ODPOVĚDI EVROPSKÉ KOMISE

NA ZVLÁŠTNÍ ZPRÁVU EVROPSKÉHO ÚČETNÍHO DVORA

Kybernetická bezpečnost orgánů, institucí a jiných subjektů EU: úroveň připravenosti neúměrná hrozbám

Obsah

Tento dokument představuje odpovědi Evropské komise na připomínky zvláštní zprávy Evropského účetního dvora v souladu s článkem 259 finančního nařízení a bude zveřejněn společně se zvláštní zprávou.

I. ODPOVĚDI KOMISE VE STRUČNOSTI

a) Obecný úvod

Kybernetická bezpečnost se stala jednou z hlavních politických a pracovních priorit Evropské komise. Krize COVID urychlila naši závislost na digitálních službách (cloud computing, mobilní zařízení, umělá inteligence). Během posledních dvou let jsme byly svědky masivního přechodu na práci z domova. To znamená, že spolu s tímto přechodem se ve velké míře rozšířila i kybernetická kriminalita a kybernetická špionáž, což jsou dvě hlavní hrozby, kterým čelí orgány, instituce a jiné subjekty EU. Komise si je tohoto trendu vědoma. V oblasti kybernetické bezpečnosti prokázala důsledné a rozhodné vedení. Akt o kybernetické bezpečnosti, který vstoupil v platnost v roce 2019, mimo jiné rozšířil mandát Agentury Evropské unie pro kybernetickou bezpečnost (ENISA) a dal mu trvalý základ. Tímto aktem byla také ustavena formální spolupráce mezi agenturou ENISA a skupinou CERT-EU (skupina pro reakci na počítačové hrozby podporující všechny orgány, instituce a jiné subjekty EU). V roce 2020 Komise navrhla posílení směrnice o bezpečnosti sítí a informací a tato věc se blíží k dohodě v zákonodárném sboru.

Strategie kybernetické bezpečnosti z roku 2020 rovněž obsahovala tři opatření týkající se kybernetické bezpečnosti orgánů, institucí a jiných subjektů EU. Oznámila nařízení o bezpečnosti informací v orgánech, institucích a subjektech EU, nařízení o společných pravidlech kybernetické bezpečnosti pro orgány, instituce a jiné subjekty EU a svůj úmysl poskytnout nový právní základ pro skupinu CERT-EU, aby posílila její mandát a financování a zajistila jí odpovídající zdroje s ohledem na narůstající hrozby, rizika a incidenty.

Pokročily práce na přípravě těchto návrhů. I když kolegium návrhy dosud nepřijalo, předpokládá se, že budou přijaty v prvním čtvrtletí roku 2022. Důležité otázky projednávané mezi institucemi v této přípravné fázi se týkají právního základu návrhu, jakož i rozpočtové kapacity všech orgánů, institucí a jiných subjektů EU s cílem vyhovět požadavkům jak z hlediska financování jejich vlastních potřeb v oblasti kybernetické bezpečnosti, tak z hlediska nalezení nezbytných zdrojů na podporu skupiny CERT-EU, rozpočtu a především pracovních míst.

Připravenost orgánů, institucí a jiných subjektů EU v oblasti kybernetické bezpečnosti je na různé úrovni vyspělosti. Některé orgány, instituce a jiné subjekty EU skutečně vykazují dobré výsledky z hlediska kybernetické připravenosti a měly by i nadále hrát vůdčí roli, kdy budou podněcovat a inspirovat pokrok a další zlepšování napříč všemi oblastmi kybernetické bezpečnosti. Pro dosažení měřitelného pokroku je důležité vzít na vědomí různé úrovně vyspělosti jednotlivých orgánů, institucí a jiných subjektů EU a stanovit priority zaměřením opatření ke zlepšení především na ty orgány, instituce a jiné subjekty EU, kde zjištěné nedostatky vedou k nejvyššímu vystavení se riziku.

b) Stanovisko Komise ke klíčovým připomínkám a doporučením Evropského účetního dvora

Komise vítá zprávu Evropského účetního dvora o kybernetické bezpečnosti orgánů, institucí a jiných subjektů EU. Konstatuje, že zpráva zdůrazňuje důležitost společných právních rámců pro všechny orgány, instituce a jiné subjekty EU za účelem zvýšení celkové úrovně kybernetické bezpečnosti ve všech oblastech. Komise konstatuje, že hlavní připomínky a doporučení Evropského účetního dvora nejsou zaměřeny na vlastní provozní kybernetickou bezpečnost Komise, nýbrž na politickou roli

Komise při navrhování právních předpisů s cílem zvýšit kybernetickou vyspělost orgánů, institucí a jiných subjektů EU.

Budoucí nařízení o „bezpečnosti informací v orgánech, institucích a jiných subjektech EU“ a „společná pravidla kybernetické bezpečnosti pro orgány, instituce a jiné subjekty EU“ stanoví společná pravidla za účelem dosažení vysokých úrovní bezpečnosti informací a kybernetické bezpečnosti, avšak jejich provádění, v rámci organizačního a provozního kontextu jednotlivých orgánů, institucí a jiných subjektů EU (zejména jejich profilů hrozeb a rizik), zůstává autonomní odpovědností orgánů, institucí a jiných subjektů EU. Navrhované nařízení o kybernetické bezpečnosti bude mít mechanismy dodržování předpisů, které jsou odpovídající a přiměřené záměru a oblasti působnosti nových pravidel, aniž by tím byla dotčena autonomie orgánů, institucí a jiných subjektů.

Komise v současné době předsedá podskupině pro kybernetickou bezpečnost interinstitucionálního výboru pro digitální transformaci (ICDT), přičemž se jedná o jmenování na rotujícím základě (na období až dvou let). Je třeba poznamenat, že na práci této podskupiny nejsou vyčleněny žádné prostředky: veškerá opatření jsou založena na dobrovolném úsilí jejích účastníků.

Komise souhlasí s obecnou myšlenkou posílit zdroje a mandát skupiny CERT-EU.

S tímto vědomím Komise podporuje klíčové připomínky a doporučení zprávy. Naše podrobné stanovisko je vysvětleno v doplněném vyjádření v oddíle III. Pokud jde o doporučení, Komise přijímá doporučení 1a, b, c, d, e, f, g a 2a, b, c.

c) Relevantní nejnovější vývoj a další kroky

Byla dokončena formální konzultace na úrovni generálních ředitelů orgánů, institucí a jiných subjektů EU ke konsolidovaným návrhům dvou nařízení (bezpečnost informací, kybernetická bezpečnost) a probíhá posouzení obdržené zpětné vazby před dokončením balíčku a přijetí kolegiem v prvním čtvrtletí roku 2022.

II. ODPOVĚDI KOMISE NA HLAVNÍ PŘIPOMÍNKY EVROPSKÉHO ÚČETNÍHO DVORA

1. Úrovně vyspělosti kybernetické bezpečnosti orgánů, institucí a jiných subjektů EU

Komise souhlasí, že při sledování výše výdajů orgánů, institucí a jiných subjektů EU na kybernetickou bezpečnost je důležité vzít v úvahu hrozby a rizika.

Obdobně je i v oblasti lidských zdrojů stabilita personálního obsazení orgánů, institucí a jiných subjektů EU ovlivněna celou řadou faktorů. Trh s náborem specializovaných odborníků na kybernetickou bezpečnost je čím dál složitější. V mnoha případech nejsou pravidla pro lidské zdroje přizpůsobena specializovaným profilům (nábor, kariérní růst, vzdělávání). Všeobecný tlak na počty zaměstnanců v orgánech, institucích a jiných subjektech EU ze strany rozpočtového orgánu také znamená, že nově vznikající oblasti s vysokou prioritou, jako je oblast kybernetické bezpečnosti, zůstávají personálně nedostatečně zajištěny, zejména v interních operačních útvarech.

Odkaz na pokrok v oblasti správy a řízení rizik by měl vzít v úvahu skutečnost, že sledování dodržování předpisů nyní přechází z pilotního provozu na plné zavedení. Je tedy normální, že pokrytí je zatím poměrně nízké. Tento projekt dodržování předpisů je další etapou dlouhodobého procesu zlepšování kybernetické vyspělosti, který začal definováním společné metodiky rizik, vytvořením společných nástrojů, zavedením řízení zranitelností a sledováním, testováním a ověřováním inventáře aktiv. Na této dlouhé cestě bylo dosaženo pokroku navzdory složitosti majetkové základny Komise sestávající z více než 1 000 informačních systémů provozovaných více než 50 generálními ředitelstvími a výkonnými agenturami.

2. Mechanismy spolupráce orgánů, institucí a jiných subjektů EU

Skupina CERT-EU je fenomenálním příkladem úspěchu, pokud jde o podporování spolupráce nejen mezi orgány, institucemi a jinými subjekty EU, ale i na evropské úrovni, a to díky své účasti jakožto plnoprávný člen sítě CSIRT zřízené podle směrnice o bezpečnosti sítí a informací. Skupina CERT-EU je tak exemplárním příkladem toho, jak lze posílit spolupráci a služby v oblasti kybernetické bezpečnosti. Zjištění Evropského účetního dvora týkající se skupiny CERT-EU velmi jasně ilustrují vynikající práci, kterou skupina CERT-EU odvádí tváří v tvář stále nepřátelštějšímu prostředí v oblasti kybernetických hrozeb a při chronickém nedostatku zdrojů.

Na základě stávajícího interinstitucionálního ujednání (IIA) jsou decentralizované subjekty a společné podniky EU oficiálně zastoupeny v řídicí radě skupiny CERT-EU agenturou ENISA. Kromě toho jejich názory na zasedáních řídicí rady vyjadřuje zástupce Poradního výboru pro informační a komunikační technologie (ICTAC), který je oprávněn účastnit se zasedání a pomáhat agentuře ENISA v její roli zastupovat zmíněné subjekty, avšak nemá žádné formální místo ani hlasovací právo. Záležitost odpovídajícího zastoupení subjektů v řídicí radě skupiny CERT-EU bude v navrhovaném nařízení řešena doplněním složení řídicí rady o až tři zástupce jmenované sítí agentur EU (EUAN) na návrh jejího Poradního výboru pro informační a komunikační technologie.

Účast v podskupině pro kybernetickou bezpečnost ICDT je založena na maximálním úsilí, přičemž o úrovni zapojení rozhodují jednotlivé orgány, instituce a jiné subjekty EU. Zlepšení sdílení informací o zadávání zakázek, což je důležité téma v rámci pracovní skupiny 2 podskupiny pro kybernetickou bezpečnost, se řeší v souvislosti s přípravou nové rámcové smlouvy o kybernetické bezpečnosti.

Co se týká společných nástrojů pro služby, jako je elektronická pošta a videokonference, existuje již možnost používat systém SECEM-2, který Komise zavedla pro všechny orgány, instituce a jiné subjekty EU, pro šifrovanou elektronickou poštu v závislosti na účinné správě šifrovacích klíčů a certifikátů. Kromě toho je ve vývoji nástroj SECABC, který má umožnit šifrování elektronické pošty mezi institucemi s úmyslem nabídnout od roku 2022 přístup k tomuto nástroji všem orgánům, institucím a jiným subjektům EU, které o to projeví zájem. Zabezpečení videokonferencí pro služby SNC již bylo dosaženo a lze jej *ad hoc* rozšířit i na další orgány, instituce a jiné subjekty EU prostřednictvím správy identit účastníků zasedání. Sdílení citlivých informací bude také řešeno v navrhovaném nařízení o bezpečnosti informací (tj. pomocí společného označování a značení).

3. Sdílení informací o závažných incidentech či zranitelných místech

Skutečnost, že ne všechny orgány, instituce a jiné subjekty EU oznamují skupině CERT-EU závažné incidenty či zranitelná místa, je řešena v návrhu nařízení o kybernetické bezpečnosti v souladu s návrhem Komise ve směrnici NIS-2[1]. Úroveň provádění bude záviset na dodatečných zdrojích, které na to vyčlení autonomní orgány, instituce a jiné subjekty EU. Prostor pro prosazování těchto oznamování zůstává omezený, a to i v rámci navrhovaného nařízení, jak je v současné době plánováno, vzhledem k institucionální autonomii orgánů, institucí a jiných subjektů EU. Navrhované nařízení o kybernetické bezpečnosti bude mít mechanismy dodržování předpisů, které jsou odpovídající a přiměřené záměru a oblasti působnosti nových pravidel, aniž by tím byla dotčena autonomie orgánů, institucí a jiných subjektů.

III. KOMISE ODPOVÍDÁ NA ZÁVĚRY A DOPORUČENÍ EVROPSKÉHO ÚČETNÍHO DVORA

Doporučení 1 – Zlepšovat kybernetickou připravenost všech orgánů, institucí a jiných subjektů EU pomocí společných závazných pravidel a navýšení zdrojů pro skupinu CERT-EU

Navrhovaný text nařízení bude obsahovat konkrétní opatření, jejichž cílem je dále zvýšit společnou úroveň kybernetické bezpečnosti. Zmíněná opatření budou rozpracována do plánů kybernetické bezpečnosti, které budou definovány a prováděny na úrovni orgánů, institucí a jiných subjektů EU podle jejich vlastního rámce pro řízení kybernetické bezpečnosti.

Komise toto doporučení přijímá. Co se týká konkrétních dílčích doporučení, Komise konstatuje následující:

a) Komise doporučení 1a přijímá. Návrh nařízení bude obsahovat ustanovení o řídicích a kontrolních rámcích vytvořených na nejvyšší úrovni výkonného řízení jednotlivých orgánů, institucí a jiných subjektů EU, aby bylo zajištěno účinné a obezřetné řízení veškerých rizik v oblasti kybernetické bezpečnosti.
b) Komise doporučení 1b přijímá. Návrh nařízení posílí důraz na přístup k řízení kybernetické bezpečnosti založený na riziku tím, že jasně stanoví, že opatření, plány bezpečnosti IT a skutečné provádění základních kontrolních mechanismů by měly následovat po posouzení.
c) Komise doporučení 1c přijímá. Jako součást základní úrovně kybernetické bezpečnosti budou v návrhu nařízení uvedeny vzdělávání, poskytování informací a programy odborné přípravy.
d) Komise doporučení 1d přijímá. Podle našich zkušeností jsou sice pravidelné audity a testy nezbytné, nepostačují však k zajištění pokroku. Nezbytnou součástí rámce pro řízení kybernetické bezpečnosti podle písmene a) je tedy pravidelné podávání zpráv a transparentnost.

[1] Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o zrušení směrnice (EU) 2016/1148, COM(2020) 823 final.

e) Komise doporučení 1e přijímá. Návrh nařízení bude obsahovat ustanovení týkající se oznamování závažných kybernetických hrozeb, zranitelných míst a incidentů ze strany orgánů, institucí a jiných subjektů EU skupině CERT-EU.
f) Komise doporučení 1f přijímá. Komise podporuje potřebu posílit zdroje skupiny CERT-EU. Ve znění návrhu nařízení budou obsažena ustanovení týkající se personálního obsazení a finančních příspěvků orgánů, institucí a jiných subjektů EU.
g) Komise doporučení 1g přijímá. Navrhované nařízení bude mít mechanismy dodržování předpisů, které jsou přiměřené a odpovídající záměru a oblasti působnosti těchto ustanovení s ohledem na institucionální autonomii orgánů, institucí a jiných subjektů EU. Obsah budoucího nařízení závisí na výsledku legislativního procesu a je výsledkem rozhodnutí přijatého zákonodárcem EU s ohledem na návrh Komise.

Doporučení 2 – Zasazovat se ve vybraných oblastech o další synergie mezi orgány, institucemi a jinými subjekty EU

Komise, která nyní předsedá podskupině pro kybernetickou bezpečnost interinstitucionálního výboru pro digitální transformaci (ICDT), souhlasí s doporučeními prosazovat řešení pro konzistentní a bezpečné sdílení citlivých informací, systematické sdílení informací o projektech v oblasti kybernetické bezpečnosti a rámce pro společné zadávání zakázek a smluv na služby v oblasti kybernetické bezpečnosti.

Komise toto doporučení přijímá. Co se týká konkrétních dílčích doporučení, Komise konstatuje následující:

a) Komise doporučení 2a přijímá. Komise do podskupiny pro kybernetickou bezpečnost interinstitucionálního výboru pro digitální transformaci (ICDT) přináší technické iniciativy a služby s cílem prosazovat a podporovat společné nástroje pro sdílení citlivých informací, které umožňují služby, jako je elektronická pošta a videokonference. Rovněž poznamenáváme, že společná označení a společná pravidla pro zacházení s citlivými neutajovanými informacemi budou řešena v navrhovaném nařízení o bezpečnosti informací.
b) Komise doporučení 2b přijímá. Stávající pracovní skupiny v rámci podskupiny pro kybernetickou bezpečnost interinstitucionálního výboru pro digitální transformaci (ICDT) se touto věcí zabývají a bude dále rozvíjena. Zlepšení sdílení informací o veřejných zakázkách je řešeno v rámci přípravy nové rámcové smlouvy o kybernetické bezpečnosti.
c) Komise doporučení 2c přijímá. Orgány, instituce a jiné subjekty EU již mají přístup k interinstitucionálním rámcovým smlouvám v oblasti informačních a komunikačních technologií, které spravuje Komise. Příprava nové rámcové smlouvy o kybernetické bezpečnosti bude koordinována s podskupinou pro kybernetickou bezpečnost interinstitucionálního výboru pro digitální transformaci (ICDT).

Doporučení 3 – Věnovat v činnosti týmu CERT-EU a agentury ENISA větší pozornost méně vyspělým orgánům, institucím a jiným subjektům EU

Toto doporučení je adresováno skupině CERT-EU a agentuře ENISA.