EURÓPSKA
KOMISIA

V Bruseli 5. 7. 2016
COM(2016) 410 final

OZNÁMENIE KOMISIE EURÓPSKEMU PARLAMENTU, RADE, EURÓPSKEMU HOSPODÁRSKEMU A SOCIÁLNEMU VÝBORU A VÝBORU REGIÓNOV

Posilnenie odolnosti kybernetického systému a podpora konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe

1. ÚVOD/KONTEXT

Každý deň spôsobujú incidenty v oblasti kybernetickej bezpečnosti veľké hospodárske škody európskym podnikov a ekonomike vo všeobecnosti. Takéto incidenty oslabujú dôveru občanov a podnikov v digitálnu spoločnosť. Krádež obchodných tajomstiev, obchodných informácií a osobných údajov, narušenie služieb – vrátane tých základných – a infraštruktúr vedú každý rok k hospodárskym stratám v stovkách miliárd eur.[1] Môžu mať dôsledky aj na základné práva občanov a na spoločnosť ako celok.

Stratégia kybernetickej bezpečnosti Európskej únie z roku 2013[2] (stratégia kybernetickej bezpečnosti EÚ) a jej hlavný výstup, teda smernica o sieťovej a informačnej bezpečnosti, ktorá bude čoskoro prijatá[3], ako aj smernica 2013/40/EÚ o útokoch na informačné systémy predstavujú doteraz jadro politickej reakcie Európskej únie na tieto problémy v oblasti kybernetickej bezpečnosti. Okrem toho má EÚ k dispozícii špecializované subjekty, ako je napríklad Agentúra Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA), Európske centrum boja proti počítačovej kriminalite (EC3) v rámci Europolu a tím EÚ pre reakciu na núdzové počítačové situácie (CERT-EU). Nedávno bolo spustených aj niekoľko odvetvových iniciatív (napr. v oblasti energetiky a dopravy) na zlepšenie kybernetickej bezpečnosti v rôznych kritických odvetviach.

Napriek tomuto pozitívnemu vývoju predstavujú kybernetické incidenty pre EÚ stálu hrozbu. To môže narušiť jednotný digitálny trh a hospodársky a sociálny život ako taký. Ich vplyv sa nemusí prejaviť len v hospodárstve. V prípade hybridných hrozieb[4] možno využiť kybernetické útoky koordinovane s ostatnými činnosťami na destabilizáciu krajiny alebo spochybnenie politických inštitúcií.

V tejto súvislosti by riešenie rozsiahleho kybernetického incidentu vo viacerých členských štátoch súčasne mohlo byť pre EÚ náročné. V súčinnosti s oznámením o boji proti hybridným hrozbám, ako aj oznámením o plnení európskeho programu v oblasti bezpečnosti[5] Komisia hľadá spôsoby, ako reagovať na vznikajúce situácie v oblasti kybernetickej bezpečnosti a posudzovať ďalšie opatrenia, ktoré môžu byť potrebné na zlepšenie odolnosti EÚ v oblasti počítačovej bezpečnosti a jej schopnosti reagovať na incidenty.

Komisia sa navyše zaoberá aj priemyselnými kapacitami počítačovej bezpečnosti v EÚ. Hoci celý hodnotový reťazec digitálnych technológií pravdepodobne nebude v Európe možné zvládnuť, je potrebné zachovať a rozvíjať aspoň určité základné kapacity. Dodávanie produktov a služieb, ktoré poskytujú najvyššiu úroveň počítačovej bezpečnosti, predstavuje pre odvetvie počítačovej bezpečnosti v Európe príležitosť, ktorá by sa mohla stať silnou konkurenčnou výhodou. Očakáva sa, že globálny trh počítačovej bezpečnosti bude jedným z najrýchlejšie rastúcich segmentov odvetvia informačných a komunikačných technológií

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II (Čisté straty: Odhad globálnych nákladov na počítačovú kriminalitu, Hospodársky vplyv počítačovej kriminality II); Center for Strategic and International Studies (Centrum pre medzinárodné a strategické štúdie); jún 2014.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.

(IKT)[6]. Aby sa EÚ stala vedúcim aktérom v tejto oblasti, musí stavať na silnej kultúre ochrany údajov vrátane osobných údajov a na účinnej reakcii na incidenty. Tento krok bude vnímaný ako silný argument pre investovanie v EÚ a pomôže aj pri dosahovaní ambicióznych cieľov jednotného digitálneho trhu v podobe vytvárania rastu a pracovných miest.

Na dosiahnutie spomenutých cieľov je potrebný silný záväzok najmä pomocou týchto krokov:

i) Posilnenie spolupráce s cieľom zlepšiť pripravenosť a riešenie počítačových incidentov

Je potrebné posilniť existujúce, ako aj dohodnuté mechanizmy spolupráce, aby sme zvýšili odolnosť a pripravenosť EÚ aj na prípadnú celoeurópsku krízu v oblasti počítačovej bezpečnosti. Tieto mechanizmy spolupráce musia byť komplexné a musia sa týkať celého cyklu existencie incidentu od prevencie po trestné stíhanie. Účinná spolupráca medzi členskými štátmi a praktické uplatňovanie bezpečnostných požiadaviek v prípade rozhodujúcich subjektov si v odvetví počítačovej bezpečnosti vyžiadajú aj spoľahlivé technické riešenia.

Zabezpečenie odolnosti kritických počítačových aktív celej EÚ si bude vyžadovať trvalé úsilie pri hľadaní medziodvetvových synergií a začlenení počítačových požiadaviek do všetkých relevantných politík EÚ. Komisia zváži, či je v blízkej budúcnosti nutné aktualizovať stratégiu kybernetickej bezpečnosti EÚ z roku 2013.

ii) Riešenie problémov, ktorým čelí jednotný trh kybernetickej bezpečnosti v Európe

V stratégii pre digitálny jednotný trh[7] sa uznalo, že v rýchlo sa vyvíjajúcej oblasti technológií a riešení internetovej bezpečnosti sietí stále existujú špecifické nedoriešené otázky. Z trhových štúdií zároveň vyplýva, že vnútorný trh EÚ je z hľadiska ponuky produktov a služieb kybernetickej bezpečnosti stále geograficky roztrieštený.[8] Týmto oznámením sa stanovuje niekoľko trhovo orientovaných politických opatrení na riešenie uvedených otázok a problémov jednotného trhu.

iii) Rozvíjanie priemyselných kapacít v oblasti kybernetickej bezpečnosti

Komisia sa v rámci stratégie kybernetickej bezpečnosti EÚ, ako aj v rámci stratégie jednotného digitálneho trhu zaviazala podporovať zvyšovanie dodávok produktov a služieb v odvetví kybernetickej bezpečnosti EÚ. Preto prijíma aj rozhodnutie, ktoré otvára cestu k zmluvnej dohode o verejno-súkromnom partnerstve v oblasti kybernetickej bezpečnosti, ktorou sa má podporiť špičkový program výskumu a inovácií v oblasti kybernetickej bezpečnosti v Európe s cieľom zvýšiť konkurencieschopnosť.

2. ROZVÍJANIE SPOLUPRÁCE, ZNALOSTÍ A SCHOPNOSTÍ

Stratégia kybernetickej bezpečnosti EÚ, a najmä nadchádzajúca smernica o sieťovej a informačnej bezpečnosti[9] vytvoria priestor na lepšiu spoluprácu členských štátov na európskej

[6] Pozri SWD(2016) 216.
[7] COM(2015) 192.
[8] Pozri SWD(2016) 216.
[9] Smernicou o sieťovej a informačnej bezpečnosti sa stanoví, aby členské štáty v rámci riešení rizík kybernetickej bezpečnosti určili skupinu poskytovateľov základných služieb v takých oblastiach, ako je energetika, doprava, financie a zdravotná starostlivosť, a aby zabezpečili, že určití poskytovatelia digitálnych služieb prijmú vhodné opatrenia na riešenie takýchto rizík.

úrovni. Rýchla a účinná implementácia smernice bude kľúčová vzhľadom na narastajúcu digitalizáciu hospodárskeho a spoločenského života (berúc do úvahy aj cloudové služby, internet vecí a komunikáciu typu stroj-stroj), rozširujúce sa cezhraničné prepojenie a rýchlo sa rozvíjajúce prostredie kybernetických hrozieb[10]. V tejto súvislosti sa EÚ musí pripraviť na možnosť rozsiahlej kybernetickej krízy[11] vrátane napríklad súbežných útokov na kritické informačné systémy vo viacerých členských štátoch[12].

Základom riešenia menších, ale potenciálne sa šíriacich kybernetických incidentov rastúceho rozsahu, ako aj prípadného rozsiahleho kybernetického útoku vo viacerých členských štátoch je preto spolupráca na úrovni EÚ. EÚ musí začleniť kybernetické aspekty do existujúcich mechanizmov krízového riadenia a takisto zabezpečiť účinnú spoluprácu a mechanizmy rýchlej výmeny informácií medzi odvetviami a členskými štátmi, aby mohla reagovať na takéto incidenty a zvládať ich. Tieto mechanizmy by mali navyše fungovať súdržne, a tým prispievať k boju proti terorizmu, organizovanej trestnej činnosti a počítačovej kriminalite. Zvýšila by sa tým schopnosť EÚ koordinovať účinnú reakciu na globálne hrozby a incidenty s jej medzinárodnými partnermi.

2.1. Najefektívnejšie využívanie mechanizmov spolupráce v oblasti sieťovej a informačnej bezpečnosti a vývoj smerom k ENISA 2.0

Základnou súčasťou národných spôsobilostí požadovaných v smernici o sieťovej a informačnej bezpečnosti sú tímy reakcie na incidenty počítačovej bezpečnosti (CSIRT) zodpovedné za rýchlu reakciu na kybernetické hrozby a incidenty. Tieto tímy vytvoria sieť CSIRT s cieľom podporiť účinnú operačnú spoluprácu na konkrétnych incidentoch v rámci kybernetickej bezpečnosti a pri výmene informácií o rizikách. Na základe tejto smernice bude zriadená aj skupina pre spoluprácu na podporu a uľahčovanie strategickej spolupráce medzi členskými štátmi a budovanie vzájomnej dôvery.

Vzhľadom na charakter a množstvo kybernetických hrozieb Komisia vyzýva členské štáty, aby čo najlepšie využívali mechanizmy spolupráce v oblasti sieťovej a informačnej bezpečnosti, a aby zlepšovali cezhraničnú spoluprácu týkajúcu sa pripravenosti na závažné kybernetické incidenty. Takejto ďalšej spolupráci pre prípad závažného kybernetického incidentu by prospel koordinovaný prístupu ku krízovej spolupráci medzi rôznymi prvkami kybernetického ekosystému. Uvedený prístup môže byť stanovený v koncepcii, ktorá by mala zabezpečiť aj súčinnosť a súlad s existujúcimi mechanizmami krízového riadenia[13]. Následne by sa mala pravidelne skúšať v rámci cvičení zameraných na riadenie kybernetických a iných kríz. Koncepcia by zahŕňala úlohu subjektov na úrovni EÚ, ako sú agentúra ENISA, tím CERT-EU, centrum EC3 pri Europole, a využívala by nástroje vyvinuté v rámci siete CSIRT. V prvej polovici roka 2017 predloží Komisia koncepciu takejto spolupráce na posúdenie skupine pre spoluprácu, sieti CSIRT a ostatným príslušným zainteresovaným stranám.

[10] Pozri SWD(2016) 216.
[11] Pozri napríklad správu agentúry ENISA: Spoločné postupy krízového riadenia na úrovni EÚ a ich uplatniteľnosť na kybernetické krízy (apríl 2016).
[12] Pozri SWD(2016) 216.
[13] Predovšetkým dojednania o integrovanej politickej reakcii na krízu vrátane rozhodnutia o vykonávaní doložky o solidarite zo strany Únie (24. júla 2014) a rozhodovacie procesy spoločnej bezpečnostnej a obrannej politiky.

V súčasnosti sú poznatky a odborné znalosti o kybernetickej bezpečnosti na úrovni EÚ dostupné, avšak v rozptýlenej a neštruktúrovanej podobe. S cieľom podporiť mechanizmy spolupráce v oblasti sieťovej a informačnej bezpečnosti by sa informácie mali zhromaždiť v „informačnom uzle“, aby boli na požiadanie ľahko dostupné pre všetky členské štáty. Tento „uzol“ by sa mal stať ústredným zdrojom, ktorý umožní inštitúciám EÚ a členským štátom vymieňať si informácie podľa potreby. Ľahší prístup k lepšie štruktúrovaným informáciám o rizikách súvisiacich s kybernetickou bezpečnosťou a k možným opravným prostriedkom by mal pomôcť členským štátom zlepšiť ich možnosti a zosúladiť ich postupy, a tým zvýšiť celkovú odolnosť proti útokom. Komisia, podporovaná agentúrou ENISA, tímom CERT-EU a vybavená odbornými znalosťami svojho Spoločného výskumného centra, uľahčí vytvorenie spomínaného centra a zabezpečí jeho udržateľnosť.

Okrem toho by sa na úrovni EÚ mala zriadiť riadna poradná skupinu na vysokej úrovni[14] pre kybernetickú bezpečnosť zložená z odborníkov a subjektov s rozhodovacími právomocami z tohto odvetvia, akademickej obce, občianskej spoločnosti a iných relevantných organizácií. Takáto skupina by umožnila Komisii otvoreným a transparentným spôsobom získať externé odborné znalosti a podklady pre jej politiky v rámci stratégie kybernetickej bezpečnosti a pre možné regulačné alebo iné opatrenia týkajúce sa verejnej politiky. Dopĺňala by a prepájala iné štruktúry pre kybernetickú bezpečnosť[15].

Komisia je navyše povinná vykonať do 20. júna 2018 hodnotenie agentúry ENISA a prípadné obnovenie alebo zmenu mandátu agentúry treba prijať do 19. júna 2020[16]. Vzhľadom na súčasnú situáciu v oblasti kybernetickej bezpečnosti je cieľom Komisie pokročiť s hodnotením a na základe výsledkov predložiť čo najskôr návrh nového mandátu.

Pri posudzovaní prípadnej potreby zmeniť mandát agentúry ENISA Komisia zohľadní už uvedené problémy kybernetickej bezpečnosti a celkové úsilie o zintenzívnenie spolupráce a výmenu poznatkov. Tento proces umožní preskúmať prípadnú potrebu posilniť spôsobilosti a kapacity agentúry podporovať udržateľným spôsobom členské štáty pri dosahovaní odolnosti v oblasti kybernetickej bezpečnosti. Pri uvažovaní o mandáte agentúry ENISA je ďalej potrebné vziať do úvahy jej nové zodpovednosti v rámci smernice o sieťovej a informačnej bezpečnosti, nové politické ciele zamerané na podporu odvetvia kybernetickej bezpečnosti (stratégia digitálneho jednotného trhu a najmä zmluvné verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti), meniace sa potreby pri zabezpečovaní kritických odvetví a nové problémy spojené s cezhraničnými incidentmi vrátane koordinovanej reakcie na kybernetické krízy.

[14] Skupina odborníkov Komisie sa riadi horizontálnymi pravidlami stanovenými rozhodnutím Komisie C(2016) 3301.

[15] Napr. platforma pre sieťovú a informačnú bezpečnosť, zmluvné verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti a odvetvové platformy, ako je napr. platforma expertov kybernetickej bezpečnosti v odvetví energetiky (EECSP). Mala by sa prepojiť aj s okrúhlym stolom na vysokej úrovni ohláseným v oznámení o digitalizácii európskeho priemyslu: COM(2016) 180.

[16] Nariadenie (EÚ) č. 526/2013, ktorým sa ruší nariadenie (ES) č. 460/2004.

Komisia

- predloží na posúdenie plán spolupráce na riešení kybernetických incidentov na úrovni EÚ v prvej polovici roku 2017,
- uľahčí vytvorenie „informačného uzla“ na podporu výmeny informácií medzi orgánmi EÚ a členskými štátmi,
- zriadi poradnú skupinu pre kybernetickú bezpečnosť na vysokej úrovni a
- do konca roku 2017 dokončí hodnotenie agentúry ENISA. Toto hodnotenie sa bude zaoberať potrebou zmeniť alebo rozšíriť mandát agentúry ENISA s cieľom predložiť čo najskôr prípadný návrh.

2.2. Zvýšenie úsilia vo vzdelávaní, odbornej príprave a cvičení v oblasti kybernetickej bezpečnosti

Primerané zručnosti a odborná príprava súvisiace s prevenciou incidentov v oblasti kybernetickej bezpečnosti, ako aj s riešením a so zmierňovaním ich vplyvov patria ku kľúčovým aspektom dosiahnutia odolnosti v oblasti kybernetickej bezpečnosti.

V súčasnosti zohrávajú agentúra ENISA, Európska skupina pre vzdelávanie a odbornú prípravu v oblasti boja proti počítačovej kriminalite (ECTEG) v spolupráci s Európskym centrom boja proti počítačovej kriminalite a Európskou policajnou akadémiou (CEPOL) dôležitú úlohu v poskytovaní podpory pri budovaní kapacít vrátane kybernetických forenzných vied vo forme vypracovávania príručiek, organizovania školení a cvičení v oblasti kybernetickej bezpečnosti.

Kybernetický priestor je zároveň rýchlo sa rozvíjajúcou oblasťou, v ktorej zásadnú úlohu zohrávajú spôsobilosti s dvojakým využitím. Preto je potrebné rozvíjať civilno-vojenskú spoluprácu a synergie v oblasti odbornej prípravy a cvičení, aby sa zvýšila odolnosť EÚ a jej schopnosť reagovať na incidenty.

S cieľom reagovať na túto potrebu a v nadväznosti na prijatie smernice o sieťovej a informačnej bezpečnosti a politického rámca EÚ pre kybernetickú obranu[17] budú útvary Komisie spolupracovať s členskými štátmi, Európskou službou pre vonkajšiu činnosť (EEAS), agentúrou ENISA a ostatnými príslušnými orgánmi EÚ[18] na zriadení platformy pre vzdelávanie, cvičenie a odbornú prípravu v oblasti kybernetickej bezpečnosti, ktorá podporí synergie medzi civilnou a obrannou odbornou prípravou.

Komisia

- bude v úzkej spolupráci s členskými štátmi, agentúrou ENISA, službou EEAS a ostatnými relevantnými orgánmi EÚ pracovať na vytvorení platformy pre odbornú prípravu v oblasti kybernetickej bezpečnosti.

[17] Prijatý Radou Európskej únie pre zahraničné veci 18. novembra 2014, dokument 15585/14.
[18] Ako je napríklad Európska akadémia bezpečnosti a obrany, centrum EC3, CEPOL, Európska obranná agentúra.

2.3. Riešenie medziodvetvových vzájomných závislostí a odolnosti kľúčových verejných sieťových infraštruktúr

Dôležitým faktorom posudzovania rizika a vplyvu rozsiahleho kybernetického incidentu je miera vzájomných cezhraničných a medziodvetvových vzájomných závislostí. Závažný kybernetický incident v jednom odvetví alebo v jednom členskom štáte môže priamo alebo nepriamo ovplyvniť iné odvetvia alebo iné členské štáty, prípadne sa do nich rozšíriť.

Cezhraničná a medziodvetvová spolupráca uľahčuje výmenu informácií a odborných znalostí, čím sa zvyšuje pripravenosť a odolnosť. Komisia podporuje prácu rôznych odvetví smerujúcu k lepšiemu pochopeniu vzájomných závislostí prostredníctvom implementácie Európskeho programu na ochranu kritickej infraštruktúry[19].

Nevyhnutným predpokladom na riešenie medziodvetvových rizík je zároveň schopnosť každého jedného odvetvia identifikovať kybernetické incidenty, pripraviť sa a reagovať na ne. Komisia posúdi riziko vyplývajúce z kybernetických incidentov v odvetviach s vysokou mierou vzájomnej závislosti v rámci štátov aj cezhranične, najmä v odvetviach, na ktoré sa vzťahuje smernica o sieťovej a informačnej bezpečnosti, aj pri zohľadnení vývoja na medzinárodnej úrovni[20]. Po tomto posúdení Komisia zváži, či sú pre takéto kritické odvetvia potrebné ďalšie osobitné pravidlá a/alebo usmernenia týkajúce sa pripravenosti na kybernetické riziká.

Na európskej úrovni môžu kľúčovú úlohu pri príprave na kybernetické incidenty a v reakcii na ne zohrávať odvetvové Centrá na výmenu a analýzu informácií (ISAC)[21] a zodpovedajúce tímy CSIRT. S cieľom zaistiť účinné vymieňanie informácií o vyvíjajúcich sa hrozbách a uľahčiť reakciu na kybernetické incidenty mali by byť ISAC motivované k tomu, aby spolupracovali so sieťou tímov CSIRT podľa smernice o sieťovej a informačnej bezpečnosti, s Európskym centrom boja proti počítačovej kriminalite pri Europole, s tímom CERT-EU, ako aj s príslušnými orgánmi presadzovania práva.

Výmena informácií medzi zúčastnenými stranami a orgánmi počas celého cyklu existencie kybernetických rizík si vyžaduje dôveru medzi účastníkmi, že nebudú vystavení zodpovednosti. Komisia zaznamenala množstvo problémov, ktoré bránia podnikom vymieňať si cenné poznatky o hrozbách vo vlastných kruhoch, v rámci rôznych odvetví alebo s orgánmi, najmä cezhranične. Bude sa preto usilovať riešiť a zmierniť tieto obavy v záujme zlepšenia výmeny informácií o kybernetických hrozbách.

Kľúčové z hľadiska podpory podnikov pri oznamovaní kybernetickej krádeže obchodných tajomstiev sú aj dôveryhodné kanály oznamovania. Týmto spôsobom by sa mohli monitorovať a posudzovať škody, ktoré európskemu priemyslu (aj v dôsledku poklesu objemu predaja a straty pracovných miest) a výskumným orgánom vznikli. Okrem toho by to bolo užitočné pri navrhovaní vhodnej politickej reakcie. S podporou agentúry ENISA, Úradu Európskej únie pre duševné vlastníctvo (EUIPO) a centra EC3 Komisia zriadi v rámci

[19] SWD(2013) 318.
[20] Napr. plán kybernetickej bezpečnosti prijatý Európskou agentúrou pre bezpečnosť letectva, plán kybernetickej bezpečnosti, práce Medzinárodnej organizácie civilného letectva a Medzinárodnej námornej organizácie.
[21] Pozri napr. európske ISAC pre energetiku (http://www.ee-isac.eu).

dialógu so súkromnými zainteresovanými stranami dôveryhodné kanály na dobrovoľné ohlasovanie kybernetických krádeží obchodných tajomstiev. To by umožnilo zhromažďovať anonymizované a agregované údaje na úrovni EÚ. Tieto údaje si členské štáty môžu navzájom vymieňať ako podklady na diplomatické úsilie a činnosti zvyšujúce informovanosť, a pomáhať tak pri ochrane nehmotného majetku EÚ pred kybernetickými útokmi.

S cieľom podporiť odvetvovú kybernetickú bezpečnosť bude Komisia podporovať aj začlenenie kybernetickej bezpečnosti do vypracovania rôznych odvetvových politík EÚ, ktorých významnou súčasťou je kybernetická bezpečnosť.

Dôležitú úlohu pri overovaní integrity kľúčových internetových infraštruktúr zohrávajú v neposlednom rade aj verejné orgány, a to pri zisťovaní problémov, informovaní strán zodpovedných za takéto siete a v prípade potreby pri poskytovaní pomoci pri náprave známych slabých miest. Vnútroštátne regulačné orgány by mohli využívať kapacity tímov CSIRT na pravidelné kontroly verejných sieťových infraštruktúr. Na základe toho by mohli nabádať prevádzkovateľov, aby napravili nedostatky alebo riešili nedostatočné zabezpečenie zistené takýmito kontrolami.

Komisia preto preskúma potrebné právne a organizačné podmienky, aby umožnila vnútroštátnym regulačným orgánom v spolupráci s vnútroštátnymi orgánmi pre kybernetickú bezpečnosť požiadať tímy CSIRT o vykonanie pravidelných kontrol nedostatkov verejných sieťových infraštruktúr. Vnútroštátne tímy CSIRT by mali byť motivované k tomu, aby v rámci siete CSIRT spolupracovali na osvedčených postupoch pri monitorovaní sietí, a tým uľahčili predchádzanie rozsiahlym incidentom.

Komisia

- bude napomáhať vzniku európskej spolupráce odvetvových Centier na výmenu a analýzu informácií, podporovať ich spoluprácu s tímami CSIRT a snažiť sa riešiť prekážky, ktoré môžu účastníkom trhu brániť pri výmene informácií,
- preskúma strategické/systémové riziko vyplývajúce z kybernetických incidentov v odvetviach s vysokou mierou vzájomnej závislosti v rámci štátov a cezhranične,
- posúdi potrebu, prípadne zváži dodatočné pravidlá a/alebo usmernenia týkajúce sa pripravenosti kritických odvetví na kybernetické riziká,
- zriadi spolu s agentúrou ENISA, úradom EUIPO a centrom EC3 dôveryhodné kanály na dobrovoľné nahlasovanie kybernetických krádeží obchodných tajomstiev,
- podporí začleňovanie opatrení v oblasti kybernetickej bezpečnosti do európskych odvetvových politík a
- preskúma nevyhnutné podmienky, ktoré umožnia vnútroštátnym orgánom požiadať tím CSIRT o vykonanie pravidelných kontrol kľúčových sieťových infraštruktúr.

3. RIEŠENIE PROBLÉMOV, KTORÝM ČELÍ JEDNOTNÝ TRH KYBERNETICKEJ BEZPEČNOSTI V EURÓPE

Európa potrebuje kvalitné, dostupné a interoperabilné produkty a riešenia v oblasti kybernetickej bezpečnosti. Dodávka produktov a služieb v oblasti bezpečnosti IKT v rámci jednotného trhu však naďalej zostáva geograficky veľmi roztrieštená. To na jednej strane

znižuje konkurencieschopnosť európskych spoločností na vnútroštátnej, európskej a celosvetovej úrovni a na druhej strane zužuje výber životaschopných a použiteľných technológií kybernetickej bezpečnosti, ku ktorým majú občania a podniky prístup[22].

Odvetvie kybernetickej bezpečnosti v Európe sa skutočne vo veľkej miere rozvinulo vďaka dopytu národných vlád vrátane odvetvia obrany. Väčšina európskych dodávateľov v oblasti obrany si zriadila oddelenie pre kybernetickú bezpečnosť[23]. Zároveň vzniklo aj mnoho inovačných malých a stredných podnikov (MSP) na špecializovaných trhoch/trhoch pre úzke cieľové skupiny (napr. šifrovacie systémy), ako aj na etablovaných trhoch, kam prinášajú nové obchodné modely (napr. antivírusové programy).

Spoločnosti však majú ťažkosti expandovať nad rámec svojich domácich vnútroštátnych trhov. Zásadným prvkom, ktorý sa vo výraznej miere objavuje vo všetkých konzultáciách uskutočnených Komisiou[24], je nedôverovanie „cezhraničným“ riešeniam. V dôsledku toho sa veľká časť verejného obstarávania realizuje v rámci daného členského štátu a mnoho spoločností má problémy s dosiahnutím úspor v rozsahu, ktorý by im umožnili byť konkurencieschopnejšími nielen v rámci vnútorného, ale aj celosvetového trhu.

K ďalším problémom ovplyvňujúcim jednotný trh v oblasti kybernetickej bezpečnosti patrí nedostatok interoperabilných riešení (technických noriem), postupov (procesných noriem) a celoeurópskych mechanizmov certifikácie. V tejto súvislosti bola kybernetická bezpečnosť označená za jednu z priorít štandardizácie IKT na jednotnom digitálnom trhu[25].

Obmedzené perspektívy rastu spoločností zaoberajúcich sa kybernetickou bezpečnosťou v rámci jednotného trhu vedú k veľkému počtu fúzií a akvizícií mimoeurópskymi investormi[26]. Hoci táto tendencia poukazuje na inovačnú kapacitu európskych podnikateľov v oblasti kybernetickej bezpečnosti, skrýva v sebe aj určité riziko, že by mohlo dôjsť k strate európskych odborných znalostí, skúseností a úniku mozgov.

Je nutné prijať naliehavé opatrenia na podporu integrovanejšieho jednotného trhu pre produkty a služby v oblasti kybernetickej bezpečnosti, ktoré uľahčia zavedenie praktickejších a cenovo dostupnejších riešení.

Prekážky súvisiace so vzájomnou dôverou priemyselných a inštitucionálnych aktérov v Európe je možné prekonať podporovaním spolupráce v ranej fáze celého inovačného životného cyklu: v rámci odvetvia kybernetickej bezpečnosti, medzi dodávateľmi a kupujúcimi, aj medziodvetvovo zapojením odvetví, ktoré už sú alebo sa pravdepodobne stanú zákazníkmi riešení v oblasti kybernetickej bezpečnosti.

Súčasne sa stáva v Európe čoraz významnejším rozvoj dvojakého využitia produktov, služieb a technológií. Zvyšuje sa počet riešení prenesených z civilného trhu na trh obrany[27].

[22] Pozri SWD(2016) 216.
[23] Pozri SWD(2016) 216.
[24] Pozri SWD(2016) 215.
[25] COM(2016) 176/2.
[26] Pozri SWD(2016) 216.
[27] V roku 2013 predstavovala doména vývozu položiek s dvojakým využitím približne 20 % celkového vývozu EÚ (z hľadiska hodnoty). Údaj zahŕňa aj obchod v rámci EÚ.

V nadchádzajúcom akčnom pláne v oblasti európskej obrany má Komisia v úmysle určiť opatrenia na ďalšie posilnenie civilno-vojenských synergií na európskej úrovni.

3.1. Certifikácia a označovanie

Pri zvyšovaní dôveryhodnosti a bezpečnosti produktov a služieb zohráva dôležitú úlohu certifikácia. To platí aj pre nové systémy, ktoré intenzívne využívajú digitálne technológie a vyžadujú vysokú úroveň bezpečnosti, ako sú prepojené a automatizované autá, elektronické zdravotníctvo, riadiace systémy priemyselnej automatizácie (IACS) alebo inteligentné siete.

Vznikajú vnútroštátne iniciatívy, ktorých cieľom je stanoviť vysokú úroveň požiadaviek na komponenty IKT v rámci tradičnej infraštruktúry z hľadiska kybernetickej bezpečnosti vrátane požiadaviek na certifikáciu. Aj keď sú dôležité, predstavujú riziko, že povedú k roztrieštenosti jednotného trhu a k problémom s interoperabilitou. Účinné systémy certifikácie bezpečnosti produktov IKT existujú iba v niekoľkých členských štátoch[28]. Predajca IKT bude musieť zrejme absolvovať niekoľko certifikačných procesov, aby mohol predávať produkty vo viacerých členských štátoch. V najhoršom prípade nemožno produkty alebo služby, ktoré boli navrhnuté v súlade s požiadavkami na kybernetickú bezpečnosť v jednom členskom štáte, uviesť na trh v inom členskom štáte.

Na uskutočnenie fungujúceho jednotného trhu v oblasti kybernetickej bezpečnosti by sa prípadný rámec certifikácie kybernetickej bezpečnosti produktov a služieb IKT mal snažiť dosiahnuť tieto ciele: i) pokryť širšiu škálu systémov, produktov a služieb IKT; ii) zabezpečiť použiteľnosť vo všetkých 28 členských štátoch a iii) zahŕňať všetky úrovne kybernetickej bezpečnosti pri zohľadnení vývoja na medzinárodnej úrovni.

Na tento účel Komisia zriadi špecializovanú pracovnú skupinu pre certifikáciu bezpečnosti produktov a služieb IKT zloženú z odborníkov z členských štátov a odvetvia. Jej cieľom bude v spolupráci s agentúrou ENISA a so Spoločným výskumným centrom vypracovať do konca roka 2016 plán, v ktorom sa preskúma možnosť vypracovania návrhu takého európskeho rámca certifikácie bezpečnosti IKT do konca roka 2017. V tejto súvislosti Komisia zváži aj nariadenie (ES) č. 765/2008 a ustanovenia o certifikácii zahrnuté do všeobecného nariadenia o ochrane údajov 2016/679[29].

Tento proces bude zahŕňať rozsiahlu diskusiu a posúdenie vplyvu. To Komisii umožní preskúmať rôzne možnosti na vytvorenie rámca certifikácie produktov a služieb v oblasti IKT. Komisia bude skúmať aj certifikáciu bezpečnosti IKT v odvetviach infraštruktúry (napr. v letectve, železničnej doprave, automobilovom priemysle) a v rámci osobitných certifikačných a validačných mechanizmov v prípade technológií pripravených na zavedenie (napr. kybernetická bezpečnosť riadiacich systémov priemyselnej automatizácie[30], internet

[28] Pozri SWD(2016) 216, pokiaľ ide o dohodu skupiny vyšších úradníkov pre informačné systémy (rozhodnutie Rady z 31. marca 1992 (92/242/EHS) a iné existujúce systémy, napr. Commercial Product Assurance v Spojenom kráľovstve a Certification Sécuritaire de Premier Niveau vo Francúzsku.

[29] V nariadení Európskeho parlamentu a Rady (EÚ) 2016/679 z 27. apríla 2016 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov sa stanovuje kódex správania, ktorý má prispieť k riadnemu uplatňovaniu pravidiel ochrany údajov, ako aj certifikačné mechanizmy, ktoré zahŕňajú zásady ochrany údajov, najmä bezpečnosť osobných údajov pri ich spracúvaní.

[30] Pozri prípadovú štúdiu tematickej skupiny Európskej referenčnej siete pre ochranu kritickej infraštruktúry (ERNCIP) „Kybernetická bezpečnosť priemyselných riadiacich systémov“, k dispozícii na https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

vecí, cloudové služby). Bude sa zaoberať aj zistenými nedostatkami v rámci uvedeného európskeho systému certifikácie bezpečnosti IKT.

Tieto snahy súvisiace s certifikáciou budú v čo najväčšej miere vychádzať z medzinárodne uznávaných noriem a pri vývoji sa bude spolupracovať s medzinárodnými partnermi.

Komisia tiež preskúma aj možnosti, ako najlepšie integrovať certifikáciu bezpečnosti IKT do budúcich odvetvových právnych predpisov, ktoré sa týkajú aj bezpečnostných aspektov.

Odhliadnuc od prípadných regulačných možností Komisia preskúma aj vytvorenie európskeho, obchodne orientovaného, dobrovoľného a zjednodušeného systému označovania bezpečnosti produktov IKT. Okrem certifikácie sa bude zameriavať na zvýšenie zrozumiteľnosti kybernetickej bezpečnosti v komerčných produktoch s cieľom zvýšiť ich konkurencieschopnosť v rámci jednotného trhu i v celosvetovom meradle. Náležitá pozornosť sa bude venovať aj prebiehajúcim odvetvovým a horizontálnym iniciatívam v danom odvetví na strane ponuky aj dopytu.

Do tohto postupu budú úzko zapojené orgány verejnej správy, aby vo verejnom obstarávaní bolo možné používať spoločné špecifikácie a odkazovať na certifikáciu. Komisia bude zároveň monitorovať využívanie príslušných certifikačných požiadaviek v oblasti verejného obstarávania na vnútroštátnej úrovni, najmä v prípade odvetvových systémov (energetika, doprava, zdravotníctvo, verejná správa atď.) a podávať o tom správy.

Komisia

- vypracuje do konca roka 2016 plán vytvorenia návrhu európskeho rámca certifikácie bezpečnosti IKT, ktorý by mal byť predložený do konca roka 2017, a posúdi uskutočniteľnosť a vplyv európskeho ľahko použiteľného rámca na označovanie kybernetickej bezpečnosti,
- preskúma, či je potrebné zaoberať sa a prípadne riešiť nedostatky v oblasti certifikácie bezpečnosti IKT v rámci existujúcich odvetvových certifikačných/validačných mechanizmov,
- v príslušných prípadoch začlení certifikáciu bezpečnosti produktov IKT do budúcich návrhov právnych predpisov pre konkrétne odvetvia,
- bude stimulovať zapojenie orgánov verejnej správy s cieľom uľahčiť používanie certifikácie a spoločných špecifikácií vo verejnom obstarávaní a
- bude monitorovať používanie príslušných certifikačných požiadaviek v rámci verejného a súkromného obstarávania a podá správu o stave trhu za posledné tri roky.

3.2. Zvýšenie investícií do kybernetickej bezpečnosti v Európe a podpora MSP

Aj keď je inovácia v oblasti kybernetickej bezpečnosti v Európe na vzostupe, EÚ stále nemá dostatočnú kultúru investovania do oblasti kybernetickej bezpečnosti. V tejto oblasti existuje mnoho inovačných malých s stredných podnikov, často však nie sú schopné svoju činnosť rozšíriť. Dôvodom je okrem iného nedostatok ľahko dostupného financovania na ich podporu v počiatočných fázach vývoja. Podniky majú navyše obmedzený prístup k rizikovému

kapitálu v Európe a nemajú dostatok prostriedkov na marketing v záujme väčšieho zviditeľnenia alebo na riešenie rôznych súborov požiadaviek v oblasti normalizácie a súladu je nedostatočný.

Zároveň je spolupráca medzi aktérmi v oblasti kybernetickej bezpečnosti dosť nerovnomerná a je potrebné ďalšie úsilie na zvýšenie hospodárskej koncentrácie a rozvoj nových hodnotových reťazcov[31].

Na zvýšenie investícií do kybernetickej bezpečnosti v Európe a podpory MSP je potrebné uľahčiť prístup k finančným prostriedkom. Takisto je potrebné podporiť rozvoj celosvetovo konkurencieschopných klastrov a centier excelentnosti v oblasti kybernetickej bezpečnosti v regionálnych ekosystémoch priaznivých pre digitálny rast. Táto podpora musí byť spojená s uplatňovaním stratégií pre inteligentnú špecializáciu a inými nástrojmi EÚ tak, aby ich odvetvie kybernetickej bezpečnosti v Európe lepšie využívalo.

Prístup Komisie bude zameraný na maximalizáciu informovanosti kruhov v oblasti kybernetickej bezpečnosti o možnostiach financovania na európskej, vnútroštátnej a regionálnej úrovni (v súvislosti s horizontálnymi nástrojmi i osobitnými výzvami[32]) pomocou existujúcich nástrojov a kanálov, napr. siete Enterprise Europe Network.

Komisia toto úsilie doplní tým, že spolu s Európskou investičnou bankou (EIB) a Európskym investičným fondom (EIF) preskúma, ako uľahčiť prístup k financovaniu. To môže byť vo forme kapitálových a kvázi kapitálových investícií, úverov, záruk na projekty alebo protizáruk sprostredkovateľom, napr. vytvorením investičnej platformy pre oblasť kybernetickej bezpečnosti v rámci Európskeho fondu pre strategické investície[33].

Komisia sa okrem toho spolu so zainteresovanými členskými štátmi bude zaoberať vývojom platformy pre inteligentnú špecializáciu kybernetickej bezpečnosti[34]. To by pomohlo koordinovať a plánovať stratégie kybernetickej bezpečnosti a zriadiť strategickú spoluprácu zainteresovaných strán v regionálnych ekosystémoch. Tento prístup by mal pomôcť uvoľniť potenciál existujúcich európskych štrukturálnych a investičných fondov pre odvetvie kybernetickej bezpečnosti.

Vo všeobecnosti Komisia podporí prístup založený na bezpečnosti už v štádiu návrhu (security-by-design). Bude sa snažiť zabezpečiť, aby požiadavky na kybernetickú bezpečnosť boli konzistentne zohľadnené vo všetkých významných investíciách do infraštruktúry, ktoré obsahujú digitálny komponent a ktoré sú spolufinancované z európskych fondov, a to postupným zavádzaním príslušných požiadaviek do pravidiel verejného obstarávania a programov.

[31] Pozri SWD(2016) 216.

[32] Pozri napr. viacodvetvovú výzvu na predkladanie návrhov v roku 2016 v rámci programu Nástroja na prepájanie Európy a výzvy COSMO z roku 2016 týkajúce sa programu internacionalizácie klastrov.

[33] V rámci Európskeho fondu pre strategické investície môžu byť jednotlivé projekty podporované priamo alebo nepriamo prostredníctvom investičných platforiem. Tieto platformy môžu pomôcť financovať menšie projekty a združovať finančné prostriedky z rôznych zdrojov s cieľom umožniť diverzifikované investície s tematickým alebo geografickým zameraním.

[34] Pozri nástroje inteligentnej špecializácie (RIS3): http://s3platform.jrc.ec.europa.eu/.

Komisia

- bude využívať existujúce nástroje na podporu MSP s cieľom zvýšiť informovanosť o existujúcich finančných mechanizmoch v komunite kybernetickej bezpečnosti,
- ďalej zintenzívni využívanie nástrojov EÚ na podporu inovačných MSP pri skúmaní synergií medzi civilným a obranným segmentom trhu s kybernetickou bezpečnosťou[35],
- preskúma s EIB a EIF, či je realizovateľné uľahčiť prístup k investíciám, napr. cez špeciálne investičné platformy pre oblasť kybernetickej bezpečnosti alebo iné nástroje,
- vyvinie platformu pre inteligentnú špecializáciu kybernetickej bezpečnosti s cieľom pomôcť členským štátom a regiónom, ktoré majú záujem investovať do odvetvia kybernetickej bezpečnosti (RIS3) a
- podporí prístup založený na bezpečnosti už v štádiu návrhu v hlavných investíciách do infraštruktúry, ktoré majú digitálnu súčasť a sú spolufinancované z fondov EÚ.

4. STIMULOVANIE A PODPORA EURÓPSKEHO ODVETVIA KYBERNETICKEJ BEZPEČNOSTI - ZRIADENIE ZMLUVNÉHO VEREJNO-SÚKROMNÉHO PARTNERSTVA V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

S cieľom stimulovať konkurencieschopnosť a inováciu odvetvia kybernetickej bezpečnosti v Európe sa uzavrie zmluvné verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti. Toto partnerstvo bude zhromažďovať priemyselné a verejné zdroje s cieľom dosiahnuť excelentnosť vo výskume a inovácii.

Jeho cieľom je vybudovať dôveru medzi členskými štátmi a priemyselnými subjektmi rozvíjaním spolupráce v raných štádiách procesu výskumu a inovácie a takisto pomôcť zosúladiť odvetvia dopytu a ponuky. To by malo priemyslu umožniť získať budúce požiadavky od koncových používateľov a odvetví, ktorí sú dôležitými zákazníkmi v oblasti riešení kybernetickej bezpečnosti (energetika, zdravotníctvo, doprava, financie). Uľahčí to ich zapojenie do vymedzovania spoločných požiadaviek v oblasti digitálnej bezpečnosti a ochrany súkromia a údajov v ich odvetviach.

Toto partnerstvo pomôže aj maximalizovať využívanie dostupných finančných prostriedkov. To sa dosiahne po prvé väčšou koordináciou s členskými štátmi a po druhé lepším zameraním na niekoľko technických priorít s cieľom pomôcť odvetviu kybernetickej bezpečnosti, aby dosiahlo technologický pokrok a zvládlo kľúčové budúce technológie kybernetickej bezpečnosti. V tejto súvislosti môže vývoj slobodného softvéru a vývoj otvorených noriem pomôcť posilniť dôveru, transparentnosť, ako aj presadiť prelomové inovácie, a preto by mal byť taktiež súčasťou investícií do tohto zmluvného verejno-súkromného partnerstva.

Práca vykonaná v rámci zmluvného verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti bude využívať aj synergie s inými európskymi projektmi, najmä ak sa zaoberajú

[35] Napríklad sieť Enterprise Europe Network a európska sieť regiónov pôsobiacich v odvetví obrany poskytnú regiónom nové príležitosti skúmať cezhraničnú spoluprácu v oblasti dvojakého využívania vrátane kybernetickej bezpečnosti a malým a stredným podnikom možnosť zapojiť sa do sprostredkovateľských činností.

bezpečnostnými aspektmi. Patria sem verejno-súkromné partnerstvá týkajúce sa tovární budúcnosti, energeticky hospodárnych budov, 5G a veľkých dát[36] a iné odvetvové verejno-súkromné partnerstvá[37], ako aj iniciatíva Internet vecí[38]. Okrem toho sa bude podporovať úzke prepojenie s otvoreným európskym cloudom pre vedu a európskou iniciatívou supervýkonných počítačov pre kvantové kybernetické technológie (napr. inovácia v oblasti kvantovej distribúcie kľúča, výskum kvantovej výpočtovej techniky).

Zmluvné verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti sa začne v rámci programu Horizont 2020[39], rámcového programu Európskej únie pre výskum a inováciu na obdobie rokov 2014 – 2020. Využije pákový efekt financovania z dvoch pilierov tohto programu: Vedúce postavenie v podporných a priemyselných technológiách (LEIT-ICT) a Spoločenské výzvy – bezpečné spoločnosti (SC7). Jeho celkový rozpočet bude až 450 miliónov EUR s trojakým pákovým faktorom na strane priemyslu. Kybernetickú bezpečnosť je potrebné riešiť a koordinovať s ostatnými príslušnými časťami programu Horizont 2020 (napr. spoločenské výzvy v oblasti energetiky, dopravy a zdravia a časť excelentnosti programu Horizont 2020). To prispeje k cieľom zmluvného verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti. Táto koordinácia by sa mala realizovať aj vopred, vo fáze navrhovania odvetvových stratégií.

Zmluvné verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti bude implementované transparentným spôsobom, s otvoreným a pružným riadením prispôsobeným rýchlo sa meniacemu prostrediu kybernetickej bezpečnosti. Zohľadní potrebu členských štátov diskutovať o vplyvoch technologických zmien na bezpečnú prevádzku vnútroštátnych a cezhraničných infraštruktúr. Výstup partnerstva musí byť udržateľný niekoľko rokov, aby sa zabezpečilo splnenie jeho cieľov.

Zmluvné verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti bude podporovať Európska organizácia kybernetickej bezpečnosti (ECSO), ktorej členstvo bude odrážať rôznorodosť trhu v oblasti kybernetickej bezpečnosti v Európe. Bude zahŕňať aj vnútroštátne, regionálne a miestne orgány verejnej správy, výskumné strediská a akademickú obec, a ďalšie zainteresované strany.

Komisia

- uzavrie s priemyslom zmluvné verejno-súkromné partnerstvo v oblasti kybernetickej bezpečnosti, aby začalo fungovať v treťom štvrťroku 2016,
- zverejní výzvy na predkladanie návrhov týkajúce sa zmluvného verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti v rámci programu Horizont 2020 v prvom štvrťroku 2017 a
- zabezpečí koordináciu zmluvného verejno-súkromného partnerstva v oblasti kybernetickej bezpečnosti s relevantnými odvetvovými stratégiami, nástrojmi programu Horizont 2020 a odvetvovými verejno-súkromnými partnerstvami.

[36] Verejno-súkromné partnerstvo pre infraštruktúru 5G a verejno-súkromné partnerstvo hodnoty veľkých dát.
[37] Napríklad verejno-súkromné partnerstvá SESAR alebo Shift to Rail (Prechod na železnicu).
[38] Aliancie pre inovácie v kontexte internetu vecí (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

5. ZÁVER

Toto oznámenie predkladá opatrenia zamerané na posilnenie odolnosti kybernetického systému v Európe a podporu konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe, ako sa uvádza v stratégii kybernetickej bezpečnosti EÚ a v stratégii pre jednotný digitálny trh. Komisia vyzýva Európsky parlament a Radu, aby tento prístup podporili.