Dansk Internet Forum

Notat

01-11-2021

DIFO's næste skridt

for mere retssikkerhed og ansvar på internettet

Resumé

Dansk Internetforum (DIFO) vil søsætte nye initiativer for at bidrage til bekæmpelsen af internetkriminalitet. På baggrund af en høring af det danske internetsamfund og en afgørelse fra Højesteret bliver de næste skridt at gå proaktivt ind i samarbejde med nye partnere, skaffe viden om og suspendere domænenavne, der bruges til phishing og malware. DIFO kommer også til at indføre en nye adgang i Vilkår for brugsret til et .dk-domænenavn til at suspendere domænenavne, der bruges i forbindelse med internetkriminalitet.

Baggrund

DIFO, som via driftsselskabet DK Hostmaster administrerer ca. 1,3 millioner .dk-domænenavne, afholdt en offentlig høring af det danske internetsamfund om DIFO's fortsatte rolle i bekæmpelsen af internetkriminalitet[1]. Der var et stort engagement og relevante tilbagemeldinger fra både borgere, myndigheder, virksomheder samt branche- og interesseorganisationer, som DIFO er meget taknemmelig for. En afrapportering over de indkomne synspunkter, bemærkninger og forslag er samlet i en rapport, der ligger her.

Sideløbende med høringen fandt der en længerevarende retssag sted om netop samme overordnede emne som høringen, og DIFO's bestyrelse besluttede derfor at lade sin afsluttende opfølgning på høringen afvente retssagens endelige udfald. Højesteret kom i foråret med en kendelse i sagen, og bestyrelsen har efterfølgende truffet beslutning om opfølgning på såvel høring som Højesterets afgørelse.

[1] Høringen blev gennemført ved et arrangement den 13. november 2019 efterfulgt af en skriftlig høringsperiode frem til den 6. januar 2020.

Resultatet af høring om DIFO's rolle i bekæmpelse af internetkriminalitet

Resultatet af bestyrelsens overvejelser om de tre centrale problemstillinger, som høringen af det danske internetsamfund handlede om, er beskrevet i det følgende:

1. **Skal DIFO kunne suspendere et domænenavn, når en offentlig myndighed beder om det, f.eks. hvis der på hjemmesiden sælges farlig medicin? Eller skal vi af hensyn til retssikkerheden først have en domstol til at vurdere, om der foregår noget ulovligt?**

   DIFO's beslutning:
   Tilbagemeldingerne fra det danske internetsamfund var ikke entydige. DIFO's bestyrelse fandt det bl.a. derfor ikke betryggende at indføre en generel ordning, hvor offentlige myndigheder og andre aktører kan anmode om og forvente, at DK Hostmaster suspenderer domænenavne uden at der foreligger en kendelse afsagt ved domstolene eller direkte lovhjemmel om blokering.

   Dette understøttes af, at DK Hostmaster i praksis har kunne spore en tendens til, at politiet og en forskellige række af forbrugermyndigheder bevist fravælger de allerede eksisterende klagemuligheder ved DK Hostmaster over uretmæssig brug af et .dk-domænenavn til fordel for de retshåndhævelsesmidler, der følger af lovgivningen. Det omfatter f.eks. kendelse mod en specifik udbyder af internetinfrastruktur (også kaldet "teknisk mellemmand") om fjernelse af indhold på en hjemmeside eller blokering af brugeradgang til hjemmesiden.

2. **Skal DIFO være opsøgende og suspendere domænenavne til hjemmesider, hvor der kan konstateres phishing eller malware-spredning? Eller er det først og fremmest et ansvar for ejerne af hjemmesider?**

   DIFO's beslutning:
   Ved høringen var der en vis overvægt i retning af, at DIFO skal være mere proaktiv i forhold til phishing og malware-spredning, der ofte er kendetegnene for uhyre effektiv, hurtig og skadelig udbredelse af cyberangreb. DIFO's bestyrelse anerkender denne trussel og har af samme grund søsat flere tiltag, der har til formål at øge sikkerheden på internettet. DK Hostmaster vil desuden via internationale kilder indhente information om spredning af phishing, malware mv. og dele denne viden med registranter og registratorer.

3. **Skal DIFO fremover kunne suspendere et hvilket som helst domænenavn, der bruges i forbindelse med åbenlys risiko for særligt alvorlige typer kriminalitet? Eller "blive ved sin læst" og fortsat afgrænse sig til de tilfælde, hvor der også er en forvekslingsrisiko med et kendt domænenavn, logo eller varemærke?**

   DIFO's beslutning:
   Tilbagemeldingerne fra det danske internetsamfund var ikke entydige. Derfor mener DIFO's bestyrelse ikke, at området for, hvornår DK Hostmaster egenhændigt kan blokere for adgang til en hjemmeside, bør udvides så markant, som det ville være tilfældet, hvis kravet om forvekslingsrisiko blev fjernet. Den førnævnte afgørelse fra Højesteret bestyrker DIFO i denne holdning. Afgørelsen fastslår, at under hensyn til karakteren af DK Hostmasters medvirken til udbredelse af indholdet på en hjemmeside må andre aktører i første omgang tage ansvar.

DIFO's reaktion på Højesteretsafgørelse om ansvar for blokering

Den 23. marts 2021 kom Højesteret med sin afgørelse i en sag om blokering af et domænenavn. DK Hostmaster blev frifundet for at skulle blokere et .dk-domænenavn, idet indholdet af hjemmesiden allerede var blevet fjernet af det pågældende webhostingselskab efter et påbud. Højesteret kom endvidere med ny principiel afklaring vedrørende retshåndhævelse på internettet ved at fastslå en indgrebsrækkefølge; at retskendelser om indgreb mod ulovligt indhold på en hjemmeside skal rettes mod bestemte aktører i en prioriteret rækkefølge.

Højesteret fastslog, at "[u]nder hensyn til karakteren af DK Hostmasters medvirken må et påbud eller forbud med henblik på at spærre for hjemmesiden dog i første række rettes mod krænkeren eller andre mellemmænd, der medvirker til udbredelsen, herunder webhostingselskabet. Kun i tilfælde, hvor dette – henset til formålet med et påbud eller forbud – ikke er en reel mulighed, må anses for udsigtsløst eller har vist sig utilstrækkeligt, kan et påbud eller forbud til DK Hostmaster komme på tale"[2].

Det betyder med andre ord, at den, der er blevet offer for ulovligt indhold på nettet, først skal gå til de parter, hvor et indgreb så præcist som muligt fjerner det ulovlige indhold. Først herefter kan man evt. gå til tekniske mellemmænd; hvis indgreb dog vil have konsekvenser, der går videre end blot at fjerne det ulovlige indhold eller adgangen hertil. Det er eksempelvis tilfældet, når DK Hostmaster får påbud om blokering af et .dk-domænenavn, idet adgangen til alt indhold på en hjemmeside fjernes samt den til domænenavnet knyttede e-mailkommunikation.

DIFO's beslutning:

DIFO anerkender som følge af Højesterets afgørelse, at det ultimativt vil kunne komme på tale, at DK Hostmaster blokerer for adgangen til en hjemmeside med ulovligt indhold, men at dette kun bør ske, når det har vist sig udsigtsløst at opnå et påbud eller forbud rettet mod andre tekniske mellemmænd.

Højesterets afgørelse har forøget retssikkerheden på internettet ved at gøre det klart for en forurettet person, hvem man skal gå til, når der er ulovligt indhold på en hjemmeside. Tilsvarende er den person, som et indgreb går ud over, også i højere grad sikret, at indgrebet er proportionelt. DIFO anser det for naturligt både at udbrede kendskabet hertil og at påtage sig sit ansvar som teknisk mellemmand. For at tilgodese dette har DIFO's bestyrelse besluttet, at der skal indføres en ny bestemmelse under afsnittet om uretmæssig brug af et domænenavn i DK Hostmasters Vilkår for brugsret til et .dk-domænenavn. Der vil blive afholdt en særskilt høring herom.

Denne bestemmelse vil gøre det muligt at suspendere et .dk-domænenavn, hvor der er tale om en åbenlys lovovertrædelse, og hvor påbud eller forbud mod alle forudgående mellemmænd i indgrebsrækkefølgen ikke er formålstjenesteligt, således som Højesteret har beskrevet det. Det er ydermere et krav, at forholdene konkret taler for, at sagen ikke indbringes for Klagenævnet for Domænenavne eller domstolene.

Højesterets afgørelse er en del af den juridiske udvikling af internettet, som finder sted i disse år. I det lys understøtter DIFO's tiltag internetudviklingen i samfundet og sikrer samtidig transparens. Begge dele er i lige så høj grad som selve administrationen af .dk-domænenavne opgaver, som påhviler DIFO efter den danske domænelov.

[2] Se afgørelsen på: https://domstol.dk/hoejesteret/aktuelt/2021/3/om-blokering-af-domaenenavn/