NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

Evropský rámec certifikace kybernetické bezpečnosti

Co je evropský rámec certifikace kybernetické bezpečnosti?

Smyslem certifikace kybernetické bezpečnosti, která je upravena přímo nařízením Evropského Parlamentu a Rady (EU) 2019/881 („Akt o kybernetické bezpečnosti“), je zvyšování důvěry v produkty, služby a procesy v oblasti informačních a komunikačních technologií skrze jejich bezpečnost. Certifikací se osvědčí, že produkty, služby a procesy splňují stanovené bezpečnostní požadavky, pokud jde o ochranu dostupnosti, důvěrnosti a integrity.

Certifikace kybernetické bezpečnosti produktů, služeb a procesů je v současné době využívána pouze v omezené míře. Pokud existuje, pak převážně na úrovni členských států nebo v rámci systémů definovaných potřebami průmyslového odvětví. V této souvislosti není certifikace udělená jedním vnitrostátním orgánem pro certifikaci kybernetické bezpečnosti v zásadě uznáván v jiných členských státech. Společnosti proto musí podstoupit certifikaci v několika členských státech, v nichž působí, například s cílem účastnit se vnitrostátních zadávacích řízení, a tím se zvyšují jejich náklady.

Stávající systémy certifikace vykazují významné nedostatky a rozdíly z hlediska pokrytí produktů, úrovní záruk, podstatných kritérií a skutečného využití, což je na překážku mechanismům vzájemného uznávání v rámci Unie. Evropský rámec pro certifikaci kybernetické bezpečnosti bude naopak jednotně zaveden ve všech členských státech, aby se zabránilo spekulativnímu výběru místa pro certifikaci v závislosti na rozdílné přísnosti požadavků v různých členských státech.

Klíčoví aktéři

Vnitrostátní orgán certifikace kybernetické bezpečnosti – NÚKIB

NÚKIB bude dohlížet na dodržování pravidel zahrnutých v evropských systémech certifikace kybernetické bezpečnosti a tato pravidla vymáhat, napomáhat Českému institutu pro akreditaci při monitorování činnosti subjektů posouvání shody, v příslušných případech autorizovat nebo pověřovat subjekty posuzování shody k udělování certifikací a řešit stížnosti podané fyzickými nebo právnickými osobami v souvislosti s evropskými certifikáty kybernetické bezpečnosti.

Vnitrostátní subjekt akreditace – Český institut pro akreditaci (ČIA)

ČIA je akreditačním orgánem, který bude akreditovat subjekty posuzování shody. Na základě této akreditace budou subjekty posuzování shody oprávněny udělovat certifikace kybernetické bezpečnosti, vyjma případů s potřebnou autorizací. ČIA je pověřen k provádění akreditace ve smyslu nařízení Evropského parlamentu a Rady (ES) č. 765/2008 rozhodnutím Ministerstva průmyslu a obchodu ČR.

Agentura Evropské unie pro kybernetickou bezpečnost (ENISA)

ENISA vypracovává návrhy systémů certifikace pro konkrétní produkty, služby a procesy. Dále může zřizovat ad hoc pracovní skupiny pro zpracovávání návrhů certifikačních systémů. ENISA bude také provozovat internetovou stránku poskytující informace o evropských systémech certifikace kybernetické bezpečnosti, o evropských certifikátech kybernetické bezpečnosti a EU *prohlášeních o shodě*, včetně informací o zrušení a pozbytí platnosti těchto certifikátů a prohlášení.

Subjekty posuzování shody (CABs)

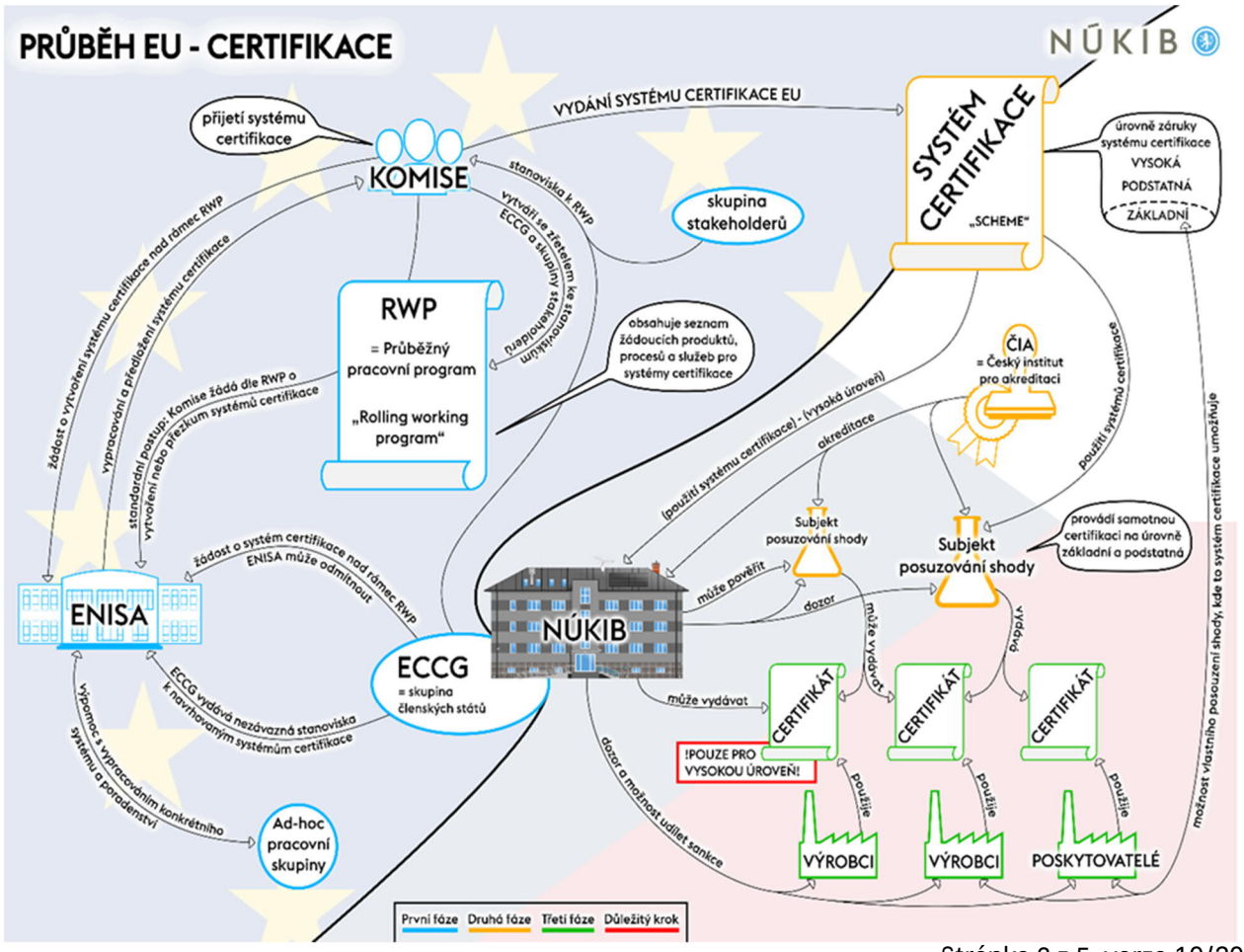
Subjekt, který uděluje certifikace v rámci daného certifikačního systému. CAB musí získat akreditaci udělovanou ČIA, případně také autorizaci udělovanou NÚKIB.

Evropská skupina pro certifikaci kybernetické bezpečnosti (ECCG)

ECCG se skládá ze zástupců vnitrostátních orgánů certifikace kybernetické bezpečnosti nebo jiných příslušných vnitrostátních orgánů. Hlavními úkoly skupiny je poskytovat poradenství a pomoc Komisi a ENISA při uplatňování evropského rámce pro certifikaci kybernetické bezpečnosti. ECCG může navrhovat nové systému EU certifikací či připomínkovat stávající návrhy certifikačních systémů.

Jak vzniká EU systém certifikace („certifikační schéma“)?

Na základě žádosti Komise či ECCG agentura ENISA vypracovává návrh systému certifikace. Pro každý návrh systému certifikace ENISA zřídí ad hoc pracovní skupinu, která agentuře ENISA poskytuje konkrétní poradenství a odborné poznatky. Návrhy systémů certifikací jsou obsaženy v Průběžném pracovním programu Unie (RWP), který bude aktualizován alespoň každé tři roky. V odůvodněných případech může Komise nebo ECCG požádat agenturu ENISA o vypracování návrhu systému nebo o přezkum stávajícího systému certifikace kybernetické bezpečnosti, jenž není zahrnut do RWP. Každý evropský systém certifikace kybernetické bezpečnosti specifikuje několik úrovní hodnocení v závislosti na náročnosti a podrobnosti použité hodnotící metodiky. Evropské systémy certifikace kybernetické bezpečnosti budou rozděleny do tří úrovní záruky: *základní, významná* a *vysoká*. Tzv. *vlastní posouzení shody* samotnými poskytovateli a výrobci je přípustné pouze na úrovni *základní*. CABs provádí certifikace na úrovně *základní* a *významná*. NÚKIB uděluje certifikace pro úroveň *vysoká*, tímto úkolem však může pověřit vybrané CABs (viz schéma).



Jak se mohu stát subjektem posuzování shody a jaké požadavky musí splnit?

CABs budou akreditovány ČIA. Akreditace bude vydávána na období nejvýše pěti let a je možné ji obnovit za stejných podmínek, pokud daný CAB stále splňuje příslušné požadavky. ČIA může omezit, pozastavit či zrušit akreditaci subjektu posuzování shody, pokud podmínky pro akreditaci nejsou nebo přestanou být splňovány.

Evropský systém certifikace kybernetické bezpečnosti může v řádně odůvodněných případech stanovit, že evropské certifikáty kybernetické bezpečnosti vyplývající z daného systému mohou vydávat pouze veřejné subjekty.

V případě, že jsou stanoveny konkrétní nebo dodatečné požadavky na subjekty posuzování shody, jsou tyto subjekty k provádění certifikací autorizovány.

Požadavky na subjekty posuzování shody[1]

✓ Právní subjektivita

✓Nezávislost na organizaci nebo produktu, který je posuzován

✓Zajistit a zdokumentovat nezávislost a neexistenci jakéhokoli střetu zájmů mezi NÚKIB a CAB v případě, že je subjekt vlastněn nebo provozován veřejným subjektem nebo institucí

✓Činnosti dceřiných společností nebo subdodavatelů nesmí ohrožovat důvěrnost, objektivitu nebo nestrannost činností posuzování shody

✓CAB musí mít zaměstnance s odbornými znalostmi a dostatečnými zkušenostmi potřebnými k plnění úkolů a popisy postupů, podle nichž je posuzování shody prováděno

✓CAB musí mít prostředky nezbytné k řádnému plnění technických a administrativních úkolů spojených s činnostmi posuzování shody a musí mít přístup k veškerému potřebnému vybavení a zařízení

✓Osoby odpovědné za plnění úkolů posuzování shody musí mít přiměřené technické a odborné vzdělání v oblasti všech činností spojených s posuzováním shody

✓Odměňování nejvyššího vedení a osob odpovědných za plnění úkolů posuzování shody nesmí záviset na počtu provedených posuzování shody ani na výsledcích těchto posuzování

✓CABs uzavřou pojištění odpovědnosti za škodu

✓Pokud jde o poplatky, CAB působí v souladu se souborem spravedlivých a přiměřených podmínek s přihlédnutím k zájmům malých a středních podniků

✓CAB zajistí, aby zkušební laboratoře používané pro účely posuzování shody plnily požadavky příslušné normy, která je harmonizována podle nařízení (ES) č. 765/2008 pro akreditaci laboratoří provádějících zkoušení

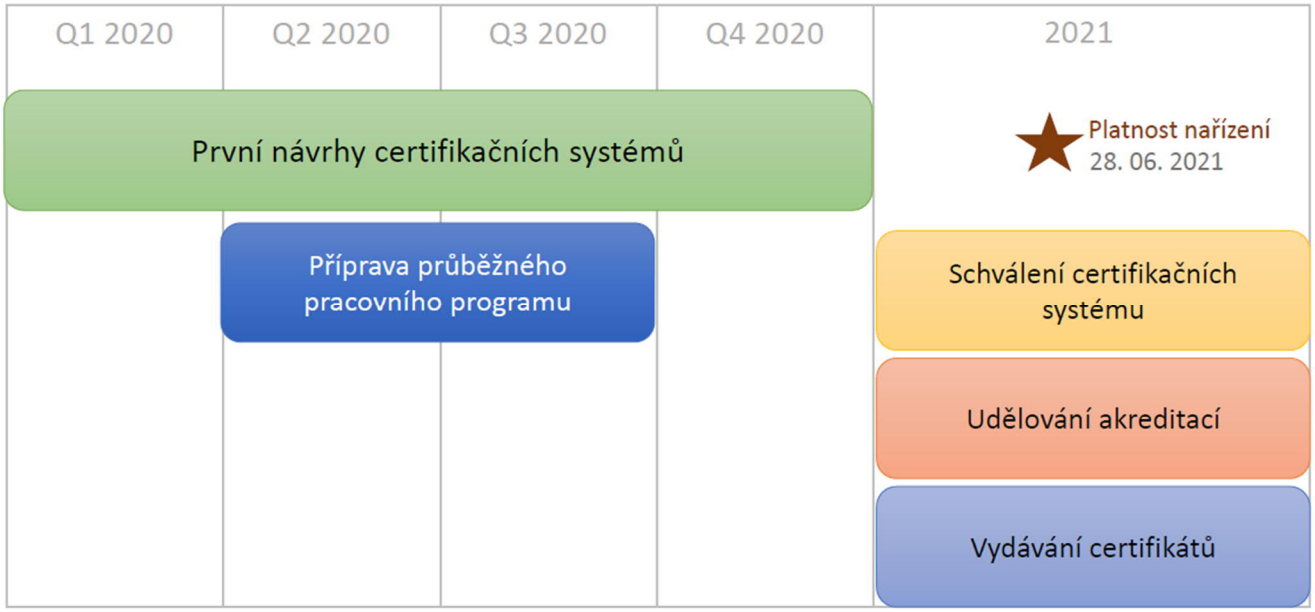
[1] Blížeji viz příloha nařízení Evropského Parlamentu a Rady (EU) 2019/881.

Jak si mohu nechat „ocertifikovat“ produkt, službu či proces?

Certifikaci produktů, služeb a procesů[2] budou provádět CABs, které získají akreditaci od ČIA, případně autorizaci od NÚKIB. Jakmile je přijat určitý evropský systém certifikace kybernetické bezpečnosti, výrobci nebo poskytovatelé produktů, služeb či procesů budou moci subjektu posuzování shody podle své volby kdekoli v Unii předložit žádost o certifikaci svých produktů nebo služeb. Žádost o certifikaci může předkládat fyzická nebo právnická osoba.

V návaznosti na úspěšné hodnocení produktu, procesu či služby bude udělena certifikace a vydán evropský certifikát kybernetické bezpečnosti. V závislosti na úrovni záruky by evropský systém certifikace kybernetické bezpečnosti měl uvádět, zda evropský certifikát kybernetické bezpečnosti vydal soukromý nebo veřejný subjekt. Evropský certifikát kybernetické bezpečnosti se vydává na dobu určenou evropským systémem certifikace kybernetické bezpečnosti a může být obnoven, budou-li nadále plněny příslušné požadavky.

Důležité milníky



Kontakty

NÚKIB
Ing. Markéta Šilhavá
Email: m.silhava@nukib.cz
Telefon: +420 702 160 590

ČIA
Ing. Milan Svoboda
Email: svobodam@cia.cz
Telefon: +420 272 096 208

[2] Certifikace kybernetické bezpečnosti informačních a komunikačních technologií podle Aktu o kybernetické bezpečnosti není certifikací, kterou je ověřována způsobilost prostředků a systémů v oblasti ochrany utajovaných informací podle zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.