SECURITY OF INFORMATION SYSTEMS

Jan SAMEK, Master Degree Programme (5)
Dept. of Intelligent Systems, FIT, BUT
E-mail: xsamek03@stud.fit.vutbr.cz

Supervised by: Dr. František Zbořil ml.

ABSTRACT

The objective of this work is an analysis of information systems from the security point of view, especially analysis of risks and threats of current commercial information systems. The primary goal of this work is a proposal of security measures for information system Alcatis. Nevertheless, this proposal must be unconditionally preceded by a study of general principles in the area of information systems and technology security.

1 ÚVOD

Informační systémy (IS) zajišťují v dnešní době velmi důležitou funkci v oblasti informačních technologií (IT) a to především uvnitř organizací - intranet. Tyto IS zpracovávají stále větší objemy dat, s mnohdy nezanedbatelnou hodnotou. Tato data lze označit jako velmi citlivé informace (např.: interní údaje o klientech a jejich účtech) a je třeba náležitě zabezpečit.

Ve své podstatě a ve své šíři je řešení informační bezpečnosti multidisciplinární obor nabízející komplexní pohled na problematiku ochrany informací, jež se zabývá otázkami organizačními, řídícími, metodickými, technickými, právními, sociálními a dalšími.

Výsledkem této prace je stanovení bezpečnostní politiky, analýza rizik a návrh bezpečnostních mechanismů konktrétního komerčního informačního systému.

2 BEZPEČNOSTNÍ POLITIKA, ANALÝZA RIZIK

Bezpečnostní politika je souhrn norem, pravidel a praktik, definující způsob správy, ochrany a distribuce citlivých dat a jiných aktivit v rámci činnosti IS [1].

Analýza rizik IS je klíčovou aktivitou v procesu řešení bezpečnosti a proto je třeba této aktivitě věnovat velkou pozornost.

Cílem analýzy je identifikovat rizika a hrozby, nalézt slabá místa IS a určit, jaké škody mohou případným útokem vzniknout. Součástí analýzy rizik by měla také být zpráva o náročnosti (finanční) implementace bezpečnostních mechanismů.

3 INFORMAČNÍ SYSTÉM ALCATIS

Informační systém *Alcatis* je modulární IS intranetového typu, který je vhodný pro malé a středně velké společnosti v nevýrobních odděleních. Alcatis je založen na třívrsvé architektuře, jednotlivé vrstvy jsou:

- Databázová vrstva - uschovává informace v IS, použit systém MySQL
- Aplikační vrstva - nejsložitější část, zde je využito několik programovacích nástrojů: PHP, CGI, Perl, BASH, C/C++. Progamovací jazyky nižší úrovně zajištují vnitřní komunikaci mezi procesy systému a nástroje PHP/CGI generují formát XUL [2], který interpretuje třetí vrstva.
- Klientská vrstva - je založena na bázi prohlížečů rodiny Mozilla, které jsou schopny reprezentova XUL formát. Dynamickou část klientské vrstvy zajištujě jazyk JavaScript za použití komponent XPCOM [3].

4 BEZPEČNOST IS ALCATIS

Analýza rizik a návrh bezpečnostních mechanismů byly řešeny pro jednotlivé vrstvy informačního systému zlášť.

4.1 DATABÁZOVÁ VRSTVA

Zde bylo třeba prověřit typ prostředí, do kterého má být systém nasazen aby mohl být stanoven plán zálohování, archivace a případného obnovení databázových dat. Zálohování databázových dat je řešeno minimálně jednou denně, kopie aktuálních dat je přímo šifrována pomocí asymetrické kryptografie systémem PGP. Dále je pak třeba řešit archivaci záloh na příslušné medium.

V technické rovině byla analýza zaměřena především na schopnosti databázového systému tak, aby nedocházelo k problému integrity dat v databázi při současných přístupech. Na tomto místě také byla provedena analýza kritických transakcí v systému a stanovena pravidla pro zajištění jejich dokončení. Mechanismus správy transakcí a současného přístupu je ve větší míře zajištěn zvoleným databázovým systémem, další speciální opatření pro zajištění integrity dat byla implementována v aplikační vrstvě.

4.2 APLIKAČNÍ VRSTVA

Zdaleka nejnáročnější je analýza a návrh bezpečnostnosních mechanismů aplikační vrstvy, ta tvoří jádro celého systému a zpostředkovává komunikaci mezi všemi vrstvami. Pro zajištění důvěrnosti je pro systém použit model nepovinného řízení přístupu. Komunikace mezi klientskou a aplikační vrtstvou je založena na protokolu SSL (HTTPS), čímž se minimalizuje možnost útoku pomocí odchytávání komunikace. Databázová a aplikační vrstva je provozována na jednom fyzickém stroji (serveru) a problém šifrování komunikace mezi těmito dvěmi vrstvami není třeba řešit. Je pouze třeba zajistit omezení přístupu (fyzického i síťového) neoprávněných osob k tomuto serveru.

Největší bezpečnostní rizika byla zjištěna při autorizaci a ověření práv uživatele systému, kdy bylo možné při vhodném upravení klientské vrstvy zadat na systém dotaz, na který neměl uživatel příslušnou úroveň oprávnění a server vrátil příslušnou odpověď. Část aplikační vrstvy, která byla schopna takovéto chování odhalit, musela být do systému dodatečně přidána. Přidána byla další nezavislá část, která má za úkol zaznamenat aktivity uživatelů v systému a na základě práv uživatelů a bezpečnostních pravidel systému se provádí analýza takto získaných informací a v případě zjištění podezřelého chování (jednotlivé aktivity systém ohodnotí stupněm možného rizika) je zásláno upozornění s podrobnými informacemi o tomto chování administrátoru systému.

4.3 KLIENTSKÁ VRSTVA

Klientská vrstvu představuje prohlížeč *Mozilla*, což je čistě Open Source produkt a jeho modifikace není pro zkušeního útočníka problémem. Bezpečnost této vrstvy nelze řešit přímo v ní, ale musí být řešena na straně serveru tak, že veškeré požadavky zadané prostřednictvím toho klienta je třeba verifikovat aplikační vrstvou. Tato verifikace se skláda z několikati stupňů v závislosti na charakteru požadavku a jeho výsledku. Problém interpretace dat (do grafického rozhraní) ze serveru na straně modifikovaného klienta nelze v současné době vyřešit bez ztráty univerzálnosti klientské vrstvy, která je dána především multiplatformností prohlížeče *Mozilla*.

5 ZÁVĚR

Výsledkem analýzy rizik je návrh bezpečnostních mechanismů. Jejich implementace ještě není zcela dokončena a mnohody je třeba brát také zřetel na požadavky a potřeby zákazníka, u kterého má být systém nasazen. Zhodnocení úspěšnosti implementovaných opatření a jejich případné přehodnocení je třeba provádět od okamžiku nasení systému až do konce jeho životního cyklu. Je důlužité si uvědomit, že v této rychle se rozvíjející oblasti IS vznikají stále nové druhy útoků a bezpečnostních rizik, čímž se proces řešení bezpečnosti IS stává nekonečným cyklem analýzy rizik a implementace bezpečnostních mechanismů.

Nakonec je třeba zdůraznit, že v případě selhání klíčového lidského faktoru jsou všechna sebelepší bezpečnostní opatření zcela neúčinná a v tomto případě přichází na řadu havarijní plán, který zajistí minimalizaci škod bezprostředně po útoku.

REFERENCE

[1] Hanáček, P., Staudek, J.: Bezpečnost informačních systémů - Praha, CZ, 2000, ISBN 80-238-5400-3

[2] XUL: XML User-interface Language
`http://www.mozilla.org/projects/xul/`

[3] XPCOM: Cross Platform Component Object Model
`http://www.mozilla.org/projects/xpcom/`