AGENTÚRA EURÓPSKEJ ÚNIE PRE KYBERNETICKÚ BEZPEČNOSŤ

DÔVERYHODNÁ A KYBERNETICKY BEZPEČNÁ EURÓPA

Stratégia ENISA

jún 2020

DÔVERYHODNÁ A KYBERNETICKY BEZPEČNÁ EURÓPA

AGENTÚRA EURÓPSKEJ ÚNIE PRE KYBERNETICKÚ BEZPEČNOSŤ

PREDSLOV

Už viac ako 15 rokov zohráva ENISA – Agentúra EÚ pre kybernetickú bezpečnosť – kľúčovú úlohu pri napĺňaní ambície EÚ zvýšiť digitálnu dôveryhodnosť a bezpečnosť v rámci Európy v spolupráci s členskými krajinami a inštitúciami a agentúrami EÚ. ENISA, ktorá spája spoločenstvá, úspešne prispela k posilneniu pripravenosti Európy na kybernetické incidenty a jej schopnosti na ne reagovať.

Súčasne sa výrazne zvýšila digitalizácia nášho hospodárstva a spoločnosti, ako sa ukázalo počas krízy spôsobenej pandémiou COVID-19, keď sa mnohé činnosti podarilo zachovať len vďaka kolektívnemu a masívnemu prechodu na vzdialené IT riešenia. Táto kríza naznačila, aká výhodná je naša závislosť od týchto technológií pre páchateľov kybernetických útokov. Ukázala aj to, ako sa oblasť kybernetických hrozieb rozšírila od cielených útokov až po nové formy masívnych ohrození miliónov podnikov a občanov vrátane rastúceho počtu sofistikovaných ransomvérových incidentov. Rýchly vývoj digitálnych produktov a služieb, od cloudu a videokonferencií po technológiu 5G a umelú inteligenciu, priniesol aj nové výzvy, ktoré je potrebné spoznať a riešiť.

ENISA má vďaka trvalému mandátu a rozšíreným úlohám a kapacitám viac ako kedykoľvek predtým zohrávať vedúcu úlohu pri podpore EÚ a jej členských štátov pri riešení týchto výziev na počiatku novej éry kybernetickej bezpečnosti v Európe.

ENISA sa má pri tom zamerať na predvídanie príslušných trendov a získavanie a spoločné využívanie aktuálnych skúseností a vedomostí určených pre všetkých. Bude podporovať Európsku komisiu a členské štáty, aby pomáhali verejnosti, súkromným subjektom a občanom pri predchádzaní rizikám súvisiacim s kybernetickými incidentmi a ich riadení. ENISA prispeje k zmene paradigmy vykonávaním rámca certifikácie kybernetickej bezpečnosti, čím sa zlepší úroveň bezpečnosti digitálnych riešení zavedených v Európe. Zvýši sa tak všeobecná schopnosť výberu a dôveryhodnosť. Agentúra bude takisto aktívne podporovať prevádzkové subjekty v oblasti európskej bezpečnosti, aby úzko spolupracovali a pripravovali sa na spoločnú reakciu na nasledujúce rozsiahle kybernetické útoky v Európe.

Pri preberaní novej úlohy budú kľúčovými prvkami každodenných činností ENISA otvorenosť, pružnosť a spoľahlivosť a užšia spolupráca s členskými štátmi a Európskou komisiou s cieľom zosúladiť prístupy. ENISA sa takisto bude snažiť o ekologickejší prístup v kontexte prebiehajúcej klimatickej krízy a vytvorenie spoločensky zodpovedného a inkluzívneho pracovného prostredia.

V tomto strategickom dokumente vypracovanom za vzájomnej spolupráce všetkých pracovníkov ENISA a členov jej správnej rady a poradnej skupiny sú stanovené jasné ciele, ktorými sa bude ENISA riadiť v nasledujúcich rokoch pri riešení budúcich výziev, ktorých nebude málo.

V mene správnej rady

Jean-Baptiste Demaison
predseda správnej rady

Krzysztof Silicki
podpredseda správnej rady

VÍZIA

Dôveryhodná a kyberneticky bezpečná Európa

POSLANIE

Poslaním Agentúry Európskej únie pre kybernetickú bezpečnosť (ENISA) je dosiahnuť vysokú všeobecnú úroveň kybernetickej bezpečnosti v rámci Únie v spolupráci so širším spoločenstvom. Svoje poslanie napĺňa tým, že pôsobí ako centrum odbornosti v oblasti kybernetickej bezpečnosti, pričom získava a poskytuje nezávislé, vysokokvalitné technické poradenstvo a pomoc členským štátom a orgánom EÚ v oblasti kybernetickej bezpečnosti. Prispieva k rozvoju a vykonávaniu politík Únie v oblasti kybernetiky.

Naším cieľom je posilniť dôveru v prepojenú ekonomiku, zvýšiť odolnosť a dôveryhodnosť infraštruktúry a služieb poskytovaných v rámci Únie a zaistiť digitálnu bezpečnosť našej spoločnosti a občanov. Chceme byť pružnou, environmentálne a spoločensky zodpovednou organizáciou zameranou na ľudí.

HODNOTY

Zameranie na spoločenstvá
ENISA v rámci plnenia svojho poslania pracuje so spoločenstvami, rešpektuje ich kompetencie a odbornosť a presadzuje synergie a dôveru.

Excelentnosť
ENISA sa pri svojej práci snaží o odbornosť na základe aktuálnych odborných znalostí a zachovanie najvyšších noriem činnosti a vyhodnocuje svoje pôsobenie v snahe o neustále zlepšovanie prostredníctvom inovácie a prognózovania.

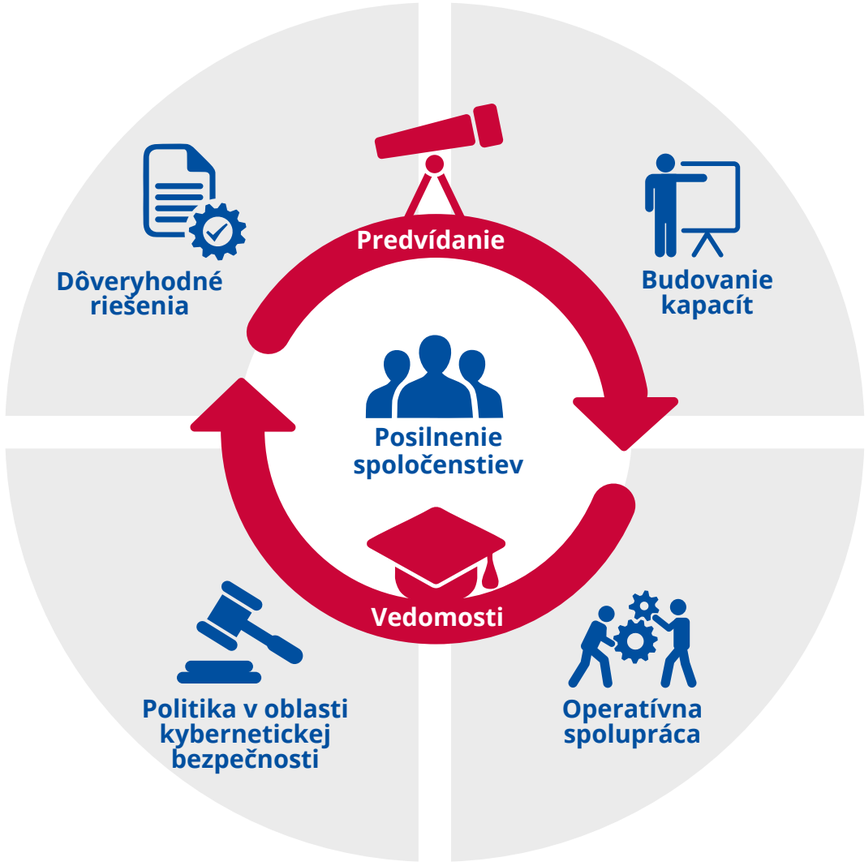
Integrita/etika
ENISA pri poskytovaní služieb a v rámci svojho pracovného prostredia dodržiava etické princípy a pravidlá a povinnosti dôležité pre EÚ, ktoré zabezpečujú spravodlivosť a inkluzívnosť.

Rešpekt
ENISA v rámci všetkých poskytovaných služieb a pracovného prostredia rešpektuje základné európske práva a hodnoty, ako aj očakávania zainteresovaných strán.

Zodpovednosť
ENISA si uvedomuje svoju zodpovednosť, preto do svojej činnosti a postupov začleňuje spoločenský a environmentálny rozmer.

Transparentnosť
ENISA zavádza postupy, štruktúry a procesy, ktoré sú otvorené, vecné a nezávislé, čo zabraňuje zaujatosti, nejednoznačnosti, podvodom a netransparentnosti.

STRATEGICKÉ CIELE



SO1

Strategický cieľ

SILNÉ A ANGAŽOVANÉ KOMUNITY V RÁMCI EKOSYSTÉMU KYBERNETICKEJ BEZPEČNOSTI

Kontext

Kybernetická bezpečnosť je spoločná zodpovednosť. Európa sa snaží vytvoriť medzisektorový komplexný rámec spolupráce. ENISA zohráva kľúčovú úlohu pri podpore aktívnej spolupráce medzi zainteresovanými stranami v oblasti kybernetickej bezpečnosti v členských štátoch a inštitúciách a agentúrach EÚ. Snaží sa zabezpečiť komplementárnosť spoločného úsilia vytvorením pridanej hodnoty pre zainteresované strany, skúmaním synergií a účinným využívaním obmedzených odborných znalostí a zdrojov v oblasti kybernetickej bezpečnosti. Spoločenstvá je potrebné posilniť s cieľom rozšíriť model kybernetickej bezpečnosti.

Čo chceme dosiahnuť

- Vytvoriť súbor aktuálnych znalostí o koncepciách a postupoch v oblasti kybernetickej bezpečnosti na úrovni EÚ, ktorý prispieva k budovaniu spolupráce medzi kľúčovými aktérmi na poli kybernetickej bezpečnosti, rozširuje získané skúsenosti a odborné znalosti v rámci EÚ a vytvára nové synergie.
- Posilnený ekosystém kybernetickej bezpečnosti zahŕňajúci úrady členských štátov, inštitúcie, agentúry a orgány EÚ, združenia, výskumné strediská a univerzity, priemysel, súkromné subjekty a občanov, ktorí všetci majú svoju úlohu pri budovaní kyberneticky bezpečnej Európy.

SO2

Strategický cieľ

KYBERNETICKÁ BEZPEČNOSŤ AKO NEODDELITEĽNÁ SÚČASŤ POLITÍK EÚ

Kontext

Kybernetická bezpečnosť je základom digitálnej transformácie a je potrebná vo všetkých odvetviach, preto je potrebné ju zohľadniť v rámci širokej škály politických oblastí a iniciatív. Kybernetická bezpečnosť sa nesmie obmedziť len na odborné kruhy technických expertov v oblasti kybernetiky. Kybernetická bezpečnosť preto musí byť súčasťou všetkých oblastí politiky EÚ. Je nevyhnutné vyhnúť sa trieštеniu a zabezpečiť súdržný prístup pri súčasnom zohľadnení osobitostí každého odvetvia.

Čo chceme dosiahnuť

- Proaktívne poradenstvo a podporu pre všetky príslušné subjekty na úrovni EÚ pri začleňovaní aspektu kybernetickej bezpečnosti do cyklu tvorby politík prostredníctvom cielených technických usmernení.
- Rámce riadenia rizík v oblasti kybernetickej bezpečnosti zavedené do všetkých odvetví a dodržiavané počas celého cyklu tvorby politík týkajúcich sa kybernetickej bezpečnosti.

SO3

Strategický cieľ

ÚČINNÁ SPOLUPRÁCA MEDZI ZÚČASTNENÝMI SUBJEKTMI V RÁMCI ÚNIE V PRÍPADE MASÍVNYCH KYBERNETICKÝCH INCIDENTOV

Kontext

Výhody európskej digitálnej ekonomiky a spoločnosti možno naplno dosiahnuť len v podmienkach kybernetickej bezpečnosti. Kybernetické útoky nepoznajú hranice. Zasiahnuté môžu byť všetky úrovne spoločnosti a Únia musí byť pripravená reagovať na masívne (rozsiahle a presahujúce hranice štátov) kybernetické útoky a kybernetickú krízu. Vzájomná prepojenosť prekračujúca hranice štátov poukázala na potrebu účinnej spolupráce medzi členskými štátmi a inštitúciami EÚ, aby dokázali rýchlejšie reagovať a lepšie koordinovať úsilie na všetkých úrovniach (strategickej, prevádzkovej, technickej a komunikačnej).

Čo chceme dosiahnuť

- Plynulú cezhraničnú a medziúrovňovú podporu spolupráce medzi členskými štátmi, ako ja inštitúciami EÚ. Najmä z hľadiska prípadných rozsiahlych incidentov a kríz podporu rozšírenia odbornej prevádzkovej, politickej a strategickej spolupráce medzi kľúčovými subjektmi s cieľom umožniť včasnú reakciu, spoločné využívanie informácií, situačnú informovanosť a krízovú komunikáciu v rámci Únie.
- Komplexnú a rýchle technické riešenie na žiadosť členských štátov s cieľom napĺňať technické a prevádzkové potreby pri riadení incidentov a kríz.

SO4

Strategický cieľ

ŠPIČKOVÉ KOMPETENCIE A SCHOPNOSTI V OBLASTI KYBERNETICKEJ BEZPEČNOSTI V RÁMCI ÚNIE

Kontext

Frekvencia a dômyselnosť kybernetických útokov sa rýchlo zvyšujú a súčasne sa výrazne rozširuje využívanie infraštruktúr a technológií IKT zo strany jednotlivcov, organizácií a priemyselných odvetví. Potreba znalostí a kompetencií v oblasti kybernetickej bezpečnosti presahuje ponuku. EÚ musela investovať do budovania kompetencií a talentov v oblasti kybernetickej bezpečnosti na všetkých úrovniach, od laikov až po vysokokvalifikovaných odborníkov. Investície by sa mali zamerať nielen na zvýšenie zručností v oblasti kybernetickej bezpečnosti v členských štátoch, ale aj na zabezpečenie toho, aby mali rôzne prevádzkové subjekty dostatočnú kapacitu na riešenie panorámy kybernetických hrozieb.

Čo chceme dosiahnuť

- Zosúladené kompetencie, odborné skúsenosti a vzdelávacie štruktúry v oblasti kybernetickej bezpečnosti, ktoré zodpovedajú neustále sa zvyšujúcej potrebe znalostí a kompetencií v tejto oblasti v EÚ.
- Vyššiu úroveň informovanosti o kybernetickej bezpečnosti a kompetencií v tejto oblasti v rámci EÚ a súčasne začlenenie kybernetiky do nových disciplín.
- Dobre pripravené a vyskúšané schopnosti spolu s príslušnou kapacitou reagovať v rámci EÚ na vyvíjajúce sa hrozby.

SO5

Strategický cieľ

VYSOKÁ ÚROVEŇ DÔVERY VOČI BEZPEČNÝM DIGITÁLNYM RIEŠENIAM

Kontext

Digitálne produkty a služby prinášajú výhody aj riziká a tieto riziká sa musia identifikovať a zmierniť. V procese posudzovania bezpečnosti digitálnych riešení a zabezpečenia ich spoľahlivosti je nevyhnutné prijať spoločný prístup s cieľom dosiahnuť rovnováhu medzi potrebami spoločnosti, trhu, hospodárstva a kybernetickej bezpečnosti. Neutrálny subjekt konajúci transparentným spôsobom zvýši dôveru zákazníka v digitálne riešenia a širšie digitálne prostredie.

Čo chceme dosiahnuť

- Kyberneticky bezpečné digitálne prostredie v rámci EÚ, kde môžu občania dôverovať produktom, službám a procesom IKT vďaka zavedeniu certifikačných systémov v kľúčových technologických oblastiach.

SO6

Strategický cieľ

PREDVÍDANIE VZNIKAJÚCICH A BUDÚCICH VÝZIEV V OBLASTI KYBERNETICKEJ BEZPEČNOSTI

Kontext

Metódy predvídania by boli prínosom pre viaceré nové technológie, na začiatku ich vývoja alebo tesne pred ich všeobecným prijatím. Vďaka štruktúrovanému procesu, ktorý umožní dialóg medzi zainteresovanými stranami, subjektmi s rozhodovacou právomocou a tvorcami politík, by malo byť možné definovať stratégie umožňujúce včasné zmiernenie rizík, ktoré zvýšia odolnosť EÚ voči hrozbám v oblasti kybernetickej bezpečnosti, a nájsť riešenia umožňujúce reagovať na vznikajúce výzvy.

Čo chceme dosiahnuť

- Pochopenie objavujúcich sa trendov a modelov pomocou predvídania a scenárov budúceho vývoja, ktoré prispievajú k zmierneniu rizík v oblasti kybernetickej bezpečnosti pre zainteresované strany.
- Včasné posúdenie výziev a rizík vyplývajúcich z prijatia vznikajúcich budúcich možností a prispôsobenia sa týmto možnostiam a súčasne spolupráca so zainteresovanými stranami na vhodných stratégiách na zmiernenie rizík.

SO7

Strategický cieľ

EFEKTÍVNE A ÚČINNÉ RIADENIE INFORMÁCIÍ A VEDOMOSTÍ V OBLASTI KYBERNETICKEJ BEZPEČNOSTI PRE EURÓPU

Kontext

Energiou, ktorá poháňa mechanizmus kybernetickej bezpečnosti, sú informácie a vedomosti. Aby boli odborníci v oblasti kybernetickej bezpečnosti schopní účinne dosahovať naše ciele, pracovať v neustále sa meniacom prostredí – z hľadiska digitálneho vývoja, ako aj vo vzťahu k zúčastneným – s cieľom čeliť výzvam tohto času, potrebujeme priebežne zberať, organizovať, sumarizovať, analyzovať, oznamovať a uchovávať informácie a vedomosti z oblasti kybernetickej bezpečnosti. Všetky fázy sú dôležité, aby sa zabezpečilo spoločné využívanie informácií a vedomostí a ich rozšírenie v rámci ekosystému kybernetickej bezpečnosti v EÚ.

Čo chceme dosiahnuť

- Riadenie spoločne využívaných informácií a vedomostí pre ekosystém kybernetickej bezpečnosti v EÚ prístupným, prispôsobeným, včasným a použiteľným spôsobom s vhodnou metodikou, infraštruktúrou a nástrojmi spolu s metódami zabezpečenia kvality s cieľom dosiahnuť neustále zdokonaľovanie služieb.

O AGENTÚRE ENISA

Agentúra Európskej únie pre kybernetickú bezpečnosť, ENISA, je agentúra Únie, ktorej úlohou je zabezpečovať vysokú spoločnú úroveň kybernetickej bezpečnosti v Európe. Agentúra Európskej únie pre kybernetickú bezpečnosť, ktorá vznikla v roku 2004 a jej postavenie posilnil akt EÚ o kybernetickej bezpečnosti, zvyšuje dôveryhodnosť produktov, služieb a procesov IKT prostredníctvom systémov certifikácie v oblasti kybernetickej bezpečnosti, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe pripraviť sa na kybernetické výzvy budúcnosti. Agentúra prostredníctvom spoločného využívania vedomostí, budovania kapacít a zvyšovania informovanosti spolupracuje s kľúčovými zainteresovanými stranami s cieľom posilniť dôveru v rámci prepojenej ekonomiky, zvýšiť odolnosť infraštruktúry Únie a v konečnom dôsledku zachovať digitálnu bezpečnosť európskej spoločnosti a občanov Európy. Ďalšie informácie o agentúre ENISA a jej práci nájdete na webovom sídle www.enisa.europa.eu.

TP-02-20-759-SK-N

ENISA
Agentúra Európskej únie pre kybernetickú bezpečnosť

Kancelária v Aténach
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Grécko

Kancelária v Heraklione
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Grécko

enisa.europa.eu