II. odborné setkání – implementace nařízení EU o certifikaci kybernetické bezpečnosti IKT

09.12.2020

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Úvodní slovo

Mgr. Luboš Fendrych
Ředitel odboru vzdělávání, výzkumu a projektů

II. odborné setkání k CSA

Program:

1. Úvodní slovo
2. Nařízení CSA – návrh novely ZKB
3. Aktuální stav přípravy systému EU certifikací kybernetické bezpečnosti v ČR:

a) informace z Českého institutu pro akreditaci, Evropské organizace pro spolupráci v oblasti akreditace

b) informace z NÚKIB, Evropské skupiny pro certifikace kybernetické bezpečnosti

4. Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti
5. Kandidátská schémata – návrh Common Criteria based European cybersecurity certification scheme (EUCC) a Cybersecurity Certification Scheme for Cloud Services, další
6. Q&A
7. Závěr

II. odborné setkání k CSA

Organizační pokyny

- Prosím, vypněte si kamery a mikrofony, pokud nemluvíte k účastníkům.
- Pokud bude v průběhu prezentace uváděn odkaz na nějaký dokument dostupný na webových stránkách, bude link zaslán v chatu.
- Na závěr setkání budou otázky a odpovědi.
  Po každé části bude prostor na krátké otázky a odpovědi k jednotlivým tématům.
  V případě otázky se, prosím, přihlaste zvednutím ruky v MSTeams.
  Pokud nebudou otázky zodpovězeny na tomto setkání, budou odpovědi zaslány emailem na všechny zúčastněné.
- S ohledem na plánovanou délku trvání tohoto setkání neplánujeme přestávku.

Nařízení CSA – návrh novely ZKB

Mgr. Pavel Štěpáník
Vedoucí oddělení vládní agendy a legislativy

II. odborné setkání k CSA

Návrh zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů s účinností ke dni 28. června 2021

Materiál - Portál Aplikace ODok

- NÚKIB je orgánem certifikace kybernetické bezpečnosti podle čl. 58 CSA
- Možnost uzavřít VPS za účelem spolupráce v oblasti certifikace kybernetické bezpečnosti a zajištění činností podle čl. 58 odst. 7 písm. c), d), e) a i) CSA
- Přestupky a sankce pro výrobce nebo poskytovatele produktů, služeb či procesů vydávajících EU prohlášení o shodě a držitele evropského certifikátu kybernetické bezpečnosti

Aktuální stav přípravy systému EU certifikací kybernetické bezpečnosti v ČR: Informace z Českého institutu pro akreditaci, o.p.s. a Evropské organizace pro spolupráci v oblasti akreditace

Ing. Milan Svoboda
Český institut pro akreditaci, o.p.s.
Garant rozvoje akreditace
pro certifikační orgány certifikující produkty (COV)
a inspekční orgány (IO)

Aktuální stav přípravy systému EU certifikací kybernetické bezpečnosti v ČR: Informace z NÚKIB a Evropské skupiny pro certifikace kybernetické bezpečnosti

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti

Kandidátské systémy: Návrhy Common Criteria based European cybersecurity certification scheme (EUCC) a Cybersecurity Certification Scheme for Cloud Services (EUCS)

Ing. Markéta Šilhavá
NÚKIB

II. odborné setkání k CSA

Informace z NÚKIB a ECCG (čl. 62 CSA)

- poskytování informací pro zainterestované strany
- způsob komunikace bude vhodně zvolen podle typu a rozsahu informací – emaily, setkání, webové stránky
- https://www.nukib.cz/cs/kyberneticka-bezpecnost/vyzkum/eu-certifikace-kyberneticke-bezpecnosti/
- The European Cybersecurity Certification Group | Shaping Europe's digital future (europa.eu)
- Agentura ENISA ENISA (europa.eu) -> Standards and Certification — ENISA (europa.eu)
  ! ENISA Cybersecurity Certification Conference — ENISA (europa.eu) 18.12.2020

II. odborné setkání k CSA

NÚKIB aktuálně připravuje postupy především pro:

- **dohled nad produkty, procesy a službami** s deklarací shody s CSA (posouzení subjektem posuzování shody nebo vlastní provedené výrobcem/poskytovatelem);
- **dohled nad subjekty posuzování shody** povinně veřejnými a spolupráci s ČIA dohledu nad akreditovanými subjekty posuzování shody
- **autorizaci subjektů posuzování shody** pro určitá schémata, dále na základě kontrol pro omezování, pozastavování nebo odebírání autorizací;
- **řešení stížností** pro úroveň vysoká nebo pro úroveň základní deklarovanou EU prohlášením o shodě na základě vlastního posouzení shody.

II. odborné setkání k CSA

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (čl. 47 CSA), tzv. URWP

- Průběžný pracovní program Unie obsahuje zejména seznam produktů, služeb a procesů IKT či jejich kategorií, pro něž by mohlo být zařazení do oblasti působnosti evropského systému kybernetické bezpečnosti prospěšné.

- Důvody pro zařazení do:
  a)dostupnost a rozvoj vnitrostátních systémů certifikace kybernetické bezpečnosti vztahujících se na konkrétní kategorii produktů, služeb nebo procesů IKT, zejména pokud jde o riziko roztříštěnosti;
  b) relevantní politika nebo právo Unie či členského státu;
  c) tržní poptávka;
  d) vývoj v oblasti kybernetických hrozeb;
  e) žádost o vypracování konkrétního návrhu systému ze strany Evropské skupiny pro certifikaci kybernetické bezpečnosti.

II. odborné setkání k CSA

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (čl. 47 CSA), tzv. URWP

- První URWP měl být do 28. června 2020. Průběžný pracovní program Unie je aktualizován alespoň každé tři roky a v případě potřeby častěji.
- Aktuálně Komise zpracovává návrh URWP sestávající z částí:
  - Strategické priority pro EU certifikaci kybernetické bezpečnosti
  - Budoucí kandidátská schémata
  - Oblasti pro další reflexi
  - Ostatní: komponenty a funkce 5G

II. odborné setkání k CSA

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (čl. 47 CSA), tzv. URWP

- Strategické priority pro EU certifikaci kybernetické bezpečnosti
  - Standardizace
  - Bezpečnost již v návrhu
  - Přístup založený na zvažování rizik
  - Koherence
  - Mezinárodní spolupráce
  - Měření účinnosti a zlepšování systému v průběhu času

II. odborné setkání k CSA

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (čl. 47 CSA), tzv. URWP

- Budoucí kandidátská schémata IoT a IACS
- Internet věcí (IoT)
  - Rozlišení: spotřebitelské a průmyslové IoT (překrývání a jiné případy použití)
  - URWP navrhuje generické kandidátské schéma pro zařízení IoT, které mohou být posouzeny pro všechny tři úrovně záruky
  - IoT pro použití v průmyslové automatizaci bude součástí schématu IACS
  - Rozsah by měl být definován s přihlédnutím k různým rizikovým prostředím, scénářům, případům použití IoT.

II. odborné setkání k CSA

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (čl. 47 CSA), tzv. URWP

- Řídicí systémy průmyslové automatizace (IACS)
  - Používá se v průmyslovém prostředí, včetně základních služeb (energie, voda, doprava)
  - Vyšší propojenost vede k většímu vystavení zranitelnostem
  - Společnosti průmyslové automatizace používají více IoT (průmyslový IoT)
  - Joint Research Centre zpracovalo technickou zprávu navrhující certifikační systém
  - Návrh certifikačního systému je v souladu s požadavky CSA (např. 3 úrovně záruky)

II. odborné setkání k CSA

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (čl. 47 CSA), tzv. URWP

- Oblasti pro další reflexi
  - Leightweight hodnotící systémy
  - Secure Development Lifecycle (SDL)
  - Umělá inteligence (AI)
  - Kryptografický mechanismus
  - Poskytovatelé služeb auditu zabezpečení

II. odborné setkání k CSA

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (čl. 47 CSA), tzv. URWP

- Ostatní: komponenty a funkce 5G
  - Toolbox 5G odkazuje na vývoj systému pro síťové komponenty 5G a procesy dodavatelů (TM09).
  - Probíhá diskuse.

II. odborné setkání k CSA

Průběžný pracovní program Unie pro evropskou certifikaci kybernetické bezpečnosti (čl. 47 CSA), tzv. URWP

- Další kroky
  - Prosinec: připomínkování draftu URWP
  - Leden: finální návrh sdílen v ECCG a SCCG
  - Q1 2021: přijetí URWP

II. odborné setkání k CSA

Kandidátské systémy:
Návrh Common Criteria based European cybersecurity certification scheme (EUCC)

Common Criteria (společná kritéria)
Common Criteria : New CC Portal (commoncriteriaportal.org), SOG-IS - Home
Společná kritéria pro hodnocení bezpečnosti informačních technologií (CC) a společná metodika pro hodnocení bezpečnosti informačních technologií (CEM) jsou technickým základem mezinárodní dohody, ujednání o uznávání společných kritérií (CCRA), která zajišťuje, že:

- Produkty mohou být hodnoceny kompetentními a nezávislými licencovanými laboratořemi, aby bylo do jisté míry nebo jistoty určeno splnění konkrétních bezpečnostních vlastností;
- Podpůrné dokumenty se používají k definování způsobu, jakým se kritéria a metody hodnocení používají při certifikaci konkrétních technologií;
- Tyto certifikáty uznávají všichni signatáři CCRA.

II. odborné setkání k CSA

Kandidátské systémy:
Návrh Common Criteria based European cybersecurity certification scheme (EUCC)
Cybersecurity Certification: EUCC Candidate Scheme — ENISA (europa.eu)

- Vychází z aktuálního SOG-IS MRA a společných kritérií s pravidly pro přechod;
- Použitelné pro produkty ICT;
- Zahrnuje úrovně záruky „významná“ a „vysoká“;
- Platnost certifikátu po dobu pěti let, lze obnovit;
- Harmonizované podmínky pro zpracování a odhalení zranitelností;
- Jasně definovaná pravidla pro monitorování a řešení nesouladu;
- Použití štítku založeného na rámci a kódu QR k zajištění snadného přístupu k přesným informacím o certifikaci.

II. odborné setkání k CSA

Kandidátské systémy:
Návrh Common Criteria based European cybersecurity certification scheme (EUCC)

- Zahájení přípravy implementace - kandidátské schéma „stabilní“
- Návrh prováděcího aktu Komise
- Zveřejnění návrhu prováděcího aktu
- Veřejná konzultace (4 týdny)
- Konec čtyřtýdenní zpětné vazby od veřejnosti a revize dokumentů
- Diskuse ve výboru a Hlasování (vyžaduje kladné stanovisko kvalifikovanou většinou)
- Přijetí (nejdříve v květnu 2021)
- Vstup v platnost

II. odborné setkání k CSA

Kandidátská schémata:
Cybersecurity Certification Scheme for Cloud Services (EUCS)
Cloud Security — ENISA (europa.eu)
Ad-hoc Working Groups calls — ENISA (europa.eu)

- Terminologie je založena na ISO/IEC 17788, ISO/IEC 27000 nebo ISO/IEC 17000
- Schéma EUCS se může vztahovat na všechny cloudové služby
- Certifikace služeb, proto zaměření na „nehmotné“ součásti - procesy a systémy řízení
- Všechny tři úrovně záruky, včetně základní
- Požadavky založené mj. na ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27017 nebo ISO 29147 a ISO 30111

II. odborné setkání k CSA

Kandidátská schémata:
Cybersecurity Certification Scheme for Cloud Services (EUCS)

- Další kroky:
  - Současné připomínkování od ECCG, SCCG, AHWG a veřejnosti:

    od cca 20.12.2020 do 07.02.2021
  - Webinář cca 11.01.2021 (není jasné, zda bude přístupný veřejnosti)

Questions & Answers

Závěr

Mgr. Luboš Fendrych
Ředitel odboru vzdělávání, výzkumu a projektů

Národní úřad
pro kybernetickou
a informační bezpečnost

DĚKUJEME ZA POZORNOST

PŘEJEME VÁM KRÁSNÉ VÁNOCE
A VŠE NEJLEPŠÍ DO NOVÉHO ROKU!