Difi
Direktoratet for forvaltning og ikt

VEDLEGG 1

Notat

Dato:	21.8.2018	**Saksnr:**	18/00643

Til:	Rune Karlsen
Kopi:	
Fra:	Seksjon for informasjonssikkerhet
Saksbehandler:	Håkon Styri

Saksframlegg til Standardiseringsrådets møte 25.09.2018

Anbefalte standarder for sikker datakommunikasjon

Dette forslaget gjelder endring av en eksisterende anbefaling[1] som ble innført 12.09.2017.

Formålet med standarden

Den eksisterende anbefalingen har til formål å oppnå sikker overføring av data til og fra nettsteder som tilhører virksomheter i offentlig sektor eller som brukes til tjenester som leveres av virksomheter i offentlig sektor. Dette omfatter både overføring av data mellom nettleser (sluttbruker) og nettjener, og mellom tjenester (API) som bruker protokollen HTTP.

Forslaget til endring opprettholder det beskrevne formålet. Formålet med endringen er å forbedre dette sikkerhetstiltaket og å presisere at sikker overføring av data til og fra nettsteder alltid skal brukes.

Hovedbegrunnelsen for forslaget er at endringer i nettlesere fra store leverandører i markedet og endringer i virkemåten til søketjenester representerer nye faktorer når nytteverdien av denne anbefalingen skal vurderes.

Kort om de foreslåtte endringene

Vi foreslår følgende endringer:

1. Vi foreslår at spesifikasjonen RFC 2817 kan benyttes som et alternativ til spesifikasjonen RFC 2818. Dette er en endring som ikke får konsekvenser for dem som allerede bruker RFC 2818, men åpner for muligheten til å velge en alternativ teknisk løsning. Endringen medfører derfor ingen økt kostnad.

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

2. For å understøtte at sikker kommunikasjon alltid brukes legges det til anbefalingen at spesifikasjonen RFC 6797 (HTTP Strict Transport Security) benyttes. Avhengig av virksomhetens eksisterende løsning kan denne endringen medføre en engangskostnad ved endring av nettstedet, men denne endringen vil ikke medføre økte driftskostnader. Vi antar at engangskostnaden er lav.
3. For å etablere en standard for hvordan omdirigering av forespørsler som ikke bruker protokollen for sikker overføring av data skal gjøres beskrives dette i anbefalingen. Ønsket standard er at omdirigering fra HTTP til HTTPS gjøres til samme URL for å gjøre det mulig å etablere automatisk testing av etterlevelse. Denne endringen kan medføre at enkelte eksisterende nettsteder må endres. En slik endring vil medføre en engangskostnad, men medfører ingen driftskostnad. Vi antar at engangskostnaden er lav.
4. Difi vurderer å be om at denne anbefalingen gjøres obligatorisk. Dette gjøres for å sikre at denne anbefalingen i større grad blir fulgt av virksomheter i offentlig sektor.

Endring av referanser til de tekniske spesifikasjonene

Dagens tekst er som følger:

> «Det anbefales at offentlige kommunikasjonstjenester har støtte for HTTP over TLS [RFC 2818] ved bruk av protokollene HTTP/1.1 [RFC 7230] og TLS 1.2 [RFC 5246].»

Difi foreslår å endre denne teksten til:

> «Det anbefales at offentlige kommunikasjonstjenester har støtte for Upgrading to TLS Within HTTP/1.1 [RFC 2817] eller HTTP over TLS [RFC 2818] ved bruk av protokollene HTTP/1.1 [RFC 7230] og TLS 1.2 [RFC 5246]. Det anbefales at HTTP Strict Transport Security (RFC 6797) blir brukt.
>
> Dersom en tjeneste får en forespørsel med bruk at HTTP uten bruk av sikker overføring med bruk av TLS skal tjenesten svare ved omdirigering til samme URL med bruk HTTP over TLS.»

Det er viktig å påpeke at virksomhetene også må ha en god veiledning for å bruke standarden riktig. Den eksisterende veiledningen fra NSM er tilstrekkelig, men må oppdateres ved endring av anbefalingen for å bidra til at de over nevnte spesifikasjoner blir brukt på riktig måte.

Begrunnelse for endring

Endring nummer 1 begrunnes med at det ikke er noen grunn til å utelukke en av de to likeverdige spesifikasjonene RFC 2817 og RFC 2818 når man skal velge teknisk løsning eller leverandør. Da må anbefalingen nevne begge spesifikasjonene.

Fordi målet med anbefalingen er at HTTPS alltid skal benyttes er det hensiktsmessig å legge til spesifikasjonen RFC 6797 som vil bidra til å oppfylle dette målet.

Mange nettsteder har behov for å bruke HTTPS som et sikkerhetstiltak for deler av nettstedet hvor det utveksles informasjon som medfører krav til konfidensialitet. Det gir i praksis ingen besparelse å bruke HTTPS kun på deler av et nettsted.

Forslaget til anbefaling omfatter ikke krav til hvilken type sertifikater som bør brukes eller krav til fremstilling av sertifikater (krav til sertifikatleverandør). Krav til sertifikater kan bidra til å redusere risiko ytterligere, men slike krav kan medføre høyere kostnader. Difi anbefaler at krav til sertifikater knyttes til risikovurdering av den enkelte tjeneste.

Det er viktig å understreke at bruk av HTTPS vil redusere risikoen for at brukere opplever at innholdet i tjenesten blir endret på veien mellom tilbyder av en tjeneste og brukerens nettleser. Dette gjelder ikke bare forskjellige typer angrep mot brukeren, men også tilfeller der et mellomledd legger reklame eller annen informasjon til den originale tjenesten. Bruk av HTTPS vil derfor medføre en fordel for brukere av tjenesten. Indirekte vil dette bidra til at brukere opprettholder tillit til virksomheter i offentlig sektor. Det er vanskelig å sette noen økonomisk verdi på disse fordelene.

Difi ønsker at Standardiseringsrådet skal vurdere om denne standarden bør bli obligatorisk. Begrunnelse for dette følger under.

Endringer i forutsetninger

Søketjenester vil rangere nettsteder som bruker HTTPS foran nettsteder som ikke bruker HTTPS. Bruk av HTTPS vil derfor være en fordel for synlighet for brukere som søker etter tjenesten, og for disse brukerne vil dette oppleves som bedre tilgjengelighet. Det er vanskelig å sette noen økonomisk verdi på denne fordelen.

Tidligere har nettlesere merket nettsteder som bruker HTTPS med en hengelås i adressefelt. Utviklingen går i retning av at nettlesere i stedet merker nettsteder som *ikke* bruker HTTPS som usikre. Enkelte nettlesere vil gjøre det vanskeligere for brukere å besøke usikre nettsteder. Dette vil i praksis bety dårligere tilgjengelighet til tjenester som bruker usikre nettsteder. Dersom offentlige virksomheter ikke bruker HTTPS er det sannsynlig at dette vil ramme brukernes tillit til tjenestene, og det vil påvirke nettstedenes tilgjengelighet negativt. Det er vanskelig å sette noen økonomisk verdi på denne ulempen.

Det er grunn til å anta at nettlesere og søketjenester også tiden fremover vil endre reglene for hvordan nettsteder som bruker sikker datakommunikasjon merkes eller på annen måte fremheves. Denne utviklingen kan medføre et behov for å endre anbefalingen dersom det er ønskelig å påvirke hvordan nettstedene til offentlig sektor fremstår i nettlesere og søketjenester.

Konsekvenser dersom eksisterende anbefaling ikke endres

Digitale tjenester som ikke bruker HTTPS eller som ikke har etablert HTTPS på en korrekt måte vil merket som usikre i nettlesere. Når tjenestene fremstår som usikre påvirker dette tilliten til tjenesten negativt. Nettlesere kan i tillegg etablere barrierer som gjør det vanskeligere for brukere å bruke tjenesten. Dersom eksisterende anbefaling ikke endres vil det øke risikoen for at slike tjenester er oppleves som utilgjengelige.

Det vil ha negative konsekvens dersom eksisterende anbefaling ikke endres.

Kostnader

De foreslåtte endringene kan medføre at virksomheter må gjøre endringer på eksisterende tjenester. Kostnaden for hvert enkelt nettsted vil variere avhengig av teknisk løsning og nettstedets kompleksitet.

Det er viktig at virksomhetene regelmessig tester sine tjenester for å verifisere at sikker datakommunikasjon er satt opp korrekt. Feil bruk av standarden kan medføre at nettlesere gir brukere varsel om at tjenesten er usikker, eller at nettleseren oppretter en barriere for bruk av tjenesten som vil påvirke tilgjengeligheten. Regelmessig testing av at denne standarden følges vil være et kostnadselement for drift, men vil ikke utgjøre noen stor del av driftsutgiftene.

Når et nettsted går fra å bruke usikret til å bruke sikker overføring av data til og fra brukere vil det kreve økt bruk av CPU-ressurser for kryptering og dekryptering av data, men økningen er i praksis liten. HTTPS medfører også en liten forsinkelse (noen millisekunder) ved oppkobling av hver forbindelse. Dette er faktorer som kan medføre noe høyere driftskostnader. Dersom den tekniske løsningen for nettstedet støtter protokollen HTTP/2 vil bruk av sikker overføring muliggjøre en langt mer effektiv og raskere overføring av data. Dette er en faktor som kan bidra til lavere driftskostnader. Vær oppmerksom på at dette avsnittet omtaler driftsutgifter knyttet til den eksisterende anbefalingen.

Kostnader for sertifikater

Ett kostnadselement som har vært diskutert ved tidligere behandling av standard for sikker datakommunikasjon er knyttet til sertifikater. Endringer i markedet har ført til at det er flere leverandører som tilbyr en enkleste klasse type sertifikater som det ikke er knyttet avgifter til å utstede eller fornye. For virksomheter vil det være en lav engangskostnad for å etablere rutiner for å bestille og fornye slike sertifikater, men denne typen sertifikater kan redusere kostnadene knyttet til å etablering og drift av sikker datakommunikasjon.

Difi vil understreke at det bør gjøres en risikovurdering av hver enkelt tjeneste før man velger hva slags sertifikat som bør brukes. For viktige tjenester bør sertifikat med utvidet validering (EV) benyttes.

Begrunnelse for endring til obligatorisk standard

Difi vurderer å be om at anbefalingen endres til å bli en obligatorisk standard. Ulempen ved at enkelte tjenester oppleves som utilgjengelige er en vesentlig faktor i denne vurderingen. Det er viktig å opprettholde tillit til tjenester som leveres av virksomheter i offentlig sektor. En obligatorisk standard er også et effektivt et virkemiddel for å unngå at digitale tjenester levert av virksomheter i offentlig sektor merkes som usikre av nettlesere eller av søketjenester.