Kultur- og likestillingsdepartementet
Via departementets høringsportal

25. mai 2023

Felles høringssvar - Tilleggshøring om DNS-blokkering av nettsted som tilbyr pengespill som ikke har tillatelse i Norge

Elektronisk Forpost Norge (EFN)
Internet Society – Norway Chapter (ISOC-NO)
Norwegian Unix User Group (NUUG)

Høringsuttalelse

Innhold

Høringsuttalelse....2
Innledning....2
Diskusjon....3
DNS-blokkering er i realiteten forfalskning....3
DNS-blokkering undergraver sikkerheten på nettet....3
En dum smartbombe for internett....4
Konklusjon....4
Vedlegg....5

Innledning

EFN er en digital rettighetsorganisasjon. Vi jobber for at menneskerettigheter skal ivaretas i det digitale samfunn. EFN består av ulønnede medlemmer med hovedsakelig teknologi, jus og biblioteks-bakgrunn, men vi har medlemmer fra et vidt spekter av yrkesgrupper. Politisk spenner vi over alle partier representert på stortinget. Internasjonalt er EFN en del av European Digital Rights (EDRi) og deltar aktivt i prosesser innenfor bl.a. EU, Europarådet og FN.

Norwegian Unix User Group (NUUG) ble dannet i juni 1984, og har som formål å stimulere til økt interesse og bruk av Unix-lignende systemer. Herunder fri programvare. For å skape gode vilkår for innhenting, bearbeiding og utveksling av informasjon og erfaring mellom brukere. NUUG samarbeider med brukergrupper tilknyttet de forskjellige utviklere, leverandører og brukere av forskjellige systemer inkludert lokale Unix- og Linux-grupper over hele landet og hele verden.

Internet Society er en internasjonal forening for fremme bruken av og tilliten til internett over hele verden. ISOC ble stiftet i 1992 av Vint Cerf og Bob Kahn[1], og blir ansett internasjonalt som en av de viktigste interessorganisasjonene for Internett, i samme kategori som ICANN og IANA. Den norske avdelingen av ISOC jobber for det samme formålet[2] i norsk kontekst.

Alle 3 organisasjoner leverte høringssvar i forrige runde. Vi kan ikke se at noen av våre bemerkninger har blitt hensyntatt. Vi vil derfor fremheve noen av de mer prinsipielle sidene i dette høringssvaret, samtidig som vi vedlegger de opprinnelige høringssvarene som fremdeles står seg.

1 *https://www.internetsociety.org/history/*
2 *https://www.internetsociety.org/mission*

Diskusjon

DNS-blokkering er i realiteten forfalskning

Helt grunnleggende er DNS-systemet et kartotek over IP-adresser, eller koordinater om man vil. Dette kan sammenliknes med gateadresser, hvor hvert enkelt hus står oppført med en egen kartkoordinat. Hvert koordinat får deg til nøyaktig ett hus. Forslaget legger opp til at om man i fremtiden i klikker deg inn på en spillside, så møter du istedet en blokkeringsside.

Forslaget betyr i korthet at man vil bli alle norske nettleverandører om å lyve. For å illustrere det, kan vi se for oss kampen mot overvekt og fast food. Selv om vi alle vil støtte redusert fettinntak i samfunnet, ville man aldri vurdert å forby skilting av gateadresser og samtidig endre oppslagsverk slik at en rekke gateadresser flyttes et annet sted. Det regjeringen gjør nå, er praktisk talt det samme som å omdirigere gateadressene for hver McDonald's og Burger King, slik at adressene nå i stedet fører til Helsedirektoratet. Det høres vanvittig ut fordi det nettopp er det. Er det ikke riktig å gjøre dette offline, er det heller ikke riktig å gjøre det online.

For å gjøre det helt klart, DNS-blokkering innebærer ikke bare et forbud mot å fortelle den kanoniske sannheten, det innebærer et påbud om å forfalske informasjon. Dette er åpenbart en innskrenkning av ytringsfriheten å bli pålagt å gi falsk informasjon. Det er etablert at ytringsfriheten kan innskrenkes når tungtveiende grunner tilsier det. Det foreslåtte systemet er imidlertid såpass hullete, at det er vi synes det er vanskelig å se for seg at det vil holde opp for en forholdsmessighetsvurdering.

DNS-blokkering undergraver sikkerheten på nettet

Når man ikke lenger kan stole på at adressene man får oppgitt er de riktige, vil man begynne å søke alternativer. En ting vi kan forutse, er at spillindustrien vil kjøre en massiv kampanje for å få folk til å benytte andre nettløsninger enn de som lyver til dem. Dette har en rekke sikkerhetsmessige utfordringer, men kanskje tydeligst vil flere og flere benytte utenlandske tjenere.

VPN-bruk i Norge er lav, men økende, opp fra 5,59% i 2020 til 8,08% i 2022.[3] Et fellestrekk ved mange av de landene som har høy VPN-bruk er at det er land som av ulike grunner oppfatter trusselen av overvåkning som sterk. Forbes-undersøkte hvorfor folk bruker VPN i 2023[4], der svarer så mange som 26% at deres primære ønske er å kunne få tilgang til regionlåst innhold. Nettspill vil i denne sammenheng være nettopp regionlåst innhold. Det er derfor sterk grunn til å tro at en blokkering ikke vil ha den ønskede effekten, men vil drive langt flere til å benytte seg av ulike omgåelsesmekanismer, herunder VPN.

Enda mer problematisk normaliserer dette forfalskning. Når man forfalsker DNS-oppslag, vil man nødvendigvis måtte bruke et falskt sertifikat på informasjonssiden. Dette er en direkte undergraving av sikkerheten på nettet. Mesteparten av alle norske internettjenester kjører nå over krypterte linjer, med sertifikater som sier at de er den de utgir seg for. Vi har i en årrekke ønsket å få folk flest til å skjønne at man ikke skal trykke OK når det kommer opp sikkerhetsadvarsler. Norske myndigheter nyter en stor grad av tillitt, når det er myndighetene selv som oppfordrer til å omgå sikkerhetsadvarsler, vil dette være svært ødeleggende for sikkerheten og bidra til å utsette den norske befolkningen for en rekke internettbaserte trusler.

3 *https://atlasvpn.com/vpn-adoption-index*
4 *https://www.forbes.com/advisor/business/vpn-statistics/*

For å gjenbruke analogien over. Når man nå går inn for at man skal la opplysningssentre tilkjennegi seg som burgerkjeder frem til man er innenfor døren, så vil folk ikke lenger ha tiltro til skiltingen.

DNS-blokkering ville vært et tiltak med liten effekt på sikkerheten i 2010, da mesteparten av nettet kjørte på ukrypterte linjer, i 2023 har mesteparten av internett gått over på https og konsekvensene av DNS-blokkering er helt andre. Vi kan ikke se at departementet vurderer konsekvensene av å måtte implementere falske sertifikater i det hele tatt.

En dum smartbombe for internett

Blokkeringsdebatten er en debatt som har kommet opp med jevne mellomrom på nasjonalt nivå, men også på EU-nivå. Det er en grunn til at man ikke har gått inn for blokkering. Det virker ikke, særlig fordi den løsningen man har valgt lekker som en sil. Blokkering er et symboltiltak som feier ting under teppet, fordi man ikke er villig til å gjøre jobben med å faktisk forby det man er imot. Slik det er i dag, så eksisterer pengespill i en merkelig limbosituasjon. Det er ikke ulovlig ihht. EØS-avtalen, men selskaper får ikke etablere seg i Norge. Vi innser at det nok ser ut som et uoverstigelig hinder å få EU til å forby gambling, men det er den jobben man må gjøre.

Konklusjon

Det er alltid noe på internett man gjerne vil forby, i 2010 hadde EFN som en del av EDRi en kampanje vi kalte Don't block them, stop them[5] Det har ikke skjedd noe nytt, DNS-blokkering et like tåpelig tiltak[6]. Forskjellen er at DNS-blokkering i dag også har et element av svekking av sikkerheten som ikke var tilstede tidligere, da bruken av https imotstening til http ikke var i nærheten av så utbredt som den er idag.

Det foreslåtte tiltaket vil derfor bidra til å svekke sikkerheten på nettet, samtidig som effekten av blokkeringen er svært tvilsom.

Vi henstiller derfor til å slutte med symboltiltak og ikke aktivt gå inn for å svekke vår sikkerhet.

5*https://edri.org/files/ecta_speech_101130.pdf*

6*I alle fall en utgave av det britiske blokkeringsregimet viste seg å blokkere for nettsteder for menneskerettsorganisasjoner, Unix-brukergrupper og til og med et forlag for teknisk litteratur, slik det er beskrevet i denne bloggposten av Peter Hansteen: The UK "Porn" Filter Blocks Kids' Access To Tech, Civil Liberties Websites - https://bsdly.blogspot.com/2013/12/the-uk-porn-filter-blocks-kids-access.html*

Vedlegg

Vedlegg 1: Høringssvar EFN og NUUG

Elektronisk Forpost Norge
Medlem av EDRi, European Digital Rights

Norwegian Unix User Group

Kulturdepartementet
Via departementets høringsportal

1. november 2021

Høringssvar - bestemmelse om DNS-blokkering av nettsider som tilbyr pengespill som ikke har tillatelse i Norge

Med vennlig hilsen

Tom Fredrik Blenning
Daglig leder - EFN

Joar Rasmussen
Leder høringsutvalg

Knut Yrvin
Styremedlem - NUUG

Innhold

Innledning 2

Sensur 2

Et internett for deg, et internett for meg 3

Sensur som virkemiddel 3

Effektene av DNS-blokkering 4

DNS-over-HTTPS (DoH) 4

Apper 4

VPN 5

Negativ påvirkning på den generelle sikkerheten på internett. 5

Sensurmekanismer 5

Konklusjon 5

Innledning

EFN er en digital rettighetsorganisasjon. Vi jobber for at menneskerettigheter skal ivaretas i det digitale samfunn. EFN består av ulønnede medlemmer med hovedsakelig teknologi, jus og biblioteks-bakgrunn, men vi har medlemmer fra et vidt spekter av yrkesgrupper. Politisk spenner vi over alle partier representert på stortinget. Internasjonalt er EFN en del av European Digital Rights (EDRi) og deltar aktivt i prosesser innenfor bl.a. EU, Europarådet og FN.

Norwegian Unix User Group (NUUG) ble dannet i juni 1984, og har som formål å stimulere til økt interesse og bruk av Unix-lignende systemer. Herunder fri programvare. For å skape gode vilkår for innhenting, bearbeiding og utveksling av informasjon og erfaring mellom brukere. NUUG samarbeider med brukergrupper tilknyttet de forskjellige utviklere, leverandører og brukere av forskjellige systemer inkludert lokale Unix- og Linux-grupper over hele landet og hele verden.

I den foreliggende saken er det satt ned et høringsutvalg bestående av Tom Fredrik Blenning og Joar R. Rasmussen.

Sensur

DNS er på mange måter en moderne telefonkatalog. En lov som pålegger blokkering er derfor analogt med å sensurere visse mennesker fra telefonkatalogen. DNS-blokkering har vært brukt før, men da som ulovfestet tiltak. Dette er første gangen det nedfelles i lovs form.[1] Det har derfor

[1] Åndsverkslovens § 88 omtaler hindring eller vanskeliggjøring av tilgang til nettsteder, men det er ikke omtalt noen konkret metodebruk.

ikke tidligere blitt utsatt for lovlighetskontroll.

Blokkering har blitt tatt i bruk i større grad i andre land. Erfaringer hentet fra Storbritannia tilsier at det er fare for både over- og under-blokkering. Open Rights Group dokumenterer overfor det engelske parlamentet at mellom 30% og 80% av alle URLer var underblokkerte, mens mellom 2% og 6% av URLene var overblokkerte.[2] Nettfilteret som benyttes i Storbritannia er av en helt annen karakter enn det som er foreslått i Norge, men vurderingene av blokkering vil være av samme karakter.

Ytringsfriheten er beskyttet gjennom grunnloven og EMK. I den norske Grunnloven gjelder et særlig vern mot forhåndssensur som går utover de forpliktelser vi har etter EMK. Overblokkering er derfor særlig problematisk i Norge. Et nettsted kan ha flere former og det er ikke sikkert at alle deler av nettstedet inneholder ulovlig informasjon, en blokkering må derfor være en vekting av de lovlige opp mot de ulovlige delene av nettstedet.

Som det påpekes i høringsnotatets kapittel 5.4, tilsier hensynet til rettsikkerheten at “domstolene vil være best til å avgjøre slike saker.” - denne vurderingen stiller vi oss bak. Vi anerkjenner at Lotteritilsynet har nødvendig kompetanse til å vurdere et spilltilbuds lovlighet, men vi mener at tilsynet må bringe blokkering inn for domstolskontroll for å bøte på potensialet for krenking av grunnleggende rettigheter ved eventuelle saksbehandlingsfeil. Hensynet til effektiv saksbehandling bør ikke tillegges vesentlig vekt.

Videre kan vi lese om “Oppheving av pålegg” at det er tilstrekkelig at tilbyder alene skal kunne begjære oppheving av pålegg. Dette er vi uenige i. En nettside som på et tidspunkt inneholder ulovlig informasjon kan på et senere tidspunkt være endret, dette innebærer at en evt. blokkeringsliste må som et minimum være gjenstand for kontinuerlig revisjon av sensurmyndighet, for ikke å komme på kant med Grunnlovens forbud mot forhåndssensur.

Et internett for deg, et internett for meg

En konsekvens av å innføre DNS-blokkering er at internett blir utsatt for en splitt. Det innebærer at nettet ser annerledes ut avhengig av hvilket land du ser det fra. Internett har på både godt og vondt gjort verden mindre og det er med en viss ærefrykt vi kan se at man i prinsippet kan se de samme tingene uavhengig av om man sitter i Gambia eller i Norge. Dette er en viktig verdi vi bør ta vare på.

Sensur som virkemiddel

EFN har tidligere argumentert for at kriminalitet skal straffes og ikke skjules.[3] I forbindelse med et EU-forslag i 2010 om innføring av DNS-blokkering for bekjempelse av utnyttelse av barn argumenterte vi i samarbeid med flere organisasjoner som arbeider for barns rettigheter for at dette viktige prinsippet.

---

[2] https://publications.parliament.uk/pa/cm201617/cmpublic/digitaleconomy/memo/DEB63.pdf
[3] Internet Blocking: Crimes Should Be Punished and Not Hidden

Til forskjell fra utnyttelse av barn er ikke pengespill anerkjent som ulovlig i hele verden, og det er heller ikke ulovlig for norske borgere som oppholder seg i Norge. Det er derfor mer problematisk å få anerkjennelse for å stenge ned problemet ved roten. Likevel er ikke sensur er et godt virkemiddel. Det er andre tiltak som kan settes inn. Et mulig eksempel er innføring av 100% skatt på gevinst fra utenlandske pengespill. Dette er et tiltak som ikke har har konsekvenser i forhold til ytringsfriheten.

Departementet skriver i høringsnotatet 5.3:

> *DNS-blokkering av nettsider begrenser en næringsdrivendes mulighet til å ytre seg på internett, og utgjør dermed et inngrep i den næringsdrivendes ytringsfrihet. Samtidig innebærer blokkeringen en begrensning av informasjonsfriheten til publikum, fordi tilgangen til innholdet blir vanskeliggjort.*

Dette er vi selvsagt enige i, men der den næringsdrivendes ytringsmulighet problematiseres, blir det ikke gjort tilsvarende forsøk på å problematisere publikums tilgang til informasjon.

En opplyst samfunnsdebatt bygger på premisset om muligheten til å sette seg inn i problemstillinger. Selv om det per dags dato er forbudt med utenlandske pengespill, kan det tenkes at man i fremtiden vil kunne gå bort fra dette forbudet. Sensur av nettsidene innebærer at man vanskeliggjør en saklig diskusjon av hvordan dette gjøres. Å lese og vurdere innholdet av nettsidene er ikke det problematiske, det er kun når tilbyder faktisk leverer pengespill at handlingen blir problematisk med henblikk på norsk lov.

Effektene av DNS-blokkering

En norsk DNS-blokkering vil ha liten effekt i praksis, selv for helt vanlige internettbrukere, av flere grunner:

DNS-over-HTTPS (DoH)

DoH er en ny standard for sikker håndtering av DNS-forespørsler. Store markedsaktører som Apple, Mozilla, Microsoft og Google støtter allerede denne i sine viktigste produkter - som Chrome, Firefox, Windows, Android og iPhone. Foreløpig er ofte funksjonaliteten slått av som standard slik at bruker selv må skru den på, men dette er i ferd med å endre seg til å bli en standardinnstilling.

DoH innebærer at DNS-forespørsler sendes kryptert, oftest til utenlandske servere. Dette i motsetning til standard DNS, der forespørslene som regel sendes til den lokale internettleverandøren ukryptert. DNS-over-https serverne i utlandet vil ikke sperre nettsider på vegne av norske myndigheter, og blokkeringen vil være uten effekt når disse er i bruk.

Ovenstående innebærer etter EFNs mening dermed at departementets i beskrivelse i

høringsnotatet av kompleksiteten av omgåelse - “brukeren må da enten laste ned og anvende en egen programvare for å omgå blokkeringen, eller manuelt overstyre hvilken DNS-server som skal brukes” ikke lenger er korrekt.

Apper

Apper i forskjellige varianter, på mobiler, nettbrett og tradisjonelle datamaskiner, overtar stadig mer av internett-trafikken. En relevant forskjell mellom apper og en nettside, er at en app ikke trenger å være avhengig av en spesifikk nettadresse. Om en sluttbruker for eksempel laster ned en app ved navn "Gambling" på sin enhet, vil den kunne fungere uavhengig av om domenene "gambling.no" eller "gambling.com" er tilgjengelige for brukeren. Hvilke nettadresser en slik app vil være avhengige av, er også trivielt for apputvikler å endre på, slik at blokkeringer enkelt kan omgås ved å oppdatere dette i en ny versjon av appen.

VPN

VPN er en teknologi som blir stadig mer populær, også hos vanlige internettbrukere. Er man pålogget et VPN, vil både DNS-forespørsler og selve internett-trafikken kryptert passere både norske internettleverandører og myndigheter, og blokkeringen vil dermed ikke ha effekt.

Samlet sett gjør disse tekniske utfordringene at norsk DNS-blokkering vil ha liten virkning, særlig om noe tid. Omgåelse for de som i utgangspunktet er motivert vil være svært enkelt, og med stadig økt utbredelse av teknologi som DoH vil brukeromgåelse etterhvert ikke være nødvendig og blokkering vil slutte å fungere uten at noen bevisst handling er påkrevd.

Negativ påvirkning på den generelle sikkerheten på internett.

Å øke sikkerheten i internett-infrastrukturen er en vesentlig samfunnsinteresse som både private og statlige aktører for tiden investerer tungt i. Blant annet jobbes det med å etablere systemer for å verifisere ektheten til DNS-responser - kjent som DNSSEC. Blokkering av nettsider i DNS slik som beskrevet i høringsnotatet kapittel 5.4, vil innebære å forfalske visse DNS-responser. Dette kan bidra til å undergrave slike sikkerhetsmekanismer, og dermed gjøre fremtidens internett mindre sikkert for alle. I de tilfellene der DNSSEC er tatt i bruk, vil videresending til blokkeringsside som foreslått i høringsnotatet i avsnittet “Påleggets utforming” ikke være teknisk mulig.

Sensurmekanismer

EFN er prinsipielt imot at sensur ved hjelp av blokkering av nettsider finner sted. Skulle lovgiver likevel konkludere med dette, er det noen viktige prinsipper som bør følges.

Sensuren må:

- … være transparent. Dette betyr at det tydelig signaliseres at sensur har funnet sted, når et budskap (i dette tilfellet en DNS-respons) mottas. Sensurerende instans må også publiser en til enhver tid oppdatert oversikt over hva som er sensurert under hvilken lovhjemmel. Dette vil bidra til at sensurmekanismer ikke enkelt kan misbrukes av tredjepart.
- … kun foregå ved hjelp av etablerte internettstandarder.
- … treffe geografisk presist: Kun mekanismer som medfører at sensuren kun er aktiv innenfor Norges grenser må benyttes. DNS-blokkering som foreslått kan resultere i at norske borgeres enheter vil oppleves som underlagt sensur også om enheten taes med ut av landet, ettersom DNS-respons mellomlagres (“caches”) i enhetene.

Konklusjon

Forslaget griper dypt inn i viktige rettigheter, og forstyrrer grunnleggende mekanismer for hvordan internett fungerer. Samtidig vil forslaget i praksis ha liten effekt. Hensikten med å forby pengespill er uttalt å være å beskytte de spilleavhengige. Dette er antageligvis den gruppen som har sterkest motivasjon for å omgå et forbud. Med tanke på hvor lite som skal til for omgåelse, kan vi ikke si oss enige i at den foreslåtte blokkeringen er proporsjonal med inngrepet i ytrings-, og informasjonsfriheten.

Vi må derfor konkludere med at forslaget bør forkastes.

Vedlegg 2: Høringssvar ISOC Norge

ISOC Norge, ved Salve J. Nilsen (styreleder)

Kulturdepartementet
Via departementets høringsportal

1. november 2021

Høringssvar - bestemmelse om DNS-blokkering av nettsider som tilbyr pengespill som ikke har tillatelse i Norge

Om Internet Society, Norway Chapter

Internet Society er en internasjonal forening for fremme bruken av og tilliten til internett over hele verden. ISOC ble stiftet i 1992 av Vint Cerf og Bob Kahn[1], og blir ansett internasjonalt som en av de viktigste interessorganisasjonene for Internett, i samme kategori som ICANN og IANA. Den norske avdelingen av ISOC jobber for det samme formålet[2] i Norsk kontekst.

Høringssvar

ISOC Norge stiller seg bak høringsuttalelsen fra Elektronisk Forpost Norge (EFN) og Norwegian Unix User Group (NUUG).

Vi vil gjerne utdype problemstillingen med undergraving av sikkerhetsmekanismen DNSSEC som vil følger av en implementering av DNS-varsling eller blokkering. En av ISOC sine hovedbekymringer med fremtidig utvikling og nyttegjøring av internett, er at det er blitt vanskeligere å ha tillit til nettet som informasjonskilde. Et av grepene som IETF[3] har gjort for å øke denne, er ved å muliggjøre kryptografisk signering av DNS-oppslag, så sluttbrukere kan få en forsikring om at nettsiden de ønsker å benytte seg av faktisk er den som er forventet, og ikke noe annet. DNSSEC hjelper da sluttbrukeren å kunne avgjøre om DNS-tjenesten er til å stole på, så lenge den leverer fra seg korrekt signerte responser.

Vår bekymring er at DNS-blokkering eller varsling vil medføre at ordinært tillitsverdige DNS-tjenere vil ikke lenger bli brukt. Dette er fordi vi forventer 100% korrekt signerte svar –

---

[1] https://www.internetsociety.org/history/
[2] https://www.internetsociety.org/mission/
[3] Internet Engineering Taskforce er en åpen standardorganisasjon som utvikler og promoterer internettstandarder.

noe som gjøre det svært vanskelig å skille mellom en forfalsket og en “legitimt blokkert” DNS-respons.

Den enkleste måten for sluttbrukere å håndtere situasjonen der DNS-tjeneren ikke lenger er tillitsverdig, er ved å bytte til et kjent alternativ (f.eks. Google sin 8.8.8.8 DNS-tjener, eller Cloudflare sin 1.1.1.1 DNS-tjener[4]).

Videre åpner blokkeringsstrategien for et slags “katt og mus” spill med aktører som ønsker å omgå blokkeringen. Vi stiller spørsmål om å spille et slikt spill er en god bruk av ressurser.

Salve Nilsen

_____

Leder - ISOC NO

[4] 1.1.1.1 og 8.8.8.8 er IPv4-adresser. Disse adressene er de “rå” telefonnumrene til en server.