Vážení zákazníci,

dovolujeme si Vás upozornit, že na tuto ukázku knihy se vztahují autorská práva, tzv. copyright.

To znamená, že ukázka má sloužit výhradně pro osobní potřebu potenciálního kupujícího (aby čtenář viděl, jakým způsobem je titul zpracován a mohl se také podle tohoto, jako jednoho z parametrů, rozhodnout, zda titul koupí či ne).

Z toho vyplývá, že není dovoleno tuto ukázku jakýmkoliv způsobem dále šířit, veřejně či neveřejně např. umisťováním na datová média, na jiné internetové stránky (ani prostřednictvím odkazů) apod.

redakce nakladatelství BEN – technická literatura
redakce@ben.cz

Část II : Přehledy a předpisy

5.0 Hlavní cíle zabezpečených systémů

Kritéria jsou dělena v rámci každé třídy do skupin požadavků. Tyto skupiny byly vyvinuty proto, aby byly plněny a nebyly přehlíženy tři základní určující cíle zabezpečených systémů. Tyto určující cíle jsou:

- ❒ bezpečnostní politika,
- ❒ odpovědnost,
- ❒ záruka.

Část II předkládá diskusi k těmto obecným určujícím cílům a zahrnuje je do pojmů navrhování zabezpečených systémů.

5.1 Požadavek shody

Hlavním cílem DoD Computer Security Center je podpořit počítačový průmysl ve vývoji zabezpečených počítačových systémů a výrobků, a zajištění jejich široké dostupnosti v obchodní síti. Splněním tohoto cíle dojde k poznání potřeby, konkretizace této potřeby současnými veřejnými a soukromými sektory, a poptávce po takových výrobcích.

Jak bylo popsáno v úvodu tohoto dokumentu, úsilí definovat problémy a vyvíjet řešení spojená se zpracováním informace státního tajemství stejně jako ostatních utajovaných údajů, například finančních, lékařských a informací použitých k zabezpečení obrany státu, trvá již mnoho let. Kritéria, tak jak byla popsána v části I, representují výsledky tohoto úsilí a popisují základní požadavky pro výstavbu zabezpečených počítačových systémů. Přesto však jsou tyto systémy viděny pouze jako zabezpečení potřeby národní bezpečnosti. Dokud bude tento názor přetrvávat, pak shoda, potřebná k motivaci výroby zabezpečených systémů, nebude.

Účelem této části je popsat některé detaily a základní určující cíle, které položí základy pro požadavky vyúsťující v kritéria. Cílem je vysvětlit,

že na základě zabezpečení vnější národní bezpečnosti lze odhadovat jejich univerzálnost a následně i univerzální aplikovatelnost kritérií požadovaných pro zpracování všech druhů utajovaných aplikací, ať již pro národní bezpečnost nebo soukromý sektor.

5.2 **Definování a použitelnost**

Termín "hlavní cíl" se shoduje s vyhlášeným záměrem zohledňujícím některé aspekty řízení a organizace zdrojů nebo procesů nebo obou. Hlavní cíle předkládají osnovu vývoje strategie úplného souboru požadavků zabezpečení jakéhokoli systému v pojmech počítačových systémů. Vývojem v souvislosti s náchylností k chybám při generování, což je například potřeba řízení a zpracování chráněných dat za účelem zabránění kompromisu nebo nutnost zajištění odpovědnosti a odhalení klamu, byly "hlavní cíle" identifikovány jako použitelná metoda vyjádření cílů zabezpečení.

Jako příklady hlavních cílů jsou uvedeny tři základní vzory požadavků pro zavádění referenčního monitoru (viz též kapitola 6). Jsou to:

- ❒ verifikační mechanizmus musí být prověřitelný,
- ❒ verifikační mechanizmus musí být volán vždy,
- ❒ verifikační mechanizmus musí být dostatečně málo přístupný subjektivní analýze a testům, aby nebylo možno zjistit jeho schopnosti [1].

5.3 **Kriteria hlavních cílů**

Tři základní kritéria hlavních cílů jsou: bezpečnostní politika, odpovědnost a záruka. Zbytek této sekce se vztahuje k těmto základním požadavkům.

5.3.1 **Bezpečnostní politika**

Ve většině případů je počítačové zabezpečení koncipováno jako řízení cesty, kde může být počítač využit, t.j., řízení procesů, kterými mohou být zpracovávané informace zpřístupněny. Přesto však se zabezpečení počítače

může na základě prověřování odvolávat na mnoho oblastí. Přesto však (viz FIPS PUB 39, Poznámky k zabezpečení počítačových systémů) neexistuje unikátní definice pro zabezpečení počítačů [16]. Namísto toho existuje jedenáct rozdílných definic pro zabezpečení, které zahrnují: zabezpečení systémů AZD, zabezpečení administrace, zabezpečení dat atd. Hlavní trend, společný všem těmto definicím, je slovo "ochrana". Další deklarované požadavky ochrany lze nalézt v direktivě DoD číslo 5200.28, která popisuje přijatelnou úroveň ochrany pro klasifikované údaje, kde se říká: "zajistit v systémech proces, který bude spolehlivě chránit paměť nebo použití klasifikovaných údajů a vytváření klasifikovaných informací a bude schopen zabránit: a) úmyslnému nebo neúmyslnému přístupu neautorizované osoby ke klasifikovaným materiálům a b) neautorizované manipulaci s počítačem a jeho připojenými vnějšími zařízeními".[8]

V souhrnu - požadavky na ochranu musí být definovány v pojmech odpovídajících ohrožení, riziku a cílům organizace. Toto je často konstatováno v pojmech bezpečnostní politiky. Jak vyplývá z literatury, jsou to externí zákony, pravidla, nařízení atd., která stanoví, který přístup k informaci je povolený, nezávisle na použití počítače. Konkrétně lze říci, že pouze takový systém je zabezpečený, který zohledňuje specifickou politiku. [30] Tedy - hlavní cíl pro bezpečnostní politiku je:

HLAVNÍ CÍL BEZPEČNOSTNÍ POLITIKY

ZÁMYSL ŘÍZENÍ PŘÍSTUPU K VYUŽITÍ A ROZŠIŘOVÁNÍ INFORMACÍ, ZNÁMÝ JAKO BEZPEČNOSTNÍ POLITIKA, MUSÍ BÝT PŘESNĚ DEFINOVANÝ A ZAVEDENÝ PRO KAŽDÝ SYSTÉM, KTERÝ JE POUŽIT PRO PRÁCI S UTAJOVANÝMI INFORMACEMI. BEZPEČNOSTNÍ POLITIKA MUSÍ PŘESNĚ ODRÁŽET ZÁKONY, PRAVIDLA A OBECNOU POLITIKU, Z NICHŽ JE ODVOZENA.

5.3.1.1 **Povinná bezpečnostní politika**

Tam, kde se bezpečnostní politika vyvíjí, tedy tam, kde je aplikováno řízení klasifikovaných nebo jinak specificky označovaných utajovaných informací, musí tato politika obsahovat podrobná pravidla, jak zvládnout tyto informace v průběhu celého jejich životního cyklu. Tato pravidla jsou

funkce pro různé stupně utajení, které lze u informací předpokládat a pro různé formy přístupu podporované systémem.

Povinné zabezpečení se vztahuje k vynucení souboru pravidel pro řízení přístupu, která nutí subjekt přistupovat k informacím na základě porovnání individuálního odbavení/ autentizace k požadovaným informacím, klasifikace/utajení informací a způsobu zprostředkování přístupu. Povinností politiky jsou buď další požadavky nebo odsouhlasení systémů, které vynucují částečné požadavky na označení, přičemž označení musí mít formu, která je matematicky známá jako "mříž". [5]

Je zřejmé, že systém musí zajistit, aby označení spojené s utajovanými údaji nemohlo být libovolně měněno, protože to by mohlo umožnit přístup k utajovaným informacím subjektům s nedostatečnou autorizací. Musí rovněž zajistit takovou systémovou kontrolu, aby požadavek pro přenos informace nemohl být splněn současně se snížením označení utajení, pokud toto "snížení" nebylo schváleno. Hlavní cíl je:

HLAVNÍ CÍL POVINNÉHO ZABEZPEČENÍ

BEZPEČNOSTNÍ POLITIKA DEFINOVANÁ PRO SYSTÉMY, KTERÉ JSOU VYUŽÍVÁNY KE ZPRACOVÁNÍ KLASIFIKOVANÝCH NEBO JINAK SPECIFICKY KATEGORIZOVANÝCH UTAJOVANÝCH INFORMACÍ, MUSÍ ZAHRNOVAT OPATŘENÍ PRO POVINNÉ ŘÍZENÍ PŘÍSTUPU. TO ZNAMENÁ, ŽE MUSÍ ZAHRNOVAT SOUBOR PRAVIDEL PRO ŘÍZENÍ PŘÍSTUPU, ZALOŽENÝ PŘÍMO NA POROVNÁNÍ INDIVIDUÁLNÍCH ČITELNÝCH NEBO AUTENTIZAČNÍCH OPRÁVNĚNÍ PRO INFORMACE S KLASIFIKACÍ NEBO OZNAČENÍM UTAJENÍ A NEPŘÍMO FYZICKÝMI A OSTATNÍMI FAKTORY PROSTŘEDKŮ ŘÍZENÍ. PRAVIDLA POVINNÉHO ŘÍZENÍ PŘÍSTUPU, MUSÍ PŘESNĚ ODRÁŽET ZÁKONY, PŘEDPISY A OBECNOU POLITIKU, Z NICHŽ JSOU ODVOZENA.

5.3.1.2 **Výběrová bezpečnostní politika**

Výběrové zabezpečení je hlavní typ řízeného přístupu, který je dnes dostupný v počítačových systémech. Základem tohoto druhu zabezpečení je,

že individuální uživatel nebo program operující v jeho prospěch je oprávněn specifikovat explicitně typy přístupu, které mohou mít ostatní uživatelé jím řízených informací. Diskrétní zabezpečení se liší od povinného zabezpečení v tom, že implementace nástrojů politiky řízení přístupu pracují na základě znalosti individuálních potřeb oproti povinnému řízení, kde je řídícím nástrojem klasifikace nebo označení utajení informace.

Výběrové řízení není náhradou za povinné řízení. V prostředí, v němž se nacházejí klasifikované informace (např. v DoD), zajišťuje výběrové zabezpečení jemnou granularitu řízení v rámci celkové koncepce povinné politiky. Přístup ke klasifikovaným informacím vyžaduje efektivní současnou implementaci typů kontroly, jako předběžné podmínky k poskytnutí přístupu. Obecně - žádná osoba nemůže mít přístup ke klasifikovaným informacím, ledaže: a) osoba byla určena jako důvěryhodná, t.j., má garantovaný individuální stupeň zabezpečení — POVINNÝ, a b) přístup je nutný pro výkon služebních povinností, t.zn., je ve skupině potřeba-znalost (need-to-know) — VÝBĚROVÝ. Jinými slovy, výběrové řízení dává individuální volnost jednání při rozhodnutí, na jehož základě bude přípustný přístup skutečně povolen pro uživatele, včetně důsledků politiky povinných restrikcí. Hlavní cíl je:

HLAVNÍ CÍL VÝBĚROVÉHO ZABEZPEČENÍ

BEZPEČNOSTNÍ POLITIKA DEFINOVANÁ PRO SYSTÉMY, KTERÉ JSOU POUŽÍVÁNY KE ZPRACOVÁNÍ KLASIFIKOVANÝCH NEBO JINAK UTAJOVANÝCH INFORMACÍ, MUSÍ ZAHRNOVAT OPATŘENÍ PRO VYNUCENÍ PRAVIDEL VÝBĚROVÉHO ŘÍZENÍ PŘÍSTUPU. TO ZNAMENÁ, ŽE MUSÍ ZAHRNOVAT SOUBOR PRAVIDEL PRO ŘÍZENÍ A OMEZENÍ PŘÍSTUPU, ZALOŽENÝ NA INDIVIDUÁLNÍ IDENTIFIKACI TOHO, KDO MÁ OPRÁVNĚNÍ PRACOVAT S INFORMACEMI.

5.3.1.3 **Označování**

V rámci implementace souboru mechanizmů účinně zajišťujících bezpečnostní politiku je nutné, aby systém označoval informace s odpovídající klasifikací nebo utajením návěstími a tato návěstí udržoval po celou dobu

jejich zpracování. Jakmile je jednou informace přesně a nezměnitelně označena, musí být porovnání povinným řízením přístupu prováděno nepřetržitě a přesně. Další výhodou systému návěstí klasifikace nebo utajení je schopnost automatického vytváření správně "návěstím označeného" výstupu. Návěstí, jsou-li vestavěna a přesně udržována systémem, zůstávají přesná při výstupu ze systému. Hlavní cíl je:

HLAVNÍ CÍL OZNAČOVÁNÍ

SYSTÉMY, KTERÉ JSOU PROJEKTOVÁNY K VYNUCENÍ POVINNÉ BEZPEČNOSTNÍ POLITIKY, MUSÍ UCHOVÁVAT A CHRÁNIT INTEGRITU KLASIFIKACE NEBO JINÝCH NÁVĚSTÍ UTAJENÍ PRO VŠECHNY INFORMACE. NÁVĚSTÍ EXPORTOVANÁ SYSTÉMEM SE MUSÍ PŘESNĚ SHODOVAT S EXPORTOVANÝMI INTERNÍMI NÁVĚSTÍMI UTAJENÍ.

5.3.2 **Odpovědnost**

Druhým základním hlavním cílem je jeden ze základních principů zabezpečení, t.j. individuální odpovědnost. Individuální odpovědnost je klíč k zabezpečení a kontrole každého systému, který zpracovává informace ve prospěch subjektu nebo skupiny subjektů. Tento požadavek musí být v souladu s hlavním cílem.

Prvním požadavkem je individuální identifikace uživatele.

Druhým je nutnost ověření identifikace:

- identifikace je funkčně závislá na ověření,

- bez ověření nemá identifikace uživatele důvěryhodnost,

- bez důvěryhodné totožnosti, neekrétní bezpečnostní politiky, protože neexistuje záruka, že mohou být zpracovány odpovídající autorizace.

Třetím požadavkem je spolehlivá kontrola práv. To znamená, že zabezpečený počítačový systém musí zajistit autorizaci osob s právy ke

kontrole každé akce, která může potenciálně zajistit přístup ke generování nebo umožní zveřejnění klasifikované nebo jinak utajované informace. Kontrolní údaje musí být získány výběrem, založeným na kontrole evidenčního záznamu potřebného pro danou instalaci a/nebo aplikaci. Přesto však musí k podpoře trasování kontrolovaných jevů ke konkrétní osobě, u které byly zachyceny akce nebo aktivity v její prospěch, existovat dostačující granularita v kontrolních údajích. Hlavní cíl je:

HLAVNÍ CÍL ODPOVĚDNOSTI

SYSTÉMY, KTERÉ JSOU POUŽITY PRO ZPRACOVÁNÍ NEBO MANIPULACI S KLASIFIKOVANÝMI NEBO JINAK UTAJOVANÝMI INFORMACEMI, MUSÍ ZAJISTIT INDIVIDUÁLNÍ ODPOVĚDNOST, KDYKOLIV JE BUĎ POVINNOU NEBO VÝBĚROVOU BEZPEČNOSTNÍ POLITIKOU VYVOLÁNA. DÁLE MUSÍ EXISTOVAT SCHOPNOST V ROZUMNĚ KRÁTKÉ DOBĚ A BEZ ZBYTEČNÝCH OBTÍŽÍ ZAJISTIT ODPOVĚDNOST SCHVÁLENÝCH A OPRÁVNĚNÝCH ČINITELŮ ZA PŘÍSTUP A HODNOCENÍ EVIDENČNÍCH INFORMACÍ O ZABEZPEČENÝCH INFORMACÍCH.

5.3.3 **Záruka**

Třetí základní cíl se zabývá garancemi nebo zajištěním faktu, že bezpečnostní politika byla zavedena správně a že bezpečnostně významné prvky systému přesně zprostředkovávají a vynucují záměry politiky. Dále musí záruka zahrnovat garanci, že zabezpečená část systému pracuje pouze tak, jak má. Ke splnění tohoto cíle jsou nutné dvě záruky: záruka životního cyklu a záruka operační.

Záruka životního cyklu se odvolává na kroky stanovené organizací k zajištění toho, že systém je projektován, vyvíjen a udržován s použitím formalizovaných a přísných kontrol a norem. [17] Počítačové systémy, které zpracovávají a uchovávají utajované nebo klasifikované informace, jsou k ochraně těchto informací závislé na hardwaru a softwaru. To znamená, že hardware a software musí být chráněny proti neautorizovaným změnám, které mohou způsobit chybnou funkci ochranných mechanizmů nebo je zcela vyloučit.

Z tohoto důvodu musí být zabezpečené počítačové systémy opatrně vyhodnocovány a testovány během projektové a vývojové fáze a revidovány vždy, kdykoliv jsou provedeny změny, které by mohly postihnout ochranné mechanizmy. Pouze tímto způsobem může být poskytnuta záruka, že hardwarová a softwarová interpretace bezpečnostní politiky je přesná a bez úprav.

Zatímco záruka životního cyklu se zabývá procedurami pro řízení projektování, vývoj a údržbu systému, operační záruka se zaměřuje na rysy a architekturu systému, které mají zajistit, že bezpečnostní politika je prosazována během činnosti systému bez možnosti obejití. To znamená, že bezpečnostní politika musí být integrována v hardwarových a softwarových možnostech ochrany systému. Příklady kroků určených k zajištění těchto možností ochrany zahrnují: metody pro testování hardwaru a softwaru na správnost funkce, izolaci kódů kritických pro ochranu a použití hardwaru a softwaru k zajištění odlišných oblastí. Hlavní cíl je:

HLAVNÍ CÍL ZÁRUKY

SYSTÉMY, KTERÉ JSOU POUŽITY PRO ZPRACOVÁNÍ NEBO MANIPULACI S KLASIFIKOVANÝMI NEBO JINAK UTAJOVANÝMI INFORMACEMI, MUSÍ BÝT KONSTRUOVÁNY TAK, ABY GARANTOVALY SPRÁVNOST A PŘESNOST INTERPRETACE BEZPEČNOSTNÍ POLITIKY A NESMÍ ZMĚNIT ZÁMĚR TÉTO POLITIKY. MUSÍ BÝT POSKYTNUTA ZÁRUKA, ŽE SPRÁVNOST REALIZACE A ČINNOST POLITIKY EXISTUJE V CELÉM ŽIVOTNÍM CYKLU SYSTÉMU.

6.0 **Přístup k hodnocení tříd**

6.1 **Koncepce referenčního monitoru**

V říjnu 1972 vydala The Computer Security Technology Planning Study, vedená Jamesem P. Andersonem a spol., zprávu pro Electronics Systems Division (ESD) US Air Force. [1] V této zprávě byla předložena koncepce "referenčního monitoru, který vyžaduje autorizovaný přístup mezi subjekty a objekty systému". Referenční monitor byl shledán jako podstatný