

15 Příloha II: Kontinuita opatření a životní cyklus certifikace

15.1 Dozorová hodnocení

Cílem dozorových hodnocení je zajistit trvalou platnost prokázání splnění požadavků systému, které musí zahrnovat tři aspekty:

- a. poskytování certifikované služby po určitou dobu;
- b. změny v certifikované službě po určitou dobu;
- c. změny v prostředí hrozeb po určitou dobu.

Současný systém používá pro udržení certifikátu čtyři různé typy hodnocení: základní dozorové hodnocení, rozšířené dozorové hodnocení, recertifikační a mimořádné hodnocení.

15.1.1 Základní dozorové hodnocení

Účelem základního dozorového hodnocení je potvrdit trvalou shodu a efektivitu certifikované služby v průběhu určitého časového období.

Hodnotící tým musí:

- a. provést analýzu změn od posledního hodnocení služby, včetně
 - posouzení vhodnosti návrhu upravených opatření;
 - ověření existence a implementace upravených opatření;
- b. orgán posuzování shody posoudí správnost analýzy změn a rozhodne o jejím přijetí.
- c. provést funkční testy funkcí a komponent ovlivněných změnami;
- d. vybrat podmnožinu požadavků s ohledem na:
 - požadavky, u kterých byla v předchozích hodnoceních nebo od předchozího hodnocení držitelem certifikátu zjištěna pozorování nebo neshody;
 - změny v prostředí hrozeb nebo pokyny identifikované certifikačním orgánem nebo poskytnuté ECCG;
- e. vyhodnotit vhodnost návrhu opatření souvisejících s dříve vybranými požadavky;
- f. vyhodnotit provozní efektivitu podmnožiny opatření, která má být stanovena při každém hodnocení od posledního hodnocení, včetně alespoň:
 1. opatření souvisejících s řízením incidentů a zranitelností;
 2. opatření souvisejících s vývojem a řízením změn.
- g. V případě změn v částech, které byly certifikovány samostatně, nebo hodnoceny podle jiných certifikačních schémat, by měl hodnotící tým zajistit, aby část i nadále splňovala požadavky systému a aby při implementaci služby byly zohledněny veškeré aktualizace v uživatelských pokynech.
- h. **V prvním dozorovém hodnocení po vydání prvního certifikátu** hodnotící tým vyhodnotí účinnost všech opatření.

POZNÁMKA: Tento požadavek je způsoben povinností certifikovat peněženku před jejím provozem, což znamená, že provozní účinnost nelze ověřit při počáteční certifikaci nebo pouze za zkušebních podmínek.

15.1.2 Rozšířené dozorové hodnocení

Účelem rozšířeného dozorového hodnocení je doplnit základní hodnocení o posouzení zranitelnosti, které se provádí každé dva roky, jak to vyžaduje CIR (EU) 2024/2981.

Vzhledem k tomu, že každé dozorové hodnocení již zohledňuje změny v prostředí hrozeb a zahrnuje i řízení zranitelností, provede se posouzení zranitelností dle kapitoly XI.1.3 přílohy XI s využitím výsledků dozorových činností dle kapitoly XI.3 přílohy XI; toto posouzení zahrnuje alespoň změny v předmětu posuzování shody a změny v prostředí hrozeb od posledního posouzení zranitelností (příloha IX bod 1 písm. b) CIR (EU) 2024/2981). Dále doporučujeme vypracovat specifickou zprávu shrnující veškerá posouzení zranitelností provedená za poslední dva roky.

15.1.3 Recertifikační hodnocení

Účelem recertifikačního hodnocení je potvrdit trvalou shodu a efektivitu služby jako celku a její trvalou relevanci a použitelnost pro rozsah certifikace. Recertifikační hodnocení musí být naplánováno a provedeno za účelem vyhodnocení trvalého plnění všech hodnotících kritérií. Toto hodnocení musí být naplánováno a provedeno včas, aby bylo možné včas obnovit certifikát před datem vypršení platnosti.

Recertifikační činnost musí zahrnovat přezkum předchozích zpráv o dozorových hodnoceních a zvážit výkonnost poskytované služby během posledního certifikačního cyklu.

POZNÁMKA: Recertifikace musí zahrnovat účinnost všech opatření. Pokud bylo v rámci dozorových hodnocení provedeno posouzení efektivity pouze na základě minimálního souboru požadavků, pak mohou být práce, které je třeba pro recertifikaci vykonat, velmi významné. Proto se doporučuje pečlivě vybírat činnosti, které mají být provedeny během těchto dozorových hodnocení, aby se předešlo pouhému odložení potenciálních obtíží.

15.1.4 Mimořádné hodnocení

Pokud je nutné mimořádné hodnocení, pak certifikační orgán určí veškeré hodnotící činnosti nezbytné k rozhodnutí o potenciálním ukončení, omezení, pozastavení nebo odebrání certifikace.

Mimořádné hodnocení se provede, pokud byl certifikát pozastaven, předtím, než je pozastavení zrušeno a certifikát je plně obnoven.

POZNÁMKA Cílem mimořádného hodnocení je provést hodnocení zaměřené na opatření, která klient přijal ke splnění požadavků, u kterých byly zjištěny neshody, nebo na změny provedené klientem v poskytované službě nebo v jejím kontrolním rámci.

Hodnotící tým musí:

- a. provést analýzu změn a neshod zjištěných od posledního hodnocení služby klienta, včetně:
 - posouzení vhodnosti návrhu dotčených opatření;
 - ověření existence a implementace dotčených opatření.
- b. vyhodnotit provozní efektivitu dotčených opatření za období od předchozího hodnocení.

15.2 Harmonogram dozoru

Dozorové činnosti se provádějí alespoň jednou ročně podle následujících pravidel:

- a. Každý rok se provádí alespoň základní dozorové hodnocení;
- b. Každé dva roky se provádí rozšířené dozorové hodnocení nebo hodnocení pro recertifikaci;
- c. Hodnocení pro recertifikaci se provádí dva měsíce před stanoveným vypršením platnosti certifikátu, a to včas pro včasné obnovení před datem vypršení platnosti certifikátu;

- d. Zvláštní hodnocení se provádí, pokud tak rozhodne certifikační orgán, po podstatných změnách nebo podstatné neshodě.

POZNÁMKA: Podle těchto pravidel, pokud je referenční doba platnosti certifikátů čtyři roky, je referenční harmonogram následující:

- Rok 1: Dozorové hodnocení
- Rok 2: Rozšířené dozorové hodnocení
- Rok 3: Dozorové hodnocení
- Rok 4: Recertifikační hodnocení

Kromě toho se po každém hodnocení provede přezkum a rozhodnutí o certifikaci s následujícími možnými výsledky:

- a. pokračování certifikátu beze změn;
- b. pozastavení certifikátu s pokyny pro uživatele a požadavky na klienta, aby ve stanoveném časovém rámci odstranil zjištěné neshody;
- c. zrušení certifikátu v případě neshod, které nelze vyřešit;
- d. doplnění certifikátu o změnu s novým popisem a pokyny, ale se stejným datem ukončení.

V případě hodnocení recertifikace je možný i následující výsledek:

- e. doplnění certifikátu o změnu s novým popisem a pokyny a s aktualizovaným datem ukončení, které nesmí být déle než čtyři roky po rozhodnutí o certifikaci.

POZNÁMKA: Maximální aktualizace data ukončení by měla odpovídat maximální době platnosti certifikátu. Pokud jsou certifikáty původně vydány na pět let, měla by recertifikace vést také k pětiletému prodloužení.

15.3 Parametry procesu údržby

Poskytovatelé služeb IKT certifikovaní v rámci tohoto schématu jsou povinni zavést procesy související s každodenní údržbou svých služeb (viz příloha I). Jedním z klíčových cílů těchto procesů je snížit počet interakcí mezi poskytovatelem služeb IKT a certifikačním orgánem, a to stanovením rozlišení mezi významnými událostmi a ostatními událostmi a stanovením různých způsobů zpracování těchto událostí:

- Významná událost (neshoda, změna nebo zranitelnost, podrobnosti viz následující pododdíly) musí být oznámena certifikačnímu orgánu bez čekání na termín následujícího hodnocení či recertifikace a certifikační orgán musí provést následnou kontrolu a poskytnout zpětnou vazbu k řešení události poskytovatelem služeb IKT.
- Ostatní události musí být řešeny přímo prostřednictvím procesu definovaného poskytovatelem služeb IKT, přičemž certifikační orgán každoročně provádí posouzení účinnosti tohoto procesu.

Posouzení účinnosti těchto procesů musí zahrnovat posouzení procesu použitého k určení významnosti událostí. V případě, že certifikační orgán zjistí v tomto přiřazení neshodu, přijme vhodná opatření k zajištění toho, aby byla neshoda vyřešena, včetně v případě potřeby povinnosti oznámit certifikačnímu orgánu všechny události během daného období, aby certifikační orgán mohl určit, zda byla událost zařazena do příslušné kategorie.

Zbývající část tohoto odstavce poskytuje definice významnosti neshod a událostí v následujících procesech: řízení změn a řízení zranitelností.

Celkově je definice významnosti „schopnost ovlivnit rozhodnutí zamýšlených uživatelů“. Významnost se tedy určuje s ohledem na důsledky negativní události pro zamýšlené uživatele.

15.3.1 Významnost neshod

Neshoda je považována za významnou, pokud činí opatření nebo kontrolní mechanismus použitý ke splnění požadavku neúčinným. Neshoda může být považována za nevýznamnou, pokud pouze vede ke snížení účinnosti opatření nebo kontrolního mechanismu.

Kromě toho neshoda, která sama o sobě není považována za významnou, může vést k významné neshodě, pokud se opakuje příliš často, a ve skutečnosti činí opatření nebo kontrolní mechanismus neúčinným.

PŘÍKLAD

V kontrolním mechanismu, který implementuje zálohovací systém k zajištění dostupnosti dat:

- ztráta zálohovaných dat nebo nemožnost jejich obnovení je velmi pravděpodobné, že bude považována za významnou neshodu;
- jednorázové selhání při zálohování systému nemusí být považováno za významné;
- stejné selhání opakované po dobu několika dnů je velmi pravděpodobné, že bude považováno za významné.

Při posuzování významnosti se bere v úvahu více než jen parametr, jako je množství dotčených dat, jejich citlivost a efektivita poskytovatele při identifikaci problému a jeho zmírnění.

15.3.2 Významnost změn

Vzhledem k tomu, že významnost změn musí být odhadnuta držitelem certifikátu, je nutné v politice řízení změn definovat podrobný postup a vyhodnotit jej CAB.

Měly by být dodržovány následující zásady:

- Změna by měla být považována za významnou, pokud může vést k významné neshodě.
- Funkční změny, které mají dopad na bezpečnost služby IKT nebo na implementaci jejich rozhraní, by měly být považovány za významné.
- Změny architektury, která je základem služeb IKT, by měly být považovány za významné.
- Změny kritických komponent, jako je WSCD nebo WSCA, by měly být považovány za významné.

15.3.3 Významnost dopadu zranitelností

Stejně jako u změn musí držitel certifikátu odhadnout závažnost dopadu zranitelností, v zásadách správy zranitelností musí být definován podrobný postup a vyhodnocen CAB.

POZNÁMKA: Toto se týká dopadu zranitelností, nikoli samotných zranitelností. Zranitelnost může být kritická, ale její dopad je malý, pokud je k dispozici oprava, která ji zmírňuje, a tato oprava se snadno aplikuje a byla aplikována včas, přičemž je zajištěno, že zranitelnost nebyla zneužita (což se u složitých IT systémů pravidelně stává).

Vytvořeno v rámci projektu ROPIM – Reforma pro optimalizaci, implementaci a metodické řízení digitalizovaných služeb vč. jejich kapacitního plánování a komunikaci informací klientům veřejné správy, financovaného Evropskou unií NextGeneration. Reg. č.: CZ.31.5.0/0.0/0.0/23_106/0008503.

