Netneutralitetsforordningen og mulighed for DNS-blokering

v. Center for Cybersikkerhed og SDFI

CENTER FOR CYBERSIKKERHED

Styrelsen for Dataforsyning og Infrastruktur

Netneutralitetsforordningens genstand og anvendelsesområde

v/ SDFI

Art. 1(1) og BEREC guidelines

- Sikre lige og ikkediskriminerende behandling af trafikken ved levering af internetadgangstjenester og slutbrugeres hertil hørende rettigheder.

- Både indholdsleverandører og forbrugere/slutbrugere er beskyttelsessubjekter.

Hovedregel og undtagelser

v/ SDFI

Hovedregel: Udbydere af internetadgangstjenester skal behandle al trafik lige, jf. art. 3(3) 1. afsnit.

Undtagelse: Rimelige trafikforanstaltninger er tilladt, jf. art. 3(3) 2. afsnit.

Trafikforanstaltningerne skal opfylde en række krav, og må navnlig *ikke blokere*, bremse, ændre, begrænse eller lign. for bestemt indhold eller bestemte applikationer eller tjenester eller bestemte kategorier heraf.

Modif.: Trafikforanstaltninger, eksempelvis blokering, er dog tilladt, *i nødvendigt omfang* og *kun så længe*, det er nødvendigt for at:

a) overholde EU-retsakter, national lovgivning eller "foranstaltninger", herunder kendelser og afgørelser fra myndigheder med relevante beføjelser",
b) opretholde integriteten og sikkerheden i nettet, af de tjenester, der udbydes via det pågældende net, og af slutbrugernes terminaludstyr, eller
c) forebygge truende overbelastning af nettet og afbøde virkningerne af ekstraordinære eller midlertidige overbelastninger af nettet … ." → ej relevant her

NN-reglernes muligheder for DNS-blokering

v/ SDFI

- Undtagelserne er underlagt **streng fortolkning og proportionalitet**
- DNS-blokering som opt-in-løsning [jf. BEREC guide lines]
- Blokering ifølge EU-regler, national lovgivning eller retskendelse, jf. art. 3(3)(a)
- Mulighed for DNS-blokering, jf. art. 3(3)(b), der kan beskytte net, tjenester og udstyr
  - Der skal være tale om konkrete trusler mod integriteten og sikkerheden
  - Nødvendighed, jf. art. 3(3)(b) → en foranstaltning skal være nødvendig, for at integriteten og sikkerheden opretholdes
  - Og kun så længe det er nødvendigt

SDFI's opmærksomhedspunkter

v/SDFI

- "Opt-out" DNS-blokering kan være i overensstemmelse med forordningen.
- SDFI kan ikke forhåndsgodkende den enkelte "opt-out"-løsning. Det afgørende er, hvordan den konkrete løsning fungerer i praksis.
- F.eks.:
  1. Spærres der for hjemmesider, der ikke udgør trussel mod integritet og sikkerhed?
  2. Hvordan sikres, at blokeringen ophæves, når hjemmesiden ikke længere udgør en konkret trussel?
  3. Er kunderne tilstrækkeligt orienterede om muligheden for at opt'e ud?
  4. Lever en "opt-out"-ordning op til kravet om, at tiltaget skal være nødvendigt, for at opretholde integriteten og sikkerheden?
     - Det vil CfCS komme nærmere ind på.

Er DNS-blokering nødvendig?

v/Center for Cybersikkerhed

- CFCS vurderer, at konkrete cybersikkerhedsmæssige hensyn er aktualiseret, hvilket medfører, at vidtgående trafikstyringsforanstaltninger, som fx blokering, kan finde sted ved konkrete trusler.
- CFCS klare vurdering, at en DNS-blokeringsordning er nødvendig, særligt set i lyset af den aktuelle cybersikkerhedssituation, hvor særligt cybertruslen fra cyberspionage og cyberkriminalitet vurderes at være meget høj (se CFCS' trusselsvurdering af 15. marts 2022).

Opt-in vs. opt-out?

v/ Center for Cybersikkerhed

- Effekten af en ”opt-in”-løsning, hvor der på forhånd er indhentet informeret samtykke hos internetbrugeren og ordningen således tilvælges, vil være meget begrænset, idet alene få brugere må forventes aktivt at tilvælge løsningen
- Dette baseres bl.a. på undersøgelser, der har vist, at en stor del af danske slutbrugere, SMV’er mv. ikke benytter helt grundlæggende sikkerhedstiltag, herunder ikke aktivt tilvælger sikkerhedsforanstaltninger som fx blokeringsmuligheder, der kan beskytte mod skadelige aktiviteter, på trods af løbende kampagner med opfordring hertil fra bl.a. Erhvervsstyrelsen, Digitaliseringsstyrelsen og Forbrugerrådet Tænk (Erhvervsstyrelsen, Digital Sikkerhed i Danske SMV’er 2021, september 2021)
- I øvrigt gør den høje frekvens, hvorved slutbrugere skifter internet- og mobiludbyder, det uhensigtsmæssigt at forlade sig på, at den enkelte bruger kontinuerligt tilvælger ordningen.
- CFCS’ vurdering, at en ”opt-in”-løsning ikke er egnet til at opnå en tilstrækkelig styrkelse af den brede cybersikkerhed.

Opt-in vs. opt-out?

v/ Center for Cybersikkerhed

- En ordning, hvor teleudbyderne som en del af deres abonnementsordning integrerer og automatiserer DNS-blokering, dvs. en ”opt-out”-løsning, vil være den mest effektive løsningsmodel.
- En ”opt-out”-løsning vil have en meget væsentlig positiv betydning for den samlede cybersikkerhed i Danmark, da den i vidt omfang understøtter, at kunden er beskyttet mod cybertrusler, herunder ondsindet aktivitet begået af ondsindede aktører, allerede inden kunden modtager sit internet.
- En ”opt-out”-løsning er nødvendig til at varetage formålet med at beskytte slutbrugerne mod skadelig aktivitet, særligt set i lyset af den aktuelle cybersikkerhedssituation, hvor cybertruslen fra særligt cyberkriminalitet og cyberspionage vurderes at være meget høj.

CFCS's bidrag ved DNS-blokering

- FE er bl.a. national it-sikkerhedsmyndighed, jf. FE-lovens § 1, stk. 3, og CFCS, der er en del af FE, har til opgave at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner er afhængige af, jf. CFCS-lovens § 1.
- CFCS er indstillet på, som Danmarks it-sikkerhedsmyndighed, at rådgive internetudbydere om de krav, der bør stilles til en udbyder af abonnementsordninger og -tjenester for blokeringer med henblik på at sikre, at blokeringerne lever op til formålet.
- CFCS kan endvidere bidrage med konkrete forslag til blokeringer, når CFCS ved varetagelsen af sine opgaver i medfør af CFCS-lovens § 1, vurderer, at det er nødvendigt med en blokering af fx et skadeligt domæne, som er identificeret ved håndtering af en cybersikkerhedshændelse mv.
- CFCS anbefaler en hybridmodel, hvor hovedparten af blokeringer sker på baggrund af oplysninger fra anerkendte abonnementsordninger og tjenester, hvorved det sikres, at CFCS kan rådgive om valget af ordning og om enkelte konkrete blokeringer, når CFCS finder det nødvendigt, uden det tydeliggøres, hvilke domæner mv. der er blokeret pba. CFCS' oplysninger.