Příloha č. 8 Zadávací dokumentace – Podmínky certifikace

Příloha F – Podmínky certifikace

1. Úvod

Každý nově nasazovaný produkt do vnitřní sítě NBÚ, certifikované pro nakládání s utajovanými informacemi, musí splňovat minimálně následující požadavky:

- Musí být dodána dokumentace v rozsahu kapitoly č. 2,
- Musí obsahovat bezpečnostní funkcionalitu v rozsahu kapitoly č. 3.

2. Dokumentace produktu

Dokumentace musí obsahovat minimálně informace popsané v následujících podkapitolách.

2.1. Popis funkcionality produktu

Nejprve je produkt popsán z hlediska jeho funkcionality.

Pokud je součástí produktu SW, pak ho tento popis pomůže zařadit do kategorie podle jeho:

- provozování:
  - SW provozovaný lokálně na jedné nebo několika pracovních stanicích bez síťového komunikačního prostředí,
  - SW provozovaný v síťovém prostředí s aktivním síťovým komunikačním prostředím,
- použití:
  - SW používaný výhradně privilegovanými uživateli pro potřeby správy IS,
  - SW používaný primárně koncovými uživateli.

Popis funkcionality produktu musí poskytnout odpovědi na následující otázky:

- K čemu je produkt určen?
- Pro koho je produkt určen?
- Jaké funkce produkt plní?

2.2. Vývoj produktu

V této části dokumentace jsou zodpovězeny otázky:

- Byl produkt primárně vyvíjen k používání v certifikovaných IS?
- Poskytuje produkt nějakou bezpečnostní funkcionalitu? Pokud ano tak jakou?

Součástí dokumentace o vývoji musí být popis:

- bezpečnostní architektury produktu,
- funkční specifikace produktu a to:
  - jednak z pohledu plnění základní funkcionality,
  - také z pohledu plnění bezpečnostních funkcí,
- návrhu produktu formou dělení na podsystémy nebo moduly plnící určité funkce.

Míra detailnosti jednotlivých popisů je závislá na typu a složitosti produktu.

2.2.1. Běžný komerční produkt

V případě běžného komerčního produktu postačuje míra detailnosti požadovaných popisů na úrovni informací získaných z dokumentace nebo jiných zdrojů výrobce.

2.2.2. Speciální komerční produkt

Speciálním komerčním produktem rozumíme produkt, který vychází z běžného komerčního produktu, ale je na základě specifikací upraven pro použití ve vnitřním certifikovaném IS NBÚ.

V případě speciálního komerčního produktu postačuje míra detailnosti požadovaných popisů na úrovni informací získaných z dokumentace nebo jiných zdrojů výrobce doplněná o informace popisující provedené úpravy a vlastní testování.

2.2.3. Speciální produkt

Do této kategorie řadíme produkty, které jsou přímo navrženy a vyvíjeny pro použití ve vnitřním certifikovaném IS NBÚ. Do této kategorie se řadí i speciální komerční produkty, kde subjekt výrobce běžného komerčního produktu a subjekt upravující tento produkt je stejná organizace nebo firma.

V případě speciálního produktu je vyžadována vysoká míra detailnosti popisů, zejména pak popisu bezpečnostní architektury.

2.3. Směrnice

Tato část dokumentace je určena pro uživatele produktu a obsahuje:

- uživatelskou příručku popisující pro všechny role definované pro produkt:
  - použití produktu z pohledu funkčního,
  - použití produktu z pohledu bezpečnostního,
  - seznam použitelných funkcí včetně případných chybových stavů,
- přípravné procedury určené zejména pro správce, které popisují instalaci a přípravu provozního prostředí potřebného pro správný a bezpečný provoz produktu.

2.4. Podpora životního cyklu

Tato část dokumentace popisuje postupy implementace a mechanizmy získávání oprav a aktualizací produktu.

2.5. Testy

Tato část dokumentace popisuje prováděné testování produktu takovým způsobem, aby bylo možné určit:

- pokrytí testů,
- funkčnost testů,
- nezávislost testů.

2.6. Analýza zranitelností

Tato část dokumentace obsahuje základní analýzu hrozeb a zranitelností produktu, která slouží především k vytvoření návrhu funkční specifikace bezpečnostní funkcionality produktu.

Analýza musí obsahovat seznam a stručný popis:

- identifikovaných hrozeb,
- identifikovaných zranitelností,
- navržených protiopatření:

- bezpečnostní funkcionalita produktu,
- omezení provozního prostředí.

3. Bezpečnostní funkcionalita

Bezpečnostní funkcionalit a obsažená v produktu musí být dostatečně podrobně popsána v rámci dokumentace (viz kapitola č. 2).

Rozsah jednotlivých bezpečnostních funkcionalit je upřesněn OIT v průběhu návrhu nasazení nebo vývoje produktu. Následující seznam požadovaných bezpečnostních funkcionalit může OIT upravit v závislosti na typu produktu a jeho funkci.

3.1. Audit

Zejména SW produkty by měly zajišťovat vytváření auditních záznamů. V dokumentaci je pak nutné uvést zejména:

- seznam typů generování auditních záznamů,
- popis formátu auditních záznamů,
- možnosti zpětného zkoumání auditních záznamů,
- způsob ochrany auditních záznamů před možným smazáním nebo modifikací.

3.2. Uživatelská data

Pokud produkt pracuje s uživatelskými daty, pak musí zajišťovat jejich ochranu. V dokumentaci je pak uvedeno plnění požadavků na ochranu uživatelských dat, zejména pak popis řízení:

- přístupu subjektů a objektů k operacím,
- přístupu subjektů k objektům,
- toku informací uvnitř produktu,
- toku informací do a z produktu,
- ochrany případných zbytkových informací.

3.3. Identifikace a autentizace

Produkt by měl zajišťovat identifikaci a autentizaci přístupů. V dokumentaci je pak uvedeno plnění požadavků na identifikaci a autentizaci uživatelů, zejména pak popis zajištění:

- obsluhy selhání autentizace,
- bezpečnostních atributů uživatelů,
- prosazování identifikace a autentizace uživatelů,
- spojení uživatel - subjekt.

3.4. Bezpečnostní správa

Produkt by měl zajišťovat bezpečnostní správu. V dokumentace je pak uvedeno plnění požadavků na bezpečnostní správu, zejména popis zajištění správy:

- chování bezpečnostních funkcí,
- bezpečnostních atributů,
- dat bezpečnostních funkcí,
- bezpečnostních rolí,
- konfiguračních mechanizmů včetně defaultní konfigurace.

3.5. Ochrana bezpečnostních funkcí

Produkt by měl zajišťovat ochranu bezpečnostních funkcí. V dokumentace je pak uvedeno plnění požadavků na ochranu bezpečnostní funkcionality, zejména popis zajištění:

- zachování bezpečnosti v případě selhání bezpečnostních funkcí,
- vlastního testování,
- kompatibility s platformou, na které je produkt provozován,
- oddělení bezpečnostních a provozních funkcí.

3.6. Využití zdrojů

Produkt by měl zajišťovat řízení využití zdrojů. V dokumentace je pak uvedeno plnění požadavků na využití zdrojů, zejména popis zajištění odolnosti vůči chybám.

3.7. Přístup k produktu

Produkt by měl zajišťovat řízení přístupu. V dokumentace je pak uvedeno plnění požadavků na přístup k produktu, zejména pak popis zajištění:

- zřízení sezení,
- evidence historie přístupů.

3.8. Důvěryhodná cesta

Produkt by měl zajišťovat použití důvěryhodných cest. V dokumentace je pak uvedeno plnění požadavků na důvěryhodné cesty, zejména zajištění ochrany dat v průběhu jejich přenosu.

4. Závěr

Dokumentace zpracovaná na základě předchozích požadavků slouží OIT k hodnocení vhodnosti použití daného produktu ve vnitřním certifikovaném IS NBÚ.

Míra podrobnosti stanovených informací a popisů je vždy individuální a závislá na mnoha faktorech, které se podrobně probírají na přípravných jednáních.