Difi
Direktoratet for forvaltning og ikt

Notat

Dato:	21.8.2018	**Saksnr:**	18/00643

Til:	Rune Karlsen
Kopi:	
Fra:	Seksjon for informasjonssikkerhet
Saksbehandler:	Håkon Styri

Saksframlegg til Standardiseringsrådets møte 21.06.2018

Anbefalt standard for sikkerhet i domenenavnsystem (DNSSEC)

Det følgende er forslag til en ny standard for å styrke sikkerheten i domenenavnsystemet (DNS), som er en underliggende funksjon som er viktig for de fleste av dagens digitale tjenester. Standarden kan enten plasseres i de eksisterende bruksområdet Grunnleggende datakommunikasjon eller det kan opprettes et nytt bruksområde med navn Digital infrastruktur.

> «Det anbefales å benytte Domain Name System Security Extensions (DNSSEC) (RFC 4033, RFC 4034 og RFC 4035 med oppdateringer) for alle domenenavn en virksomhet har registrert, og at det kun benyttes resolvere[1] som validerer DNS-oppslag.»

Difi ønsker også å vurdere denne standarden som en obligatorisk standard på et senere tidspunkt.

Formålet med standarden

Standarden skal bidra til bedre sikkerhet i domenenavnsystemet, og vil redusere risiko for at det oppstår sårbarheter knyttet til bruk av DNS i andre sikkerhetstiltak.

Begrunnelse for anbefalingen

Formålet med anbefalingen er å styrke integriteten i domenenavnsystemet og på den måten redusere risikoen for flere typer angrep mot digitale tjenester. Den tekniske løsningen er moden og andelen norske domenenavn som allerede er sikret med DNSSEC er rundt 58 prosent.

DNSSEC bidrar også til å styrke sikkerheten ved bruk av andre tiltak som DMARC, DKIM, SPF og DANE, ettersom de benytter DNS til lagring av informasjon. DNSSEC bidrar til å sikre integriteten til data fra DNS. For DANE er det en forutsetning at DNSSEC benyttes.

[1] Resolvere er tekniske komponenter som brukes når digitale tjenester utfører oppslag i domenenavnsystemet.

Kostnader

Kostnaden for å bruke DNSSEC vurderes som lav, og etableringskostnader vil i hovedsak være knyttet til virksomheter som har etablert og drifter sin egen DNS-infrastruktur. For andre virksomheter vil standarden medføre at man må velge underleverandører som tilbyr DNSSEC eller som kan dokumentere at de har etablert andre sikkerhetstiltak som beskytter mot de trusler og sårbarheter hvor DNSSEC gir redusert risiko.

Hvilke utfordringer DNSSEC ikke løser

Det er viktig å påpeke at domenenavn også er knyttet til den utfordringen brukere har med å forsikre seg om at et domenenavn faktisk representerer en virksomhet i offentlig sektor. Norge har kun delvis tatt i bruk kategoridomener (f.eks. kommune.no, herad.no, stat.no og dep.no). Noen virksomheter i offentlig sektor bruker flere domenenavn knyttet til forskjellige tjenester. Noen virksomheter i offentlig sektor bruker internasjonale domenenavn i stedet for eller i tillegg til domenenavn i det norske toppdomenet. Det eksisterer heller ingen samlet og fullstendig oversikt over bruken av de forskjellige domenenavnene.

Det er nødvendig å etablere en god domenenavnehygiene i offentlig sektor for å understøtte effekten av andre sikkerhetstiltak, for eksempel bruk av DNSSEC og HTTPS.