NSM

NASJONAL
SIKKERHETSMYNDIGHET

Beskrivelse av grunnleggende tiltak for sikring av overføring av e-post mellom e-posttjenere.

GRUNNLEGGENDE TILTAK FOR **SIKRING AV E-POST**

INNHOLD

OM
VEILEDEREN

Dette dokumentet er NSMs anbefaling for grunnleggende sikring av overføring av e-post mellom e-posttjenere. Målgruppen er personell som utvikler og forvalter ugraderte systemer i offentlig forvaltning. Dokumentet er ikke ment brukt i forbindelse med formell sikkerhetsgodkjenning av graderte systemer.

Anbefalte sikringstiltak i denne rapporten er STARTTLS, SPF, DKIM og DMARC.

INNLEDNING

Dette dokumentet beskriver fire beskyttelsesmekanismer for overføring av e-post mellom e-posttjenere. Beskyttelsesmekanismene bidrar til å beskytte mot misbruk av egne e-posttjenere til utsendelse av e-post med skadevare under falsk flagg. Beskyttelsesmekanismene sørger for autentisering av e-posttjenere og konfidensialitetssikring av e-postoverføringen, og beskyttelsesmekanismer for å begrense uønsket e-post (spam, phishing og spoofing). Dokumentet omhandler ikke beskyttelsesmekanismer på klientsiden, eller mekanismer for vasking av e-post (antivirus o.l.).

Målgruppen er personell som utvikler og drifter ugraderte systemer i offentlig forvaltning som tilbyr e-post-tjenester. I tillegg anbefaler NSM at private bedrifter også følger dokumentet, slik at størsteparten av e-post som kommuniseres i Norge blir autentisert og konfidensialitetssikret.

Nyhetsbildet har vist at det er nødvendig med konfidensialitetssikring av e-postoverføring. I tillegg er det nødvendig med autentisering av e-posttjenere slik at man unngår man-in-the-middle-angrep mellom e-posttjenerne.

Kontaktpunkt for denne veiledningen er post@nsm.stat.no. Vennligst bruk veiledningens navn som emne for kommentarer og innspill.

1. Beskrivelse

E-post er den foretrukne digitale kommunikasjonskanalen for norske offentlige og private virksomheter, selv om ny teknologi muliggjør andre metoder å kommunisere elektronisk. I følge SSB benyttet 90% av den norske befolkningen i 2016 Internett til e-post[1]. Dette er en økning fra 83% i 2010. Dette gjør e-post til en attraktiv angrepsvektor, med et bredt nedslagsfelt som har potensiale til å ramme mange.

Det store flertallet av alle alvorlige registrerte IKT-hendelser rettet mot nasjonal kritisk IKT-infrastruktur startet med en forfalsket e-post som lurer bruker til å åpne et vedlegg med ondsinnet programvare eller klikke på en link som fører til infeksjon av maskinen. Trusselaktørens mål er å få kontroll over din maskin, eller å lure mottaker til å avgi verdifull informasjon. Løsepengevirus («ransomware»), som NSM har registrert en kraftig økning av de siste årene, spres også i stor grad gjennom e-post.

Teknologien som muliggjør e-post ble unnfanget i en tid hvor nettbasert oppførsel og kommunikasjon var preget av tillitt. E-post er i utgangspunktet en usikker teknologi som er enkel å forfalske, avlytte og endre. Opp gjennom årene har nye utvidelser og sikringstiltak rettet mot e-post blitt utviklet for å håndtere det endrede trusselbildet. Den store popularitet e-post nyter som angrepsvåpen, tilsier at mottiltak som hindrer og begrenser denne type digitale angrep bør være høyt prioritert.

1. SSB «Bruk av IKT i husholdningene»: https://www.ssb.no/teknologi-og-innovasjon/statistikker/ikthus/aar/2016-09-06

2. Anbefalte tiltak

NSM anbefaler fire beskyttelsesmekanismer for å sikre e-post på e-posttjenere:

1. **STARTTLS**: En beskyttelsesmekanisme for overføring av e-post mellom e-posttjenere. Beskyttelsesmekanismen sørger for autentisering av e-posttjenere og konfidensialitetssikring. Følgende tre tiltak vil relativt enkelt sørge for at en stor del av e-postkommunikasjonen ikke vil kunne avlyttes:
   a. Aktiver STARTTLS for utgående e-post.
   b. Installer tiltrodd sertifikat for sikring av innkommende e-post.
   c. Krev kryptering for bestemte mottagere og avsendere.
2. **SPF** (Sender Policy Framework): Benyttes for å spesifisere hvilke e-posttjenere som er autorisert til å sende e-post på vegne av et gitt domene (eksempelvis for example.com).
3. **DKIM** (DomainKeys Identified Mail): Elektronisk signatur som legges på all utgående e-post sendt på vegne av et domene, som så kan verifiseres mot en nøkkel lagret i DNS for avsenders domene.
4. **DMARC** (Domain based Message Authentication, Reporting and Conformance): Beskriver hvordan du ønsker at e-post som feiler SPF og DKIM-sjekker skal håndteres, og muliggjør at andre e-post-servere kan rapportere tilbake på e-post de mottar.

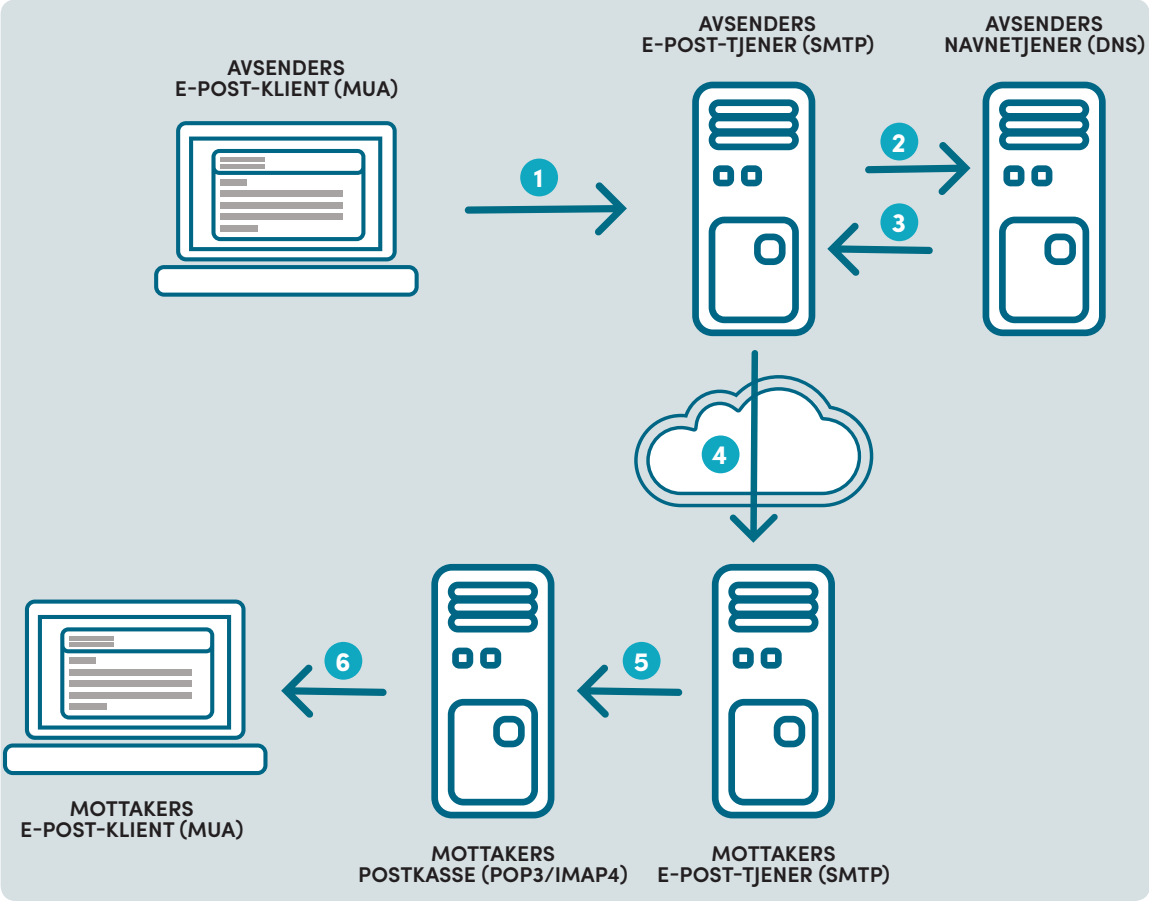
E-post-angrep med skadevare i lenker og vedlegg kan i tillegg adresseres med både tiltak på klientmaskinene samt i lokalnettet. Klienter bør herdes, og som et minimum bør NSMs dokument "S-02 Sjekkliste: Ti viktige tiltak mot dataangrep"[2] følges . I tillegg bør lokalnettet ha sikringstiltak som beskytter klientene mot skadelig kommunikasjon utad[3]. Les mer i NSMs «Grunnprinsipper for IKT-sikkerhet» for anbefalte sikringstiltak for å sikre både klienter, servere og nettverk[4].

Anbefalingene bruker informasjon fra DNS og det er derfor viktig at denne er korrekt. Domenet bør sikres med DNSSEC, slik at mottakerne av e-post kan validere anvisningen i DNS. Lær mer om DNSSEC på Norids hjemmesider[5].

2. NSM dokument «S-02 Sjekkliste: Ti viktige tiltak mot dataangrep»: https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-02-ti-viktige-tiltak-mot-dataangrep.pdf.
3. Se bl.a. NSM dokument «S-03 Sjekkliste: Ti grunnleggende tiltak for sikring av egne nettverk» og «U-12: DNS Response Policy Zone (RPZ) - Filtrering av DNS-forespørsler ved hjelp av svartelister».
4. NSMs «Grunnprinsipper for IKT-sikkerhet»: https://www.nsm.stat.no/publikasjoner/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/.
5. https://www.norid.no/no/dns/dette-er-dnssec/

3. E-post

Hvordan transporteres e-post mellom brukere? Dette er en forenklet fremstilling:



1 Avsender forfatter en e-post i sin e-post-klient («Mail User Agent» (MUA)). Når bruker trykker «Send», blir e-posten overført fra MUA til virksomhetens e-posttjener.

2 Virksomhetens e-posttjener, («Mail Transport Agent» (MTA)), ser på mottaker-domenet (det som står etter '@' i en e-postadresse). MTAen benytter så en DNS-tjener (Domain Name System) for å slå opp hvilken IP-adresse mottakers e-posttjener har (MX eller A-records).

3 DNS-tjeneren sender IP-adressen tilbake til MTA.

4 MTA sender e-posten til mottakers MTA ved hjelp av protokollen SMTP [1].

5 Mottakers MTA leverer så e-posten til den tjenesten som har ansvaret for å levere og lagre e-post i mottakers postkasse («Mail Delivery Agent» (MDA)). De to mest kjente protokollene for å hente e-post fra postkassen er POP3 og IMAP.

6 Mottakers MUA aksesserer postkassen via POP3 eller IMAP og leser e-posten[6].

6. MS Exchange benytter et internt format for overføring av e-post internt i virksomheten (MAPI/RPC).

Anbefalingene i dette dokumentet omhandler steg 4 i beskrivelsen til venstre.

Anbefaling 1: STARTTLS

Tradisjonelt når man snakker om e-postkryptering, handler det om ende-til-ende-konfidensialitetsbeskyttelse. Det vil si at avsender krypterer e-posten og denne sendes kryptert gjennom e-posttjenere og rutere til mottager, som så dekrypterer e-posten. Selv om dette er en veldig sikker løsning, krever det betydelig innsats hos avsender og mottaker, med kryptering og forvaltning av nøkler.

NSM anbefaler derfor at man først tar i bruk STARTTLS [2], som er en utvidelse til blant annet e-postoverføringsprotokollen som benyttes mellom e-posttjenere. Dette gir sikker overføring av e-posten mellom avsenders og mottakers e-posttjenere, uten at det krever noen innsats av brukerne.

En bruker som sender e-post, skriver denne i klartekst og leverer denne til sin egen e-posttjener[7]. Deretter vil e-posttjeneren lese hvem den skal sende e-posten til og etablere en forbindelse til mottagerens e-posttjener.

TLS benyttes for denne forbindelsen, og STARTTLS spør om e-posttjeneren den kobler seg til støtter kryptert forbindelse. Hvis den svarer ja, prøver de å etablere en kryptert forbindelse og overføre e-posten kryptert. Hvis ikke blir e-posten overført i klartekst til en ikke-autentisert e-posttjener. Dette er en best effort-løsning for kryptering.

3.1. Aktiver STARTTLS for utgående e-post

Første steg er å aktivere STARTTLS for all utgående e-post. Det betyr at e-posttjeneren som skal sende en e-post, vil prøve å etablere kryptert forbindelse. På samme måte som man ikke trenger eget sertifikat for å sikre kommunikasjonen mot et sikkert nettsted (HTTPS), trenger man ikke egne sertifikater for å sende fra seg kryptert e-post.

Ved å aktivere STARTTLS sørger man for at all utgående e-post er kryptert til mottagere som allerede har skaffet sertifikat.

Det er viktig at man aktiverer STARTTLS på e-posttjeneren som er «ytterst» og håndterer all innkom-mende og utgående e-post mellom organisasjonens system og Internett. For mer informasjon, se kapittel 3.5: Beskyttelse mot skadevare.

3.2. Installér tiltrodd sertifikat for sikring av innkommende e-post

7. Merk at kommunikasjonen mellom brukers e-postklient og e-posttjener ikke blir sikret av STARTTLS, men normalt er dette sikret i bedriftens interne nett eller ved hjelp av VPN-baserte løsninger.

For å sikre innkommende kommunikasjon trenger virksomheten et eget sertifikat. Dette sertifikatet må også installeres på «ytterste» e-posttjener slik at man ikke forhindrer inspeksjon av innhold. Se kapittel 4.5: Beskyttelse mot skadevare.

Bruk av tiltrodde sertifikater gir både autentisering av e-posttjenere og konfidensialitetsbeskyttelse av konvolutt, hode og kropp til e-poster. For mer informasjon, se kapittel 4.4: Tiltrodd sertifikatutsteder.

Når man har installert eget sertifikat er det viktig å oppfordre samarbeidspartnere til å aktivere STARTTLS og installere sitt eget sertifikat, slik at man får to-veis sikring av e-post.

Noen systemer støtter ikke såkalte wildcard -sertifikater[8]. For systemer med mange e-post-domener bør derfor multidomain -sertifikater[9] benyttes.

3.3. Krev kryptering for bestemte mottagere og avsendere

Som nevnt innledningsvis er STARTTLS en best effort-løsning for sikring av e-post. Når man har installert eget sertifikat og har betydelig e-post-kommunikasjon med bestemte samarbeidsparter, vil det være fornuftig å stramme inn bruken av sertifikater.

Det er flere måter å gjøre dette på. Gjennom standardinstallasjoner av operativsystemer og e-post-tjenester, kan en rekke sertifikater bli installert som man nødvendigvis ikke har tillit til. Man kan derfor redusere antall rot-sertifikater man har tillit til, for å unngå at ikke-tiltrodde sertifikater benyttes.

I tillegg kan man spesifisere enkeltsertifikater som skal benyttes mot enkeltmottagere. Dette er ikke en skalerbar løsning, men vil være nyttig for å sikre spesielt sensitiv, men ugradert informasjon mellom spesielt tette samarbeidsparter. Alternativt, eller i tillegg, kan man lage en liste over domene-navn hvor sertifikater skal valideres før bruk, og kryptering skal benyttes.

Når dette er testet og verifisert, vil man da være sikker på at e-post blir kryptert til samarbeidsparten. Om noen fikler med løsningen slik at krypteringen ikke aktiveres, vil e-posten forbli usendt.

For slike forbindelser bør det være gode rutiner for å opprette kommunikasjon mellom driftsavdelingene, slik at man får rettet opp i eventuelle feil i sertifikatvalidering som hindrer overføring av e-post.

3.4. Tiltrodd sertifikatutsteder

STARTTLS kan gi både autentisering og konfidensialitetsbeskyttelse. Konfidensialitetsbeskyttelse kan oppnås ved hjelp av selvsignerte sertifikater, men

8. Wildcard-sertifikater er sertifikater med uspesifiserte DNS-navn, som *.example.com.

9. Multidomain-sertifikater er sertifikater med multiple DNS-navn, som mx1.example.com og mx2.example.com.

autentisering får man bare om man benytter sertifikater utstedt av en tiltrodd tredjepart.

NSM anbefaler derfor å bruke sertifikater utstedt fra en tiltrodd tredjepart. Etter flere hendelser med sertifikatutstedere og angrep ved hjelp av sertifikater, anbefaler NSM at sertifikater utstedt under norsk lovgivning benyttes.

3.5. Beskyttelse mot skadevare

Mange systemer benytter en tiltrodd man-in-the-middle for inspeksjon av e-postkommunikasjon. Denne inspeksjonen benyttes både for å sjekke at skadevare verken mottas eller sendes, og hindre at sensitiv informasjon slipper ut. Sistnevnte kalles gjerne data leakage prevention.

For at slike systemer skal fungere når man etablerer STARTTLS er det mest hensiktsmessig at STARTTLS etableres på dette systemet.

Om man etablerer STARTTLS på en e-posttjener bak dette systemet, må systemet få en kopi av sertifikat og privat nøkkel for å kunne utføre innholdsinspeksjonen. Hvis ikke nøkler blir tilgjengelige, vil ikke innholdsinspeksjonen kunne utføres.

3.6. Sikring av e-post internt

For organisasjoner med distribuerte e-posttjenere anbefales det å sikre forbindelsene mellom disse. Hvis e-poster sendes over Internett mellom indre og ytre e-posttjener, bør disse forbindelsene krypteres. Dette kan for eksempel gjøres ved hjelp av kryptert VPN.

3.7. Konfigurasjon av STARTTLS og sertifikat

NSM har ikke utarbeidet konfigurasjons- og installasjonsveiledninger for STARTTLS og sertifikater. Dersom ytterligere informasjon er nødvendig for å konfigurere og installere STARTTLS, anbefaler NSM å ta kontakt med utvikler og/eller leverandør av organisasjonens e-post-løsning.

Anbefaling 2: Sender Policy Framework (SPF)

HVA: Sender Policy Framework (SPF) [3] er en mekanisme for mottakers MTA for å sjekke om IP-adressen til avsenders MTA er autorisert til å sende e-post på vegne av avsender-domenet. Hvis dette ikke er tilfellet, kan SPF angi om eposten skal forkastes eller ikke.

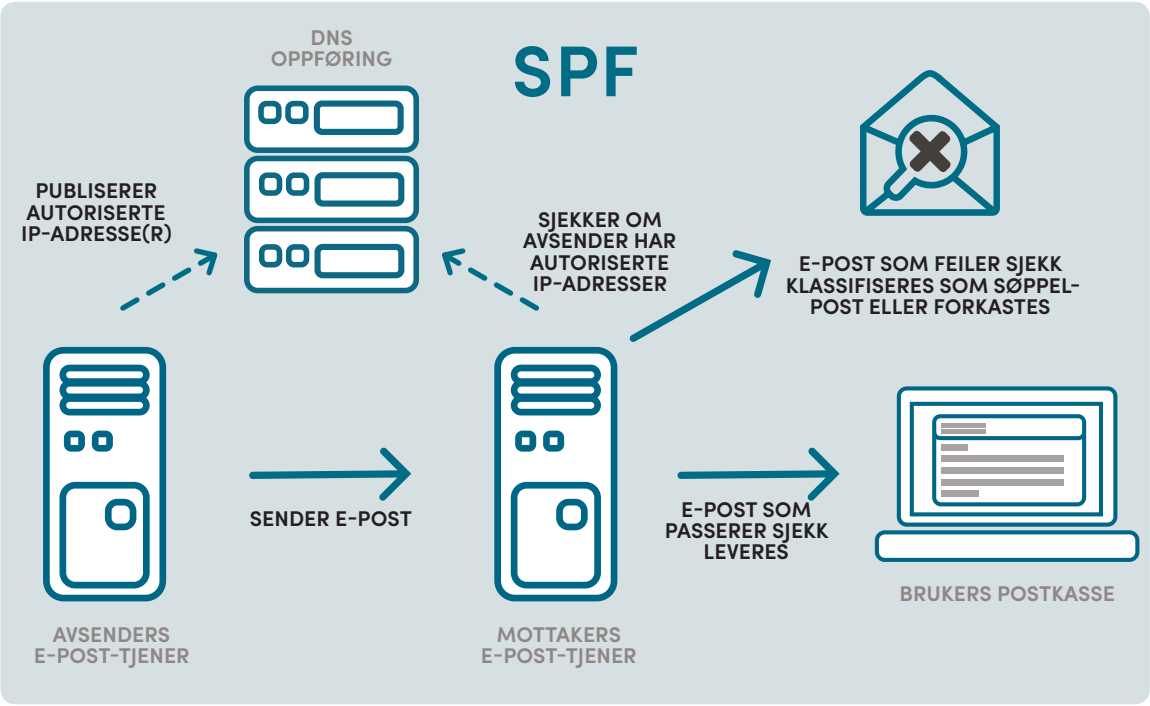
SPF stopper ikke all uønsket e-post. Hvis en trusselaktør har kontroll over en e-post-konto/klient for en virksomhet som benytter SPF, vil e-post sendt fra den kompromitterte konto/klienten passere en SPF-sjekk. Uønsket e-post sendt på vegne av domener som ikke benytter SPF vil ikke fanges opp i en slik SPF-sjekk.

HVORDAN: Mottakers MTA sjekker mot DNS om det finnes en SPF-record for avsender-domenet og om avsender-MTAs IP-adresse korresponderer med denne. Hvis IP-adressen til avsenders MTA korresponderer med tillatte IP-adresser i SPF-recorden til avsender-domenet i RFC5321. MailFrom (også kjent som envelope-from), blir den levert som normalt. Hvis informasjonen ikke stemmer kan e-posten avvises, merkes som spam, eller leveres på vanlig måte avhengig av hvordan SPF-recorden er satt opp.

Eksempel på enkel og streng SPF-policy satt i DNS:

```
example.com IN TXT “v=spf1 mx -all”
```

"Kun MX-tjenere for example.com har lov til å sende e-post på vegne example.com."[10]



***Figur 1** Virkemåte for Sender Policy Framework (SPF)*

10. Eksemplet forutsetter at tjener for mottak og sending er den samme.

HVORFOR: Hvis et domene benytter SPF, blir sending av spam eller phishing («nettfiske») med det domenet som avsender langt vanskeligere. Spam-filtre som sjekker mot SPF vil gi e-poster som feiler SPF en høy «spam-score» noe som hever sjansen for at meldingen klassifiseres som spam/uønsket e-post og avvises/ikke leveres til mottaker. Siden SPF håndteringen kommer før søppelpost-filtreringen, kan mye e-post bli forkastet allerede her. De domener som benytter SPF blir dermed mindre attraktive for spammere/phishere.

Merk: Gjennom bruk av SPF forteller du resten av verden hva de bør eller skal gjøre, men du vet faktisk ikke om a) de gjør som du anbefaler i din SPF, eller b) om andre forsøker å utgi seg for å være deg. SMTP protokollen og e-postklienten henter informasjon av avsender fra ulike felter (envelope from/ message from), og en angriper kan derfor forfalske avsenderen som vises til mottaker. SPF hindrer ikke slik forfalskning, men med «identifier alignment» i DMARC kreves det at begge felter er like.

Det er minst like viktig å bruke SPF på egne domener som ikke brukes til å sende e-post ("v=spf1 -all"). Dette vil redusere risikoen for at en angriper effektivt kan sende falsk e-post på vegne av virksomhetens domener (spoofing). Et eksempel på dette er der bedriften benytter et domene til utsending av epost («example.com») mens nettsiden er på et annet domene («example.org»).

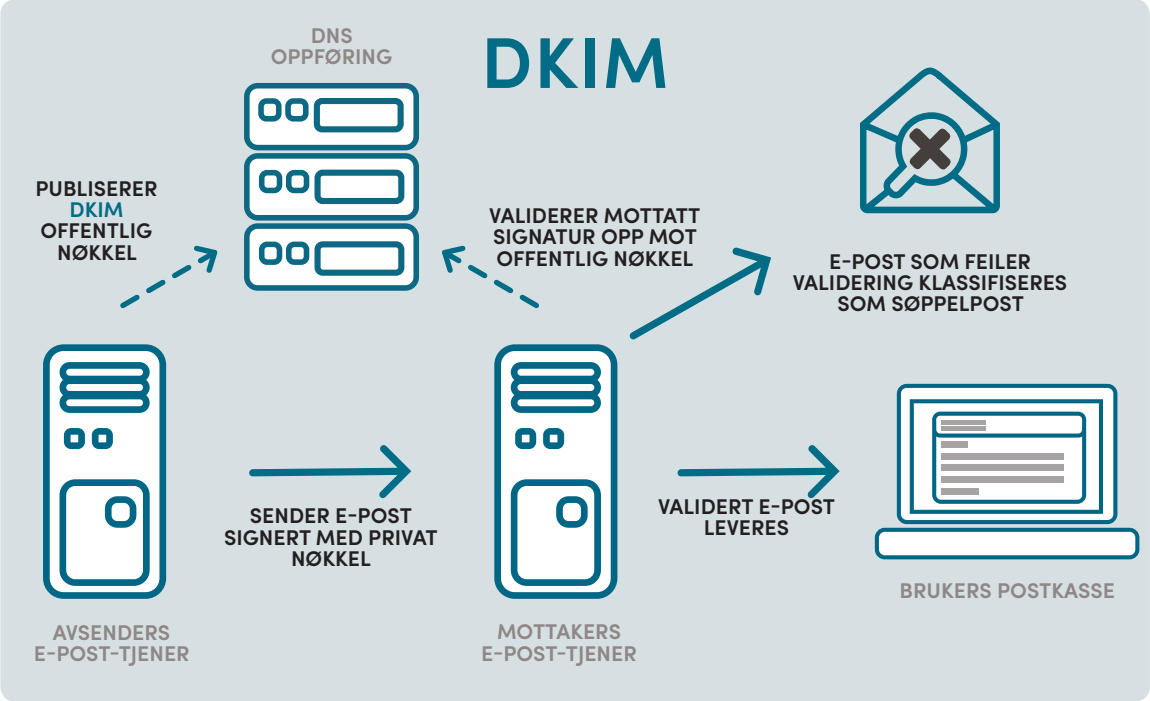
SPF er et viktig første skritt mot å være en del av løsningen, men er ikke nok i seg selv.

Anbefaling 3: DomainKeys Identified Mail (DKIM)

HVA: DomainKey Identified Mail (DKIM) [4] er en metode å legge til en digital signatur som autentiserer avsenders domene og verifisere at (deler av) e-posten ikke har blitt endret under sending. Mottakers MTA kan verifisere den digitale signaturen og filtrere ut e-poster som feiler DKIM-sjekken.

HVORDAN: Avsenders MTA legger en digital signatur på all utgående e-post. Mottakers MTA kan sjekke signatur mot informasjon publisert i DNS

DKIM benytter asymmetrisk kryptering med en offentlig og en privat nøkkel. En digital signatur blir lagt til som en egen e-post-header før e-posten sendes. Mottakers MTA gjør så et oppslag i DNS for å hente den offentlige nøkkelen for å validere signaturen. Hvis DKIM-sjekken feiler, kan e-posten avvises.



Figur 2 *Virkemåte for DomainKeys Identified Mail (DKIM)*

HVORFOR: DKIM kan bekrefte at en e-post er sendt på en måte som er autorisert av eier av domenet.

Uønsket e-post kan ofte ha forfalsket avsenderadresse og innhold (meldingskropp). For eksempel kan en trusselaktør sende en e-post som ser ut som den kommer fra datasikkerhetsleder@example.com, selv om avsender ikke er fra denne konto/bruker eller fra noen fra avsenders virksomhet. Hensikten til trusselaktøren kan være å overbevise mottaker om å lese og godta e-posten, levere skadevare eller få mottaker til å besøke en URL. Det kan være vanskelig for mottaker å avgjøre hvorvidt en e-post er legitim. DKIM imøtekommer denne problemstillingen, ved at avsenders domene og e-post-meldingen valideres mot den inkluderte signaturen.

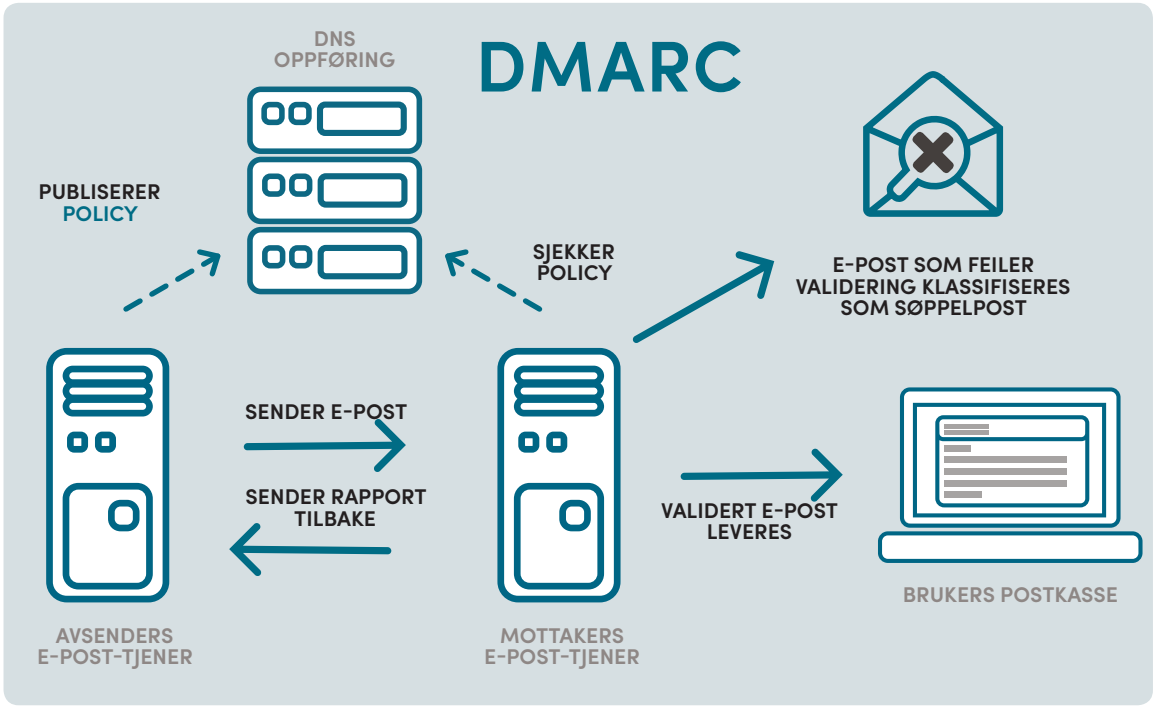
Anbefaling 4: Domain based Message Authentication, Reporting and Conformance (DMARC)

HVA: DMARC [5] baserer seg på SPF og/eller DKIM, og forteller hvordan mottaker skal behandle e-post som feiler disse sjekkene. I tillegg tilbyr standarden en rapporteringsprotokoll som muliggjør en større grad av rapportering av feilet e-post for både mottaker og avsender MTA. Dette medfører at du kan få tilbakemeldinger på:

- Hvordan e-post fra deg blir behandlet hos mottakers MTA (akseptert, satt i karantene eller avvist).
- E-post som er sendt på vegne av ditt domene, men som ikke er autorisert ved hjelp av SPF og/eller DKIM.

HVORDAN: DMARC sjekker om innkommende e-post faktisk kommer fra domenet det påstår ved å sjekke SPF og/eller DKIM. Standarden muliggjør videre at et domene kan publisere en «policy» på hvilke mekanismer (SPF og/eller DKIM) som benyttes og hva mottaker bør gjøre hvis disse sjekkene feiler. Et eksempel på en slik policy kan være: «Hvis DKIM-signaturen er ugyldig, eller hvis SPF-sjekken feiler, så skal e-posten behandles som søppelpost, og det skal sendes en kopi tilbake til meg. I tillegg skal aggregerte rapporter sendes til meg.»[11]

I tillegg tilbyr DMARC rapportering tilbake til (administrator av) avsender-domenet, slik at disse blir varslet om at noen benytter deres domene for å forsøke å sende uønsket e-post.



Figur 3 Virkemåte for Domain-based Message Authentication, Reporting and Conformance (DMARC).

HVORFOR: For mottaker av e-post som utfører DKIM er det opp til mottaker å gjette hvordan e-post som feiler disse skal behandles. DMARC fjerner denne «gjettingen», da avsender i tillegg publiserer hvordan e-post som feiler SPF/DKIM bør behandles. En viktig funksjonalitet i DMARC er rapporteringsmekanismen som SPF og DKIM mangler. DMARC har også en strengere mekanisme for sjekk av e-post («alignment»). SPF og DMARC er ment å fungere før søppelpostfilter, men på ingen måte som et søppelpostfilter.

11. Dette vil angis som følger: `_dmarc.example.com IN TXT "v=DMARC1; p=reject; rua=mailto:dmarc@example.com; ruf=mailto:dmarcfull@example.com"`

Vedlegg A Dokumenthistorie

2013-11-21 Dokument etablert på bakgrunn av foredrag under Nasjonal sikkerhetsmåned 2013 og blogginnlegg «Kryptert e-post».

2014-01-17 Dokumentet sendt på intern høring.

2014-02-03 Dokumentet godkjent for publisering.

2017-10-21 Dokumentet omarbeidet til å inkludere beskyttelsesmekanismene SPF, DKIM og DMARC.

2017-11-08 Dokument sendt på intern høring, og ekstern høring til sektorvise responsmiljøer (SRM) og Norid.

Vedlegg B Referanser

[1] IETF, « Simple Mail Transfer Protocol,» IETF, 2008.

[2] IETF, «SMTP Service Extension for Secure SMTP over Transport Layer Security,» IETF, 2002.

[3] IETF, «Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1,» IETF, 2014.

[4] IETF, «DomainKeys Identified Mail (DKIM) Signatures,» IETF, 2011.

[5] IETF, «Domain-based Message Authentication, Reporting, and Conformance (DMARC),» IETF, 2015.

NASJONAL SIKKERHETSMYNDIGHET (NSM)

67 86 40 00

Postboks 814
1306 Sandvika

post@nsm.stat.no
www.nsm.stat.no