

SL

SL

SL



KOMISIJA EVROPSKIH SKUPNOSTI

Bruselj, 30.3.2009
COM(2009) 149 konč.

**SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU
EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ**

o zaščiti kritične informacijske infrastrukture

**„Kako zaščititi Evropo pred obsežnimi kibernetскими napadi in prekinitvami: izboljšati
pripravljenost, varnost in odpornost“**

{SEC(2009) 399}

{SEC(2009) 400}

(predložila Komisija)

SPOROČILO KOMISIJE EVROPSKEMU PARLAMENTU, SVETU, EVROPSKEMU EKONOMSKO-SOCIALNEMU ODBORU IN ODBORU REGIJ

o zaščiti kritične informacijske infrastrukture

„Kako zaščititi Evropo pred obsežnimi kibernetскими napadi in prekinitvami: izboljšati pripravljenost, varnost in odpornost“

1. Uvod

Informacijske in komunikacijske tehnologije (IKT) so vedno tesneje povezane z našimi vsakodnevnimi dejavnostmi. Nekateri od teh sistemov, storitev, omrežij in infrastruktur IKT (na kratko: infrastrukture IKT) so pomemben del evropskega gospodarstva in družbe, saj zagotavljajo osnovno blago in storitve oziroma so osnova za druge kritične infrastrukture. Običajno se štejejo za kritične informacijske infrastrukture (KII)¹, ker bi prekinitve njihovega delovanja ali njihovo uničenje resno vplivalo na pomembne družbene funkcije. Med zadnje primere spadajo obsežni kibernetски napadi na Estonijo leta 2007 in pretrganje čezcelinskih kablov leta 2008.

Svetovni gospodarski forum je leta 2008 ocenil, da obstaja 10- do 20-odstotna verjetnost večje okvare KII v naslednjih desetih letih, ki bi na svetovni ravni lahko povzročila gospodarske stroške v višini približno 250 milijard USD².

V tem sporočilu so poudarjeni preprečevanje, pripravljenost in ozaveščenost ter opredeljen je načrt za takojšnje ukrepe za krepitev varnosti in odpornosti KII. Ta poudarek je v skladu z razpravo, ki se je začela na zahtevo Sveta in Evropskega parlamenta, da bi se obravnavali izzivi in prednostne naloge politike varnosti omrežij in informacij (VOI) ter najprimernejši instrumenti, ki so potrebni na ravni EU za njihovo reševanje. Predlagani ukrepi dopolnjujejo tudi ukrepe za preprečevanje in boj proti kriminalnim in terorističnim dejavnostim, usmerjenim v KII, ter njihov pregon in so v sinergiji s trenutnimi in možnimi prihodnjimi raziskovalnimi prizadevanji EU na področju varnosti omrežij in informacij kot tudi z mednarodnimi pobudami na tem področju.

2. OZADJE POLITIKE

V tem sporočilu je oblikovana evropska politika za krepitev varnosti informacijske družbe in zaupanja vanjo. Komisija³ je že leta 2005 poudarila nujno potrebo po uskladitvi prizadevanj, da bi se ustvarilo zaupanje zainteresiranih strani v elektronske komunikacije in storitve. V ta namen je bila leta 2006 sprejeta strategija za varno informacijsko družbo⁴. Glavni elementi te strategije, vključno z varnostjo in odpornostjo infrastruktur IKT, so bili potrjeni v Resoluciji

¹ Opredelitev pojma KII je bila predlagana v COM(2005) 576 konč.

² *Global Risks 2008*.

³ COM(2005) 229.

⁴ COM(2006) 251.

Sveta 2007/068/01. Vendar se zdi, da sta lastništvo in izvajanje s strani zainteresiranih strani nezadovoljiva. Ta strategija je na taktični in operativni ravni tudi okrepila vlogo Evropske agencije za varnost omrežij in informacij (ENISA), ki je bila ustanovljena leta 2004, da bi prispevala k ciljem zagotovitve visoke in učinkovite stopnje VOI v Skupnosti ter razvoja kulture VOI v korist državljanzov, potrošnikov, podjetij in uprav EU.

Leta 2008 je bil mandat ENISA brez sprememb podaljšan do marca 2012⁵. Hkrati sta Svet in Evropski parlament zahtevala „*nadaljevanje razprave o prihodnosti ENISA ter o splošni usmeritvi evropskih prizadevanj za povečanje varnosti omrežij in informacij*“. V podporo tej razpravi je Komisija novembra lani začela javno spletno posvetovanje⁶, katerega analiza bo v kratkem na voljo.

Dejavnosti, ki se načrtujejo v tem sporočilu, se izvajajo v okviru evropskega programa za varovanje kritične infrastrukture (EPVKI)⁷ in vzporedno z njim. Ključni element EPVKI je direktiva⁸ o ugotavljanju in določanju evropske kritične infrastrukture⁹, ki opredeljuje sektor IKT kot prihodnji prednostni sektor. Drugi pomembni element EPVKI je informacijsko omrežje za opozarjanje o ključni infrastrukturi (CIWIN)¹⁰.

V regulativnem smislu vsebuje predlog Komisije o reformi regulativnega okvira za elektronska komunikacijska omrežja in storitve¹¹ nove določbe glede varnosti in celovitosti, predvsem da bi se okrepile obveznosti upravljavcev ter tako zagotovilo sprejetje ustreznih ukrepov za odpravljanje znanih tveganj, neprekinjeno opravljanje storitev in prijavljanje kršitev varnosti¹². Ta pristop prispeva k splošnemu cilju izboljšanja varnosti in odpornosti KII. Evropski parlament in Svet močno podpirata te določbe.

V tem sporočilu predlagani ukrepi dopolnjujejo obstoječe in možne prihodnje ukrepe na področju policijskega in pravosodnega sodelovanja zaradi preprečevanja in boja proti kriminalnim in terorističnim dejavnostim, usmerjenim v KII, ter njihovega pregona, kot je med drugim predvideno v okvirnem sklepu Sveta o napadih na informacijske sisteme¹³ in načrtovani posodobitvi tega sklepa¹⁴.

Ta pobuda upošteva dejavnosti NATO v zvezi s skupno politiko o kibernetiski obrambi v okviru Urada za upravljanje kibernetске obrambe in Centra odličnosti za sodelovanje pri kibernetiski obrambi.

Poleg tega se ustrezno upošteva tudi razvoj mednarodne politike, zlasti načela G8 o VKII¹⁵, Resolucija Generalne skupščine Združenih narodov 58/199 o vzpostavitvi svetovne kulture kibernetске varnosti in zaščiti ključnih informacijskih infrastruktur ter nedavno sprejeto priporočilo OECD glede varovanja kritičnih informacijskih infrastruktur.

⁵ Uredba (ES) št. 1007/2008.

⁶ http://ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=4464.

⁷ COM(2006) 786 konč.

⁸ 2008/114/ES.

⁹ http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/gena/104617.pdf.

¹⁰ COM(2008) 676 konč.

¹¹ COM(2007) 697, COM(2007) 698, COM(2007) 699.

¹² Člen 13 okvirne direktive.

¹³ 2005/222/PNZ.

¹⁴ COM(2008) 712.

¹⁵ http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf.

3. ZA KAJ PRAVZAPRAV GRE

3.1. Kritične informacijske infrastrukture so bistvene za gospodarsko in družbeno rast EU

Gospodarska in družbena vloga sektorja IKT in infrastruktur IKT je poudarjena v najnovejših poročilih o inovacijah in gospodarski rasti. Sem spadajo sporočilo o vmesnem pregledu strategije i2010¹⁶, poročilo skupine Aho¹⁷ in letna gospodarska poročila Evropske unije¹⁸. OECD poudarja pomen IKT in interneta „za povečanje gospodarske storilnosti in družbene blaginje ter krepitev storilnosti družb, da bi se izboljšala kakovost življenja državljanov po vsem svetu“¹⁹. Poleg tega priporoča sprejetje politik za povečanje zaupanja v internetno infrastrukturo.

Sektor IKT je bistven za vse segmente družbe. Podjetja so odvisna od sektorja IKT tako pri sami prodaji, kot tudi pri učinkovitosti notranjih postopkov. IKT predstavljajo pomemben element inovacij in so zaslužne za skoraj 40 % rasti proizvodnje²⁰. Poleg tega imajo vedno pomembnejšo vlogo tudi pri delu vlad in javnih uprav: zaradi uvedbe storitev e-vlade na vseh ravneh ter novih aplikacij, kot so inovativne rešitve v zvezi z zdravjem, energijo in politično udeležbo, je javni sektor močno odvisen od IKT. Nenazadnje pa se tudi državljani vedno bolj zanašajo na IKT in jih uporabljajo pri svojih vsakodnevni dejavnostih: okrepitev varnosti KII bi povečala zaupanje državljanov v IKT, med drugim tudi zaradi boljšega varovanja osebnih podatkov in zasebnosti.

3.2. Tveganja za kritične informacijske infrastrukture

Tveganja, povezana z napadi, ki jih povzroči človek, naravnimi nesrečami ali tehničnimi okvarami, pogosto niso povsem jasna in/ali dovolj analizirana. Zato je stopnja ozaveščenosti zainteresiranih strani prenizka, da bi se lahko predlagali učinkoviti varstveni ukrepi in protiukrepi.

Kibernetski napadi še nikoli niso bili tako kompleksni. Preprosti poskusi se spreminjajo v izpopolnjene dejavnosti, ki se izvajajo zaradi dobička ali političnih razlogov. Nedavni obsežni kibernetski napadi na Estonijo, Litvo in Gruzijo so najbolj znani primeri, ki odražajo splošni trend. Veliko število virusov, črvov in drugih oblik zlonamerne programske opreme, širitev botnetov in vedno večja količina nezaželene elektronske pošte potrjujejo resnost problema²¹.

Zaradi velike odvisnosti od KII, njihove čezmejne medsebojne povezanosti in odvisnosti od drugih infrastruktur kot tudi šibkih točk in groženj, s katerimi se soočajo, je nujno treba sistematično obravnavati njihovo varnost in odpornost ter se tako že v prvi obrambni črti zavarovati pred napakami in napadi.

¹⁶ COM(2008) 199 konč.

¹⁷ http://ec.europa.eu/invest-in-research/action/2006_ahogroup_en.htm.

¹⁸ Pregled gospodarstva EU za leto 2007:

http://ec.europa.eu/economy_finance/publications/publication10130_en.pdf.

¹⁹ <http://www.oecd.org/dataoecd/1/29/40821707.pdf>.

²⁰ <http://epp.eurostat.ec.europa.eu/> – Science and Technology/Information Society.

²¹ COM(2006) 688 konč.

3.3. Varnost in odpornost kritičnih informacijskih infrastruktur za povečanje zaupanja v informacijsko družbo

Da bi se zagotovila čim večja možna uporaba infrastruktur IKT, s čimer bi se v celoti izkoristile gospodarske in družbene priložnosti informacijske družbe, je potrebna visoka stopnja zaupanja vseh zainteresiranih strani. Na to vplivajo različni elementi, najpomembnejši med njimi pa je zagotovitev visoke stopnje varnosti in odpornosti. Raznolikost, odprtost, interoperabilnost, uporabnost, preglednost, odgovornost, možnost presoje različnih komponent in konkurenčnost so ključna gonila za razvoj varnosti ter spodbujajo uporabo izdelkov, procesov in storitev, ki krepijo varnost. Kot je Komisija že poudarila²², gre pri tem za deljeno odgovornost: posamezne zainteresirane strani namreč nimajo sredstev za zagotovitev varnosti in odpornosti vseh infrastruktur IKT ter ne morejo prevzeti vseh odgovornosti, ki so s tem povezane.

Prevzem takšnih odgovornosti zahteva pristop obvladovanja tveganja in kulturo, ki se lahko odzivata na znane grožnje in predvidevata neznane v prihodnosti, ne da bi se pri tem pretirano odzivala ter onemogočala pojav inovativnih storitev in aplikacij.

3.4. Izzivi za Evropo

Poleg vseh dejavnosti, povezanih z izvajanjem direktive o ugotavljanju in določanju evropske kritične infrastrukture, zlasti z določanjem posebnih meril za sektor IKT, je treba za okrepitev varnosti in odpornosti KII obravnavati številne obsežnejše izzive.

3.4.1. Neenotni in neusklajeni nacionalni pristopi

Kljub skupnim značilnostim obravnavanih izzivov in vprašanj se ukrepi in ureditve za zagotavljanje varnosti in odpornosti KII ter raven strokovnosti in pripravljenosti v posameznih državah članicah razlikujejo.

Z zgolj nacionalnim pristopom nastaja tveganje razdrobljenosti in neučinkovitosti po vsej Evropi. Zaradi razlik v nacionalnih pristopih in preslabega sistematičnega čezmejnega sodelovanja so domači protiukrepi bistveno manj učinkoviti, med drugim tudi zato, ker lahko zaradi medsebojne povezanosti KII nizka raven varnosti in odpornosti KII v eni državi poveča ranljivost in tveganja v drugih.

Da bi rešili ta položaj, so potrebna prizadevanja na evropski ravni, ki bodo nacionalnim politikam in programom dala dodano vrednost s spodbujanjem ozaveščenosti in skupnega razumevanja izzivov, spodbujanjem sprejetja skupnih političnih ciljev in prednostnih nalog, krepitvijo sodelovanja med državami članicami ter vključevanjem nacionalnih politik v bolj evropsko in svetovno usmerjen okvir.

3.4.2. Potreba po novem evropskem modelu upravljanja za KII

Krepitev varnosti in odpornosti KII je povezana s posebnimi izzivi na področju upravljanja. Medtem ko nosijo države članice končno odgovornost za določitev politik v zvezi s KII, pa je njihovo izvajanje odvisno od vključenosti zasebnega sektorja, ki ima v lasti ali nadzira veliko število KII. Poleg tega trgi ne zagotavljajo vedno dovolj pobud za zasebni sektor, da bi ta vlagal v zaščito KII v taki meri, kot to ponavadi zahtevajo vlade.

²² COM(2006) 251 konč.

Da bi rešili ta problem upravljanja, so na nacionalni ravni kot referenčni model nastala javno-zasebna partnerstva. Kljub konsenzu, da bi bila takšna partnerstva zaželena tudi na evropski ravni, pa se evropska javno-zasebna partnerstva še niso izoblikovala. Vseevropski okvir upravljanja, ki bi vključeval več interesnih skupin in v katerem bi imela verjetno okrepljeno vlogo tudi ENISA, bi lahko spodbudil vključenost zasebnega sektorja v določanje strateških ciljev javne politike ter tudi operativnih prednostnih nalog in ukrepov. Ta okvir bi pomagal premostiti vrzel med oblikovanjem politike na nacionalni ravni in operativno stvarnostjo.

3.4.3. Omejena zmogljivost Evrope na področju zgodnjega opozarjanja in odzivanja na incidente

Mehanizmi upravljanja bodo resnično učinkoviti le, če se bodo vsi udeleženi pri svojem ravnanju lahko oprli na zanesljive informacije. To je zlasti pomembno za vlade, ki nosijo končno odgovornost za zagotovitev varnosti in dobrega počutja državljanov.

Vendar se postopki in prakse spremljanja in poročanja o varnostnih incidentih na omrežje v posameznih državah članicah zelo razlikujejo. Nekatere med njimi nimajo referenčne organizacije, ki bi bila pristojna za spremljanje. Še več, zdi se, da sodelovanje ter izmenjava zanesljivih in konkretnih podatkov o varnostnih incidentih med državami članicami nista dovolj razvita, saj sta bodisi neformalna ali omejena na dvostranske oziroma večstranske izmenjave z omejenim številom udeležencev. Poleg tega sta simulacija incidentov in organizacija vaj za preverjanje zmogljivosti odzivanja strateškega pomena pri izboljševanju varnosti in obstojnosti KII, zlasti ker se osredotočata na prožne strategije in postopke za obravnavanje nepredvidljivosti morebitnih kriz. V EU so vaje na področju kibernetске varnosti še v dokaj začetni fazi. Vaje, ki segajo prek državnih meja, pa so zelo omejene. Kot se je pokazalo pri nedavnih dogodkih²³, je vzajemna pomoč bistveni element ustreznega odziva na obsežne grožnje in napade na KII.

Močna zmogljivost Evrope za zgodnje opozarjanje in odzivanje na incidente je odvisna od dobrega delovanja nacionalnih/vladnih skupin za odzivanje na računalniške grožnje (CERT), tj. skupne osnovne sposobnosti. Ti organi morajo delovati kot nacionalni spodbujevalci interesov zainteresiranih strani in zmogljivosti za ukrepanje javne politike (vključno z ukrepi v zvezi s sistemi za izmenjavo informacij in opozarjanje, namenjenimi državljanom in MSP) ter se vključiti v učinkovito čezmejno sodelovanje in izmenjavo informacij, od česar bodo lahko imele koristi tudi obstoječe organizacije, kot je evropska skupina vladnih CERT (EGC)²⁴.

3.4.4. Mednarodno sodelovanje

Zaradi vse večjega pomena interneta kot ključne KII je treba posebno pozornost nameniti njegovi odpornosti in stabilnosti. Internet se je zaradi svoje distribucijske, redundantne zasnove izkazal za zelo odporno infrastrukturo. Vendar je njegova neverjetna rast povzročila povečanje fizične in logične zapletenosti ter pojav novih storitev in uporab, zato se upravičeno dvomi, če se bo internet lahko uprl vse večjemu številu prekinitev in kibernetičnih napadov.

Razlike v mnenjih glede pomembnosti elementov, ki sestavljajo internet, delno pojasnjujejo različna stališča, ki so jih vlade izrazile v mednarodnih forumih, in pogosto nasprotujoča si

²³ http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/large_scale/.

²⁴ <http://www.egc-group.org/>.

dojemanja pomembnosti tega vprašanja. To bi lahko oviralo ustrezno preprečevanje groženj, ki vplivajo na internet, pripravljenost nanje in sposobnost odprave njihovih posledic. V okviru varnosti KII je treba na primer oceniti tudi posledice prehoda z IPv4 na IPv6.

Internet je svetovno in zelo distribuirano omrežje omrežij, katerega nadzorni centri ne upoštevajo vedno državnih mej. Za zagotovitev njegove odpornosti in stabilnosti je zato potreben poseben, usmerjen pristop, ki temelji na dveh usklajenih ukrepih. Prvi ukrep je doseči konsenz glede evropskih prednostnih nalog za odpornost in stabilnost interneta, in sicer z vidika javne politike ter delovanja in uporabe. Drugi ukrep pa je vključitev svetovne skupnosti v razvoj ter določitev načel odpornosti in stabilnosti interneta, ki odražajo temeljne evropske vrednote, v okviru strateškega dialoga ter sodelovanja s tretjimi državami in mednarodnimi organizacijami. Osnova teh ukrepov bi bilo priznanje pomena stabilnosti interneta na Svetovnem vrhu o informacijski družbi²⁵.

4. POT NAPREJ: ZA BOLJŠE USKLAJEVANJE IN SODELOVANJE V EU

Zaradi skupnostne in mednarodne razsežnosti problema bi povezani pristop EU k izboljšanju varnosti in odpornosti KII dopolnil nacionalne programe ter obstoječe programe dvo- in večstranskega sodelovanja med državami članicami in jim dodal vrednost.

Iz javnopolitičnih razprav po napadu na Estonijo je razvidno, da je učinke podobnih dogodkov mogoče omejiti s preventivnimi ukrepi in usklajenimi ukrepi med dejansko krizo. Bolj strukturirana izmenjava informacij in dobrih praks po vsej EU bi lahko zelo olajšala boj proti grožnjam, ki segajo prek državnih meja.

Treba je okrepiti obstoječe instrumente sodelovanja, vključno z ENISA, in ustvariti nove, če je to potrebno. Na evropski ravni je nujno potreben proces na več ravneh, v katerega bi bilo vključenih več zainteresiranih strani ter ki bi v celoti spoštoval in dopolnjeval nacionalne pristojnosti.

Potrebno je temeljito razumevanje okolja in omejitev. Skrb zbujača je na primer distribucijska narava interneta, kjer se obrobna vozlišča lahko uporabijo kot vektorji napada, npt. botneti. Vendar je ta distribucijska narava ključni element odpornosti in stabilnosti ter lahko bolj pripomore k hitrejši odpravi posledic kot običajni preveč formalizirani postopki od zgoraj navzdol. To zahteva previdno analizo posameznih primerov javnih politik in operativnih postopkov.

Pomemben je tudi časovni okvir. Jasno je, da je treba takoj ukrepati in hitro vzpostaviti elemente, potrebne za oblikovanje okvira, ki nam bo omogočil odzvati se na trenutne izzive ter ki se bo vključil v prihodnjo strategijo za varnost omrežij in informacij.

Za obvladovanje teh izzivov se predlaga pet področij ukrepanja:

- (1) pripravljenost in preprečevanje: zagotovitev pripravljenosti na vseh ravneh;
- (2) odkrivanje in odziv: zagotovitev ustreznih mehanizmov zgodnjega opozarjanja;

²⁵

Tuniška agenda za informacijsko družbo, <http://www.itu.int/wsis/docs2/tunis/off/6rev1.html>.

- (3) ublažitev in odprava posledic: okrepitev obrambnih mehanizmov EU na področju KII;
- (4) mednarodno sodelovanje: spodbujanje prednostnih nalog EU na mednarodni ravni;
- (5) merila za sektor IKT: podpora izvajanju direktive o ugotavljanju in določanju evropske kritične infrastrukture²⁶.

5. AKCIJSKI NAČRT

5.1. Pripravljenost in preprečevanje

Osnova zmogljivosti in storitev za vseevropsko sodelovanje. Komisija poziva države članice in zadevne zainteresirane strani, naj

- v podporo vseevropskemu sodelovanju skupaj z ENISA opredelijo najnižjo raven zmogljivosti in storitev za nacionalne/vladne CERT ter operacije odzivanja na incidente;
- zagotovijo, da bodo nacionalne/vladne CERT ključni element nacionalne zmogljivosti za pripravljenost, izmenjavo informacij, usklajevanje in odzivanje.

Cilj: dogovor glede minimalnih standardov do konca leta 2010; vzpostavitev dobro delujočih nacionalnih/vladnih CERT v vseh državah članicah do konca leta 2011.

Evropsko javno-zasebno partnerstvo za odpornost. Komisija bo

- spodbujala sodelovanje med javnim in zasebnim sektorjem na področju ciljev varnosti in odpornosti, osnovnih zahtev, dobrih političnih praks in ukrepov. Evropsko javno-zasebno partnerstvo za odpornost bi se osredotočilo predvsem na evropsko razsežnost s strateškega (npr. dobra politična praksa) in taktičnega/operativnega (npr. industrijska uporaba) vidika. Temeljiti bi morale na obstoječih nacionalnih pobudah in operativnih dejavnostih ENISA ter jih dopoljevati.

Cilj: določitev načrta za evropsko javno-zasebno partnerstvo za odpornost do konca leta 2009; ustanovitev evropskega javno-zasebnega partnerstva za odpornost do sredine leta 2010; prvi rezultati delovanja evropskega javno-zasebnega partnerstva za odpornost do konca leta 2010.

Evropski forum za izmenjavo informacij med državami članicami. Komisija bo

- vzpostavila evropski forum, prek katerega bodo lahko države članice izmenjevale informacije in dobre politične prakse na področju varnosti in odpornosti KII. Pri tem bodo koristni rezultati dejavnosti drugih organizacij, zlasti ENISA.

Cilj: začetek delovanja foruma do konca leta 2009; prvi rezultati njegovega delovanja do konca leta 2010.

²⁶

Direktiva Sveta 2008/114/ES.

5.2. Odkrivanje in odziv

Evropski sistem za souporabo informacij in opozarjanje (EISAS). Komisija podpira

razvoj in uvedbo Evropskega sistema za izmenjavo informacij in opozarjanje, ki bi bil namenjen državljanom in MSP ter bi temeljil na nacionalnih in zasebnih sistemih za izmenjavo informacij in opozarjanje. Komisija finančno podpira dva dopolnjujoča se prototipna projekta²⁷. ENISA se poziva, naj prouči rezultate teh projektov in drugih nacionalnih pobud ter pripravi načrt za nadaljnji razvoj in uporabo Evropskega sistema za izmenjavo informacij in opozarjanje.

Cilj: zaključek izvajanja prototipnih projektov do konca leta 2010; načrt za pripravo evropskega sistema do konca leta 2010.

5.3. Ublažitev in odprava posledic

Nacionalni načrti odzivnosti na incidente in vaje. Komisija poziva države članice, naj

- za izboljšanje vseevropskega usklajevanja pripravijo nacionalne načrte odzivnosti na incidente in redno organizirajo vaje za odziv na obsežne varnostne incidente na omrežje ter odpravo posledic nesreč. Nacionalne/vladne CERT/CSIRT bi lahko imele nalogo, da vodijo nacionalne načrte odzivnosti na incidente in vaje ter vanje vključijo zainteresirane strani iz javnega in zasebnega sektorja. ENISA se poziva, naj pomaga pri izmenjavi dobrih praks med državami članicami.

Cilj: organiziranje vsaj ene nacionalne vaje v vsaki državi članici do konca leta 2010.

Vseevropske vaje o odzivanju na obsežne varnostne incidente na omrežje. Komisija bo

- finančno podprla razvoj vseevropskih vaj o odzivanju na varnostne internetne incidente²⁸, ki bi lahko sestavljale tudi operativno platformo za vseevropsko udeležbo pri mednarodnih vajah o odzivanju na varnostne incidente na omrežje, kot je na primer *Cyber Storm* v Združenih državah Amerike.

Cilj: načrtovanje in izvedba prve vseevropske vaje do konca leta 2010; vseevropska udeležba na mednarodnih vajah do konca leta 2010.

Okrepljeno sodelovanje med nacionalnimi/vladnimi CERT. Komisija poziva države članice, naj

- okrepijo sodelovanje med nacionalnimi/vladnimi CERT, med drugim tudi s spodbujanjem in razširjanjem obstoječih mehanizmov sodelovanja, kot je EGC²⁹. ENISA se poziva, naj aktivno sodeluje ter spodbuja in podpira vseevropsko sodelovanje med nacionalnimi/vladnimi CERT, ki bi lahko izboljšalo pripravljenost, okrepilo zmogljivost Evrope za odzivanje na incidente ter podprlo izvedbo vseevropskih (in/ali regionalnih) vaj.

²⁷ V okviru programa ES „Preprečevanje, pripravljenost in obvladovanje posledic terorizma ter drugih tveganj, povezanih z varnostjo“, http://ec.europa.eu/justice_home/funding/cips/funding_cips_en.htm.

²⁸ Glej opombo 27 zgoraj.

²⁹ Glej opombo 24 zgoraj.

Cilj: podvojitev števila nacionalnih organov, udeleženih v EGC, do konca leta 2010; ENISA pripravi referenčni material za podporo vseevropskemu sodelovanju do konca leta 2010.

5.4. Mednarodno sodelovanje

Odpornost in stabilnost interneta. Predvidene so tri dopolnjujoče se dejavnosti:

- Evropske prednostne naloge na področju dolgoročne odpornosti in stabilnosti interneta. Komisija bo pripravila vseevropsko razpravo, v katero bodo vključene vse pomembne javne in zasebne zainteresirane strani ter katere cilj bo določiti prednostne naloge EU na področju dolgoročne odpornosti in stabilnosti interneta.

Cilj: določitev prednostnih nalog EU na področju ključnih internetnih komponent in vprašanj do konca leta 2010.

- Načela in smernice za odpornost in stabilnost interneta (na evropski ravni). Komisija bo skupaj z državami članicami določila smernice za odpornost in stabilnost interneta, pri tem se bo med drugim osredotočila na regionalne ukrepe za odpravo pomanjkljivosti, sporazume o medsebojni pomoči, strategije za usklajeno odpravo posledic in neprekinjenost delovanja, geografsko razširjenost ključnih internetnih virov, tehnološke varstvene ukrepe v internetni arhitekturi in protokolih kot tudi ponavljanje in raznolikost storitev in podatkov. Komisija že financira projektno skupino za odpornost DNS, ki bo poleg drugih pomembnih projektov pomagala pri doseganju konsenza³⁰.

Cilj: določitev evropskega načrta za načela in smernice za odpornost in stabilnost interneta do konca leta 2009; dogovor o prvem osnutku takšnih načel in smernic do konca leta 2010.

- Načela in smernice za odpornost in stabilnost interneta (na svetovni ravni). Komisija bo skupaj z državami članicami pripravila načrt za spodbujanje načel in smernic na svetovni ravni. Kot sredstvo za doseganje konsenza na svetovni ravni se bo razvijalo strateško sodelovanje s tretjimi državami, zlasti v dialogu na področju informacijske družbe³¹.

Cilj: določitev načrta za mednarodno sodelovanje pri pripravi načel in smernic za varnost in odpornost do začetka leta 2010; priprava prvega osnutka mednarodno priznanih načel in smernic, o katerih se bo s tretjimi državami razpravljalo v ustreznih forumih, vključno s Forumom o upravljanju interneta, do konca leta 2010.

Svetovne vaje na področju odprave in ublažitve posledic obsežnih internetnih incidentov. Komisija poziva evropske zainteresirane strani, naj

- razmislijo o praktičnem načinu, kako razširiti vaje, ki se izvajajo v okviru ublažitve in odprave posledic, na svetovni ravni, ter pri tem upoštevajo regionalne načrte odzivnosti na incidente in zmogljivosti.

Cilj: Komisija pripravi predlog okvira in načrta za podporo vključenosti in sodelovanju Evrope v svetovnih vajah na področju odprave in ublažitve posledic obsežnih internetnih incidentov do konca leta 2010.

³⁰ Glej opombo 27 zgoraj.

³¹ COM(2008) 588 konč.

5.5. Merila za evropske kritične infrastrukture v sektorju IKT

Posebna merila za sektor IKT. Komisija bo na podlagi začetnih dejavnosti, ki so se izvajale v letu 2008,

- skupaj z državami članicami in vsemi ustreznimi zainteresiranimi stranmi še naprej razvijala merila za določitev evropskih kritičnih infrastruktur za sektor IKT. V ta namen se bodo iz posebne študije, ki se je začela izvajati³², zbrale ustrezne informacije.

Cilj: Komisija opredeli merila za evropske kritične infrastrukture za sektor IKT do prve polovice leta 2010.

6. SKLEPNE UGOTOVITVE

Varnost in odpornost KII sta najpomembnejši pri obrambi pred okvarami in napadi. Njuna okrepitev po celotni EU je nujno potrebna, če želimo v celoti izkoristiti prednosti informacijske družbe. Za doseg tega ambicioznega cilja se predlaga akcijski načrt za izboljšanje taktičnega in operativnega sodelovanja na evropski ravni. Uspeh teh ukrepov je odvisen od tega, kako uspešno lahko gradijo na podlagi dejavnosti javnega in zasebnega sektorja ter kako jim lahko koristijo, pa tudi od zavezanosti in polnega sodelovanja držav članic, evropskih institucij in zainteresiranih strani.

Zato bo 27. in 28. aprila 2009 organizirana ministrska konferenca, na kateri se bo z državami članicami razpravljalo o predlaganih pobudah ter okrepila njihova zavezanost za razpravo o posodobljeni in okrepljeni politiki VOI v Evropi.

Poleg tega je okrepitev varnosti in odpornosti KII dolgoročen cilj, katerega strategijo in ukrepe je treba redno ocenjevati. Ker pa je ta cilj skladen s splošno razpravo o prihodnosti politike varnosti omrežja in informacij v EU po letu 2012, bo Komisija proti koncu leta 2010 začela s pregledom stanja, da bi ocenila prvo fazo ukrepov ter po potrebi opredelila in predlagala prihodnje ukrepe.

³² Glej opombo 27 zgoraj.