EURÓPSKA KOMISIA

VYSOKÁ PREDSTAVITEĽKA
EURÓPSKEJ ÚNIE PRE
ZAHRANIČNÉ VECI
A BEZPEČNOSTNÚ POLITIKU

V Bruseli 7. 2. 2013
JOIN(2013) 1 final

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

Stratégia kybernetickej bezpečnosti Európskej únie:

Otvorený, bezpečný a chránený kybernetický priestor

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

Stratégia kybernetickej bezpečnosti Európskej únie:

Otvorený, bezpečný a chránený kybernetický priestor

1. ÚVOD

1.1. Súvislosti

Počas posledných dvoch desaťročí internet a v širšom meradle kybernetický priestor nesmierne ovplyvnil všetky vrstvy spoločnosti. Náš každodenný život, základné práva, sociálna interakcia a hospodárstvo závisia od bezproblémového fungovania informačných a komunikačných technológií. Otvorený a slobodný kybernetický priestor podporil politické a sociálne začlenenie v celosvetovom meradle; odstránil prekážky medzi krajinami, komunitami a občanmi a umožnil globálnu interakciu a výmenu informácií; poskytol fórum na slobodu prejavu a výkon základných práv a dal ľuďom možnosť dôraznejšie sa dožadovať demokratickej a spravodlivejšej spoločnosti – čo sa najvýraznejšie prejavilo počas Arabskej jari.

Aby kybernetický priestor zostal otvorený a slobodný, rovnaké normy, zásady a hodnoty, aké EÚ podporuje mimo internetu, by sa mali uplatňovať aj na internete. V kybernetickom priestore treba chrániť základné práva, demokraciu a zákonnosť. Naša sloboda a prosperita v čoraz väčšej miere závisia od spoľahlivého a inovačného internetu, ktorý sa bude naďalej rozvíjať, ak inovácie súkromného sektora a občianska spoločnosť podporia jeho rast. Ale aj online sloboda vyžaduje bezpečnosť a ochranu. Kybernetický priestor by mal byť chránený pred incidentmi, škodlivými činnosťami a zneužívaním; a vlády plnia významnú úlohu pri zabezpečovaní slobodného a bezpečného kybernetického priestoru. Vlády majú niekoľko úloh: zabezpečiť prístup a otvorenosť, rešpektovať a chrániť základné práva online a udržiavať spoľahlivosť a interoperabilitu internetu. Významný podiel kybernetického priestoru však vlastní a prevádzkuje súkromný sektor, a preto všetky iniciatívy, ktoré chcú byť v tejto oblasti úspešné, musia uznávať jeho vedúcu úlohu.

Informačné a komunikačné technológie sa stali hlavnou oporou nášho hospodárskeho rastu a rozhodujúcim zdrojom, o ktorý sa opierajú všetky sektory hospodárstva. Sú základom komplexných systémov, ktoré udržiavajú naše hospodárstva v chode v kľúčových sektoroch, ako sú financie, zdravotníctvo, energetika a doprava. Pritom mnohé podnikateľské modely sú postavené na nepretržitej dostupnosti internetu a hladkom fungovaní informačných systémov.

Dokončením jednotného digitálneho trhu by Európa mohla zvýšiť svoj HDP o takmer 500 miliárd EUR ročne[1]; to znamená priemer 1000 EUR na osobu. Pre rozbeh nových prepojených technológií vrátane elektronických platieb, cloud computingu alebo komunikácie medzi strojmi[2] bude potrebné, aby im občania dôverovali a mali pri nich pocit istoty. Žiaľ, jeden z prieskumov Eurobarometra za rok 2012[3] naznačil, že takmer tretina Európanov nedôveruje svojim schopnostiam využívať internet na bankové operácie alebo nákupy. Drvivá

[1] http://www.epc.eu/dsm/2/Study_by_Copenhagen.pdf.

[2] Napríklad rastliny vybavené snímačmi, ktoré oznámia zavlažovaciemu systému, kedy ich treba zaliať.

[3] 2012 Špeciálny Eurobarometer 390 o kybernetickej bezpečnosti.

väčšina okrem toho uviedla, že sa vyhýba prezrádzaniu osobných informácií online v dôsledku obáv o bezpečnosť. V celej EÚ sa už najmenej každý desiaty z používateľov internetu už stal obeťou online podvodu.

V posledných rokoch sa ukazuje, že hoci digitálny svet prináša obrovské výhody, je aj zraniteľný. Incidenty v rámci kybernetickej bezpečnosti[4], či už úmyselné, alebo náhodné, narastajú alarmujúcim tempom a mohli by narušiť poskytovanie základných služieb, ktoré považujeme za samozrejmé, ako je zásobovanie vodou, zdravotná starostlivosť, dodávka elektrickej energie alebo mobilné služby. Hrozby môžu mať rôzny pôvod – vrátane zločineckých, politicky motivovaných, teroristických alebo štátom podporovaných útokov, ako aj prírodných katastrof a neúmyselných chýb.

Hospodárstvo EÚ je už ovplyvňované činnosťami kybernetickej kriminality[5] zameranými na súkromný sektor a jednotlivcov. Kybernetickí zločinci používajú čoraz sofistikovanejšie metódy na neoprávnený prístup k informačným systémom, krádeže kritických údajov alebo požadovanie výkupného od spoločností. Nárast hospodárskej špionáže a štátom podporovaných činností v kybernetickom priestore predstavujú novú kategóriu hrozieb pre vlády a spoločnosti v EÚ.

V krajinách mimo EÚ môžu vlády tiež zneužívať kybernetický priestor na dohľad a kontrolu nad vlastnými občanmi. EÚ môže čeliť tejto situácii presadzovaním slobody a zabezpečovaním dodržiavania základných práv v online prostredí.

Všetky tieto faktory vysvetľujú, prečo vlády na celom svete začali vyvíjať stratégie kybernetickej bezpečnosti a uvažovať o kybernetickom priestore ako o čoraz dôležitejšom medzinárodnom probléme. Nadišiel čas, aby EÚ zintenzívnila svoju činnosť v tejto oblasti. Tento návrh stratégie kybernetickej bezpečnosti Európskej únie, ktorý predložila Komisia a vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku a podpredsedníčka Komisie (ďalej len „vysoká predstaviteľka“), načrtáva víziu EÚ v tejto oblasti, objasňuje úlohy a zodpovednosti a stanovuje opatrenia, ktoré sa vyžadujú na základe silnej a účinnej ochrany a podpory práv občanov na to, aby sa online prostredie EÚ stalo najbezpečnejším na svete.

1.2. Zásady kybernetickej bezpečnosti

Bezhraničný a mnohovrstevný internet sa stal jedným z najúčinnejších nástrojov pre celosvetový pokrok bez vládnej kontroly alebo regulácie. Aj keď súkromný sektor by mal naďalej zohrávať vedúcu úlohu pri budovaní a každodennom riadení internetu, potreba zaviesť požiadavky týkajúce sa transparentnosti, zodpovednosti a bezpečnosti je čoraz významnejšia. Táto stratégia objasňuje zásady, ktorými by sa mala riadiť politika kybernetickej bezpečnosti v EÚ a na medzinárodnej úrovni.

---

[4] Kybernetická bezpečnosť sa všeobecne vzťahuje na bezpečnostné záruky a opatrenia, ktoré možno použiť na ochranu kybernetickej domény, tak v civilnej, ako aj vojenskej oblasti, pred hrozbami, ktoré sa týkajú jej vzájomne závislých sietí a informačných infraštruktúr alebo ktoré ich môžu poškodiť. Kybernetická bezpečnosť sa snaží zachovať dostupnosť a integritu sietí a infraštruktúry a dôvernosť informácií, ktoré sú v nich obsiahnuté.

[5] Pojem kybernetická kriminalita (alebo počítačová trestná činnosť) sa zvyčajne vzťahuje na širokú škálu trestnej činnosti, v rámci ktorej sú počítače a informačné systémy buď primárne nástroje alebo primárne ciele. Kybernetická kriminalita zahŕňa tradičné trestné činy (napr. podvod, falšovanie a krádež totožnosti), trestné činy súvisiace s obsahom (napr. online distribúcia detskej pornografie alebo podnecovanie k rasovej nenávisti) a trestné činy špecifické pre počítače a informačné systémy (napr. útok na informačné systémy, odopretie služby a škodlivý softvér).

Základné hodnoty EÚ platia rovnako v digitálnom, ako aj vo fyzickom svete

Tie isté zákony a normy, ktoré sa uplatňujú v iných oblastiach nášho každodenného života, sa uplatňujú aj v kybernetickej doméne.

Ochrana základných práv, slobody prejavu, osobných údajov a súkromia

Kybernetická bezpečnosť môže byť riadna a účinná, len ak je založená na základných právach a slobodách, ktoré sú zakotvené v Charte základných práv Európskej únie, a základných hodnotách EÚ. A naopak, práva jednotlivcov nie je možné zaistiť bez bezpečných sietí a systémov. Akékoľvek zdieľanie informácií na účely kybernetickej bezpečnosti, keď sú v hre osobné údaje, by malo byť v súlade s právnymi predpismi EÚ o ochrane údajov a malo by plne zohľadňovať práva jednotlivcov v tejto oblasti.

Prístup pre všetkých

Obmedzený alebo žiadny prístup na internet a digitálna negramotnosť predstavujú nevýhody pre občanov, vzhľadom na to, ako veľmi digitálny svet preniká do činností v rámci spoločnosti. Každý by mal mať prístup k internetu a k neobmedzenému toku informácií. Integrita a bezpečnosti internetu musí byť zaručená, aby sa umožnil bezpečný prístup pre všetkých.

Demokratické a efektívne mnohostranné riadenie

Digitálny svet nepodlieha kontrole jediného subjektu. V súčasnosti existuje niekoľko zainteresovaných strán, pričom mnohé sú komerčné a mimovládne subjekty, ktoré sa podieľajú na každodennom riadení internetových zdrojov, protokolov a noriem, ako aj na budúcom rozvoji internetu. EÚ opätovne potvrdzuje dôležitosť všetkých zainteresovaných strán v súčasnej podobe modelu riadenia internetu a podporuje tento mnohostranný prístup k riadeniu[6].

Spoločná zodpovednosť za zaistenie bezpečnosti

Rastúca závislosť od informačných a komunikačných technológií vo všetkých oblastiach ľudského života viedla k odhaleniu slabých miest, ktoré musia byť náležite definované, dôkladne analyzované a odstránené alebo obmedzené. Všetky relevantné subjekty, či už verejné orgány, súkromný sektor alebo jednotliví občania, musia uznať túto spoločnú zodpovednosť, prijať opatrenia na vlastnú ochranu a v prípade potreby zaistiť koordinovanú reakciu s cieľom posilniť kybernetickú bezpečnosť.

2. STRATEGICKÉ PRIORITY A OPATRENIA

EÚ by mala chrániť online prostredie a pritom poskytovať všetkým najvyššiu možnú slobodu a bezpečnosť. Hoci uznáva, že riešenie bezpečnostných výziev v kybernetickom priestore je predovšetkým úlohou členských štátov, táto stratégia navrhuje konkrétne opatrenia, ktoré môžu prispieť k zvýšeniu celkovej výkonnosti EÚ Sú to krátkodobé i dlhodobé opatrenia

[6] Pozri tiež KOM (2009) 277, oznámenie Komisie Európskemu parlamentu a Rade „ Správa internetu: Ďalšie kroky“.

zahŕňajúce celý rad politických nástrojov[7] a dotýkajúce sa rôznych druhov aktérov, či ide o inštitúcie EÚ, členské štáty alebo priemyselné odvetvie.

Vízia EÚ prezentovaná v tejto stratégii je sformulovaná do piatich strategických priorít, ktoré riešia problémy uvedené vyššie:

- Dosiahnutie kybernetickej odolnosti
- Radikálne zníženie kybernetickej kriminality
- Rozvoj politiky a spôsobilostí kybernetickej obrany v súvislosti so spoločnou bezpečnostnou a obrannou politikou (SBOP)
- Rozvoj priemyselných a technologických zdrojov pre kybernetickú bezpečnosť
- Vytvorenie koherentnej medzinárodnej politiky kybernetického priestoru Európskej únie a podpora kľúčových hodnôt EÚ

2.1. Dosiahnutie kybernetickej odolnosti

Na podporu kybernetickej odolnosti v EÚ verejné orgány a súkromný sektor musia rozvíjať spôsobilosti a účinne spolupracovať. V nadväznosti na pozitívne výsledky dosiahnuté prostredníctvom činností, ktoré boli do dnešného dňa vykonané[8], ďalšie opatrenia EÚ môžu pomôcť najmä zamedziť kybernetickým rizikám a hrozbám, ktoré majú cezhraničný rozmer, a prispieť ku koordinovanej reakcii v núdzových situáciách. Toto výrazne podporí dobré fungovanie vnútorného trhu a posilní vnútornú bezpečnosť EÚ.

Európa bude aj naďalej zraniteľná, ak nevyvinie značné úsilie na posilnenie verejných a súkromných kapacít, zdrojov a procesov s cieľom predchádzať incidentom v oblasti kybernetickej bezpečnosti, prípadne ich odhaľovať a riešiť ich následky. To je dôvod, prečo Komisia navrhla politiku v oblasti bezpečnosti sietí a informácií (NIS)[9]. **Európska agentúra pre bezpečnosť sietí a informácií ENISA** bola založená v roku 2004[10] a Rada a Parlament rokujú o novom nariadení na posilnenie agentúry ENISA a modernizáciu jej mandátu[11]. Okrem toho sa v rámcovej smernici pre elektronické komunikačné siete a služby[12] vyžaduje, aby poskytovatelia elektronických komunikácií primerane riadili riziká, ktoré hrozia ich sieťam, a informovali o každom narušení bezpečnosti, ktoré malo významný vplyv. V právnych predpisoch EÚ o ochrane údajov[13] sa vyžaduje aj to, aby prevádzkovatelia zaistili všetky požiadavky a záruky ochrany údajov vrátane opatrení súvisiacich s bezpečnosťou, a v oblasti verejne dostupných elektronických komunikačných služieb prevádzkovatelia musia oznamovať incidenty týkajúce sa porušenia osobných údajov príslušným vnútroštátnym orgánom.

---

7 Opatrenia súvisiace so zdieľaním informácií, ktoré sa týkajú osobných údajov, by mali byť v súlade s právnymi predpismi EÚ o ochrane údajov.

8 Pozri odkazy v tomto oznámení, ako aj v pracovnom dokumente útvarov Komisie Hodnotenie vplyvu, ktorý je pripojený k návrhu Komisie na smernicu o bezpečnosti sietí a informácií, najmä odseky 4.1.4, 5.2, príloha 2, príloha 6, príloha 8,

9 V roku 2001 Komisia prijala oznámenie „Bezpečnosť sietí a informácií: Návrh európskeho politického prístupu“ (KOM (2001) 298); v roku 2006 prijala stratégiu pre bezpečnú informačnú spoločnosť (KOM (2006) 251). Od roku 2009 Komisia prijala aj plán opatrení a oznámenie o ochrane kritickej informačnej infraštruktúry (CIIP) **(**KOM(2009)149, ktoré schválila Rada uznesením 2009/C 321/01; a KOM(2011)163, schválený v záveroch Rady 10299/11).

10 Nariadenie (EÚ) č. 460/2004.

11 KOM(2010) 521. Opatrenia navrhnuté v tejto stratégii nemajú za následok zmenu a doplnenie súčasného alebo budúceho mandátu agentúry ENISA.

12 Články 13a a 13b smernice 2002/21/ES.

13 Článok 17 smernice 95/46/ES; článok 4 smernice 2002/58/ES.

Napriek pokroku, ktorý sa zakladá na dobrovoľných záväzkoch, naďalej existujú medzery v celej EÚ, najmä pokiaľ ide o národné spôsobilosti, koordináciu v prípadoch incidentov presahujúcich hranice a zapojenie súkromného sektora a jeho pripravenosť. K tejto stratégii je pripojený **legislatívny návrh**, ktorý umožní najmä:

- stanoviť spoločné minimálne požiadavky na bezpečnosť sietí a informácií na vnútroštátnej úrovni, ktoré by od členských štátov vyžadovali, aby: určili príslušné vnútroštátne orgány pre bezpečnosť sietí a informácií; vytvorili riadne fungujúci tím CERT; a prijali vnútroštátnu stratégiu bezpečnosti sietí a informácií a národný plán spolupráce v oblasti bezpečnosti sietí a informácií. Budovanie kapacít a koordinácia sa týkajú aj inštitúcií EÚ: Tím reakcie na núdzové počítačové situácie zodpovedný za bezpečnosť IT systémov inštitúcií, agentúr a orgánov EÚ („CERT-EU“) bol permanentne zriadený v roku 2012.
- zaviesť koordinované mechanizmy v rámci prevencie, odhaľovania, zmierňovania a reakcie, čo umožní zdieľanie informácií a vzájomnú pomoc medzi jednotlivými vnútroštátnymi orgánmi príslušnými pre oblasť bezpečnosti sietí a informácií. Od vnútroštátnych orgánov príslušných pre oblasť bezpečnosti sietí a informácií sa bude požadovať, aby zabezpečili vhodnú spoluprácu v rámci celej EÚ, a to najmä na základe plánu spolupráce v oblasti bezpečnosti sietí a informácií na úrovni Únie, zameraného na reakcie na kybernetické incidenty s cezhraničným rozmerom. Táto spolupráca bude vychádzať aj z pokroku dosiahnutého v kontexte „Európskeho fóra pre členské štáty (EFMS)“[14], na ktorom prebehli produktívne diskusie a výmeny názorov o verejnej politike v oblasti bezpečnosti sietí a informácií, a možno ju integrovať do mechanizmu spolupráce po jeho zriadení.
- zlepšiť pripravenosť a zapojenie súkromného sektora. Keďže veľká väčšina sietí a informačných systémov je v súkromnom vlastníctve a súkromne prevádzkovaná, je nevyhnutné zlepšiť spoluprácu na podpore kybernetickej bezpečnosti so súkromným sektorom. Súkromný sektor by mal rozvíjať na technickej úrovni svoje vlastné kapacity kybernetickej odolnosti a zdieľať najlepšie postupy v rámci sektorov. Nástroje vytvorené priemyselným odvetvím ako prostriedky reakcie na incidenty, identifikácie príčin a vedenia forenzného vyšetrovania by mali prinášať prospech aj verejnému sektoru.

Súkromné subjekty však stále nepociťujú účinné stimuly na poskytovanie spoľahlivých údajov o existencii alebo následkoch incidentov spojených s bezpečnosťou sietí a informácií, na osvojenie si kultúry riadenia rizika alebo na investovanie do bezpečnostných riešení. Navrhovaný právny predpis je preto zameraný na zabezpečenie toho, aby aktéri v niekoľkých kľúčových oblastiach (najmä v oblasti energetiky, dopravy, bankovníctva, búrz cenných papierov a podpory kľúčových internetových služieb, ako aj vo verejnej správe) posudzovali riziká kybernetickej bezpečnosti, ktorým sú vystavení, zabezpečili spoľahlivosť a odolnosť sietí a informačných systémov prostredníctvom vhodného riadenia rizík a zdieľali identifikované informácie s vnútroštátnymi orgánmi príslušnými pre oblasť bezpečnosti sietí a informácií. Zavádzanie kultúry kybernetickej bezpečnosti by mohlo zlepšiť podnikateľské príležitosti a konkurencieschopnosť v súkromnom sektore, čo by z kybernetickej bezpečnosti mohlo urobiť zaujímavý predajný artikel.

Tieto subjekty by museli hlásiť vnútroštátnym orgánom príslušným pre oblasť bezpečnosti sietí a informácií incidenty s výrazným vplyvom na kontinuitu základných služieb a dodávok tovaru opierajúcich sa o siete a informačné systémy.

[14] Európske fórum pre členské štáty sa vytvorilo na základe dokumentu KOM(2009) 149 ako platforma na podporu diskusie medzi verejnými orgánmi členských štátov o osvedčených politických postupoch týkajúcich sa bezpečnosti a odolnosti kritickej informačnej infraštruktúry.

Vnútroštátne orgány príslušné pre oblasť bezpečnosti sietí a informácií by mali spolupracovať a vymieňať si informácie s inými regulačnými orgánmi, a to najmä s orgánmi na ochranu osobných údajov. Orgány príslušné pre oblasť bezpečnosti sietí a informácií by zase mali oznamovať incidenty, pri ktorých existuje podozrenie o ich závažnom trestnom charaktere, orgánom presadzovania práva. Príslušné vnútroštátne orgány by taktiež mali pravidelne zverejňovať na osobitnej internetovej stránke neutajované skutočnosti o aktuálnych včasných varovaniach o incidentoch a rizikách a o koordinovaných reakciách. Právne záväzky by sa nemali stávať náhradou ani prekážkou rozvíjajúcej sa neformálnej a dobrovoľnej spolupráce, vrátane spolupráce medzi verejným a súkromným sektorom, s cieľom zvýšiť úroveň bezpečnosti a vymieňať si informácie a najlepšie postupy. Najmä Európske verejno-súkromné partnerstvo pre odolnosť (EP3R)[15] je vhodná a spoľahlivá platforma na úrovni EÚ a malo by sa ďalej rozvíjať.

Nástroj „ Spájame Európu “ (CEF)[16] by poskytol finančnú podporu pre kľúčové infraštruktúry spájajúce schopnosti členských štátov v oblasti bezpečnosti sietí a informácií, a tak uľahčil spoluprácu v celej EÚ.

Napokon, cvičenia s témou kybernetických incidentov na úrovni EÚ sú nevyhnutné na simuláciu spolupráce medzi členskými štátmi a súkromným sektorom. Prvé cvičenie, na ktorom sa zúčastnili členské štáty, prebehlo v roku 2010 („Kybernetická Európa 2010“) a druhé cvičenie, na ktorom sa zúčastnil aj súkromný sektor, sa konalo v októbri 2012 („Kybernetická Európa 2012“). Simulované cvičenie EÚ-USA sa uskutočnilo v novembri 2011 („Kybernetický Atlantik 2011“). Ďalšie cvičenia vrátane cvičení s medzinárodnými partnermi sú naplánované na nasledujúce roky.

Komisia:

- Bude pokračovať vo svojich činnostiach, ktoré vykonáva Spoločné výskumné centrum v úzkej spolupráci s orgánmi členských štátov a majiteľmi a prevádzkovateľmi kritickej infraštruktúry v oblasti bezpečnosti sietí a informácií, pri určovaní slabých stránok európskej kritickej infraštruktúry a podporovať rozvoj odolných systémov.
- Začiatkom roku 2013 spustí pilotný projekt financovaný EÚ[17] zaoberajúci sa **bojom proti botnetom a škodlivému softvéru (malware)** s cieľom poskytnúť rámec pre koordináciu a spoluprácu medzi členskými štátmi EÚ, organizáciami súkromného sektora, ako sú napríklad poskytovatelia internetových služieb, a medzinárodnými partnermi.

Komisia žiada agentúru ENISA, aby:

- Pomáhala členským štátom pri rozvíjaní silnej **vnútroštátnej kybernetickej**

[15] Európske verejno-súkromné partnerstvo pre odolnosť sa začalo realizovať na základe dokumentu KOM(2009) 149. Táto platforma iniciovala činnosť a podporila spoluprácu medzi verejným a súkromným sektorom, pokiaľ ide o identifikáciu kľúčových prostriedkov, zdrojov, funkcií a základných požiadaviek na odolnosť systémov, ako aj potreby spolupráce a mechanizmy reakcie na rozsiahle narušenia ovplyvňujúce elektronickú komunikáciu.

[16] https://ec.europa.eu/digital-agenda/en/connecting-europe-facility. CEF, rozpočtová položku 09.03.02 – telekomunikačné siete (na podporu vzájomného prepojenia a súčinnosti národných verejných služieb online, ako aj prístupu do týchto sietí).

[17] CIP-ICT PSP-2012-6, 325188. Celkový rozpočet je 15 mil. EUR, pričom finančné prostriedky EÚ dosahujú 7,7 mil. EUR.

odolnosti, predovšetkým prostredníctvom budovania odborných znalostí v oblasti bezpečnosti a odolnosti priemyselných kontrolných systémov, dopravy a energetickej infraštruktúry.

- V roku 2013 preskúmala možnosti vytvorenia tímov reakcie na núdzové počítačové situácie pre priemyselné kontrolné systémy (ICS-CSIRT) pre EÚ.
- Naďalej podporovala členské štáty a inštitúcie EÚ pri vykonávaní pravidelných **celoeurópskych cvičení na tému riešenia kybernetických incidentov**, ktoré budú zároveň predstavovať prevádzkovú základňu pre účasť EÚ na medzinárodných cvičeniach na tému riešenia kybernetických incidentov.

Komisia vyzýva Európsky parlament a Radu, aby:

- Urýchlene prijali návrh smernice o **spoločnej vysokej úrovni bezpečnosti sietí a informácií (NIS)** v celej Únii, ktorá sa zaoberá spôsobilosťami a pripravenosťou na vnútroštátnej úrovni, spoluprácou na úrovni EÚ, zavádzaním postupov riadenia rizika a zdieľaním informácií o NIS.

Komisia vyzýva priemyselné odvetvie, aby:

- Prevzalo vedúce postavenie pri **investovaní** do vysokej úrovne kybernetickej bezpečnosti a rozvíjaní najlepších postupov a spoločného využívania informácií na úrovni sektora a s verejnými orgánmi s cieľom zabezpečiť silnú a účinnú ochranu majetku a osôb, najmä cez verejno-súkromné partnerstvá, akými sú napríklad EP3R a Dôvera v digitálny život (TDL, z angl. Trust in Digital Life)[18].

Zvyšovanie informovanosti

Zabezpečenie kybernetickej bezpečnosti je spoločnou zodpovednosťou. Koncoví používatelia zohrávajú kľúčovú úlohu pri zaisťovaní bezpečnosti sietí a informačných systémov: Je potrebné, aby si uvedomovali, akým rizikám sú vystavení online, a mali možnosť podniknúť jednoduché opatrenia na ochranu pred nimi.

V posledných rokoch sa rozvinulo niekoľko iniciatív a malo by sa v nich naďalej pokračovať. ENISA sa predovšetkým podieľala na zvyšovaní informovanosti prostredníctvom uverejňovania správ, organizovania odborných seminárov a rozvíjania verejno-súkromných partnerstiev. Europol, Eurojust a národné orgány na ochranu údajov taktiež aktívne prispievajú k zvyšovaniu informovanosti. V októbri 2012 ENISA s niektorými členskými štátmi realizovala pilotnú akciu „Európsky mesiac kybernetickej bezpečnosti“. Zvyšovanie informovanosti je jednou z oblastí, v ktorých pracovná skupina EÚ-USA pre kybernetickú bezpečnosť a kybernetickú kriminalitu[19] dosahuje pokroky a ktorá je takisto dôležitá v súvislosti s programom Bezpečnejší internet[20] (zameraný na bezpečnosť detí na internete).

---

18 http://www.trustindigitallife.eu/.

19 Táto pracovná skupina, zriadená na samite EÚ-USA v novembri 2010 (MEMO/10/597) je poverená vypracovaním kolaboratívnych prístupov k širokej škále otázok kybernetickej bezpečnosti a kybernetickej kriminality.

20 Z programu bezpečnejší internet sa financuje sieť mimovládnych organizácií činných v oblasti starostlivosti o deti online, sieť orgánov presadzovania práva, ktoré si navzájom vymieňajú informácie a najlepšie postupy týkajúce sa kriminálneho využívania internetu na šírenia materiálov obsahujúcich pohlavné zneužívanie detí a sieť výskumných pracovníkov, ktorí zbierajú informácie o používaní online technológií, ich rizikách a ich dôsledkoch pre život detí.

Komisia žiada agentúru ENISA, aby:

- Navrhla v roku 2013 plán zameraný na vytvorenie „vodičského preukazu pre oblasť bezpečnosti sietí a informácií“ ako dobrovoľného certifikačného programu na podporu zlepšovania zručností a schopností IT odborníkov (napr. administrátorov webových sídel).

Komisia:

- Za podpory agentúry ENISA v roku 2014 zorganizuje **šampionát** kybernetickej bezpečnosti, na ktorom budú univerzitní študenti súťažiť v navrhovaní riešení pre oblasť bezpečnosti sietí a informácií.

Komisia vyzýva členské štáty[21], aby:

- Od roku 2013 každoročne organizovali **mesiac kybernetickej bezpečnosti** s podporou agentúry ENISA a zapojením súkromného sektora , s cieľom zvyšovať informovanosť koncových používateľov. Synchronizovaný mesiac kybernetickej bezpečnosti EÚ-USA sa začne organizovať v roku 2014.
- **Zintenzívnili svoje úsilie zamerané na vzdelávanie a odbornú prípravu v oblasti bezpečnosti sietí a informácií**, a to zavedením odbornej prípravy v oblasti bezpečnosti sietí a informácií v školách do roku 2014; odbornej prípravy v oblasti bezpečnosti sietí a informácií a zabezpečením vývoja softvéru a ochrany osobných údajov pre študentov informatiky; a základnej odbornej prípravy v oblasti NIS pre zamestnancov vo verejnej správe.

Komisia vyzýva priemyselné odvetvie, aby:

- Podporilo **informovanosť** o kybernetickej bezpečnosti **na všetkých úrovniach**, a to tak v podnikateľských postupoch ako aj vo vzťahu k zákazníkom. Priemyselné odvetvie by sa najmä malo zamerať na spôsoby, ako dosiahnuť väčšiu zodpovednosť generálnych riaditeľov a správnych rád za zaistenie kybernetickej bezpečnosti.

2.2. Radikálne zníženie kybernetickej kriminality

Čím dlhšie žijeme v digitálnom svete, tým viac príležitostí sa ponúka pre kybernetických zločincov. Kybernetická kriminalita je jednou z najrýchlejšie rastúcich foriem trestnej činnosti, pričom každý deň sa stane jej obeťou viac ako milión ľudí na celom svete. Sofistikovanosť kybernetických zločincov a sietí kybernetického zločinu rastie a na ich riešenie potrebujeme správne operatívne nástroje a kapacity. Kybernetická kriminalita je vysoko zisková a vyznačuje sa nízkym rizikom, pričom zločinci často zneužívajú anonymitu webových domén. Kybernetická kriminalita nepozná hranice – globálny dosah internetu znamená, že pri presadzovaní práva sa musí prijať koordinovaný prístup k cezhraničnej spolupráci, ktorá bude schopná reagovať na túto rastúcu hrozbu.

Silné a účinné právne predpisy

[21] Aj za účasti príslušných vnútroštátnych orgánov vrátane orgánov príslušných pre oblasť bezpečnosti sietí a informácií a orgánov na ochranu údajov.

EÚ a členské štáty potrebujú silné a účinné právne predpisy na boj proti kybernetickej kriminalite. Dohovor Rady Európy o kybernetickej kriminalite známy ako Budapeštiansky dohovor je záväzná medzinárodná dohoda, ktorá poskytuje účinný rámec na prijímanie vnútroštátnych právnych predpisov.

EÚ už prijala právne predpisy o kybernetickej kriminalite vrátane smernice o boji proti pohlavnému zneužívaniu detí na internete a detskej pornografii[22]. EÚ sa však už čoskoro dohodne na smernici o útokoch na informačné systémy, najmä s využitím botnetov.

Komisia:

- Zabezpečí rýchlu transpozíciu a implementáciu smerníc vzťahujúcich sa na kybernetickú kriminalitu.
- Vyzve tie členské štáty, ktoré ešte neratifikovali **Budapeštiansky dohovor Rady Európy o kybernetickej kriminalite**, aby ho ratifikovali a implementovali jeho ustanovenia čo najskôr.

Posilnenie operačnej spôsobilosti na boj proti kybernetickej kriminalite

Vývoj techník kybernetickej kriminality sa rapídne zrýchlil: Orgány presadzovania práva nemôžu bojovať proti kybernetickej kriminalite zastaranými operatívnymi nástrojmi. V súčasnosti všetky členské štáty EÚ nemajú operačné spôsobilosti potrebné na účinné reagovanie na kybernetickú kriminalitu. Všetky členské štáty potrebujú účinné národné jednotky na boj proti kybernetickej kriminalite.

Komisia:

- Prostredníctvom svojich programov financovania[23] podporí členské štáty **pri odhaľovaní medzier a pri posilňovaní spôsobilosti** vyšetrovať prípady kybernetickej kriminality a bojovať proti nej. Komisia bude okrem toho podporovať subjekty, ktoré vytvárajú prepojenie medzi výskumným a akademickým prostredím, praktickými vykonávateľmi presadzovania práva a súkromným sektorom, podobným spôsobom, akým to už funguje v centrách excelentnosti pre kybernetickú kriminalitu, ktoré financuje Komisia a ktoré sa už zriadili v niektorých členských štátoch.
- Spolu s členskými štátmi a aj s podporou Spoločného výskumného centra bude koordinovať úsilie o identifikáciu najlepších postupov a najlepších dostupných techník boja proti kybernetickej kriminalite (napr. pokiaľ ide o rozvoj a využívanie forenzných nástrojov alebo analýzy ohrozenia).
- Bude úzko spolupracovať s nedávno vytvoreným **Európskym centrom pre kybernetickú kriminalitu (EC3)** v rámci Europolu a spolu s Eurojustom, pričom cieľom je zosúladiť tieto politické prístupy s najlepšími postupmi v operatívnej činnosti.

[22] Smernica 2011/93/EÚ, ktorou sa nahrádza rámcové rozhodnutie Rady 2004/68/SVV.

[23] V roku 2013 v rámci programu Predchádzanie trestnej činnosti a boj proti nej (ISEC). Po roku 2013 v rámci fondu vnútornej bezpečnosti (nový nástroj v rámci VFR).

Zlepšená koordinácia na úrovni EÚ

EÚ môže dopĺňať činnosť členských štátov uľahčovaním koordinovaného a kolaboratívneho prístupu, spájajúceho orgány presadzovania práva a justičné orgány s verejnými a súkromnými zainteresovanými stranami z EÚ i mimo nej.

Komisia:

- Podporí nedávno otvorené **Európske centrum pre kybernetickú kriminalitu** (EC3) ako európsky ohniskový bod boja proti kybernetickej kriminalite. EC3 bude poskytovať analýzy a vyvíjať spravodajskú činnosť, podporovať vyšetrovania, zabezpečovať vysokú úroveň forenzných techník, uľahčovať spoluprácu, vytvárať kanály na výmenu informácií medzi príslušnými orgánmi členských štátov, súkromným sektorom a inými zainteresovanými stranami a postupne slúžiť ako hlas komunity zaoberajúcej sa presadzovaním práva[24].
- Bude podporovať snahy o zvýšenie zodpovednosti registrátorov názvov domén a zabezpečovať presnosť informácií o vlastníctve webových sídel predovšetkým na základe odporúčaní na presadzovanie práva pre Internetovú spoločnosť pre prideľovanie mena a čísla (ICANN), v súlade s právom Únie vrátane právnych predpisov na ochranu údajov.
- Bude vychádzať z najnovších právnych predpisov a naďalej posilňovať úsilie v boji proti sexuálnemu zneužívaniu detí na internete. Komisia prijala Európsku stratégiu pre lepší internet pre deti[25] a spolu s EÚ a nečlenskými krajinami EÚ vytvorila **Globálnu alianciu proti sexuálnemu zneužívaniu detí na internete**[26]. Aliancia je nástroj pre ďalšie opatrenia členských štátov podporované Komisiou a EC3.

Komisia žiada Europol (EC3), aby:

- Spočiatku zameriaval svoju analytickú a operačnú podporu vyšetrovania prípadov kybernetickej kriminality v členských štátoch na pomoc pri odstraňovaní a narušaní sietí kybernetickej kriminality najmä v oblasti sexuálneho zneužívania detí, platobných podvodov, botnetov a neoprávnených vniknutí.
- Pravidelne pripravoval strategické a operačné správy o trendoch a objavujúcich sa hrozbách s cieľom určenia priorít a zamerania vyšetrovacej činnosti tímov pre kybernetickú kriminalitu v členských štátoch.

Komisia žiada Európsku policajnú akadémiu (CEPOL), aby v spolupráci s Europolom:

- Koordinovala navrhovanie a plánovanie kurzov odbornej prípravy s cieľom vybaviť orgány presadzovania práva vedomosťami a odbornosťou umožňujúcimi účinný boj proti kybernetickej kriminalite.

---

24 Dňa 28. marca 2012 Európska komisia prijala oznámenie „Boj proti zločinu v digitálnom veku: Zriadenie Európskeho centra pre kybernetickú kriminalitu."

25 COM (2012) 196 final.

26 Závery Rady na tému Globálna aliancia proti sexuálnemu zneužívaniu detí na internete (spoločné vyhlásenie EÚ a USA) zo 7. a 8. júna 2012 a vyhlásenie o vytvorení Globálnej aliancie proti sexuálnemu zneužívaniu detí na internete (http://europa.eu/rapid/press-release_MEMO-12-944_en.htm)

Komisia žiada Eurojust, aby:

- Identifikoval hlavné prekážky justičnej spolupráce na vyšetrovaní kybernetickej kriminality a koordinácie medzi členskými štátmi a s tretími krajinami a podporil oblasti vyšetrovania a trestného stíhania kybernetickej kriminality tak na operačnej a strategickej úrovni, ako aj v rámci príslušnej odbornej prípravy.

Komisia žiada Eurojust a Europol (EC3), aby:

- Úzko spolupracovali, okrem iného prostredníctvom výmeny informácií, s cieľom zvýšiť ich efektívnosť v boji proti kybernetickej kriminalite v súlade s ich príslušnými právomocami a schopnosťami.
-

2.3. Rozvoj politiky a spôsobilostí kybernetickej obrany v súvislosti s rámcom spoločnej bezpečnostnej a obrannej politiky (SBOP)

Úsilie v oblasti kybernetickej bezpečnosti v EÚ zahŕňa aj rozmer kybernetickej obrany. Na zvýšenie odolnosti informačných a komunikačných systémov, ktoré podporujú obranné záujmy a záujmy národnej bezpečnosti členských štátov, by sa rozvoj spôsobilostí kybernetickej obrany mal sústrediť na odhaľovanie sofistikovaných kybernetických hrozieb, reakciu na ne a zotavenie z ich následkov.

Vzhľadom na to, že hrozby majú mnoho podôb, súčinnosť medzi civilnými a vojenskými prístupmi k ochrane kritických kybernetických prostriedkov by sa mala zvýšiť. Tieto snahy by mali byť podporené výskumom a vývojom, ako aj užšou spoluprácou medzi vládami, súkromným sektorom a akademickou obcou v EÚ. S cieľom vyhnúť sa duplicite EÚ preskúma možnosti, ako vzájomne dopĺňať úsilie EÚ a NATO o posilnenie odolnosti informačných infraštruktúr najdôležitejších orgánov štátnej správy, sektora obrany a iných sektorov, na ktorých sú členovia oboch organizácií závislí.

Vysoký predstaviteľ sa zameria na tieto kľúčové činnosti, pričom vyzve členské štáty a Európsku obrannú agentúru, aby na nich spolupracovali:

- Posúdenie požiadaviek operačných potrieb kybernetickej obrany EÚ a podpora rozvoja kapacít a technológií kybernetickej obrany EÚ s cieľom riešiť všetky aspekty rozvoja spôsobilostí vrátane doktríny, otázok vedenia, organizácie, pracovníkov, odbornej prípravy, technológie, infraštruktúry, logistiky a interoperability;

- Rozvoj rámcových politík kybernetickej obrany EÚ zameraných na ochranu sietí v rámci misií a operácií SBOP vrátane dynamického riadenia rizík, zlepšenia analýzy hrozieb a spoločného využívania informácií. Zlepšenie príležitostí na odbornú prípravu a cvičenia v rámci kybernetickej obrany pre armádne zložky v európskom a nadnárodnom kontexte vrátane začlenenia prvkov kybernetickej obrany do existujúcich plánov cvičení;

- Podpora dialógu a koordinácie medzi civilnými a vojenskými aktérmi v EÚ – so zvláštnym dôrazom na výmenu osvedčených postupov, výmenu informácií a včasných varovaní, reakcie na incidenty, posúdenie rizík, zvyšovanie informovanosti a stanovenie kybernetickej bezpečnosti ako priority;

- Zabezpečenie dialógu s medzinárodnými partnermi vrátane NATO, inými medzinárodnými organizáciami a medzinárodnými centrami excelentnosti s cieľom zabezpečiť účinnú obrannú spôsobilosť, identifikovať oblasti spolupráce a zabrániť duplicite úsilia.

2.4. Rozvoj priemyselných a technologických zdrojov pre kybernetickú bezpečnosť

Európa má špičkové výskumné a vývojové kapacity, ale mnoho svetových lídrov poskytujúcich inovačné produkty a služby IKT má sídlo mimo územia EÚ. Existuje riziko, že Európa sa stane príliš závislou nielen od IKT produkovaných inde, ale aj od bezpečnostných riešení vyvíjaných mimo jej hraníc. Rozhodujúcou úlohou je zabezpečiť, aby technické a programové komponenty vyrábané v EÚ a v tretích krajinách, ktoré sa používajú v kritických službách a infraštruktúrach a čoraz častejšie aj v mobilných zariadeniach, boli dôveryhodné, bezpečné a zaručovali ochranu osobných údajov.

Podpora jednotného trhu s produktmi kybernetickej bezpečnosti

Vysoký stupeň bezpečnosti sa môže zaistiť iba vtedy, ak všetky zložky hodnotového reťazca (napr. výrobcovia zariadení, softvéroví vývojári, poskytovatelia služieb informačnej spoločnosti) urobia z bezpečnosti svoju prioritu. Zdá sa však[27], že mnohé subjekty ešte vždy považujú bezpečnosť len za dodatočnú záťaž a že existuje iba obmedzený dopyt po bezpečnostných riešeniach. Vhodné výkonnostné požiadavky na kybernetickú bezpečnosť treba implementovať v celom hodnotovom reťazci produktov IKT, ktoré sa používajú v Európe. Súkromný sektor potrebuje stimuly na zabezpečenie vysokej úrovne kybernetickej bezpečnosti. Napríklad nálepky vyjadrujúce adekvátnu úroveň výkonnosti kybernetickej bezpečnosti umožnia spoločnostiam s dobrými výsledkami v tejto oblasti upozorniť na túto skutočnosť pri predaji a získať tak konkurenčnú výhodu. Okrem toho povinnosti stanovené v návrhu smernice o bezpečnosti sietí a informácií by podstatne prispeli k zvýšeniu konkurencieschopnosti podnikov v príslušnom odvetví.

Mal by sa podporiť aj celoeurópsky dopyt po trhu s vysoko bezpečnými výrobkami. Po prvé, táto stratégia sa zameriava na posilnenie spolupráce a transparentnosti, pokiaľ ide o bezpečnosť výrobkov IKT. Vyzýva na zriadenie platformy, ktorá spojí príslušné európske verejné a súkromné zainteresované strany s cieľom určiť osvedčené postupy kybernetickej bezpečnosti v celom hodnotovom reťazci a vytvoriť priaznivé trhové podmienky pre vývoj a prijímanie bezpečných IKT riešení. Hlavným zameraním by malo byť vytváranie stimulov pre vykonávanie náležitého riadenia rizika a prijímanie bezpečnostných noriem a riešení, ako aj prípadné vytvorenie dobrovoľného systému certifikácie v rámci celej EÚ vychádzajúceho z programov existujúcich v EÚ a na medzinárodnej úrovni. Komisia bude podporovať prijímanie prístupov koherentných v rámci členských štátov, aby sa bolo možné vyhnúť rozdielom vytvárajúcim pre podniky nevýhody súvisiace s polohou.

Po druhé, Komisia bude podporovať vývoj bezpečnostných noriem a pomáhať pri dobrovoľných schémach osvedčovania v oblasti cloud computingu v rámci celej EÚ, pričom náležite zohľadní potrebu zabezpečiť ochranu údajov. Činnosť by sa mala zamerať na bezpečnosť dodávateľského reťazca, najmä v kritických hospodárskych odvetviach (priemyselné kontrolné systémy, energetické a dopravné infraštruktúry). Táto práca by mala vychádzať z prebiehajúcej normalizačnej činnosti v európskych normalizačných

[27] Pozri pracovný dokument útvarov Komisie o posúdení vplyvu, sprievodný dokument k návrhu Komisie na smernicu o bezpečnosti sietí a informácií, oddiel 4.1.5.2.

organizáciách (CEN, CENELEC a ETSI)[28] a v koordinačnej skupine pre kybernetickú bezpečnosť (CSCG), ako aj z odborných znalostí agentúry ENISA, Komisie a ostatných relevantných aktérov.

Komisia:

- V roku 2013 vytvorí verejno-súkromnú **platformu pre riešenia NIS** na rozvoj stimulov pre prijímanie bezpečných riešení IKT a zavádzanie osvedčených metód kybernetickej bezpečnosti s cieľom uplatniť ich na produkty IKT, ktoré sa používajú v Európe.
- V roku 2014 navrhne odporúčania týkajúce sa zaistenia kybernetickej bezpečnosti v rámci celého hodnotového reťazca IKT, pričom bude vychádzať z práce tejto platformy.
- Preskúma, akým spôsobom by významní poskytovatelia hardvéru a softvéru IKT mohli informovať príslušné vnútroštátne orgány o zistených slabých miestach, ktoré by mohli mať výrazný vplyv na bezpečnosť.

Komisia žiada agentúru ENISA, aby:

- V spolupráci s príslušnými vnútroštátnymi kompetentnými orgánmi, príslušnými zainteresovanými stranami, medzinárodnými a európskymi normalizačnými orgánmi a Spoločným výskumným centrom Európskej komisie vypracovala **technické usmernenia a odporúčania pre prijatie noriem v oblasti bezpečnosti sietí a informácií a osvedčené postupy** vo verejnom a súkromnom sektore.

Komisia vyzýva verejné a súkromné zainteresované strany, aby:

- Stimulovali vývoj a prijatie **bezpečnostných noriem**, technických noriem a zásad implementácie prvkov bezpečnosti a ochrany súkromia už v štádiu návrhu pod vedením priemyselného odvetvia výrobcami a poskytovateľmi služieb IKT vrátane poskytovateľov cloudových služieb; nové generácie softvéru a hardvéru by mali byť vybavené **silnejšími, zabudovanými a jednoducho použiteľnými bezpečnostnými** prvkami.
- Vyvinuli pre spoločnosti priemyselné normy stanovujúce úrovne kybernetickej bezpečnosti a zlepšili informovanosť verejnosti vytvorením **bezpečnostných nálepiek** alebo registrovaných certifikačných značiek („kite marks“), ktoré by spotrebiteľom pomáhali orientovať sa na trhu.

Podpora investícií do výskumu a vývoja a inovácie

Výskum a vývoj môžu podporiť silnú priemyselnú politiku, prispieť k propagácii dôveryhodného európskeho výrobného odvetvia IKT, naštartovať rozvoj vnútorného trhu a znížiť európsku závislosť na zahraničných technológiách. Výskum a vývoj by mal zaplniť technologické štrbiny v oblasti bezpečnosti IKT, pripraviť odvetvie na ďalšiu generáciu bezpečnostných výziev, vziať do úvahy stály vývoj potrieb používateľov a zožať ovocie

[28] Najmä v rámci normy pre inteligentné siete M/490 – ide o prvý súbor noriem pre inteligentné siete a referenčné architektúry.

technológií dvojakého použitia. Takisto by mal pokračovať v podpore rozvoja kryptografie. Toto sa musí doplniť úsilím pretransformovať výsledky výskumu a vývoja do komerčných riešení poskytnutím potrebných stimulov a zavedením príslušných politických podmienok.

EÚ by mala čo najlepšie využiť rámcový programom Horizont 2020[29] pre výskum a inovácie, ktorý sa začne realizovať v roku 2014. Návrh Komisie obsahuje konkrétne ciele pre dôveryhodné IKT, ako aj pre boj proti kybernetickej kriminalite, ktoré sú v súlade s touto stratégiou. Horizont 2020 bude podporovať výskum v oblasti bezpečnosti súvisiaci s vynárajúcimi sa informačnými a komunikačnými technológiami; poskytovať riešenia pre koncové bezpečné systémy, služby a aplikácie informačných a komunikačných technológií; poskytovať stimuly pre implementovanie a prijímanie existujúcich riešení; a zameriavať sa na interoperabilitu medzi sieťovými a informačnými systémami. Osobitná pozornosť bude venovaná na úrovni EÚ optimalizácii a lepšej koordinácii jednotlivých programov financovania (Horizont 2020, fond vnútornej bezpečnosti, výskum EDA vrátane Európskej rámcovej spolupráce).

Komisia:

- Využije Horizont 2020 na pokrytie viacerých oblastí týkajúcich sa súkromia a bezpečnosti informačných a komunikačných technológií, od výskumu a vývoja až po inovácie a zavádzanie. V rámci Horizontu 2020 sa budú tiež rozvíjať nástroje a prostriedky na boj proti kriminálnym a teroristickým činnostiam namiereným proti kybernetickému prostrediu.
- Vytvorí mechanizmy na lepšiu koordináciu výskumných plánov inštitúcií Európskej únie a členských štátov a podnieti členské štáty, aby viac investovali do výskumu a vývoja.

Komisia vyzýva členské štáty, aby:

- Do konca roka 2013 vyvinuli osvedčené postupy na využívanie **kúpnej sily orgánov verejnej správy** (napríklad prostredníctvom verejného obstarávania) s cieľom podnietiť vývoj a zavádzanie bezpečnostných prvkov v oblasti výrobkov a služieb IKT.
- Podporili včasné zapojenie priemyslu a akademickej obce do vývoja a koordinácie príslušných riešení. Toto by sa malo uskutočniť za maximálneho využitia priemyselnej základne Európy a súvisiaceho výskumu a vývoja inovatívnych technológií a koordinácie výskumných programov civilných a vojenských organizácií.

Komisia žiada Europol a agentúru ENISA, aby:

- Identifikovali novovznikajúce trendy a potreby vzhľadom na vývoj a zvyklosti v oblasti kybernetickej kriminality a kybernetickej bezpečnosti, aby sa mohli vypracovať primerané digitálnej forenzné nástroje a technológie.

Komisia vyzýva verejné a súkromné zainteresované strany, aby:

[29] Horizont 2020 je finančný nástroj implementujúci Úniu inovácií, hlavnú iniciatívu stratégie Európa 2020, zameranú na zabezpečenie konkurencieschopnosti Európy vo svete. Od roku 2014 do roku 2020 sa nový rámcový program EÚ pre výskum a inovácie stane súčasťou sústredeného úsilia o zabezpečenie nového rastu a vytvorenie nových pracovných miest v Európe.

- V spolupráci so sektorom poisťovníctva vyvíjali **harmonizovanú metriku pre výpočet rizikových prirážok**, umožňujúcich spoločnostiam, ktoré investovali do bezpečnosti, využívať nižšie rizikové prirážky.

2.5. Vytvorenie koherentnej medzinárodnej politiky Európskej únie týkajúcej sa kybernetického priestoru a podpora kľúčových hodnôt EÚ

Uchovanie otvoreného, slobodného a bezpečného kybernetického priestoru je globálny problém, ktorý by EÚ mala riešiť spolu s príslušnými medzinárodnými partnermi a organizáciami, súkromným sektorom a občianskou spoločnosťou.

Vo svojej medzinárodnej politike týkajúcej sa kybernetického priestoru sa EÚ bude snažiť podporovať otvorenosť a slobodu internetu, povzbudzovať k úsiliu o vytvorenie noriem správania a uplatňovať existujúce medzinárodné právne normy v kybernetickom priestore. EÚ bude takisto pracovať na preklenutí digitálnej priepasti a bude sa aktívne zúčastňovať na medzinárodnom úsilí smerujúcom k vybudovaniu kapacity kybernetickej bezpečnosti. Medzinárodná angažovanosť EÚ v problémoch kybernetického priestoru sa bude riadiť základnými hodnotami, ktoré EÚ uznáva v oblastiach ľudskej dôstojnosti, slobody, demokracie, rovnosti, právneho štátu a dodržiavania základných práv.

Začlenenie problémov kybernetického priestoru do politík vonkajších vzťahov EÚ a spoločnej zahraničnej a bezpečnostnej politiky

Komisia, vysoká predstaviteľka a členské štáty by mali sformulovať koherentnú medzinárodnú politiku EÚ týkajúcu sa kybernetického priestoru, ktorá sa zameria na zvýšenú angažovanosť a posilnenie vzťahov s kľúčovými medzinárodnými partnermi a organizáciami, ako aj so zástupcami občianskej spoločnosti a súkromného sektora. Mali by sa navrhnúť, koordinovať a realizovať konzultácie EÚ s medzinárodnými partnermi o problémoch kybernetického priestoru, a to tak, aby sa zhodnotili existujúce dvojstranné dialógy medzi členskými štátmi EÚ a tretími krajinami. EÚ bude klásť opätovný dôraz na dialóg s tretími krajinami, s osobitným zameraním na podobne zmýšľajúcich partnerov, ktorí s EÚ zdieľajú rovnaké hodnoty. Podporí dosiahnutie vysokej úrovne ochrany údajov, a to aj v prípade prevodu osobných údajov do tretej krajiny. Na riešenie globálnych výziev v kybernetickom priestore sa EÚ bude usilovať o užšiu spoluprácu s organizáciami, ktoré pôsobia aktívne v tejto oblasti, ako napríklad Rada Európy, OECD, OSN, OBSE, NATO, AÚ, ASEAN a OAS. Na bilaterálnej úrovni je obzvlášť dôležitá spolupráca s USA a bude sa ďalej rozvíjať, a to predovšetkým v kontexte pracovnej skupiny EÚ-USA pre kybernetickú bezpečnosť a kybernetickú kriminalitu.

Jedným z hlavných prvkov medzinárodnej kybernetickej politiky EÚ bude podpora kybernetického priestoru ako priestoru slobody a základných práv. Rozšírenie prístupu na internet by malo prispievať k demokratickým reformám a ich celosvetovej podpore. Zvýšenú globálnu prepojiteľnosť by nemala sprevádzať cenzúra ani masový dohľad. EÚ by mala podporovať sociálnu zodpovednosť podnikov[30] a prichádzať s medzinárodnými iniciatívami na zlepšenie globálnej koordinácie v tejto oblasti.

Zodpovednosť za bezpečnejší kybernetický priestor nesú všetci aktéri globálnej informačnej spoločnosti, od občanov až po vlády. EÚ podporuje úsilie zamerané na definovanie noriem správania v kybernetickom priestore, ktorými by sa všetky zainteresované strany mali riadiť.

[30] *Obnovená stratégia EÚ pre sociálnu zodpovednosť podnikov na obdobie rokov 2011 – 2014*; KOM (2011) 681 v konečnom znení.

Rovnako ako EÚ očakáva, že občania počas prítomnosti online budú rešpektovať občianske povinnosti, sociálnu zodpovednosť a zákony, tak aj štáty by mali dodržiavať normy a existujúce právne predpisy. V otázkach medzinárodnej bezpečnosti EÚ podporuje rozvoj opatrení na budovanie dôvery v rámci kybernetickej bezpečnosti s cieľom zvýšiť transparentnosť a znížiť riziko nepochopenia správania štátu.

EÚ nevyžaduje vytváranie nových medzinárodných právnych nástrojov na riešenie kybernetických problémov.

Právne záväzky zakotvené v Medzinárodnom pakte o občianskych a politických právach, v Európskom dohovore o ľudských právach a v Charte základných práv EÚ by sa mali rešpektovať aj na internete. EÚ sa sústredí na hľadanie spôsobu, akým by sa dalo dosiahnuť, aby sa tieto opatrenia presadzovali aj v kybernetickom priestore.

Pokiaľ ide o riešenie kybernetickej kriminality, Budapeštiansky dohovor je nástroj, ktorý môžu prijať aj tretie krajiny. Predstavuje vzor pre vypracúvanie vnútroštátnych právnych predpisov na boj proti kybernetickej kriminalite a základ pre medzinárodnú spoluprácu v tejto oblasti.

Ak by sa ozbrojené konflikty rozšírili na kybernetický priestor, takýto prípad by sa posudzoval podľa medzinárodného humanitárneho práva a prípadne ľudských práv. **Rozvoj budovania kapacít v oblasti kybernetickej bezpečnosti a odolnosti informačných infraštruktúr v tretích krajinách**

Bezproblémové fungovanie príslušných infraštruktúr, ktoré poskytujú a uľahčujú komunikačné služby, sa ľahšie dosiahne vďaka zvýšenej medzinárodnej spolupráci. Tá zahŕňa výmenu najlepších postupov a zdieľanie informácií, spoločné cvičenia na tému riadenie incidentov v kontexte včasného varovania atď. EÚ bude prispievať k dosiahnutiu tohto cieľa zintenzívnením prebiehajúceho medzinárodného úsilia o posilnenie sietí spolupráce na ochrane kritických informačných infraštruktúr (CIIP), ktoré zahŕňajú vlády a súkromný sektor.

Nie všetky časti sveta majú osoh z pozitívneho vplyvu internetu, pretože im chýba otvorené, bezpečné, interoperabilné a spoľahlivé pripojenie na internet. Európska únia bude preto pokračovať v podpore krajín v ich snahe zlepšiť prístup k internetu a jeho používaniu pre svojich občanov s cieľom zabezpečiť jeho integritu a bezpečnosť a účinne bojovať proti kybernetickej kriminalite.

V spolupráci s členskými štátmi Komisia a vysoká predstaviteľka budú:

- Pracovať na približovaní sa ku koherentnej medzinárodnej politike EÚ týkajúcej sa kybernetického priestoru s cieľom zvýšiť spoluprácu s kľúčovými medzinárodnými partnermi a organizáciami, začleniť problémy kybernetického priestoru do SZBP a zlepšiť koordináciu celosvetových problémov kybernetického priestoru;
- Podporovať vývoj noriem správania a opatrení na budovanie dôvery v oblasti kybernetickej bezpečnosti. Uľahčovať dialóg o tom, ako uplatňovať existujúce medzinárodné právo v kybernetickom priestore, a podporovať Budapeštiansky dohovor ako nástroj riešenia kybernetickej kriminality;
- Podporovať presadzovanie a ochranu základných práv vrátane prístupu k

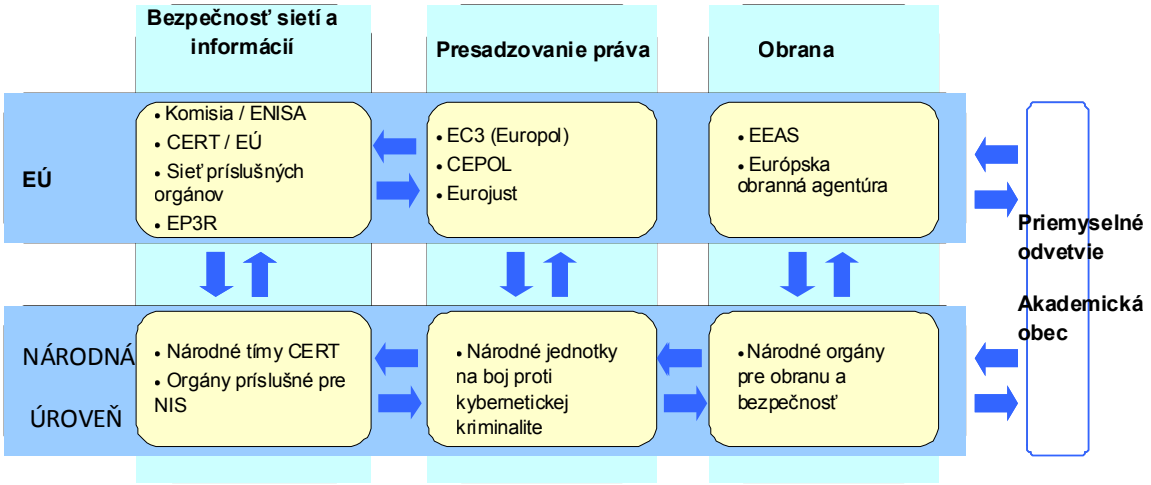
informáciám a slobody prejavu, so zameraním na: a) prípravu nových verejných usmernení o slobode prejavu online a offline; b) monitorovanie vývozu výrobkov alebo služieb, ktoré by mohli byť použité na cenzúru alebo masové sledovanie online; c) prípravu opatrení a nástrojov na rozšírenie prístupu k internetu a jeho otvorenosti a odolnosti a na riešenie problému cenzúry alebo masového sledovania pomocou komunikačných technológií; d) vytváranie možností pre zainteresované strany na využívanie komunikačných technológií na podporu základných práv;

- Spolupracovať s medzinárodnými partnermi a organizáciami, súkromným sektorom a občianskou spoločnosťou s cieľom podporovať globálne schopnosti budovania kapacít v tretích krajinách umožňujúce zlepšiť prístup k informáciám a k otvorenému internetu, vykonávať prevenciu a čeliť kybernetickým hrozbám vrátane náhodných udalostí, bojovať proti kybernetickej kriminalite a kybernetickému terorizmu a rozvíjať koordináciu darcov v rámci riadeného budovania kapacít;
- Využívať rozličné nástroje pomoci EÚ na budovanie kapacít kybernetickej bezpečnosti vrátane pomoci pri odbornom vzdelávaní personálu orgánov presadzovania práva, súdneho personálu a technického personálu zameranom na riešenie kybernetických hrozieb; a súčasne podporiť vytváranie príslušných národných politík, stratégií a inštitúcií v tretích krajinách;
- Zvyšovať koordináciu politík a zdieľanie informácií prostredníctvom medzinárodných sietí na ochranu kritických informačných infraštruktúr ako napríklad siete Meridián, spolupráce medzi orgánmi príslušnými pre oblasť bezpečnosti sietí a informácií a iných spôsobov.

3. ÚLOHY A ZODPOVEDNOSTI

Kybernetické incidenty sa v digitálne prepojenej ekonomike a spoločnosti nezastavujú na hraniciach. Všetci aktéri, od orgánov príslušných pre oblasť bezpečnosti sietí a informácií cez tímy CERT a orgány presadzovania práva až po priemysel, musia prevziať zodpovednosť na vnútroštátnej úrovni a na úrovni EÚ a spolupracovať na posilňovaní kybernetickej bezpečnosti. Keďže môže ísť o prepojenie odlišných právnych rámcov a jurisdikcií, kľúčovou výzvou pre EÚ je objasniť úlohy a zodpovednosť tohto množstva zainteresovaných aktérov.

Vzhľadom na zložitosť otázky a rôznorodosť škály zúčastnených aktérov centralizovaný európsky dohľad nie je riešením. Vlády členských štátov majú najlepšiu pozíciu na organizovanie prevencie a reakcie na kybernetické incidenty a útoky a na vytváranie kontaktov a sietí so súkromným sektorom a širokou verejnosťou v rámci svojich zavedených smerov politík a právnych rámcov. Zároveň však, vzhľadom na potenciálnu alebo skutočne bezhraničnú povahu rizík, by si účinná národná reakcia často vyžadovala angažovanosť na úrovni EÚ. Pri riešení kybernetickej bezpečnosti komplexným spôsobom by mali činnosti prebiehať v rámci troch základných pilierov – v oblasti bezpečnosti sietí a informácií, presadzovania práva a obrany – ktoré takisto pôsobia v odlišných právnych rámcoch:



3.1. Koordinácia medzi orgánmi príslušnými pre oblasť bezpečnosti sietí a informácií / tímami CERT a orgánmi presadzovania práva a obrany

Vnútroštátna úroveň

Členské štáty by mali mať, buď už dnes, alebo ako dôsledok tejto stratégie, štruktúry, ktoré sa zaoberajú kybernetickou odolnosťou, kybernetickou kriminalitou a obranou; a mali by dosiahnuť požadovanú úroveň spôsobilostí na riešenie kybernetických incidentov. Vzhľadom na to, že mnoho subjektov môže mať operatívnu zodpovednosť za rôzne rozmery kybernetickej bezpečnosti, a vzhľadom na dôležitosť zapojenia súkromného sektora, koordinácia na vnútroštátnej úrovni by sa mala optimalizovať v rámci všetkých ministerstiev. Členské štáty by mali stanoviť vo svojich národných stratégiách kybernetickej bezpečnosti úlohy a zodpovednosť rôznych svojich vnútroštátnych subjektov.

Výmena informácií medzi vnútroštátnymi orgánmi a súkromným sektorom by sa mala podporovať, aby si členské štáty a súkromný sektor mohli udržať celkový prehľad o rôznych hrozbách, lepšie chápať nové trendy a techniky používané pri kybernetických útokoch a rýchlejšie na ne reagovať. Prostredníctvom vytvárania národných plánov spolupráce v oblasti bezpečnosti sietí a informácií, podľa ktorých sa postupuje v prípade kybernetických incidentov, členské štáty by mali byť schopné jasne rozdeliť úlohy a zodpovednosti a optimalizovať odvetné opatrenia.

Úroveň EÚ

Rovnako ako na vnútroštátnej úrovni, na úrovni EÚ existujú viaceré subjekty, ktoré sa zaoberajú kybernetickou bezpečnosťou. Konkrétne ENISA, Europol/EC3 a EDA sú tri agentúry činné z hľadiska bezpečnosti sietí a informácií, presadzovania práva a obrany. Tieto agentúry majú správne rady, v ktorých sú zastúpené členské štáty, a ponúkajú platformy pre koordináciu na úrovni EÚ.

Koordinácia a spolupráca medzi agentúrami ENISA, Europol/EC3 a EDA sa bude podporovať v celom rade oblastí, kde sú spoločne činné, najmä pokiaľ ide o analýzy trendov, hodnotenie rizika, odborné vzdelávanie a zdieľanie najlepších postupov. Mali by spolupracovať, a pritom si zachovávať svoje špecifiká. Tieto agentúry spolu s tímom CERT-EU, Komisiou a členskými štátmi by mali podporovať vytvorenie dôveryhodnej komunity technických odborníkov a odborníkov na príslušné politiky v tejto oblasti.

Neformálne kanály pre koordináciu a spoluprácu budú doplnené viacerými štrukturálnymi prepojeniami. Vojenský štáb Európskej únie a tím EDA, ktorý má na starosti projekt kybernetickej obrany, môžu vytvoriť vektor pre koordináciu v oblasti obrany. Programový výbor Europolu/EC3 spojí okrem iného Eurojust, CEPOL, členské štáty[31], agentúru ENISA a Komisiu a ponúkne im príležitosť podeliť sa o ich rozdielne know-how a zabezpečiť, aby centrum EC3 podnikalo opatrenia v rámci partnerstva, pri súčasnom uznaní pridaných odborných znalostí a rešpektovaní mandátov všetkých zainteresovaných strán. Nový mandát agentúry ENISA by mal umožniť zvýšiť jej prepojenie s Europolom a posilniť prepojenia so zúčastnenými stranami z priemyselného odvetvia. Najdôležitejšie je, že legislatívny návrh Komisie z oblasti bezpečnosti sietí a informácií by vytvoril rámec spolupráce prostredníctvom siete národných orgánov príslušných pre oblasť bezpečnosti sietí a informácií a upravil by zdieľanie informácií medzi oblasťou bezpečnosti sietí a informácií a orgánmi presadzovania práva.

Medzinárodná oblasť

Komisia a vysoká predstaviteľka zabezpečia v súčinnosti s členskými štátmi koordinované medzinárodné opatrenie v oblasti kybernetickej bezpečnosti. Pritom Komisia a vysoká predstaviteľka budú presadzovať základné hodnoty EÚ a propagovať mierové, otvorené a transparentné využívanie kybernetických technológií. Komisia, vysoká predstaviteľka a členské štáty sa zapoja do politického dialógu s medzinárodnými partnermi a s medzinárodnými organizáciami, ako je napríklad Rada Európy, OECD, OBSE, NATO a OSN.

3.2. Podpora EÚ v prípade veľkého kybernetického incidentu alebo útoku

Rozsiahle kybernetické incidenty alebo útoky pravdepodobne budú mať vplyv na vlády, podniky a jednotlivcov v rámci EÚ. V dôsledku tejto stratégie, a najmä v súvislosti s navrhovanou smernicou o NIS, by sa prevencia kybernetických incidentov, ich odhaľovanie a reakcie na ne mali zlepšiť a členské štáty a Komisia by sa mali stále lepšie navzájom informovať o rozsiahlych kybernetických incidentoch alebo útokoch. Mechanizmy odozvy sa však budú líšiť v závislosti od povahy, rozsahu a cezhraničných dôsledkov incidentov.

Ak incident má vážny vplyv na zabezpečenie kontinuity činnosti, v smernici o bezpečnosti sietí a informácií sa navrhuje, aby sa aktivovali národné alebo únijné plány spolupráce v oblasti bezpečnosti sietí a informácií, podľa toho, či má incident cezhraničný charakter, alebo nie. Sieť orgánov príslušných pre oblasť bezpečnosti sietí a informácií by sa v tomto kontexte využila na zdieľanie informácií a podporu. To by umožnilo zachovanie a/alebo obnovu postihnutých sietí a služieb.

Ak sa zdá, že incident je spojený s trestnou činnosťou, je vhodné informovať Europol/EC3, aby spolu s orgánmi presadzovania práva z postihnutých krajín mohli začať vyšetrovanie, zabezpečiť dôkazy, určiť páchateľov a v konečnom dôsledku zaistiť, aby boli stíhaní.

Ak za zdá, že incident sa týka kybernetickej špionáže alebo štátom podporovaného útoku, alebo má vplyv na národnú bezpečnosť, orgány národnej bezpečnosti a obrany upozornia svojich príslušných partnerov, aby vedeli, že sú vystavení útoku, a mohli sa brániť. Mechanizmus včasného varovania sa potom aktivuje, a ak je to potrebné, tak sa aktivuje aj

[31] Prostredníctvom zastupovania v rámci pracovnej skupiny EÚ pre kybernetickú kriminalitu, ktorá sa skladá z vedúcich predstaviteľov jednotiek na boj proti kybernetickej kriminalite v rámci EÚ vytvorených v členských štátoch.

krízové riadenie alebo iné postupy. Obzvlášť závažné prípady kybernetických incidentov alebo útoku by mohli predstavovať pre členský štát dostatočný dôvod na uplatnenie doložky o solidarite EÚ (článok 222 Zmluvy o fungovaní Európskej únie).

Ak sa zdá, že pri incidente došlo k ohrozeniu osobných údajov, mali by sa zapojiť vnútroštátne orgány na ochranu údajov alebo národný regulačný orgán v súlade so smernicou 2002/58/ES.

Napokon, pri riešení kybernetických incidentov a odvracaní útokov je vhodné využiť siete kontaktov a pomoc poskytnutú medzinárodnými partnermi. To môže zahŕňať technické zmierňovanie dôsledkov, vyšetrovanie trestných činov alebo aktiváciu mechanizmov reakcie krízového riadenia.

4. ZÁVERY A NÁSLEDNÉ ČINNOSTI

Táto navrhovaná stratégia kybernetickej bezpečnosti Európskej únie, ktorú predkladá Komisia a vysoká predstaviteľka Únie pre zahraničné veci a bezpečnostnú politiku, načrtáva víziu EÚ a požadované opatrenia, vychádzajúc zo silnej ochrany a podpory práv občanov EÚ, s cieľom premeniť online prostredie EÚ na najbezpečnejšie na svete[32].

Táto vízia sa dá dosiahnuť len prostredníctvom skutočného partnerstva medzi mnohými aktérmi ochotnými prevziať zodpovednosť a čeliť budúcim výzvam.

Komisia a vysoká predstaviteľka preto vyzývajú Radu a Európsky parlament, aby schválili stratégiu a napomáhali realizácii uvedených opatrení. Silná podpora a záväzok sú potrebné aj od súkromného sektora a občianskej spoločnosti, ktorí sú kľúčovými aktérmi, pokiaľ ide o prehĺbenie našej úrovne bezpečnosti a ochrany práv občanov.

Nastal čas, aby sme konali. Komisia a vysoká predstaviteľka sú odhodlané spolupracovať so všetkými aktérmi s cieľom dosiahnuť pre Európu potrebnú bezpečnosť. Aby sa zabezpečila včasná implementácia stratégia a jej posúdenie z hľadiska možného vývoja, pozvú všetky relevantné strany na konferenciu na vysokej úrovni a posúdia pokrok dosiahnutý v priebehu 12 mesiacov.

[32] Financovanie stratégie bude prebiehať v rámci predpokladaných súm pre každú z príslušných oblastí politiky (CEF, Horizonte 2020 fond pre vnútornú bezpečnosť, SZBP a oblasť vonkajšej spolupráce, najmä Nástroj stability), ako sa uvádza v návrhu Komisie na viacročný finančný rámec na roky 2014 – 2020 (podliehajúci súhlasu rozpočtového orgánu a konečným finančným prostriedkom v prijatom viacročnom finančnom rámci na roky 2014 – 2020). Vzhľadom na potrebu zabezpečiť celkovú zlučiteľnosť s počtom pracovných miest pre decentralizované agentúry a na podstrop pre decentralizované agentúry pre každý výdavkový okruh budúceho viacročného finančného rámca, agentúry (CEPOL, EDA, ENISA, Eurojust a Europol/EC3), na ktoré sa v tomto oznámení vznáša požiadavka, aby prevzali nové úlohy, sa budú nabádať, aby tak urobili, pokiaľ sa určila skutočná kapacita agentúry absorbovať nárast zdrojov a boli identifikované všetky možnosti presunu zamestnancov.