PRODUKT

Sikker e-post

Hva oppnår du med å aktivere riktig sikkerhetsfunksjonalitet i Office 365?

Phising og spoofing øker risikoen for at data og brukernavn og passord kommer på avveie. DMARC/SPF/DKIM forhindrer identitetstyveri ved blant annet å autorisere hvilke IP-adresser som har lov å sende e-post fra kundens domene.

- Kun godkjente e-post servere kan sende e-post fra ditt e-post domene
- Redusert risiko for identitetstyveri, både m.h.t virksomheten og de ansatte

Ved å aktivere sikkerhets-funksjonaliteten i Office 365 reduseres risikoen for spoofing og phishing. Har din virksomhet implementert DMARC sammen med SPF/DKIM, vil du enklere kunne finne ut om en e-post kommer fra en verifisert avsender eller om avsenderen har mistbrukt noens e-postdomene. Du vil også motta rapporter som viser om domenet ditt misbrukes i svindel.

NYTTIGE BEGREPER:

SPF (Sender Policy Framework) brukes av en e-postserver for å sjekke om avsenderens e-postserver faktisk har lov til å sende e-post på vegne av det oppgitte domenet, for så å forhindre at falske e-poster går gjennom.

DKIM (DomainKeys Identified Mail)
Med DKIM legges det med en signatur som bekrefter at e-posten ble sendt på en måte som er autorisert av eieren av avsenderdomenet, og at aktuelle deler av e-posten ikke har blitt endret.

DMARC (Domain based Message Authentication, Reporting and Conformance) er en autentiseringsmetode som bruker SPF og DKIM for å verifisere at e-posten er sendt av den som faktisk eier domenet.

Pris: Etablering: 2990,-
Annet: Bruker må ha Microsoft 365®

Vil du vite mer, kontakt:
salg@eltele.serit.no eller 400 16 300 (innvalg Salg).