

Vedlegg B: Behandling i Standardiseringsrådet, DANE

Innhold:

- Saksframlegg til Standardiseringsrådets møte 20180925-B
- Oppsummering av hørings svar - DANE
- Oppdatert forslag til anbefaling - DANE

Dato:	21.8.2018	Saksnr:	18/00643
--------------	-----------	----------------	----------

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

Saksframlegg til Standardiseringsrådets møte 21.06.2018

Anbefalt standard for transportsikring av e-post

Dette forslaget gjelder endring av en eksisterende anbefaling¹ som ble innført 1.12.2016.

Formålet med forslaget

Forslaget medfører ingen endring av formålet med gjeldende anbefaling.

Begrunnelsen for endringen er at den eksisterende anbefalingen har en kjent sårbarhet hvor det er laget en ny spesifisering som inneholder tiltak mot denne sårbarheten. Difi anser at den nye spesifiseringen har tilstrekkelig modenhet til at den kan vurderes som ny del av anbefalingen.

Endring av eksisterende anbefaling

Dagens tekst er som følger:

«Det anbefales å benytte SMTP Service Extension for Secure SMTP over Transport Layer Security (RFC 3207) i opportunistisk modus for transportsikring av e-post mellom e-post servere, både ved sending av e-post til offentlige virksomheter og ved sending av e-post til innbyggere og næringsliv.

Dette gjelder e-post utveksling som går over Internett (SMTP), og ikke annen meldingsutveksling som skal foregå ved hjelp av løsning for utveksling av meldinger mellom offentlige virksomheter.»

Difi foreslår å endre ordlyden til følgende:

«Det anbefales å benytte transportsikring av e-post mellom e-post servere, både ved sending av e-post til offentlige virksomheter og ved sending av e-post til innbyggere og næringsliv. Som

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

prioritert løsning anbefales det å benytte SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (RFC 7672). Dersom motpart i utvekslingen av en e-postmelding ikke støtter denne spesifikasjonen skal SMTP Service Extension for Secure SMTP over Transport Layer Security (RFC 3207) i opportunistisk modus brukes.

Dette gjelder e-post utveksling som går over Internett (SMTP), og ikke annen meldingsutveksling som skal foregå ved hjelp av løsning for utveksling av meldinger mellom offentlige virksomheter.»

Begrunnelse

Den nåværende anbefalingen som viser til spesifikasjonen RFC 3207 medfører at løsninger som er tatt i bruk kan ha sårbarheter for angrep fra mellommann. IETF publiserte i oktober 2015 spesifikasjonen RFC 7672 som reduserer denne risikoen og som kan benyttes sammen med gjeldende anbefaling i referanse katalogen. En alternativ løsning er foreslått og har vært under arbeid hos IETF siden mars 2016, men er ennå ikke ferdigstilt som IETF-spesifikasjon.

Det er uheldig å anbefale sikkerhetstiltak med sårbarheter hvor risikoen er betydelig redusert i nyere løsninger uten i det minste å gi veiledning om dette. Et minimum er å gjøre oppmerksom på den nye løsningen, men den nye løsningen vil ha liten effekt dersom kun noen få virksomheter bruker den. Difi foreslår derfor å anbefale spesifikasjonen RFC 7672 for transportsikring av e-post.

Den sikkerhetsmessige gevinsten knyttet til denne endringen er redusert risiko for at sikker transport av e-post kan angripes av en trusselaktør.

Kostnader

Difi antar at den største kostnaden for å ta i bruk RFC 7672 er knyttet til at standarden krever at DNSSEC (RFC 4033 m.fl.) er etablert, men det er nødvendig å kartlegge hvor mange virksomheter som har leverandører av e-post som ikke tilbyr RFC 7672 og som derfor må vurdere å bytte leverandør. Dette ønsker Difi å få tilbakemelding på når endringsforslaget legges ut til høring.

Konsekvens dersom gjeldende anbefaling ikke endres

Selv om denne anbefalingen ikke endres så forventes det at virksomhetene har gjort en vurdering om risikoen for at sårbarheten som følger av RFC 3207 er akseptabel. Det er likevel fare for at en uendret anbefaling kan gi et utilsiktet signal om at risikoen knyttet til denne sårbarheten er akseptabel.

Forslag B – DANE – Oppsummering av høringsvar

Det følgende er en oppsummering av vesentlige merknader fra svarene på høringen med kommentarer fra Difi.

Regjeringsadvokaten (RA) uttaler «RFC 3207 anses som ikke akseptabel risiko for RA.»

Difi har gjort en tilsvarende vurdering i forkant av forslaget om å endre den eksisterende anbefalingen. Det eksisterer flere initiativer for å løse utfordringen, men foreløpig er det kun RFC 7672 som har fått status som en standard.

Statistisk sentralbyrå (SSB) har uttalt følgende: «En uformell sjekk av ulike offentlige instanser, viser at mange ikke støtter dette per i dag, og det er dermed høyst usikkert hvor stor effekt det har å anbefale bruk av DANE på kort sikt.» Passordninja AS har uttalt følgende: «Det er per september 2018 kun en større kommersiell leverandør av dns+epost tjenester i Norge som tilbyr støtte for DNSSEC (RFC 4033 m.fl.) i kombinasjon med DANE (RFC 7672). Imidlertid finnes det en rekke produkter og tjenester internasjonalt som har støtte for DNSSEC, og som enten har eller ventes å snart kunne tilby DANE (RFC 7672) støtte.»

Difi har gjennom arbeidet funnet at RFC 7672 har lav aksept i markedet internasjonalt. Selv Nederland som har vært aktive for å etablere bruk av standarden har fremdeles liten utbredelse. Så langt vi kan se er det Tyskland som kommer best ut når det gjelder å ta standarden i bruk.

I saksframlegget som ble sendt på høring har Difi nevnt at en alternativ løsning er foreslått og har vært under arbeid hos IETF siden mars 2016. Denne har den foreløpige betegnelsen «SMTP MTA Strict Transport Security» og arbeidet med denne er på nåværende tidspunkt kommet så langt at Difi vurderer det som sannsynlig at den blir publisert som en RFC i nær fremtid. Dette vil påvirke vurderingen av aksept i markedet for RFC 7672.

Det er også foreslått en ny spesifikasjon som sannsynligvis vil bli en oppdatering av både RFC 3207 og RFC 7672. Arbeidet med denne har hatt rask fremdrift og det er sannsynlig at også denne standarden vil bli publisert som en RFC i nær framtid.

Difi vil foreslå at Standardiseringsrådet utsetter behandlingen av dette forslaget til sitt neste møte.

Oppdatert forslag til anbefaling – Saksframlegg B – DANE

Den følgende utgaven av teksten er oppdatert etter behandling av hørings svar.

Difi ønsker å utsette behandling av dette saksfremlegget til neste møte i Standardiseringsrådet.