EVROPSKA KOMISIJA

Bruselj, 30.9.2010
COM(2010) 517 konč.

2010/0273 (COD)

Predlog

DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA

o napadih na informacijske sisteme in razveljavitvi Okvirnega sklepa Sveta 2005/222/PNZ

{SEC(2010) 1122 final}
{SEC(2010) 1123 final}

OBRAZLOŽITVENI MEMORANDUM

1. RAZLOGI ZA PREDLOG IN NJEGOVI CILJI

Namen predloga je nadomestitev Okvirnega sklepa Sveta 2005/222/PNZ z dne 24. februarja 2005 o napadih na informacijske sisteme[1]. Okvirni sklep je, kot je navedeno v njegovih uvodnih izjavah, odziv na načrtovano izboljšanje sodelovanja med pravosodnimi in drugimi pristojnimi organi, vključno s policijo in drugimi specializiranimi službami kazenskega pregona držav članic, s približevanjem določb kazenskega prava v državah članicah na področju napadov na informacijske sisteme. Okvirni sklep uvaja zakonodajo EU za obravnavanje kaznivih dejanj, kot so nezakonit dostop do informacijskih sistemov, nezakonito poseganje v sisteme in nezakonito poseganje v podatke, ter posebna pravila glede odgovornosti pravnih oseb, sodne pristojnosti in izmenjave informacij. Države članice so morale potrebne ukrepe za izpolnitev določb Okvirnega sklepa sprejeti do 16. marca 2007.

Komisija je 14. julija 2008 objavila poročilo o izvajanju Okvirnega sklepa[2]. V sklepih poročila sta bila ugotovljena znaten napredek in razmeroma dobra raven izvajanja v večini držav članic, vendar v nekaterih državah članicah izvajanje še ni bilo končano. Poleg tega poročilo navaja, da so „[o]d sprejetja OS [...] nedavni napadi po Evropi opozorili na [številne] nove grožnje, zlasti pojav istočasnih napadov na informacijske sisteme in večja kazniva uporaba tako imenovanih botnetov“. Ti napadi ob sprejetju Okvirnega sklepa niso bili v središču pozornosti. Komisija bo kot odziv na ta potek dogodkov proučila ukrepe za opredelitev boljših odzivov na grožnjo (glej naslednji oddelek za razlago izraza „botnet“).

Pomembnost dodatnih ukrepov za pospešitev boja proti kibernetski kriminaliteti je poudarjena v Haaškem programu za krepitev svobode, varnosti in pravice v Evropski uniji iz leta 2004 ter v stockholmskem programu iz leta 2009 in pripadajočem akcijskem načrtu[3]. Poleg tega nedavno predstavljena Evropska digitalna agenda[4], prva vodilna pobuda, sprejeta v okviru strategije Evropa 2020, priznava potrebo po obravnavanju porasta novih oblik kriminala, zlasti kibernetske kriminalitete na evropski ravni. Na področju ukrepov, osredotočenih na zaupanje in varnost, se Komisija zavezuje ukrepom za boj proti kibernetskim napadom na informacijske sisteme.

Na mednarodni ravni se Konvencija Sveta Evrope o kibernetski kriminaliteti („Konvencija o kibernetski kriminaliteti“), ki je bila podpisana 23. novembra 2001, obravnava kot najbolj celovit mednarodni standard do zdaj, saj zagotavlja celosten in skladen okvir različnih vidikov na področju kibernetske kriminalitete[5]. Do zdaj je Konvencijo podpisalo vseh 27 držav članic, vendar jo je od teh ratificiralo le 15[6]. Konvencija je začela veljati 1. julija 2004. EU ni podpisnica Konvencije. Zaradi pomembnosti tega instrumenta Komisija dejavno spodbuja preostale države članice EU, da Konvencijo ratificirajo čim prej.

---

1 UL L 69, 16.3.2005, str. 68.

2 Poročilo Komisije Svetu na podlagi člena 12 Okvirnega sklepa Sveta z dne 24. februarja 2005 o napadih na informacijske sisteme, COM(2008) 448.

3 UL C 198, 12.8.2005, UL C 115, 4.5.2010, COM(2010) 171, 20.4.2010.

4 Sporočilo Komisije, COM(2010) 245, 19.5.2010.

5 Konvencija Sveta Evrope o kibernetski kriminaliteti, Budimpešta, 23.11.2001, STCE št. 185.

6 Pregled ratifikacij Konvencije (STCE št. 185) je na voljo na: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG

- **Splošno ozadje**

Glavni razlog za kibernetsko kriminaliteto je ranljivost, ki izhaja iz različnih dejavnikov. Nezadosten odziv mehanizmov kazenskega pregona prispeva k razširjenosti tega pojava in povečuje težave v zvezi z njim, saj nekatere vrste kaznivih dejanj presegajo državne meje. Poročanje o tej vrsti kriminala je pogosto nezadostno, deloma zato, ker se nekatera kazniva dejanja sploh ne opazijo, in deloma zato, ker žrtve (gospodarski subjekti in podjetja) kaznivih dejanj ne prijavijo, saj se bojijo slabega slovesa in negativnega vpliva, ki bi ga lahko javno izpostavljanje njihove ranljivosti imelo na poslovne možnosti v prihodnosti.

Poleg tega lahko razlike v nacionalnem kazenskem pravu in postopkih povzročijo razlike pri preiskavah in kazenskem pregonu, zaradi česar se lahko pojavijo razlike pri obravnavanju teh kaznivih dejanj. Razvoj na področju informacijske tehnologije je te težave dodatno povečal, saj sta se poenostavila izdelava in distribucija orodij („zlonamerna programska oprema“ in „botneti“), hkrati pa je storilcem zagotovljena anonimnost in odgovornost je razpršena v različnih sodnih pristojnostih. Težave v zvezi s sodnim pregonom organiziranemu kriminalu omogočajo velike dobičke ob majhnem tveganju.

Ta predlog upošteva nove metode izvajanja kibernetske kriminalitete, zlasti uporabo botnetov. Izraz „botnet“ pomeni mrežo računalnikov, ki so okuženi z zlonamerno programsko opremo (računalniškim virusom). Tako mrežo okuženih računalnikov („zombijev“) je mogoče sprožiti za izvedbo nekaterih dejanj, kot je napad na informacijske sisteme (kibernetski napad). Te „zombije“ je mogoče nadzirati, pogosto brez vednosti uporabnikov okuženih računalnikov, prek drugega računalnika. Ta „nadzorni“ računalnik se lahko imenuje tudi „center za upravljanje in nadzor“. Osebe, ki nadzorujejo ta center, so storilci kaznivega dejanja, saj okužene računalnike uporabljajo za napade na informacijske sisteme. Storilce je zelo težko izslediti, saj so lahko računalniki, ki sestavljajo botnet in izvajajo napad, na drugi lokaciji kot storilci.

Napadi prek botneta so pogosto obsežni. Obsežni napadi so lahko napadi z orodji, ki vplivajo na znatno število informacijskih sistemov (računalnikov), ali napadi, ki povzročijo znatno škodo, npr. v smislu motenih sistemskih storitev, finančnih stroškov, izgube osebnih podatkov itd. Škoda, ki jo povzročijo obsežni napadi, zelo vpliva na delovanje tarče napadov in/ali njeno delovno okolje. V tem smislu lahko „veliki botnet“ povzroči resno škodo. Botnete je težko opredeliti glede na velikost, vendar se ocenjuje, da je imel največji odkriti botnet od 40 000 do 100 000 povezav (tj. okuženih računalnikov) na 24 ur[7].

[7] Število povezav na 24 ur je običajna merska enota za oceno velikosti botnetov.

- **Obstoječe določbe na področju predloga**

Na ravni EU Okvirni sklep uvaja najnižjo raven približevanja zakonodaje držav članic pri kriminalizaciji številnih kibernetskih kaznivih dejanj, vključno z nezakonitim dostopom do informacijskih sistemov, nezakonitim poseganjem v sisteme, nezakonitim poseganjem v podatke ter napeljevanjem, pomočjo in podpiranjem takih dejanj.

Čeprav so države članice določbe Okvirnega sklepa na splošno izvajale, ima Sklep več pomanjkljivosti zaradi trenda pri velikosti in številu kaznivih dejanj (kibernetskih napadov). Zakonodajo približuje le pri omejenem številu dejanj, vendar morebitne grožnje, ki jo za družbo predstavljajo obsežni napadi, ne obravnava v celoti. Prav tako v zadostnem obsegu ne upošteva resnosti kaznivih dejanj in sankcij zoper njih.

Druge pobude in programi EU, ki se izvajajo ali so načrtovani, bolje obravnavajo težave, povezane s kibernetskimi napadi ali vprašanji, kot sta omrežna varnost in varnost internetnih uporabnikov. Vključujejo ukrepe, ki jih podpirajo programi „Preprečevanje kriminala in boj proti njemu“[8], „Kazensko pravosodje“[9], „Varnejši internet“[10] in „Pobuda o kritični informacijski infrastrukturi“[11]. Poleg Okvirnega sklepa je pomemben veljavni pravni instrument tudi Okvirni sklep 2004/68/PNZ o boju proti spolnemu izkoriščanju otrok in otroški pornografiji.

Na administrativni ravni so okužbe računalnikov s spreminjanjem v botnete prepovedane v okviru pravil EU o zasebnosti in varstvu podatkov[12]. Zlasti nacionalne upravne agencije že sodelujejo v okviru evropske kontaktne mreže organov za boj proti neželeni elektronski pošti. V skladu s temi pravili morajo države članice prepovedati prestrezanje komunikacije v javnih komunikacijskih omrežjih in v okviru javno dostopnih elektronskih komunikacijskih storitev, če nimajo dovoljenja zadevnih uporabnikov ali uradnega pooblastila.

Ta predlog je v skladu z navedenimi pravili. Države članice morajo pozornost nameniti izboljšanju sodelovanja med upravnimi organi in organi kazenskega pregona v zadevah, za katere so predvidene upravne in kazenske sankcije.

- **Usklajenost z drugimi politikami in cilji Unije**

Cilji so v skladni s politikami EU na področju boja proti organiziranemu kriminalu, povečanju odpornosti računalniških omrežij, zaščite kritične informacijske infrastrukture in varstva podatkov. Cilji so skladni tudi s programom „Varnejši internet“, oblikovanim za spodbujanje varnejše uporabe interneta in novih spletnih tehnologij ter za boj proti nezakonitim vsebinam.

Ta predlog je bil natančno pregledan, da se zagotovi celovita skladnost njegovih določbe s temeljnimi pravicami in zlasti z varstvom osebnih podatkov, pravicama do svobode izražanja in informiranja, pravico do pravičnega sojenja, načelom domneve nedolžnosti in pravico do obrambe ter tudi načeloma zakonitosti in sorazmernosti kaznivih dejanj in kazni.

---

8 Glej: http://ec.europa.eu/justice_home/funding/isec/funding_isec_en.htm

9 Glej: http://ec.europa.eu/justice_home/funding/jpen/funding_jpen_en.htm.

10 Glej: http://ec.europa.eu/information_society/activities/sip/index_en.htm.

11 Glej: http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm.

12 Direktiva o zasebnosti in elektronskih komunikacijah (UL L 201, 31.7.2002), kakor je bila spremenjena z Direktivo 2009/136/ES (UL L 337, 18.12.2009).

2. POSVETOVANJE Z ZAINTERESIRANIMI STRANMI IN OCENA UČINKA

- **Posvetovanje z zainteresiranimi stranmi**

Na več različnih srečanjih so potekala posvetovanja s številnimi strokovnjaki na tem področju, ki so obravnavala različne vidike boja proti kibernetski kriminaliteti, vključno s sodnim spremljanjem (sodnim pregonom) takšnih kaznivih dejanj. Posvetovanja so zlasti vključevala predstavnike vlad držav članic ter zasebni sektor, specializirane sodnike in tožilce, mednarodne organizacije, evropske agencije in strokovne organe. Številni strokovnjaki in organizacije so naknadno predložili stališča in posredovali informacije.

Ključne ugotovitve posvetovanja so:

– EU mora na tem področju ukrepati;

– kot kaznive je treba opredeliti nove oblike dejanj, ki niso vključene v trenutni Okvirni sklep, zlasti nove oblike kibernetskih napadov (botneti);

– odpraviti je treba ovire pri preiskavi in kazenskem pregonu čezmejnih primerov.

Informacije, pridobljene med posvetovanjem, so upoštevane v oceni učinka.

Zbiranje in uporaba izvedenskih mnenj

Zunanje izvedensko mnenje je bilo pridobljeno med različnimi srečanji z zainteresiranimi stranmi.

Ocena učinka

Proučene so bile različne možnosti politik kot sredstva za dosego cilja.

- Možnost (1): ohranitev obstoječega stanja/brez novih ukrepov EU

Ta možnost pomeni, da EU ne bo sprejela novih ukrepov za boj proti tej vrsti kibernetske kriminalitete, tj. napadom na informacijske sisteme. Tekoči ukrepi se bodo še naprej izvajali, zlasti programi za krepitev zaščite kritične informacijske infrastrukture in izboljšanje javno-zasebnega sodelovanja pri boju proti kibernetski kriminaliteti.

- Možnost (2): razvoj programa za krepitev prizadevanja na področju boja proti napadom na informacijske sisteme z nezakonodajnimi ukrepi

Nezakonodajni ukrepi bi se osredotočali na program za zaščito kritične informacijske infrastrukture, čezmejni kazenski pregon in javno-zasebno sodelovanje. Cilj teh nezavezujočih pravnih instrumentov mora biti spodbujanje dodatnih usklajenih ukrepov na ravni EU, vključno s krepitvijo obstoječe mreže kontaktnih točk za organe kazenskega pregona, ki so na voljo 24 ur na dan sedem dni v tednu, ustanovitev mreže javno-zasebnih kontaktnih točk v EU, ki bo vključevala strokovnjake na področju kibernetske kriminalitete in organe kazenskega pregona, pripravo standardnega sporazuma EU o ravni storitev za sodelovanje organov kazenskega pregona z nosilci dejavnosti v zasebnem sektorju ter podpora pri organizaciji programov usposabljanja za organe kazenskega pregona na področju preiskav kibernetske kriminalitete.

- Možnost (3): ciljna posodobitev pravil Okvirnega sklepa (nova direktiva, ki bi nadomestila veljavni Okvirni sklep) za obravnavanje grožnje, ki jo predstavljajo obsežni napadi na informacijske sisteme (botneti) in, če je kaznivo dejanje storjeno s prikrito identiteto storilca in je pri tem oškodovan zakoniti lastnik identitete, učinkovitosti kontaktnih točk organov kazenskega pregona držav članic ter pomanjkanja statističnih podatkov o kibernetskih napadih.

Ta možnost uvaja posebno ciljno (tj. omejeno) zakonodajo, ki preprečuje obsežne napade na informacijske sisteme. Tako okrepljeno zakonodajo bodo spremljali nezakonodajni ukrepi za krepitev operativnega čezmejnega sodelovanja proti takim napadom, ki bo spodbujalo izvajanje zakonodajnih ukrepov. Ti ukrepi bi bili namenjeni višji stopnji pripravljenosti, varnosti in odpornosti kritične informacijske infrastrukture ter izmenjavi najboljših praks.

- Možnost (4): uvedba celostne zakonodaje EU proti kibernetski kriminaliteti

Ta možnost vključuje novo celostno zakonodajo EU. Poleg uvedbe nezavezujočih pravnih ukrepov iz možnosti (2) in posodobitve iz možnosti (3) obravnava tudi druge pravne težave, povezane z uporabo interneta. Taki ukrepi ne bi zajemali le napadov na informacijske sisteme, ampak tudi vprašanja, kot so finančna kibernetska kriminaliteta, nezakonite internetne vsebine, zbiranje/shranjevanje/prenos elektronskih dokazov in podrobnejša pravila o sodni pristojnosti. Zakonodaja bi se uporabljala vzporedno s Konvencijo Sveta Evrope o kibernetski kriminaliteti in vključevala navedene spremne nezakonodajne ukrepe.

- Možnost (5): posodobitev Konvencije Sveta Evrope o kibernetski kriminaliteti

Ta možnost bi zahtevala obsežna ponovna pogajanja o veljavni Konvenciji, kar je dolgotrajen postopek, ki je v nasprotju s časovnim okvirom za ukrepe, predlaganim v oceni učinka. Zdi se, da se mednarodna skupnost ni pripravljena ponovno pogajati o Konvenciji. Posodobitve Konvencije torej ni mogoče obravnavati kot izvedljive možnosti, saj presega zahtevani časovni okvir za ukrepe.

Najprimernejša možnost: kombinacija nezakonodajnih ukrepov (možnost (2) s ciljno posodobitvijo Okvirnega sklepa (možnost (3)

Na podlagi analize gospodarskih in socialnih vplivov ter vplivov na temeljne pravice sta možnosti (2) in (3) najboljši pristop k obravnavanju problematike ter način za uresničitev ciljev predloga.

Pri pripravi tega predloga je Komisija izvedla oceno učinka.

3. PRAVNI ELEMENTI PREDLOGA

- **Povzetek predlaganih ukrepov**

Direktiva bo razveljavila Okvirni sklep 2005/222/PNZ, vendar bo ohranila njegove določbe in vključila naslednje nove elemente:

– Na področju kazenskega materialnega prava na splošno Direktiva:

A. kaznuje izdelavo, prodajo, naročilo za uporabo, uvoz, distribucijo ali drugo dajanje na voljo naprav/orodij, ki se uporabljajo za kazniva dejanja;

B. vključuje obteževalne okoliščine:

- vidik obsežnosti napadov – botnetov ali podobnih orodij bi bil obravnavan z uvedbo nove obteževalne okoliščine, in sicer da je dejanje vzpostavitve botneta ali podobnega orodja obteževalni dejavnik pri storitvi kaznivih dejanj, naštetih v obstoječem Okvirnem sklepu,

- če so taki napadi storjeni s prikrito identiteto storilca in je pri tem oškodovan zakoniti lastnik identitete. Vsa taka pravila bi morala biti v skladu z načeli zakonitosti in sorazmernosti kaznivih dejanj in kazni ter v skladu z obstoječo zakonodajo na področju varstva osebnih podatkov[13];

C. uvaja „nezakonito prestrezanje“ kot kaznivo dejanje;

D. uvaja ukrepe za izboljšanje sodelovanja evropskega kazenskega pravosodja s krepitvijo obstoječe strukture kontaktnih točk, ki so na voljo 24 ur na dan sedem dni v tednu[14]:

- predlaga se obveznost delovanja v skladu z zahtevo po pomoči operativnih kontaktnih točk (iz člena 14 Direktive) v okviru predvidene časovne omejitve. Konvencija o kibernetski kriminaliteti v zvezi s tem nima zavezujoče določbe. Namen tega ukrepa je zagotoviti, da kontaktne točke v predvidenem času navedejo, ali lahko najdejo rešitev za zahtevo po pomoči in v kolikšnem času lahko kontaktna točka, ki je zahtevo vložila, pričakuje rešitev. Dejanska vsebina rešitev ni določena;

E. obravnava potrebo po zagotovitvi statističnih podatkov o kibernetski kriminaliteti, pri čemer morajo države članice zagotoviti vzpostavitev ustreznega sistema za beleženje, pripravo in predložitev statističnih podatkov o kaznivih dejanjih iz obstoječega Okvirnega sklepa ter o na novo dodanem „nezakonitem prestrezanju“.

Direktiva v opredelitvah kaznivih dejanj iz členov 3, 4 in 5 (nezakonit dostop do informacijskih sistemov, nezakonito poseganje v sisteme in nezakonito poseganje v podatke) vsebuje določbo, ki omogoča, da se med prenosom v nacionalno zakonodajo inkriminirajo samo „primeri, ki niso majhnega pomena“. S takšno prožnostjo naj bi se državam članicam omogočilo da ne bi pokrivale primerov, ki bi jih *in abstracto* pokrivala osnovna opredelitev, a sicer štejejo za neškodljive za zaščiteni pravni interes, npr. zlasti dejanja mladih, ki skušajo dokazati svojo strokovnost na področju informacijske tehnologije. Ta možnost omejevanja področja uporabe inkriminacije ne bi smela povzročiti uvedbe dodatnih sestavnih elementov kaznivih dejanj, poleg že obstoječih v Direktivi, saj bi tako nastala situacija, v kateri bi bila pokrita samo kazniva dejanja, storjena pod obteževalnimi okoliščinami. Med prenosom zakonodaje se morajo države članice vzdržati od dodajanja drugih sestavnih elementov osnovnim kaznivim dejanjem, kot sta posebni namen pridobitve premoženjske koristi iz kaznivih dejanj ali povzročitev znatne škode.

---

[13] Kot sta Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37) (trenutno v reviziji), ter Direktiva 95/46/ES o splošnem varstvu podatkov.

[14] Uvedeni s Konvencijo in Okvirnim sklepom 2005/222/PNZ o napadih na informacijske sisteme.

- **Pravna podlaga**

Člen 83(1) Pogodbe o delovanju Evropske unije[15].

- **Načelo subsidiarnosti**

Načelo subsidiarnosti se uporablja za ukrepe Evropske unije. Države članice ciljev predloga ne morejo zadovoljivo doseči iz naslednjih razlogov:

kibernetska kriminaliteta in zlasti napadi na informacijske sisteme imajo veliko čezmejno razsežnost, ki je najbolj očitna pri obsežnih napadih, saj so povezani elementi napada pogosto na različnih lokacijah in v različnih državah. To zahteva ukrepanje na ravni EU, zlasti za omejitev trenutnega trenda obsežnih napadov v Evropi in po svetu. K ukrepanju na ravni EU in posodobitvi Okvirnega sklepa 2005/222/PNZ pozivajo tudi Sklepi Sveta iz novembra 2008[16], ker države članice ne morejo same zadovoljivo dosegati cilja učinkovite zaščite državljanov pred kibernetsko kriminaliteto.

Ukrepi Evropske unije bodo učinkoviteje dosegli cilje predloga iz naslednjih razlogov:

predlog bo dodatno približal kazensko materialno in procesno pravo držav članic, kar bo pozitivno vplivalo na boj proti tem kaznivim dejanjem. To je način, da se storilcem prepreči selitev v države članice, v katerih je zakonodaja proti kibernetski kriminaliteti manj stroga. Poleg tega skupne opredelitve omogočajo izmenjavo informacij ter zbiranje in primerjanje zadevnih podatkov. Tako se bosta okrepila tudi učinkovitost preventivnih ukrepov po vsej EU in mednarodno sodelovanje.

Predlog je zato v skladu z načelom subsidiarnosti.

- **Načelo sorazmernosti**

Predlog je v skladu z načelom sorazmernosti iz naslednjih razlogov:

Ta okvirni sklep je omejen na minimum, ki je potreben za uresničitev navedenih ciljev na evropski ravni in ne presega tega, kar je potrebno za uresničitev teh ciljev, in sicer ob upoštevanju
potrebe po natančnosti kazenske zakonodaje.

- **Izbira instrumentov**

Predlagani instrument: direktiva.

Druga sredstva ne bi bila ustrezna iz naslednjega razloga:

Pravna podlaga zahteva direktivo.

Nezakonodajni ukrepi in samonadzor bi izboljšali razmere na nekaterih področjih, na katerih je izvajanje bistveno. Vendar bi bile na drugih področjih, na katerih je nova zakonodaja nujna, koristi majhne.

---

15 UL C 83, 30.3.2010, str. 49.

16 „Usklajena strategija dela in praktični ukrepi proti kibernetski kriminaliteti“, 2987. zasedanje Sveta za pravosodje in notranje zadeve, Bruselj, 27.–28. november 2008.

4. PRORAČUNSKE POSLEDICE

Predlog v majhnem obsegu vpliva na proračun Unije. Več kot 90 % ocenjenih stroškov, ki znašajo 5 913 000 EUR, bi krile države članice, pri čemer obstaja možnost za predložitev vlog za financiranje EU za zmanjšanje stroškov.

5. DODATNE INFORMACIJE

- **Razveljavitev obstoječe zakonodaje**

S sprejetjem predloga se razveljavi obstoječa zakonodaja.

- **Ozemeljska veljavnost**

Ta direktiva je naslovljena na države članice v skladu s Pogodbama.

2010/0273 (COD)

Predlog

DIREKTIVA EVROPSKEGA PARLAMENTA IN SVETA

o napadih na informacijske sisteme in razveljavitvi Okvirnega sklepa Sveta 2005/222/PNZ

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti

člena 83(1) Pogodbe,

ob upoštevanju predloga Evropske komisije[17],

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora,

ob upoštevanju mnenja Odbora regij,

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Cilj te direktive je približati pravila kazenskega prava držav članic na področju napadov na informacijske sisteme ter izboljšati sodelovanje med pravosodnimi in drugimi pristojnimi organi, vključno s policijo in drugimi specializiranimi službami kazenskega pregona držav članic.

(2) Napadi na informacijske sisteme, zlasti kot posledica groženj organiziranega kriminala, so vedno večja grožnja, povečuje pa se tudi zaskrbljenost zaradi možnosti terorističnih ali politično motiviranih napadov na informacijske sisteme, ki so del ključne infrastrukture držav članic in Unije. To ogroža uresničevanje ciljev varnejše informacijske družbe ter območja svobode, varnosti in pravice ter zato zahteva odziv na ravni Evropske unije.

(3) Obstajajo dokazi o težnjah k vedno bolj nevarnim in ponavljajočim se obsežnim napadom na informacijske sisteme, ki so ključni za države ali za posebne funkcije v javnem ali zasebnem sektorju. Te težnje spremlja razvoj vedno bolj zahtevnih orodij, ki jih storilci kaznivih dejanj lahko uporabljajo za različne vrste kibernetskih napadov.

(4) Skupne opredelitve na tem področju, zlasti opredelitve informacijskih sistemov in računalniških podatkov, so pomembne za zagotovitev skladnega pristopa k uporabi te direktive v državah članicah.

---

[17] UL C […], […], str. […].

(5) Skupni pristop k sestavnim elementom kaznivih dejanj je treba doseči z uvedbo skupnih opredelitev za kazniva dejanja nezakonitega dostopa do informacijskega sistema, nezakonitega poseganja v sisteme, nezakonitega poseganja v podatke in nezakonitega prestrezanja podatkov.

(6) Države članice morajo zagotoviti potrebne kazni za napade na informacijske sisteme. Te morajo biti učinkovite, sorazmerne in odvračilne.

(7) Primerno je uvesti strožje kazni za napade na informacijske sisteme, ki jih izvede hudodelska združba, kakor je opredeljena v Okvirnem sklepu Sveta 2008/841/PNZ z dne 24. oktobra 2008 o boju proti organiziranemu kriminalu[18], če je napad obsežen ali če je kaznivo dejanje storjeno s prikrito identiteto storilca in je oškodovan zakoniti lastnik identitete. Prav tako je primerno predvideti strožje kazni, kadar takšen napad povzroči veliko škodo ali so zaradi njega prizadeti bistveni interesi.

(8) Iz Sklepov Sveta z dne 27.–28. novembra 2008 izhaja, da morajo države članice in Komisija razviti novo strategijo, pri čemer morajo upoštevati vsebino Konvencije Sveta Evrope o kibernetski kriminaliteti iz leta 2001. Navedena konvencija je referenčni pravni okvir za boj proti kibernetski kriminaliteti, vključno z napadi na informacijske sisteme. Ta direktiva nadgrajuje navedeno konvencijo.

(9) Glede na različne možne načine izvajanja napadov ter hiter razvoj programske in strojne opreme se ta direktiva sklicuje na „orodja“, ki se lahko uporabijo za storitev kaznivih dejanj iz te direktive. Orodja so lahko na primer zlonamerna programska oprema, vključno z botneti, ki se uporabljajo za kibernetske napade.

(10) Ta direktiva ni namenjena uvedbi kazenske odgovornosti, če so kazniva dejanja storjena nenaklepno, kot sta pooblaščeno preverjanje ali zaščita informacijskih sistemov.

(11) Ta direktiva krepi pomen mrež, kot sta mreža kontaktnih točk držav G8 ali Sveta Evrope, ki so dosegljive 24 ur na dan in sedem dni v tednu za izmenjavo informacij zaradi zagotavljanja takojšnje pomoči za preiskave ali postopke v zvezi s kaznivimi dejanji, povezanimi z informacijskimi sistemi in podatki, ali za zbiranje dokazov o kaznivem dejanju v elektronski obliki. Glede na hitrost, s katero je mogoče izvesti obsežne napade, morajo biti države članice sposobne zagotoviti hiter odziv na nujne zahteve te mreže kontaktnih točk. Ta pomoč mora vključevati spodbujanje ali neposredno izvajanje ukrepov, kot so: zagotavljanje tehničnega svetovanja, ohranjanje podatkov, zbiranje dokazov, zagotavljanje pravnih informacij in iskanje osumljencev.

(12) V skladu s to direktivo je treba zbirati podatke o kaznivih dejanjih, da se pridobi celostno podobo težave na ravni Unije in tako oblikuje učinkovitejše odzive. Poleg tega ti podatki specializiranim agencijam, kot sta Europol in Evropska agencija za varnost omrežij in informacij (ENISA), omogočajo boljšo oceno razširjenosti kibernetske kriminalitete ter stanja varnosti omrežij in informacij v Evropi.

(13) Velike vrzeli in razlike v zakonodaji držav članic na področju napadov na informacijske sisteme lahko ovirajo boj proti organiziranemu kriminalu in terorizmu ter otežijo učinkovito policijsko in pravosodno sodelovanje na tem področju. Sodobni

---

[18] UL L 300, 11.11.2008, str. 42.

informacijski sistemi so nadnacionalni in brezmejni, kar pomeni, da so napadi na takšne sisteme čezmejni, zato so dodatni ukrepi za približevanje kazenskega prava na tem področju nujni. Poleg tega mora sprejetje Okvirnega sklepa Sveta 2009/948/PNZ o preprečevanju in reševanju sporov o izvajanju pristojnosti v kazenskih postopkih olajšati usklajevanje pregona primerov napadov na informacijske sisteme.

(14) Ker ciljev te direktive, tj. zagotoviti, da so za napade na informacijske sisteme v vseh državah članicah predpisane učinkovite, sorazmerne in odvračilne kazni, ter izboljšati in spodbujati pravosodno sodelovanje z odpravo morebitnih zapletov, ne morejo zadovoljivo doseči države članice same, saj morajo biti pravila skupna in združljiva, ter jih je zato mogoče lažje doseči na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. Ta direktiva ne presega tistega, kar je potrebno za dosego teh ciljev.

(15) Osebne podatke, obdelane v okviru izvajanja te direktive, je treba varovati v skladu s pravili o varstvu podatkov iz Okvirnega sklepa Sveta 2008/977/PNZ z dne 27. novembra 2008 o varstvu osebnih podatkov, ki se obdelujejo v okviru policijskega in pravosodnega sodelovanja v kazenskih zadevah[19] v zvezi z obdelavo, ki spada na področje uporabe Direktive, ter Uredbo (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov[20].

(16) Ta direktiva spoštuje temeljne pravice in načela, ki jih priznava zlasti Listina Evropske unije o temeljnih pravicah, vključno z varstvom osebnih podatkov, pravicama do svobode izražanja in informiranja, pravico do pravičnega sojenja, načelom domneve nedolžnosti, pravico do obrambe ter tudi načeloma zakonitosti in sorazmernosti kaznivih dejanj in kazni. Namen te direktive je zlasti zagotovitev spoštovanja navedenih pravic in načel v celoti, pri čemer je Direktivo treba ustrezno izvajati.

(17) [V skladu s členi 1, 2, 3 in 4 Protokola o stališču Združenega kraljestva in Irske glede območja svobode, varnosti in pravice, ki je priložen Pogodbi o delovanju Evropske unije, sta Združeno kraljestvo in Irska uradno izrazila željo po sodelovanju pri sprejetju in uporabi te direktive] ALI [Ne glede na člen 4 Protokola o stališču Združenega kraljestva in Irske glede območja svobode, varnosti in pravice Združeno kraljestvo in Irska ne bosta sodelovala pri sprejetju te direktive, ki zato zanju ne bo zavezujoča in jima je ne bo treba uporabljati].

(18) V skladu s členoma 1 in 2 Protokola o stališču Danske, ki je priložen Pogodbi o delovanju Evropske unije, Danska ne sodeluje pri sprejetju te direktive, ki zato zanjo ni zavezujoča in se v njej ne uporablja –

SPREJELA NASLEDNJO DIREKTIVO:

Člen 1
Vsebina

Ta direktiva opredeljuje kazniva dejanja na področju napadov na informacijske sisteme in določa minimalna pravila glede kazni za taka dejanja. Namenjena je tudi uvedbi skupnih

[19] UL L 350, 30.12.2008, str. 60.
[20] UL L 8, 12.1.2001, str. 1.

določb za preprečevanje takih napadov in izboljšanje sodelovanja evropskega kazenskega pravosodja na tem področju.

Člen 2
Opredelitev pojmov

V tej direktivi 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 samodejno 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 informacijskemu sistemu omogoči, da opravi svojo nalogo;

(c) „pravna oseba“ pomeni vsak subjekt, ki ima status pravne osebe po veljavni zakonodaji, to pa niso države ali drugi javni organi, ki izvajajo javna pooblastila in javnih mednarodnih organizacij;

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

Člen 3
Nezakonit dostop do informacijskih sistemov

Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se namerni neupravičen dostop do celotnega ali katerega koli dela informacijskega sistema kaznuje kot kaznivo dejanje, vsaj v primerih, ki niso majhnega pomena.

Člen 4
Nezakonito poseganje v sisteme

Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se namerno resno oviranje ali prekinjanje delovanja informacijskega sistema z vnašanjem, prenašanjem, poškodovanjem, brisanjem, slabšanjem, spreminjanjem, preprečevanjem ali onemogočanjem dostopa do računalniških podatkov kaznuje kot kaznivo dejanje, če je storjeno neupravičeno, vsaj v primerih, ki niso majhnega pomena.

Člen 5
Nezakonito poseganje v podatke

Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se namerno brisanje, poškodovanje, slabšanje, spreminjanje računalniških podatkov v informacijskem sistemu ter preprečevanje ali onemogočanje dostopa do njih kaznuje kot kaznivo dejanje, če je storjeno neupravičeno, vsaj v primerih, ki niso majhnega pomena.

Člen 6

Nezakonito prestrezanje

Države članice sprejmejo potrebne ukrepe, da neupravičeno namerno prestrezanje zasebnih prenosov računalniških podatkov s tehničnimi sredstvi v informacijski sistem, iz ali znotraj njega, vključno z elektromagnetnimi emisijami iz informacijskega sistema, po katerih se taki računalniški podatki prenašajo, opredelijo za kaznivo dejanje.

Člen 7

Orodja, ki se uporabljajo za kazniva dejanja

Države članice sprejmejo potrebne ukrepe, da se za kaznivo dejanje opredelijo izdelava, prodaja, naročilo za uporabo, uvoz, distribucija ali drugo dajanje na voljo, če so storjeni naklepno in neupravičeno zaradi storitve kaznivih dejanj iz členov 3 do 6, in sicer naslednjih orodij:

(a) naprav, vključno z računalniškim programom, zasnovanim ali prilagojenim predvsem za namene storitve katerega koli kaznivega dejanja iz členov 3 do 6,

(b) računalniškega gesla, kode za dostop ali podobnih podatkov, s katerimi je mogoč dostop do celotnega informacijskega sistema ali katerega koli njegovega dela.

Člen 8

Napeljevanje, pomoč in podpiranje ter poskus

1. Države članice zagotovijo, da se napeljevanje k dejanjem iz členov 3 do 7, pomoč pri njihovi izvedbi in njihovo podpiranje kaznuje kot kaznivo dejanje.

2. Države članice zagotovijo, da se poskus storitve dejanj iz členov 3 do 6 kaznuje kot kaznivo dejanje.

Člen 9

Kazni

1. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da so za dejanja iz členov 3 do 8 predpisane učinkovite, sorazmerne in odvračilne kazni.

2. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da je za kazniva dejanja iz členov 3 do 7 najvišja zagrožena kazen najmanj dve leti zapora.

Člen 10

Obteževalne okoliščine

1. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da je za kazniva dejanja iz členov 3 do 7, če so bila storjena v okviru hudodelske združbe, kakor je opredeljena v Okvirnem sklepu 2008/841/PNZ, najvišja zagrožena kazen najmanj pet let zapora.

2. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da je za kazniva dejanja iz členov 3 do 6, če so bila storjena z orodjem, zasnovanim za izvajanje napadov, ki vplivajo na znatno število informacijskih sistemov, ali napadov, ki povzročijo znatno škodo, kot so motnje v sistemskih storitvah, finančni stroški ali izgube osebnih podatkov, najvišja zagrožena kazen najmanj pet let zapora.

3. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da je za dejanja iz členov 3 do 6, če so bila storjena s prikrito identiteto storilca in je oškodovan zakoniti lastnik identitete, najvišja zagrožena kazen najmanj pet let zapora.

Člen 11
Odgovornost pravnih oseb

1. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo odgovornost pravnih oseb za dejanja iz členov 3 do 8, ki jih je v njihovo korist, 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;

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

   (c) pristojnosti za opravljanje nadzora znotraj pravne osebe.

2. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo odgovornost pravne osebe, če je pomanjkljiv nadzor ali kontrola osebe iz odstavka 1 omogočila, da je oseba, ki je podrejena tej pravni osebi, v njeno korist storila katero koli kaznivo dejanje iz členov 3 do 8.

3. Odgovornost pravnih oseb iz odstavkov 1 in 2 ne izključuje kazenskih postopkov proti fizičnim osebam, ki so storilci ali sostorilci katerega koli kaznivega dejanja iz členov 3 do 8.

Člen 12
Kazni za pravne osebe

1. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da so za pravno osebo, odgovorno v skladu s členom 11(1), predpisane učinkovite, sorazmerne in odvračilne kazni, ki vključujejo denarne kazni po kazenskem ali drugem pravu, ter ki lahko vključujejo tudi naslednje kazni:

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

   (b) začasno ali stalno prepoved opravljanja poslovnih dejavnosti;

   (c) uvedbo sodnega nadzora;

   (d) sodno likvidacijo;

   (e) začasno ali trajno zaprtje poslovalnic, ki so bile uporabljene za storitev kaznivega dejanja.

2. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da so za pravno osebo, odgovorno v skladu s členom 11(2), predpisane učinkovite, sorazmerne in odvračilne kazni ali ukrepi.

Člen 13
Sodna pristojnost

1. Države članice imajo sodno pristojnost za kazniva dejanja iz členov 3 do 8, če:

   (a) so bila ta storjena na celotnem ozemlju zadevne države članice ali njenem delu ali

   (b) jih je storil njihov državljan ali oseba, ki ima običajno prebivališče na ozemlju zadevne države članice, ali

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

2. Pri ugotavljanju sodne pristojnosti v skladu z odstavkom (1)(a) države članice zagotovijo, da njihova sodna pristojnost vključuje primere, kadar:

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

   (b) gre za kaznivo dejanje zoper informacijski sistem na ozemlju zadevne države članice, ne glede na to, ali storilec stori kaznivo dejanje, ko je fizično prisoten na njenem ozemlju.

Člen 14
Izmenjava informacij

1. Zaradi izmenjave informacij o dejanjih iz členov 3 do 8 in v skladu s pravili o varstvu podatkov države članice uporabljajo obstoječo mrežo operativnih kontaktnih točk, ki so na voljo 24 ur na dan vse dni v tednu. Države članice tudi zagotovijo, da so vzpostavljeni postopki, ki omogočajo odziv na nujne zahteve najpozneje v osmih urah. Takšen odziv mora vključevati vsaj odgovor, ali bo zahtevi po pomoči ugodeno in v kakšni obliki ter kdaj.

2. Vsaka država članica obvesti Komisijo o svojih kontaktnih točkah, imenovanih za namene izmenjave informacij o kaznivih dejanjih iz členov 3 do 8. Komisija informacije pošlje drugim državam članicam.

Člen 15
Spremljanje in statistika

1. Države članice zagotovijo vzpostavitev sistema za beleženje, pripravo in predložitev statističnih podatkov o kaznivih dejanjih iz členov 3 do 8.

2. Statistični podatki iz odstavka 1 zajemajo vsaj število kaznivih dejanj iz členov 3 do 8, sporočenih državam članicam, in nadaljnje ukrepanje v zvezi s temi dejanji ter navajajo število preiskovanih primerov letno, število kazensko preganjanih oseb in število oseb, obsojenih za kazniva dejanj iz členov 3 do 8.

3. Države članice pošljejo Komisiji podatke, zbrane na podlagi tega člena. Te zagotovijo tudi objavo zbirnega pregleda teh statističnih poročil.

Člen 16
Razveljavitev Okvirnega sklepa 2005/222/PNZ

Okvirni sklep 2005/222/PNZ se razveljavi ne glede na obveznosti držav članic v zvezi z roki za prenos v nacionalno zakonodajo.

Sklicevanja na razveljavljeni Okvirni sklep se štejejo kot sklicevanja na to direktivo.

Člen 17
Prenos

1. Države članice sprejmejo in objavijo, najkasneje do [dve leti po sprejetju] zakone in druge predpise, potrebne za uskladitev s to direktivo. Komisijo takoj obvestijo o besedilu teh predpisov in o primerjalni tabeli med temi predpisi in to direktivo. Države članice se v sprejetih predpisih sklicujejo na to direktivo ali pa sklic nanjo navedejo ob njihovi uradni objavi. Način sklicevanja določijo države članice.

2. Države članice Komisijo obvestijo o besedilu temeljnih predpisov nacionalnega prava, ki jih sprejmejo na področju, ki ga ureja ta direktiva.

Člen 18
Poročanje

1. Komisija do [ŠTIRI LETA PO SPREJETJU] in vsaka tri leta za tem Evropskemu parlamentu in Svetu predloži poročilo o izvajanju te direktive v državah članicah, vključno z vsemi potrebnimi predlogi.

2. Države članice Komisiji pošljejo vse informacije, potrebne za pripravo poročila iz odstavka 1. Informacije vključujejo natančen opis zakonodajnih in nezakonodajnih ukrepov, sprejetih za izvajanje te direktive.

Člen 19
Začetek veljavnosti

Ta direktiva začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

Člen 20
Naslovniki

Ta direktiva je naslovljena na države članice v skladu s Pogodbama.

V Bruslju,

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*