Difi
Direktoratet for forvaltning og ikt

Notat

Dato:	30.10.2018	**Saksnr:**	18/00643

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

Saksframlegg til Standardiseringsrådets møte 11.12.2018

Anbefalt standard for transportsikring av e-post

Dette forslaget gjelder endring av gjeldende anbefaling for transportsikring av e-post.[1]

Vedlegg 1 til dette saksframlegget er forslag til endring som ble sendt på høring for å bli behandlet på Standardiseringsrådets møte 25.09.2018. Det ble vedtatt og publisert nye standarder på dette området samtidig med at saksframlegget var på høring. Derfor er behandling av saken utsatt til 11.12.2018. Sammendrag av de opprinnelige høringssvarene er vedlegg 2 til dette saksframlegget.

Det følgende er et revidert forslag som tar hensyn til nye standarder i vurderingen.

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 spesifikasjon som inneholder tiltak mot denne sårbarheten. Difi foreslår at to av standardene fra IETF bør tas inn i anbefalingen og dette saksframlegget beskriver tre alternativer til oppdatert anbefaling.

Begrunnelse

Den nåværende anbefalingen som viser til spesifikasjonen RFC 3207 «SMTP Service Extension for Secure SMTP over Transport Layer Security» medfører at løsninger som er tatt i bruk kan ha sårbarheter for angrep fra mellommann. Difi foreslår å endre anbefalingen for å redusere risiko for at sikker transport av e-post kan angripes av en trusselaktør.

---

[1] https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/referansekatalogen/grunnleggende-datakommunikasjon-0 - anbefaling fra 1.12.2016

Nye standarder

IETF publiserte i oktober 2015 spesifikasjonen RFC 7672 «SMTP Security via Opportunistic DNS-Based Authentication of Named Entities» som reduserer denne risikoen og som kan benyttes sammen med gjeldende anbefaling i referansekatalogen.

Tyskland krever RFC 7672 for sertifisering av sikker e-post.[2] Nederland har besluttet at RFC 7672 er en anbefalt standard i offentlig sektor, med krav[3] om at tekniske tiltak som følger standarden etableres innen utgangen av 2019.[4] EU-kommisjonen har besluttet at RFC 7672 kan brukes på linje med internasjonale standarder i offentlige anskaffelser.[5]

26.09.29018 publiserte IETF en alternativ løsning: standarden RFC 8461 «SMTP MTA Strict Transport Security». Dette er en løsning som ikke er avhengig av DNSSEC selv om det også for denne gir bedre sikkerhet dersom DNSSEC er på plass. Den nye standarden er allerede tatt i bruk av enkelte store kommersielle tilbydere.

Både RFC 7672 og RFC 8461 vil i omtrent like stor grad redusere risikoen knyttet til sårbarheten i den gjeldende anbefalingen. Løsningen RFC 8461 bruker påvirker ikke Difis vurdering av behovet for å etablere DNSSEC som anbefalt standard i offentlig sektor. Det er også mulig å bruke både RFC 7672 og RFC 8461 på samme e-postsystem.

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.

IETF publiserte 26.09.2018 en annen standard som kan bidra til å redusere risiko knyttet til transportsikring av e-post: RFC 8460 «SMTP TLS Reporting». Denne standarden gjør det mulig for mottager av e-post å definere hvordan den som forsøker å sende e-post med transportsikring kan rapportere om feil. Dette gir langt bedre mulighet for å identifisere problemer eller forsøk på angrep og bedre grunnlag for effektiv retting av feil. Denne standarden har nytteverdi for alle standardene som er nevnt over: RFC 3207, RFC 7672 og RFC 8461. Difis vurdering er at denne standarden bør inkluderes i en anbefaling.

---

[2] BSI TR-03108-1: “Secure E-Mail Transport”, Requirements for E-Mail Service Providers (EMSP) regarding a secure Transport of E-Mails

[3] Comply-or-explain

[4] https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken

[5] Commission Implementing Decision (EU) 2017/2288 of 11 December 2017 on the identification of ICT Technical Specifications for referencing in public procurement

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.»

Å beholde dagens anbefaling er 0-alternativet i dette saksframlegget. Difi foreslår tre alternativer i en rekkefølge som reduserer risiko fra liten til stor grad. Alternativ 2 er identisk med endringen som ble foreslått i forrige høringsrunde.

Alternativ 1:

> «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. Det anbefales også at «SMTP TLS Reporting» (RFC 8460) 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.»

Alternativ 2:

> «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 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.»

Alternativ 3:

> «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 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. Det anbefales også at «SMTP TLS Reporting» (RFC 8460) 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.»

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.

Kostnaden ved å ta i bruk RFC 8460 er i hovedsak knyttet til behandling av rapporter og de korrigerende tiltak som følger av rapportene.

Konsekvens dersom gjeldende anbefaling ikke endres (0-alternativet)

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 alltid vil være akseptabel.

Risikoreduserende virkning i alternativ 1

Alternativ 1 er en løsning som ikke fjerner sårbarhetene i RFC 3207. Faktoren som reduserer risiko er at mottaker av en e-post får mulighet til å detektere en eventuell utnyttelse av sårbarheten. I tillegg vil RFC 8460 bidra til at feil raskere blir identifisert, noe som muliggjør mer effektiv feilretting.

Risikoreduserende virkning i alternativ 2

Alternativ 2 er en løsning hvor muligheten for angrep fra mellommann er mindre ved bruk av RFC 7672 og på den måten er risiko redusert.

Risikoreduserende virkning av alternativ 3

Alternativ 3 er en kombinasjon av alternativ 1 og 2 og representerer den største reduksjonen av risiko. Muligheten for angrep fra mellommann er redusert, og mottaker av e-post får mulighet til å detektere forsøk på utnyttelse av sårbarheter og rapporter om feil.

Prioritert alternativ

Difi foretrekker at alternativ 3 velges, men avventer kommentarer fra høringsrunden.