenavnsystemet.

1.2.3 Kort beskrivelse av fire tiltak for sikker informasjonsutveksling

Sikkerhetstiltak som kan beskrives som standarder er normalt løsninger som er stabile over tid, som tilbys av flere leverandører og som kan brukes på flere plattformer. Dette gjør at tiltakene kan brukes som felles tiltak for alle IKT-systemer en virksomhet benytter.

For noen av standardene er det viktig at tilstrekkelig mange bruker standardene for at de skal ha nytteverdi.

I den innledende diskusjonen mellom Nkom, Uninett Norid, NSM og Difi identifiserte vi følgende problemstillinger som aktuelle for å bruke standarder som sikkerhetstiltak.

1. Sikker kommunikasjon mellom bruker og nettsted
2. Transportsikring av e-post
3. Tiltak for å motvirke falske avsendere av e-post
4. Tiltak for bedre sikring av domenenavnsystemet

Sikker kommunikasjon mellom bruker og nettsted

Formålet med dette tiltaket er å styrke konfidensialitet og integritet når data overføres mellom offentlige virksomheters nettsteder og brukerens nettleser. Konfidensialitet innebærer at opplysninger ikke blir kjent for uvedkommende. Integritet innebærer at opplysninger ikke blir endret utilsiktet eller endret av uvedkommende. Tiltaket har ingen virkning når det gjelder sårbarheter i selve nettstedet til en virksomhet.

Difi har allerede publisert en anbefaling for bruk av HTTPS i Referansekatalogen. Det er hensiktsmessig å oppdatere denne anbefalingen for å gjøre det helt klart at alle nettsteder alltid skal bruke sikker kommunikasjon med brukere. Forsøk på å bruke usikret kommunikasjon skal alltid omdirigeres til sikker kommunikasjon.

Usikret kommunikasjon mellom bruker og nettsted gjør det mulig for en mellommann å endre data som sendes fra bruker til nettsted. Dette kan føre til at feil opplysninger blir registrert eller det kan være et angrep på virksomhetens nettsted. Det er også lett å endre både opplysninger som vises i brukerens nettleser og å legge inn programvare som kjøres på brukerens maskin. Her vil negative konsekvenser opptre hos brukeren, mens tiltak for å

redusere risiko må gjennomføres hos den som tilbyr nettstedet. Dette er et argument for at standard bør blir obligatorisk.

Transportsikring av e-post

Formålet med dette tiltaket er å styrke konfidensialitet og integritet når data overføres mellom e-postsystemer.[12] Tiltaket har ingen virkning på sikkerheten når meldinger overføres mellom brukerens e-postleser og e-post tjenermaskinen.

Difi har allerede publisert en anbefaling for SMTP-STARTTLS[13] i Referansekatalogen. Løsningen som er anbefalt bruker sikker overføring av e-post mellom virksomhetenes e-postsystemer, og effekten av tiltaket øker med antall virksomheter som bruker standarden. Enkelte e-postapplikasjoner viser om meldinger man mottar er overført med sikker transport.

Standarden som er anbefalt i dag har en kjent sårbarhet, og Difis vurdering er at denne anbefalingen ikke bør gjøres obligatorisk. Et forslag til en oppdatert anbefaling er lagt fram for Standardiseringsrådet. Fordi det ble publisert to nye standarder for transportsikring av e-post samme uke som Standardiseringsrådet behandlet forslagene i dette notatet er behandlingen av dette tiltaket utsatt til neste møte som er 11. desember 2018. Når anbefalingen kan oppdateres til en sikrere standard kan det gjøres en ny vurdering om den oppdaterte standarden bør gjøres obligatorisk.

Tiltak for å motvirke falske avsendere av e-post

Formålet med dette tiltaket er å øke sannsynligheten for å oppdage e-postmeldinger som har forfalsket avsenderadresse i meldingshodet. Tiltaket reduserer ikke risiko for å oppdage e-postmeldinger med skadevare i vedlegg eller e-postmeldinger som inneholder lenker som er knyttet til skadevare.

Bruk av falsk avsender i e-postmeldinger kalles «spoofing» og er en av flere utfordringer knyttet til automatisk filtrering av uønsket e-post. Det er særlig viktig i tilfeller der en forfalsket avsender er brukt i den hensikt at mottager skal ha tillit til innholdet i meldingen. Når virksomheter man har tillit til bruker standardene som skal motvirke falske avsendere, kan vi ha større tillit til e-postmeldinger som sendes fra disse virksomhetene.[14] Dette kan bidra til større effektivitet.

Det er viktig å være oppmerksom på at e-postmeldinger som kommer fra adresse man ikke har etablert noe tillitsforhold til, kan representere uønsket e-post og at innholdet i meldingene kan forsøke å gi inntrykk at meldingene kommer fra en kjent avsender. Aktører som sender ut store mengder reklame og det som ofte betegnes som spam eller uønsket e-post har vært raske til selv å ta i bruk standardene som er omtalt i dette notatet. Det er derfor nødvendig at virksomhetene vurderer restrisiko og behovet for å supplere den anbefalte standarden med

[12] Det vil si når meldingen sendes ut fra e-post tjenermaskinen i avsenders virksomhet eller nettleverandør og til meldingen når fram til e-post tjenermaskinen som tilhører mottagerens virksomhet eller nettleverandør.

[13] RFC 3207 «SMTP Service Extension for Secure SMTP over Transport Layer Security» (Denne omtales også som STARTTLS, men det er mer enn en standard som bruker mekanismen STARTTLS)

[14] Det er likevel viktig å være oppmerksom på at en trusselaktør også kan sende en e-postmelding fra en brukers adresse etter å ha gjennomført et datainnbrudd.

andre tiltak mot uønsket e-post. Standarden som anbefales (DMARC) vil likevel bidra til at mottakere kan ha større tillit til e-postmeldinger som er sendt fra virksomheter i offentlig sektor.

Tiltak for bedre sikring av domenenavnsystemet

Formålet med dette tiltaket er å styrke integriteten til domenenavnsystemet. En utfordring som standarden vi anbefaler ikke løser, er konfidensialitet knyttet til navneoppslagene i domenenavnsystemet.[15]

En hovedoppgave for domenenavnsystemet (DNS) er å oversette navnet på en tjeneste, for eksempel www.regjeringen.no, med adressen til tjenesten som er nødvendig for at brukerens maskin kan kommunisere med tjenesten. Vi må forutsette at domenenavnsystemet svarer med riktig adresse. Angrep som utnytter sårbarheter i denne grunnleggende funksjonen kan utnyttes til å gjennomføre flere slags trusler hvor uønsket trafikk kun er et eksempel.

Det er laget en standard, DNSSEC, for en teknisk løsning som sikrer integriteten for denne delen av domenenavnsystemet. Difi vurderer at alle virksomheter i offentlig sektor bør bruke denne for å beskytte samfunnets grunnleggende funksjonalitet. I dag bruker virksomheter i offentlig sektor denne standarden i langt mindre grad enn den brukes av privat sektor.

1.2.4 Bruk av Referansekatalogen for IT-standarder for å iverksette tiltak

Referansekatalogen for IT-standarder er en oversikt over IT-standarder som er obligatoriske eller anbefalte for offentlig sektor. Når det gjelder begrepet «anbefalte standarder» forutsetter Difi at disse skal benyttes med mindre virksomheten har gode grunner til å la være. De obligatoriske fastsettes i «Forskrift om IT-standarder i offentlig forvaltning».

En standard kan beskrive en løsning på en eller flere sikkerhetsutfordringer. For slike sikkerhetstiltak som krever at alle parter som kommuniserer følger samme standard, vil det være effektivt om en standard blir tatt inn i Referansekatalogen. Slike standarder er gjerne stabile løsninger på kjente sikkerhetsutfordringer som det er hensiktsmessig å etablere som et fellestiltak, det vil si at tiltaket etableres på de fleste IKT-systemer i en virksomhet.

1.2.5 Bruk av forskrift for å iverksette tiltak

Når en av Referansekatalogens standarder gjøres obligatorisk skal den fastsettes i «Forskrift om IT-standarder i offentlig forvaltning». Å gjøre tekniske standarder for utveksling av informasjon via Internett obligatoriske å benytte, medvirker til at flere virksomheter etablerer tiltakene, og vi oppnår den ønskede effekten på tvers av forvaltningen. Samtidig er det viktig at dette er sikkerhetstiltak som er godt utprøvd og vil være stabile over tid. Det er også viktig å avdekke om det er andre barrierer som gjør at virksomheter ikke bruker en anbefalt standard. Dette er et argument for å la standarder ha status som anbefalt en periode før man vurderer å gjøre standarden obligatorisk.

Selv om en teknisk standard er etablert som et risikoreduserende tiltak på tvers av virksomheter vil det likevel alltid være opp til forvaltningsorganer å gjøre egne vurderinger

[15] Dette er en risiko som er knyttet til andre trusler enn uønsket trafikk, men det er viktig å være oppmerksom på at det pågår arbeid med standarder for å redusere denne typen risiko.

om risiko for sin virksomhet. At én eller flere standarder relatert til tekniske sikkerhetstiltak er obligatoriske betyr på ingen måte at restrisikoen er tilfredsstillende for virksomheter med høyere krav til sikkerhet.

1.2.6 Virkningen av tiltakene for privat sektor

Sikkerhetstiltakene beskrevet i standardene som er omtalt i dette notatet vil ha større nytteverdi når flere virksomheter tar dem i bruk. Når mange virksomheter allerede har etablert sikkerhetstiltaket, vil nytteverdien være større for den neste virksomheten som vurderer å etablere sikkerhetstiltaket.

Dersom alle virksomheter i offentlig sektor ber om og aksepterer forespørsler om sikker transport av utgående og innkommende e-postmeldinger, vil det øke nytten virksomheter i privat sektor vil ha ved å etablere dette tiltaket selv.

Dersom alle virksomheter i offentlig sektor bruker standarden som gir bedre mulighet til å avdekke e-postmeldinger med falsk avsender, vil virksomheter i privat sektor ha større nytte av å bruke denne standarden i egen virksomhet.

Difi vurderer derfor at å anbefale eller gjøre en standard obligatorisk bidrar til økt bruk av standarden også i privat sektor. Difi har ikke vurdert nytten av, eller utfordringer knyttet til, å gi pålegg om bruk av standardene i hele eller deler av privat sektor og i så fall hvilke regelverk som skal brukes til dette.

2 Etablering av fire tiltak i Referansekatalogen

Dette kapittelet oppsummerer vurderinger av tekniske tiltak mot uønsket trafikk på Internett. Alle tiltakene relaterer seg til sikring av tjenester virksomheter forvalter. Til tross for at virksomhetene forvalter disse tjenestene kan driften av disse være satt ut til eksterne tjenesteleverandører. Kostnadene av innføringen av tiltakene vil derfor være avhengig av driftsmodell for den enkelte virksomheten.

2.1 Sikker kommunikasjon mellom bruker og nettsted

HTTPS ble tatt inn i Referansekatalogen som *anbefalt* forvaltningsstandard for sikring av nettsteder 12. september 2017.[16]

Negative effekter ved bruk av usikre nettsteder inkluderer:

- Utviklingen går i retning av at nettlesere merker nettsteder som ikke bruker HTTPS som usikre.[17] Dersom offentlige tjenester merkes som usikre, er det sannsynlig at dette vil ramme brukernes tillit til tjenestene. Det kan også ramme brukernes tillit til forvaltningen som helhet.
- Noen nettlesere viser feilmeldinger om nettstedet ikke bruker sikker kommunikasjon. Slike feilmeldinger gir redusert brukervennlighet, og kan føre til redusert tilgjengelighet for tjenester som ikke er sikret. Per i dag omfatter ikke «Forskrift om universell utforming av IKT-løsninger»[18] slike feilmeldinger, noe som kan skape utfordringer for brukere med nedsatt funksjonsevne.
- HTTPS er en faktor som søkemotorer bruker for å rangere nettsteder.[19] Tjenester som ikke er sikret kan dermed bli mindre synlige i søkeresultatene, og blir da mindre brukervennlige.
- Trusselen mot usikrede nettsteder er vedvarende og man må anta at ressursbruk for håndtering av hendelser vil fortsette å være et problem.
- Når et nettsted bruker usikker kommunikasjon mot en bruker, vil brukeren utsettes for en større risiko for uønskede hendelser. Bruk av usikker kommunikasjon mellom offentlige tjenester og brukere bidrar ikke til å skape en bedre forståelse for informasjonssikkerhet i samfunnet.

2.1.1 Oppdatering av eksisterende anbefaling

Tjenesteeiere i forvaltningen har sterke insentiver til å ta i bruk HTTPS uavhengig av endringer i Referansekatalogen. Mange tjenesteeiere vil trolig ikke at deres tjenester skal merkes som usikre i nettlesere eller at kommunikasjonen mellom nettsted og bruker er usikker.

[16] https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/referansekatalogen/grunnleggende-datakommunikasjon-0

[17] https://www.blog.google/products/chrome/milestone-chrome-security-marking-http-not-secure/

[18] Forskrift om universell utforming av informasjons- og kommunikasjonsteknologiske (IKT)-løsninger

[19] https://webmasters.googleblog.com/2014/08/https-as-ranking-signal.html

Utbredelsen av HTTPS i forvaltningen er da også betydelig. Per september 2018 anslår Difi utbredelsen av HTTPS til å være opp imot 80 prosent basert på stikkprøver av offentlige tjenester.[20]

På tross av sterke insentiver til å ta i bruk HTTPS for den enkelte tjenesteeier og betydelig utbredelse av standarden, mener Difi likevel det er nødvendig å utrede forskriftsfesting av HTTPS.

Ved å gjøre HTTPS til en obligatorisk forvaltningsstandard vil vi trolig oppnå raskere og mer fullstendig utbredelse av standarden enn dersom standarden ikke gjøres obligatorisk. En raskere og mer fullstendig utbredelse av HTTPS blant forvaltningens tjenester er ønskelig for å motvirke de negative effektene ved bruk av usikker kommunikasjon mellom bruker og nettsted.

De identifiserte kostnadene ved bruk av HTTPS for forvaltningen er hovedsakelig:

- Kjøp av sertifikater. Vi anser ikke dette som kostnadsdrivende.
- Utgifter til kompetanseheving for riktig bruk av HTTPS.

Økt kompetanse hos tjenesteeierne er nødvendig for å ta i bruk standarden på den mest fordelaktige måten. Stikkprøver Difi har utført viser at mange nettsteder har implementert HTTPS med svake konfigurasjoner. Det er for eksempel god praksis å teknisk omdirigere eller oppgradere trafikk som forsøker å kontakte nettsteder på en usikker måte til å benytte HTTPS. *HTTPS redirect* og *HTTP Strict Transport Security* (HSTS) er tiltak for å oppnå dette. Av domenene Difi analyserte var det henholdsvis kun 34 prosent og 21 prosent av tjenestene med HTTPS som benyttet seg av disse funksjonene. Et viktig formål med den oppdaterte anbefalingen er å sikre god bruk av *HTTPS redirect* og *HTTPS Strict Transport Security*.

Kompetanse om riktig bruk av HTTPS er videre viktig for å unngå uønskede hendelser som følge av sertifikatfeil.

Svake konfigurasjoner av HTTPS går på bekostning av effekten av sikringstiltaket til tross for at kostnaden ved å iverksette tiltaket allerede er tatt. Sertifikatfeil kan i ytterste konsekvens gjøre tjenesten utilgjengelig for brukerne. NSM har publisert veiledninger om bruk av HTTPS[21] og TLS[22]. Dette er et viktig risikoreduserende tiltak for å motvirke svake konfigurasjoner og sertifikatfeil og vi forutsetter at disse veiledningene oppdateres som følge av at anbefalingen oppdateres.

2.1.2 Etablering av tiltak gjennom forskrift

Basert på Difis foreløpige analyser fremstår de identifiserte nyttevirkningene ved å forskriftsfeste HTTPS som større enn tiltakets kostnadsvirkninger. Standardiseringsrådet ga

[20] Vedlegg F - Liste over offentlige domener som Difi har brukt i kartleggingen av utbredelse av standardene vurdert i dette notatet.

[21] IT-veiledning for ugraderte systemer nr. 15 (U-15) «Hypertext Transport Protocol Secure» https://nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/https.pdf

[22] IT-veiledning for ugraderte systemer nr. 14 (U-14) «Sikring av kommunikasjon med TLS» https://nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/tls.pdf

råd om at det var ønskelig å ta HTTPS videre som obligatorisk forvaltningsstandard (se Vedlegg E).

For å gjøre en forvaltningsstandard obligatorisk gjennom forskrift, skal det gjennomføres en utredning av tiltaket.[23] Dette vil være en mer omfattende kartlegging og tallfesting av nytte- og kostnadsvirkninger av tiltaket. Difi vurderer å gå videre med en slik utredning.

2.2 Transportsikring av e-post

Gjeldende anbefaling for transportsikring av e-post er standarden SMTP-STARTTLS[24] og denne ble behandlet i Standardiseringsrådet 16. september 2015. Standardiseringsrådet sitt råd var å gjøre standarden midlertidig anbefalt og gå videre med en samfunnsøkonomisk analyse for å vurdere om standarden bør være obligatorisk. Difi har ikke sett det hensiktsmessig å fremme forslag om å gjøre denne anbefalingen obligatorisk nå, ettersom nye standarder har vært i sluttfasen.

Difi begrunner dette med at standarden har en kjent sårbarhet når det gjelder angrep fra mellommann, og det er derfor viktig at virksomhetene gjennomfører en risikovurdering for å håndtere restrisiko. Samtidig har det pågått arbeid med å standardisere to nye løsninger som skal gi bedre sikkerhet på dette området.

En av de nye løsningene ble publisert av IETF[25] den 10. oktober 2015 og kalles SMTP-DANE[26]. Denne er anbefalt standard for forvaltningen i Nederland og den kreves for sertifisering av sikker e-post i Tyskland. SMTP-DANE har fremdeles begrenset utbredelse internasjonalt.

Den andre løsningen ble publisert av IETF den 26. september 2018 og kalles MTA-STS[27]. Blant dem som har foreslått MTA-STS er store aktører som Google og Microsoft. Dette vil ha betydning for en vurdering av markedsaksept for de to nye løsningene.

Den 26. september 2018 ble det også publisert en ny standard, SMTP TLS Reporting[28], som er en rapporteringsmekanisme for SMTP-STARTTLS, SMT-DANE og MTA-STS som bidrar til å oppdage om systemer som bruker en eller flere av disse standardene er feil konfigurert eller om systemene er utsatt for angrep. Dette er derfor en standard som er relevant både for gjeldende anbefaling og for en mulig oppdatert anbefaling.

2.2.1 Oppdatering av eksisterende anbefaling

På grunn av at to nye standarder med stor sannsynlighet vil publiseres i nær fremtid og fordi disse vil påvirke både vurdering av markedsaksept og ordlyden i anbefalingen, har Difi utsatt behandling av dette forslaget til neste møte i Standardiseringsrådet.

---

[23] Ref. Standardiseringsrådets arbeidsmetodikk

[24] RFC 3207 «SMTP Service Extension for Secure SMTP over Transport Layer Security» (Omtales også som STARTTLS, men det er mer enn en standard som bruker mekanismen STARTTLS)

[25] Internet Engineering Task Force https://www.ietf.org/

[26] RFC 7672 «SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)» (Omtales også som DANE, men det er mer enn en standard som bruker mekanismen DANE.)

[27] RFC 8461 «SMTP MTA Strict Transport Security (MTA-STS)»

[28] RFC 4860 «SMTP TLS Reporting»

2.3 Tiltak for å motvirke falske avsendere av e-post

Det er et ønske om å redusere risiko for angrep som utnytter e-post uten at dette påvirker levering av ordinære e-postmeldinger. En faktor som kan bidra til dette er å bruke mekanismer som styrker evnen til å bekrefte at en e-postmelding kommer fra den organisasjonen som er oppgitt som avsender i meldingen. Dette vil gjøre det lettere å fange opp meldinger som har forfalsket avsender.

SPF og DKIM er to standarder som beskriver forskjellige mekanismer for å verifisere e-postavsender. DMARC er en overordnet spesifikasjon[29] som gir en virksomhet mulighet til å velge hvilke av verifiseringsmekanismene som skal benyttes, samt å informere e-postmottakere om hva som skal gjøres om e-postavsenderen ikke blir gyldig verifisert. Alternative tiltak ved verifiseringsavvik er eksempelvis at mottaker sender en rapport tilbake til eieren av avsenderdomenet og muligheten for at e-posten automatisk forkastes.

Tabellen under viser utbredelse av de tre tiltakene per september 2018 basert på en analyse Difi har utført på et utvalg offentlige tjenester.

Standard/tiltak	**Utbredelse**
SPF	76%
DKIM	35%
DMARC	24%

Årsaken til at det er DMARC som foreslås som forvaltningsstandard er at det er denne standarden som potensielt kan være en pådriver til å redusere antallet falske e-poster på Internett. Konfigurasjonsalternativene i DMARC muliggjør at virksomheter selv kan avgjøre hvor sterkt de ønsker å konfigurere dette for sine domener basert på deres behov. Resultatene fra analysen i tabellen over viser at SPF allerede har stor utbredelse i offentlig forvaltning. Dette betyr at det for mange virksomheter vil kreve lite å nyttiggjøre seg av gevinstene DMARC gir. Eksempelvis vil det for enkelte være tilstrekkelig å sette opp DMARC med kun SPF-basert verifisering av avsender, mens for andre vil det være behov for DKIM eller eventuelt begge metodene.

Hovedutfordringen er dermed å øke utbredelsen av DMARC. Difi anser nyttevirkningene ved DMARC som store. Kostnadene ved tiltaket kan derimot variere betydelig basert på ulike virksomheters kompetanse og behov. Foreløpig er utbredelsen av DMARC i forvaltningen lav.

De sentrale positive effektene som Difi identifiserte ved å ta i bruk DMARC inkluderer:

[29] IETF har publisert DMARC (RFC 7489) med status «informational» og har ikke behandlet denne som et forslag til en standard. Dette har konsekvenser for bruk av DMARC i offentlige anskaffelser, se vedlegg G i dette notatet.

- Økt tillit til e-poster som mottas fra virksomheter som har tatt i bruk DMARC da avsenderadressen verifiseres.
- Mulighet for automatisk forkasting av uønsket e-post. Reduksjon i uønskede mottatte e-poster åpner opp for en mer effektiv forvaltning. Denne effekten blir større jo flere virksomheter som benytter seg av DMARC.
- Rapporteringsmulighetene i DMARC kan ha stor verdi for virksomhetene. De kan følge med på tilfeller hvor e-poster fra deres domener ikke blir verifisert hos mottakere. Dette gir også innsikt i om andre forsøker å sende falske e-poster på vegne av virksomhetens domene.

Identifiserte kostnader ved å ta i bruk DMARC:

- Oppfølging av rapporter som genereres ved bruk av DMARC, krever driftsressurser. Disse rapportene krever oppfølging både for virksomheter som drifter e-post selv og de som har satt tjenesten ut til en ekstern leverandør. Antallet rapporter som genereres og bør følges opp, vil avhenge av for eksempel hvor strengt virksomheten har konfigurert DMARC, antallet e-poster virksomheten sender og antallet aktører virksomheten har e-postdialog med. Siden utbredelsen av DMARC foreløpig er lav i forvaltningen, og variasjonen mellom virksomhetenes behov vil være betydelig, har ikke Difi nå gjort nærmere beregninger på hvilke kostnader virksomhetene vil ha til oppfølging av slike rapporter.
- For virksomheter som har ekstern drifting av e-posttjenester antas det å være lave kostnader knyttet til å ta i bruk DMARC da de fleste e-posttilbydere allerede tilbyr disse mekanismene som konfigurasjoner i sine tjenester.[30]
- For virksomheter som har intern drifting av e-posttjenester vil det kreve noe mer konfigurering, men også dette anses det å være begrenset kostnader knyttet til.

Feil konfigurasjon av DMARC kan i ytterste konsekvens resultere i at legitime e-poster fra en virksomhet blir forkastet hos mottakere. Et viktig risikoreduserende tiltak for å hindre uønskede konfigurasjoner, vil være å tilgjengeliggjøre god veiledning som beskriver hvordan standarden kan tas i bruk av virksomhetene på en mest mulig hensiktsmessig måte.

Difi tar DMARC inn i Referansekatalogen som en *anbefalt* standard for sikker e-post i offentlig sektor. Etter hvert som flere virksomheter tar standarden i bruk vil vi få et bedre bilde av kostnadene ved å benytte standarden i forvaltningen. Det vil gi et bedre beslutningsgrunnlag for å vurdere om standarden på sikt bør gjøres obligatorisk.

2.3.1 Etablering av ny anbefaling

Standardiseringsrådet ga råd om at DMARC blir en anbefalt forvaltningsstandard (Se Vedlegg E). Difi vil publisere anbefalingen i referansekatalogen i forbindelse med NSMs arbeid med å informere om DMARC, DKIM og SPF i sikkerhetsmåneden 2018.

[30] Vedlegg A - Saksframlegg til Standardiseringsrådets møte 20180925-C

2.4 Tiltak for bedre sikkerhet i domenenavnsystemet

Domenenavnsystemet (DNS) er av vital betydning for kommunikasjon på Internett. Derfor er det viktig for de fleste tjenester at tilliten til navneoppslag er høy. Usikrede navneoppslag har kjente sårbarheter som kan utnyttes. Dette gjør også de fleste tjenester som er avhengig av navneoppslag sårbare.[31]

En nylig publisert studie[32] tilsier at det globale omfanget av omdirigering av oppslag til uønskede adresser er begrenset. Konsekvensene ved omdirigering av forvaltningens tjenester kan likevel være svært negative, både for brukerne og tjenestene som direkte rammes og for tilliten til forvaltningens tjenester som helhet.

Vi anser derfor nytteeffektene ved å sikre navneoppslag som store. DNSSEC gir direkte nytte ved å sikre navneoppslagene. Videre avhenger mange andre sikkerhetstiltak av navneoppslag eller direkte krav om at DNSSEC er tatt i bruk for domenet.

Kostnadene ved å aktivere DNSSEC for en tjenesteeier avhenger særlig av om de drifter sin egen DNS-infrastruktur eller ikke:

- For tjenesteeiere som kjøper ekstern drift av DNS-infrastrukturen, krever aktivering av DNSSEC at de benytter en leverandør som tilbyr DNSSEC og at de velger å ta tiltaket i bruk. Norid opplyser til Difi at de 10 største domeneforhandlerne ikke tar noen ekstra kostnad for å aktivere DNSSEC. Norid tar ingen kostnad knyttet til å signere et domenenavn. Registeret for norske domenenavn viser per september 2018 at 87 prosent av offentlige virksomheter har minst ett av sine domener registrert hos leverandør som tilbyr DNSSEC.
- For tjenesteeiere som drifter DNS-infrastruktur internt krever aktivering av DNSSEC kompetanseheving. Norid opplyser til Difi at de estimerer kostnaden ved en slik kompetanseheving til om lag 10 000 til 15 000 kroner per ansatt i intern driftsenhet som gis opplæring. Registeret for norske domenenavn viser per september 2018 at maksimalt 16 prosent av domener registrert på offentlige virksomheter drives med egen DNS-infrastruktur.

Stikkprøven Difi gjennomførte og opplysninger fra Norid viser at omkring 21 til 22 prosent av domenenavn registrert av virksomheter i offentlig sektor benytter seg av DNSSEC. Totalt er 58 prosent av norske domenenavn sikret med DNSSEC.

Difi anser nytteeffekten ved å ta i bruk DNSSEC som stor. Vi anser videre at kostnaden ved tiltaket er begrenset, spesielt for virksomheter som ikke drifter sin egen DNS-infrastruktur. Foreløpig er utbredelsen av DNSSEC i forvaltningen lav.

Difi mener derfor det er ønskelig å ta DNSSEC inn i Referansekatalogen som en *anbefalt* standard nå. Etter en periode som anbefalt standard er det ønskelig å vurdere om standarden skal gjøres obligatorisk.

[31] https://dypdykk.norid.no/dnssec.html

[32] https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-liu_0.pdf

2.4.1 Etablering av ny anbefaling

Standardiseringsrådet ga råd om at DNSSEC bør etableres som anbefalt forvaltningsstandard (Se Vedlegg E). Difi vil publisere den nye standarden i Referansekatalogen.

3 Muligheter for forsterkende tiltak

Difi har identifisert noen tiltak som kan være egnet for å gi bedre etterlevelse av standardene og bidra til å bevare tilliten til forvaltningen. Vi vil vurdere om disse tiltakene skal følges opp videre.

Difi har ikke utredet de økonomiske og administrative konsekvensene av de forsterkende tiltakene. Dette må bli en del av beslutningsgrunnlaget før eventuell igangsettelse.

3.1 Tjeneste for å sjekke etterlevelse av standarder

I Nederland er det etablert en offentlig tjeneste, internet.nl, hvor innbyggere og næringsliv selv kan undersøke i hvilken grad deres e-post og nettsider følger myndighetenes anbefalinger. Denne tjenesten gir også veiledning om hva som må forbedres for at e-post og nettsider skal være i samsvar med myndighetenes anbefalinger. En tilsvarende tjeneste i Norge kan bidra til å øke andelen som følger standardene, fordi det blir enklere å undersøke om en følger disse.

I kombinasjon med en oversikt over offentlige digitale tjenester, vil det være mulig å få statistikk på hvor stor andel som følger anbefalingene i referansekatalogen og forskriften om IT-standarder i offentlig forvaltning.

3.2 Oversikt over offentlige digitale tjenester

Kunnskap om etterlevelse av anbefalte og obligatoriske standarder vil være nyttig for å vurdere om det skal settes inn ytterligere sentrale virkemidler for å få opp andelen som følger anbefalingene. En oversikt eller et utvalg av offentlige digitale tjenester vil være nødvendig for å kunne måle etterlevelse av offentlige anbefalinger. Norge.no er en veiviser til offentlige tjenester på nett og har en tjenestekatalog i dag. Difi vil kunne legge til rette for at denne kan videreutvikles og benyttes som kilde ved måling av etterlevelse av anbefalinger.

3.3 Bruk av sertifikater for å opprettholde høy tillit til tjenestene

Det er viktig for tilliten til offentlig forvaltning at brukere gjenkjenner digitale tjenester som leveres av offentlig sektor og at ikke brukere forveksler tjenester levert av andre aktører med tjenester levert av offentlig sektor.

Et eksempel på hvorfor dette er viktig er at det hvert år sendes ut falske meldinger om skatteoppgjør som kan inneholde lenker til nettsider som ikke leveres av offentlig sektor. I tillegg til tekniske tiltak som skal redusere risiko for at brukere mottar slike falske meldinger, er det viktig at nettsteder som leveres fra offentlig sektor er tydelig merket.

Et element som er knyttet til den enkelte tjeneste og som er en viktig faktor når brukere identifiserer hvilken tjeneste de bruker, er domenenavnet som brukes til å adressere tjenesten på Internett. Flere land har samlet tjenestene til offentlig sektor under ett eller noen få domenenavn. Norge har gjort dette delvis med domenenavnene dep.no, kommune.no og herad.no, men de fleste domenenavn registrert av virksomheter i offentlig sektor er ikke gruppert på denne måten. Difi har ikke vurdert en omlegging av hvordan offentlig sektor bruker domenenavn som et hensiktsmessig tiltak, men vil understreke at domenene dep.no og kommune.no bidrar til å gi disse tjenestene en tydelig identitet.

Et virkemiddel som kan brukes effektivt som en følge av anbefalingen om at alle nettstedene til offentlig sektor skal bruke sikker kommunikasjon mellom brukere og nettsted (HTTPS) er at virksomhetene kan knytte et sertifikat med utvidet validering (EV-sertifikat) til nettstedet. I dagens nettlesere vil denne typen sertifikat vise en bekreftelse av virksomhetens identitet. Dette virkemiddelet er i samsvar med anbefalingen i IT-veiledning for ugraderte systemer U-14 «Sikring av kommunikasjon med TLS» utgitt av Nasjonal sikkerhetsmyndighet. Difi oppfordrer flere til å følge denne anbefalingen og at det tas opp for eksempel gjennom digitaliseringsrundskrivet.

4 Vedlegg

Vedlegg A Behandling i Standardiseringsrådet - HTTPS
Vedlegg B Behandling i Standardiseringsrådet - DANE
Vedlegg C Behandling i Standardiseringsrådet - DMARC
Vedlegg D Behandling i Standardiseringsrådet - DNSSEC
Vedlegg E Møtereferat, rådsmøte 25.september 2018
Vedlegg F Domener Difi har brukt i kartlegging av utbredelse
Vedlegg G Bruk av standardene i offentlige anskaffelser