Rozvoj certifikace kybernetické bezpečnosti Evropské Unie

Autor: ENISA – Evropská agentura pro bezpečnost sítí a informací (březen 2023)

Zdroj: Informační portály ENISA

Souhrn

Ad https://www.enisa.europa.eu/topics/certification

Evropská Unie (dále jen „EU“) prostřednictvím agentury ENISA vyvíjí certifikaci kybernetické bezpečnosti EU, která poskytuje důkaz o shodě s danou úrovní důvěry.

Poslání agentury ENISA v tomto směru: „Proaktivně přispívat ke vznikajícímu rámci EU pro certifikaci produktů a služeb v oblasti informačních a komunikačních technologií (dále jen „ICT“) a provádět sestavování kandidátských certifikačních schémat v souladu se zákonem o kybernetické bezpečnosti o doplňkové služby a úkoly“.

Certifikace kybernetické bezpečnosti EU je představena na následující webové stránce. V dnešní době je to krátké a jednoduché s cílem zajistit transparentnost a rozšířit koncept certifikace kybernetické bezpečnosti EU. Web bude dlouhodobě prezentovat harmonizaci kybernetické bezpečnosti mezi zeměmi EU prostřednictvím zobrazení katalogu EU certifikovaných ICT řešení a jejich certifikátů a také zveřejněných schémat a informací o přechodu.

Ad https://certification.enisa.europa.eu/

Certifikace je nástroj, který umožňuje prodejcům produktů a poskytovatelům služeb demonstrovat a propagovat kybernetickou bezpečnost jejich řešení. **Cílem rozvoje certifikace** kybernetické bezpečnosti na úrovni EU je harmonizovat uznávání úrovně kybernetické bezpečnosti řešení ICT v celé Unii, což prodejcům a poskytovatelům služeb umožní oslovit více zákazníků.

K tomu slouží zejména:

- směrnice pro vysokou úroveň kybernetické bezpečnosti v celé Unii (NIS2) se zaměřením na kritickou infrastrukturu,
- navrhované nařízení o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním trhu (nařízení eIDAS) s nařízením o peněžence,
- navrhovaný zákon Cyber Resilience Act (CRA), který ke kritériím pro získání označení CE přidává kybernetickou bezpečnost,
- navrhovaný zákon o umělé inteligenci.

V různých fázích jsou aktuálně vyvíjena tři schémata:

- **EUCC – První** schéma European Cybersecurity Certification Scheme on Common Criteria se zaměřuje na produkty ICT, jako jsou hardwarové a softwarové produkty a komponenty. ENISA s podporou ad-hoc pracovní skupiny a členských států vyvinula kandidátský systém, který získal kladné stanovisko od členských států zastoupených v ECCG (The European Cybersecurity Certification Group). Schéma bylo předáno Evropské komisi, aby bylo transformováno do prováděcího zákona. Po dokončení vstoupí certifikační schéma v platnost.
- **EUCS – Evropské** certifikační schéma pro cloudové služby bylo navrženo s podporou ad-hoc pracovní skupiny a s podporou členských států. Text by nyní měl vstoupit do procesu stanoviska ECCG.
- **EU5G – Evropský** systém certifikace kybernetické bezpečnosti pro 5G se vyvíjí ve dvou fázích. Během první fáze, která skončila na podzim 2022, analyzovali odborníci ENISA v rámci ad-hoc pracovní skupiny s Komisí EU a členskými státy stávající průmyslová hodnocení a certifikační schémata a jejich nezbytné aktualizace, aby byly v souladu se zákonem o kybernetické bezpečnosti. První návrh schématu by měl být k dispozici k veřejné konzultaci kolem poloviny roku 2023.

Kdo je těmito procesy dotčený:

Národní certifikační úřady pro kybernetickou bezpečnost (NCCA)

Jak vyžaduje zákon o kybernetické bezpečnosti, každý členský stát určil NCCA, která bude mít na starosti dohled, certifikaci a monitorování certifikací EU v oblasti kybernetické bezpečnosti na vnitrostátní úrovni a výměnu na úrovni EU.

Orgány posuzování shody (CAB)

Systémy certifikace kybernetické bezpečnosti EU vyvíjí agentura ENISA s podporou odborníků z členských států a z odvětví, včetně komunity posuzování shody. Tyto systémy jsou navrženy tak, aby vyhovovaly potřebám členských států, průmyslu a požadavkům evropské regulace, což z nich činí cenný nástroj na evropské úrovni pro podporu bezpečnosti produktů a služeb. Tato nová hodnota představuje významnou příležitost pro SPS, které budou akreditovány k vydávání certifikátů nebo k provádění hodnotících činností (testů, auditů) pro tato schémata.

Prodejci produktů a poskytovatelé služeb

Certifikace kybernetické bezpečnosti EU přinese nové příležitosti na trhu v celé EU tím, že zjednoduší úsilí při prokazování souladu s kybernetickou bezpečností. Certifikovaná řešení se budou moci na trhu prosadit a práce za nimi podpoří rozvoj interní odbornosti. Pro ty, kteří již získali certifikaci se stávajícími systémy, poskytnou ENISA a členské státy pokyny k usnadnění procesu přechodu a porovnají požadavky ze stávajících systémů na systémy EU, aby přechod usnadnily.

Uživatelé certifikátů

Certifikáty kybernetické bezpečnosti EU jsou udělovány certifikovaným ICT produktům a službám podle certifikačních schémat EU pro kybernetickou bezpečnost. Prokazují, že testovaná řešení jsou odolná vůči určitým úrovním útoků, nastavují procesy nápravy při zohlednění nejnovějšího vývoje.

Jsou uznávány v celé Unii a umožňují prodejcům produktů a poskytovatelům služeb předvést soulad jejich řešení s konkrétním schématem, úrovní jistoty, rozsahem a potenciálně rozšířením nebo bezpečnostními profily.

Certifikáty jsou platné po omezenou dobu, kterou lze prodloužit přehodnocením řešení.