EUROPA-
KOMMISSIONEN

Bruxelles, den 13.9.2017
COM(2017) 474 final

RAPPORT FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om vurdering af, i hvilket omfang medlemsstaterne har truffet de nødvendige foranstaltninger til at overholde direktiv 2013/40/EU om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/JHA

Indholdsfortegnelse

1. Indledning

Ifølge Europols trusselsvurdering af organiseret internetkriminalitet (IOCTA) for 2016 bliver IT-kriminalitet mere aggressiv og konfrontationssøgende. Dette kan ses i forskellige former for IT-kriminalitet, herunder angreb mod informationssystemer[1]. Visse alvorlige former for angreb, som Europol omtaler, er brugen af skadelig software og social engineering til at infiltrere og få kontrol over et informationssystem eller aflytte kommunikation og iværksættelse af omfattende netangreb, herunder angreb på kritisk infrastruktur. Disse angreb er blevet identificeret som værende centrale trusler for vores samfund.

I takt med at flere og flere oplysninger lagres i skyen, og eftersom oplysninger og kriminelle nu er meget mobile, har grænseoverskridende samarbejde mellem retshåndhævende myndigheder fået afgørende betydning for de fleste undersøgelser på IT-kriminalitetsområdet.

For at bekæmpe disse forbrydelser effektivt er det nødvendigt, at medlemsstaterne i fællesskab definerer, hvilke handlinger der bør anses for angreb på informationssystemer. De skal også foretage en indbyrdes tilnærmelse af sanktionerne og de operationelle midler til at anmelde forbrydelser og udveksle oplysninger mellem myndigheder. Derfor vedtog Europa-Parlamentet og Rådet den 12. august 2013 direktiv 2013/40/EU ("direktivet") om angreb på informationssystemer og om erstatning af Rådets rammeafgørelse 2005/222/RIA[2].

1.1. Direktivets mål og anvendelsesområde

Direktivets formål er at tilnærme medlemsstaternes strafferet til hinanden[3] med hensyn til angreb på informationssystemer og at forbedre samarbejdet mellem de kompetente myndigheder. Dette sker ved at fastsætte minimumsregler for definitionen af strafbare handlinger og sanktioner med hensyn til angreb på informationssystemer og ved at anmode om funktionsdygtige kontaktpunkter, der er tilgængelige døgnet rundt.

Om **definitionen** af relevante begreber i direktivet:

- Et "informationssystem" i artikel 2, litra a)[4]. Definitionen ligger tæt på definitionen af et edb-system som fastsat i artikel 1, litra a), i Europarådets konvention om IT-kriminalitet af 23. november 2001 (Budapestkonventionen) med den undtagelse, at direktivet også udtrykkeligt omfatter edb-data.
- "Edb-data" i artikel 2, litra b). Definitionen følger definitionen i artikel 1, litra b), i Budapestkonventionen om et informationssystem i stedet for et edb-system.
- En "juridisk person" i artikel 2, litra c). Definitionen skal sikre ansvar hos fysiske og juridiske personer, men ikke stater og offentlige organer eller offentlige internationale organisationer.

[1] Europol, 2016, Internet Organised Crime Threat Assessment (IOCTA), findes på https://www.europol.europa.eu/sites/default/files/documents/europol_iocta_web_2016.pdf.

[2] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:da:pdf.

[3] Nedenfor henviser, medmindre andet udtrykkeligt er anført, "medlemsstater" eller "alle medlemsstater" til de medlemsstater, der er bundet af direktivet, dvs. alle EU-medlemsstater undtagen Danmark, som ikke deltog i vedtagelsen af direktivet i overensstemmelse med artikel 1 og 2 i protokollen om Danmarks stilling, der er knyttet som bilag til traktaten om Den Europæiske Union og til traktaten om Den Europæiske Unions funktionsmåde (TEUF). I overensstemmelse med artikel 3 i protokol nr. 21 om Det Forenede Kongeriges og Irlands stilling, deltog begge i vedtagelsen af direktivet og er bundet heraf.

[4] Alle artikler, der nævnes, henviser til dem, der er fastsat i direktivet, medmindre andet er angivet.

- "Uretmæssig" i artikel 2, litra d). Definitionen vedrører et generelt strafferetligt princip og tager sigte på at undgå et strafferetligt ansvar for personer, der handler enten som tilladt i henhold til national lovgivning eller i henhold til en tilladelse udstedt af ejeren eller en anden retmæssig indehaver af systemet eller en del af det.

Specifikke strafbare handlinger er defineret, nemlig:

- ulovlig adgang til informationssystemer som sådan (artikel 3)
- ulovligt indgreb i informationssystemer (artikel 4), hvilket omfatter ulovlig adgang til et informationssystem, der forårsager en alvorlig hindring eller afbrydelse af et informationssystems drift
- ulovligt indgreb i data (artikel 5), hvilket henviser til ulovlige indgreb i computerdata, som forringer integriteten eller tilgængeligheden
- ulovlig opfangning (artikel 6) af ikke-offentlige overførsler af edb-data og elektromagnetisk udsending fra et informationssystem, der indeholder disse edb-data
- ulovlig tilvejebringelse af værktøjer, der anvendes til at begå de nævnte strafbare handlinger (artikel 7). I denne forbindelse kan sådanne redskaber være et edb-program samt en adgangskode eller andre data, der muliggør adgang til et informationssystem.

Desuden pålægger direktivet **strafferetligt ansvar** hos fysiske og/eller juridiske personer for anstiftelse, medvirken og tilskyndelse til at begå samt forsøg på at begå ovennævnte strafbare handlinger (artikel 8). Anstiftelse, medvirken og tilskyndelse omfatter alle de lovovertrædelser, der henvises til i artikel 3-7, mens forsøg kun henviser til artikel 4 og 5.

Mindsteniveauer for **maksimumsstraffe** for strafbare handlinger, som er omhandlet i direktivet, findes i artikel 9:

- Grundlæggende er der en maksimal fængselsstraf på mindst to år for alle de strafbare handlinger undtagen de, der fremgår af artikel 8 (artikel 9, stk. 2).
- Mindst tre års frihedsstraf som maksimumsstraf finder anvendelse på strafbare handlinger i henhold til artikel 4 og 5, når et betydeligt antal informationssystemer er blevet berørt (almindeligvis benævnt "botnet"-overtrædelser) (artikel 9, stk. 3).
- Der kræves mindst fem års frihedsstraf som maksimumsstraf for strafbare handlinger i henhold til artikel 4 og 5, som er begået af en kriminel organisation (artikel 9, stk. 4, litra a)), som forvolder alvorlig skade (artikel 9, stk. 4, litra b)) eller er begået mod et kritisk infrastruktur-informationssystem (artikel 9, stk. 4, litra c)).
- Når en lovovertrædelse efter artikel 4 og 5 begås i forbindelse med misbrug af en anden persons personoplysninger, bør medlemsstaterne sikre, at det kan betragtes som skærpende omstændigheder, medmindre disse omstændigheder allerede er omfattet af en anden lovovertrædelse (artikel 9, stk. 5).

De efterfølgende artikler indeholder minimumsbetingelser for **juridiske personers ansvar** (artikel 10) og en liste med eksempler på mulige sanktioner mod dem (artikel 11).

Idet det anerkendes, at ovennævnte strafbare handlinger kan begås (i betydningen "udføres") på et sted, hvor lovovertræderen faktisk handler, mens indvirkningen på det informationssystem, den strafbare handling er rettet mod, kan foregå et andet sted, fastsættes der i artikel 12 forpligtelser til at fastslå **straffemyndigheden**, idet der skelnes mellem:

- det sted, hvor lovovertræderen er fysisk til stede, når den strafbare handling begås,

- placeringen af det informationssystem, den strafbare handling er rettet mod,
- lovovertræderens nationalitet,
- hans/hendes sædvanlige opholdssted, og
- etableringsstedet for en juridisk person, til hvis fordel lovovertrædelsen er begået.

For så vidt angår udveksling af oplysninger skal medlemsstaterne ifølge artikel 13, stk. 1, sikre, at de har funktionsdygtige nationale **kontaktpunkter** til rådighed 24 timer i døgnet, syv dage om ugen, så de kan besvare eventuelle hastende udenlandske anmodninger inden for otte timer.

Derudover skal medlemsstaterne træffe de nødvendige foranstaltninger til at **lette anmeldelsen** af ovennævnte strafbare handlinger til de kompetente nationale myndigheder (artikel 13, stk. 3) og indsamle og dele et vist minimum af **statistiske oplysninger** om disse overtrædelser (artikel 14).

1.2 Rapportens formål og metode

I henhold til direktivets artikel 16 skal medlemsstaterne sætte de nødvendige love og administrative bestemmelser i kraft for at efterkomme direktivet senest den 4. september 2015 og meddele dem til Kommissionen.

Denne rapport opfylder kravet i direktivets artikel 17 om, at Kommissionen skal forelægge en rapport for Europa-Parlamentet og Rådet med en vurdering af, i hvilket omfang medlemsstaterne har truffet de nødvendige foranstaltninger for at efterkomme direktivet. Formålet med rapporten er således at give et kortfattet, men informativt overblik over de vigtigste gennemførelsesforanstaltninger, som medlemsstaterne har truffet.

Medlemsstaternes gennemførelse bestod i at indsamle oplysninger om den relevante lovgivning og administrative foranstaltninger, analysere disse, udarbejde ny lovgivning eller – i de fleste tilfælde – ændre eksisterende retsakter, vedtage dem og endelig rapportere dem til Kommissionen.

Inden for fristen for gennemførelse havde 22 medlemsstater meddelt Kommissionen, at de havde fuldført gennemførelsen af direktivet. I november 2015 indledte Kommissionen overtrædelsesprocedurer for manglende meddelelse af nationale gennemførelsesforanstaltninger mod de resterende fem medlemsstater: BE, BG, EL, IE og SI[5]. Den 31. maj 2017 var overtrædelsesprocedurer for manglende meddelelse af nationale gennemførelsesforanstaltninger mod BE, BG og IE fortsat verserende[6].

Beskrivelsen og analysen i denne rapport er baseret på de oplysninger, som medlemsstaterne forelagde den 31. maj 2017[7]. Anmeldelser, som er modtaget efter denne dato, er ikke blevet taget i betragtning. Alle anmeldte foranstaltninger med henvisning til national lovgivning blev taget i betragtning såvel som retsafgørelser og – hvor det er relevant – fælles juridisk teori.

[5] Medlemsstaterne i dette dokument er forkortet i henhold til: http://publications.europa.eu/code/da/da-5000600.htm.

[6] Oplysninger om Kommissionens afgørelser om overtrædelsesprocedurer kan findes her: http://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=da.

[7] IE meddelte fuldstændig gennemførelse af direktivet den 31. maj 2017.

Endvidere kontaktede Kommissionen i løbet af undersøgelsen medlemsstaterne direkte, såfremt det var nødvendigt og hensigtsmæssigt at modtage yderligere oplysninger eller præciseringer. Alle de indsamlede oplysninger blev taget i betragtning i forbindelse med analysen.

Ud over de spørgsmål, der identificeres i denne rapport, kan der være tale om yderligere udfordringer i forbindelse med gennemførelsen og andre bestemmelser, som ikke er indberettet til Kommissionen eller fremtidige lovgivningsmæssige og ikke-lovgivningsmæssige tiltag. Denne rapport er derfor ikke til hinder for, at Kommissionen kan foretage en yderligere evaluering af visse bestemmelser og fortsætte med at støtte medlemsstaterne med gennemførelsen og anvendelsen af direktivet.

2. Gennemførelsesforanstaltninger

2.1 Juridiske definitioner (direktivets artikel 2)

Direktivets artikel 2 indeholder retlige definitioner af "informationssystem", (litra a)), "edb-data", (litra b)), "juridisk person" (litra c)) og "uretmæssig" (litra d)). Kun CY og UK (Gibraltar) har indført lovgivning, der dækker alle aspekter af de definitioner, der er nævnt ovenfor. Nærmere bestemt indebærer dette:

a) Informationssystem

Direktivets definition er baseret på definitionen af udtrykket "edb-system" som fastsat i artikel 1, litra a), i Budapestkonventionen, hvor edb-data er en del af informationssystemet. CY, EL, IE, FI, HR, MT, PT og UK (Gibraltar) har indført lovbestemmelser med definitionen af et informationssystem, mens oplysningerne fra DE, ES, FR, LU, LV, PL, SE og SK ikke var entydige. For de øvrige medlemsstater, nemlig AT, BE, BG, CZ, EE, HU, IT, LT, NL, RO, SI og UK (undtagen Gibraltar), nævner de respektive juridiske definitioner ikke specifikt "edb-data". Dette indebærer en henvisning til artikel 1, litra a), i Budapestkonventionen med et identisk anvendelsesområde for definitionen af et edb-system.

b) Edb-data

"Edb-data" er fastlagt i lovgivningen i AT, BG, CY, CZ, DE, EE, EL, IE, FI, HR, LT, MT, NL, PT, RO og UK (Gibraltar), mens oplysningerne fra ES, FR, IT, LU, LV, PL, SE, SK og UK (undtagen Gibraltar) ikke var entydige. For så vidt angår SE, betyder den særlige opbygning af artiklerne, at denne definition er overflødig. For så vidt angår de resterende medlemsstater, henviser HU i definitionen af edb-data kun til strafbare handlinger, der er beskrevet i stk. 4 og 5 i direktivet, mens hverken BE eller SI har medtaget "et program, som kan anvendes til at få et informationssystem til at udføre en funktion" i definitionen af edb-data.

c) Juridisk person

Bortset fra LU, der ikke har afgivet tilstrækkelige oplysninger om gennemførelsen af artikel 2, litra c), gav gennemførelsen af definitionen af "juridisk person" ikke anledning til problemer. Dette skyldes generelt, at dette allerede er fastlagt i de fleste civilretlige eller handelsretlige bestemmelser i medlemsstaterne. Kun CY har en specifik bestemmelse i de foranstaltninger, der er vedtaget til gennemførelse af direktivet.

d) Uretmæssig

Med hensyn til definitionen af begrebet "uretmæssig" i artikel 2, litra d), er det kun CY, IE, RO og UK (Gibraltar), som underrettede om gennemførelse, mens 23 medlemsstater ikke havde nogen gennemførelsesforanstaltninger for denne definition. Det skal imidlertid

bemærkes, at der i alle medlemsstater er et generelt princip om ikke at ifalde strafferetligt ansvar for handlinger, som er udført med rettigheder.

2.2 Specifikke strafbare handlinger (direktivets artikel 3-7)

a) Ulovlig adgang til informationssystemer
Under henvisning til ulovlig adgang til informationssystemer er direktivets artikel 3 omfattet af den nationale lovgivning i AT, CY, CZ, EL, ES, IE, FI, FR, LT, LU, NL, PL, PT, SE og SK.

For så vidt angår alle resterende medlemsstater (BE, BG, DE, EE, HR, HU, IT, LV, MT, RO, SI og UK), adskiller den respektive nationale beskrivelse af den strafbare handling sig ikke fra at få adgang til hele eller kun en del af informationssystemet, selv om dette udtrykkeligt er fastsat i direktivet. Desuden omfatter DE's gennemførelse ikke blot adgang til computerhardware, og der er fastsat supplerende krav i AT og LU om en særlig hensigt (til at opnå viden, forvolde skade eller bedragerisk hensigt) og LV vedrørende årsagen til væsentlig skade. For så vidt angår BE, BG, FR, HR, LU, MT, PT, RO, SI og UK, er anvendelsesområdet for de nationale bestemmelser bredere end direktivet, da disse bestemmelser ikke kræver omgåelse af sikkerhedsforanstaltninger for at fastslå et strafansvar. De resterende medlemsstater henviser enten til, at den strafbare handling er begået ved overtrædelse af en sikkerhedsforanstaltning (CY, EL og SK), eller de anvender samme terminologi til at beskrive aspektet (AT, CZ, DE, EE, ES, FI, HU, IT, LV, LT, NL, PL og SE).

b) Ulovligt indgreb i informationssystemer
Direktivets artikel 4 vedrører ulovligt indgreb i informationssystemer. Direktivet indeholder otte mulige handlinger (indlæse edb-data, overføre, beskadige, slette, forvanske, ændre eller tilbageholde sådanne data eller at gøre sådanne data utilgængelige) og to mulige resultater af den pågældende retsakt (alvorlig hindringer eller afbrydelse af et informationssystems drift). BE, CY, CZ, EL, IE, FR, HR, LU, MT, PT, SE og UK (undtagen Gibraltar) har indført tilsvarende lovgivningsmæssige foranstaltninger. BG henviser kun til indtastning af et virus, mens der for de resterende medlemsstater (AT, DE, EE, ES, HU, IT, LV, NL, PL, RO, SI, SK og UK) gælder, at en eller op til fire af de mulige handlinger ikke er nævnt specifikt. I denne forbindelse kan det konstateres, at de fleste spørgsmål opstod i forbindelse med termerne "forvanske" (manglede i otte tilfælde) og "gøre utilgængelige" (i ni tilfælde).

c) Ulovligt indgreb i data
Direktivets artikel 5 omfatter ulovligt indgreb i data og indeholder en liste over de følgende seks handlinger: slette, beskadige, forvanske, ændre eller tilbageholde data eller gøre sådanne data utilgængelige. CY, EL, IE og MT har gennemført bestemmelsen ordret. BE, CZ, LT, PT og SE har anvendt mere generiske termer til at dække alle de mulige handlinger. Alle andre medlemsstaters gennemførelsesforanstaltninger dækker ikke hver af mulighederne, men henviser snarere til kun fem alternativer (FI og SK) eller mindre (AT, BG, DE, EE, FR, HR, HU, IT, LU, NL, PL, RO, SI og UK). De fleste spørgsmål opstod i forbindelse med "beskadige" (otte gange), "forvanske" (13 gange) og "gøre data utilgængelige" (13 gange). Ud over direktivets ordlyd kræver FI, "en hensigt om at forvolde skade eller økonomisk tab" for strafferetligt ansvar, mens LT og LV kræver en "påføring af alvorlig skade eller betydelig skade".

d) Ulovlig opfangning
Artikel 6 vedrører ulovlig opfangning og er målrettet ikke-offentlig fremsendelse af edb-data og elektromagnetiske emissioner fra et informationssystem, der bærer sådanne data. CY, CZ,

DE, ES, IE, FI, HR, LV, MT, RO, SE, SK og UK (Gibraltar) har indført lovgivning, som fuldt ud dækker artikel 6. Det generelle anvendelsesområde for direktivet, der henviser til aflytning af edb-data, er begrænset til meddelelser (AT og BG), observation af en person (EE) eller korrespondance (FR og HU). Kommissionen bemærker endvidere, at medlemsstaternes gennemførelsesforanstaltninger ikke dækker aflytning af elektromagnetisk stråling: BE, BG, EE, FR, HU, IT, LT, LU, NL, PL, PT, SI og UK (undtagen Gibraltar). Desuden kræver nogle medlemsstater særlig hensigt (f.eks. at opnå viden eller økonomiske fordele eller ulemper (AT, EL, HU) eller specifikke supplerende handlinger (f.eks. registrering af eller blive bekendt med det opfangede indhold – se BG og HU).

e) Værktøjer, der anvendes til at begå strafbare handlinger
Artikel 7 kriminaliserer en række handlinger vedrørende redskaber såsom computerprogrammer eller adgangskoder til at begå de lovovertrædelser, der er nævnt i artikel 3-6: fremstilling af sådanne værktøjer, salg, erhvervelse med henblik på brug, import, distribution eller på anden måde stillen til rådighed. AT, BE, CY, DE, EL, IE og SK har indført tilsvarende national lovgivning. Nogle medlemsstater dækker ikke alle de omhandlede strafbare handlinger (EE, IT, MT, PL og SI). Nogle henviser ikke til lovovertræderen i artikel 7 som en anden person end gerningsmanden i de nævnte strafbare handlinger i artikel 3-6 (CZ og SI). Nogle kræver en specifik hensigt (om at forvolde skade eller handle svigagtigt – se FI, IT og LU), et bestemt resultat, f.eks. overtrædelse af fortrolighed (BG), eller i det mindste en fremstilling af de omhandlede lovovertrædelser (SE). Endelig findes der uoverensstemmelser mellem artikel 7 og de nationale foranstaltninger i den manglende gennemførelse af alle de handlinger, der er opført på listen. Dette er tilfældet for BG, CZ, EE, ES, FR, HR, HU, IT, LT, LU, LV, PL, PT, RO, SI og UK. Blandt disse nævner LU's lovgivning specifikt fem af de seks mulige handlinger, der er nævnt i direktivet, mens andre medlemsstater udtrykkeligt henviser til kun fire eller færre.

Kun ES har gennemført alternativet erhvervelse med henblik på brug.

2.3 Generelle regler for de pågældende lovovertrædelser (direktivets artikel 8-12)

a) Anstiftelse, medvirken og tilskyndelse
I henhold til artikel 8, stk. 1, skal medlemsstaterne sikre, at det er strafbart at anstifte eller medvirke og tilskynde til at begå en strafbar handling som omhandlet i artikel 3-7. Alle medlemsstater har gennemført denne bestemmelse.

b) Forsøg
I henhold til artikel 8, stk. 2, er det strafbart at anstifte eller medvirke og tilskynde til at begå en strafbar handling som omhandlet i artikel 4-5. Mens PT ikke dækker alle former for forsøg på at begå strafbare handlinger i artikel 4, og SE mangler strafferetligt ansvar for forsøg på overtrædelse af "tavshedspligten", har alle andre medlemsstater indført lovgivning, der gennemfører denne bestemmelse.

c) Sanktioner
aa) Almindelig bestemmelse
I henhold til artikel 9, stk. 1, skal medlemsstaterne generelt sikre, at de strafbare handlinger i direktivet kan straffes med strafferetlige sanktioner, der er effektive, står i et rimeligt forhold til den strafbare handlings grovhed og har afskrækkende virkning. Selv om dette forudsættes for næsten alle medlemsstater, opfylder AT, BE, BG, IT, PT, SE og SI ikke de minimumsniveauer for de maksimumsstraffe, der er fastsat i artikel 9, stk. 2 (se afsnit 1.1 ovenfor), i alle tilfælde. Dette påvirker gennemførelsen af artikel 9, stk. 1, eftersom det kan

konkluderes, at minimumskravene i artikel 9, stk. 2, er et minimum for at påtage sig en effektiv, forholdsmæssig og afskrækkende sanktion.

bb) Generelt minimumsniveau for maksimumsstraffen

I henhold til artikel 9, stk. 2, skal mindsteniveauet for maksimumsstraffen for de standardlovovertrædelser, der er omhandlet i artikel 3-7, straffes med fængsel i mindst to år. De fleste medlemsstater overholder denne bestemmelse. Kun seks medlemsstater udviser visse forskelle: AT (højst seks måneders fængsel), BG (højst et års fængsel for alle strafbare handlinger med undtagelse af ulovlig opfangning), IT (højst et års fængsel for den strafbare handling i artikel 7b), PT (højst et års fængsel for den strafbare handling i artikel 3), SE (højst et års fængsel for den strafbare handling at "forvolde skade") og SI (højst et års fængsel for overtrædelse af artikel 3, 6 og 7). For så vidt angår BE, er minimumsniveauet for maksimumsstraffen for artikel 3, 6 og 7 først nået, når lovovertrædelsen er begået med bedragerisk hensigt.

cc) Et stort antal informationssystemer påvirkes.

I artikel 9, stk. 3, hæves minimumsniveauet for maksimumsstraffene til tre års fængsel, når et betydeligt antal informationssystemer berøres af en lovovertrædelse, der er omhandlet i artikel 4 og 5. Generelt har medlemsstaterne indført tilsvarende lovgivning, DE henviser kun til informationssystemer "som er af væsentlig betydning for en anden", FI kræver, at den strafbare handling skal vurderes "som helhed" for at anvende den højeste sanktion, og LV henviser ikke til et betydeligt antal informationssystemer (eller tilsvarende ordlyd), men kun til at forårsage "væsentlig skade". Oplysningerne fra BG og SI var ikke fyldestgørende.

dd) Kriminelle organisationer

I henhold til artikel 9, stk. 4, litra a), kan de strafbare handlinger i artikel 4 og 5 straffes med fængsel med en maksimumsstraf på mindst fem år, når de er begået af en kriminel organisation som defineret i rammeafgørelse 2008/841/RIA.

Igen overholder de fleste medlemsstater bestemmelsen i artikel 9, stk. 4, litra a). I henhold til straffeloven i LU og SI dækker bestemmelserne for en lovovertrædelse, som er begået inden for rammerne af en kriminel organisation, ikke IT-kriminalitet. BE's lovgivning indeholder en maksimumsstraf på tre års fængsel for lovovertrædelserne i artikel 5, DE's lovgivning omfatter ikke fysiske personer som ofre for de strafbare handlinger, i FI's lovgivning kræves en yderligere vurdering af overtrædelsen "som helhed", og SE's lovgivning fastsætter en maksimumsstraf på fire års fængsel for "grov forvoldelse af skade".

ee) Alvorlig skade

I artikel 9, stk. 4, litra b), fastsættes mindst fem år som den maksimale fængselsstraf for de strafbare handlinger, der er omhandlet i artikel 4 og 5, hvis de forvolder alvorlig skade. Selv om der ikke findes nogen definition af, hvad der skal betragtes som alvorlig skade, har alle medlemsstater undtagen BG, DE, FI, HU, LU og SE indført lovgivning, der svarer til direktivet. Oplysningerne fra HU var ikke fyldestgørende. BG når ikke op på maksimumsstraffen på mindst fem år, mens LU henviser til en almen sanktion for alvorlige skader, som ikke omfatter nogen IT-kriminalitet. Der forekommer mindre forskelle i DE (fysiske personer som ofre for de forbrydelser, som ikke er omfattet), FI (højere straf kræver yderligere vurdering af overtrædelsen "som helhed") og SE (maksimalt fire års fængsel for "grov forvoldelse af skade").

ff) Kritiske infrastrukturers informationssystemer

Inddragelse af kritiske infrastrukturers informationssystemer i lovovertrædelser, der er omhandlet i artikel 4 og 5, medfører også fængsel med en maksimumsstraf på mindst fem år som anført i artikel 9, stk. 4, litra c).
De fleste medlemsstater overholder denne bestemmelse, men BG gav ingen specifikke oplysninger om gennemførelsen. BE har fastsat et maksimum på tre år for overtrædelser af artikel 5. DE dækker ikke fysiske personer som ofre. FI kræver en yderligere vurdering af overtrædelsen "som helhed", IT kræver, at der faktisk er forårsaget "ødelæggelse", PT kræver et angreb på en "alvorlig og varig måde" og henviser ikke til artikel 5, og SE opfylder kun direktivets krav for "grov sabotage".

gg) Identitetstyveri og andre identitetsrelaterede strafbare handlinger

I henhold til artikel 9, stk. 5, skal medlemsstaterne sikre, at når de strafbare handlinger i artikel 4 og 5 begås ved at misbruge en anden persons personoplysninger med det formål at vinde tredjemands tillid og derved skade den, som identiteten egentlig tilhører, kan det, i overensstemmelse med national ret, betragtes som skærpende omstændigheder, medmindre disse omstændigheder allerede er omfattet af en anden lovovertrædelse. Den brede vifte af skønsbeføjelser har medført en lang række gennemførelsesforanstaltninger i medlemsstaterne. BE og EL har ikke meddelt nogen gennemførelse, og der findes ikke nogen specifik bestemmelse i CZ's strafferetlige lovgivning. Den skærpede tilgang blevet valgt af AT, CY, ES, IE, MT, PT og SE (sidstnævnte henviser til "særlig planlægning"), mens alle andre medlemsstater henviser til ekstra bestemmelser for en bestemt strafbar handling. Blandt dem, der henviser til særlige bestemmelser, kan gennemførelsesproblemer ses på følgende måde: BG og NL kræver en særlig hensigt ("om at få en fordel" og "det formål at skjule eller misbruge identiteten"), mens DE kun henviser til "personoplysninger, som ikke er almindeligt tilgængelige", FR kun henviser til navnet på en person og ingen andre personoplysninger, LV kræver "væsentlig skade", RO omfatter kun anvendelsen af "et dokument" og kræver, at der er begået svig.

d) Juridiske personers ansvar

aa) Generelt

I henhold til artikel 10, stk. 1, skal juridiske personers ansvar i forbindelse med strafbare handlinger, der er omfattet af artiklerne 3-8, fastslås, hvis gerningsmanden har en beføjelse til at repræsentere den juridiske person, litra a), har en bemyndigelse til at træffe beslutninger på den juridiske persons vegne, litra b) eller en bemyndigelse til at udøve intern kontrol inden for den juridiske person, litra c). Alle medlemsstater har indført lovgivning, der svarer til denne artikel med følgende forhold af mindre betydning: BG dækker ikke overtrædelsen af artikel 6, og HR henviser ikke til en gerningsmand, der har beføjelse til at udøve kontrol inden for den juridiske person (artikel 10, stk. 1, litra c)).

bb) Manglende tilsyn eller kontrol

I henhold til artikel 10, stk. 2, skal medlemsstaterne sikre, at den juridiske person kan drages til ansvar, hvis manglende tilsyn eller kontrol fra en af de i stk. 1 omhandlede personers side har gjort det muligt for en person at begå nogen af de i artikel 3-8 omhandlede strafbare handlinger. Selv om næsten alle medlemsstaterne overholder denne bestemmelse, var oplysningerne fra LU ikke fyldestgørende, og BG henviser ikke til en strafbar handling, som er omfattet af artikel 6.

e) Sanktioner over for juridiske personer

aa) Obligatoriske sanktioner

I direktivets artikel 11, stk. 1, pålægges medlemsstaterne at sikre, at juridiske personer, kan straffes med sanktioner, der er effektive, står i et rimeligt forhold til handlingens grovhed og

har afskrækkende virkning. Alle medlemsstater har meddelt de nationale foranstaltninger med undtagelse af IE og UK. I disse to lande er højest mulige beløb for sanktioner fortsat uafklaret på grund af manglen på konkrete lovbestemmelser. Således kan det ikke vurderes, om de enkelte sanktioner er effektive, står i et rimeligt forhold til handlingens grovhed og har afskrækkende virkning.

bb) Frivillige sanktioner

Artikel 11, stk. 1 fortsætter med en liste over muligheder for yderligere sanktioner over for juridiske personer. Disse er følgende: udelukkelse fra offentlige ydelser eller tilskud (valgt af CY, CZ, EL, ES, HR, HU, LU, MT, PL, PT og SK), midlertidigt eller varigt forbud mod at udøve erhvervsvirksomhed (AT, BE, CY, CZ, EL, ES, FR, HR, HU, IT, LT, LV, MT, PL, PT, RO, SE, SI og SK), anbringelse under retsligt tilsyn (CY, ES, FR, MT, PT og RO), tvangsopløsning (CY, CZ, EL, ES, FR, HR, HU, LT, LU, LV, MT, PT, RO, SI og SK) samt midlertidig eller permanent lukning af forretningssteder, der er blevet brugt til at begå den strafbare handling (BE, CY, WS, FR, LT, MT, PT og RO). Dermed har BG, DE, EE, IE, FI, NL og UK ikke valgt nogen af løsningsmulighederne.

cc) Sanktioner for undladelse

I henhold til artikel 11, stk. 2, skal medlemsstaterne sikre, at juridiske personer, som er ansvarlige for undladelse af lovovertrædelser som omhandlet i artikel 10, stk. 2, kan straffes med sanktioner eller andre foranstaltninger, der er effektive, står i et rimeligt forhold til handlingens grovhed og har afskrækkende virkning. Oplysningerne fra LU var ikke fyldestgørende. Alle andre medlemsstater med undtagelse af IE og UK har indført tilsvarende lovbestemmelser. For så vidt angår IE og UK, gør det samme sig gældende for artikel 11, stk. 1: (se punkt aa) ovenfor).

f) Straffemyndighed

aa) Obligatoriske regler vedrørende straffemyndighed

Artikel 12, stk. 2 og 3, i direktivet forpligter medlemsstaterne til selv at fastlægge deres straffemyndighed for de strafbare handlinger i artikel 3-8, når den strafbare handling er begået helt eller delvist på deres område – det være sig at gerningsmanden på gerningstidspunktet var fysisk til stede på tidspunktet for handlingen, eller at det berørte informationssystem var beliggende på medlemsstatens område – eller hvis den strafbare handling er begået i udlandet af en af medlemsstatens egne statsborgere. De fleste medlemsstater har indført tilsvarende national lovgivning, IT's lovgivning fastlægger ikke kompetence for statsborgere i udlandet for de grundlæggende lovovertrædelser, LV's og SI's lovgivning henviser til uklare bestemmelser, hvad angår territoriale aspekter, MT's kompetence for delvis anvendelse på eget område er uklar, og UK henviser til en computer i stedet for et informationssystem.

bb) Andre regler vedrørende straffemyndighed

Artikel 12, stk. 3, bestemmer, at hvis medlemsstater fastlægger straffemyndighed i tilfælde, hvor gerningsmanden har sit sædvanlige opholdssted på deres respektive område (valgt af AT, CY, CZ, FI, HR, IE, LT, LV, NL, SE og SK), eller hvis den strafbare handling er begået til fordel for en juridisk person, som har sit hjemsted på deres respektive område (CY, CZ, LV, PT, RO og SK), skal dette meddeles Kommissionen.

2.4 Operationelle spørgsmål (artikel 13-14 i direktivet)

a) Bestemmelse om funktionsdygtige nationale kontaktpunkter

I artikel 13, stk. 1, opfordres medlemsstaterne til at oprette funktionsdygtige nationale kontaktpunkter med henblik på udveksling af oplysninger om de strafbare handlinger i

artikel 3-8. På grundlag af den omhandlede bestemmelse er det nødvendigt, at medlemsstaterne sikrer, at der er indført procedurer til at give den kompetente myndighed mulighed for at svare inden for otte timer efter modtagelsen af en hurtig anmodning om bistand. Ifølge de anmeldte oplysninger har de fleste medlemsstater etableret den nødvendige infrastruktur. IE og RO anførte, at de respektive kontaktpunkter kun er disponible i et begrænset tidsrum hver dag, hvilket ikke vil gøre det muligt for myndigheden at give en tilbagemelding inden for otte timer efter modtagelsen af en anmodning i alle tilfælde. Flere medlemsstater oplyste, at de gør brug af eksisterende netværk af kontaktpunkter, der er etableret gennem G7-netværket eller inden for rammerne af Europarådets Budapestkonvention om IT-kriminalitet.

b) Oplysninger om etablerede funktionsdygtige nationale kontaktpunkter
I henhold til artikel 13, stk. 2, er medlemsstaterne forpligtede til at videregive kontaktoplysningerne på deres kontaktpunkter til Kommissionen, som sender disse oplysninger videre til de øvrige medlemsstater. Alle medlemsstater har fremlagt de nødvendige oplysninger.

c) Indberetningskanaler
I henhold til artikel 13, stk. 3, skal medlemsstaterne sikre, at der stilles passende anmeldelseskanaler til rådighed med henblik på at lette anmeldelsen til de kompetente nationale myndigheder om de i artikel 3-6 omhandlede strafbare handlinger. Oplysningerne fra HR, IT, IE og PT var ikke entydige. For de resterende medlemsstater synes der at være forskellige tilgange til gennemførelse af anmeldelseskanaler. De fleste medlemsstater (BE, BG, CY, CZ, DE, EE, EL, FI, FR, HR, HU, IT, LT, LV, MT, NL, PL, PT, RO, SE, SI, SK og UK) har meddelt foranstaltninger med kanaler til at gøre anmeldelsen lettere for den person eller organisation, der oprindeligt anmeldte en strafbar handling, f.eks. et offer for et IT-angreb (idet de faktiske anmeldelseskanaler fortsat er uklare for LV). Andre medlemsstater (AT, ES og LU) har imidlertid afgivet identiske oplysninger om gennemførelsen af artikel 13, stk. 1 og 2, hvoraf det fremgår, at deres foranstaltninger hovedsagelig vil lette kommunikationen mellem myndighederne.

d) Indsamling af statistiske data
I henhold til artikel 14, stk. 1 og 2, skal medlemsstaterne sikre, at der findes et system til registrering, fremstilling og fremlæggelse af statistiske oplysninger, som minimum om det antal strafbare handlinger omhandlet i artikel 3-7, som er registreret i medlemsstaterne, og antallet af personer, der er blevet retsforfulgt og dømt for disse lovovertrædelser. På grundlag af anmeldelserne synes de fleste medlemsstater at have indført både lovgivningsmæssige og administrative foranstaltninger for at sikre, at der indsamles oplysninger, almindeligvis på grundlag af et generelt nationalt elektronisk system. Oplysninger fra en række medlemsstater var ikke fyldestgørende (EL, IE, UK (Gibraltar, Nordirland og Skotland). En af grundene hertil var, at specifikke oplysninger om de lovovertrædelser, der er nævnt i direktivet, ikke må indsamles særskilt (BE, DE og SE), eller de indsamlede oplysninger ikke må omfatte alle de lovovertrædelser, der er nævnt i direktivet (RO).

e) Indberetning af statistiske oplysninger til Kommissionen
I artikel 14, stk. 3, opfordres medlemsstaterne til at fremsende de respektive statistiske oplysninger til Kommissionen. Alle medlemsstater, der anmeldte foranstaltninger, med undtagelse af UK (Gibraltar, Nordirland og Skotland) og HU, har bekræftet gennemførelsen af retlige eller administrative foranstaltninger eller begge dele for at sikre overholdelse af denne forpligtelse. For EL, ES, LU og SI var de fremlagte oplysninger ikke afgørende.

3. Konklusion og næste skridt

Direktivet har medført store fremskridt med hensyn til kriminalisering af IT-angreb på et sammenligneligt niveau i alle medlemsstater, hvilket letter det grænseoverskridende samarbejde mellem retshåndhævende myndigheder, der undersøger denne type strafbare handlinger. Medlemsstaterne har ændret straffelove og anden relevant lovgivning, effektiviseret procedurer og indført eller forbedret samarbejdsordninger. Kommissionen anerkender den store indsats fra medlemsstaterne til at gennemføre direktivet.

Der er dog stadig betydelige muligheder for at udnytte direktivets potentiale fuldt ud, hvis medlemsstaterne gennemfører alle bestemmelserne i fuldt omfang. Analysen viser indtil videre, at nogle af de vigtigste forbedringer, som medlemsstaterne skal opnå, omfatter anvendelse af definitionerne (artikel 2), som har en indvirkning på omfanget af de lovovertrædelser, som er defineret i den nationale lovgivning på grundlag af direktivet. Desuden synes medlemsstaterne at have fundet det vanskeligt at medtage alle mulighederne for at definere foranstaltninger med hensyn til lovovertrædelser (artikel 3-7) og de fælles normer for sanktioner for IT-angreb (artikel 9). Andre spørgsmål synes at vedrøre gennemførelsen af administrative bestemmelser om passende anmeldelseskanaler (artikel 13, stk. 3) og overvågning og statistik for de strafbare handlinger, der er omfattet af direktivet (artikel 14).

Kommissionen vil fortsat yde støtte til medlemsstaterne i deres gennemførelse af direktivet. Med hensyn til det potentielle bidrag til det grænseoverskridende samarbejde drejer dette sig navnlig om operationelle bestemmelser i direktivet om udveksling af oplysninger (artikel 13, stk. 1 og 2), anmeldelseskanaler (artikel 13, stk. 3) og overvågning og statistik (artikel 14). Med henblik herpå vil Kommissionen skabe yderligere muligheder for medlemsstaterne for at kortlægge og udveksle bedste praksis i anden halvdel af 2017.

Kommissionen ser på nuværende tidspunkt ikke noget behov for at foreslå ændringer af direktivet. I denne sammenhæng, og for også at understøtte kriminalefterforskninger af angreb på informationssystemer, cyberkriminalitet og andre typer kriminalitet, overvejer Kommissionen foranstaltninger, som skal forbedre den grænseoverskridende adgang til elektronisk bevismateriale i forbindelse med kriminalefterforskninger, herunder at stille forslag om lovgivningsmæssige foranstaltninger i begyndelsen af 2018.[8] Kommissionen overvejer også betydningen af kryptering i efterforskningen, og den vil rapportere om resultaterne senest i oktober 2017[9].

Kommissionen er fast besluttet på at sikre, at gennemførelsen afsluttes i hele EU, og at bestemmelserne gennemføres korrekt, bl.a. ved at holde øje med, at de nationale foranstaltninger er i overensstemmelse med de tilsvarende bestemmelser i direktivet. Kommissionen vil udnytte de håndhævelsesbeføjelser, den er tillagt i henhold til traktaterne, til om nødvendigt at indlede traktatbrudsprocedurer.

[8] Den indledende konsekvensanalyse af bedre grænseoverskridende adgang til elektroniske beviser af 4. august 2017 findes på ec.europa.eu.

[9] Communication on the Eighth progress report towards an effective and genuine Security Union, COM(2017) 354 final.