Více úrovňové informační systémy a jejich certifikace podle zákona č.412/2005 Sb., ve znění pozdějších předpisů

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.

Bezpečnostní provozní módy

- vyhrazený
- s nejvyšší úrovní
- s nejvyšší úrovní s formálním řízením přístupu k informacím
- víceúrovňový

definovány v předpisech NATO, EU, národních (vyhláška č. 523/2005 Sb.)

prvé tři jsou jednoúrovňové, nicméně opětovně zavedený bezpečnostní provozní mód s nejvyšší úrovní s formálním řízením přístupu k informacím („compartmented“) přináší zvýšený dohled nad přístupy uživatelů k informacím

Bezpečnostní provozní mód s nejvyšší úrovní s formálním řízením přístupu k informacím (Compartmented)

Prostředí umožňující zpracování utajovaných informací různého stupně utajení, přičemž všichni uživatelé musí splňovat podmínky pro přístup k utajované informaci nejvyššího stupně utajení, se kterým se může v IS nakládat, avšak nejsou oprávněni pracovat se všemi informacemi obsaženými v IS. Je umožněno pouze formální řízení přístupu zajišťované formální centrální správou kontroly přístupu.

Požadavky: splnit všechny minimální požadavky počítačové bezpečnosti, opatření administrativní, personální a fyzické bezpečnosti a zabezpečení dat během přenosu na úrovni požadované pro nejvyšší stupeň utajení informací v IS. Zajistit výlučně formální centrální správu přístupových práv.

Poznámka

IS v bezpečnostním provozním módu vyhrazeném, s nejvyšší úrovní a s nejvyšší úrovní s formálním řízením přístupu k informacím nemají implementovány takové bezpečnostní mechanismy, které by zaručovaly rozlišování stupně utajení objektů. Proto v těchto IS jsou veškeré informace v IS chráněny na úrovni odpovídající nejvyššímu stupni utajení, pro jaký je daný IS určen. Pokud z IS vystupují informace, musí být buďto uživatelem, bezpečnostním správcem apod. určen jejich skutečný stupeň utajení nebo se s nimi musí i nadále nakládat jako s utajovanou informací nejvyššího stupně utajení, který může být IS obsažen.

Bezpečnostní provozní mód víceúrovňový

Bezpečnostní provozní mód víceúrovňový

je takové prostředí, které umožňuje v jednom informačním systému současné zpracování utajovaných informací klasifikovaných různými stupni utajení, ve kterém nemusí všichni uživatelé splňovat podmínky přístupu k utajovaným informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy, přičemž všichni uživatelé nemusí být oprávněni pracovat se všemi utajovanými informacemi.

Bezpečnostní funkce

- jednoznačná identifikace a autentizaci uživatele informačního systému, ochrana důvěrnosti a integrity autentizační informace,
- volitelné řízení přístupu k objektům informačního systému na základě přístupových práv uživatele a jeho identity nebo členství ve skupině uživatelů,
- nepřetržité zaznamenávání bezpečnostně relevantních událostí do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením

Bezpečnostní funkce

- možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele,
- ošetření paměťových objektů před jejich dalším použitím, zejména před přidělením jinému subjektu informačního systému, které znemožní zjistit jejich předchozí obsah,
- ochrana důvěrnosti dat během přenosu mezi zdrojem a cílem, a dále
- **povinné řízení přístupu**

Povinné řízení přístupu

- Funkce povinného řízení přístupu subjektů IS k objektům IS musí zabezpečit
  - trvalé spojení každého subjektu a objektu IS s bezpečnostním atributem, který
    - pro subjekt IS vyjadřuje úroveň jeho oprávnění
    - pro objekt IS jeho stupeň utajení,
  - ochranu integrity bezpečnostního atributu,

Povinné řízení přístupu

- výlučné oprávnění bezpečnostního správce IS k provádění změn bezpečnostních atributů subjektů i objektů informačního systému

- přidělení předem definovaných hodnot atributů pro nově vytvořené objekty IS a zachování atributu při kopírování objektu IS

Povinné řízení přístupu

- bezpečnostní funkce povinného řízení přístupu musí zajistit tyto zásady
  - subjekt informačního systému může číst informace v objektu informačního systému pouze tehdy, je-li úroveň jeho oprávnění stejná nebo vyšší než stupeň utajení objektu informačního systému,
  - subjekt informačního systému může zapisovat informaci do objektu informačního systému pouze tehdy, je-li úroveň jeho oprávnění stejná nebo nižší než stupeň utajení objektu informačního systému,

Povinné řízení přístupu

- přístup subjektu IS k informaci obsažené v objektu IS je možný, jestliže jej povolují jak pravidla povinného řízení přístupu, tak pravidla volitelného řízení přístupu,
- IS v bezpečnostním provozním módu víceúrovňovém, musí být schopen přesně označit stupněm utajení utajované informace vystupující z IS a umožnit přiřadit stupeň utajení utajované informaci vstupující do IS,
- bezpečnostní funkce musí být realizovány identifikovatelnými programově technickými mechanismy, dokumentovány tak, aby bylo možné jejich nezávislé prověření a zhodnocení.

Bellův a LaPadulův formální model bezpečnostní politiky

- Bell D.E., La Padula L.J., 1976, zpráva MITRE Corporation, vyvinut pro DoD US
- vliv na TCSEC
- vliv na ITSEC
- vliv na profily v CC

Bellův a LaPadulův formální model bezpečnostní politiky

- bezpečnost formálně popsána a dokázána
- stavový model - stav je bezpečný pokud je v souladu s bezpečnostní politikou pro přístup subjektu k objektu; porovnává se úroveň prověření subjektu a stupeň utajení objektu + „need-to-know“ subjektu k objektu; přechod do dalšího stavu zajišťován tak, že nový stav je opět bezpečný
- základní zásady bezpečnostní politiky pro MAC:

  - Simple Security Condition: subjekt nesmí číst z objektu vyšší bezpečnostní úrovně (no read-up)

  - * Property: subjekt nesmí zapisovat do objektu nižší bezpečnostní úrovně (no write-down)

  - Discretionary security property (dle přístupových práv, jako v jednoúrovňovém IS)

Bezpečná realizace

- víceúrovňový operační systém ohodnocený podle některých z kritérií bezpečnosti (CC)
- na aplikační úrovni – obtížné navrhnout, implementovat, poté prokázat bezpečnost
- využití kryptografické ochrany - obtížnost návrhu, implementace, prokázání bezpečnosti

Bezpečná realizace

- aktuálně stále neznáme v oblasti utajovaných informací realizaci víceúrovňového IS v NATO ani EU
- některé operační systémy hodnocené podle CC mají modul zajišťující povinné řízení přístupu (IBM z/OS v módu Labeled Security mode, některé UNIX/LINUX se zabudovaným volitelným i povinným řízením přístupu, které ale musí být aktivováno, např. Free BSD, Red Hat,AIX, Solaris)
- režie na správu víceúrovňového systému je údajně vysoká, funkce MAC není využívána

Bezpečná realizace

Poznámky

- stěžejním problémem je přesná implementace Bell-LaPadula modelu, zejména udržení integrity atributů subjektů a objektů a neobejitelnost pravidel pro přístup
- některé certifikované IS v bezpečnostním provozním módu s nejvyšší úrovní využívají labelů s označením stupně utajení a kategorie informace připojených k některým objektům (např. e-mailová zpráva); to z nich ještě nedělá víceúrovňový systém
- přímo na OS Windows postavit víceúrovňový systém nelze

Bezpečné propojení informačních systémů

Novela vyhlášky č. 523/2005, kterou je vyhláška č. 453/2011 Sb.,

Propojením informačních systémů (IS) se zde rozumí:

propojení dvou nebo více informačních systémů za účelem jednosměrného nebo vícesměrného sdílení údajů a dalších informačních zdrojů

POZN. Může se jednat o IS pro nakládání s utajovanými informacemi i IS pro nakládání s neutajovanými informacemi

Bezpečné propojení informačních systémů

Novela vyhlášky č. 523/2005, kterou je vyhláška č. 453/2011 Sb.,

Propojení informačního systému pro nakládání s utajovanými informacemi s informačním systémem pro nakládání s neutajovanými informacemi lze realizovat pouze v případě nezbytné provozní potřeby.

Bezpečné propojení informačních systémů

Novela vyhlášky č. 523/2005, kterou je vyhláška č. 453/2011 Sb.,

Vzájemné propojení certifikovaných IS lze realizovat, pokud

- **je propojení na základě analýzy rizik schváleno v rámci jejich certifikace,**
- **je mezi nimi realizováno bezpečnostní rozhraní a**
- **jsou buďto certifikovány pro nakládání s utajovanými informacemi stejného stupně utajení, nebo je propojení realizováno tak, aby bylo zabráněno přenosu utajované informace vyššího stupně utajení, nežli je stupeň utajení, pro který je IS certifikován.**

Bezpečné propojení informačních systémů

Novela vyhlášky č. 523/2005, kterou je vyhláška č. 453/2011 Sb

Pokud by nastala nezbytná provozní potřeba pro propojení certifikovaného IS s veřejnou komunikační sítí, pak pouze v případě, že je instalováno vhodné bezpečnostní rozhraní schválené na základě analýzy rizik v rámci certifikace IS tak, aby bylo zamezeno průniku do certifikovaného IS a byl umožněn pouze kontrolovaný přenos dat, nenarušující důvěrnost, integritu a dostupnost utajované informace a dostupnost služeb certifikovaného IS. Zakázáno pro Přísně tajné.

Bezpečné propojení informačních systémů

Novela vyhlášky č. 523/2005, kterou je vyhláška č. 453/2011 Sb

Pokud je veřejná komunikační síť využívána výhradně k přenosu dat mezi certifikovanými IS nebo mezi lokalitami certifikovaného IS a přenášené informace jsou chráněny certifikovaným kryptografickým prostředkem, nepovažuje se takové spojení za propojení.

Opět musí být ale realizováno vhodné bezpečnostní rozhraní, zamezující průniku do IS (analýza rizik, schválení v rámci certifikace IS).

Dotazy ?

Národní bezpečnostní úřad
RNDr. Anna Mašková, Csc.
odbor informačních technologií
a.maskova@nbu.cz
tel. 527 583 348