JUSTITSMINISTERIET

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 3. april 2009
Kontor: Civil- og Politiafdelingen
Sagsnr.: 2009-150-1061
Dok.: JEE41725

Hermed sendes besvarelse af spørgsmål nr. 494 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 23. februar 2009. Spørgsmålet er stillet efter ønske fra Marlene Harpsøe (DF).

Brian Mikkelsen

/

Barbara Bertelsen

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 494 (Alm. del) fra Folketingets Retsudvalg:

> ”Hvad vil ministeren gøre for at stoppe de mange tyverier fra danskeres netbank-konti, og vil ministeren kontakte myndighederne i de lande, hvor gerningsmændene kommer fra, for at få disse myndigheder til at tage sagerne alvorligt og få stoppet kriminaliteten?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet følgende udtalelser fra Rigspolitiet, Statsadvokaten for Særlig Økonomisk Kriminalitet og Økonomi- og Erhvervsministeriet, hvortil der henvises:

Rigspolitiet har oplyst:

> ”Anmeldelser om it-kriminalitet, herunder netbank-kriminalitet behandles og efterforskes som udgangspunkt af de respektive politikredse.
>
> Rigspolitiet har igennem de seneste år gennemført en række initiativer med henblik på at sikre, at politiet også kan yde en effektiv og tidssvarende indsats mod it-kriminalitet.
>
> Dansk politis særlige efterforskningsekspertise på it-området er samlet i en særlig afdeling (NITEC) i Rigspolitiet. Rigspolitiet fastlægger bl.a. retningslinjer for det tekniske udstyr og de arbejdsmetoder, der anvendes som led i it-efterforskninger. Hertil kommer, at Rigspolitiet yder konkret efterforskningsmæssig bistand til politikredsene.
>
> Rigspolitiet er endvidere som led i bekæmpelsen af it-kriminalitet ansvarlig for dansk politis samarbejde med andre såvel nationale som internationale myndigheder og organisationer mv.
>
> De enkelte politikredse kan således som led i efterforskningen af kriminalitet, der begås under anvendelse af it, herunder i sager vedrørende netbank-kriminalitet, rette henvendelse til Rigspolitiet med anmodning om efterforskningsmæssig bistand.
>
> I et vist omfang indgives anmeldelser om it-kriminalitet direkte til Rigspolitiet. I sådanne sager udfører Rigspolitiet eventuelle uopsættelige efterforskningsskridt med henblik på bevissikring mv., hvorefter sagerne overdrages til den rette politikreds, der varetager den videre efterforskning samt tager

stilling til, hvorvidt der er grundlag for at rejse sigtelse og eventuel tiltale.

Det er karakteristisk for sager om netbank-kriminalitet, at sagerne som oftest er grænseoverskridende, og at sagerne rammer danske internetbrugere mere eller mindre tilfældigt. De forurettede er således som oftest bosiddende i forskellige politikredse, og gerningsmændene, der som regel befinder sig i udlandet, anvender ofte flere servere og computere placeret i forskellige lande, ligesom gerningsmændene anvender flere forskellige mellemmænd til at føre de ved netbank-kriminaliteten tilegnede penge ud af landet.

I det omfang efterforskning af sagernes elektroniske spor fører til udlandet eksempelvis i form af en i udlandet identificeret IP-adresse, tager Rigspolitiet – eventuelt i samarbejde med Statsadvokaten for Særlig Økonomisk Kriminalitet – kontakt til de relevante udenlandske myndigheder med henblik på efterforskningsmæssig bistand. I sager om it-kriminalitet, der kan spores til lande udenfor EU, er det væsentligt, at politiet hurtigt kommer i besiddelse af de fornødne oplysninger med henblik på at identificere gerningsmændene, idet der er forskel på, hvor lang tid elektroniske spor gemmes i de enkelte lande.

Erfaringsmæssigt bliver de fleste sager om netbank-kriminalitet begået med udgangspunkt i lande udenfor EU, herunder særligt i Rusland og Ukraine. Besvarelse af forespørgsler fra dansk politi om efterforskningsmæssig bistand i sådanne sager tager oftest meget lang tid, og de modtagne svar har i de fleste tilfælde ikke været af større betydning for efterforskningen.

Rigspolitiet deltager i et tæt internationalt samarbejde om bekæmpelse af it-kriminalitet. Rigspolitiet samarbejder således både med de øvrige EU-lande på området, ligesom Rigspolitiet har taget initiativ til etablering af en nordisk arbejdsgruppe under de nordiske rigspolitichefer. Arbejdsgruppen under de nordiske rigspolitichefer drøfter fælles problemstillinger i relation til bekæmpelse af it-kriminalitet, herunder netbank-kriminalitet, og udveksler best practice på området.

Sammen med de øvrige EU-lande deltager Danmark endvidere i et projekt vedrørende cyber-crime, der også omfatter netbank-kriminalitet. Formålet med projektet er bl.a. at udbygge det allerede eksisterende samarbejde på området og at udveksle erfaringer, herunder navnlig med henblik på at kunne opnå et bedre samarbejde med myndighederne i de lande, hvor gerningsmændene formodes at befinde sig."

Rigsadvokaten har oplyst:

> ”**1.** Statsadvokaten for Særlig Økonomisk Kriminalitet (SØK) deltager i et vist omfang i behandlingen af sager om netbankkriminalitet. Statsadvokaturen gennemfører selv efterforskning og strafforfølgning i enkelte sager og tilbyder endvidere politikredsene at bistå med den helt indledende efterforskning af elektroniske spor i udlandet. Statsadvokaturens nærmere funktion i den forbindelse er omtalt nedenfor under pkt. 3, efter at der indledningsvist er redegjort for egenskaberne ved netbankkriminalitet under pkt. 2.
>
> **2.** Det kan mere generelt oplyses, at netbankkriminalitet i praksis udføres ved, at en gerningsmand - almindeligvis i et andet land - skaffer sig adgang til en dansk netbankkundes computer ved såkaldt hacking. For at sløre sin identitet vil gerningsmanden typisk skaffe sig adgang via en række såkaldte springbræt, dvs. computere, hvortil gerningsmanden tillige skaffer sig adgang ved hacking, og som gerningsmanden alene anvender for at sløre efterforskningssporet fra den forurettede netbankkunde.
>
> Sideløbende hermed udsender gerningsmanden e-mails med tilbud om ansættelse i en pengeoverførselsvirksomhed el. lign. Det tilbudte arbejde består i realiteten i at hæve penge, der overføres fra en forurettet netbankkundes konto til den ansattes konto, og afsende disse penge fra en pengeoverførselsvirksomhed til en person i et andet land. Den ansattes løn betales almindeligvis som en vis procentdel af det overførte beløb.
>
> Når gerningsmanden har skaffet sig adgang til netbankkundens computer, vil netbankkriminaliteten almindeligvis blive udført således, at der overføres et beløb til en dansk konto, der indehaves af en person, der har ladet sig ansætte i gerningsmandens pengeoverførselsvirksomhed. Denne ”medarbejder” instrueres i at hæve pengene i kontanter hurtigst muligt og overføre 90-95 procent af pengene via en pengeoverførselsvirksomhed til en navngiven person – almindeligvis i et andet land.
>
> Når denne konstruktion anvendes, vil transaktionssporene i sagen blive sløret i en række led.
>
> For det første vil gerningsmandens anvendelse af sagesløse personers computere som såkaldte springbrætter indebære, at en eventuel efterforskning af det elektroniske spor vil omfatte it-efterforskning vedrørende alle springbrætter for at finde tilbage til gerningsmandens computer. Eftersom datasporet gennem disse springbrætter ofte vil krydse indtil flere lande-

grænser, vil denne efterforskning være meget omfattende og ressourcekrævende.

Hertil kommer, at denne efterforskning kan være resultatløs. SØK har kendskab til ét tilfælde, hvor det elektroniske spor er fulgt tilbage til en server i et østeuropæisk land. I dette land havde gerningsmanden kunnet leje computerkapacitet på en større server uden opgivelse af nødvendige identifikationsoplysninger til at udfinde den pågældende.

For det andet vil pengesporet blive sløret, når en "ansat" hæver pengene kontant på sin konto og overfører dem til en modtager i et andet land. Denne modtager vil ofte tillige være en "ansat", der atter vil hæve pengene kontant og overføre dem til et andet land på vej tilbage til hovedgerningsmanden.

På den baggrund er det erfaringsmæssigt mest effektivt at koncentrere efterforskningsindsatsen mod de personer, der har ladet sig "ansætte" som pengeoverførere. Disse personer er i en række tilfælde blevet straffet for hæleri i relation til databedrageri, jf. straffelovens § 290, jf. § 279 a.

3. Spørgsmålet om forankring af sager om netbankkriminalitet blev drøftet mellem Rigspolitiet og SØK medio 2007. Det blev i den forbindelse aftalt, at sager om netbankkriminalitet skal forankres i politikredsene.

Rigspolitiet og SØK vil dog i et vist omfang kunne assistere i den indledende efterforskning af sagerne. For Rigspolitiets vedkommende vil det i hovedsagen dreje sig om teknisk assistance, mens SØK vil kunne bistå med den helt indledende retshjælp med henblik på at følge et elektronisk spor til udlandet.

SØK vejleder ofte politikredsene om håndteringen af denne type sager, herunder også om spørgsmål om formulering af en eventuel tiltale, men har kun sjældent bistået med retshjælp i relation til et elektronisk spor i udlandet.

SØK's Hvidvasksekretariat holder endvidere de finansielle institutioner underrettet om sager om netbankkriminalitet, der er kendte af sekretariatet."

Økonomi- og Erhvervsministeren har oplyst følgende, hvortil der henvises:

> ”Det kan oplyses, at Forbrugerombudsmanden i medfør af betalingsmiddelloven bl.a. fører tilsyn med netbankernes indretning og sikkerhed.
>
> Forbrugerombudsmanden er bekendt med, at der særligt fra 4. kvartal 2008 har forekommet en række tilfælde, hvor kriminelle via netbankskunders pc´ere har kunnet få adgang til kunders netbank. Netbank-indbrudene sker ved, at it-kriminelle lægger "spionprogrammer" på kundernes pc. Spionprogrammet giver de it-kriminelle adgang til alt på kundens pc, fx adgangskoder, fotos og mailboks, og dermed også til kundens netbank.
>
> Forbrugerombudsmanden har løbende været i dialog med Finansrådet om initiativer for at forebygge kriminalitet af denne karakter. Det er med Finansrådet aftalt, at rådet hvert kvartal indberetter statistik om netbankindbrud til Forbrugerombudsmanden.
>
> Det har i denne forbindelse været centralt, at de tab, som har kunnet konstateres, fuldt ud er dækket af bankerne i henhold til reglerne i betalingsmiddelloven.
>
> Finansrådet har over for Forbrugerombudsmanden bl.a. oplyst, at banksektoren har iværksat en række initiativer, der skal forebygge den her omhandlede kriminalitet. Blandt initiativerne kan nævnes forskellige informationskampagner rettet dels direkte mod netbankkunderne, dels mere generelt advaret danskerne om at lade sig rekruttere til mellemmænd (såkaldte muldyr) til at hvidvaske pengene fra netbankindbrudene.
>
> Derudover anvender bankerne såkaldte "fraud-detection-systemer", der har til formål at identificere mistænkelige netbanktransaktioner. Såfremt en given transaktion vurderes at være mistænkelig, tager banken kontakt til kunden for at sikre sig, at kunden ønsker overførslen gennemført.
>
> Finansrådet er endvidere i tæt dialog med NITEC i Rigspolitiet for derigennem at koordinere indsatsen mod de kriminelle.
>
> Endelig arbejder bankerne med løbende at øge sikkerheden i eksisterende netbanksystemer og er derudover i gang med at udvikle en ny løsning, hvor sikkerheden suppleres med engangskoder. Den nye løsning vil nå ud til netbankkunderne i løbet af det kommende år.

Forbrugerombudsmanden vil løbende følge fremdriften i og resultaterne af disse initiativer."