CENTER FOR CYBERSIKKERHED

Falske mails fra passive domæner

To trin til at beskytte domæner, der ikke anvendes til mail, mod misbrug

Indhold

CENTER FOR CYBERSIKKERHED

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

1. udgave december 2019.

Indledning

Som beskrevet i CFCS' vejledning "Reducér risikoen for falske mails", kan DMARC hjælpe med at beskytte en virksomhed eller myndighed (herefter "organisationen") mod, at dennes domæner misbruges til udsendelse af falske mails. Organisationen medvirker dermed også til at beskytte de potentielle ofre for en falsk mail mod at blive udsat for et cyberangreb. Domæner, der bruges til afsendelse af mail, bør derfor altid beskyttes med anvendelse af DMARC. Organisationen råder dog ofte over mange andre domæner end de, der bruges til mail. De domæner kan også misbruges til falske mails.

Denne korte guide beskriver, i to simple trin, hvordan domæner, der normalt ikke anvendes til udsendelse af mail, bør beskyttes på tilsvarende vis.

Guiden er henvendt til de it-driftsfolk, der er ansvarlige for mailsikkerhed og navneserveradministration.

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.

For yderligere information om CFCS' anbefalinger vedrørende DMARC henvises til vejledningen "Reducér risikoen for falske mails" på CFCS' hjemmeside.

Baggrund
Ud over en organisations primære domæne(r), der dagligt anvendes til udsendelse af mails, har organisationen som oftest registreret andre domæner til andre formål. Det kan for eksempel være i forbindelse med en kampagne eller præventivt for at forhindre andre i at registrere et domæne, der har til formål at udnytte organisationens identitet.

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 passive domæner mod at blive misbrugt til eksempelvis udsendelse af spoofede phishingmails.

Tekniske minimumskrav for statslige myndigheder[1]
I regi af den nationale cyber-og informationssikkerhedsstrategi er der udgivet en række tekniske minimumskrav til it-sikkerheden hos statslige myndigheder. Blandt disse er kravet om at: "DMARC REJECT policy implementeres på alle domæner tilhørende myndigheden."

To trin til at beskytte passive domæner mod misbrug

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

NB: Husk at tilpasse domænenavne!

De to trin er:

Trin 1: SPF
Opret en SPF record[2] 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[3] for domænet, der med en REJECT policy angiver, at modtageren bør afvise mails fra dette domæne, der ikke lever op til SPF og DKIM kontrollerne:

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

At reducere risikoen for, at falske mails udsendes fra ens domæner, hjælper både til at beskytte organisationens navn og rygte, men også mailmodtagerne mod at blive ofre for eksempelvis phishing. Ved implementering af de to 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 policy, men alle andre domæneejere bør ligeledes overveje tilsvarende tiltag og dermed bidrage til bekæmpelsen af blandt andet phishingmails.

[1] https://sikkerdigital.dk/myndighed/tekniske-tiltag/tekniske-minimumskrav/
[2] https://tools.ietf.org/html/rfc7208
[3] https://tools.ietf.org/html/rfc7489

Ekstra tiltag

De to simple trin ovenfor bør være tilstrækkelige for at opdage forsøg på forfalskning af mails. Der er dog yderlige tiltag en organisation kan 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:

DMARC med rapportering

Hvis en organisation er interesseret i at få indsigt i de falske mails der er forsøgt afsendt fra det passive domæne, kan der tilføjes en mail adresse til den eksisterende DMARC record, som angivet herunder:

```
_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.

Tom DKIM

En tom DKIM record[4] 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="
```

NULL MX

Hvis et domæne ikke anvendes til mail, men anvendes til en hjemmeside, kan en NULL MX record[5] 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/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 sub-domæner, refereres der til M3AAWG's Protecting Parked Domains Best Common Practices.

CFCS anbefaler, at alle domæner beskyttes mod misbrug, uanset om de anvendes til udsendelse af mails eller ej.

[4] https://tools.ietf.org/html/rfc6376
[5] https://tools.ietf.org/html/rfc7505

Referencer

Center for Cybersikkerhed (2017):
Reducér risikoen for falske mails
(https://fe-ddis.dk/cfcs/publikationer/Vejledninger/Pages/default.aspx)

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

Messaging Malware Mobile Anti-abuse Working Group (2016):
Protecting Parked Domains Best Common Practices
*(*https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12.pdf)

Center for Cybersikkerhed vil gerne takke Henrik Schack (https://dmarc.dk) for faglig sparring i forbindelse med udarbejdelsen af denne vejledning.