CENTER FOR CYBERSIKKERHED

Vejledning

DMARC

Reducér risikoen for falske mails

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

Forsideillustration: Areality Studio/Shutterstock

2. udgave februar 2022.

Indledning

Center for Cybersikkerhed (CFCS) vurderer, at phishing ved hjælp af mails udgør en vedvarende og alvorlig cybertrussel mod alle myndigheder, virksomheder og borgere i Danmark. CFCS vurderer, at de fleste cyberangreb i dag indledes med en phishing-mail.

Et redskab til at øge organisationens modstandsdygtighed over for phishing, misbrug og forfalskning af organisationens maildomæner er Domain-based Message Authentication, Reporting and Conformance (DMARC). DMARC er en teknisk standard, der kan bruges til at reducere risikoen for, at forfalskede mails kan udgive sig for at komme fra et domæne tilhørende en anden.

For mindre organisationer med få domæner og en simpel mail-anvendelse kan implementering af DMARC gennemføres med få ressourcer. Det kræver blot, at man implementerer en række relativt simple sikkerhedstiltag på organisationens mailsystem og på organisationens navnetjeneste (DNS).

Denne vejledning forklarer, hvilke tiltag der skal til og kommer med gode råd til at implementere DMARC. Den henvender sig først og fremmest til organisationers it-driftsafdeling.

Hvad er DMARC?
DMARC er en mail-standard, som sætter en politik for anvendelsen af to andre protokoller: Sender Policy Framework (SPF) og DomainKeys Identified Mail (DKIM). Tilsammen giver de den bedste beskyttelse mod domænemisbrug.

For statslige myndigheder er det et krav, at DMARC REJECT er implementeret på alle myndighedens domæner.

Overordnede anbefalinger

Nedenfor opstilles Center for Cybersikkerheds anbefalinger til anvendelse af DMARC for at beskytte organisationen mod misbrug af dens domæner som afsender på forfalskede mails og beskytte dens medarbejdere mod modtagelse af mails med falsk afsender. Anbefalingerne herunder uddybes på de følgende sider.

- Anvend DMARC med en REJECT-politik på alle domæner.
- Implementer SPF og DKIM på alle domæner.
- Behandl indkommende mails i henhold til afsenderdomænets DMARC politik.
- Gennemgå løbende de DMARC-rapporter, der modtages.

Hvad er DMARC?

Domain-based Message Authentication, Reporting and Conformance (DMARC)
DMARC er en mail-standard, der kan anvendes til at sætte en politik for to andre standarder: SPF og DKIM. Formålet er at give domæneejere mulighed for at beskytte deres domæne mod at blive misbrugt til afsendelse af forfalskede mails. Tilsammen giver DMARC, SPF og DKIM den bedste beskyttelse mod misbrug af organisationens domæne(r).

Ved at validere DMARC-politikken på indkommende mails kan visse forfalskede mails opdages, inden de leveres til modtagere i organisationen.

DMARC indeholder en rapporteringsfunktion, der gør det muligt for en domæneejer at modtage rapporter over andres forsøg på at sende forfalskede mails på vegne af domænet. Uden brug af DMARC vil ejeren af et misbrugt domæne ikke blive informeret om misbruget.

Sender Policy Framework (SPF)
SPF giver domæneejere muligheden for at bruge DNS til at offentliggøre, hvilke mail-servere der har tilladelse til at sende mails på vegne af domænet.

Grundlæggende indeholder SPF en liste over IP-adresserne på alle servere/gateways, der har tilladelse til at sende mails på vegne af et specifikt domæne. SPF giver derved den modtagende mailserver mulighed for at kontrollere at en mail, der hævder at komme fra et specifikt domæne, er sendt fra en IP-adresse, som er godkendt af det pågældende domænes ejer/administrator.

DomainKeys Identified Mail (DKIM)
DKIM er domæneejeres mulighed for kryptografisk at signere afsendte mails på vegne af domænet, de er sendt fra. Det fungerer ved at signere hver enkelt mail med en privat nøgle, så den modtagende mailserver kan bekræfte, at den kommer fra det angivne domæne ved at verificere signaturen med den tilhørende offentlige nøgle. Den offentlige nøgle for domænet kan hentes via DNS og er sikret mod manipulation, såfremt domænet er DNSSEC-signeret.

Fordele
DMARC kan beskytte organisationens domæner mod misbrug. Hvis en ondsindet aktør sender en mail og angiver et DMARC-, SPF- og DKIM-beskyttet domæne som afsender, vil modtagerens mailserver kunne bruge de tre teknologier til at opdage forfalskningen og afvise mailen.

Ulemper/Udfordringer
For organisationer med mange domæner og decentral administration af dem kan det være vanskeligt at have et fuldstændigt overblik over alle servere/tjenester, der kan sende mails på vegne af domænerne. Et eksempel på dette er organisationer, som udsender nyhedsbreve gennem eksterne leverandører. For at identificere servere/tjenester, der sender mails på vegne af organisationen, kan man starte DMARC-implementeringen i monitoreringstilstand (sæt DMARC-politikken til ”None”) og gennemgå de indkomne leveringsrapporter.

Domæner, der ikke er beskyttet med DMARC, vil fortsat kunne misbruges. Det er derfor vigtigt at implementere DMARC på alle organisationens domæner og ikke kun dem, der aktivt anvendes til mail (se afsnit: ”Beskyt alle organisationens domæner”). I

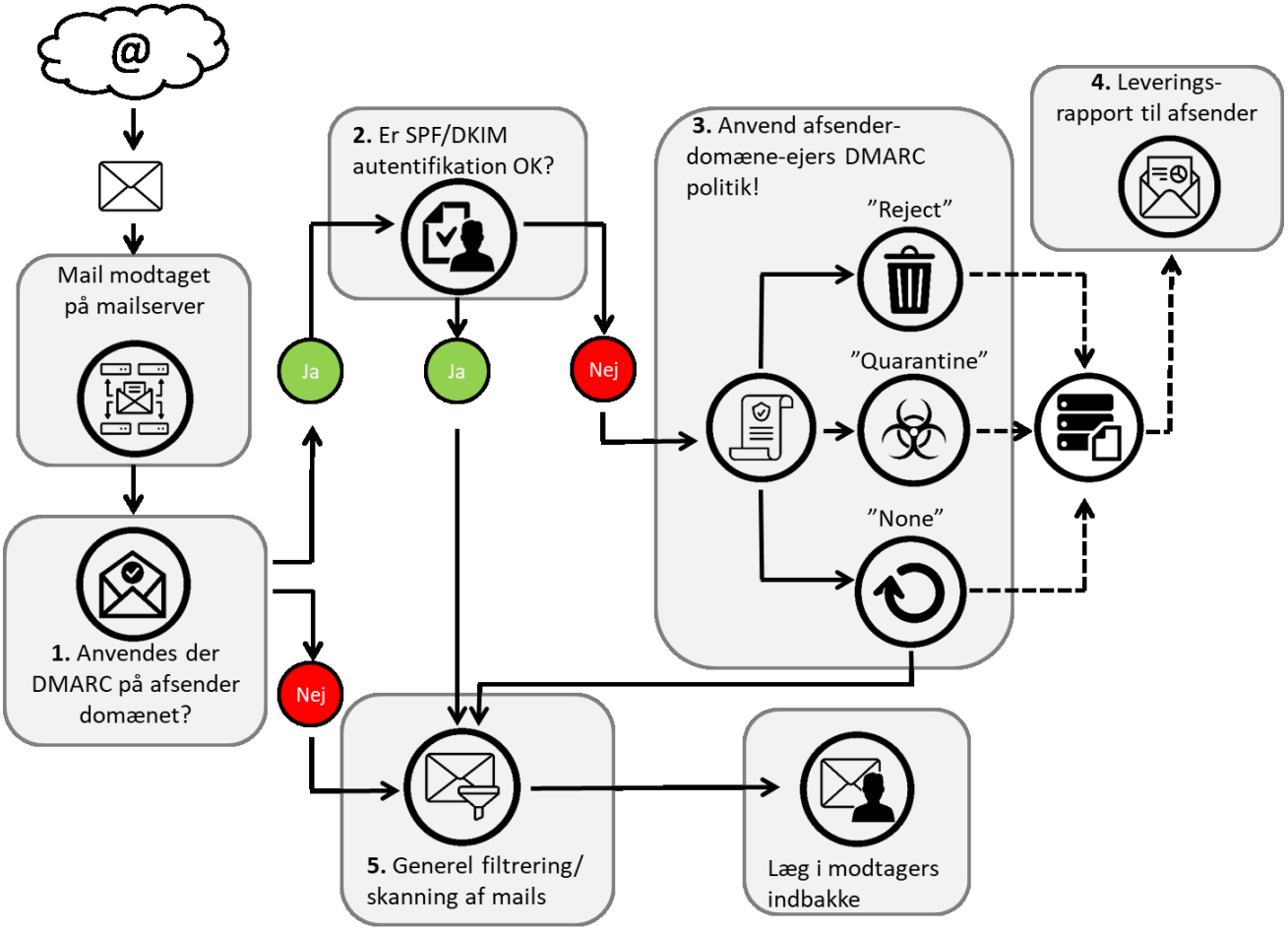
takt med at flere organisationer anvender DMARC, stiger værdien ved at validere indgående mails og evnen til at beskytte egne brugere mod phishing-angreb.

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. Det er muligt at opsætte DMARC uden DKIM og kun have DMARC og SPF. I sådan et tilfælde vil DKIM-tjek altid fejle.

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

CFCS anbefaler, at organisationer anvender DMARC med en REJECT-politik på alle domæner.

Sådan fungerer DMARC-verificering



Figur 1 - Oversigt over DMARC-verifikationen

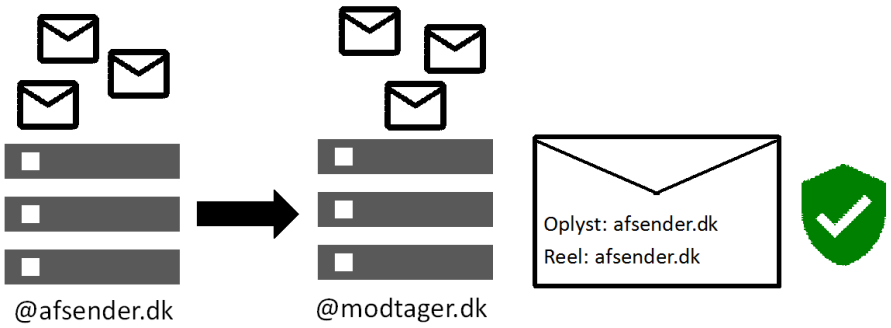
DMARC fungerer ved at verificere både autentifikationsoplysninger (baseret på DKIM) i den enkelte mails header, og autorisations- og håndteringsoplysninger fra det afsendende domænes DNS-registrering (baseret på SPF). Figur 1 viser, hvordan verifikation af autentifikations-, autorisations- og håndteringsoplysninger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

1. Ved modtagelse af en mail kontrollerer modtagers mail-tjeneste, om afsender anvender DMARC (1). Dette kan kontrolleres med et DNS-opslag. Anvender afsender DMARC, kontrolleres SPF- og DKIM-oplysningerne, herunder den afsendende mailtjenestes IP-adresse og DKIM-signering (2). Hvis afsender ikke anvender DMARC, vil den aktuelle mail blive sendt videre i processen til punkt (5) generel filtrering/skanning af mails.
2. Hvis SPF- eller DKIM-kontrollen viser, at mailen er autentisk, kan der foretages yderligere filtrering/skanning (5).
3. Viser kontrollen, at mailen muligvis er falsk, bør modtageren håndtere mailen i henhold til afsenders politik (3) og sætte den i karantæne (QUARANTINE) eller afvise den (REJECT).
4. Hvis afsender i sin DNS-record har defineret, at der skal leveres en rapport, afsendes rapporten (4). Det er 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 mails. Disse valg angives i organisationens DMARC-record.
5. Endelig gennemføres håndteringen (filtrering/skanning) af en mail i modtagers system (5). Hvis filtrerings- og skanningsmekanismerne ikke finder skadeligt indhold, leveres den til den endelige modtagers indbakke.

CFCS anbefaler, at organisationer behandler indkommende mails i henhold til afsenderdomænets DMARC-politik.

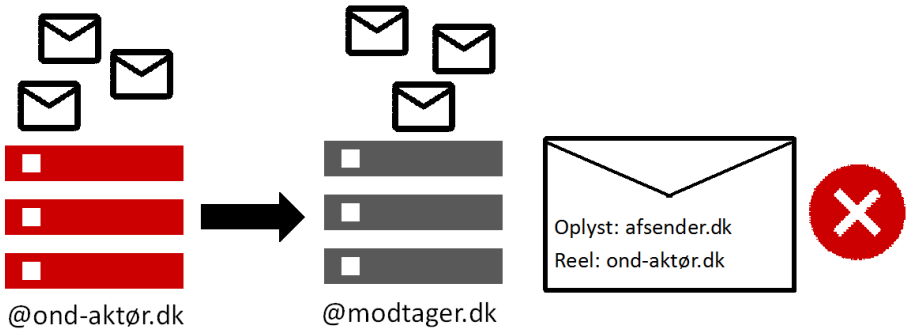
Tre scenarier for DMARC-beskyttelse
I de to første af nedenstående scenarier beskytter anvendelse af DMARC, mens det tredje scenarie kræver yderligere tiltag som f.eks. registrering af potentielle typosquatting-domæner.

Scenarie 1 (normale forhold)
DMARC-teknikken vil tillade, at mails sendes og modtages på normal vis (afsender = angivet afsender).



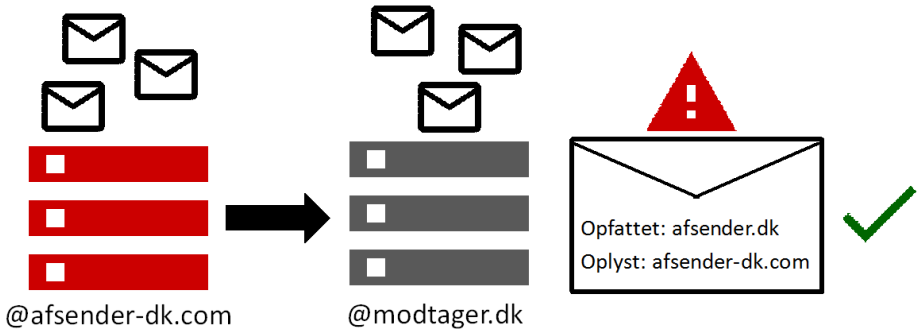
Figur 2 – Scenarie 1

Scenarie 2 (domæne ændret af ondsindet aktør)
Hvis en ondsindet aktør bevidst har forfalsket domænenavnet for at foregive, at mailen er afsendt af en anden, kan DMARC bruges til at opdage dette.



Figur 3 – Scenarie 2

Scenarie 3 (domænenavne ligger tæt op ad hinanden)
Hvis den ondsindede aktørs domænenavn blot ligner organisationens domænenavn, vil anvendelsen af DMARC ikke yde nogen beskyttelse. Derfor er der fortsat risiko for, at modtageren af mailen forveksler den ondsindede aktørs mail med en uforfalsket mail. Her vil det være op til den modtagende organisations øvrige sikringsforanstaltninger mod uønskede mails at opdage forfalskningen. Et væsentligt sikringstiltag er at medarbejdere løbende uddannes og trænes i at have en kritisk tilgang til mails.



Figur 4 – Scenarie 3

Forudsætning for aktivering af DMARC
Etableringen af DMARC behøver ikke at være en stor udfordring. Før en organisation kan gå i gang med en implementering, er der dog en række forudsætninger, som bør være på plads.

1. Der skal være overblik over, hvilke domæner organisationen ejer. Det kan være en omfattende opgave, hvis oprettelsen af domæner ikke er styret centralt.

2. Der skal være en proces for administrationen af organisationens DNS-oplysninger.

3. Organisationen skal have et overblik over alle tjenester, gateways og enheder, der kan sende mails på organisationens vegne. Overblikket er nødvendigt for, at eksempelvis nyhedsbreve, der udsendes via eksterne partnere, ikke blokeres.

4. Der skal aktivt tages stilling til, hvordan implementeringsprocessen håndteres. Eksempelvis hvorvidt der startes med en monitoreringsfase (NONE) og evt. (QUARANTINE), inden der implementeres (REJECT). Såfremt organisationens mailplatform varetages af en tredjepart, skal det sikres, at leverandøren håndterer mails ud fra organisationens ønsker.

5. Der skal tages stilling til, hvorledes rapporteringen fra DMARC skal håndteres. Da rapporterne ikke er i et manuelt letlæseligt format (XML), er der udviklet en række løsninger til automatiseret behandling af rapporterne, hvilket gør gennemgangen mere effektiv og mindre ressourcekrævende. Rapporterne kan eksempelvis anvendes til at opdage phishing-kampagner, der misbruger organisationens domæner og eventuelle nye servere/tjenester, som sender mails på organisationens vegne. Vær opmærksom på, at DMARC-fejl/forensics-rapporter indeholder personlig identificerbar information, og at nogle leverandører derfor har valgt ikke at understøtte dem. Aggregerede rapporter understøttes dog bredt.

CFCS anbefaler, at organisationer løbende gennemgår de DMARC-rapporter, der modtages.

Gode råd til implementering
Nedenstående råd er ikke en udtømmende liste, men bør indgå i arbejdet med implementering af DMARC.

Råd til organisationen:

- Informer topledelsen om fordele og ulemper ved anvendelsen af DMARC.
- Start med implementering i egen organisation, og indgå derefter i dialog med samarbejdspartnere om, at de også implementerer DMARC.
- Inddrag ekstern bistand, når organisationen ikke selv råder over relevante kompetencer til at implementere DMARC, SPF og DKIM.
- Afsæt ressourcer til håndtering og løbende gennemgang af DMARC-aggregerede leveringsrapporter.
- Forsæt arbejdet med awareness og adfærd blandt medarbejderne om mail-relaterede trusler, herunder phishing og domæne-spoofing.

Råd til implementering af DMARC:

- Udarbejd en plan for implementering af DMARC.
- Etabler et overblik over alle domæner, som organisationen ejer.
- Test eventuelt domæners status på https://sikkerpånettet.dk for at kortlægge, hvor der er mangler i forhold til opsætning af DMARC, DKIM og SPF.
- Implementer DMARC på alle domæner. Start med at monitorere (sæt DMARC-politikken til ”None”) og gennemgå de indkomne leveringsrapporter.
- Verificer, at løsningen virker efter hensigten. Tilret om nødvendigt opsætningen med henblik på at rette fejl og mangler.
- Eskaler håndhævelsen af DMARC-politikken til ”REJECT”.
- Sørg for, at SPF er implementeret på alle domæner.
- Sørg for, at DKIM er implementeret på alle domæner.
- Sørg for, at indgående mailgateways respekterer afsenders DMARC-politik.
- Gennemgå jævnligt DMARC-aggregerede leveringsrapporter.

Beskyt alle organisationens domæner

Trin til at beskytte domæner, der anvendes til mail
Når forudsætningerne for aktivering af DMARC er på plads, kan beskyttelsen implementeres i tre overordnede trin.

Trin 1: DKIM Genererer offentlig og privat nøglepar for hvert domæne. Publicer offentlig nøgle i DNS som TXT record(s). I eksemplet herunder er selector=test-mail, domæne=eksempel.dk, og den offentlige nøgle p er fiktiv:

```
test-mail._domainkey.eksempel.dk IN TXT "k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADowheeDCBiQKBgQCehqKMB6znGXo/pC83mGObm8
OWo4daBYBb9wqqDaflz7Mf9KW1oaUm9j7hQq7af7jh+DSw0tXWr4HbJrI50DW/QVHqYKlP
X3hvYUohBxg//T0u0rK3OSJss3OrpkoRqd150ynYxwwLymsjIwODT7Gf9WZPcL86rdboSR
m/ost4mwIDAQAB"
```

Konfigurer afsendende mailservere til at signere udgående mail med den private nøgle (følg leverandørens vejledning for, hvordan det gøres for det pågældende produkt).

Trin 2: SPF Opret en SPF record[1] for domænet, der angiver den eller de IP-adresser, som er godkendte til udsendelse af mails fra det respektive domæne. Brug eventuelt "include" for hvert tredjepartdomæne, der bruges til at sende mail på organisationens vegne. Eksempel:

```
eksempel.dk TXT " v=spf1 ip4:123.45.67.89
ip6:2a05:d018:e4:8c00:bb71:dea8:8b83:851e include:tredjepartdomæne.dk
-all "
```

Hvis der er tvivl om, hvorvidt man har fået identificeret alle tjenester, gateways og enheder, der kan sende mails på organisationens vegne, kan det overvejes at starte med at angive "softfail" (`~all`) og derefter ændre den til "hardfail" (`-all`), når alle godkendte afsendere er identificeret. Når der bruges "softfail", beder man modtager om, at mailen leveres videre i mailsystemet, eksempelvis til spamfolder, selvom den fejler SPF check. Ved brug af "hardfail" beder man modtager om at kassere mailen, når den fejler SPF check.

Trin 3: DMARC Opret en DMARC record[2] for domænet. Start med at sætte `p=none` og gennemgå leveringsrapporterne for at identificere fejl i konfigurationen og tilret om nødvendigt. Sæt herefter `p=reject` for at angive, at modtageren bør afvise mails, hvis SPF- og DKIM-kontrollerne for domænet fejler.

I eksemplet herunder er DMARC-politikken sat til "REJECT" for både domæne `p` og subdomæner `sp`. DMARC-aggregerede rapporter `rua` sendes til "dmarc-rua@eksempel.dk", DMARC-fejl/forensicsrapporter `ruf` sendes til "dmarc-ruf@eksempel.dk", hver gang enten SPF eller DKIM-tjek fejler `fo=1`, og modtageren anmodes om at behandle alle mails fra domænet i henhold til denne politik `pct=100`.

[1] https://tools.ietf.org/html/rfc7208
[2] https://tools.ietf.org/html/rfc7489

```
_dmarc.eksempel.dk TXT "v=DMARC1;p=reject;sp=reject;rua=mailto:dmarc-rua@eksempel.dk;ruf=mailto:dmarc-ruf@eksempel.dk;fo=1;pct=100
```

For mere detaljeret forklaring af valgmuligheder og indstillinger henvises til referencer sidst i vejledningen.

Trin til at beskytte domæner, der ikke anvendes til mail

Ud over en organisations domæne(r), der dagligt anvendes til mails, har organisationen som oftest registreret andre domæner til andre formål.

Selvom disse domæner ikke anvendes til udsendelse af mails af organisationen selv, kan de potentielt misbruges af andre til at sende falske mails i organisationens navn. Det er derfor vigtigt også at beskytte disse domæner mod at blive misbrugt.

De nedenstående trin vil hjælpe et potentielt offers mailsystem med at opdage falske mails sendt fra domæner, der ikke burde sende mails.

De tre trin er:

Trin 1: SPF Opret en SPF record[3] for domænet, der angiver, at ingen IP-adresser er godkendte til udsendelse af mails fra det respektive domæne:

```
eksempel.dk TXT "v=spf1 -all"
```

Trin 2: DMARC Opret en DMARC record[4] for domænet, der med en "REJECT"-politik angiver, at modtageren bør afvise mails fra dette domæne, som ikke lever op til SPF og DKIM kontrollerne:

```
_dmarc.eksempel.dk TXT "v=DMARC1; p=reject;"
```

Trin 3: Tom DKIM En tom DKIM record[5] er umiddelbart ikke nødvendig, men kan i nogle tilfælde skabe yderligere mistro til forfalskede mails. En tom DKIM record, som den nedenstående, angiver, at den offentlige signaturnøgle for domænet er udløbet:

```
*._domainkey.eksempel.dk TXT "v=DKIM1; p="
```

At reducere risikoen for, at falske mails udsendes fra ens domæne(r), hjælper både til at beskytte organisationens navn og rygte, men også mailmodtagerne mod at blive ofre for eksempelvis phishing. Ved implementering af de tre ovenstående tiltag har både domæneejer og modtagere af falske mails de bedste forudsætninger for at opdage forfalskningen.

Statslige myndigheder er pålagt at sikre alle domæner med en DMARC "REJECT"-politik, men alle andre domæneejere bør ligeledes overveje tilsvarende tiltag og dermed bidrage til bekæmpelsen af blandt andet phishing-mails.

Yderligere tiltag til domæner, der ikke anvendes til mail

De tre simple trin ovenfor bør være tilstrækkelige til at opdage forsøg på forfalskning af mails. Der er dog yderlige tiltag, en organisation bør overveje, hvis de vil have bedre indsigt i forsøg på misbrug af domænet, eller hvis de vil hjælpe det potentielle offers mailsystem til at foretage yderligere kontroller:

[3] https://tools.ietf.org/html/rfc7208
[4] https://tools.ietf.org/html/rfc7489
[5] https://tools.ietf.org/html/rfc6376

Trin 4: DMARC med rapportering Hvis en organisation er interesseret i at få indsigt i de falske mails, der er forsøgt afsendt fra domænet, kan der tilføjes en mailadresse til den eksisterende DMARC record som angivet nedenfor:

```
_dmarc.eksempel.dk TXT
"v=DMARC1; p=reject; rua=mailto:dmarc@andeteksempel.dk"
```

Den angivne mailadresse vil modtage aggregerede rapporter om falske mails sendt fra domænet. Adressen kan være en postkasse i et andet domæne tilhørende organisationen eller tilhøre en udbyder af DMARC-rapporterings- og analysetjenester, som organisationen har indgået en aftale med.

Trin 5: NULL MX Hvis et domæne ikke anvendes til mail, men anvendes til en hjemmeside, kan en NULL MX record[6] hjælpe med gøre det tydeligt for nogle mailsystemer, at den forfalskede mail ikke kan besvares. Sæt den til højeste prioritet (0):

```
eksempel.dk MX 0 .
```

Det er muligt, at den navneservertjeneste eller -software, der anvendes, ikke understøtter dette tiltag. Hvis det er tilfældet, eller hvis domænet ikke anvendes til en hjemmeside, kan tiltaget udelades.

For yderligere detaljer, eller hvis der anvendes subdomæner, refereres der til M3AAWG's Protecting Parked Domains Best Common Practices.

CFCS anbefaler, at organisationer implementerer SPF og DKIM på alle domæner.

[6] https://tools.ietf.org/html/rfc7505

Referencer

Sikker på nettet.dk – e-mailtesten
https://sikkerpånettet.dk/test-mail/

NIST Special Publication 800-177 Revision 1 (2019)- Trustworthy Email
https://csrc.nist.gov/publications/detail/sp/800-177/rev-1/final

National Cyber Security Centre (2019):
Protecting parked domains for the UK public sector
(https://www.ncsc.gov.uk/blog-post/protecting-parked-domains)

The Internet Engineering Task Force (IETF) Request For Comments (RFC)
https://datatracker.ietf.org/doc/html/rfc7489

M3AAWG Protecting Parked Domains Best Common Practices
https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12.pdf

Generel gennemgang af DMARC og oplysninger og værktøjer:

- www.dmarc.org
- https://dmarc.globalcyberalliance.org/how-it-works/
- https://mxtoolbox.com/dmarc/details/dmarc-tags

Center for Cybersikkerhed vil gerne takke Henrik Schack for faglig sparring i forbindelse med udarbejdelsen af denne vejledning.