Európska komisia

STAV ÚNIE
2018

Budovanie silnej kybernetickej bezpečnosti v Európe

#SOTEU

12. september 2018

„Kybernetické útoky nepoznajú hranice, no schopnosť jednotlivých krajín reagovať na ne sa značne líši, takže vznikajú slabé miesta, ktoré ešte viac priťahujú útoky. EÚ potrebuje spoľahlivejšie a účinnejšie štruktúry, ktoré zaistia silnú kybernetickú odolnosť a reakciu na kybernetické útoky. Nechceme byť najslabším článkom v tejto globálnej hrozbe.“

Jean-Claude Juncker, digitálny samit v Tallinne, 29. september 2017

S cieľom vybaviť Európu správnymi nástrojmi, ktoré si poradia s neustále sa meniacimi kybernetickými hrozbami, Európska komisia a vysoká predstaviteľka navrhli v roku 2017 rozsiahly súbor opatrení zameraných na budovanie silnej kybernetickej bezpečnosti v EÚ. K tomuto úsiliu prispieva aj návrh, vďaka ktorému EÚ dokáže združovať zdroje a odborné poznatky z výskumu a inovácií a môže sa stať lídrom v oblasti kybernetickej bezpečnosti a digitálnych technológií budúcej generácie.

Súčasné kybernetické útoky

V roku 2016 sa každý deň vyskytlo **viac ako 4 000 ransomwarových útokov**

80 % európskych podnikov zaznamenalo minulý rok aspoň jeden kybernetický incident

Bezpečnostné incidenty vo všetkých odvetviach **vzrástli o 38 %** – najväčší nárast za posledných 12 rokov

V niektorých členských štátoch predstavuje počítačová kriminalita **50 % všetkých spáchaných trestných činov**

Útok vírusom Wannycry v máji 2017 zasiahol **viac ako 150 krajín a viac ako 230 000 systémov**, čo malo významný dosah na základné služby pripojené na internet, a to vrátane nemocníc a záchranných služieb.

Posilnenie odolnosti proti kybernetickým útokom

Komisia už podporuje úsilie o ráznejšie odrádzanie od kybernetických útokov v EÚ a lepšiu odolnosť a reakciu v týchto situáciách, napríklad aj týmito krokmi:

Podpora pre účinné uplatňovanie prvého právneho predpisu EÚ v oblasti kybernetickej bezpečnosti (smernice o bezpečnosti sietí a informačných systémov), ktorý prináša tieto opatrenia:

VÄČŠIE SPÔSOBILOSTI

Členské štáty musia zlepšiť svoje spôsobilosti v oblasti kybernetickej bezpečnosti

SPOLUPRÁCA

Intenzívnejšia spolupráca na úrovni EÚ

PREDCHÁDZANIE RIZIKÁM

Aktéri v kľúčových odvetviach (napríklad v energetike, doprave, zdravotníctve) sú povinní zaviesť opatrenia na predchádzanie rizikám a zvládnutie kybernetických incidentov

Spolupráca s členskými štátmi:

AGENTÚRA EÚ PRE KYBERNETICKÚ BEZPEČNOSŤ

Posilnenie Agentúry Európskej únie pre kybernetickú bezpečnosť tak, aby lepšie pomáhala členským štátom

CERTIFIKAČNÝ RÁMEC EÚ

Celoúnijný certifikačný rámec na zaistenie kybernetickej bezpečnosti produktov a služieb

KOORDINOVANÁ REAKCIA

Zaistenie rýchlej a koordinovanej odpovede na kybernetické útoky veľkého rozsahu

Agentúra pre sieťovú a informačnú bezpečnosť (ENISA) pomáha orgánom členských štátov, ktoré sa špecializujú na kybernetickú bezpečnosť, lepšie chrániť EÚ pred kybernetickými útokmi.

Združovanie zdrojov a odborných poznatkov v oblasti kybernetickobezpečnostných technológií

Okrem už existujúcich iniciatív EÚ v oblasti kybernetickej bezpečnosti Komisia dnes navrhuje posilniť toto úsilie tým, že sa zriadi sieť kompetenčných centier a Európske centrum odvetvových, technologických a výskumných kompetencií v oblasti kybernetickej bezpečnosti, ktoré budú vyvíjať a zavádzať nástroje a technológie potrebné na to, aby sme udržali krok s neustále sa meniacimi hrozbami.

Európske centrum bude spoločne s členskými štátmi zodpovedať za čo najadresnejšiu koordináciu prostriedkov plánovaných na oblasť kybernetickej bezpečnosti v ďalšom dlhodobom rozpočte EÚ. V Európe to pomôže vytvoriť nové kybernetické spôsobilosti.

V rámci EÚ pôsobí viac ako **660 kompetenčných centier kybernetickej bezpečnosti**, takže Európa už disponuje veľkým počtom odborníkov. S cieľom využiť a efektívne uplatniť ich odbornosť Komisia navrhuje mechanizmus, ako:

Združiť, zdieľať a sprístupniť existujúce odborné poznatky

Pomáhať zavádzať produkty a riešenia kybernetickej bezpečnosti EÚ

Zabezpečiť dlhodobú strategickú spoluprácu medzi odvetviami, výskumnými strediskami a vládami

Spoločne investovať do nákladnej infraštruktúry a zabezpečiť jej spoločné využívanie

Európske kompetenčné centrum:

Bude koordinovať využívanie finančných prostriedkov vyčlenených na oblasť kybernetickej bezpečnosti v ďalšom dlhodobom rozpočte EÚ na roky 2021 – 2027 v programoch Digitálna Európa a Európsky horizont. Centrum bude poskytovať podporu pre sieť a komunitu s cieľom presadzovať výskum a inovácie v oblasti **kybernetickej bezpečnosti**. Zároveň bude organizovať **spoločné investície** EÚ, členských štátov a priemyslu. V rámci programu Digitálna Európa sa napríklad investujú **2 miliardy eur** do ochrany digitálneho hospodárstva EÚ, spoločnosti a demokracie. Tieto prostriedky poslúžia na posilnenie odvetvia kybernetickej bezpečnosti EÚ a financovanie najmodernejšieho vybavenia a infraštruktúry.

Sieť národných koordinačných centier:

Každý členský štát nominuje jedno národné koordinačné centrum, ktoré bude viesť danú sieť a bude sa podieľať na vývoji nových spôsobilostí v oblasti kybernetickej bezpečnosti a budovaní širších kompetencií. Sieť pomôže identifikovať a podporiť najvýznamnejšie kyberneticko-bezpečnostné projekty v členských štátoch.

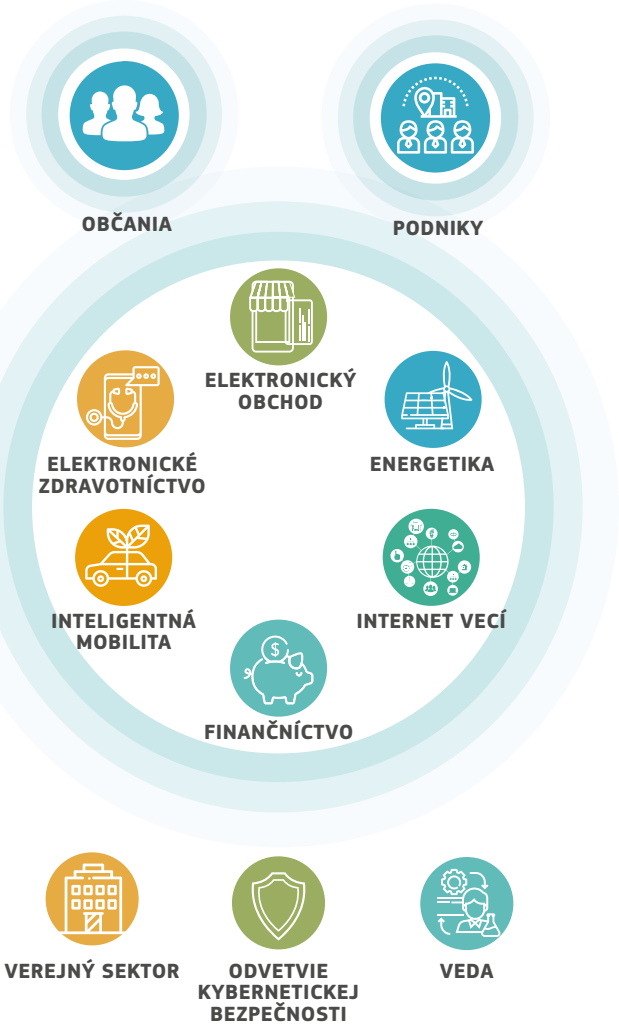
Komunita kompetencií:

Veľká, otvorená a rôznorodá skupina zahŕňajúca členov zainteresovaných na kybernetickej bezpečnosti pochádzajúcich z výskumných kruhov, súkromnej aj verejnej sféry, vrátane civilných aj vojenských orgánov.

Čo sa zlepší?

- Lepšia koordinácia práce
- Prístup k odborným vedomostiam
- Prístup k testovacím a experimentálnym zariadeniam
- Hodnotenie kybernetickej bezpečnosti výrobkov
- Prístup k inovačným produktom a riešeniam kybernetickej bezpečnosti
- Podpora pri uvádzaní výrobkov a služieb na trh
- Zviditeľnenie pre potenciálnych investorov a obchodných partnerov
- Úspora nákladov spoločnými investíciami s ostatnými členskými štátmi
- Možnosť, aby EÚ nezávisle chránila svoje hospodárstvo a demokraciu
- Možnosť, aby sa EÚ stala globálnym lídrom v oblasti kybernetickej bezpečnosti

Kto z tohto bude mať osoh?



Úrad pre publikácie

Print ISBN 978-92-79-92461-3 doi:10.2775/63604 NA-04-18-693-SK-C
PDF ISBN 978-92-79-92505-4 doi:10.2775/6876 NA-04-18-693-SK-N