Undgå falske mails med DMARC

Flere og flere virksomheder udsættes for cyberangreb – og især spam, phishing og spoofing er stigende i antal. En meget almindelig angrebsmetode består i, at en medarbejder modtager mails med en forfalsket afsender.

Protokollen DMARC (Domain-based Message Authentication, Reporting and Conformance) 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. DMARC beskytter således afsenders omdømme ved at gøre det vanskeligere at udsende falske e-mails og beskytter samtidig modtagers medarbejdere.

Med DMARC sikrer du, at...

- I på sigt undgår misbrug af organisationens domæner i falske e-mails
- I reducerer antallet af SPAM-mails, som organisationen modtager
- phishing ikke giver anledning til læk af data
- alle jeres mails er autoriserede og troværdige, så jeres brand ikke lider skade pga. falske mails.

DMARC giver altså en organisation mulighed for at kontrollere brugen af sine domæner, og jo flere organisationer der anvender denne teknologi, jo større virkning har den. 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.

Bemærk: DMARC, SPF og DKIM beskytter ikke mod f.eks. 'typosquatting' / 'URL hijacking', - altså misbrug, hvor et domænenavn, som kan forveksles med et legitimt domæne, anvendes til afsendelse af en phishing-mail.

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 (fupmails med falsk afsender).

DKIM (DomainKeys Identified Mail) beskriver, hvordan der kan knyttes et domænespecifikt id til en mail.