EVROPSKÝ ÚČETNÍ DVŮR

CS

Tisková zpráva

Lucemburk 29. března 2022

Subjekty EU musí zvýšit svou připravenost v oblasti kybernetické bezpečnosti

Počet kybernetických útoků na subjekty EU prudce roste. Míra připravenosti v oblasti kybernetické bezpečnosti v subjektech EU u nich různá a obecně není úměrná rostoucím hrozbám. Jelikož subjekty EU jsou výrazně propojeny, nedostatky v jednom subjektu mohou zbývající subjekty vystavit bezpečnostním hrozbám. To je závěr zvláštní zprávy Evropského účetního dvora, která zkoumá, jak jsou správní subjekty EU připraveny čelit hrozbám v oblasti kybernetické bezpečnosti. Auditoři doporučují zavést závazná pravidla pro oblast kybernetické bezpečnosti a zvýšit objem zdrojů, které jsou dány k dispozici pracovní skupině pro reakci na počítačové hrozby (CERT-EU). Auditoři se domnívají, že Evropská komise by také měla podporovat další spolupráci subjektů EU a skupina CERT-EU a Agentura Evropské unie pro kybernetickou bezpečnost by měly zaměřit svou podporu na subjekty EU s nižší úrovní vyspělosti kybernetické bezpečnosti.

Počty závažných incidentů se mezi lety 2018 a 2021 zvýšily více než desetinásobně; práce na dálku výrazně zvýšila počet potenciálních přístupových bodů pro útočníky. Závažné incidenty jsou obecně způsobovány komplexními kybernetickými útoky, které obvykle zahrnují použití nových metod a technologií a vyšetřit je a eliminovat jejich následky může trvat týdny, pokud ne měsíce. Jedním z nedávných příkladů byl kybernetický útok na Evropskou agenturu pro léčivé přípravky, při němž došlo k úniku citlivých údajů, s nimiž bylo následně manipulováno tak, aby byla narušena důvěra v očkovací látky.

Pro potenciální útočníky, zejména pak skupiny schopné provádět vysoce sofistikované skryté útoky za účelem kybernetické špionáže i jinými nekalými účely, jsou orgány, instituce a jiné subjekty EU lákavým cílem, uvedla Bettina Jakobsenová, členka Evropského účetního dvora odpovědná za audit. *Úspěšné kybernetické útoky na subjekty EU mohou mít závažné politické důsledky, mohou poškodit celkovou pověst Evropské unie a podrývat důvěru v její instituce. EU musí zintenzívnit své úsilí a své organizace chránit.“*

Auditoři především zjistili, že orgány, instituce a jiné subjekty EU nejsou vždy dobře chráněny před kybernetickými hrozbami. Ke kybernetické bezpečnosti nepřistupují důsledně, ne vždy byly zavedeny zásadní kontroly a důležité osvědčené postupy v oblasti kybernetické bezpečnosti a odborná příprava v oblasti kybernetické bezpečnosti se neposkytuje systematicky. Alokace zdrojů na kybernetickou bezpečnost se výrazně liší a řada subjektů EU vydává na tuto oblast podstatně

Účelem této tiskové zprávy je informovat o hlavních sděleních zprávy Evropského účetního dvora o připravovaném auditu. Plné znění této zprávy je k dispozici na internetové stránce eca.europa.eu.

ECA Press

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

méně prostředků než ostatní subjekty srovnatelné velikosti. Auditoři zdůrazňují, že i když rozdíly v míře kybernetické připravenosti by teoreticky mohly být odůvodněny různými rizikovými profily organizací a rozdíly v míře citlivosti údajů, s nimiž operují, slabá místa jednoho subjektu přesto mohou vystavit kybernetickým hrozbám i řadu dalších organizací (subjekty EU jsou všechny vzájemně provázány a často napojeny na organizace ze soukromého i veřejného sektoru v členských státech).

Dvěma hlavními subjekty pověřenými poskytováním podpory v oblasti kybernetické bezpečnosti jsou skupina pro reakci na počítačové hrozby (CERT-EU) a Agentura Evropské unie pro kybernetickou bezpečnost (ENISA). Nicméně kvůli omezeným zdrojům nebo tomu, že jsou prioritně řešeny jiné oblasti, nebyly schopny poskytovat subjektům EU veškerou potřebnou podporu. Nedostatečné je, podle auditorů, i sdílení informací: například ne všechny subjekty EU včas poskytují informace o slabých místech a závažných incidentech v oblasti kybernetické bezpečnosti, které je zasáhly a které mohou zasáhnout i jiné subjekty.

Obecné informace

V současnosti neexistuje právní rámec pro informační bezpečnost a kybernetickou bezpečnost v orgánech, institucích a jiných subjektech EU. Nevztahuje se na ně nejširší právní úprava kybernetické bezpečnosti v EU, směrnice o bezpečnosti sítí a informací (NIS) z roku 2016, ani její navrhovaná revize, směrnice o kybernetické bezpečnosti (NIS2). Nejsou k dispozici ani souhrnné informace o finančních prostředcích vynakládaných subjekty EU na kybernetickou bezpečnost. Společná pravidla týkající se bezpečnosti informací a kybernetické bezpečnosti platná pro všechny subjekty EU jsou uvedena ve sdělení o strategii bezpečnostní unie EU na období 2020–2025, které Komise zveřejnila v červenci 2020. Ve strategii kybernetické bezpečnosti EU pro digitální dekádu, zveřejněné v prosinci 2020, se Komise zavázala navrhnout nařízení o společných pravidlech kybernetické bezpečnosti pro subjekty EU. Navrhla rovněž vytvoření nového právního základu pro CERT-EU, jenž by posílil mandát a financování této skupiny.

Zvláštní zpráva č. 5/2022 *Kybernetická bezpečnost orgánů, institucí a jiných subjektů EU: úroveň připravenosti obecně není úměrná hrozbám* je k dispozici na internetové stránce EÚD. EÚD také poukázal na výzvy související s účinnou politikou EU v oblasti kybernetické bezpečnosti ve svém přezkumu z roku 2019.

Kontakt pro tisk

Tiskové oddělení EÚD: press@eca.europa.eu

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