Difi
Direktoratet for
forvaltning og ikt

Vedlegg D: Behandling i Standardiseringsrådet, DNSSEC

Innhold:

Difi
Direktoratet for
forvaltning og ikt

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.

Forslag D – DNSSEC – Oppsummering av høringssvar

Det følgende er en oppsummering av vesentlige merknader fra svarene på høringen med kommentarer fra Difi.

Uninett Norid AS har uttalt at «Norid ser på DNSSEC som en viktig sikkerhetskomponent i domenenavnsystemet, som de aller fleste domeneabonnenter kan ta i bruk uten å gjøre større tiltak.» Uninett AS har uttalt at «I punktet om "Kostnader" bør man vurdere å nevne at den teknologiske kompleksiteten øker signifikant i forhold til det å drive en infrastruktur som ikke støtter DNSSEC. Det kan spille inn i avgjørelsen om organisasjonen skal fortsette å drive sin egen publiserende DNS-infrastruktur eller ikke.» Uninett har videre uttalt at «Det bør også understrekes at man med DNSSEC og egen drift av DNS publiserings-infrastruktur må sikre at organisasjonen har gode og veldokumenterte rutiner i forbindelse med rotasjon av nøkler, og tilhørende oppdatering mot moder-domenet. Svikter rutinene på dette feltet er det fare for at virksomheten DNSSEC-messig blir "kjent ugyldig", altså at ingen andre som bruker resolvere som gjør validering av DNSSEC vil kunne slå opp organisasjonens domenenavn.»

Difi er enig i at det stilles større krav til kompetanse for virksomheter som ønsker å etablere og drifte sin egen infrastruktur for DNSSEC. Det er særlig viktig at disse virksomhetene har etablert tiltak som sikrer at ikke domener blir utilgjengelige på grunn av mangelfull administrasjon av nøkler. Difi legger til grunn at det kun er noen få virksomheter i offentlig sektor som kommer drifter sin egen DNS-infrastruktur.

Uninett har uttalt at «Delen av setninga som sier "... 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*" kan leses som om det finnes andre metoder enn å bruke DNSSEC som kan løse de samme problemene som DNSSEC løser. Vi kjenner ingen alternativer til hvordan man f.eks. skal kunne sikre autentisk oppslag av informasjon for DANE på andre måter enn ved å bruke DNSSEC, og anbefaler derfor at den uthevede delen av setninga tas bort.»

Difi legger til grunn at virksomhetene i offentlig sektor vil ha registrert mange domenenavn som ikke vil brukes til å sende eller motta e-post, og som dermed ikke vil ha behov for DANE.

Statistisk sentralbyrå (SSB) har uttalt at «Vi ønsker imidlertidig å bemerke at det tidligere har vært påpekt svakheter ved DNSSEC som har vært utnyttet for å øke omfanget av DDOS-angrep, men vi anser at fordelene er større enn ulempene ved å ta i bruk standarden. Det kan også være en utfordring ved teknologivalg at store DNS-leverandører som Microsoft (Azure) og AWS per i dag ikke fullt ut har implementert støtte for DNSSEC.»

Difi vurderer det som viktig å utforme anbefalingen på en måte som gir rom for å vurdere om en leverandør har etablert andre tiltak som sikrer tilstrekkelig integritet i domenenavnsystemet. I denne sammenheng er det viktig å merke seg at det også eksisterer løsninger som sikrer konfidensialitet i bruk av DNS, for eksempel DNS over TLS og DNS over HTTPS, som vil påvirke vurderingen av risiko for DNS-infrastrukturen generelt.

Passordninja AS har uttalt at «Saksfremlegget nevner at andelen norske domenenavn som er sikret med DNSSEC er rundt 58 prosent. Det nevnes ikke noe om hvor mange klienter som antas sikret gjennom bruk av DNSSEC.»

Difi antar at tallet som etterspørres er hvor stor andel av domenenavnoppslagene som besvares av en resolvere som validerer svarene. Informasjonsmateriell publisert av Norid opplyser at per 30. august 2018 valideres 80 prosent av domeneoppslagene i Norge.

Buypass AS har uttalt at «Bruk av DNSSEC sammen med CAA vil sikre at domeneeiere har god kontroll på hvilke sertifikatutstedere som kan utstede sertifikater på deres domener. Vi foreslår at bruk av CAA tas inn som en del av anbefalingen - enten sett i sammenheng med DNSSEC eller under saksfremlegg 1.»

Difi vurderer det som relevant å vurdere å anbefale RFC 6844 DNS Certification Authority Authorization (DNS CAA) sammen med en anbefaling om bruk av DNSSEC. Det er i så fall et forslag som må gjennom en høringsrunde og behandles av Standardiseringsrådet på et senere tidspunkt. Difi vil allerede nå oppfordre virksomheter til å vurdere å ta denne standarden i bruk og vil be Standardiseringsrådet om en foreløpig tilbakemelding om RFC 6844 bør tas inn som en del av denne standarden som skal bidra til å sikre integriteten i DNS-infrastrukturen.

Oppdatert forslag til anbefaling – Saksframlegg D – DNSSEC

Den følgende utgaven av teksten er oppdatert etter behandling av høringssvar.

«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 som validerer DNS-oppslag»

Det er viktig at denne standarden brukes riktig og vi forutsetter at det blir publisert en norsk veileder før anbefalingen publiseres i referansekatalogen.