DIREKTIVA 2013/40/EU EVROPSKEGA PARLAMENTA IN SVETA

z dne 12. avgusta 2013

o napadih na informacijske sisteme in nadomestitvi 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,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora ([1]),

v skladu z rednim zakonodajnim postopkom ([2]),

ob upoštevanju naslednjega:

(1) Cilji te direktive so z uvedbo minimalnih pravil glede opredelitve kaznivih dejanj in zadevnih sankcij na področju napadov na informacijske sisteme približati kazensko pravo držav članic ter izboljšati sodelovanje med pristojnimi organi, vključno s policijo in drugimi specializiranimi službami kazenskega pregona držav članic, pa tudi med pristojnimi specializiranimi agencijami in organi Unije, kot so Eurojust, Europol z evropskim centrom za kibernetski kriminal in Evropska agencija za varnost omrežij in informacij (ENISA).

(2) Informacijski sistemi so ključnega pomena za politično, družbeno in gospodarsko sodelovanje v Uniji. Družba je zelo in vedno bolj odvisna od tovrstnih sistemov. Nemoteno delovanje in varnost teh sistemov v Uniji sta bistvena za razvoj notranjega trga ter konkurenčnega in inovativnega gospodarstva. Zagotavljanje ustrezne ravni zaščite informacijskih sistemov bi moralo biti del učinkovitega celostnega okvira preventivnih ukrepov, ki spremljajo kazenskopravne ukrepe proti kibernetskemu kriminalu.

(3) Napadi na informacijske sisteme in zlasti napadi, povezani z organiziranim kriminalom, so vedno večja grožnja v Uniji in po svetu, vedno večja pa je tudi zaskrbljenost zaradi možnosti terorističnih ali politično motiviranih napadov na informacijske sisteme, ki so del kritične infrastrukture držav članic in Unije. To ogroža uresničevanje ciljev varnejše informacijske družbe ter območja svobode, varnosti in pravice, zato zahteva odziv na ravni Unije ter boljše sodelovanje in usklajevanje na mednarodni ravni.

(4) V Uniji je nekaj kritičnih infrastruktur, katerih okvara ali uničenje bi imela resne čezmejne posledice. Zahteva po povečanju zmogljivosti za zaščito kritične infrastrukture v Uniji kaže na to, da bi morali biti ukrepi proti kibernetskim napadom dopolnjeni s strogimi kaznimi, ki bi odražale resnost teh napadov. Kritično infrastrukturo bi se lahko razumelo kot zmogljivost, sistem ali njegov del, ki se nahaja v državah članicah in je bistven za vzdrževanje osnovnih družbenih funkcij, zdravja, varnosti, zaščite, gospodarske ali družbene blaginje ljudi, kot so elektrarne, prometna omrežja ter vladna omrežja, in katerega okvara ali uničenje bi imelo zaradi nezmožnosti vzdrževanja teh funkcij v državi članici resne posledice.

(5) Kažejo se težnje k vedno bolj nevarnim in ponavljajočim se obsežnim napadom na informacijske sisteme, ki so lahko pogosto ključni za države ali za posebne funkcije v javnem ali zasebnem sektorju. Te težnje spremlja razvoj vedno bolj izpopolnjenih metod, kot sta vzpostavitev in uporaba tako imenovanih „botnetov“, kar vključuje več faz kaznivega dejanja, pri čemer lahko vsaka faza zase močno ogrozi javni interes. V tej zvezi je namen te direktive tudi uvedba kazni za vzpostavitev „botneta“, in sicer ko je s ciljno usmerjenimi kibernetskimi napadi nad znatnim številom računalnikov vzpostavljen nadzor na daljavo in so ti okuženi z zlonamerno programsko opremo. Kasneje se okužena mreža računalnikov, ki sestavljajo „botnet“, lahko brez vednosti njihovih uporabnikov aktivira za kibernetski napad velikega obsega, ki je navadno zmožen povzročiti resno škodo, kakor je navedeno v tej direktivi. Države članice lahko v skladu s svojo nacionalno zakonodajo in prakso opredelijo, kaj pomeni resna škoda, kot je prekinitev sistemskih storitev velikega javnega pomena, povzročitev velikih finančnih stroškov ali izguba osebnih podatkov ali občutljivih informacij.

(6) Kibernetski napadi velikega obsega lahko povzročijo znatno gospodarsko škodo tako zaradi prekinitve delovanja informacijskih sistemov in komunikacij kot tudi zaradi izgube ali spremembe gospodarsko pomembnih zaupnih ali drugih podatkov. Posebno pozornost bi bilo treba nameniti ozaveščanju inovativnih malih in srednjih podjetij o grožnjah, povezanih s tovrstnimi napadi in njihova ranljivosti ob tovrstnih napadih, saj so ta vedno bolj odvisna od ustreznega delovanja in razpoložljivosti informacijskih sistemov in imajo pogosto omejena sredstva za informacijsko varnost.

([1]) UL C 218, 23.7.2011, str. 130.

([2]) Stališče Evropskega parlamenta z dne 4. julija 2013 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 22. julija 2013.

(7) Skupne opredelitve na tem področju so pomembne za zagotovitev skladnega pristopa v državah članicah k uporabi te direktive.

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

(9) Prestrezanje vključuje, vendar ni nujno omejeno na, poslušanje, spremljanje ali nadzor vsebine sporočil in pridobitev vsebine podatkov bodisi neposredno z dostopom v informacijski sistem in njegovo uporabo bodisi posredno z uporabo elektronskega prisluškovanja ali tehničnih naprav za prisluškovanje.

(10) Države članice bi morale določiti kazni za napade na informacijske sisteme. Te kazni bi morale biti učinkovite, sorazmerne in odvračilne ter vključevati zaporno in/ali denarne kazni.

(11) Ta direktiva določa kazni vsaj za primere, ki niso majhnega pomena. Države članice lahko v skladu s svojim nacionalnim pravom in prakso določijo, kaj je primer majhnega pomena. Posamezni primer lahko šteje za primer majhnega pomena, kadar sta škoda, ki jo povzroči dejanje, in/ali tveganje za javni ali zasebni interes, kot so integriteta računalniškega sistema ali računalniških podatkov ali integriteta, pravice ali drugi interesi posameznika, zanemarljiva ali takšna, da naložitev kazni v okviru zakonskega praga ali uvedba kazenske odgovornosti nista potrebna.

(12) Identifikacija ter prijava groženj in tveganj, ki jih povzročijo kibernetski napadi, ter s tem povezana ranljivost informacijskih sistemov so pomembni element za učinkovito preprečevanje kibernetskih napadov in odzivanja nanje ter izboljšanja varnosti informacijskih sistemov. K temu bi lahko prispevale tudi spodbude za prijavo varnostnih vrzeli. Države članice bi si morale prizadevati, da zagotovijo možnosti za zakonito odkrivanje in prijavo varnostnih vrzeli.

(13) Ustrezno 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 ([1]), kadar je napad obsežen in zato prizadene znatno število informacijskih sistemov, tudi kadar je namen napada ustvariti „botnet“ali kadar kibernetski napad povzroči resno škodo, tudi kadar se napad izvede prek „botneta“. Ustrezno je predvideti tudi strožje kazni za primere, ko gre za napad na kritično infrastrukturo držav članic ali Unije.

([1]) UL L 300, 11.11.2008, str. 42.

(14) Vzpostavitev učinkovitih ukrepov proti kraji identitete in drugim kaznivim dejanjem, povezanim z identiteto, je prav tako pomemben element celovitega pristopa k boju proti kibernetski kriminaliteti. Pri ocenjevanju potrebe po celovitem horizontalnem instrumentu Unije bi lahko razmislili tudi o morebitni potrebi po ukrepu na ravni Unije proti tovrstnim kaznivim dejanjem.

(15) Iz Sklepov Sveta z dne 27. do 28. novembra 2008 izhaja, da bi morale države članice in Komisija oblikovati novo strategijo, pri tem pa upoštevati vsebino Konvencije Sveta Evrope o kibernetski kriminaliteti iz leta 2001. Ta konvencija je referenčni pravni okvir za boj proti kibernetski kriminaliteti, vključno z napadi na informacijske sisteme. Ta direktiva nadgrajuje to konvencijo. Vse države članice bi morale prednostno in čim prej zaključiti postopek ratifikacije te konvencije.

(16) Glede na različne možne načine izvajanja napadov ter hiter razvoj strojne in programske opreme se ta direktiva sklicuje na „orodja“, ki se lahko uporabijo za storitev kaznivih dejanj, določenih v tej direktivi. Tovrstna orodja bi lahko vključevala zlonamerna programska oprema, vključno s tisto, s katero se lahko ustvarijo „botneti“, ki se uporabljajo za kibernetske napade. Tudi kadar so tovrstna orodja primerna ali še posebej primerna za storitev enega od kaznivih dejanj, določenih v tej direktivi, so bila morda izdelana za zakonit namen. Z namenom, da se izogne kriminalizaciji, kadar so bila tovrstna orodja proizvedena in dana na trg za zakonite namene, kot je preverjanje zanesljivosti produktov informacijske tehnologije ali varnosti informacijskih sistemov, v takem primeru ni dovolj, da ima oseba splošni naklep, ampak mora imeti neposreden naklep, da se ta orodja uporabijo za storitev enega ali več od kaznivih dejanj, določenih v tej direktivi.

(17) Ta direktiva ne uvaja kazenske odgovornosti, kadar so izpolnjene objektivna merila kaznivih dejanj, določenih v tej direktivi, vendar dejanja niso storjena naklepno, na primer, če oseba ne ve, da dostop ni dovoljen, ali v primeru pooblaščenega preverjanja ali zaščite informacijskih sistemov, na primer kadar podjetje ali prodajalec osebi naloži, naj preveri odpornost varnostnega sistema. V okviru te direktive pogodbene obveznosti ali dogovori za omejitev dostopa do informacijskih sistemov s pogoji uporabe ali pogoji opravljanja storitve, kakor tudi delovni spori v zvezi z dostopom do informacijskih sistemov delodajalca in njihovo uporabo v zasebne namene, ne povzročijo kazenske odgovornosti, kadar bi se dostop pod takšnimi pogoji štel za nepooblaščenega in bi to pomenilo edino podlago za sodni postopek. Ta direktiva ne posega v pravico dostopa do informacij, kot je določena v nacionalnem pravu in pravu Unije, hkrati pa ne sme služiti kot opravičilo za nezakonit ali arbitraren dostop do informacij.

(18) Kibernetski napad lahko olajšajo različne okoliščine, na primer kadar ima storilec dostop do varnostnih sistemov, ki so del prizadetih informacijskih sistemov v okviru svoje zaposlitve. Take okoliščine bi bilo treba - kot je primerno - v okviru nacionalnega prava ustrezno upoštevati v sodnih postopkih.

(19) Države članice bi morale v skladu z veljavnimi predpisi v zvezi z obteževalnimi okoliščinami, določenimi v njihovem pravnem sistemu, v svojem nacionalnem pravu predvideti obteževalne okoliščine. Zagotoviti bi morale, da lahko sodniki te obteževalne okoliščine upoštevajo ob izrekanju kazni storilcem kaznivih dejanj. Sodnik ohrani diskrecijsko pravico, da te okoliščine presodi skupaj z drugimi dejstvi v konkretnem primeru.

(20) Ta direktiva ne ureja pogojev za izvrševanje sodno pristojnost za katero koli v njej navedeno kaznivo dejanje, kot je prijava, ki jo opravi žrtev v kraju, kjer je bilo kaznivo dejanje storjeno, prijava, ki jo opravi država, v kateri je bilo kaznivo dejanje storjeno, ali dejstvo, da storilec ni bil sodno preganjan v kraju, kjer je bilo kaznivo dejanje storjeno.

(21) V okviru te direktive so države ter javni organi še naprej polno zavezani, da v skladu z obstoječimi mednarodnimi obveznostmi zagotavljajo spoštovanje človekovih pravic in temeljnih svoboščin.

(22) Ta direktiva krepi pomen mrež, kot sta mreža kontaktnih točk držav G8 ali Sveta Evrope, ki so dosegljive 24 ur na dan in vse dni v tednu. Te kontaktne točke bi morale biti zmožne zagotavljati učinkovito pomoč in tako olajšati na primer izmenjavo razpoložljivih zadevnih informacij in zagotavljanje tehničnih nasvetov ali pravnih informacij za preiskave ali postopke v zvezi s kaznivimi dejanji, povezanimi z informacijskimi sistemi in zadevnimi podatki, ki zadevajo državo članico prosilko. Da se zagotovi nemoteno delovanje omrežij, bi morala vsaka kontaktna točka imeti zmožnost, da po pospešenem postopku komunicira s kontaktno točko druge države članice, pri čemer bi imela med drugim na voljo usposobljeno osebje in ustrezno opremo. Glede na hitrost, s katero je mogoče izvesti kibernetske napade velikega obsega, bi morale biti države članice sposobne zagotoviti hiter odziv na nujne zahtevke te mreže kontaktnih točk. V takih primerih bi bilo morda smiselno, da se v zahtevku za informacije navede telefonski kontakt, da lahko zaprošena država članica zahtevek hitro obravnava in v osmih urah tudi odgovori.

(23) Sodelovanje javnih organov na eni z zasebnim sektorjem in s civilno družbo na drugi strani je velikega pomena pri preprečevanju napadov na informacijske sisteme in boju proti njim. Treba je spodbujati in izboljšati sodelovanje med ponudniki storitev, proizvajalci, organi pregona in sodnimi organi, pri tem pa dosledno spoštovati načelo pravne države. Tovrstno sodelovanje lahko vključuje pomoč ponudnikov storitev v smislu ohranjanja morebitnih dokazov, zagotavljanja elementov, ki omogočajo prepoznavanje storilcev, ter, kot zadnjo možnost, popolne ali delne prekinitve delovanja informacijskih sistemov ali funkcij, ki so bili ogroženi ali uporabljeni v nezakonite namene, v skladu z nacionalnim pravom in prakso. Države članice bi morale razmisliti tudi o vzpostavitvi omrežij za sodelovanje in partnerstvo s ponudniki storitev in proizvajalci za namene izmenjave informacij o kaznivih dejanjih, ki spadajo v področje uporabe te direktive.

(24) Treba je zbrati primerljive podatke o kaznivih dejanjih, določenih v tej direktivi. Zadevne podatke bi bilo treba dati na voljo pristojnim specializiranim agencijam in organom Unije, kot sta Europol in ENISA, v skladu z njihovimi nalogami in informacijskimi potrebami, da bi dobili jasnejšo sliko problema kibernetske kriminalitete ter varnosti omrežij in informacij na ravni Unije in tako prispevali k oblikovanju učinkovitejšega odziva. Države članice bi morale Europolu in njegovemu evropskemu centru za kibernetski kriminal posredovati informacije o načinu delovanja storilcev, da bi se lahko izvedla ocena nevarnosti in strateška analiza kibernetske kriminalitete v skladu s Sklepom Sveta 2009/371/PNZ z dne 6. aprila 2009 o ustanovitvi Evropskega policijskega urada (Europol) ([1]). Zagotavljanje informacij lahko pripomore k boljšemu razumevanju sedanjih in prihodnjih groženj in tako prispeva k ustreznejšemu in ciljnemu odločanju o preprečevanju napadov na informacijske sisteme in boju proti njim.

(25) Komisija bi morala predložiti poročilo o uporabi te direktive in potrebne zakonodajne predloge, ki bi lahko razširili področje njene uporabe, pri tem pa upoštevati razvoj na področju kibernetske kriminalitete. Tovrsten razvoj bi lahko pomenil kakršen koli tehnološki razvoj, ki bi omogočil na primer učinkovitejši pregon napadov na informacijske sisteme ali lajšal preprečevanje oziroma blažil učinke takih napadov. V ta namen bi morala Komisija upoštevati razpoložljive analize in poročila zadevnih akterjev, zlasti Europola in ENISA.

(26) Za učinkovit boj proti kibernetski kriminaliteti je treba sprejeti ustrezne ukrepe za izboljšanje odpornosti informacijskih sistemov, da se jih učinkoviteje zaščiti pred kibernetskimi napadi. Države članice bi morale sprejeti potrebne ukrepe za zaščito informacijskih sistemov, ki so del njihove kritične infrastrukture pred kibernetskimi napadi, v okviru katerih bi morale razmisliti o zaščiti svojih informacijskih sistemov in s tem povezanih podatkov. Bistveni element celovitega pristopa k učinkovitemu

([1]) UL L 121, 15.5.2009, str. 37.

boju proti kibernetski kriminaliteti je tudi zagotavljanje ustrezne ravni zaščite in varnosti informacijskih sistemov s strani pravnih oseb, na primer pri zagotavljanju javno dostopnih elektronskih komunikacijskih storitev v skladu z veljavno zakonodajo Unije o zasebnosti in elektronskih komunikacijah ter varstvu podatkov. Proti razumno opredeljivim grožnjam in ranljivostim bi bilo treba zagotoviti ustrezne ravni zaščite, v skladu z najsodobnejšo tehnologijo za posamezne sektorje in konkretnimi okoliščinami obdelave podatkov. Stroški in breme take zaščite bi morali biti sorazmerni z verjetno škodo, ki bi jo prizadetim povzročil kibernetski napad. Države članice se spodbuja, da v okviru nacionalnega prava določijo ustrezne ukrepe, ki vključujejo odgovornost v primerih, ko pravna oseba očitno ne zagotovi ustrezne ravni zaščite pred kibernetskimi napadi.

(27) Velike vrzeli in razlike v zakonodaji in kazenskih postopkih 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. Nadnacionalna in brezmejna narava sodobnih informacijskih sistemov pomeni, da imajo napadi na takšne sisteme čezmejno razsežnost, zato so dodatni ukrepi za približevanje kazenskega prava na tem področju nujni. Dodatno bi moralo ustrezno izvajanje in uporaba Okvirnega sklepa Sveta 2009/948/PNZ z dne 30. novembra 2009 o preprečevanju in reševanju sporov o izvajanju pristojnosti v kazenskih postopkih [1] olajšati usklajevanje pregona primerov napadov na informacijske sisteme. Države članice bi si morale v sodelovanju z Unijo prizadevati tudi za izboljšanje mednarodnega sodelovanja v zvezi z varnostjo informacijskih sistemov, računalniških omrežij in računalniških podatkov. V vsakem mednarodnem dogovoru, ki vključuje izmenjavo podatkov, bi bilo treba ustrezno pozornost nameniti varnosti prenosa in hrambe podatkov.

(28) Izboljšano sodelovanje med pristojnimi organi kazenskega pregona in sodnimi organi v Uniji je bistvenega pomena za učinkovit boj proti kibernetski kriminaliteti. V tem okviru bi bilo treba spodbujati odločnejša prizadevanja, da se pristojnim organom zagotovi ustrezno usposabljanje, da bi izboljšali razumevanje kibernetske kriminalitete in njenih učinkov ter spodbudili sodelovanje in izmenjavo najboljših praks, na primer prek pristojnih specializiranih agencij in organov Unije. Tovrstno usposabljanje bi moralo med drugim biti namenjeno ozaveščanju o različnih nacionalnih pravnih sistemih, o morebitnih pravnih in o tehničnih izzivih v okviru kazenskih preiskav ter razdelitvi pristojnosti med zadevnimi nacionalnimi organi.

(29) Ta direktiva zagotavlja spoštovanje človekovih pravic in temeljnih svoboščin ter načel, ki jih priznavata zlasti Listina Evropske unije o temeljnih pravicah ter Evropska konvencija o varstvu človekovih pravic in temeljnih svoboščin, vključno z varstvom osebnih podatkov, pravico do zasebnosti, 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 zagotoviti dosledno spoštovanje navedenih pravic in načel, zato jo je treba ustrezno izvajati.

(30) Varstvo osebnih podatkov je temeljna pravica v skladu s členom 16(1) PDEU in členom 8 Listine Evropske unije o temeljnih pravicah. Zato bi morala biti vsaka obdelava osebnih podatkov v okviru izvajanja te direktive povsem v skladu z zadevnim pravom Unije o varstvu podatkov.

(31) V skladu s členom 3 Protokola o stališču Združenega kraljestva in Irske glede območja svobode, varnosti in pravice, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije, sta obe državi članici podali uradno obvestilo, da želita sodelovati pri sprejetju in uporabi te direktive.

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

(33) Ker ciljev te direktive, in sicer zagotoviti, da so za napade na informacijske sisteme v vseh državah članicah predpisane učinkovite, sorazmerne in odvračilne kazni, ter izboljšati in spodbujati pravosodno sodelovanje, države članice ne morejo zadovoljivo doseči in ker se te cilje lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta direktiva ne presega tistega, kar je potrebno za doseganje navedenih ciljev.

(34) Namen te direktive je spremeniti in razširiti določbe Okvirnega sklepa Sveta 2005/222/PNZ z dne 24. februarja 2005 o napadih na informacijske sisteme [2]. Ker so spremembe vsebinske in jih je veliko, bi bilo treba za tiste države članice, ki sodelujejo pri sprejetju te direktive, Okvirni sklep 2005/222/PNZ zaradi jasnosti v celoti nadomestiti –

[1] UL L 328, 15.12.2009, str. 42.

[2] UL L 69, 16.3.2005, str. 67.

SPREJELA NASLEDNJO DIREKTIVO:

Člen 1

Predmet urejanja

Ta direktiva določa minimalna pravila glede opredelitve kaznivih dejanj in sankcije na področju napadov na informacijske sisteme. Poleg tega je njen cilj preprečiti taka dejanja in izboljšati sodelovanje med pravosodnimi in drugimi pristojnimi organi.

Člen 2

Opredelitev pojmov

Za namene te direktive se uporabljajo naslednje opredelitve pojmov:

(a) „informacijski sistem“ pomeni 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, pridobljeni ali se po tej napravi ali skupini naprav prenašajo zaradi njenega ali njihovega delovanja, uporabe, varovanja in vzdrževanja;

(b) „računalniški podatki“ pomeni predstavitev dejstev, informacij ali konceptov v obliki, primerni za obdelavo v informacijskem sistemu, vključno s programom, ki lahko informacijskemu sistemu omogoči, da opravlja svojo funkcijo;

(c) „pravna oseba“ pomeni subjekt, ki ima status pravne osebe po veljavni zakonodaji, vendar ne vključuje držav članic, tretjih držav ali drugih javnih organov, ki izvajajo javna pooblastila, ali javnih mednarodnih organizacij;

(d) „neupravičeno“ pomeni ravnanje iz te direktive, vključno z dostopom, poseganjem ali prestrezanjem, ki ga ni odobril lastnik ali drugi imetnik pravice do sistema ali dela sistema, ali ki ni dovoljeno po nacionalnem pravu.

Člen 3

Nezakonit dostop do informacijskih sistemov

Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se v primeru naklepnega ravnanja neupravičen dostop do celotnega informacijskega sistema ali katerega koli njegovega dela kaznuje kot kaznivo dejanje, kadar je to storjeno s kršitvijo varnostnega ukrepa, vsaj v primerih, ki niso majhnega pomena.

Člen 4

Nezakonito poseganje v sistem

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

Člen 5

Nezakonito poseganje v podatke

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

Člen 6

Nezakonito prestrezanje

Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se naklepno in neupravičeno tehnično prestrezanje zasebnih prenosov računalniških podatkov v informacijski sistem, iz ali znotraj njega, vključno z elektromagnetnimi emisijami iz informacijskega sistema, po katerih se taki računalniški podatki prenašajo, kaznuje kot kaznivo dejanje, vsaj v primerih, ki niso majhnega pomena.

Člen 7

Orodja, ki se uporabljajo za izvedbo kaznivih dejanj

Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se kaznuje kot kaznivo dejanje vsaj v primerih, ki niso majhnega pomena, naklepna izdelava, prodaja, naročilo za uporabo, uvoz, distribucija ali drugo dajanje na voljo enega od navedenih orodij, če je storjeno neupravičeno in z namenom, da se uporabi za katero koli kaznivo dejanje iz členov 3 do 6:

(a) računalniški program, zasnovan ali prilagojen predvsem za namene storitve katerega koli kaznivega dejanja iz členov 3 do 6;

(b) računalniško geslo, koda za dostop ali podobni podatki, s katerimi je mogoč dostop do celotnega informacijskega sistema ali katerega koli njegovega dela.

Člen 8

Spodbujanje, pomoč in podpiranje ter poskus

1. Države članice zagotovijo, da se spodbujanje k, ali pomoč in podpiranje storitve kaznivega dejanja iz členov 3 do 7 kaznuje kot kaznivo dejanje.

2. Države članice zagotovijo, da se poskus storitve kaznivega dejanja iz členov 4 in 5 kaznuje kot kaznivo dejanje.

Člen 9

Kazni

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

2. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se kazniva dejanja iz členov 3 do 7 kaznujejo z najvišjo zaporno kaznijo najmanj dveh let, vsaj za primere, ki niso majhnega pomena.

3. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se kazniva dejanja iz členov 4 in 5 kaznujejo z najvišjo zaporno kaznijo najmanj treh let, če so bila storjena

naklepno in prizadenejo znatno število informacijskih sistemov z uporabo orodja iz člena 7, zasnovanega ali prilagojenega predvsem za ta namen.

4. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se kazniva dejanja iz členov 4 in 5 kaznujejo z najvišjo zaporno kaznijo najmanj pet let, kadar:

(a) so storjena v okviru hudodelske združbe, kot je opredeljena v Okvirnem sklepu 2008/841/PNZ, ne glede na višino kazni, navedeno v Okvirnem sklepu;

(b) povzročijo resno škodo, ali

(c) so storjena nad informacijskim sistemom kritične infrastrukture.

5. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da se v primeru kaznivih dejanj iz členov 4 in 5, ki so storjena z zlorabo osebnih podatkov druge osebe z namenom, da se pridobi zaupanje tretje osebe, in oškoduje zakoniti lastnik identitete, lahko to v skladu z zadevnimi določbami nacionalnega prava šteje za obteževalne okoliščine, razen če so te okoliščine že zajete v drugem kaznivem dejanju, ki se kaznuje na podlagi nacionalnega prava.

Člen 10

Odgovornost pravnih oseb

1. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da so lahko pravne osebe odgovorne za kazniva 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, in sicer na podlagi:

(a) pooblastila 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, da so lahko pravne osebe odgovorne, če je oseba iz odstavka 1 s pomanjkljivim nadzorom ali kontrolo 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, napeljevalci ali sostorilci katerega koli kaznivega dejanja iz členov 3 do 8.

Člen 11

Sankcije za pravne osebe

1. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da so za pravno osebo, odgovorno v skladu s členom 10(1), predpisane učinkovite, sorazmerne in odvračilne sankcije, ki vključujejo denarne kazni po kazenskem ali drugem pravu, in lahko vključujejo tudi drugačne sankcije, kot so:

(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 10(2), predpisane učinkovite, sorazmerne in odvračilne sankcije ali drugi ukrepi.

Člen 12

Sodna pristojnost

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

(a) so bila ta v celoti ali delno storjena na njihovem ozemlju, ali

(b) jih je storil eden od njihovih državljanov, vsaj v primerih, kadar dejanje velja za kaznivo dejanje na kraju, kjer je bilo storjeno.

2. Pri ugotavljanju sodne pristojnosti v skladu s točko (a) odstavka 1 država članica zagotovi, da ima sodno pristojnost, kadar:

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

3. Država članica obvesti Komisijo, če se odloči, da bo uveljavila pristojnost za kaznivo dejanje iz členov 3 do 8, storjeno zunaj njenega ozemlja, vključno kadar:

(a) ima storilec običajno prebivališče na njenem ozemlju, ali

(b) je kaznivo dejanje storjeno v korist pravne osebe s sedežem na njenem ozemlju.

Člen 13

Izmenjava informacij

1. Za namene izmenjave informacij o kaznivih dejanjih iz členov 3 do 8 države članice zagotovijo, da imajo delujočo nacionalno kontaktno točko, in uporabljajo obstoječo mrežo operativnih kontaktnih točk, ki so na voljo 24 ur na dan in vse dni v tednu. Države članice tudi zagotovijo, da so vzpostavljeni postopki, da lahko v primeru nujnih zahtevkov za pomoč, lahko pristojni organ v največ osmih urah po prejemu navede vsaj, ali bo na zahtevo za pomoč odgovoril, ter v kakšni obliki in predvidoma v kolikšnem času.

2. Države članice obvestijo Komisijo o svojih kontaktnih točkah iz odstavka 1. Komisija informacijo posreduje drugim državam članicam ter pristojnim specializiranim agencijam in organom Unije.

3. Države članice sprejmejo potrebne ukrepe, s katerimi zagotovijo, da so na voljo ustrezni kanali za prijavo, ki olajšajo pravočasno prijavo kaznivih dejanj iz členov 3 do 6 pristojnim nacionalnim organom.

Člen 14

Spremljanje in statistika

1. Države članice zagotovijo, da je vzpostavljen sistem za beleženje, pripravo in predložitev statističnih podatkov o kaznivih dejanjih iz členov 3 do 7.

2. Statistični podatki iz odstavka 1 zajemajo vsaj obstoječe podatke o številu kaznivih dejanj iz členov 3 do 7, ki so jih evidentirale države članice, in številu oseb, ki so bile zaradi storitve kaznivih dejanj iz členov 3 do 7 sodno preganjane in obsojene.

3. Države članice pošljejo Komisiji podatke, zbrane na podlagi tega člena. Komisija zagotovi objavo zbirnega pregleda teh statističnih poročil in ga predloži pristojnim specializiranim agencijam in organom Unije.

Člen 15

Nadomestitev Okvirnega sklepa 2005/222/PNZ

Okvirni sklep 2005/222/PNZ se nadomesti za države članice, ki sodelujejo pri sprejetju te direktive, ne glede na obveznosti držav članic v zvezi z rokom za prenos Okvirnega sklepa v nacionalno zakonodajo.

V zvezi z državami članicami, ki sodelujejo pri sprejetju te direktive, se sklicevanja na Okvirni sklep 2005/222/PNZ štejejo kot sklicevanja na to direktivo.

Člen 16

Prenos

1. Države članice najpozneje do 4. septembra 2015 sprejmejo zakone in druge predpise, potrebne za uskladitev s to direktivo.

2. Države članice Komisiji predložijo besedilo ukrepov, ki v njihovo nacionalno zakonodajo prenašajo obveznosti iz te direktive.

3. Ko države članice sprejmejo navedene ukrepe, se sklicujejo na to direktivo ali pa ta sklic navedejo ob njihovi uradni objavi. Način sklicevanja določijo države članice.

Člen 17

Poročanje

Komisija do 4. septembra 2017 Evropskemu parlamentu in Svetu predloži poročilo, v katerem oceni, v kolikšni meri so države članice sprejele potrebne ukrepe za uskladitev s to direktivo, ter po potrebi priloži zakonodajne predloge. Komisija upošteva tudi tehnični in pravni razvoj na področju kibernetske kriminalitete, zlasti glede na področje uporabe te direktive.

Člen 18

Začetek veljavnosti

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

Člen 19

Naslovniki

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

V Bruslju, 12. avgusta 2013

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*
M. SCHULZ	L. LINKEVIČIUS