JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K
DK Danmark

Dato: 24. september 2021
Kontor: Politikontoret
Sagsbeh: Morten Pilgaard Pedersen
Sagsnr.: 2021-0030-6501
Dok.: 2115853

Besvarelse af spørgsmål nr. 1505 (Alm. del) fra Folketingets Retsudvalg

Hermed sendes besvarelse af spørgsmål nr. 1505 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 30. august 2021. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Justitsministeriet skal anmode om, at det vedlagte bilag behandles **fortroligt**, da bilaget indeholder oplysninger om enkeltpersoners private forhold.

Nick Hækkerup

/

Christian Fuglsang

Slotsholmsgade 10
1216 København K.

T +45 3392 3340
F +45 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 1505 (Alm. del) fra Folketingets Retsudvalg:

> ”Vil ministeren kommentere og redegøre for sagen, der omtales i henvendelsen vedr. hacking, jf. REU alm. del - bilag 414 og herunder redegøre for politiets nuværende beføjelser og redskaber til opklaring af sager om hacking, og specifikt forholde sig til, hvilke barrierer politiet kan møde i forhold til opklaring af sådanne sager?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> ”Rigspolitiet kan oplyse, at hacking er kriminaliseret i straffelovens § 263, hvorefter en person kan straffes for uberettiget at skaffe sig adgang til en andens datasystem eller data, som er bestemt til at bruges i et datasystem. Efterforskning af sager vedrørende hacking er generelt lige så forskelligartet som efterforskning af andre former for kriminalitet og afhænger i meget høj grad af gerningspersonens anvendte modus, gerningspersonens tekniske kompetencer samt den forurettedes mulighed for at sikre dokumentation af den begåede forbrydelse.
>
> I den indledende efterforskningsfase vil politiet søge efter spor på den enhed, hvortil der er skaffet uberettiget adgang. Afhængigt af enhedens type og opsætning kan det eksempelvis være muligt at sikre oplysninger om den IP-adresse, hvorfra den uberettigede adgang er foretaget, eller hvortil kommunikation/data sendes. For at det kan lykkes, skal enheden, som der er skaffet uberettiget adgang til, være sat op med logning. Derudover må gerningspersonen ikke have ”ryddet op” efter sig selv i form af sletning af disse logfiler. Såfremt IP-adresse identificeres, er der mulighed for at slå op i en offentligt tilgængelig database over, hvem der har brugsretten over den pågældende IP-adresse. Det kan f.eks. være en virksomhed, der har brug for en fast IP-adresse, eller en internetudbyder, som stiller IP-adressen til rådighed for deres kunder. Ved henvendelse til vedkommende, der har brugsretten over den pågældende IP-adresse, kan det være muligt at få oplyst, hvem der har benyttet IP-adressen på tidspunktet for den begåede kriminalitet.
>
> Der er en række forhold, der kan bevirke, at det ikke er muligt at få oplyst identiteten på brugeren af en IP-adresse. For det første anvender internetudbydere i stort omfang en teknik, der medfører, at mange hundrede brugere kan anvende samme IP-adresse på samme tid. Hvis mange brugere anvender samme IP-adresse, kan disse brugere adskilles ved, at de får tilføjet et

Source Port Number til IP-adressen. I disse tilfælde kræver identifikation af brugerne, at der på den angrebne enhed er foretaget en logning af Source Port Number, hvilket sjældent sker, idet der ikke er behov for Source Port Number, hvis der er tilstrækkeligt med IP-adresser. For det andet er det ikke muligt at foretage identifikation på baggrund af IP-adresse, såfremt gerningspersonen har anvendt TOR-netværket eller VPN-tjeneste, hvor der ikke foretages logning eller registrering af den enkelte bruger. Endelig kan identifikation være vanskelig, hvis gerningspersonens angreb er gået via en eller flere kompromitterede servere uden for Danmark, idet sporene på de pågældende servere ofte vil være forsvundet, før lokalt politi med en international retsanmodning forsøger at sikre data.

I en række sager om hacking kan der foruden IP-sporet tillige være andre relevante efterforskningsmuligheder, herunder kommunikationssporet og et eventuelt pengespor. For så vidt angår kommunikationssporet vil det være relevant at undersøge, hvilke kommunikationskanaler gerningspersonen benytter til f.eks. at indgå aftaler. I forhold til pengesporet kan dette afstedkomme en undersøgelse af transaktioner med virtuelle valuta."

Justitsministeriet kan for så vidt angår den del af spørgsmålet, der vedrører en redegørelse for den konkrete sag, der henvises til i spørgsmålet, henvise til vedlagte bilag, som Justitsministeriet som følge af hensyn til enkeltpersoners private forhold skal anmode om bliver behandlet fortroligt.