(Akti, sprejeti v skladu z naslovom VI Pogodbe o Evropski uniji)

OKVIRNI SKLEP SVETA 2005/222/PNZ

z dne 24. februarja 2005

o napadih na informacijske sisteme

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o Evropski uniji in zlasti členov 29, 30(1)(a), 31(1)(e) in 34(2)(b) Pogodbe,

ob upoštevanju predloga Komisije,

ob upoštevanju mnenja Evropskega parlamenta [1],

ob upoštevanju naslednjega:

(1) Cilj tega okvirnega sklepa je s približevanjem določb kazenskega prava držav članic izboljšati sodelovanje med pravosodnimi in drugimi pristojnimi organi, vključno s policijo in drugimi specializiranimi službami kazenskega pregona držav članic, na področju napadov na informacijske sisteme.

(2) Obstajajo dokazi o napadih na informacijske sisteme, zlasti kot posledica groženj s strani organiziranega kriminala, ter vse večja zaskrbljenost zaradi možnosti terorističnih napadov na informacijske sisteme, ki so del ključne infrastrukture držav članic. To predstavlja grožnjo doseganju cilja varnejše informacijske družbe ter območja svobode, varnosti in pravice in zato zahteva odgovor na ravni Evropske unije.

(3) Učinkovit odgovor na te grožnje zahteva celovit pristop do varnosti omrežij in informacij, kot je poudarjeno v akcijskem načrtu eEvropa, v sporočilu Komisije „Varnost omrežij in informacij: predlog evropske politike pristopa“ in Resoluciji Sveta z dne 28. januarja 2002 o skupnem pristopu in posebnih ukrepih na področju varnosti omrežij in informacij [2].

(4) Potreba po nadaljnjem ozaveščanju o problemih, povezanih z informacijsko varnostjo, in zagotavljanju praktične pomoči je prav tako poudarjena v Resoluciji Evropskega parlamenta z dne 5. septembra 2001.

(5) Velike vrzeli in razlike v zakonodaji držav članic na tem področju lahko ovirajo boj proti organiziranemu kriminalu in terorizmu ter otežijo učinkovito policijsko in pravosodno sodelovanje na področju napadov na informacijske sisteme. Ker so sodobni informacijski sistemi nadnacionalni in brezmejni, so napadi na takšne sisteme pogosto čezmejne narave; zato so nujno potrebni nadaljnji ukrepi za približevanje določb kazenskega prava na tem področju.

(6) Akcijski načrt Sveta in Komisije o čim boljšem izvajanju določb Pogodbe iz Amsterdama na področju svobode, varnosti in pravice [3], zasedanje Evropskega sveta v Tampereju 5. in 16. oktobra, zasedanje Evropskega svet v Santa Marii da Feiri 19. in 20. junija 2000, Komisija v „preglednici dosežkov“ in Evropski parlament v svoji resoluciji z dne 19. maja 2000 navajajo ali pozivajo na zakonodajne ukrepe proti kriminalu na področju visokih tehnologij, vključno s skupnimi opredelitvami, obtožnicami in sankcijami.

(7) Z zagotovitvijo skupnega pristopa do tega področja v Evropski uniji je treba dopolniti delo, ki so ga opravile mednarodne organizacije, zlasti delo Sveta Evrope na področju približevanja kazenske zakonodaje in delo skupine G8 o transnacionalnem sodelovanju na področju kriminala na področju visokih tehnologij. Ta poziv je bil še podrobneje opredeljen v sporočilu Komisije Svetu, Evropskemu parlamentu, Ekonomsko-socialnemu odboru in Odboru regij o „oblikovanju varnejše informacijske družbe z izboljšanjem varnosti informacijskih infrastruktur in bojem proti računalniškem kriminalu“.

(8) Kazensko zakonodajo na področju napadov na informacijske sisteme je treba približati, da se zagotovi največje možno policijsko in pravosodno sodelovanje na področju kaznivih dejanj, povezanih z napadi na informacijske sisteme, ter pripomore k boju proti organiziranemu kriminalu in terorizmu.

[1] UL C 300 E, 11.12.2003, str. 26.
[2] UL C 43, 16.2.2002, str. 2.
[3] UL C 19, 23.1.1999, str. 1.

(9) Vse države članice so ratificirale Konvencijo Sveta Evrope z dne 28. januarja 1981 o varstvu posameznikov pri avtomatski obdelavi osebnih podatkov. Osebne podatke, obdelane v okviru izvajanja tega okvirnega sklepa, je treba varovati v skladu z načeli te konvencije.

(10) Skupne opredelitve na tem področju, zlasti informacijskih sistemov in računalniških podatkov, so pomembne za zagotovitev doslednega pristopa pri uporabi tega okvirnega sklepa v državah članicah.

(11) Z zagotovitvijo skupnih opredelitev kaznivega dejanja nezakonitega dostopa do informacijskega sistema, nezakonitega poseganja v sistem in nezakonitega poseganja v podatke je treba doseči skupni pristop do sestavnih elementov kaznivih dejanj.

(12) Vsaka država članica mora v interesu boja proti računalniškemu kriminalu zagotoviti učinkovito pravosodno sodelovanje glede dejanj, ki temeljijo na ravnanjih, opisanih v členih 2, 3, 4 in 5.

(13) Treba se je izogniti prekomerni kriminalizaciji, zlasti v primerih majhnega pomena, in tudi kriminalizaciji imetnikov pravic in pooblaščenih oseb.

(14) Države članice zagotovijo potrebne kazni za napade na informacijske sisteme. Takšne kazni so učinkovite, sorazmerne in odvračilne.

(15) Primerno je predvideti strožje kazni za napade na informacijske sisteme, ki se izvedejo v okviru hudodelske združbe, kakor je opredeljena v Skupnem ukrepu 98/733/PNZ z dne 21. decembra 1998 o kaznivosti udeležbe v hudodelski združbi v državah članicah Evropske unije [1]. Prav tako je primerno predvideti strožje kazni, kadar takšen napad povzroči veliko škodo ali so bili prizadeti bistveni interesi.

(16) Predvideti je treba tudi ukrepe za sodelovanje med državami članicami zaradi zagotavljanja učinkovitega ukrepanja proti napadom na informacijske sisteme. V ta namen morajo države članice za izmenjavo informacij uporabiti obstoječo mrežo operativnih točk za stike iz Priporočila Sveta z dne 25. junija 2001 o točkah za stike s 24-urnim delovanjem za boj proti kriminalu na področju visokih tehnologij [2].

(17) Ker ciljev tega okvirnega sklepa, to je zagotoviti, da so za napade na informacijske sisteme v vseh državah članicah predpisane učinkovite, sorazmerne in odvračilne kazenske sankcije, ter izboljšati in spodbujati pravosodno sodelovanje z odstranjevanjem morebitnih zapletov, ne morejo v zadostni meri doseči države članice same, ker morajo pravila biti skupna in združljiva in se jih torej lažje doseže na ravni Unije, lahko Unija sprejme ukrepe, v skladu z načelom subsidiarnosti iz člena 5 Pogodbe ES. V skladu z načelom sorazmernosti iz omenjenega člena ta okvirni sklep ne presega tistega, kar je potrebno za dosego teh ciljev.

(18) Ta okvirni sklep spoštuje temeljne pravice in upošteva načela, ki jih priznava člen 6 Pogodbe o Evropski uniji in jih izraža Listina o temeljnih pravicah Evropske unije, zlasti Poglavji II in VI Listine –

SPREJEL NASLEDNJI OKVIRNI SKLEP:

Člen 1

Opredelitve pojmov

Za namene tega okvirnega sklepa se uporabljajo naslednje opredelitve pojmov:

(a) „Informacijski sistem“ pomeni vsako napravo ali skupino med seboj povezanih ali sorodnih naprav, od katerih ena ali več ob uporabi programa opravlja avtomatsko obdelavo računalniških podatkov, kakor tudi računalniške podatke, ki so shranjeni, obdelani, dostopni ali se po njih prenašajo zaradi njihovega delovanja, uporabe, varovanja in vzdrževanja.

(b) „Računalniški podatki“ pomeni vsako predstavitev dejstev, informacij ali konceptov v obliki, primerni za obdelavo v informacijskem sistemu, vključno s programom, ki lahko omogoči informacijskemu sistemu, da opravi svojo nalogo.

(c) „Pravna oseba“ pomeni vsak subjekt, ki ima status pravne osebe po ustrezni zakonodaji, razen držav ali drugih javnih organov pri izvrševanju državne oblasti, ter javnih mednarodnih organizacij.

[1] UL L 351, 29.12.1998, str. 1.

[2] UL C 187, 3.7.2001, str. 5.

(d) „Neupravičeno“ pomeni dostop ali poseganje brez odobritve lastnika, drugega imetnika pravice do sistema ali dela sistema, ali ki ni dovoljeno po nacionalni zakonodaji.

Člen 2

Nezakonit dostop do informacijskih sistemov

1. Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi, da se namerni neupravičeni dostop do celotnega ali katerega koli dela informacijskega sistema kaznuje kot kaznivo dejanje, vsaj v primerih, ki niso majhnega pomena.

2. Vsaka država članica lahko odloči, da je dejanje iz prvega odstavka kaznivo le v primerih, ko je storjeno s kršitvijo varnostnih ukrepov.

Člen 3

Nezakonito poseganje v sistem

Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi, da se namerno resno oviranje ali prekinjanje delovanja informacijskega sistema z vnašanjem, prenašanjem, poškodovanjem, brisanjem, slabšanjem, spreminjanjem, preprečevanjem in onemogočanjem dostopa do računalniških podatkov kaznuje kot kaznivo dejanje, ko je storjeno neupravičeno, vsaj v primerih, ki niso majhnega pomena.

Člen 4

Nezakonito poseganje v podatke

Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi, da se namerno brisanje, poškodovanje, slabšanje, spreminjanje, preprečevanje ali onemogočanje dostopa do računalniških podatkov na informacijskem sistemu kaznuje kot kaznivo dejanje, ko je storjeno neupravičeno, vsaj v primerih, ki niso majhnega pomena.

Člen 5

Napeljevanje, pomoč in podpiranje ter poskus

1. Vsaka država članica zagotovi, da se napeljevanje, pomoč in podpiranje dejanj iz členov 2, 3 in 4 kaznuje kot kaznivo dejanje.

2. Vsaka država članica zagotovi, da se poskus storitve dejanj iz členov 2, 3 in 4 kaznuje kot kaznivo dejanje.

3. Vsaka država članica se lahko odloči, da za dejanja iz člena 2 ne bo uporabljala odstavka 2.

Člen 6

Kazni

1. Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi, da so za dejanja iz členov 2, 3, 4 in 5 predpisane učinkovite, sorazmerne in odvračilne kazenske sankcije.

2. Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi, da je za dejanja iz členov 3 in 4 najvišja zagrožena kazenska sankcija najmanj eno do tri leta zapora.

Člen 7

Obteževalne okoliščine

1. Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi, da je za dejanje iz člena 2(2) ter za dejanja iz členov 3 in 4, kadar so bila storjena v okviru hudodelske združbe, kakor je opredeljena v Skupnem ukrepu 98/733/PNZ, poleg kazni predvidenih v navedenem Skupnem ukrepu, najvišja zagrožena kazenska sankcija najmanj dve do pet let zapora.

2. Država članica lahko sprejme ukrepe iz odstavka 1 tudi kadar je dejanje povzročilo veliko škodo ali prizadelo bistvene interese.

Člen 8

Odgovornost pravnih oseb

1. Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi odgovornost pravnih oseb za dejanja iz členov 2, 3, 4 in 5, ki jih je v njihovo korist, bodisi samostojno ali kot član organa pravne osebe, storila katera koli oseba na vodilnem položaju te pravne osebe, ki temelji na:

(a) pooblastilu za zastopanje pravne osebe; ali

(b) pristojnosti za sprejemanje odločitev v imenu pravne osebe; ali

(c) pristojnosti za opravljanje nadzora znotraj pravne osebe.

2. Razen za primere iz odstavka 1, države članice zagotovijo odgovornost pravne osebe tudi v primeru, ko sta pomanjkljiv nadzor ali kontrola osebe iz odstavka 1 omogočila, da je oseba, ki je podrejena tej pravni osebi v njeno korist storila dejanja iz členov 2, 3, 4 in 5.

3. Odgovornost pravne osebe iz odstavkov 1 in 2 ne izključuje kazenskega postopka zoper fizične osebe, ki so vpletene kot storilci, napeljevalci ali sostorilci dejanj iz členov 2, 3, 4 in 5.

Člen 9

Kazni za pravne osebe

1. Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi, da so za pravno osebo, odgovorno na podlagi člena 8(1), predpisane učinkovite, sorazmerne in odvračilne kazni, ki vključujejo kazenske sankcije ali denarne kazni, in ki lahko vključujejo tudi naslednje kazni:

(a) izključitev iz upravičenosti do državnih ugodnosti ali pomoči;

(b) začasna ali stalna prepoved opravljanja poslovnih dejavnosti;

(c) uvedba sodnega nadzora; ali

(d) sodni nalog za likvidacijo.

2. Vsaka država članica sprejme potrebne ukrepe, s katerimi zagotovi, da so za pravno osebo, odgovorno v skladu s členom 8(2), predpisane učinkovite, sorazmerne in odvračilne kazni ali ukrepi.

Člen 10

Sodna pristojnost

1. Vsaka država članica ima sodno pristojnost za dejanja iz členov 2, 3, 4 in 5, kadar je dejanje:

(a) bilo v celoti ali delno storjeno na njenem ozemlju; ali

(b) storil njen državljan; ali

(c) je bilo storjeno v korist pravne osebe s sedežem na ozemlju te države članice.

2. Pri ugotavljanju sodne pristojnosti v skladu z odstavkom (1)(a) vsaka država članica zagotovi, da njena sodna pristojnost vključuje primere, kadar:

(a) storilec stori dejanje, ko je fizično prisoten na njenem ozemlju, ne glede na to, ali gre za dejanje zoper informacijski sistem na njenem ozemlju; ali

(b) gre za dejanje zoper informacijski sistem na njenem ozemlju, ne glede na to, ali je storilec v času storitve dejanja fizično prisoten na njenem ozemlju.

3. Država članica, ki v skladu s svojo zakonodajo še ne izroča ali predaja svojih državljanov, sprejme potrebne ukrepe za vzpostavitev svoje sodne pristojnosti in pregona, kadar je to primerno, za dejanja iz členov 2, 3, 4 in 5, ko jih stori njen državljan izven njenega ozemlja.

4. Kadar dejanje spada v sodno pristojnost več kot ene države članice in lahko katera koli zadevna država upravičeno uvede kazenski pregon na podlagi istih dejstev, zadevne države članice s sodelovanjem odločijo, katera bo kazensko preganjala storilce, da se, če je le mogoče, postopek centralizira v eni sami državi članici. Zato se države članice za lažje sodelovanje med njihovimi pravosodnimi organi in usklajevanje njihovih dejavnosti lahko obrnejo na kateri koli organ ali mehanizem, ustanovljen v okviru Evropske unije. Pri tem se lahko zaporedno upoštevajo naslednji dejavniki:

— država članica je tista, na ozemlju katere so bila dejanja storjena glede na odstavek 1(a) in odstavek 2;

— država članica je tista, katere državljan je storilec;

— država članica je tista, v kateri je bil storilec najden.

5. Država članica se lahko odloči, da ne bo uporabljala pravil o sodni pristojnosti iz odstavkov 1(b) in 1(c), ali da jih bo uporabljala samo v posebnih primerih ali okoliščinah.

6. Kadar se države članice odločijo uporabljati odstavek 5, o tem obvestijo Generalni sekretariat Sveta in Komisijo, in če je primerno, navedejo tudi posebne primere ali okoliščine, na katere se njihova odločitev nanaša.

Člen 11

Izmenjava informacij

1. Zaradi izmenjave informacij o dejanjih iz členov 2, 3, 4 in 5 ter v skladu s pravili o varovanju podatkov države članice zagotovijo uporabo obstoječe mreže operativnih točk za stike, ki so na voljo štiriindvajset ur na dan in sedem dni na teden.

2. Vsaka država članica obvesti Generalni sekretariat Sveta in Komisijo o svojih točkah za stike, imenovanih zaradi izmenjave informacij o dejanjih v zvezi z napadi na informacijske sisteme. Generalni sekretariat informacije posreduje drugim državam članicam.

Člen 12

Izvajanje

1. Države članice sprejmejo potrebne ukrepe za izpolnitev določb tega okvirnega sklepa do 16. marca 2007.

2. Države članice posredujejo Generalnemu sekretariatu Sveta in Komisiji do 16. marca 2007 besedila vseh predpisov, ki v nacionalni pravni red prenašajo obveznosti iz tega okvirnega sklepa. Na podlagi poročila, izdelanega na osnovi teh podatkov, in pisnega poročila Komisije, Svet do 16. septembra 2007 oceni, v kolikšni meri države članice izpolnjujejo določbe tega okvirnega sklepa.

Člen 13

Začetek veljavnosti

Ta okvirni sklep začne veljati na dan objave v *Uradnem listu Evropske unije*.

V Bruslju, 24. februarja 2005

Za Svet

Predsednik

N. SCHMIT