Difi
Direktoratet for forvaltning og ikt

Vedlegg C: Behandling i Standardiseringsrådet, DMARC

Innhold:

- Saksframlegg til Standardiseringsrådets møte 20180925-C
- Oppsummering av høringssvar - DMARC
- Oppdatert forslag til anbefaling - DMARC

Difi
Direktoratet for forvaltning og ikt

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

Forslag C – DMARC – Oppsummering av høringssvar

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

Justis- og beredskapsdepartementet (JD) foreslår i sitt høringssvar at standarden gjøres obligatorisk og viser i den forbindelse til at «IKT-hendelser rettet mot nasjonal kritisk IKT-infrastruktur ofte innledes med en forfalsket e-post».

Difi vektlegger at denne standarden må brukes riktig av virksomhetene. Der er viktig å unngå at e-post på grunn av feil bruk av standarden ikke kommer frem til mottager. Derfor er det avgjørende at en veiledning er oppdatert og kvalitetssikret, og at standarden er stabil før den gjøres obligatorisk.

Statistisk sentralbyrå (SSB) har uttalt at «DMARC har vært en mulighet for sikring lenge, men dessverre benytter svært få denne løsningen.» Difi legger til grunn at det ikke er så mange som bruker DMARC, men at den underliggende standarden SPF har større utbredelse.

Uninett AS har uttalt at «standardene SPF og SRS bør sterkt anbefales, med SPF satt passiv, dvs. til NEUTRAL eller SOFTFAIL.» Difi antar at forkortelsen SRS viser til Sender Rewriting Scheme som ikke er noen selvstendig standard. Difi vurderer derfor at SRS er en mekanisme som bør beskrives i en veiledning.

Uninett uttaler videre «Derimot er det prematurt å anbefale DMARC da flere av standardene som forutsettes ikke er klare enda, som f.eks. ARC. For organisasjoner som velger å innføre DMARC på nåværende tidspunkt bør bruken anbefales begrenset til at administrator av sendende postkontor får tilsendt loggmeldinger om avvik. Mottakende epostkontor bør anbefales å ikke kaste epost som følge av DMARC-feil, men heller markere den som spam.»

Difi er enig i en vurdering av DMARC hvor det på nåværende tidspunkt kun anbefales å bruke en begrenset del av funksjonaliteten i standarden. Dette understreker nødvendigheten av å etablere en god veiledning. Når det gjelder ARC (Authenticated Received Chain) så er dette et forslag til eksperimentell standard som fremdeles er under arbeid i IETF.

Uninett uttaler videre at «SPF kan potensielt medføre en betydelig ekstrakostnad, spesielt dersom man skal kunne sende epost i organisasjonens domenenavn fra flere ulike tjenestemaskiner som også kan tenkes at befinner seg i ulike infrastrukturer. En av årsakene til dette er at mange programvareprodukter forutsetter å kunne sende epost med kundens domenenavn som avsender, men fra leverandørens egen infrastruktur.» Eika AS har uttalt at «Vi vil derimot påpeke at en innføring av DMARC, SPF og DKIM trolig vil føre til en ekstra kostnad i form av en (eller deler av en) dedikert ressurs hos de virksomheter som administrerer et større antall domener.»

Difi er enig i vurderingen at for enkelte virksomheter kan forvaltning av et stort antall domener og underdomener være krevende. Vi mener likevel at dette kun gjelder en liten andel av virksomhetene i offentlig sektor.

Eika AS har videre uttalt at «Det er også viktig at den enkelte virksomhet kartlegger egne domener og eksterne tjenester som nødvendigvis ikke er i aktiv bruk.» Difi vil understreke at det er viktig å sikre at registrerte domener som en virksomhet ikke bruker til e-post ikke blir misbrukt. Dette medfører at SPF og DMARC bør brukes også på registrerte domener som ikke brukes til å sende e-post.

Statens lånekasse for utdanning har uttalt at «For at DKIM skal være nyttig over tid, mener vi standarden også bør belyse behovet for organisering og forvaltning av nøkler. Dette vil kunne kreve noe spesialkompetanse i virksomhetene.» Uninett har uttalt at «Siden DMARC ikke forutsetter både SPF og DKIM, men kan fungere med bare en av dem, burde anbefalingen ta høyde for at man kan innføre SPF og sette opp DMARC basert på denne alene. Kostnaden med innføring av DKIM kan dermed tas på et senere tidspunkt.» Uninett har videre uttalt at «Ved sending forutsetter DKIM at eposten passerer gjennom et DKIM-kapabelt ledd, mens SPF ikke krever noe tilsvarende».

Difi er enig i vurderingen at det krever høyere kompetanse og kan medføre større kostnader å bruke DKIM. Det er viktig å understreke at Standarden DMARC ikke krever at både SPF og DKIM benyttes på utgående e-post, og det er den enkelte virksomhet som velger hvilken av disse to mekanismene som er best egnet.

Uninett har uttalt at «Epostmottak bør derimot kunne tolke både SPF og DKIM, for å redusere spam og angrep via epost.»

Difi er enig i at for å lojalt følge opp rapportering i DMARC må dette gjøres. Difi vil likevel understreke at enkelte virksomheter kan ha etablert løsninger for identifisering av uønsket e-post eller e-post med ondartet innhold som er mer kostnadseffektive enn å bruke DKIM.

Uninett har uttalt at «Siden SPF, DKIM og DMARC annonseres til verden via DNS er DNS-leverandøren svært sentral ved innføring av DMARC, ikke bare epost-leverandøren. Erfaringsmessig tilbyr ikke alle DNS-leverandører ennå god støtte til å sette opp SPF, og spesielt ikke DKIM-records. Det ligger dermed potensiell ekstrakostnad i dette også.»

Difi legger vekt på at måten SPF, DKIM og DMARC bruker DNS på er et argument for å bruke DNSSEC. Eventuelle kostnader forbundet med at en DNS-leverandør ikke tilbyr støtte for å sette opp SPF og DKIM må ses i sammenheng med de kostnader det kan medføre å bytte til en DNS-leverandør som tilbyr støtte for DNSSEC.

Oppdatert forslag til anbefaling – Saksframlegg C – DMARC

Den følgende utgaven av teksten er oppdatert etter behandling av høringssvar.

«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.

Det anbefales at man for domener som ikke benyttes til sending av e-post bruker Sender Policy Framework (SPF) for å angi at det ikke sendes e-post fra domenet.

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.»

Det er viktig at denne standarden brukes riktig og vi viser til veiledning fra Nasjonal sikkerhetsmyndighet (NSM): *Grunnleggende tiltak for sikring av e-post*.