Evropské systémy certifikace kybernetické bezpečnosti

Ing. Hana Švecová

Národní úřad
pro kybernetickou
a informační bezpečnost

OBSAH

- Zahájení odborného setkání
- Organizační pokyny
- Cíle odborného setkání
- Dílčí části
- Diskuze

CÍLE ODBORNÉHO SETKÁNÍ

- Představení a diskuze s odbornou veřejností nad Evropským systémem certifikace kybernetické bezpečnosti procesů, produktů a služeb.
- Navázání další spolupráce v oblasti kybernetické bezpečnosti, jejíž cílem bude zvyšování kybernetické bezpečnosti na úrovni ČR při zapojení akademických institucí, veřejné správy (krajů) a dalších významných organizací.
- Zvýšení kybernetické bezpečnosti v ČR

PROGRAM ODBORNÉHO SETKÁNÍ

- Zahájení odborného setkání a přivítání účastníků
- Nařízení EU – aktuální stav
- Vznik a důvody pro přijetí nařízení
- Český institut pro akreditaci o.p.s.
- Postavení a role NÚKIB, dopady na právní řád ČR
- Evropské systémy certifikace kybernetické bezpečnosti - certifikace procesů, produktů a služeb
- Přínosy EU certifikace kybernetické bezpečnosti procesů, produktů a služeb
- Možné dopady nařízení na povinné osoby podle ZKB
- Diskuze

NAŘÍZENÍ - CYBER SECURITY ACT (CSA)

Aktuální stav:

- Implementace nařízení EU do národní legislativy.
- ECCG
- Spolupráce s akademickou obcí, veřejnou správou a dalšími významnými organizacemi v oblasti kybernetické bezpečnosti.
- Další vývoj

VZNIK A DŮVODY PRO PŘIJETÍ NAŘÍZENÍ

- CSA (Cyber Security Act) v čase příprav a schvalování nařízení.
- Legislativní role a postavení NÚKIB při schvalování nařízení na úrovni EU.
- Mezinárodní dopady nařízení na legislativu členských států EU.

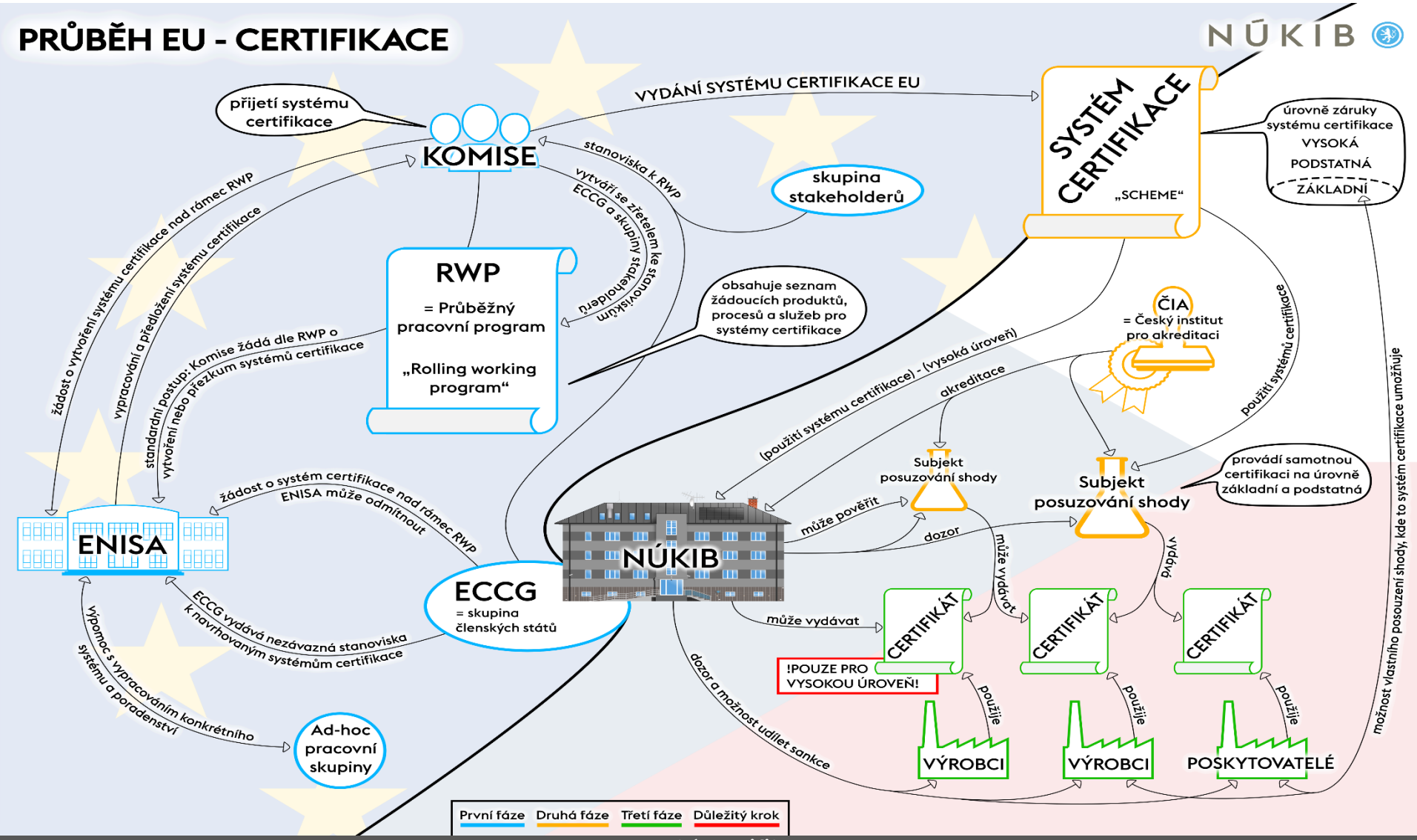
ROLE NÚKIB

- Vnitrostátní orgán certifikace.
- Kontrolní činnost při dodržování pravidel v evropských systémech certifikace.
- Řešení stížností v souvislosti s evropskými certifikáty.
- Sankční činnost.
- Spolupráce s akademickou obcí, veřejnou správou a organizacemi řešící kybernetickou bezpečnost.

DOPADY NA PRÁVNÍ ŘÁD ČR

- Nařízení EU – povinnost implementace do národní legislativy.
- Členským státům ponechána možnost vlastní úpravy (dobrovolné a povinné certifikace).
- Novela z.č. 181/2014 Sb. O kybernetické bezpečnosti (ZKB).
- Vztah nařízení EU k povinným subjektům podle ZKB.
- Účinnost implementace nařízení.

GRAFICKÉ SCHÉMA



ČESKÝ INSTITUT PRO AKREDITACI - ČIA

- Představení a působnost organizace v návaznosti na nařízení EU.
- Představení podmínek pro udělení akreditace.

NÁRODNÍ AKREDITAČNÍ ORGÁN

AGENTURA ENISA

Hlavní role:

- Zajištění vysoké a účinné úrovně bezpečnosti sítí a informací.
- Vytvoření unijní kultury s cílem zvýšení kybernetické bezpečnosti v zájmu občanů, spotřebitelů, podniků a veřejné správy.
- Boj proti kyberkriminalitě.

AGENTURA ENISA

Povinnosti agentury ENISA v rámci nařízení při zvyšování kybernetické bezpečnosti:

- Plnění úkolů dle nařízení.
- Poskytování poradenství.
- Centrum informací a znalostí v EU.
- Referenční politické místo pro iniciativy členských států.
- Vytváření expertních skupin pro řešení stanovené problematiky.

Evropská skupina pro certifikaci kybernetické bezpečnosti (ECCG)

Skupina zřízena dle čl. 62 a složená ze zástupců představitelů členských států.

Úkoly ECCG:

- Poskytovat pomoc a poradenství Komisi.
- Poskytovat poradenství a pomoc agentuře ENISA při vypracování certifikačních schémat.
- Podporovat výměnu informací v oblasti kybernetické bezpečnosti mezi členskými státy EU.

PRACOVNÍ SKUPINY ZŘIZOVANÉ AGENTUROU ENISA

V rámci vypracovávání certifikačních schémat jsou zřizovány pracovní skupiny dle zaměření:

- Schéma pro certifikaci cloudových služeb.
- Schéma pro certifikaci produktů (SOGIS).
- Schéma pro certifikace IoT.
- Schéma pro certifikaci procesů.

EVROPSKÉ SYSTÉMY CERTIFIKACE KYBERNETICKÉ BEZPEČNOSTI

- Hlavní důvody pro přijetí nařízení
- Bezpečnostní cíle
- Úrovně záruk certifikovaných produktů, procesů a služeb
- Dobrovolné certifikace
- Povinné certifikace
- Subjekty posuzování shody
- Dopady na veřejný rozpočet
- Dotčené subjekty

EVROPSKÉ SYSTÉMY CERTIFIKACE PROCESŮ, PRODUKTŮ A SLUŽEB

Hlavní důvody pro přijetí nařízení:

- Sjednocení systémů pro certifikaci procesů, produktů a služeb v rámci EU.
- Vytvoření jednotných certifikačních schémat, vzájemné uznávání certifikátů mezi členskými státy EU.
- Zvýšení kybernetické bezpečnosti procesů, produktů a služeb.

BEZPEČNOSTNÍ CÍLE SYSTÉMŮ CERTIFIKACE

Bezpečnostní cíle evropských systémů kybernetické bezpečnosti jsou uvedeny v čl. 51 např.:

- identifikace a eliminace zranitelností,
- zajištění kontroly a přístupů dat k IS,
- ochrana ukládaných a zpracovávaných dat,
- zavedení procesů pro řízení bezpečnostních incidentů.

ÚROVNĚ ZÁRUK CERTIFIKACE

Evropský systém certifikace kybernetické bezpečnosti u produktů, služeb a procesů uvádí v čl. 52 tři úrovně:

- základní,
- Významná,
- vysoká.

DOBROVOLNÉ CERTIFIKACE

Využití evropské certifikace kybernetické bezpečnosti a EU prohlášení o shodě by mělo zůstat dobrovolné, pokud právo Unie nebo právní předpisy členských států přijaté v souladu s právem Unie nestanoví jinak.

Dle čl. 56

Certifikace kybernetické bezpečnosti je dobrovolná, nestanoví-li unijní nebo vnitrostátní právo jinak.

POVINNÉ CERTIFIKACE

- Zavedení povinných certifikací je uvažováno do budoucna na základě hodnocení komise, která každé dva roky vyhodnotí aktuální stav kybernetické bezpečnosti v členských státech EU.
- První hodnocení proběhne nejpozději do 31.12. 2023
- Lze předpokládat zavedení povinných certifikací od roku 2024.

SUBJEKTY POSUZOVÁNÍ SHODY

- Subjekty posuzování shody jsou akreditovány vnitrostátními akreditačními orgány stanovenými podle nařízení (ES) č. 765/2008. Akreditace se vydá, pouze pokud subjekt posuzování shody splňuje požadavky stanovené v příloze tohoto nařízení.
- Akreditace je udělována po splnění požadavků akreditačního orgánu, kterým je v ČR ČIA o.p.s.
- Akreditace je udělována na dobu 5 let.

DOTČENÉ SUBJEKTY

Dotčenými subjekty mohou být:

- kraje, města, obce,
- organizace zřizované kraji a městy (nemocnice, ZŠ, SŠ a další organizace),
- komerční sektor,
- spotřebitelé.

DOPADY NA ROZPOČET

Zvýšení rozpočtů krajů, měst, obcí a dalších organizací jimiž jsou zřizovatelé.

PŘÍNOSY EU CERTIFIKACÍ KYBERNETICKÉ BEZPEČNOSTI PROCESŮ, PRODUKTŮ A SLUŽEB

- Kvalifikační kritéria při výběrových řízeních a veřejných zakázkách.
- Zvýšení kybernetické bezpečnosti v ČR - kraje, města, komerční sektor, spotřebitelé.

KVALIFIKAČNÍ KRITÉRIA PŘI VÝBĚROVÝCH ŘÍZENÍCH A VEŘEJNÝCH ZAKÁZKÁCH

- Dobrovolné využití certifikovaných produktů, procesů a služeb při veřejných zakázkách – **optimální varianta.**

- Povinné využití certifikovaných produktů, procesů a služeb při veřejných zakázkách – implementace do z.č. 134/2016 Sb. o veřejných zakázkách - **náročná a zdlouhavá varianta.**

Dopady nařízení na povinné subjekty podle ZKB a VKB

- Dobrovolné certifikace
- Povinné certifikace

ODBORNÁ DISKUZE

- Dopady na veřejnou správu např. v souvislosti se zlepšením zadáváním veřejných zakázek
- Evropská certifikační schémata – cloud computing, procesy, produkty, služby, IoT, dodavatelský řetězec, Smart technologie
- Jiné

BIBLIOGRAFICKÉ CITACE

Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“) (Text s významem pro EHP), roč. 151. 2019.

DĚKUJEME ZA POZORNOST