DIFO – Dansk Internet Forum
Kalvebod Brygge 45, 3. Sal
1560 København V

Sendes per email:
info@difo.dk

København, den 22. august 2016

Høringsbidrag vedrørende DIFOs rolle i bekæmpelsen af it-kriminalitet

Tak for muligheden for at komme med bidrag i forbindelse med DIFOs rolle i bekæmpelse af it-kriminalitet.

Distribution af piratkopier bruges stadig i omfattende grad som platform og indtægtskilde for kriminelle. Vi – danske virksomheder, der er afhængige af et marked med rimelige konkurrencevilkår – ønsker en mere dedikeret og effektiv indsats mod IP-kriminalitet på internettet. De kriminelle er i rivende udvikling med digitalisering af deres aktiviteter, og vi oplever, at retssystemet og håndhævelsen ikke er fulgt med.

Derfor er det positivt, at DIFO påtager sig en vigtig rolle i bekæmpelsen af it-kriminalitet. Vi ser gerne at DIFO, via sin rolle som administrator af .dk-domæner, påtager sig en mere aktiv rolle for både at skabe tryghed om .dk-zonen og samtidig for at udstikke principper for håndtering af denne del af internettets infrastruktur. Vi ser, at Danmark kan gå foran og inspirere andre lande til at følge tilsvarende principper.

Piratkopiering er som al anden kriminalitet på internettet per definition grænseoverskridende. De digitale kriminelle er agile, de kan flytte deres aktiviteter på kort tid, de er anonyme og de opererer typisk uden for Danmarks grænser. Vi står derfor skakmat, hvis vi forsøger at bekæmpe den digitale kriminalitet alene med traditionelle håndhævelsesværktøjer. Helt grundlæggende handler det om, at vi udvikler et mindset, ressourcer, kompetencer og praksis, der tager højde for de digitale udfordringer, vi står over for i dag. Derfor er det også helt afgørende, at vi kan bruge andre værktøjer end de traditionelle for at stoppe de kriminelles aktiviteter og pengestrømme. De værktøjer forudsætter involvering af nye centrale aktører på internettet. Kriminalitet inden for IP-området foregår typisk

ikke på .dk domænet. Grunden til dette er blandt andet, at vi i Danmark har været dygtige til at gøre det sværere at drive kriminelle aktiviteter, end det fx er i Sverige, hvor der findes adskillelige personer, der mere eller mindre åbenlyst driver eksempelvis pirattjenester. DIFOs rolle er helt afgørende i bestræbelserne på at sikre, at Danmark opretholder sin status som et land, hvorfra det er vanskeligt at drive kriminelle aktiviteter.

At det er vanskeligt at drive kriminelle aktiviteter fra Danmark er desværre ikke det samme som at der ikke foregår en masse kriminelle aktiviteter i Danmark. De kriminelle aktiviteter drives (også af danskere) blot fra udlandet (fx fra et .org, eller .com-domæne), det vil sige fra lande hvor sandsynligheden for at blive opdaget og stillet til ansvar er mindre end i Danmark.

På det civilretlige område har vi over de seneste 10 år udviklet forskellige værktøjer, som i dag er dynamiske og tilpasset den digitale udvikling, og som en bred gruppe af aktører står bag. Et af dem er et blokeringsværktøj, der gør det enkelt og smidigt at blokere for adgang til ulovlige (internationale) hjemmesider[1].

Denne form for samarbejde og model udbredes i øjeblikket til andre områder fx annonce- og betalingsområdet[2]. Det er vores ambition at modellen også kan inspirere inden for domæner og hosting. Vi kan se, at denne "Danske Model", virker på positivt på at dæmme op for kriminelle pengestrømme og trafik.

Den danske, dynamiske tilgang til håndhævelse, som er baseret på et "follow the money"-princip, får stor opmærksomhed internationalt, og derfor deltager vi bl.a. i ekspertgrupper i EU-Kommissionen, ligesom vi bliver inviteret af myndigheder i mange lande til at fortælle om tilgangen. Danmark står altså som en meget central spiller i den internationale udvikling af digital håndhævelse, og derfor er også den danske udvikling af domæneområdet centralt for udviklingen af de principper, der skal bære fremtidens håndhævelse på internettet.

I RettighedsAlliancen arbejder vi hver dag med at håndhæve digital kriminalitet. Helt konkret møder vi blandt andet følgende centrale udfordringer:

- **De digitale kriminelle etablerer sig uden for dansk jurisdiktion, mens deres aktiviteter foregår i Danmark.** Derfor er det helt centralt, at vi kan gøre andet end at stoppe en bagmand eller den kriminelle virksomhed. Vi skal i Danmark kunne stoppe kriminelle aktiviteter, pengestrømme og internettrafik lige så hurtigt som de kriminelle kan sætte dem i gang.
- **Det er meget nemt at være anonym på internettet.** På internettet stilles der ofte ikke krav om, at man skal legitimere sig, ligesom der hele tiden udvikles nye værktøjer, som de kriminelle bruger til at gemme sig. Vi ser, at kendskabet til og interessen omkring brug af anonymiseringsværktøjer er stigende.

---

1 http://www.teleindu.dk/wp-content/uploads/2014/10/TI-code-of-conduct-blokeringer.pdf

2 http://kum.dk/fileadmin/KUM/Documents/Nyheder%20og%20Presse/Pressemeddelelser/2015/Hensigtserklæring_7__maj_2015__3_.pdf

Oprettelsen af et suspensionsnævn, der kan agere dynamisk i forhold til ulovligt indhold på en hjemmeside, vil være et effektivt værn mod kriminelle aktiviteter på visse hjemmesider. Vi anerkender ikke, at etableringen af sådan et nævn i sig selv indebærer udfordringer i forhold til retssikkerhed eller ytringsfrihed. Tværtimod er sådanne hensyn med til at berettige og støtte oprettelsen af sådan et nævn. I forbindelse med tilrettelæggelsen af dette, vil der naturligvis skulle tages hensyn til fundamentale principper og retssikkerhedsmæssige hensyn, ligesom ved enhver anden form for håndhævelse. Inden for IP-området er det enkelt at konstatere, om der er tale om ulovlige aktiviteter (når der ikke er givet tilladelse til distribution af indhold), og der findes i dag en omfattende praksis, der belyser, hvornår der er tale om ulovlig virksomhed. Samtidig illustrer de civilretlige initiativer, som eksempelvis code of conduct, nævnt ovenfor, på bedste vis, at det er muligt at etablere dynamiske håndhævelsesværktøjer, der tager hensyn til de fundamentale hensyn og gældende retsprincipper.

En mere restriktiv validering af registranters identitet i forbindelse med registrering af .dk-domænenavne ser vi også som en meget vigtig indsats i bestræbelserne på at holde Danmark fri for bagmænd. For at sikre brugertryghed og sikkerhed er det centralt, at man skal identificere sig. Vi ser den samme udvikling i andre sammenhænge, fx på online-auktionshuse, som Gul og Gratis, hvor sælgere har mulighed for at identificere sig med NemID, hvilket giver tryghed for den køber, der handler med vedkommende. Gul og Gratis oplyser, at de har set mange positive effekter af at tilbyde dette værktøj, blandt andet fordi det gør det sværere for kriminelle at være på deres platforme, og dermed skaber tryghed for brugerne.

Muligheden for at undlade at opgive identitetsoplysninger, eller at opgive falske oplysninger, er en af de centrale barrierer for håndhævelse, og har derfor også internationalt fokus. EU IPO har netop udgivet denne rapport[3], der nævner muligheden for at opgive falsk eller ingen identitet i forbindelse med registrering af domænenavne, som en central drivkraft bag IP-kriminelle forretningsmodeller. Derfor er en restriktiv validering af registrantoplysninger afgørende for at forebygge kriminalitet.

Vi er positive over for alle initiativer, der kan bidrage til at forebygge og skride hurtigere ind over for kriminelle aktiviteter og pengestrømme, og vi deltager gerne i et videre arbejde med at udvikle håndhævelse og værktøjer til at bekæmpe it-kriminalitet.

Med venlig hilsen

Maria Fredenslund
Direktør, RettighedsAlliancen

T: +45 21647448
E: maria@rettighedsalliancen.dk

[3] https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/resources/Research_on_Online_Business_Models_IBM/Research_on_Online_Business_Models_IBM_en.pdf