Nasjonal kommunikasjons-myndighet

Referanse:	2109259
Dato:	15. november 2021
Saksbehandler:	Lars Edvard Storjord, Frode Sørensen

Prinsippnotat om DNS-baserte sikkerhetstiltak

Dette notatet gir en generell vurdering av sikkerhetsunntaket i nettnøytralitetsforordningens artikkel 3(3)(b), samt spesifikk vurdering av sikkerhetsunntaket for DNS-basert filtrering av internettilknytningen, særlig med tanke på formuleringene «når nødvendig, og bare så lenge som nødvendig» (artikkel 3(3)) basert på en «streng fortolkning» (fortale 11).

Beskrivelse av problemstillingen

Er det tillatt for en ISP (Internet Service Provider) å tilby et «sikkerhetsfilter» til internettjenesten som kan forhindre abonnentene å komme i kontakt med nettsteder som truer sikkerheten, som for eksempel inneholder skadelig programvare, brukes til hacking, identitetstyveri eller liknende?

Prinsipielt sett er sakens kjerne at i dette tilfellet etablerer ISP-en en liste over nettsteder som blokkeres for abonnentene, hvilket i utgangspunktet vil være stikk i strid med NN-reguleringens kjerne, at sluttbrukeren selv skal kunne bestemme bruken av internettilknytningen. Et viktig poeng i denne sammenheng er at ISP-en ikke skal styre abonnentenes bruk av internettilknytningen.

I så måte vil bruk av sikkerhetsprogramvare på sluttbrukerutstyret være en mindre inntrengende metode, siden installasjon og bruk av denne programvaren er fullstendig under sluttbrukerens kontroll. Videre er brukerutstyret utenfor virkeområdet til NN-forordningen.

En annen løsning kan være at ISP-en tilbyr et valgfritt DNS-sikkerhetsfilter (Domain Name System) som i utgangspunktet er deaktivert, og som abonnenten selv kan aktivere for å ta det i bruk (BEREC guidelines para 32b). Et slikt filter kjører på en alternativ DNS resolver som vil være utenfor NN-forordningens virkeområde (BEREC guidelines para 78c).

Det vanskelige spørsmålet er om DNS-sikkerhetsfilteret også kan være i samsvar med forordningen hvis filteret i utgangspunktet er aktivert av ISP-en, men at abonnenten selv kan deaktivere det om ønskelig. En slik filtrering vil være under ISP-ens kontroll, og vil være innenfor NN-forordningens virkeområde fordi funksjonen er forhåndsaktivert, dvs. funksjonen kjører på default DNS resolver (BEREC guidelines para 78a). Med «resolver» menes her oppslagstjener eller oppslagsserver.

NN-forordningen inneholder unntak for blokkeringer som er begrunnet i sikkerhetsformål. Sentralt i vurderingen av hvilke sikkerhetstiltak som er tilstrekkelig godt begrunnet for at unntaket kommer til anvendelse, er kravet om at unntak kun kan gis «når nødvendig, og bare så lenge som nødvendig» (art. 3.3). Videre at denne vurderingen skal legge til grunn en «streng fortolkning» (fortale 11).

Nasjonal kommunikasjons-myndighet

Generell vurdering av sikkerhetsunntaket

Artikkel 3(3)(b) beskriver at sikkerhetsunntakene gjelder «ivaretakelse av integritet og sikkerhet for nettverket, tjenester som tilbys via nettverket og terminalutstyret til sluttbrukeren». Bestemmelsen inkluderer altså også beskyttelse av tjenestene som tilbys til sluttbruker, samt beskyttelse av brukerutstyret til sluttbrukeren.

Videre beskriver punkt 14 i fortalen at eksempler på relevante sikkerhetstrusler er «nettangrep som forårsakes av skadelig programvare eller identitetstyveri av sluttbruker på grunn av spionprogramvare». Fortalen beskriver altså to eksempler som omhandler beskyttelse av henholdsvis brukerutstyr og sluttbrukeren selv.

BERECs NN-retningslinjer nevner også angrep mot sluttbrukerutstyr og tiltak mot skadelig programvare som eksempler på relevante sikkerhetstrusler som unntaket omfatter. Videre beskriver retningslinjene blokkeringslister fra anerkjente sikkerhetsorganisasjoner som kilde til informasjon om aktuelle sikkerhetstrusler.

Til sist understreker BERECs retningslinjer at siden sikkerhetsunntaket kan benyttes som basis for omgåelse av NN-forordningen, så bør regulatørene vurdere nøye om kravene i forordningen er oppfylt og at man i denne vurderingen også innhenter begrunnelse fra ISP-en. I denne sammenheng foreslår BERECs retningslinjer videre å benytte ENISAs spesifikke retningslinjer for sikkerhetstiltak.

Spesifikk vurdering basert på ENISAs retningslinjer

Gitt at blokkering av visse sikkerhetstrusler faller inn under sikkerhetsunntaket, er det videre et sentralt spørsmål hvorvidt anvendelse av ***forhåndsaktivert DNS-sikkerhetsblokkering som metode*** er i henhold til nødvendighetskravet, basert på streng fortolkning.

ENISAs retningslinjer nevner eksplisitt filtrering ved hjelp av DNS som eksempel på sikkerhetstiltak, ved å liste opp «DNS-skjerming» (DNS blackholing) som ikke returnerer IP-adresse ved navneoppslag, og «DNS-viderekobling» (DNS redirection) som returnerer en alternativ (og trygg) adresse ved navneoppslag.

ENISAs retningslinjer anbefaler at disse fire momentene legges til grunn for vurderinger av nødvendighetskravet: ***Sikkerhetsrisiko, effektivitet, proporsjonalitet og egnethet***.

Når det gjelder vurdering av sikkerhetsrisikoen, avhenger dette av de spesifikke sikkerhetstruslene som blokkeres, og dette er nærmere omtalt i neste seksjon. Analysen i denne seksjonen forutsetter at sikkerhetstiltak er rettet mot konkrete sikkerhetstrusler med høy risiko. Typisk eksempler på slike sikkerhetstrusler vil kunne være hacking og skadelig programvare.

Effektivitet

ENISAs retningslinjer beskriver at det kan tas i betraktning i hvor stor grad tiltaket reduserer sikkerhetsrisikoen. DNS-blokkering vil kunne gi relativt god beskyttelse for vanlige internettbrukere, siden mesteparten av internettkommunikasjon gjennomfører DNS-oppslag før kommunikasjonen utføres. Sikkerhetsfilteret vil kunne omgås ved å benytte alternativ DNS-resolver, eller ved å kommunisere direkte mot IP-adresser uten å benytte DNS-oppslag. Slike endringer i kommunikasjonsmønsteret er imidlertid ikke noe som ofte forekommer hos vanlige internettbrukere.

Sammenligner man forhåndsaktivert DNS-filter med valgfritt DNS-filter, samt med sikkerhetsprogramvare installert på brukerens PC, vil forhåndsaktivert DNS-filter ha større effektivitet, siden ikke alle sluttbrukere i praksis vil aktivere valgfritt DNS-filter eller installere sikkerhetsprogramvare på PC-ene sine.

Hvis færre bruker slike sikkerhetstiltak, vil dette også kunne negativt påvirke sikkerheten til de som faktisk bruker sikkerhetstiltakene, siden ubeskyttet brukerutstyr vil utgjøre innfallsport for sikkerhetsangrep og spredning av skadelig programvare.

Effektiviteten ved å bruke DNS-filtrering som sikkerhetstiltak ansees derfor for å være rimelig god for vanlige internettbrukere, forutsatt at de nettstedene som blokkeres av filteret er korrekt identifisert.

Proporsjonalitet

ENISAs retningslinjer forklarer videre at sikkerhetstiltakets omfang kan vurderes, samt begrensningen av eventuelle bivirkninger. Videre beskriver retningslinjene at det er viktig å vurdere hvorvidt tiltaket også kan føre til blokkering av innhold som ikke skal blokkeres (overblokkering). For DNS-filtrering vil det være en risiko for overblokkering, siden listene med blokkerte nettsteder til en viss grad risikerer også å identifisere nettsteder som er «friskmeldt», samt at noen av nettstedene som har innhold som ønskes blokkert av sikkerhetsgrunner, samtidig kan ha innhold som ikke ønskes blokkert.

ENISAs retningslinjer foreslår angående proporsjonalitet også å vurdere om sikkerhetstiltaket er begrenset til spesifikk trafikk, spesifikke nettverk eller spesifikke brukere. Sammenlignet med valgfritt DNS-filter, samt med sikkerhetsprogramvare installert på brukerens PC, vil forhåndsaktivert DNS-filter være mer inngripende i og med at dette vil gjelde for alle abonnentene til tilbyderen.

Proporsjonaliteten ved å bruke DNS-filtrering som sikkerhetstiltak ansees derfor for å være noe begrenset når det innføres forhåndsaktivert for alle abonnenter, samt at det er en viss risiko for overblokkering. Antall abonnenter som i praksis påvirkes kan imidlertid begrenses ved å etablere brukervennlige metoder til å deaktivere filteret, samt informere godt om muligheten til deaktivering. Videre kan tendensen til overblokkering motvirkes ved at tilbyderen etablerer og gjennomfører gode kontrollrutiner for blokkeringslistene, samt at det informeres godt om muligheten for å melde fra hvis feilblokkering forekommer. Korrektheten til blokkeringsfilteret er avgjørende for dette kriteriet.

Egnethet

ENISAs retningslinjer beskriver videre at det kan vurderes hvorvidt tiltaket for eksempel er å betrakte som industristandard, samt om det eventuelt finnes alternative sikkerhetstiltak som er mer effektive eller mer proporsjonale.

DNS-blokkering er allerede vanlig å bruke for å blokkere abonnentenes tilgang til nettsteder som domstolene har pålagt ISP-ene å blokkere (i henhold til artikkel 3(3)(a)). Filtrering av nettsteder implementert ved hjelp av DNS-blokkering vil dermed kunne sies å være industristandard.

Når det gjelder alternative sikkerhetstiltak, som diskutert over, vil valgfritt DNS-filter og sikkerhetsprogramvare installert på brukerens PC på den ene side være mindre effektivt, men på den andre side være et mer proporsjonalt tiltak.

Oppsummering

Oppsummert vil forhåndsaktivert DNS-filter kunne ha rimelig god effektivitet som sikkerhetstiltak for vanlige internettbrukere. Samtidig vil proporsjonaliteten være noe begrenset fordi tiltaket berører alle abonnenter, samt at det er en viss risiko for overblokkering. Når det gjelder egnethet, kan DNS-filtrering ansees som industristandard, samtidig som det finnes alternative metoder, men at alternativene vil ha mindre effekt, selv om metodene vil være mer proporsjonale. (Angående vurdering av sikkerhetsrisiko, se neste seksjon.)

Konklusjonen for sammenligningen mellom forhåndsaktivert DNS-filter, valgfritt DNS-filter og sikkerhetsprogramvare installert på brukerens PC, er at de to siste ubetinget vil kunne tas i bruk uten å stride mot NN-forordningen. Forhåndsaktivert DNS-filter vil imidlertid også kunne tas i bruk i enkelte tilfeller, under forutsetning av at tilbyderen iverksetter gode prosedyrer for håndtering av korrektheten

til filteret, samt utviser høy grad av transparens angående filteret. Disse forholdene er utdypet i neste seksjon.

Nkoms veiledning til norske ISP-er

Nkoms standpunkt samsvarer med BERECs retningslinjer (se punkt 32b) som klargjør at ved vurdering av begrensninger som implementeres av en ISP i forbindelse med endepunkt-baserte tjenester (som for eksempel valgfritt DNS-filter og sikkerhetsprogramvare installert på brukerens PC), kan regulatøren ta i betraktning hvorvidt sluttbruker har full kontroll over internettjenesten og har anledning til å aktivere og deaktivere tjenesten, og hvorvidt forhåndsinnstillingen til ISP-en er i full overensstemmelse med reglene for åpen internettilgang.

Videre har Nkom, basert på en «streng fortolkning (jf. fortale 11), vurdert forhåndsaktivert DNS-basert filtrering av internettilknytningen i lys av sikkerhetsunntaket (artikkel 3(3)(b)), særlig med tanke på formuleringene «når nødvendig, og bare så lenge som nødvendig».

Konklusjonen er at dette unntaket ***vil kunne få anvendelse under visse betingelser***.

Om vurdering av sikkerhetsrisiko for ulike sikkerhetstrusler

Vanlige sluttbrukere av internettilknytningstjenester vil stort sett være teknisk ukyndige med begrenset kunnskap om hvordan tilknytningen best kan beskyttes mot sikkerhetstrusler. Samtidig ser vi at sluttbrukerne i dag utsettes for en rekke sikkerhetstrusler, noe som både truer brukerne selv, men som også utgjør et ***betydelig samfunnsproblem*** som det er vanskelig å få bukt med. I og med at samfunnet blir stadig mer avhengig av internett som ekomtjeneste, er behovet for å ivareta god sikkerhet for internettjenesten stort.

Når det gjelder hvilke ***typer sikkerhetstrusler*** som kan ansees for å ha tilstrekkelig høy risiko (jf. kriteriene i ENISAs retningslinjer), mener Nkom at følgende ***generiske trusler*** kan være aktuelle eksempler på konkrete sikkerhetstrusler som kan vurderes å inkludere i DNS-filteret:

- virus, nettormer og annen skadelig programvare (malware)
- hacking, botnet og tjenestenektangrep (Denial of Service)
- nettsteder med phishing-aktivitet
- identitetstyveri og annen nettsvindel

Når det gjelder nødvendighetskravet, «når nødvendig, og bare så lenge som nødvendig», er det en forutsetning at ISP-en sikrer at ***den enkelte, konkrete sikkerhetsblokkering*** faktisk utgjør en reell trussel og at den fjernes fra listen når den ikke utgjør en trussel lenger. Nkom henviser ISP-ene til ENISAs retningslinjer for beskrivelse av kriterier for hvordan gjennomføre vurdering av den enkelte, konkrete sikkerhetsblokkering. Nkom vil kontrollere etterlevelse og etter behov anmode ISP-en om å redegjøre nærmere for hvordan nødvendighetskravet håndheves i praksis.

Nærmere veiledning om forhåndsaktivert DNS-basert sikkerhetsfilter

For å tilby forhåndsaktivert DNS-basert sikkerhetsfilter mener Nkom det er en forutsetning at ISP-en:

- Sikrer at de ulike sikkerhetsblokkeringene som inngår i blokkeringslisten utgjør en reell trussel i henhold til kravene i NN-forordningen, og sørger for at listen til enhver tid er oppdatert. Nkom kan også be om innsyn i hvilke konkrete vurderinger ISP-en har gjort for sine spesifikke sikkerhetsblokkeringer i henhold til NN-forordningens artikkel 5(2).
- Informerer godt om sikkerhetstiltaket og hvilke sikkerhetstrusler det beskytter mot, samt informerer om hvordan tilbyderen sikrer at disse samsvarer med nettnøytralitetsregelverket.

- Informerer godt om muligheten for å melde fra om overblokkering, og tilrettelegger brukervennlige metoder for å formidle slike meldinger.
- Informerer abonnentene godt om muligheten for å kunne deaktivere filtreringen, samt etablerer brukervennlige metoder for å deaktivere filtreringen.
- Ved hvert konkrete tilfelle hvor blokkering forekommer, gir sluttbruker lett forståelig informasjon om hvorfor blokkeringen fant sted, samt informerer om hvordan filteret eventuelt kan deaktiveres av sluttbrukeren.
- Informerer om sikkerhetsfiltreringen sammen med øvrig informasjon om nettnøytralitet på en dedikert nettside. Nkom mener at dette vil bidra til å øke synligheten og tilgjengeligheten til informasjonen om sikkerhetsfilteret, hvilket er en forutsetning for at abonnentene og andre internettbrukere i praksis vil være informert.

Nkom vil innhente informasjon fra norske ISP-er om deres sikkerhetstiltak, blant annet i forbindelse med utarbeiding av den årlige nettnøytralitetsrapporten.