CENTER FOR CYBERSIKKERHED

Reducér risikoen for falske mails

Center for Cybersikkerhed

November 2017

Indledning
Center for Cybersikkerhed oplever i stigende grad, at danske myndigheder og virksomheder udsættes for cyberangreb. Det sker ofte ved, at medarbejderen modtager en e-mail, som ser ud til at være sendt fra eksempelvis en kollega, samarbejdspartner eller offentlig myndighed.

Et redskab til at imødegå denne trussel er protokollen DMARC (Domain-based Message Authentication, Reporting and Conformance), som gør det muligt at forhindre mails med en forfalsket afsender i at nå ud til slutbrugere og samtidig begrænse misbrug af de domænenavne, organisationen ejer.

Angreb via spam, phishing og spoofing er stigende i antal, og det er derfor værd at vurdere ethvert tiltag, der kan reducere risikoen. Derfor anbefaler Center for Cybersikkerhed, at organisationer implementerer teknologien DMARC. Center for Cybersikkerhed har selv igangsat processen med at implementere DMARC på centrets domæner.

Center for Cybersikkerhed beskriver i vejledningen "Spear-phishing – Et voksende problem" denne type angreb og giver en række anbefalinger til at imødegå truslen.

For mindre organisationer med ét eller få domæner og en simpel e-mail-anvendelse kan implementering af DMARC gennemføres med få ressourcer. Det forudsætter, at man implementerer en række sikkerhedstiltag både på organisationens e-mail-server og i forbindelse med registreringen af organisationens domæner. Denne vejledning forklarer, hvad DMARC gør for at øge sikkerheden, og hvilke tiltag der skal til for at komme i gang.

Vejledningen henvender sig først og fremmest til organisationers it-ledelse. Det er hensigten, at vejledningen leverer grundlaget for it-ledelsens kommunikation til topledelsen om, hvad DMARC kan bidrage med fra et forretningsmæssigt perspektiv. Herudover er det målet at understøtte it-ledelsens overvejelser inden implementering af DMARC i organisationen samt at levere et indblik i, hvordan DMARC virker, og hvordan teknologien kan implementeres i praksis.

Formål med DMARC
DMARC giver en organisation mulighed for at kontrollere brugen af sine domæner. Herudover bidrager DMARC til at håndtere indkomne e-mails, der ikke lever op til det DMARC-regelsæt, som domæneejeren har defineret, herunder e-mails med en falsk afsender.

Siden oktober 2016 har det været et krav, at statslige myndigheder i Storbritannien anvender DMARC.

I oktober 2017 blev det et krav, at statslige myndigheder i USA skal implementere DMARC.

Hvad får man ud af at implementere DMARC?
Implementeringen af DMARC giver som nævnt organisationen nogle fordele i forsvaret mod en række konkrete angrebsmetoder, såsom phishing og spoofing. Herudover:

- DMARC giver mulighed for at få overblik over misbrug af organisationens domæner.
- DMARC kan på sigt bidrage til at imødegå misbruget af organisationens domæner i falske e-mails.
- DMARC kan reducere antallet af SPAM-mails, som organisationen modtager.
- DMARC giver organisationens kunder, samarbejdspartnere mv. garanti for afsenderautenticiteten i de e-mails, der er udsendt med organisationens domæne som afsender.

Anbefalinger til implementering af DMARC

DMARC løser ikke alle problemer i forbindelse med spam og phishing, men Center for Cybersikkerhed anbefaler, at organisationer anvender denne teknologi, fordi den bidrager til at imødegå disse trusler. Jo flere der anvender denne teknologi, jo større virkning har den.

I forbindelse med implementering af DMARC skal følgende gennemføres og vurderes:

- Topledelsen skal informeres om fordele og ulemper ved anvendelsen af DMARC.
- En ekstern leverandør kan inddrages, hvis organisationen ikke selv råder over relevante kompetencer til at implementere DMARC.
- Udarbejd en plan for implementering af DMARC.
- Etabler et overblik over alle aktive domæner, samt passive domæner som organisationen ønsker at beskytte mod misbrug.
- Afsæt ressourcer til gennemgang af DMARC-aggregerede leveringsrapporter.
- Start med at bruge monitorerings-optionen (DMARC-politik for håndhævelse sættes til ”None”) og gennemgå de indkomne leveringsrapporter. Rapporterne kan sammen med statistik og observationer i øvrigt være med til at give indsigt i de fordele, implementering af DMARC vil have for organisationen.
- Verificer, at løsningen virker efter hensigten. Tilret om nødvendigt opsætningen med henblik på at rette fejl og mangler.
- Start selv med implementeringen, og indgå derefter dialog med samarbejdspartnere om, at de også implementerer DMARC.
- Eskaler håndhævelsen af DMARC-politikken til ”Karantæne” eller ”Afvis”.
- Forsæt arbejdet med awareness blandt medarbejderne om mail-trusler, herunder phishing og domæne-spoofing.

Hvad er DMARC?
DMARC er en e-mail-autentifikations-protokol, som sætter en politik for anvendelsen af to andre protokoller: SPF og DKIM. Tilsammen giver de den bedste beskyttelse mod domænemisbrug.

SPF (Sender Policy Framework) er et simpelt system til validering af mails, og er designet til at detektere spoofing. Modtageren af en mail kan kontrollere, at indgående mails fra et domæne kommer fra en server (IP-adresse), der er godkendt af domæne-ejeren (afsender). Listen over godkendte servere for et domæne publiceres via domænets DNS-oplysninger.

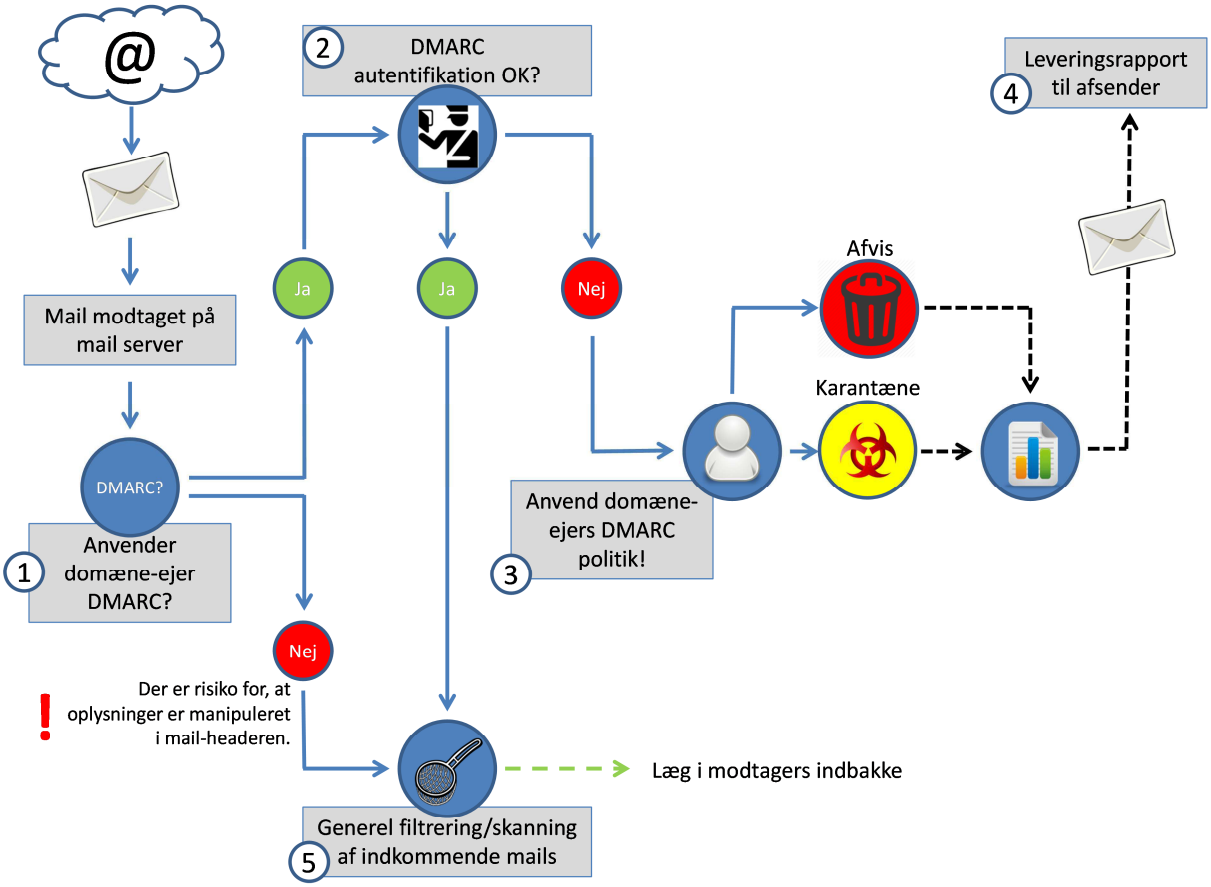
DKIM (DomainKeys Identified Mail) beskriver, hvordan der kan knyttes et domæne-specifikt id til en mail. Domæne-ejeren kan signere den enkelte mail med en privat signeringsnøgle og dermed give modtageren mulighed for at verificere, om mailen er afsendt fra en server, der er registreret i DNS (Domain Name System). Verifikationen sker på baggrund af den afsendende servers offentlige signeringsnøgle, der er tilgængelig via DNS.

DMARC indeholder en rapporteringsfunktion, der gør det muligt for domæneejere at overvåge og forbedre beskyttelsen af afsenderes domæner mod misbrug gennem falske mails.

Uden brug af DMARC vil ejeren af et misbrugt domæne således ikke blive informeret om misbruget. Afsender af en e-mail sikret med SPF/DKIM alene vil ikke blive informeret, når SPF/DKIM-kontrollen fejler hos modtageren, og mailen derfor afvises. Det skal bemærkes, at en e-mail stort set aldrig afvises alene pga. en forkert DKIM-signatur, medmindre der samtidig anvendes DMARC.

Hvis et domæne misbruges i en e-mail – og organisationen har implementeret DMARC-regelsættet – så vil den falske e-mail blive opdaget og slettet. DMARC giver domæneejeren mulighed for at blive informeret om årsagen til, at e-mails afvises i DMARC-kontrollen.

Sådan håndterer DMARC en e-mail



Figur 1 - Oversigt over DMARC verifikationen

Konkret fungerer DMARC ved at verificere både autentifikationsoplysninger (baseret på DKIM) i den enkelte e-mails header og autorisations- og håndteringsoplysninger fra det afsendende domænes DNS-registrering (baseret på SPF). Figur 1 viser, hvordan verifikation af autentifikations-, autorisations- og håndteringsoplysninger forløber. Tallene i parentes henviser til tallene på figuren.

1. Ved modtagelse af en e-mail kontrollerer mail-server (eller mail-gateway), om afsender anvender DMARC (1). Denne oplysning findes i DNS-serveren (Domain Name System). Anvender afsender DMARC, kontrolleres SPF- og DKIM-oplysningerne, herunder den afsendende e-mail-servers IP-adresse og DKIM-signering (2). Hvis afsender ikke anvender DMARC, vil den aktuelle e-mail blive sendt til efterfølgende håndtering (filtrering/skanning) i modtagerens generelle mail-sikrings løsning (5).
2. Hvis SPF- og DKIM-kontrollen viser, at e-mailen er autentisk, sendes den til håndtering (filtrering/skanning) i modtagerens generelle mail-sikringsløsning (5).
3. Viser kontrollen, at e-mailen muligvis er falsk, vil håndteringen afhænge af domæneejerens, dvs. af afsenderens DMARC-politik (3). På baggrund af den opsatte DMARC-politik, som er angivet i domæneejerens DNS-record, vil den pågældende e-mail som udgangspunkt blive afvist eller sat i karantæne til håndtering. Den opsatte DMARC-politik kan være defineret, så e-mailen videresendes til modtager med en advarsel, eller videresendelse kan ske i den efterfølgende håndtering.

4. Hvis afsender i sin DNS-record har defineret, at der skal leveres en rapport, afsendes rapporten øjeblikkeligt (4). Det er også muligt at få daglige, aggregerede rapporter. Leveringsrapporten kan tilpasses i overensstemmelse med det niveau for fejlrapportering, som organisationen ønsker at modtage. Det kan vurderes, om leveringsrapporten skal sendes til en ekstern mailboks, med henblik på at adskille denne fra organisationens øvrige e-mails f.eks. for at undgå overbelastning af interne mailservere. Disse valg angives i organisationens DMARC-record.
5. Endelig gennemføres håndteringen (filtrering/skanning) af en e-mail i modtagers system (5), og hvis den godkendes som autentisk, oversendes den til den endelige brugers indbakke hos modtager.

Fordele, udfordringer og begrænsninger

DMARC beskytter organisationens domæner mod misbrug. Hvis en ondsindet aktør sender en e-mail og angiver et DMARC-, SPF- og DKIM-beskyttet domæne som afsender, så vil modtagerens mailserver kunne bruge de tre protokoller til at afvise mailen og beskytte slutbrugeren mod e-mails med en falsk afsenderadresse. DMARC understøtter således både beskyttelse af afsenders omdømme ved at gøre det vanskeligere at udsende falske e-mails og beskyttelse af modtagers medarbejdere.

Domæner, der ikke er beskyttet med DMARC, vil fortsat kunne misbruges. Organisationens brugere vil derfor kunne modtage falske e-mails, der ser ud til at komme fra autentiske domæner. Gevinsterne ved anvendelse af DMARC stiger således i takt med, at flere organisationer anvender teknologien.

DMARC er mest effektiv, hvis man har implementeret både SPF og DKIM. Omvendt er disse to teknologier også mest effektive, hvis man samtidig anvender DMARC. Uden DMARC er det alene op til modtagers mailserver, hvordan SPF og DKIM skal håndteres og respekteres.

For organisationer med en kompleks e-mail-infrastruktur, hvor der udsendes nyhedsbreve gennem eksterne leverandører på vegne af forskellige afdelinger, vil implementering af DMARC kunne udgøre en udfordring. Dette kan løses i forbindelse med definition af rapportering.

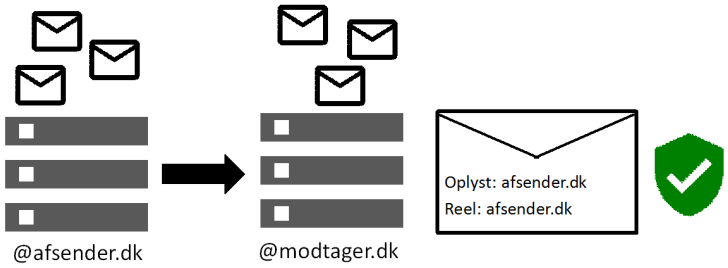
DMARC, SPF og DKIM beskytter ikke mod f.eks. ”typosquatting”. Det vil sige misbrug, hvor et domænenavn, som kan forveksles med et legitimt domæne, anvendes til afsendelse af en phishing-mail.

Tre scenarier for DMARC-beskyttelse

I de to første af nedenstående scenarier beskytter anvendelse af DMARC, mens det tredje scenarie kræver yderligere tiltag som f.eks. registrering af potentielle typosquatting-domæner.

Scenarie 1 (normale forhold)

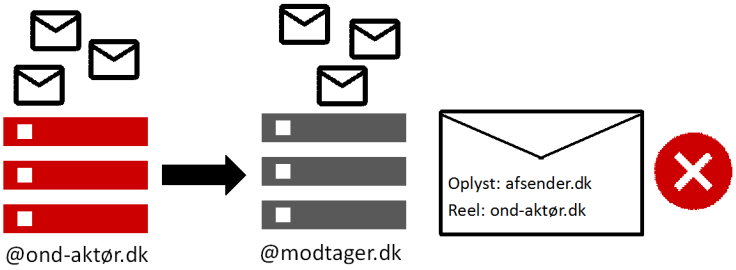
DMARC-teknikken vil tillade, at mails sendes og modtages på normal vis (afsender = opfattet afsender).



Figur 2 – Scenarie 1

Scenarie 2 (domæne ændret af ondsindet aktør)

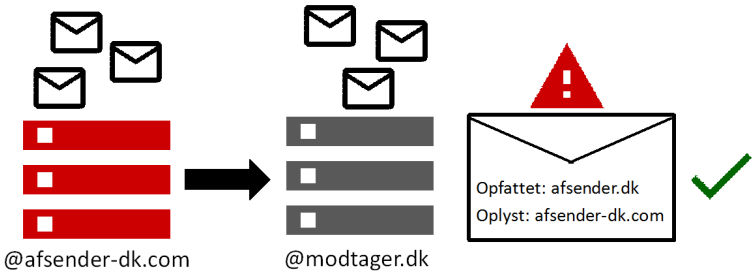
Hvis en ondsindet aktør bevidst har ændret domænenavnet til noget andet, f.eks. til domænet på en kendt virksomhed, vil DMARC afvise denne.



Figur 3 - Figur 2 – Scenarie 2

Scenarie 3 (domænenavne ligger tæt op af hinanden)

Hvis den ondsindede aktørs domænenavn ligger tæt op ad en kendt virksomheds domænenavn, vil anvendelsen af DMARC ikke blokere for en mail sendt fra domænet. Derfor er der risiko for at brugeren, der modtager mailen, forveksler den ondsindede aktørs mail med en mail fra den kendte virksomhed. Her vil det være op til den modtagende organisations øvrige sikringsforanstaltninger mod uønskede mails. For eksempel domænefiltrering og awareness blandt medarbejderne for at sikre, at modtagerne er opmærksomme på risikoen for forveksling. Medarbejderne bør løbende uddannes i at have en "kritisk" tilgang til mails.



Figur 4 - Figur 2 – Scenarie 3

Forudsætning for aktivering af DMARC

Etableringen af DMARC behøver ikke at være en stor udfordring, men før en organisation kan gå i gang med en implementering, er der en række forudsætninger, som bør være på plads.

1. Der skal være overblik over, hvor mange domæner organisationen råder over (og anvender). Det kan være en omfattende opgave, hvis oprettelsen af domæner ikke er styret fra centralt hold i organisationen.
2. Der skal være en proces for, hvem der kan varetage administrationen af DNS-oplysningerne.
3. Organisationen skal have et overblik over de domæner, der anvendes til mail, herunder hvilke mail-servere der indgår. Overblikket er nødvendigt for at eksempelvis nyhedsbreve, der udsendes fra eksterne bureauer, ikke blokeres.
4. Det skal identificeres, hvem der varetager administrationen af organisationens mail-anvendelse. Sker dette hos en it-service-udbyder, skal der foreligge en klar aftale om relevante forhold ved anvendelse af DMARC.
5. Der skal tages stilling til, hvorledes rapporteringen fra DMARC skal håndteres. Ved en aktivering af DMARC vil organisationen i yderste konsekvens modtage en leveringsrapport for hver afsendt mail, med mindre det er defineret, hvordan leveringsrapporterne skal aggregeres. Der er udviklet en række løsninger til automatiseret behandling af rapporterne, hvilket gør gennemgangen effektiv og mindre ressourcekrævende.

Referencer

Center for Cybersikkerhed vil gerne takke følgende for samarbejdet og den faglige sparring i forbindelse med udarbejdelsen af denne vejledning:

- Digitaliseringsstyrelsen
- Statens It
- Poul Otto Schousboe, Danske Bank
- Henrik Schack, www.dmarc.dk

Generel gennemgang og oplysninger om DMARC:

- www.dmarc.org
- https://dmarc.globalcyberalliance.org/how-it-works.html

Video om DMARC:

- https://www.youtube.com/watch?v=Ct0pEIguGsY