EUROPSKA
KOMISIJA

Bruxelles, 5.7.2016.
COM(2016) 410 final

KOMUNIKACIJA KOMISIJE EUROPSKOM PARLAMENTU, VIJEĆU, EUROPSKOM GOSPODARSKOM I SOCIJALNOM ODBORU I ODBORU REGIJA

Jačanje europskog sustava kibernetičke sigurnosti

i poticanje konkurentne i inovativne industrije kibernetičke sigurnosti

1. UVOD/KONTEKST

Incidenti povezani s kibernetičkom sigurnošću svakodnevno uzrokuju znatnu gospodarsku štetu europskim poduzećima i gospodarstvu u cjelini te narušavaju povjerenje građana i poduzetnika u digitalno društvo. Krađa poslovnih tajni, poslovnih informacija i osobnih podataka, prekid pružanja usluga, među ostalim i temeljnih, kao i smetnje u radu infrastrukture, uzrokuju gospodarske gubitke koji se mjere stotinama milijardi eura godišnje[1]. Sve to moglo bi se odraziti i na temeljna prava građana i društvo u cjelini.

Strategija Europske unije za kibernetičku sigurnost iz 2013.[2] (Strategija kibernetičke sigurnosti EU-a) i njezin glavni rezultat, direktiva o mrežnoj i informacijskoj sigurnosti (MIS)[3], koja će uskoro biti donesena, kao i Direktiva 2013/40 o napadima na informacijske sustave, najvažniji su odgovor politike Europske unije na navedene izazove u pogledu kibernetičke sigurnosti. Osim toga, EU-u su na raspolaganju i specijalizirana tijela, kao što su Agencija Europske unije za mrežnu i informacijsku sigurnost (ENISA), Europski centar za kibernetički kriminal (EC3) pri Europolu te tim za hitne računalne intervencije (CERT-EU). Nedavno je pokrenuto i nekoliko sektorskih inicijativa (npr. u području energetike i prijevoza) u cilju povećanja kibernetičke sigurnost u različitim ključnim sektorima.

EU je unatoč tim pozitivnim postignućima osjetljiv na kibernetičke incidente. To bi moglo narušiti jedinstveno digitalno tržište te gospodarski i socijalni život u cjelini. Nije samo gospodarstvo izloženo njihovu utjecaju. U slučaju hibridnih prijetnji[4] kibernetički napadi mogu biti koordinirani s drugim aktivnostima kako bi se destabilizirala zemlja ili dovelo u pitanje funkcioniranje političkih institucija.

U tom kontekstu, rješavanje kibernetičkog incidenta većih razmjera istodobno u nekoliko država članica moglo bi biti zahtjevno za EU. Uzimajući u obzir i komunikacije o suzbijanju hibridnih prijetnji i izradi Europskog programa sigurnosti[5], Komisija traži moguća rješenja u pogledu kibernetičke sigurnosti koja se stalno mijenja te procjenjuje dodatne mjere koje bi se mogle pokazati potrebnima radi poboljšanja otpornosti kibernetičke sigurnosti EU-a i odgovora na incidente.

Nadalje, Komisija se bavi i pitanjem kibernetičke sigurnosti industrijskih kapaciteta u EU-u. Iako nije moguće ovladati cijelim vrijednosnim lancem digitalnih tehnologija u Europi, potrebno je barem zadržati i razviti neke najvažnije kapacitete. Opskrba proizvodima i uslugama kojima se osigurava najviša razina kibernetičke sigurnosti velika je prilika za industriju kibernetičke sigurnosti u Europi i mogla bi prerasti u snažnu konkurentsku prednost. Očekuje se da će globalno tržište kibernetičke sigurnosti biti jedno od najbrže rastućih segmenata u sektoru informacijskih i komunikacijskih tehnologija[6]. Vodeću ulogu EU-a u ovom području treba poduprijeti snažnom kulturom sigurnosti podataka, među ostalim

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies; June 2014.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.
[6] Vidi SWD(2016) 216.

i osobnih podataka, i učinkovitim odgovorom na incidente. To će biti snažan argument u prilog ulaganja u EU-u i podrška ostvarenju ambicioznih ciljeva jedinstvenog digitalnog tržišta u pogledu rasta i otvaranja radnih mjesta.

U tu je svrhu potrebna snažna predanost, posebno u pogledu sljedećeg:

i. jačanja suradnje u cilju poboljšanja pripremljenosti za kibernetičke incidente i njihova rješavanja

Potrebno je osnažiti postojeće i dogovorene mehanizme suradnje radi unapređenja otpornosti i pripremljenosti EU-a, među ostalim i za moguće paneuropske krize u pogledu kibernetičke sigurnosti. Ti mehanizmi suradnje trebali bi biti sveobuhvatni tijekom životnog ciklusa incidenta, od sprečavanja do kaznenog progona. Za učinkovitu suradnju među državama članicama i praktičnu provedbu sigurnosnih zahtjeva za ključne operatere bit će potrebna i kvalitetna tehnička rješenja industrije kibernetičke sigurnosti.

Istovremeno će za osiguranje otpornosti ključne kibernetičke imovine u cijeloj Europskoj uniji biti potrebni kontinuirani napori u cilju pronalaženja međusektorske sinergije i uključivanja zahtjeva u pogledu kibernetike u sve relevantne politike EU-a. Komisija će razmotriti je li u skoroj budućnosti potrebno ažurirati Strategiju kibernetičke sigurnosti EU-a iz 2013.

ii. rješavanja problema s kojima se suočava europsko jedinstveno tržište kibernetičke sigurnosti

U Strategiji jedinstvenog digitalnog tržišta[7] navedeno je da još uvijek postoje određene praznine u dinamičnom području tehnologija i rješenja za sigurnost internetskih mreža. Istovremeno, ispitivanja tržišta pokazuju da je unutarnje tržište EU-a još uvijek zemljopisno rascjepkano u pogledu opskrbe proizvodima i uslugama za kibernetičku sigurnost[8]. U ovoj se Komunikaciji iznosi nekoliko mjera politike usmjerenih na tržište u cilju pronalaženja rješenja za te praznine i izazove povezane s jedinstvenim tržištem.

iii. poticanja razvoja kapaciteta industrije u području kibernetičke sigurnosti

Komisija se u Strategiji kibernetičke sigurnosti EU-a i Strategiji jedinstvenog digitalnog tržišta obvezala da će promicati povećanu opskrbu proizvodima i uslugama industrije kibernetičke sigurnosti u EU-u. Stoga je Komisija donijela i odluku kojom se utire put ugovornom javno-privatnom partnerstvu (uJPP) o kibernetičkoj sigurnosti, kojim će se nastojati promicati vrhunska istraživanja europske kibernetičke sigurnosti i program inovacija za povećanu konkurentnost.

[7] COM(2015) 192.
[8] Vidi SWD(2016) 216.

2. UNAPREĐENJE SURADNJE, ZNANJA I KAPACITETA

Strategijom kibernetičke sigurnosti EU-a, a posebno direktivom o MIS-u[9] otvorit će se put prema boljoj suradnji u državama članicama na razini EU-a. Brza i učinkovita provedba direktive bit će ključna s obzirom na sve veću digitalizaciju gospodarskog i društvenog života (uzimajući u obzir i oblak, internet stvari te komunikaciju između uređaja), rastuću prekograničnu povezanost i sve brojnije kibernetičke prijetnje[10]. U tom se kontekstu EU treba pripremiti za moguću kibernetičku krizu velikih razmjera[11], među ostalim primjerice ozbiljne istovremene napade na ključne informacijske sustave u nekoliko država članica[12].

Stoga je nužna suradnja na razini EU-a radi rješavanja kibernetičkih incidenata manjih razmjera koji bi se mogli proširiti, kao i mogućeg kibernetičkog napada velikih razmjera u nekoliko država članica. EU treba uvrstiti kibernetičke aspekte u postojeće mehanizme za upravljanje krizama. Također treba osigurati učinkovite mehanizme za suradnju i brzu razmjenu informacija među sektorima i državama članicama, u cilju odgovora na takve incidente i njihova ograničavanja. Nadalje, ti bi mehanizmi trebali usklađeno funkcionirati, što bi doprinijelo borbi protiv terorizma, organiziranog kriminala i kibernetičkog kriminala. Time bi se povećala i sposobnost EU-a u pogledu koordinacije s međunarodnim partnerima u svrhu pružanja učinkovitog odgovora na globalne prijetnje i incidente.

2.1. Maksimalno iskorištavanje mehanizama suradnje u području MIS-a i prijelaz agencije ENISA na inačicu 2.0

Važan dio nacionalnih kapaciteta propisanih direktivom o MIS-u jesu timovi za odgovor na računalne sigurnosne incidente (CSIRT-ovi) odgovorni za brzu reakciju na kibernetičke prijetnje i incidente. Oni će uspostaviti mrežu CSIRT-ova radi promicanja učinkovite operativne suradnje o određenim kibernetičkim sigurnosnim incidentima i razmjene informacija o rizicima. Nadalje, na temelju direktive bit će uspostavljena skupina za suradnju u cilju pružanja potpore i pomoći strateškoj suradnji među državama članicama i izgradnje njihova uzajamnog povjerenja.

S obzirom na prirodu i brojnost kibernetičkih prijetnji, Komisija potiče države članice da u najvećoj mogućoj mjeri iskoriste mehanizme suradnje u području MIS-a te da unaprijede prekograničnu suradnju koja se odnosi na pripremljenost za kibernetički incident velikih razmjera. Koordinirana suradnja u slučaju krize u različitim dijelovima kibernetičkog ekosustava bila bi korisna za takvu dodatnu suradnju u slučaju ozbiljnog kibernetičkog incidenta. Takav se pristup može utvrditi „planom" kojim bi se osigurale i sinergija i usklađenost s postojećim mehanizmima za upravljanje krizama[13]. Potrebno ga je redovito testirati u vježbama koje se odnose na kibernetiku i upravljanje krizama. U njemu bi sudjelovala i tijela na razini EU-a, kao što su ENISA, CERT-EU i Europski centar za

[9] U skladu s direktivom o MIS-u države članice bit će dužne utvrditi pružatelje temeljnih usluga u područjima kao što su energetika, prijevoz, financije i zdravlje, rješavati rizike kibernetičke sigurnosti i osigurati da određeni pružatelji digitalnih usluga poduzimaju odgovarajuće mjere za rješavanje tih rizika.

[10] Vidi SWD(2016) 216.

[11] Vidi npr. izvješće ENISA-e: Uobičajeni postupci upravljanja krizama na razini EU-a i njihova primjenjivost na kibernetičke krize (travanj 2016.)

[12] Vidi SWD(2016) 216.

[13] Posebno integrirani aranžmani EU-a za politički odgovor na krize, među ostalim odluka o aranžmanima za provedbu klauzule o solidarnosti u Uniji (24. srpnja 2014.) i postupci odlučivanja o zajedničkoj sigurnosnoj i obrambenoj politici.

kibernetički kriminal (EC3) pri Europolu, a upotrebljavali bi se alati razvijeni u okviru mreže CSIRT-ova. Komisija će u prvoj polovici 2017. predložiti takav plan suradnje kako bi se skupina za suradnju, mreža CSIRT-ova i ostali relevantni dionici mogli o njemu očitovati.

Trenutačno su spoznaje i stručna znanja o kibernetičkoj sigurnosti dostupni na razini EU-a, ali u rascjepkanom i nestrukturiranom obliku. U cilju pružanja potpore mehanizmima suradnje u području MIS-a, informacije bi trebalo prikupiti u „informacijski centar" kako bi bile lako dostupne svim državama članicama na njihov zahtjev. Taj bi „centar" postao središnji izvor informacija kojim bi se, prema potrebi, institucijama EU-a i državama članicama omogućila razmjena informacija. Lakšim pristupom bolje strukturiranim informacijama o rizicima kibernetičke sigurnosti i mogućim načinima za njihovo ublažavanje države članice mogle bi povećati svoje kapacitete i uskladiti svoja postupanja te tako unaprijediti ukupnu otpornost na napade. Komisija će uz potporu ENISA-e i CERT-EU-a te na temelju stručnih znanja svojeg Zajedničkog istraživačkog centra olakšati uspostavu centra i osigurati njegovu održivost.

Osim toga, trebalo bi na razini EU-a uspostaviti stalnu savjetodavnu skupinu visoke razine[14] za pitanja kibernetičke sigurnosti, sastavljenu od stručnjaka i donositelja odluka iz industrije, akademske zajednice, civilnog društva i ostalih relevantnih organizacija. Ta bi skupina Komisiji omogućila otvoren i transparentan pristup vanjskim stručnim znanjima i informacijama za njezine strateške politike u području kibernetičke sigurnosti te potencijalne regulatorne ili druge mjere javne politike. Skupina bi se dopunjavala i povezivala s ostalim strukturama u području kibernetičke sigurnosti.[15]

Štoviše, od Komisije se zahtijeva da do 20. lipnja 2018. ocijeni rad ENISA-e, a moguća izmjena ili obnova ENISA-ina mandata mora biti odobrena do 19. lipnja 2020.[16] S obzirom na trenutačno stanje u području kibernetičke sigurnosti, Komisija namjerava provesti ocjenjivanje i na temelju njegovih rezultata što prije predstaviti prijedlog.

Komisija će pri razmatranju moguće izmjene ENISA-ina mandata uzeti u obzir prethodno opisane izazove u području kibernetičke sigurnosti, kao i ukupne napore koji se poduzimaju u pogledu poboljšanja suradnje i razmjene znanja. Taj će postupak biti prilika za sagledavanje mogućeg unapređenja sposobnosti i kapaciteta Agencije za održivo pružanje podrške državama članicama pri ostvarenju otpornosti u području kibernetičke sigurnosti. Pri razmatranju ENISA-ina mandata treba uzeti u obzir i nove odgovornosti Agencije u skladu s direktivom o MIS-u, nove ciljeve politike radi pružanja potpore industriji kibernetičke sigurnosti (Strategija jedinstvenog digitalnog tržišta i posebno uJPP), rastuće potrebe za osiguranjem ključnih sektora te nove izazove povezane s prekograničnim incidentima, uključujući koordinirani odgovor na kibernetičke krize.

[14] Stručne skupine Komisije podliježu horizontalnim propisima iz Odluke Komisije C(2016)3301.
[15] Npr. Platforma za MIS, uJPP za kibernetičku sigurnost te sektorske platforme, kao npr. Platforma stručnjaka za energetiku u području kibernetičke sigurnosti (EECSP). Trebalo bi uspostaviti i poveznicu s okruglim stolom na visokoj razini koji je najavljen u Komunikaciji o digitalizaciji europske industrije: COM(2016) 180.
[16] Uredba (EU) br. 526/2013 o stavljanju izvan snage Uredbe (EZ) br. 460/2004.

Komisija će učiniti sljedeće:

- u prvoj polovici 2017. dostaviti na razmatranje plan suradnje u cilju rješavanja kibernetičkih incidenata velikih razmjera na razini EU-a,
- pomoći pri uspostavi „informacijskog centra" u cilju pružanja potpore razmjeni informacija među tijelima EU-a i državama članicama,
- uspostaviti savjetodavnu skupinu na visokoj razini za pitanja kibernetičke sigurnosti i
- završiti ocjenjivanje ENISA-e do kraja 2017. Pri ocjenjivanju će razmotriti je li potrebno izmijeniti ili proširiti mandat ENISA-e i u najkraćem će roku predstaviti svoj prijedlog.

2.2. Pojačani napori u pogledu obrazovanja, osposobljavanja i vježbi u području kibernetičke sigurnosti

Odgovarajuće vještine i osposobljavanje koji se odnose na sprečavanje incidenata u području kibernetičke sigurnosti i ublažavanje njihovih učinaka neki su od ključnih aspekata otpornosti u području kibernetičke sigurnosti.

Trenutačno ENISA, Europska skupina za osposobljavanje i obrazovanje u području kibernetičkog kriminala (ECTEG), u suradnji s Europskim centrom za kibernetički kriminal pri Europolu i Europskom policijskom akademijom (CEPOL), imaju važnu ulogu u pružanju potpore izgradnji kapaciteta, među ostalim i za kibernetičku forenziku, i to izradom priručnika, organiziranjem osposobljavanja i vježbi u području kibernetičke sigurnosti.

Istovremeno, kibernetički je prostor područje koje se vrlo brzo razvija i u kojem kapaciteti dvojne namjene imaju ključnu ulogu. Stoga je potrebno razvijati civilno-vojnu suradnju i sinergiju u području osposobljavanja i vježbi, a radi povećanja otpornosti i sposobnosti EU-a za odgovor u slučaju incidenta.

Kako bi odgovorile na tu potrebu, službe Komisije surađivat će nakon donošenja direktive o MIS-u i okvira za politiku kibernetičke obrane EU-a[17] s državama članicama, Europskom službom za vanjsko djelovanje (EEAS), ENISA-om i ostalim relevantnim tijelima EU-a[18] radi uspostave platforme za obrazovanje, osposobljavanje i vježbe u području kibernetičke sigurnosti kojom će se promicati sinergija između osposobljavanja za civilne i obrambene potrebe.

Komisija će učiniti sljedeće:

- blisko surađivati s državama članicama, ENISA-om, EEAS-om i ostalim relevantnim tijelima EU-a u cilju uspostave platforme za osposobljavanje u području kibernetičke sigurnosti.

[17] Vijeće za vanjske poslove Europske unije donijelo je okvir 18. studenoga 2014., dokument 15585/14.
[18] Kao što su Europska akademija za sigurnost i obranu, EC3, CEPOL, Europska obrambena agencija.

2.3. Pitanja međusektorske međuovisnosti i otpornosti ključne javne infrastrukture

Stupanj prekograničnih i međusektorskih međuovisnosti važan je čimbenik pri procjeni rizika i učinka kibernetičkog incidenta velikih razmjera. Ozbiljan kibernetički incident u jednom sektoru ili jednoj državi članici može izravno ili neizravno utjecati na ostale sektore ili države članice, ili se u njima proširiti.

Prekograničnom i međusektorskom suradnjom omogućuje se razmjena informacija i stručnih znanja te unapređuju pripremljenost i otpornost. Komisija podupire rad različitih sektora u cilju boljeg razumijevanja međuovisnosti i to provedbom Europskog programa zaštite ključne infrastrukture[19].

Istovremeno je sposobnost svakog pojedinačnog sektora za prepoznavanje kibernetičkih napada, pripremu za napade i odgovor na njih nužan preduvjet za rješavanje međusektorskih rizika. Komisija će procijeniti rizike koji proizlaze iz kibernetičkih incidenata u sektorima koji su međusobno vrlo ovisni unutar i preko nacionalnih granica, a posebno u sektorima koji su obuhvaćeni direktivom o MIS-u, uzimajući u obzir i razvoj situacije na međunarodnoj razini[20]. Komisija će nakon te procjene razmotriti ima li potrebe za dodatnim posebnim propisima i/ili uputama o pripremljenosti za kibernetičke rizike u tim ključnim sektorima.

Na europskoj razini, sektorski centri za razmjenu i analizu informacija[21] (ISAC-ovi) te odgovarajući CSIRT-ovi mogu imati vrlo važnu ulogu u pripremama za kibernetičke napade i odgovoru na njih. Kako bi se osigurao učinkovit protok informacija o sve brojnijim prijetnjama i olakšao odgovor na kibernetičke incidente, treba poticati ISAC-ove na uključivanje u mrežu CSIRT-ova na temelju direktive o MIS-u, kao i na suradnju s Europskim centrom za kibernetički kriminal pri Europolu i relevantnim izvršnim tijelima.

Sudionici u razmjeni informacija među dionicima i s nadležnim tijelima tijekom životnog ciklusa kibernetičkih rizika moraju znati da zbog toga neće snositi odgovornost. Komisija je utvrdila nekoliko takvih slučajeva u kojima poduzetnici zbog zabrinutosti nisu razmijenili važne obavještajne podatke o prijetnjama s drugim poduzetnicima, sektorima ili tijelima, a posebno s onima preko granica. Komisija će u interesu unapređenja razmjene informacija o kibernetičkim prijetnjama nastojati riješiti i otkloniti takve zabrinutosti.

Pouzdani načini izvješćivanja kojima se osigurava povjerljivost iznimno su važni i kao poticaj poduzetnicima na prijavljivanje kibernetičkih krađa poslovnih tajni. Time bi se omogućilo praćenje i procjena štete nanesene europskoj industriji (koja uzrokuje gubitak prodaje i radnih mjesta) te istraživačkim tijelima. Bilo bi to korisno i za pronalaženje odgovarajućeg odgovora politike. Komisija će uz potporu ENISA-e, Ureda Europske unije za intelektualno vlasništvo (EUIPO) i centra EC3 pri Europolu te u okviru dijaloga s privatnim dionicima uspostaviti pouzdane načine za dobrovoljno prijavljivanje kibernetičkih krađa poslovnih tajni. To bi trebalo omogućiti prikupljanje podataka na razini EU-a u anonimnom i agregiranom obliku. Ti bi se podaci mogli razmjenjivati s državama članicama kao osnova za diplomatske korake i

[19] SWD(2013) 318.
[20] Npr. plan kibernetičke sigurnosti koji je donijela Europska agencija za sigurnost zračnog prometa, plan kibernetičke sigurnosti, djelovanje Međunarodne organizacije civilnog zrakoplovstva, Međunarodne pomorske organizacije.
[21] Vidi npr. European Energy ISAC (http://www.ee-isac.eu).

mjere za podizanje svijesti u svrhu zaštite nematerijalne imovine Europske unije od kibernetičkih napada.

Komisija će u svrhu sektorske kibernetičke sigurnosti promicati uključivanje kibernetičke sigurnosti u postupak razvoja raznih sektorskih politika na razini EU-a koje su najviše povezane sa sektorskom sigurnošću.

Naposljetku, tijela javne vlasti važna su za provjeru integriteta ključne internetske infrastrukture u pogledu otkrivanja problema, obavješćivanja subjekta odgovornog za te mreže te, prema potrebi, pružanja pomoći pri otklanjanju poznatih slabosti. Nacionalna regulatorna tijela mogla bi iskoristiti kapacitete CSIRT-ova u svrhu redovitih dubinskih provjera stanja javnih mrežnih infrastruktura. Na temelju toga mogla bi poticati operatore na otklanjanje nedostataka ili slabosti koji bi se takvim dubinskim provjerama mogli utvrditi.

Komisija će stoga ispitati potrebne pravne i organizacijske uvjete pod kojima bi nacionalna regulatorna tijela u suradnji s nacionalnim tijelima za kibernetičku sigurnost mogla podnijeti zahtjev CSIRT-ovima za provođenje redovitih provjera slabih točaka javnih mrežnih infrastruktura. Nacionalne CSIRT-ove treba poticati na suradnju u okviru mreže CSIRT-ova i to u vezi s najboljim praksama praćenja mreža te tako olakšati sprečavanje incidenata velikih razmjera.

Komisija će učiniti sljedeće:

- promicati suradnju centara za razmjenu i analizu sektorskih informacija na europskoj razini, poticati njihovu suradnju s CSIRT-ovima i nastojati otkloniti prepreke razmjeni informacija među sudionicima na tržištu,
- istražiti strateški/sustavni rizik koji proizlazi iz kibernetičkih incidenata u sektorima koji su međusobno vrlo ovisni unutar i izvan nacionalnih granica,
- procijeniti i prema potrebi razmotriti jesu li potrebni dodatni propisi i/ili upute o pripremljenosti ključnih sektora za kibernetički rizik,
- u suradnji s ENISA-om, EUIPO-om i centrom EC3 uspostaviti pouzdane načine za dobrovoljno prijavljivanje kibernetičkih krađa poslovnih tajni,
- promicati uključivanje mjera kibernetičke sigurnosti u europske sektorske politike i
- ispitati potrebne uvjete pod kojima bi nacionalna tijela mogla podnijeti zahtjev CSIRT-ovima za provođenje redovitih provjera ključnih mrežnih infrastruktura.

3. RJEŠAVANJE PROBLEMA S KOJIMA SE SUOČAVA EUROPSKO JEDINSTVENO TRŽIŠTE KIBERNETIČKE SIGURNOSTI

Europi su potrebni visokokvalitetni, povoljni te interoperabilni proizvodi i rješenja za kibernetičku sigurnost. No, opskrba proizvodima i uslugama za sigurnost IKT-a na jedinstvenom tržištu i dalje je geografski vrlo rascjepkana. S jedne strane, time je europskim poduzećima otežano tržišno natjecanje na nacionalnoj, europskoj i svjetskoj razini, a s druge

strane ograničen je izbor održivih i iskoristivih tehnologija u području kibernetičke sigurnosti kojima građani i poduzeća imaju pristup[22].

Industrija kibernetičke sigurnosti u Europi uglavnom se razvijala u skladu s potrebama nacionalnih vlada, među ostalim i s potrebama obrambenog sektora. Većina vanjskih suradnika u području obrane osnovali su odjele za kibernetičku sigurnost[23]. Istovremeno se pojavio veliki broj inovativnih MSP-ova i na specijaliziranim tržištima / u tržišnim nišama (npr. sustavi za šifiranje) i na razvijenim tržištima s novim poslovnim modelima (npr. antivirusni softveri).

No, poduzećima nije lako širiti se izvan domaćeg, nacionalnog tržišta. U svim savjetovanjima koje je Komisija provela jasno se pokazalo da je ključni razlog tome nepovjerenje u „prekogranična" rješenja[24]. Stoga veliki dio nabave i dalje ostaje unutar granica određene države članice, a brojna poduzeća teško postižu ekonomije razmjera zahvaljujući kojima bi bila konkurentnija i na domaćem i na svjetskom tržištu.

Nepostojanje interoperabilnih rješenja (tehnički standardi), praksi (postupci i norme) i mehanizama certificiranja na razini EU-a neki su od nedostataka koji utječu na jedinstveno tržište kibernetičke sigurnosti. U tom je kontekstu utvrđeno da je kibernetička sigurnost jedan od prioriteta normizacije IKT-a za jedinstveno digitalno tržište[25].

Zbog ograničenih izgleda za rast poduzeća koja posluju u području kibernetičke sigurnosti na jedinstvenom tržištu često se spajaju ili ih preuzimaju ulagači izvan EU-a[26]. Iako taj trend ukazuje na inovativnost europskih poduzetnika u području kibernetičke sigurnosti, on može uzrokovati i gubitak europskog stručnog znanja i iskustva te odljev mozgova.

Potrebne su hitne mjere kojima će se potaknuti veća povezanost jedinstvenog tržišta za proizvode i usluge za kibernetičku sigurnost i olakšati uvođenje praktičnijih i povoljnijih rješenja.

Nepovjerenje među europskim industrijskim i institucijskim dionicima može se prevladati poticanjem suradnje u ranoj fazi životnog ciklusa inovacije: unutar same industrije kibernetičke sigurnosti, između dobavljača i kupaca te među sektorima u koje su uključene industrije koje već jesu ili će vjerojatno postati kupci rješenja za kibernetičku sigurnost.

Istovremeno, razvoj proizvoda, usluga i tehnologija dvojne namjene postaje sve važniji u Europi. Na obrambenom je tržištu sve više rješenja iz civilnog sektora[27]. U budućem Akcijskom planu za europsku obranu Komisija namjerava utvrditi mjere za poticanje vojno-civilne sinergije na europskoj razini.

3.1. Certificiranje i označavanje

Certificiranje je važno za povećanje povjerenja i sigurnosti proizvoda i usluga. To vrijedi i za nove sustave u kojima se u velikoj mjeri upotrebljavaju digitalne tehnologije i koji zahtijevaju

[22] Vidi SWD(2016) 216.
[23] Vidi SWD(2016) 216.
[24] Vidi SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Vidi SWD(2016) 216.
[27] U 2013. izvoz robe dvojne namjene činio je 20 % vrijednosti ukupnog izvoza EU-a. U to je uključena trgovina unutar EU-a.

visok stupanj sigurnosti, primjerice povezani i automatizirani automobili, e-zdravlje, kontrolni sustavi za industrijsku automatizaciju ili pametne mreže.

Pojavljuju se nacionalne inicijative za utvrđenje zahtjeva u pogledu visoke razine kibernetičke sigurnosti za komponente IKT-a u tradicionalnoj infrastrukturi, među ostalim zahtjeva za certificiranje. Bez obzira na njihovu važnost, prisutan je rizik rascjepkavanja jedinstvenog tržišta i pojave problema u pogledu interoperabilnosti. Samo u nekoliko država članica postoje programi učinkovitog certificiranja proizvoda za IKT[28]. Moguće je da prodavatelj IKT-a zbog toga mora proći nekoliko postupaka certificiranja kako bi mogao prodavati u nekoliko država članica. U najgorem slučaju, proizvod ili usluga za IKT koji su osmišljeni tako da ispunjavaju zahtjeve u pogledu kibernetičke sigurnosti u jednoj državi članici, ne mogu biti stavljeni na tržište u drugoj.

U cilju postizanja funkcionalnog jedinstvenog tržišta u području kibernetičke sigurnosti mogućim okvirom za sigurnosno certificiranje proizvoda i usluga za IKT trebalo bi težiti postizanju sljedećih ciljeva: i. obuhvatiti široki spektar sustava, proizvoda i usluga za IKT; ii. osigurati primjenu u svih 28 država članica; i iii. obuhvatiti sve razine kibernetičke sigurnosti, a sve to uzimajući u obzir razvoj situacije na međunarodnoj razini.

U tu će svrhu Komisija osnovati posebnu radnu skupinu za područje sigurnosnog certificiranja proizvoda i usluga za IKT, čiji će članovi biti stručnjaci iz država članica i te industrije. Njezin cilj do kraja 2016. bit će u suradnji s ENISA-om i Zajedničkim istraživačkim centrom izraditi smjernice za razradu moguće pripreme prijedloga takvog europskog okvira za sigurnosno certificiranje u području IKT-a do kraja 2017. U tom će smislu Komisija razmotriti i Uredbu (EZ) br. 2008/765 i odredbe o certificiranju iz Opće uredbe o zaštiti podataka 2016/679[29].

Taj će postupak obuhvaćati opsežna savjetovanja i procjenu rizika. Time će se Komisiji omogućiti istraživanje različitih mogućnosti za izradu okvira za certificiranje proizvoda i usluga za IKT. Komisija će istražiti i sigurnosno certificiranje u području IKT-a u okviru infrastrukturnih sektora (npr. zrakoplovstvo, željeznice, automobilska industrija) i u okviru određenih mehanizama certificiranja i vrednovanja tehnologije koja je spremna za uvođenje (npr. kibernetička sigurnost kontrolnih sustava za industrijsku automatizaciju[30], internet stvari, oblak). Utvrđene nedostatke rješavat će i u okviru navedenog programa za sigurnosno certificiranje u području IKT-a.

Certificiranje će se u najvećoj mogućoj mjeri temeljiti na priznatim standardima, a razvijat će se u suradnji s međunarodnim partnerima.

---

[28] Vidi SWD(2016) 216 za sporazum o Skupini visokih dužnosnika za informatičke sustave (Odluka Vijeća od 31. ožujka 1992. (92/242/EEZ)) i druge postojeće programe npr. *Commercial Product Assurance* u Ujedinjenoj Kraljevini i *Certification Sécuritaire de Premier Niveau* u Francuskoj.

[29] Uredbom (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka predviđaju se i kodeksi ponašanja koji su namijenjeni pružanju doprinosa ispravnoj provedbi pravila o zaštiti osobnih podataka i mehanizmi certificiranja te obuhvaća sva načela zaštite podataka, a posebno sigurnost podataka tijekom obrade osobnih podataka.

[30] ERNCIP-ova tematska skupina za „kibernetičku sigurnost industrijskih kontrolnih sustava" dostupna je na sljedećoj poveznici: https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

Komisija će ispitati i najbolje načine za integraciju sigurnosnog certificiranja u području IKT-a u buduće zakonodavstvo o tom sektoru, kao i sigurnosne aspekte.

Uz regulatorne mogućnosti, Komisija će razmotriti i izradu europskog komercijalnog, dobrovoljnog i jednostavnog programa označavanja proizvoda za sigurnost IKT-a. Uz certificiranje, cilj joj je poboljšati razumljivost podataka o kibernetičkoj sigurnosti na komercijalnim proizvodima radi povećanja njihove konkurentnosti na jedinstvenom i svjetskom tržištu. U obzir će se uzeti aktualne sektorske i horizontalne inicijative koje su u tom području pokrenuli i dobavljači i potrošači.

Blisko će se surađivati s javnim upravama kako bi se omogućila upotreba zajedničkih specifikacija i upućivanja na certificiranje u ugovorima javne nabave. Komisija će na nacionalnoj razini pratiti upotrebu odgovarajućih zahtjeva u pogledu certificiranja u javnoj nabavi, a posebno u sektorskim sustavima (energetika, prijevoz, zdravlje, javna uprava itd.) i izvješćivati o tome.

Komisija će učiniti sljedeće:

- do kraja 2016. izraditi smjernice za pripremu prijedloga europskog okvira za sigurnosno certificiranje koji će vjerojatno biti predstavljen do kraja 2017. te procijeniti izvedivost i učinak europskog okvira za jednostavno označavanje u području kibernetičke sigurnosti;
- istražiti je li potrebno sigurnosno certificiranje u području IKT-a i prema potrebi ukloniti nedostatke postojećih mehanizama certificiranja/vrednovanja u tom sektoru;
- u buduće zakonodavne prijedloge u tom sektoru prema potrebi uključiti integraciju sigurnosnog certificiranja proizvoda za IKT;
- poticati suradnju s javnim upravama kako bi se olakšala upotreba certificiranja i zajedničkih specifikacija u javnoj nabavi i
- pratiti upotrebu odgovarajućih zahtjeva za certificiranje u javnoj nabavi i nabavi u privatnom sektoru te za tri godine izvijestiti o stanju na tržištu.

3.2. Unaprjeđenje kibernetičke sigurnosti u Europi i potpora MSP-ovima

Iako se u sektoru kibernetičke sigurnosti u Europi bilježi porast inovacija, EU-u i dalje nedostaje kultura ulaganja u kibernetičku sigurnost. Postoje brojni inovativni MSP-ovi u tom području, no oni često ne mogu unaprijediti svoje poslovanje. Među ostalim, zbog nedostatka lako dostupnog financiranja u ranim fazama razvoja. Poduzećima je ograničen pristup poduzetničkom kapitalu u Europi i ne raspolažu dostatnim sredstvima za poboljšanje njihove vidljivosti na tržištu ili ispunjenje zahtjeva u pogledu standardizacije i usklađenosti.

Istovremeno, suradnja među dionicima u području kibernetičke sigurnosti prilično je neujednačena te su potrebni daljnji napori za povećanje koncentracije ekonomskih subjekata i razvoj novih vrijednosnih lanaca[31].

Olakšan pristup financiranju preduvjet je za rast ulaganja u kibernetičku sigurnost u Europi i potporu MSP-ovima. Treba podupirati razvoj globalno konkurentnih klastera u području kibernetičke sigurnosti te centara izvrsnosti u odgovarajućim regionalnim ekosustavima za digitalni razvoj. Ta potpora mora biti povezana s provedbom strategija pametnih specijalizacija i drugim instrumentima EU-a kako bi ih se bolje iskoristilo u industriji kibernetičke sigurnosti u Europi.

Komisija će što je moguće bolje informirati zajednicu kibernetičke sigurnosti o mogućnostima financiranja na europskoj, nacionalnoj i regionalnoj razini (u pogledu horizontalnih instrumenata i u pogledu posebnih poziva[32]) s pomoću postojećih instrumenata i kanala npr. Europska poduzetnička mreža.

Komisija će usto s Europskom investicijskom bankom i Europskim investicijskim fondom ispitati mogućnosti lakšeg pristupa financiranju. Financiranje bi moglo biti u obliku vlasničkih i kvazivlasničkih ulaganja, zajmova, jamstava za projekte ili protujamstava posrednicima, npr. uspostavom platforme za ulaganja u području kibernetičke sigurnosti u okviru Europskog fonda za strateška ulaganja[33].

Usto, Komisija će sa zainteresiranim državama članicama i regijama istražiti platformu za pametnu specijalizaciju u području kibernetičke sigurnosti[34]. Time bi se pridonijelo koordinaciji i planiranju strategija u području kibernetičke sigurnosti te uspostavila strateška suradnja među zainteresiranim stranama u regionalnim ekosustavima. Na taj bi se način mogli iskoristiti potencijali postojećih europskih strukturnih i investicijskih fondova za sektor kibernetičke sigurnosti.

Komisija će općenito promicati pristup integrirane sigurnosti. Nastojat će osigurati dosljedno rješavanje zahtjeva u pogledu kibernetičke sigurnosti u svim velikim infrastrukturnim ulaganjima koja imaju digitalnu komponentu i koja se sufinanciraju iz europskih fondova, a sve to postupnim uvođenjem odgovarajućih zahtjeva u propise o javnoj nabavi i programima.

Komisija će učiniti sljedeće:

- koristiti se alatima za potporu MSP-ovima u cilju informiranja zajednice

[31] Vidi SWD(2016) 216.

[32] Vidi npr. višesektorski poziv na podnošenje prijedloga za 2016. u okviru programa Instrument za povezivanje Europe, 2016 COSMO pozivi za Program za internacionalizaciju klastera.

[33] U okviru Europskog fonda za strateška ulaganja potpora pojedinačnim projektima može biti izravna ili neizravna, preko investicijskih platformi. Takve platforme mogu biti korisne za financiranje manjih projekata i objedinjavanje sredstava iz različitih izvora kako bi se omogućila geografski ili tematski diversificirana ulaganja.

[34] Instrumenti strategije pametnih specijalizacija dostupni su na sljedećoj poveznici: http://s3platform.jrc.ec.europa.eu/.

kibernetičke sigurnosti o postojećim mehanizmima financiranja;
- unaprijediti upotrebu alata i instrumenata EU-a u cilju pružanja potpore inovativnim MSP-ovima u istraživanju sinergije između civilnog i obrambenog tržišta u području kibernetičke sigurnosti[35];
- s Europskom investicijskom bankom i Europskim investicijskim fondom istražiti mogućnost lakšeg pristupa ulaganjima, npr. preko posebne platforme za ulaganja u području kibernetičke sigurnosti i s pomoću drugih alata;
- osnovati platformu za pametnu specijalizaciju u području kibernetičke sigurnosti kao potpore državama članicama i regijama koje su zainteresirane za ulaganja u sektor kibernetičke sigurnosti (RIS3); i
- promicati pristup integrirane sigurnosti u velikim infrastrukturnim ulaganjima koja imaju digitalnu komponentu i koja se sufinanciraju iz fondova EU-a.

4. PROMICANJE I POTICANJE EUROPSKE INDUSTRIJE KIBERNETIČKE SIGURNOSTI INOVACIJAMA – USPOSTAVA UJPP-A ZA KIBERNETIČKU SIGURNOST

U cilju promicanja konkurentnosti europske industrije kibernetičke sigurnosti i njezinih inovacija, sklopit će se ugovorna javno-privatna partnerstva (uJPP) za kibernetičku sigurnost. U okviru uJPP-a prikupljat će se industrijski i javni resursi radi postizanja izvrsnosti u istraživanju i inovacijama.

Cilj je uJPP-a izgraditi povjerenje među državama članicama i dionicima u toj industriji poticanjem suradnje u ranim fazama istraživanja i inovacija. Cilj mu je i doprinijeti usklađivanju sektora ponude i potražnje. Time bi se industriji trebalo omogućiti da buduće zahtjeve dobije od krajnjih korisnika i sektora koji su važni kupci rješenja za kibernetičku sigurnost (npr. energetika, zdravlje, prijevoz, financije). Olakšat će se i njihovo sudjelovanje u definiranju zajedničkih zahtjeva u pogledu digitalne sigurnosti, privatnosti i zaštite podataka za njihove sektore.

Zahvaljujući uJPP-u u području kibernetičke sigurnosti povećat će se iskorištenost raspoloživih sredstava. To će se postići, prije svega, boljom koordinacijom s državama članicama. Nadalje, naglasak će biti na nekoliko tehničkih prioriteta kako bi se omogućio tehnološki napredak industrije kibernetičke sigurnosti i usavršile buduće ključne tehnologije za kibernetičku sigurnost. U tom smislu, razvojem računalnog programa otvorenog koda i otvorenih standarda mogu se potaknuti povjerenje, transparentnost i disruptivne inovacije te bi ih stoga trebalo uzeti u obzir pri ulaganju u taj uJPP.

Sinergije s drugim europskim projektima, pogotovo s onima u području sigurnosti, također će koristiti radu na kibernetičkoj sigurnosti u okviru uJPP-a, npr. Tvornice budućnosti, Energetski učinkovita gradnja, JPP-ovi za 5G, JPP-ovi za velike podatke[36], drugi sektorski JPP-ovi[37] te inicijativa internet stvari[38]. Nadalje, promicat će se i precizno usklađivanje s

[35] Primjerice Europska poduzetnička mreža i Europska mreža regija angažiranih u području obrane regijama pružit će nove mogućnosti istraživanja prekogranične suradnje u području dvojne namjene, među ostalim kibernetičke sigurnosti, a MSP-ovima sudjelovanje u aktivnostima povezivanja.
[36] Javno-privatno partnerstvo za 5G infrastrukturu i javno-privatno partnerstvo za vrijednost velikih podataka.
[37] Primjerice Europski sustav upravljanja zračnim prometom (SESAR) ili javno-privatno partnerstvo za prelazak na željeznicu.

europskim oblakom za otvorenu znanost i europskom inicijativom superračunala u području kvantnih kibernetičkih tehnologija (npr. inovacije u distribuciji kvantnih ključeva, istraživanja u području kvantnog računalstva).

UJPP za kibernetičku sigurnost osnovan je u okviru programa Obzor 2020.[39], okvirnog programa EU-a za istraživanja i inovacije za razdoblje 2014. – 2020. Njime će se osigurati financiranje iz sljedeća dva stupa programa: vodeći položaj u razvojnim i industrijskim tehnologijama (LEIT-ICT) i društveni izazov – sigurna društva (SC7). Ukupan proračun tog uJPP-a iznosit će do 450 milijuna EUR s trostrukim faktorom financijske poluge za industriju. Pitanje kibernetičke sigurnosti trebalo bi rješavati i koordinirati s drugim odgovarajućim dijelovima Obzora 2020. (npr. energetika, prijevoz, zdravstveni i društveni izazovi te dio Obzora 2020. koji se odnosi na izvrsnost). Time će se pridonijeti postizanju ciljeva uJPP-a za kibernetičku sigurnost. Koordinaciju bi trebalo provesti unaprijed, u fazi stvaranja sektorskih strategija.

UJPP će se provesti transparentno, s otvorenom i fleksibilnom strukturom za upravljanje prilagođenom okruženju kibernetičke sigurnosti koje se brzo razvija. Pritom će se u obzir uzeti činjenica da države članice moraju raspraviti kako promjene u tehnologijama utječu na sigurno upravljanje nacionalnim i prekograničnim infrastrukturama. Jednako tako, rezultat partnerstva mora biti održiv tijekom nekoliko godina kako bi se mogli postići njegovi ciljevi.

Europska organizacija za kibernetičku sigurnost (ECSO) podržat će uJPP, a njezino će članstvo biti odraz raznolikosti tržišta kibernetičke sigurnosti u Europi. U njemu će sudjelovati nacionalne, regionalne i lokalne javne uprave, istraživački centri, akademske zajednice te druge zainteresirane strane.

Komisija će učiniti sljedeće:

- s industrijom sklopiti ugovorno javno-privatno partnerstvo za kibernetičku sigurnost kako bi ono postalo operativno u trećem tromjesečju 2016.;
- objaviti pozive na podnošenje prijedloga koji se odnose na uJPP za kibernetičku sigurnost u prvom tromjesečju 2017.; i
- uskladiti uJPP za kibernetičku sigurnost s odgovarajućim sektorskim strategijama, instrumentima programa Obzor 2020. i sektorskim JPP-ovima.

5. ZAKLJUČAK

U ovoj su Komunikaciji predstavljene mjere za jačanje europskog sustava kibernetičke otpornosti te poticanje konkurentne i inovativne industrije za kibernetičku sigurnost u Europi, kako je najavljeno u Strategiji EU-a za kibernetičku sigurnost i u Strategiji jedinstvenog digitalnog tržišta. Komisija poziva Europski parlament i Vijeće da podupru taj pristup.

[38] Savez za inovaciju u području interneta stvari (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.