Difi
Direktoratet for forvaltning og ikt

VEDLEGG 3

**Notat**

| | | | |
|---|---|---|---|
| **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 å motvirke falske avsendere av e-post

Det følgende er forslag om en ny anbefalt standard på bruksområdet Grunnleggende datakommunikasjon. Difi ønsker å sende dette forslaget på høring så raskt som praktisk mulig.

> «Det anbefales å benytte Domain-based Message Authentication, Reporting, and Conformance (DMARC) (RFC 7489) med de underliggende standardene Sender Policy Framework (SPF) og Domain Keys Identified Mail (DKIM) for å sikre utveksling 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.»

### Formålet med anbefalingen

Formålet med anbefalingen er å etablere bruk av en standard som gir mottager av e-post bedre mulighet til å verifisere om en melding faktisk er sendt fra det domenet avsender har angitt i meldingen. Dette medfører at meldinger som forsøker å bruke en forfalsket avsenderadresse kan identifiseres og stoppes. Det betyr også at mottager kan ha større tillit til angivelsen av avsender når en melding som er korrekt merket skal vurderes opp mot regler for å stoppe uønsket e-post (eller slippe gjennom meldinger fra tiltrodde avsendere).

Det må understrekes at avsendere av uønsket e-post (spam) eller meldinger som sendes av en trusselaktør som en del av et angrep (for eksempel phishing) selvsagt kan merkes korrekt ifølge denne standarden. Formålet med standarden er kun å redusere risiko for at avsenderadresse er forfalsket.

Standarden gir også mulighet for at avsender kan motta rapporter om at virksomhetens e-postadresse blir forsøkt misbrukt av andre. Slike tilbakemeldinger fra mottagere vil også bidra til at avsender får varsel dersom systemet er satt opp feil.

## Begrunnelse

Det har vært en sterk økning i bruk av e-post med forfalsket avsender både i forbindelse med digitale angrep mot virksomheter og ved utsending av uønsket e-post (spam). Misbruk av virksomheter i offentlig sektor som tilsynelatende avsendere av forfalsket e-post kan bidra til å svekke tilliten til digitaliseringen i offentlig sektor, og det øker risiko for at e-post som er sendt fra virksomhetene blir stoppet i spam-filter.

Sikkerhetstiltak som DMARC, SPF og DKIM er tiltak som etableres på virksomhetsnivå og som gir *mottager* bedre forutsetninger for å avvise e-post med forfalsket avsender. Samtidig reduseres risikoen for at e-post som sendes av en tiltrodd virksomhet blir stoppet i spam-filter hos mottager.

Det må understrekes at dette er et teknisk tiltak som ikke reduserer risiko for at en angriper eller bedrager bruker domener med navnelikhet eller bare sender fra en tilfeldig, gyldig adresse. Det er derfor vanskelig å anslå i hvor stor grad bruk av DMARC vil redusere risiko for at forsøk på digitalt angrep lykkes og redusere tidsbruk som følge av uønsket e-post (spam) generelt.

## Gevinster knyttet til anbefalingen

For den enkelte virksomhet vil den direkte gevinsten av å følge anbefalingen være sikrere håndtering av e-post mellom virksomheter i offentlig sektor. Det kan også regnes som en gevinst at risikoen for at e-post som sendes ut fra virksomheten feilaktig blir filtrert ut som uønsket e-post hos mottager reduseres. Det er ikke mulig å anslå en økonomisk verdi av denne typen gevinster.

En indirekte gevinst av at virksomheter i offentlig sektor følger anbefalingen er at mottagere får større tillit til e-post som kommer fra en avsender i offentlig sektor.

## Kostnader knyttet til anbefalingen

Kostnaden for å etablere og drifte SPF er meget lav. Kostnaden for å etablere DMARC er også lav, men drift av DMARC gir først verdi når rapportene som genereres følges opp. Kostnaden for å etablere DKIM er noe høyere og kan medføre at enkelte virksomheter må bytte leverandør av e-post som tjeneste. Risikoen for at en leverandør av e-posttjeneste ikke kan levere DMARC vurderes som lav. Flere virksomheter har allerede tatt en eller flere av tiltakene i bruk. DMARC er innført som standard for offentlig sektor i andre land, bl.a. USA og Storbritannia.

Et eksempel på en tjeneste som understøtter DMARC er Microsoft Office 365. Det er publisert veiledning for etablering av SPF, DKIM og DMARC i den delen dokumentasjonen[1] som betegnes «cyberthreat protection».

DMARC, SPF og DKIM bruker DNS til å distribuereopplysninger. Det vil være en fordel om også DNSSEC (RFC 4033 m.fl.) er etablert, men DNSSEC er ingen forutsetning for å etablere DMARC.

[1] https://docs.microsoft.com/en-us/office365/securitycompliance/eop/exchange-online-protection-overview