EURÓPSKY DVOR AUDÍTOROV

SK

Tlačová správa

Luxemburg 29. marca 2022

Orgány EÚ musia zlepšiť svoju pripravenosť v oblasti kybernetickej bezpečnosti

Počet kybernetických útokov na orgány EÚ prudko narastá. Úroveň kybernetickej pripravenosti sa v jednotlivých orgánoch EÚ líši a celkovo nezodpovedá silnejúcim hrozbám. Keďže orgány EÚ sú úzko prepojené, slabé miesto v jednom z nich môže vystaviť bezpečnostným hrozbám aj ostatné. Toto je záver osobitnej správy Európskeho dvora audítorov, v ktorej sa analyzuje, ako sú na kybernetické hrozby pripravené riadiace orgány EÚ. Audítori odporúčajú, aby sa zaviedli záväzné pravidlá v oblasti kybernetickej bezpečnosti a zvýšil objem zdrojov, ktoré má k dispozícii tím reakcie na núdzové počítačové situácie (CERT-EU). Podľa audítorov by Európska komisia mala tiež ďalej podporovať spoluprácu medzi orgánmi EÚ, a tím CERT-EU a Agentúra Európskej únie pre kybernetickú bezpečnosť by sa mali viac zamerať na tie orgány EÚ, ktoré majú s riadením kybernetickej bezpečnosti menej skúseností.

Počet závažných incidentov v oblasti kybernetickej bezpečnosti v orgánoch EÚ sa v rokoch 2018 až 2021 zvýšil viac než desaťnásobne. Práca na diaľku výrazne zvýšila počet potenciálnych prístupových miest pre útočníkov. Závažné incidenty sú spravidla spôsobené komplexnými kybernetickými útokmi, ktoré zvyčajne zahŕňajú použitie nových metód a technológií a ich vyšetrenie a odstránenie ich dôsledkov môže trvať týždne alebo až mesiace. Jedným z príkladov je kybernetický útok na Európsku agentúru pre lieky, pri ktorom unikli citlivé údaje, ktoré boli zmanipulované tak, aby narušili dôveru vo vakcíny.

„Inštitúcie, orgány a agentúry EÚ sú lákavým terčom pre potenciálnych útočníkov, najmä pre skupiny, ktoré sú schopné uskutočniť veľmi sofistikované utajené útoky s cieľom kybernetickej špionáže či na iné účely,“ uviedla Bettina Jakobsen, členka EDA, ktorá tento audit viedla. *„Takéto útoky môžu mať vážne politické dôsledky, poškodiť celkovú povesť EÚ a oslabiť dôveru v jej inštitúcie. EÚ musí posilniť úsilie o ochranu svojich vlastných inštitúcií.“*

Hlavným zistením audítorov bolo, že inštitúcie, orgány a agentúry EÚ nie sú vždy dobre chránené pred kybernetickými hrozbami. Ku kybernetickej bezpečnosti nepristupujú jednotne, nemajú vždy zavedené základné kontroly a kľúčové osvedčené postupy týkajúce sa kybernetickej bezpečnosti, a poskytovaná odborná príprava v tejto oblasti nie je systematická. Prideľovanie zdrojov na kybernetickú bezpečnosť sa značne líši a niektoré orgány EÚ na ňu vynakladajú výrazne menej prostriedkov ako ich partneri podobnej veľkosti. Hoci rozdielne úrovne kybernetickej bezpečnosti by sa teoreticky dali vysvetliť odlišnými rizikovými profilmi orgánov a rôznou mierou citlivosti

Účelom tejto tlačovej správy je prezentovať hlavné body osobitnej správy Európskeho dvora audítorov. Úplné znenie správy je uverejnené na webovom sídle eca.europa.eu.

ECA Press

12, rue Alcide De Gasperi – L-1615 Luxembourg
E: press@eca.europa.eu @EUAuditors eca.europa.eu

údajov, s ktorými pracujú, audítori zdôrazňujú, že slabiny v oblasti kybernetickej bezpečnosti v jednom orgáne EÚ môžu vystaviť kybernetickým hrozbám aj niekoľko ďalších subjektov (všetky orgány EÚ sú navzájom prepojené a často sú napojené aj na verejné a súkromné organizácie v členských štátoch).

Dvomi hlavnými subjektmi EÚ poverenými poskytovaním podpory v oblasti kybernetickej bezpečnosti sú tím reakcie na núdzové počítačové situácie v inštitúciách, orgánoch a agentúrach EÚ (CERT-EU) a Agentúra Európskej únie pre kybernetickú bezpečnosť (ENISA). Pre obmedzené zdroje a skutočnosť, že sa prioritne riešia iné oblasti, však nedokážu orgánom EÚ poskytnúť všetku potrebnú podporu. Audítori konštatujú, že výmena informácií tiež nie je dostatočná: nie všetky orgány EÚ včas informujú o zraniteľných miestach a o závažných incidentoch v oblasti kybernetickej bezpečnosti, ktoré ich zasiahli a ktoré môžu zasiahnuť iné orgány.

Základné informácie

V súčasnosti neexistuje právny rámec pre informačnú a kybernetickú bezpečnosť v inštitúciách, orgánoch a agentúrach EÚ. Nevzťahuje sa na ne najvšeobecnejšia právna úprava EÚ o kybernetickej bezpečnosti, smernica o sieťovej a informačnej bezpečnosti (NIS) z roku 2016, ani jej navrhovaná revízia – smernica NIS2. K dispozícii nie sú ani ucelené informácie o finančných prostriedkoch, ktoré orgány EÚ vynaložili na kybernetickú bezpečnosť. Spoločné pravidlá v oblasti informačnej a kybernetickej bezpečnosti pre všetky orgány EÚ sú stanovené v oznámení o stratégii EÚ pre bezpečnostnú úniu na obdobie 2020 – 2025, ktoré Komisia zverejnila v júli 2020. V stratégii kybernetickej bezpečnosti EÚ v digitálnej dekáde, uverejnenej v decembri 2020, sa Komisia zaviazala predložiť návrh nariadenia o spoločných pravidlách kybernetickej bezpečnosti pre všetky orgány EÚ. Takisto navrhla vytvorenie nového právneho základu pre tím CERT-EU s cieľom posilniť jeho mandát a financovanie.

Osobitná správa 05/2022 *Kybernetická bezpečnosť inštitúcií, orgánov a agentúr EÚ: celková úroveň pripravenosti nezodpovedá hrozbám* je dostupná na webovom sídle EDA. EDA už na výzvy súvisiace s účinnou politikou EÚ v oblasti kybernetickej bezpečnosti upozornil aj vo svojom preskúmaní z roku 2019.

Kontakt pre tlač

Tlačové oddelenie EDA: press@eca.europa.eu

- Claudia Spiti: claudia.spiti@eca.europa.eu – Mobil: (+352) 691 553 547
- Vincent Bourgeais: vincent.bourgeais@eca.europa.eu – Mobil: (+352) 691 551 502
- Damijan Fišer: damijan.fiser@eca.europa.eu – Mobil: (+352) 621 552 224