DMARC Overview

Opnå sikkerhed på e-mails med DMARC

Udsender du nyhedsmails og vigtige informationer til kunder og brugere, så bør du sørge for sikkerhed på e-mails – især hvis du er ansvarlig for domænet hos organisationen hvor e-mail er en vigtig kommunikationsvej. Dette uanset om I er en uddannelsesinstitution, et forsikringsselskab, bank, webbutik, større eller mindre virksomhed. DMARC-opsætning er vigtig for alle.

Flere og flere organisationer bliver ramt af, at udefrakommende forsøger at sende phishing- eller spammails via organisationens domænenavn. De Cyber kriminelle misbruger tilliden til organisationen eller organisationens brand. Falske e-mails er en nem måde at stjæle passwords, kreditkortnumre, få adgang til brugerkonti m.m. Det er derfor et eksplosivt viksende problem for organisationerne, da det svækker deres troværdighed og kan begrænse organisationens kommunikation via e-mail.

Falske e-mails et voksende problem

For kunder og brugere, som modtager e-mails, kan det være svært at skelne falske e-mails fra de rigtige, mens det for mailudbydere i stigende grad er blevet vanskeligere at blokere alle falske e-mails. For afsenderen er det vigtigt, at de e-mails, som organisationen sender ud, når frem. Ofte er afsenderen imidlertid uvidende om problemerne med verificeringen af egne e-mails i praksis, da man som afsender ofte, mangler indsigt i, hvilke e-mails der ikke når frem og hvorfor de ikke gør det.

De udfordringer kan du adressere med DMARC (Domain-based Message Authentication, Reporting & Conformance).

Sikker e-mailkommunikation

Med DMARC kan du beskytte dine brugere og kunder mod falske e-mails sendt fra dit domæne. Du kan samtidig sikre, at så stor en procentdel som muligt modtager dine e-mails, og at afsendte e-mails ikke bliver ændret undervejs, ikke havner i spamfoldere og karantæne eller bliver afvist.

Verificering af afsender

DMARC er en godkendelsesprocedure for e-mails. DMARC er designet til at beskytte mod domæne spoofing – dvs. når en e-mail sendes fra en uautoriseret afsender fra f.eks. en virksomheds domænenavn. Via protokollerne SPF (Sender Policy Framework) og DKIM (Domain Keys Identified Message – dvs. en signatur på e-mailen) gør DMARC det nemt for mailservere hos f.eks. Google, Hotmail eller Office 365 at verificere afsenderens identitet og dermed identificere evt. falske eller potentielt skadelige e-mails sendt fra dit domæne.

Ens håndtering af falske e-mails

Mailservere har hver deres policy omkring verificeringen af e-mails. Det betyder, at mens en e-mail hos f.eks. Google bliver markeret som spam, så vil den samme e-mail hos en anden udbyder ryge direkte videre i indbakken hos brugeren. Med DMARC kan du via egne policies guide mailserverne (via DNS) til, hvordan de

skal håndtere falske eller potentielt skadelige e-mails sendt fra dit domænenavn. Ved at anmode om at visse e-mails (som ikke er beskyttet med SPF og/eller DKIM) blokeres eller slettes, kan du eliminere modtagerens eksponering af falske e-mails fra dit domæne og dermed tilsikre at tilliden til organisationen ikke kompromitteres

Med DMARC sikrer du således, at alle mailservere håndterer dine e-mails på samme måde, når det gælder anmeldelse af spam, karantæne eller afvisning af e-mails. Via DMARC kan du desuden få feedback, når e-mails bliver modtaget eller blokeret. På den måde får man et større overblik og viden om hvor stor en del af de e-mails, du sender ud, som når frem.