

POLITIAFDELINGEN

Polititorvet 14
1780 København V

Telefon: 3314 8888
Direkte: 3391 0910
Lokal: 5050
Telefax: 3343 0006

Redegørelse

for udviklingen i IT-kriminalitet samt den politimæssige indsats på området

1. Indledning

I takt med den løbende udvikling og udbredelse af moderne informations- og kommunikationsteknologi kan der konstateres en stigning i såvel IT-kriminaliteten som anvendelsen af moderne informations- og kommunikationsteknologi i forbindelse med andre former for kriminalitet.

Udviklingen stiller politiet over for stadig større udfordringer i den kriminalitetsbekæmpende indsats.

2. Kriminalitetsudviklingen

For så vidt angår antallet af anmeldelser og sigtelser for visse former for IT-kriminalitet har udviklingen gennem de seneste år været følgende:



Sagstype	2000		2001		2002		2003		2004		2005	
	A	S	A	S	A	S	A	S	A	S	A	S
Elektronisk pengefalsk, strfl. § 169a ^{*)}	-	-	-	-	-	-	-	-	2	0	1	0
Børnepornografi, strfl. § 235	151	111	163	100	168	133	188	152	302 ***)	300 ***)	131	126
Hacking, strfl. § 263, stk. 2	83	44	67	31	50	30	33	13	35	27	38	14
Ulovlig anvendelse af kode til informationssystemer, strfl. § 263a ^{*)}	-	-	-	-	-	-	-	-	0	0	0	0
Databedrageri, strfl. § 279a	135	82	282	320	877	1722 **)	425	164	362	232	532	591
Elektronisk rådighedshindring, strfl. § 293, stk. 2	1	0	4	3	2	0	2	2	6	5	4	3
Piratkopiering, strfl. § 299b ^{*)}	-	-	-	-	-	-	-	-	7	6	26	22
Uberettiget anvendelse/videregivelse af betalingsmiddel/-kort, strfl. § 301 ^{*)}	-	-	-	-	-	-	-	-	19	2	14	8
Uberettiget anvendelse/videregivelse af kode til informationssystem, strfl. § 301a ^{*)}	-	-	-	-	-	-	-	-	0	0	4	4

*) indsat i straffeloven ved L 2004 352

**) Antallet af såvel anmeldelser som sigtelser for databedrageri efter straffelovens § 279a steg betydeligt i 2002. Dette skal formentlig ses i lyset af befolkningens generelt øgede tillid til forretningssteder på internettet og den kraftige stigning i anvendelsen af kreditkort til køb af varer og tjenesteydelser på internettet. Den hastige udvikling i antallet af kreditkortbetalinger medførte en øget interesse fra kriminelle, som udnyttede den manglende sikkerhed på området. Med indførelsen af kontrolcifre (CVV-kode) på nyudstedte Visa-/Dankort fra april 2002 blev sikkerheden i forbindelse med brugen af betalingskort ved køb af varer og tjenesteydelser på internettet væsentligt forbedret. Pr. 1. februar 2005 var samtlige Dankort og Visa-/Dankort udskiftet og bar således kontrolcifre.

***) Det bemærkes, at antallet af anmeldelser og sigtelser vedrørende børnepornografi i 2004 skal ses i sammenhæng med, at politiet dette år gennemførte to landsdækkende operationer rettet mod distribution af børnepornografi via internettet.

3. Særlige udviklingstendenser

Side 3

Strafbare forhold i forbindelse med børnepornografi begås i meget vidt omfang via internettet, hvor distribution af børnepornografi tidligere hovedsagelig har fundet sted under anvendelse af e-mail, chatprogrammer og nyhedsgrupper. Gennem de seneste år har politiet imidlertid konstateret, at distributionen i stadig større grad sker i lukkede chatfora og under anvendelse af fildelingstjenester.

Herudover modtager politiet stadig flere henvendelser om voksne, der via internettet har forsøgt at opnå seksuelt samkvem med børn, eller som har udsat børn for blufærdighedskrænkelser via internettet. Forholdene kan i visse situationer have karakter af ”grooming”, der begrebsmæssigt omfatter tilfælde, hvor en voksen opbygger et tillidsforhold til et barn, typisk via internet-chat eller mobiltelefoni, med henblik på senere at begå seksuelle overgreb på barnet.

Tilsvarende modtager politiet stadig flere henvendelser vedrørende ”phishing”, det vil sige forsøg via internettet på at franarre en person bl.a. bankoplysninger med henblik på misbrug af disse oplysninger.

Udviklingen inden for hacking er gået i retning af, at hackerne generelt sigter efter at opnå en uberettiget økonomisk gevinst med deres kriminelle aktiviteter, hvor motivet til hacking tidligere hovedsagelig var at efterlade en signatur og herved opnå en vis status i hackermiljøet. Hacking bliver således ofte en del af anden kriminalitet, herunder f.eks. databedrageri efter straffelovens § 279a.

Endelig har politiet i forbindelse med de tekniske undersøgelser af beslaglagt IT-udstyr konstateret, at de computere, der beslaglægges af politiet, har stadig større lagerkapacitet, og at de lagrede data stadig oftere er krypterede.

4. Den politimæssige indsats

Side 4

4.1. Generelt

Bekæmpelsen af IT-kriminalitet har høj prioritet for politiet, og gennem de seneste år er der løbende truffet foranstaltninger med henblik på at sikre, at politiet kan yde en effektiv og tidssvarende indsats på området, hvilket bl.a. forudsætter, at politiet råder over den fornødne efterforskningsmæssige kapacitet samt de nødvendige efterforskningsredskaber og specialiserede kompetencer på området.

I overensstemmelse med flerårsaftalen om politiets bevillingsmæssige forhold 2000-2003 og Rigspolicefens udmøntningsplan i tilknytning til flerårsaftalen blev der i forligsperioden afsat 14 årsværk inden for politiet med henblik på en forstærket indsats overfor udbredelse af børnepornografi på internettet og andre former for IT-kriminalitet.

De 14 polititjenestemænd gennemgik i 2002 en særlig uddannelse, som var etableret af Politiskolen i samarbejde med en ekstern udbyder. Målet med uddannelsen var primært at sætte deltagerne i stand til selvstændigt og i samarbejde med andre at efterforske IT-kriminalitet, herunder i forbindelse med udbredelse af børnepornografi, hacking og E-handel, og at give deltagerne forståelse for såvel kompleksiteten i relation til omfang og udbredelse af IT-kriminalitet som den relevante lovgivning på området. Endvidere tog uddannelsen sigte på at give deltagerne den nødvendige tekniske viden med henblik på efterforskningen af IT-kriminalitet.

I 2003 gennemførte Rigspolitiet en evaluering af den forstærkede indsats mod IT-kriminalitet, og der blev i den forbindelse udarbejdet en plan for en yderligere styrkelse af indsatsen, som blev iværksat i 2004.

Som led i planens gennemførelse er der tilført yderligere ressourcer til IT-efterforskningen, ligesom politiets særlige efterforskningsmæssige ekspertise på området er blevet samlet i et nationalt IT-efterforskningscenter (NITEC) under Rigspolitiets Politiafdeling.

IT-efterforskningscentret har i dag ca. 50 medarbejdere, herunder et antal medarbejdere, der er tilknyttet IT-efterforskningscentrets regionale enhed i Århus, samt en række medarbejdere, der ikke er politiuddannede, men som varetager opgaver i tilknytning til de politimæssige efterforskninger, bl.a. programudviklingen, der forudsætter særlig IT-ekspertise.

IT-efterforskningscentret yder bistand til politikredsene som led i efterforskningen og retsforfølgningen af kriminalitet, der er begået under anvendelse af moderne informations- og kommunikationsteknologi.

Bistanden ydes bl.a. i forbindelse med

- ransagninger i IT-miljøer,
- data-sikring og data-analyse,
- IT-relaterede kosterundersøgelser,
- åbning af krypterede og passwordbeskyttede data samt
- undersøgelse og udlæsning af data fra mobiltelefoner, organisere m.v.

Endvidere yder IT-efterforskningscentret bistand med henblik på efterforskningen af internet-relateret kriminalitet, herunder særligt i sager vedrørende distribution af børnepornografi på internettet samt sager vedrørende E-handel og hacking.

Herudover er IT-efterforskningscentret såvel nationalt som internationalt ansvarlig for dansk politis samarbejde med andre myndigheder og organisationer m.v. som led i bekæmpelsen af IT-kriminalitet. IT-efterforskningscentret kan i den forbindelse modtage og videreformidle henvendelser om strafbare forhold bl.a. på internettet.

IT-efterforskningscentret arbejder tæt sammen med de IT-efterforskningskoordinatorer, der er udpeget i politikredsene, og som koordinerer politikredsenes bistandsanmodninger og indgår i en løbende drøftelse med IT-efterforskningscentret om behandlingen og prioriteringen af disse anmodninger. IT-efterforskningskoordinatorerne indgår ligeledes i målgruppen for Politiskolens efteruddannelseskurser i IT-efterforskning.

Anmeldelser vedrørende IT-kriminalitet indgives som udgangspunkt til det stedlige politi. I et vist omfang indgives anmeldelser, herunder elektroniske, ligeledes direkte til IT-efterforskningscentret, som ved modtagelsen af anmeldelser udfører visse uopsættelige efterforskningskridt med henblik på bevissikring m.v. og i øvrigt søger anmeldelserne forankret i politikredsene efter de almindelige værnetingsregler.

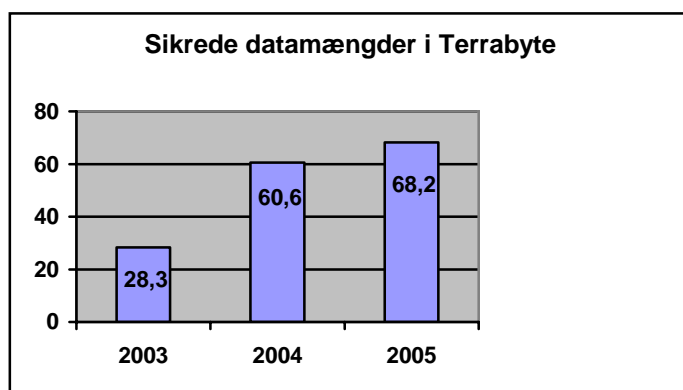
Antallet af henvendelser og anmeldelser til IT-efterforskningscentret vedrørende IT-kriminalitet har gennem de seneste år udvist en markant stigende tendens og kan - for så vidt angår en række af centrets kerneopgaver - opgøres således:

Sagstype	2003	2004	2005
Børnepornografi, strfl. § 235	259	461	791
Hacking, strfl. § 263, stk. 2	41	108	228
Phishing, strfl. § 279	0	2	117

Antallet af sager, hvor IT-efterforskningscentret på begæring af politikredsene har gennemført tekniske undersøgelser, kan gennem de seneste år - på udvalgte områder - opgøres på følgende vis:

Sagstype	ca. antal i 2003	ca. antal i 2004	ca. antal i 2005
Børnepornografi, strfl. § 235	134	277	129
Hacking, strfl. § 263, stk. 2	73	175	10
Databedrageri, strfl. § 279a	3	5	18

Som led i IT-efterforskningscentrets samlede tekniske undersøgelser er der konstateret en markant stigning i den sikrede datamængde:



Særligt for så vidt angår phishing bemærkes, at IT-efterforskningscentret har været inddraget i en række sager vedrørende falske phishing-hjemmesider på internettet, hvor de falske hjemmesider ikke har haft tilknytning til Danmark, hvorfor sagerne er blevet overdraget til udenlandske myndigheder. Herudover har IT-efterforskningscentret indledt et efterforskningsmæssigt samarbejde med udenlandske politimyndigheder i et antal sager, hvor falske phishing-hjemmesider var hostet hos danske internet-udbydere. Materiale fra internet-udbydere er i disse tilfælde blevet sikret og fremsendt til de relevante udenlandske politimyndigheder, idet sagerne ikke umiddelbart havde anden tilknytning til fysiske eller juridiske personer i Danmark, og hjemmesiderne er efterfølgende blevet lukket.

4.1. Indsatsen mod børnepornografi

Side 8

Rigspolitiet har gennem de seneste år truffet en række foranstaltninger med henblik på at styrke indsatsen mod distribution af børnepornografi på internettet.

Rigspolitiet har i den forbindelse indgået samarbejdsaftaler med en række internet-udbydere i bestræbelserne på i videst muligt omfang at søge at forhindre adgangen via internettet til børnepornografisk materiale, som det efter straffelovens § 235 vil kunne være strafbart at udbrede, besidde eller mod vederlag at gøre sig bekendt med.

Som led i samarbejdet med internet-udbydere videregiver Rigspolitiets IT-efterforskningscenter løbende - og på grundlag af de konkrete samarbejdsaftaler - oplysninger til internet-udbydere om internet-adresser, som IT-efterforskningscentret finder kan indeholde materiale, det efter straffelovens § 235 er strafbart at udbrede, besidde eller mod vederlag at gøre sig bekendt med. Samtidig med videregivelsen af oplysninger opfordres internet-udbydere til at blokere adgangen til de relevante internet-adresser. IT-efterforskningscentret underretter i øvrigt løbende internet-udbydere om ændringer i forhold til de oplysninger m.v., som tidligere er videregivet til internet-udbydere.

Det fremgår udtrykkeligt af de samarbejdsaftaler, som Rigspolitiet har indgået med internet-udbydere, at den enkelte internet-udbyder er bekendt med, at afgørelsen af, hvorvidt der konkret vil være tale om strafbare forhold, henhører under domstolene, og at eventuel beslutning om at indlede strafferetlig efterforskning og retsforfølgning træffes af politi og anklagemyndighed efter retsplejelovens regler. Beslutning om iværksættelse af efterforskning og retsforfølgning træffes i øvrigt uafhængigt af videregivelsen af oplysninger til internet-udbydere.

Endvidere fremgår det udtrykkeligt af samarbejdsaftalerne, at beslutningen om på grundlag af oplysningerne fra Rigspolitiets IT-efterforskningscenter at blokere for adgangen til visse internet-adresser og om den tekniske gennemførelse heraf træffes af den enkelte internet-udbyder i overensstemmelse med dennes forretningsbetingelser.

I forbindelse med blokeringen af adgangen til bestemte internet-adresser på grundlag af oplysninger fra IT-efterforskningscentret kan internet-udbyderne anvende en såkaldt stop-side. Indholdet af denne stop-side er nærmere fastlagt i samarbejdsaftalen mellem Rigspolitiet og den enkelte internet-udbyder.

Den aftalte stop-side redegør bl.a. for indholdet af straffelovens § 235. Herudover anføres det på stop-siden, at Rigspolitiets IT-efterforskningscenter har underrettet internet-udbyderen om, at den relevante internet-side kan indeholde materiale, der vil kunne anses for børnepornografisk, og at internet-udbyderen derfor efter opfordring fra Rigspolitiets IT-efterforskningscenter har valgt at blokere adgangen til internet-siden. Desuden fremgår det, at der kan rettes henvendelse til internet-udbyderen, hvis man har indvendinger imod, at adgangen til internet-siden er blokeret.

Samarbejdet har indtil videre ført til, at mere end 4000 hjemmesider er blevet blokeret. Statistiske opgørelser fra internet-udbyderne viser i øvrigt, at ca. 1700 danske internet-brugere dagligt søger at få adgang til de blokerede hjemmesider.

I foråret 2004 gennemførte Rigspolitiet i samarbejde med politikredsene to målrettede aktioner mod personer, der mistænktes for at besidde og distribuere børnepornografisk materiale. Aktionerne fik navnene ”Mjølner” og ”Enea”.

Efterforskningen i ”Mjølner”-aktionen blev gennemført på baggrund af informationer fra amerikanske myndigheder, der bl.a. dokumenterede, hvorledes danske betalingskort havde været anvendt til indkøb af børnepornografisk

materiale. Den 30. marts 2004 blev der på denne baggrund gennemført en koordineret politiaktion mod 119 mistænkte personer i Danmark. Side 10

Baggrunden for ”Enea”-aktionen var en række henvendelser fra politikredsene, offentligheden, Red Barnet og udenlandske politimyndigheder om distribution af børnepornografi under anvendelse af fildelingssystemer på internettet. Rigspolitiet udviklede i samarbejde med det norske Datakrimcenter et computerprogram, der kunne afsløre brugere, der havde stillet børnepornografisk materiale til rådighed for andre via fildelingssystemer på internettet. Efterforskningen identificerede 35 danske mistænkte, og fra en tilsvarende aktion i Italien modtog dansk politi oplysninger om yderligere 8 mistænkte personer i Danmark. Den 25. maj 2004 gennemførte norsk og dansk politi en koordineret politiaktion mod de mistænkte personer.

Tilsvarende aktioner – om end i mindre omfang – gennemføres i øvrigt løbende i samarbejde mellem politikredsene og Rigspolitiet.

4.2. Indsatsen mod ”grooming” på internettet

Rigspolitiet har i juli måned 2006 taget initiativ til at styrke indsatsen med henblik på at forebygge samt efterforske og retsforfølge strafbare forhold i forbindelse med ”grooming” på internettet.

Rigspolitiet har i den forbindelse over for politikredsene understreget vigtigheden af, at der i forbindelse med modtagelsen af anmeldelser om ”grooming” på internettet iværksættes en nærmere undersøgelse med henblik på om muligt at sikre oplysningerne i sagen, identificere de involverede personer og afdække, om der er grundlag for at indlede en egentlig efterforskning og retsforfølgning af et eventuelt strafbart forhold.

Rigspolitiet har endvidere henledt politikredsene opmærksomhed på mulighederne for at søge bistand i sager vedrørende ”grooming” på internettet fra Rigspolitiets IT-efterforskningscenter, ligesom Rigspolitiet har anmodet politikredsene om at underrette IT-efterforskningscentret om alle anmeldelser vedrørende ”grooming” på internettet, der modtages direkte i politikredsene.

På baggrund af disse indberetninger vil Rigspolitiets IT-efterforskningscenter i samarbejde med de relevante politikredse overveje mulighederne for i konkrete tilfælde at træffe særlige efterforskningsmæssige foranstaltninger, herunder efter omstændighederne ved, at politiet overtager kommunikationen på internettet under anvendelse af retsplejelovens regler om agentvirksomhed.

Rigspolitiet vil ligeledes tage initiativ til at udbygge samarbejdet mellem politiet og relevante tjenesteudbydere med henblik på at forebygge og bekæmpe ”grooming” på internettet. Dette udbyggede samarbejde vil bl.a. tage sigte på at indlede en nærmere dialog mellem politiet og relevante tjenesteudbydere om den information i form af advarsler og vejledninger vedrørende ”grooming”, som er tilgængelige i chatrooms på internettet, om administratorers løbende tilsyn med den kommunikation, der finder sted i chatrooms på internettet, om anvendelsen af særlige filtre i chatrooms på internettet, om logning og videregivelse af oplysninger til politiet samt om de særlige forhold, som tjenesteudbydere og administratorer i øvrigt skal være opmærksomme på i forbindelse med ”grooming” på internettet. Rigspolitiet vil tillige i samarbejde med relevante tjenesteudbydere undersøge mulighederne for et skærpet tilsyn med den kommunikation, der finder sted i lukkede kommunikationssystemer.

Efter Rigspolitiets opfattelse kan der ligeledes være grund til at fokusere på den forebyggende indsats i forhold til ”grooming” på internettet.

Forudsætningen for, at ”grooming” kan finde sted, er, at det udsatte barn foretager sig noget aktivt. Det er derfor afgørende, at voksne, der har ansvaret for børns

velfærd og trivsel, ligeledes ser det som deres opgave at sikre, at børn lærer nogle grundlæggende regler om kommunikationen med andre via bl.a. internettet, så de kan forholde sig kritisk til de mange muligheder og er opmærksomme på de risici, som denne kommunikation indebærer. Børn bør således sættes i stand til at gennemskue og sige fra over for potentielle krænkerer, og især forældre bør interessere sig for deres børns kommunikation via internettet, bl.a. ved selv at danne sig et indtryk af de chatrooms, som børnene anvender, og det materiale, som eventuelt lagres på computeren. Voksne, der har det daglige ansvar for børn, bør ligeledes være opmærksomme på børns internet-forbrug, herunder hvor og hvornår samt under hvilke omstændigheder et barn har adgang til internettet, og på barnets eventuelt ændrede adfærd i forbindelse hermed, f.eks. om barnet taler meget om seksuelle emner eller om en chatven, som ikke siden nævnes.

Allerede i dag er nærmere vejledning om emnet tilgængelig på hjemmesiden www.sikkerchat.dk, der er udarbejdet af Det Kriminalpræventive Råd i samarbejde med Red Barnet. På hjemmesiden kan børn og unge finde en række gode råd, interaktive spil og tests, historier fra det virkelige liv samt et debatforum m.v. Hjemmesiden indeholder desuden oplysninger, dialogredskaber og undervisningsmateriale til brug for forældre og lærere.

Det Kriminalpræventive Råd har ligeledes udgivet publikationen ”Overgreb mod Børn. Ser du det? Gør du noget?”. Publikationen retter sig mod faggrupper, der arbejder med børn og unge, og formidler viden om, hvordan overgreb mod børn, herunder i forbindelse med kommunikation på internettet, forebygges.

Rigspolitiet vil inddrage Det Kriminalpræventive Råds sekretariat i drøftelserne med relevante tjenesteudbydere med det sigte yderligere at styrke den kriminalpræventive indsats på området.

5. Det internationale samarbejde

Side 13

IT-kriminalitet er ofte af grænseoverskridende karakter, og Rigspolitiets IT-efterforskningscenter indgår derfor i et tæt internationalt samarbejde om bekæmpelse af IT-kriminalitet. Som led i dette samarbejde er der bl.a. taget initiativ til i en række lande, herunder i Danmark, at udpege døgnbetjente kontaktpunkter, så der hurtigt kan formidles kontakt mellem relevante politimyndigheder som led i efterforskningen af bl.a. strafbare forhold på internettet.

I forbindelse med bekæmpelsen af kriminalitet i tilknytning til E-handel indgår Rigspolitiets IT-efterforskningscenter bl.a. i IAFCI (International Association of Financial Crimes Investigators), der er en sammenslutning af myndigheder og civile organisationer og virksomheder, som beskæftiger sig med bekæmpelsen af økonomisk kriminalitet.

For så vidt angår hacker-kriminalitet har der i konkrete sager været etableret samarbejde mellem dansk politi og en række udenlandske politimyndigheder, herunder i Storbritannien, USA og Estland.

Særligt i relation til bekæmpelse af børnepornografi er der etableret et tæt samarbejde mellem Rigspolitiets og en række udenlandske samarbejdspartnere.

Samarbejdet indebærer bl.a., at Rigspolitiets IT-efterforskningscenter

- fungerer som nationalt kontaktpunkt for alle henvendelser vedrørende IT-kriminalitet fra internationale samarbejdspartnere, herunder Europol og Interpol,
- modtager efterforskningsoplæg vedrørende IT-kriminalitet fra udenlandske samarbejdspartnere, som videreformidles til relevante politikredse,
- deltager i internationale efterforskningsmøder og internationale efterforskningshold vedrørende IT-kriminalitet,

- identificerer filer med børnepornografisk indhold samt opdaterer og koordinerer billeddatabaser,
- foretager koordinering med udenlandske myndigheder med henblik på opdatering af hashset (elektronisk fingeraftryk på kendt børnepornografisk materiale),
- deltager i internationale møder med henblik på etablering af en international billeddatabase vedrørende børnepornografi og med henblik på identifikation af ofrene.

Rigspolitiet bidrager ligeledes til den internationale bekæmpelse af IT-kriminalitet ved i et vist omfang at stille medarbejdere fra IT-efterforskningscentret til rådighed for andre landes politimyndigheder med henblik på undervisning og rådgivning, ligesom IT-efterforskningscentret løbende deltager i uddannelsesaktiviteter og ekspertmøder m.v., der gennemføres i samarbejde med udenlandske samarbejdspartnere, herunder FBI og det amerikanske toldvæsen.

6. Afslutning

Rigspolitiet følger løbende udviklingen i IT-kriminaliteten med henblik på om nødvendigt yderligere at styrke indsatsen gennem uddannelsesmæssige, ressourcemæssige og teknologiske tiltag. Det bemærkes herved, at IT-efterforskningscentret fortsat vil yde politikredsene bistand også efter politireformens gennemførelse, og at Rigspolitiet for tiden er i færd med at ansætte foreløbigt yderligere fire politiuddannede medarbejdere i IT-efterforskningscentret og planlægger i løbet af 2007/2008 at ansætte yderligere otte medarbejdere.