VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA INFORMAČNÍCH TECHNOLOGIÍ
FACULTY OF INFORMATION TECHNOLOGY

ÚSTAV INTELIGENTNÍCH SYSTÉMŮ
DEPARTMENT OF INTELLIGENT SYSTEMS

BEZPEČNOSTNÍ METRIKY PLATFORMY SAP

SECURITY METRICS OF SAP PLATFORM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. LENKA TŘEŠTÍKOVÁ**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. MATEJ KAČIC**
SUPERVISOR

BRNO 2017

Zadání diplomové práce/20134/2016/xtrest01

Vysoké učení technické v Brně - Fakulta informačních technologií

Ústav inteligentních systémů Akademický rok 2016/2017

Zadání diplomové práce

Řešitel: **Třeštíková Lenka, Bc.**
Obor: Informační systémy
Téma: **Bezpečnostní metriky platformy SAP**
Security Metrics of SAP Platform
Kategorie: Bezpečnost

Pokyny:

1. Prostudujte standardy, postupy a metodiky pro ohodnocení stavu bezpečnosti informačních systémů.
2. Navrhněte metriky a metodiku pro bezpečnostní zhodnocení systémů založených na platformě SAP. Definujte kritičnost jednotlivých bezpečnostních metrik.
3. Navrženou metodiku formalizujte a vytvořte dotazník pro ohodnocení celkového stavu bezpečnosti systému. Metriky, které je možné vyhodnotit strojově, implementujte pomocí vhodného skriptovacího jazyka.
4. Pomocí navržených postupů v předcházejícím bodě zhodnoťte stav bezpečnosti na poskytnutém vzorovém systému od společnosti SAP.
5. Diskutujte možnosti dalšího rozšíření.

Literatura:

- Layton, Timothy P. *Information Security: Design, implementation, measurement, and compliance*. CRC Press, 2016.
- Landoll, Douglas J., and Douglas Landoll. *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press, 2005.
- Bishop, Matt. "Introduction to computer security", 2005.

Podrobné závazné pokyny pro vypracování diplomové práce naleznete na adrese http://www.fit.vutbr.cz/info/szz/

Technická zpráva diplomové práce musí obsahovat formulaci cíle, charakteristiku současného stavu, teoretická a odborná východiska řešených problémů a specifikaci etap, které byly vyřešeny v rámci dřívějších projektů (30 až 40% celkového rozsahu technické zprávy).

Student odevzdá v jednom výtisku technickou zprávu a v elektronické podobě zdrojový text technické zprávy, úplnou programovou dokumentaci a zdrojové texty programů. Informace v elektronické podobě budou uloženy na standardním nepřepisovatelném paměťovém médiu (CD-R, DVD-R, apod.), které bude vloženo do písemné zprávy tak, aby nemohlo dojít k jeho ztrátě při běžné manipulaci.

Vedoucí: **Kačic Matej, Ing.**, UITS FIT VUT
Datum zadání: 1. listopadu 2016
Datum odevzdání: 24. května 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
Fakulta informačních technologií
Ústav inteligentních systémů
612 66 Brno, Božetěchova 2

L.S.

doc. Dr. Ing. Petr Hanáček
vedoucí ústavu

Abstrakt

Cílem práce je zanalyzovat možná rizika působící na platformu SAP NetWeaver, využívané pro běh podnikových systémů společnosti SAP, a identifikovat nejrůznější zranitelnosti plynoucí ze špatné konfigurace systému, nedůkladného oddělení rolí v systému či nedůsledné aplikace záplat. V rámci této práce bude vytvořena metodika pro evaluaci platformy definující zranitelnosti a navrhující bezpečnostními požadavky a opatření pomáhající eliminovat rizika působící na systém.

Abstract

Main goal of this thesis is analyzing potential security risks of the SAP NetWeaver platform and identifying various vulnerabilities, that are results of poor system configuration, incorrect segregation of duties or insufficient patch management. Methodology for platform evaluation is defined by vulnerabilities, security requirements and controls will be created.

Klíčová slova

SAP NetWeaver, SAP Business Suite, Enterprise Resource Planning, podnikový software, ABAP aplikační server, bezpečnost, hodnocení bezpečnosti, bezpečnostní metriky, bezpečnostní analýza

Keywords

SAP NetWeaver, SAP Business Suite, Enterprise Resource Planning, enterprise software, ABAP application server, security, security evaluation, security metrics, security analysis

Citace

TŘEŠTÍKOVÁ, Lenka. *Bezpečnostní metriky platformy SAP*. Brno, 2017. Diplomová práce. Vysoké učení technické v Brně, Fakulta informačních technologií. Vedoucí práce Kačic Matej.

Bezpečnostní metriky platformy SAP

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně pod vedením pana Ing. Mateje Kačice. Uvedla jsem všechny literární prameny a publikace, ze kterých jsem čerpala.

.....
Lenka Třeštíková
23. května 2017

Poděkování

Ráda bych poděkovala svému vedoucímu panu Ing. Mateji Kačicovi za metodické vedení, vstřícný přístup a cenné odborné rady využité při psaní této diplomové práce. Dále děkuji svým kolegům ze společnosti SAP, zejména pak panu Ing. Tomášovi Hladíkovi a panu Petrovi Babičovi, za poskytnutí studijní literatury a odborných konzultací.

Obsah

Kapitola 1

Úvod

Podnikové informační systémy jsou dnes jádrem každé větší společnosti, integrují a automatizují velkou část důležitých činnosti daného podniku z oblasti financí, personalistiky, výroby, logistiky a prodeje. Největším poskytovatelem těchto systémů je německá společnost SAP, jejíž nejznámější produkt je softwarový balík pro řízení podniku SAP Business Suite běžící na platformě SAP NetWeaver. Veškeré informace vytvářené, zpracovávané a ukládané v tomto typu systému jsou pro společnosti citlivé. Neautorizovaný přístup k těmto informacím, jejich narušení či zničení mohou způsobit narušení obchodního procesu, což v důsledku znamená pro podnik kritické ztráty. Bezpečnost systému je markantně snížena nesprávnou konfigurací nebo ignorováním bezpečnostních záplat vydávaných společností SAP. Systém pro řízení podniku je velice komplexní a aplikace záplat většinou vyžaduje i manuální zásahy, proto nejsou bezpečnostní záplaty často nasazovány včas.

Cílem práce je zanalyzovat možná rizika působící na platformu SAP NetWeaver a identifikovat nejrůznější zranitelnosti plynoucí ze špatné konfigurace systému, nedůkladného oddělení rolí v systému či nedůsledné aplikace záplat. Pravidelné auditování SAP systémů pomáhá odhalit a následně minimalizovat nebo úplně odstranit tyto zranitelnosti aplikací správných bezpečnostních opatření. V rámci této práce bude vytvořena metodika pro evaluaci platformy SAP NetWeaver definující zranitelnosti a navrhující bezpečnostními požadavky a opatření, která pomáhají eliminovat rizika působící na systém, a tím minimalizovat obchodní ztráty.

V úvodu práce je představeno softwarové řešení společnosti SAP a jeho historický vývoj od roku 1972, kdy byla společnost založena, až po současnost. Další část kapitoly 2 se soustředí na architekturu systému, technologické požadavky, proprietální jazyk společnosti ABAP a technologickou platformu SAP NetWeaver na níž běží aktuálně nejpopulárnější produkt společnosti SAP Business Suite. V závěru kapitoly je představen způsob práce se systémem SAP.

Důležité pojmy z hlediska bezpečnosti informačních systémů a jednotlivé fáze analýzy rizik, konkrétně analýza aktiv, hrozeb, zranitelností a ochranných opatření jsou definovány v kapitole 3. Ta také popisuje historický vývoj standardů a metod pro ohodnocení stavu bezpečnosti informačních systémů začínající v USA vytvořením Kritérií hodnocení důvěryhodných výpočetních systémů *TCSEC*, z nichž se postupně vyvinuly další standardy jako Kritéria hodnocení bezpečnosti informačních systémů *ITSEC*, Kanadská kritéria hodnocení bezpečnosti *CTCPEC* a Federální kritéria *FC*. Dále jsou rozebrána Všeobecná kritéria *CC* vyvinutá z předešlých, řada norem ISO/IEC 27000 a projekty komunity *OWASP* zabývající se zejména bezpečností webových aplikací. Poslední část kapitoly 3 definuje využití metrik v oblasti bezpečnosti informačních systémů, dělí je dle různých kritérií, představuje

měření dle normy ISO/IEC 27004 a blíže se soustředí na metriky pro ohodnocení zranitelností *CVSS*. V závěru kapitoly je definována vlastní metodika pro ohodnocení kritičnosti bezpečnostních požadavků.

Kapitola 4 představuje analýzu platformy SAP NetWeaver 7.5 s aplikačním serverem ABAP na níž běží v dnešní době nejrozšířenější produkt společnosti SAP ERP z balíku SAP Business Suite. Uvádí dokumenty z nichž lze vycházet pro ohodnocení bezpečnostního stavu databáze a operačního systému a soustředí se na opatření pro zajištění bezpečnosti aplikační platformy, vycházející z požadavků vytvořených komunitou *OWASP*, standardu ISO/IEC 27002 a známých potenciálních zranitelností aplikační platformy systémů SAP popsaných ve vydaných SAP Security Notes. Analýza aplikační platformy je rozdělena do šesti kategorií zahrnující správu záplat a aktualizací, řízení přístupu, analýzu nepoužívaných funkcionalit, analýzu přístupu k rozhraním vzdálené správy, bezpečnost přenosu a logování bezpečnostních událostí.

Kapitola 5 popisuje tvorbu metodiky a jednotlivých metrik pro ohodnocení celkového stavu bezpečnosti systému, vytvořených v podobě dotazníku s definovanými bezpečnostními riziky a požadavky pro platformu ohodnocenými dle kritičnosti.

Předposlední část práce se věnuje testování postupů popsaných v předešlé kapitole a v dotazníku. Hodnotí stav bezpečnosti testovaného systému nejmenované společnosti s řešením SAP ERP běžícím na SAP NetWeaver 7.5. Výsledky jsou reprezentovány v podobě grafů ukazujících situaci testovaného systému. Je uveden přehled všech nesplněných bezpečnostních požadavků daným systémem.

Závěr hodnotí dosažené výsledky a uvádí možnosti využití a dalšího rozšíření práce.

Kapitola 2

Softwarové řešení společnosti SAP

SAP[1] je německá společnost se sídlem ve Walldorfu založena roku 1972. Jedná se o jednoho z největších poskytovatelů podnikových aplikací. Nabízí software pro řízení podniku, řešení pro datové sklady, software pro malé a střední podniky, platformy pro vývoj webových i standardních aplikací, software pro integraci jednotlivých počítačových systémů, či různá řešení pro cloud computing [3].

Společnost vyvinula vícejazyčnou a mnohonárodní platformu, do níž lze snadno zahrnout nové standardní podnikové procesy a postupy. Systém může být provozován na různých hardwarových platformách a operačních systémech s využitím různých databází.

SAP ve svém softwaru odráží osvědčené postupy z různých odvětví a tím podnikům usnadňuje nasazení softwaru i využití osvědčených postupů [3]. Odvětvová řešení společnosti SAP se dělí do dvaceti pěti oblastí, jako jsou bankovnictví, letectví a obrana, pojišťovnictví, zdravotní péče a další[2].

Systém SAP je dnes využíván téměř 345 tisíci zákazníků ve více než 180 zemích světa[3] a představuje univerzální řešení pro všechny podniky. Lze jej rozdělit na komponenty představující podnikové aplikace. Určitou funkcionalitu v rámci jedné komponenty nabízí moduly, typickým příkladem komponenty může být SAP ERP *Enterprise Resource Planning*, jejíž moduly jsou modul finančního účetnictví, modul plánování výroby, modul pro řízení lidských zdrojů či modul korporátních služeb. Každý modul řeší problematiku určitého pracovního úseku nebo funkční oblasti.

Součástí podnikového procesu je mnoho různých transakcí. Každá transakce představuje jeden krok celého procesu. V mnoha případech jsou všechny transakce součástí jednoho modulu. Některé podnikové procesy však vyžadují spuštění transakcí v několika různých modulech a někdy i v několika různých komponentách. Typickým příkladem podnikového procesu může být například proces prodeje, který zahrnuje transakce jako zadání zákaznické objednávky do systému, odběr zásob, vytvoření dodávky a vystavení faktury za odeslané zboží [3].

[1] SAP je akronymem z německého Systeme, Anwendungen und Produkte in der Datenverarbeitung či anglického Systems, Applications and Products in Data Processing.

[2] Výčet odvětví a lze nalézt na webové stránce společnosti: https://www.sap.com/cz/solution.html.

[3] Údaj dostupný na oficiálních stránkách společnosti: https://www.sap.com/corporate/en/company.fast-facts.html.

2.1 Historie systémů SAP

Od roku 1972 prošlo softwarové řešení SAP četnými změnami. Prvním řešením byl SAP R/1, což byl systém finančního účetnictví, který běžel na sálových počítačích od IBM a operačním systému MS DOS. Roku 1979 se na trhu objevil produkt SAP R/2 běžící také na sálových počítačích firmy IBM a Siemens, jeho součástí bylo již více funkčních modulů pro řízení podniku [21]:

- finanční účetnictví *FI*,
- řízení lidských zdrojů *HR*,
- skladové hospodářství *MM*,
- plánování a řízení výroby *PP*,
- podpora prodeje *SD*.

Produkt SAP R/3 byl pro společnost velkým úspěchem, díky kterému se stala lídrem na trhu mezi poskytovateli ERP řešení. Vznikl roku 1992, jednalo se o systém s architekturou klient-server, který využíval relační databázi. Toto řešení bylo kompatibilní s většinou operačních systémů a bylo nezávislé na hardwarové platformě. SAP R/3 obsahoval stejné moduly jako jeho předchůdce SAP R/2 a byl rozšířen o sedm dalších modulů [19]:

- evidence majetku *AM*,
- kontroling *CO*,
- údržba *PO*,
- management kvality *QM*,
- řízení oběhu dokumentů *WF*,
- specifická řešení různých odvětví *IS*,
- plánování dlouhodobých projektů *PS*.

Koncem devadesátých let začal SAP vyvíjet další komponenty: Product Lifecycle Management *PLM*, Supplier Relationship Management *SRM*, Customer Relationship Management *CRM*, Supply Chain Management *SCM*. Jejich spojením s komponentou ERP vznikl roku 1999 produkt SAP R/3 Enterprise. V roce 2004 byl uveden na trh balík SAP Business Suite spolu s technologickou platformou SAP NetWeaver, oba tyto produkty budou blíže popsány v sekcích 2.6 a 2.5. SAP Business Suite běžící na SAP NetWeaver je dnes nejrozšířenějším řešením mezi zákazníky společnosti.

K SAP Business Suite vzniká roku 2015 nová alternativa nazvaná SAP S/4HANA[4] běžící na SAP HANA Platform[5]. Toto cloudové řešení se stále dynamicky vyvíjí a je možné jej provozovat pouze na databázi SAP HANA, což je in-memory databáze vytvořena společností SAP[6].

[4] Zkratka S/4HANA pochází z anglického *SAP Business Suite 4 SAP HANA*.

[5] Zkratka HANA vznikla z anglického High-performance ANalytic Appliance.

[6] Více informací o HANA databázi může čtenář získat v knize A Course in In-Memory Data Managemen od jednoho ze zakladatelů SAP, Hasso Plattnera.

2.2 Technologické požadavky

Systém SAP je balíkem business aplikací, jehož technologické požadavky můžeme rozdělit na hadrwarové a softwarové požadavky.

2.2.1 Hardwarové požadavky

Společnost SAP vyvinula nástroj Quick Sizer[7] převádějící business požadavky na technické. Nástroj pomáhá definovat minimální hardwarove požadavky pro provoz konkrétního systému mezi než patří požadavky na server a úložiště.

Server je nezbytný pro provoz systému SAP. Může být fyzicky instalovaný a běžící ve vlastním datovém centru podniku či hostovaný u nějakého tradičního poskytovatele. Výkon je v případě SAP měřen jednotkou SAPS (SAP Application Performance Standard)[8].

Úložiště je nezbytné pro uložení databází systému SAP, jeho instalačních a spustitelných souborů. Systémy SAP mohou využívat následující typy úložišť [3]:

- **Úložiště typu SAN** *Storage Area Network* sestává z desítek až stovek fyzických disků. Všechny disky jsou propojeny databázovým serverem systému SAP prostřednictvím vstup-výstupních karet HBA (Host Bus Adapter). Tato úložiště jsou rychlá a mohou být využívána více aplikacemi. Většina soudobých systémů SAP využívá SAN jako své primární úložiště.
- **Úložiště typu NAS** *Network Attached Storage* jsou levnější a obecně i méně výkonná než SAN. Jsou připojena k databázi pomocí karty instalované v databázovém serveru, využívají tedy standardní síťové karty a ne karty HBA. Síťové karty mohou být využívané i aplikačními servery systému SAP a dalšími aplikacemi, proto se v případě použití úložišť typu NAS může vyskytnout zpomalení.
- **Přímo připojená úložiště** jsou u některých systémů SAP dodnes využívána. Mohou být tvořena několika pevnými disky umístěnými ve skříni databázového serveru nebo v malých skříních propojených s databázovým serverem. Z hlediska malých podniků je toto řešení výhodné, neboť přímo propojená úložiště jsou rychlá a poměrně levná. Náklady však narůstají s přidáváním dalších komponent systému SAP či prostředí (produktivní, vývojové, školící).
- Pro **cloudová úložiště** je největší výzvou výkon, neboť aktivní databáze systému SAP potřebuje zpracovat tisíce vstupně/výstupních operací za sekundu. K cloudovému úložišti přistupujeme přes internet. Další výzvou je bezpečnost dat, veškerá data jsou skladována na serveru poskytovatele.

[7] Více o nástroji Quick Sizer na oficiální stránce společnosti: https://www.sap.com/solution/benchmark/sizing.html.

[8] SAPS je hardwarově nezávislá měrná jednotka vyjadřující výkon a podobající se obecnějšímu hodnocení výkonu tpmC. SAPS je specifická pro systém SAP a je založena na modulu SD (Sales and Distribution) komponenty SAP ERP. Podle definice platí, že výkon 100 SAPS odpovídá 2000 plně zpracovaných zákaznických zakázek za hodinu, přičemž každá z těchto zakázek má 5 položek. Zpracování 2000 zákaznických zakázek odpovídá cca 6000 změnám obrazovek. Více informací: www.sap.com/solution/benchmark/measuring.html.

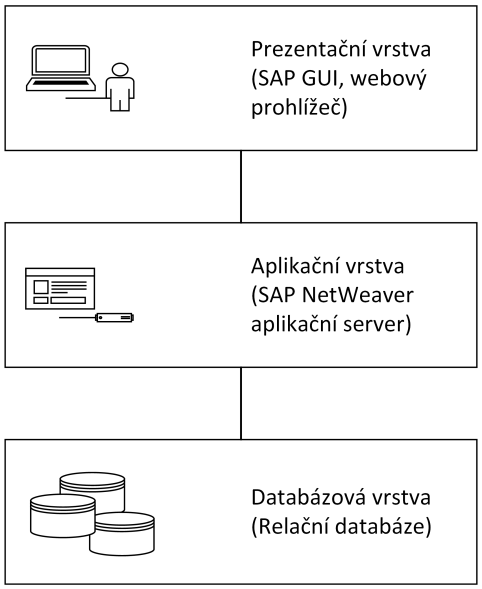
2.2.2 Softwarové požadavky

Operační systém může být pro provoz soudobých SAP systémů vybrán z následujícího výčtu: Windows, AIX, HP-UX, Solaris a SuSE Linux[9]. Z hlediska operačního systému je SAP sadou spustitelných souborů a knihoven propojujích uživatele s daty a logikou aplikace.

Databáze slouží jako úložiště zdrojových kódů programů, jejich spustitelných binárních verzí a dat. SAP podporuje většinu databázových strojů - Microsoft SQL Server, Microsoft SQL Azure, několik verzí Oracle a IBM DB2[10]. Dále existují dva databázové stroje společnosti SAP – MaxDB, který je určen spíše pro menší systémy, a SAP HANA, což je in-memory databáze. Každá komponenta systému SAP většinou vyžaduje svoji vlastní databázi obsahující tisíce tabulek s informacemi.

2.3 Architektura systému

Systémy SAP běží na třívrstvé architektuře zobrazené na obrázku 2.1, jejímž smyslem je vzájemně oddělit prezentační vrstvu, aplikační vrstvu a datové úložiště. Výhodou třívrstvé architektury je rozdělení výkonu mezi zařízení uživatele a server [40].



Obrázek 2.1: Třívrstvá architektura, zdroj: [23]

2.3.1 Prezentační vrstva

Prezentační vrstva je zodpovědná za interakci s uživatelem, reprezentuje ji především nástroj SAP GUI, který je dnes nejrozšířenějším grafickým uživatelským rozhraním používaným pro přístup k aplikacím SAP. Dalším uživatelským rozhraním je Java GUI pro SAP

[9]Seznam podporovaných operačních systémů lze nalézt na oficiálních stránkách společnosti v tzv. Product Availability Matrix: https://support.sap.com/release-upgrade-maintenance/pam.html.

[10]Seznam podporovaných databázových strojů lze nalézt na oficiálních stránkách společnosti v tzv. Product Availability Matrix: https://support.sap.com/release-upgrade-maintenance/pam.html.

(označované jako Platin GUI) umožňující přístup k systému SAP z počítačů s jiným operačním systémem než je Windows [23].

Vedle tlustého klienta je možné přistupovat k systému SAP přes webový prohlížeč. Nejčastěji je používán prohlížeč Microsoft Internet Explorer[11]. V případě, že má uživatel k dispozici přihlašovací údaje k systému SAP a funkční síťové připojení k systému SAP, je schopný se do systému připojit v podstatě odkudkoliv.

2.3.2 Aplikační vrstva

Aplikační server je základem pro SAP software. Poskytuje platformu pro vývoj, distribuci a provoz robustních webových služeb a business aplikací. Aplikační server podporuje programovací jazyk ABAP popsaný v sekci 2.4, Javu a webové služby. Návrh byl zaměřen na poskytnutí vysoké úrovně robustnosti a udržovatelnosti pro běžící aplikace. Do detailů bude SAP NetWeaver aplikační server popsán v kapitole 2.5.5.

2.3.3 Datová vrstva

Relační databáze se stovkami až tisíci tabulek představující datovou vrstvu je nejnižší vrstvou modelu zajišťující práci s daty [23].

2.4 Programovací jazyk ABAP

Programovací jazyk ABAP[12] je proprietálním jazykem společnosti SAP vytvořeným v sedmdesátých letech. Jedná se o programovací jazyk čtvrté generace odvozený z jazyka COBOL. Později byl přizpůsoben objektově orientovanému konceptu [22].

ABAP je hlavním programovacím jazykem společnosti SAP. Zdrojové programy jsou ukládány v SAP databázi, kde je uložena i jejich zkompilovaná binární verze. Programy jsou vyvíjeny, kompilovány a spouštěny v SAP prostředí.

2.5 Platforma SAP NetWeaver

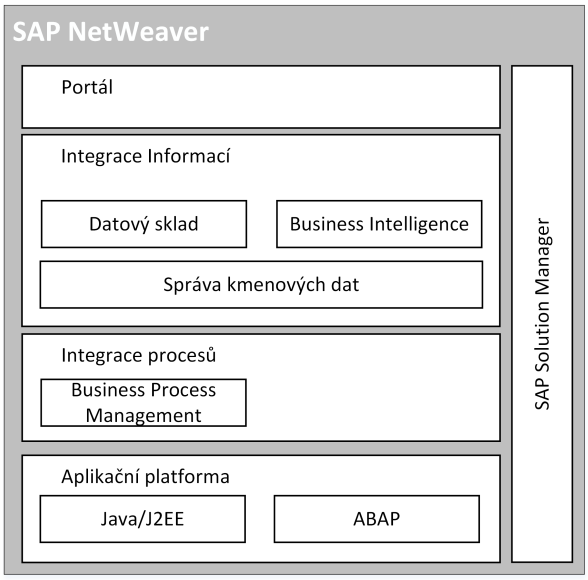
Technologickým základem pro produkt SAP Business Suite, popsaný v kapitole 2.6, je integrační a aplikační platforma SAP NetWeaver zahrnující kolekci aplikací, utilit a nástrojů uspořádaných do čtyř integračních úrovní, které jsou ilustrovány obrázkem 2.2. Z pohledu zákazníka je ze všech částí SAP NetWeaver k chodu komponenty ERP ze SAP Business Suite popsané v kapitole 2.6.1 potřeba pouze ABAP aplikační server napojený na databázi. Nicméně SAP NetWeaver je dodáván jako jeden balík s mnoha dalšími nástroji usnadňujícími aplikaci záplat *SAP Solution Manager*, propojení SAP systému s ne-SAP systémy *SAP Process Integration* a podobně.

2.5.1 Portál

SAP Portál nabízí uživatelům přístup ke zdrojům informací, podnikovým aplikacím a službám v rámci organizace přes webové rozhraní. Uživatelé vyžadující pouze omezenou funkcionalitu komponent SAP mohou využívat pouze portál, neinstalují tlustého klienta. V rámci

[11] Seznam podporovaných prohlížečů lze opět nalézt v Product Availability Matrix na webu společnosti https://support.sap.com/release-upgrade-maintenance/pam.html.

[12] ABAP je akronymem z německého Allgemeiner BerichtsAufbereitungsProzessor nebo anglického Advanced Business Application Programming.



Obrázek 2.2: Komponenty platformy SAP NetWeaver, zdroj: [32]

portálu mohou například sdílet dokumenty, vyhledávat informace o osobách v rámci organizace či zadávat své pracovní aktivity. SAP Netweaver Portál je J2EE aplikace komunikující se SAP Java aplikačním serverem, který je popsán v kapitole 2.5.5.

2.5.2 Integrace informací

Skupina pro integraci informací představuje funkcionalitu datového skladu a platformu pro *Business Intelligence* poskytující flexibilní nástroje pro vytváření přehledů, analýzu, a plánování usnadňující vyhodnocování a distribuci dat. Dále zahrnuje komponentu pro správu znalostí *Knowledge Warehouse* pro ukládání strukturovaných a nestrukturovaných dat a komponentu pro harmonizaci kmenových dat *Master Data Management*, která je využívána pro zajištění konzistence dat v případě, kdy jsou kmenová data využívána ve více systémech.

2.5.3 Integrace procesů

Poskytuje technickou infrastrukturu pro výměnu zpráv umožňující propojení SAP systémů a non-SAP systémů od různých výrobců, různých verzí, implementovaných v různých jazycích. Úkolem této úrovně je přesouvat a sdílet data mezi různými zdrojovými a cílovými systémy.

2.5.4 Správa a administrace aplikací

SAP Solution Life Cycle Manager je řešení pro správu a administraci aplikací. Nabízí sadu nástrojů pro podporu provozu SAP softwaru. Významnou funkcionalitou je správa aktualizací. Společnost SAP průběžně vylepšuje kvalitu a bezpečnost svých produktů a v rámci podpory jsou zákazníkům pravidelně nabízeny různé aktualizace a záplaty v podobě takzvaných *SAP Notes*. Existuje několik typů balíků záplat a aktualizací:

- **Bezpečnostní záplaty** *Security Patches* zveřejňované jedenkrát měsíčně jsou souborem takzvaných Security Notes obsahující důležité opravy z pohledu bezpečnosti. Solution Manager vyhodnocuje na základě zákazníkova implementovaného řešení, které záplaty by měly být aplikovány do zákazníkova systému. Aplikace záplat není povinná, ale je společností SAP silně doporučovaná, je poloautomatizovaná, někdy je třeba ruční zásah. Každá SAP Security Note opravující jednu specifickou zranitelnost nalezenou v řešení SAP obsahuje popis zranitelnosti, její hodnocení většinou ve formě CVSS skóre (více o CVSS skóre v kapitole 3.3.3) a automatické nebo manuální korekční instrukce pro aplikaci oprav do zákazníkova systému.

- **Balíky oprav** *SAP Support Packages* jsou souborem více bezpečnostních a funkcionálních záplat, který vychází několikrát ročně. Zákazníkům je doporučováno Support Package aplikovat alespoň jedenkrát ročně.

- **Balíky rozšíření** *SAP Enhancement Packages* jsou balíky zahrnující všechny předchozí SAP Support Packages a zároveň přidávají nové funkcionality. Jsou kumulativní, což znamená, že každý nový SAP Enhancement Package zahrnuje všechna rozšíření dodaná s předchozím.

- **Aktualizace systému** *SAP System Upgrade* znamená povýšení SAP systému na vyšší verzi systému zahrnující veškeré SAP Enhancement Packages a další vylepšení.

- **Přechod na novou verzi systému** *SAP Transition* představovalo převedení R/2 systémů na R/3 systémy. V dnešní době se jedná o převedení SAP Business Suite na NetWeaver platformě na S/4HANA na HANA Cloud Platform. Jedná se o složitý a komplexní proces, při kterém je většinou třeba asistence SAP specialisty.

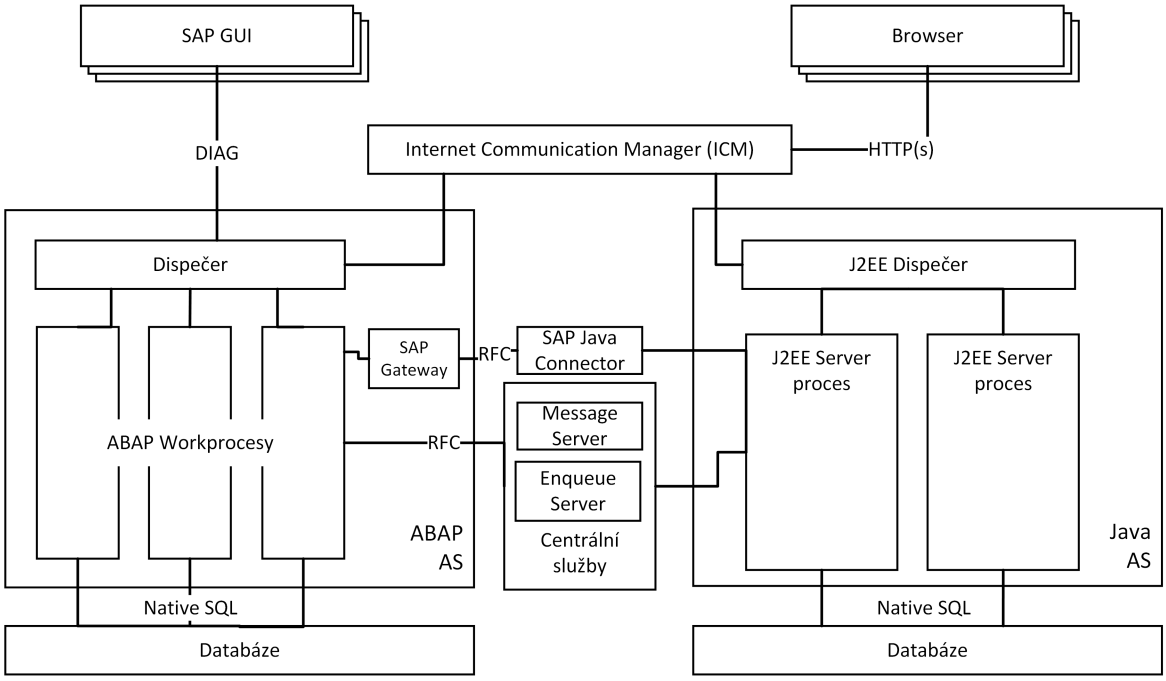
2.5.5 Aplikační platforma

Aplikační platforma sestává z jedné centrální instance aplikačního serveru a několika dalších instancí sloužících pro vyrovnání zátěže. Obrázek 2.3 ukazuje jednotlivé komponenty centrální instance ABAP a Java aplikačního serveru [32]. Existují tři varianty SAP NetWeaver aplikačního serveru:

- **ABAP Netweaver aplikační server** je instalace, se kterou je možné spouštět ABAP programy a vybrané jednoduché SAP Java aplikace. Java aplikace mohou běžet v ABAP Workprocesu díky Virtual Memory Container technologii. Na této variantě běží například SAP ERP.

- **Java Netweaver aplikační server** je řešení, na kterém běží například SAP NetWeaver Portál. Zákazník má možnost spouštět J2EE aplikace, ale žádné ABAP programy.

- **Kombinace ABAP a Java aplikačních serverů** umožňuje spouštět ABAP programy i Java aplikace. Tato verze umožňuje využívání SAP GUI i zpracování webových požadavků pro J2EE aplikační server a běží na ní například Netweaver Process Integration [32].



Obrázek 2.3: Centrální instance aplikačního serveru podporujícího ABAP i Javu [32]

Dispečer je centrální proces na aplikačním serveru. Je zodpovědný za spouštění workprocesů a distribuuje jednotlivé požadavky workprocesům. Pokud jsou všechny workprocesy vytížené, požadavky se uchovávají ve frontě dispečera. Jedná se o přístupový bod k aplikační vrstvě z hlediska vrstvy prezentační [23].

Workproces je logická komponenta systému, jejímž úkolem je spuštění aplikace či provedení kroku v již spuštěné aplikaci. Každý aplikační server zapisuje informace o svých workprocesech do databáze. Každý workproces může komunikovat s dispečerem, spouštět interpret dialogů, spouštět interpret jazyka ABAP či kontrolovat zápis uživatelského kontextu. Workprocesy můžeme rozdělit na několik typů [23]:

- **Dialogový workproces** vykonává všechny úlohy související s jednotlivými dialogovými kroky.
- **Aktualizační workproces** provádí databázové aktualizace. Existují dva aktualizační workprocesy U1 a U2. U1 typicky provádí časově kritické aktualizace, které jsou definované přímo v kódu příkazem IN UPDATE TASK, tyto aktualizace jsou zpracovávány synchronně. U2 provádí nekritické statistické aktualizace jako jsou například replikační mechanismy zahrnující kopii dat z jednoho systému do druhého a podobně.
- **Dávkový workproces** provádí dávkové požadavky a úlohy na pozadí, při kterých není nutná interakce uživatele.
- **Spool Workproces** je za přenos dat do výstupních zařízení jako jsou tiskárny. Platí, že na každém aplikačním serveru smí existovat poze jeden spoolový workproces.
- **Enqueue workproces** udržuje tabulku zámků. Díky nim se nemůže stát, aby dva různí uživatelé upravovali současně shodný datový objekt.

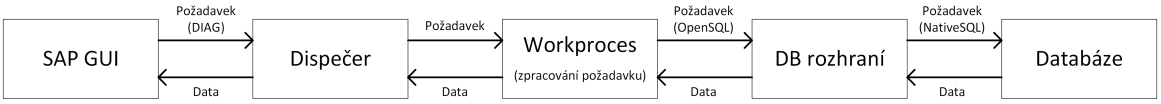
Gateway umožňuje komunikaci mezi různými SAP systémy prostřednictvím protokolu RFC *Remote Function Call*.

Message Server je součástí centrální instance aplikačního serveru, stará se o výměnu zpráv a vyrovnává zátěž v SAP systému. Rozhoduje, na který ze serverů se uživatel přihlásí. Komunikuje s dispečerem a získává statistická data o zátěži [23].

SAP Java Connector je middleware založený na Java Native Interface, umožňuje komunikaci mezi ABAP a Java prostředím. Převádí Java metody na RFC volání a obráceně [32].

Typický tok dat pro požadavek ze SAP GUI, ilustrovaný na obrázku 2.4, probíhá následovně:

1. Uživatel se přihlásí k požadovanému SAP systému přes SAP GUI.
2. Uživatel je přiřazen dispečeru, u kterého zůstává až do odhlášení.
3. Dispečer rozdistribuuje uživatelský požadavek workprocesům. Pokud jsou všechny workprocesy obsazeny, požadavek čeká ve frontě.
4. Workproces provede ABAP program.
5. Pokud je třeba, workproces se připojí přes databázové rozhraní k relační databázi.
6. Databázové rozhraní konvertuje Open SQL používané workprocesem na Native SQL a získá z databáze data.
7. Data jsou zpracována workprocesem a poslána uživateli.

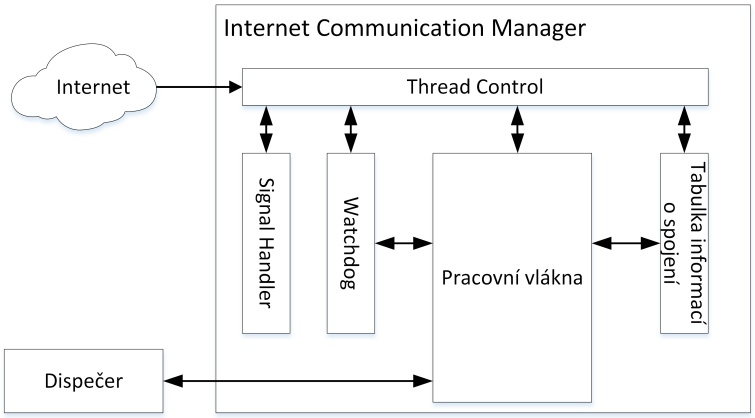


Obrázek 2.4: Požadavek provedený ze SAP GUI

Pro požadavky z prohlížeče je tok dat lehce rozdílný. SAP NetWeaver aplikační server ABAP může přijímat přicházející HTTP či HTTPS požadavky a posílat požadovaná data. Zároveň může požadovat data z jiných webových serverů. Při požadavcích z webu prochází veškerá komunikace přes ICM *Internet Communication Manager*. Požadavky z prohlížeče jsou předávány ICM a ten rozhodne, zda mají být zpracovány na ABAP nebo Java engine [23]. Struktura ICM, znázorněna na obrázku 2.5, zahrnuje:

- **Thread control** přijímající TCP/IP požadavky a vytvářející pracovní vlákna, inicializující informace o spojení.
- **Pracovní vlákna** zpracovávající požadavky. Existuje několik typů vláken:
  - logovací, zaznamenávající HTTP požadavky,
  - ověřovací, vyvolávající kontrolu oprávnění,

  - pro správu cache, využívané pro čtení a zapisování do ICM cache,
  - pro přesměrování, přeposílající HTTP(s) požadavky na jiný server,
  - pro ABAP operace, přeposílající požadavky na ABAP dispečer,
  - pro Java operace, přeposílající požadavky na Java dispečer.
- **Watchodog**, který čeká na odpověď po timeoutu pracovního procesu. Po získání odpovědi informuje Thread control, který znovu volá pracovní vlákno.
- **Signal handler** zpracovávající signály od dispečera.
- **Tabulku informací** o spojení.



Obrázek 2.5: Internet Communication Manager

2.6 Balík aplikací SAP Business Suite

Sada Business Suite představuje řešení pro velké podniky. Nabízí podporu důležitých procesů v daném podniku. Jedná se o aktuálně nejrozšířenější produkt SAP a zahrnuje komponenty popsané níže. Zákazník se může rozhodnout, zda zakoupí celou sadu nebo pouze zvolené komponenty. Přehled komponent byl zpracován na základě informací z oficiálních webových stránek společnosti SAP [32].

2.6.1 SAP Enterprise Resource Planning *ERP*

Komponenta SAP ERP integrující a automatizujicí mnoho podnikových procesů je jádrem balíku Business Suite a dělí se na:

- **Finanční řízení** *SAP ERP Financials* obsahující moduly finančního účetnictví, správy rizik, controlling, nemovitosti, majetek a další. Umožňuje řízení, napomáhá řízení rizik, nabízí větší transparentnost v oblasti finančních operací a zjednodušuje další složité procesy týkající se fakturace a zpracování plateb.
- **Provozní operace** *SAP ERP Operations*, který obsahuje moduly logistiky, vývoj a výrobu produktu, odbyt a služby.

- **Řízení lidských zdrojů** *SAP ERP Human Capital Management* se člení na několik oblastí, jako jsou řízení personálního procesu, nasazení personálu, poskytování služeb koncovým uživatelům, řízení kvalifikovaných pracovníků a analýzy personálu. Prostřednictvím SAP Employee Self-Service portálu mohou zaměstnanci provádět nejrůznější administrativní úkony, jako jsou například plánování služebních cest či údržbu osobních dat.
- **Koncernové služby** *SAP ERP Corporate Services* pomáhá podnikům zjednodušit interní procesy. Moduly koncernových služeb jsou služby globálního obchodování, správa a údržba nemovitostí, správa podnikového majetku a management jakosti.

2.6.2 SAP Customer Relationship Management *CRM*

Jedná se o souhrn podnikových funkcí pro řízení vztahů se zákazníky a podporu klíčových obchodních procesů podniku. Řízení vztahů se zákazníky umožňuje shromažďovat, zpracovávat a využívat informace týkající se zákazníků. Pomáhá snížit náklady a zvýšit schopnost rozhodování a dosáhnout konkurenční výhody. Mezi klíčové funkce patří:

- **marketing** podporující řízení marketingových zdrojů a kampaní,
- **prodej** zahrnující funkce pro plánování a vytváření prognóz prodeje, správu oblastí prodeje,
- **servis** zajišťující efektivnější řízení objednávek na služby, smluv, reklamací a oprav,
- **webový kanál** vedoucí ke zvýšení prodeje a snížení nákladů díky efektivnímu propojení podniku se zákazníky,
- **řízení komunikačního centra** podporující telemarketing, zákaznický servis a podobně,
- **řízení partnerských kanálů** zlepšující procesy pro hledání partnerů a komunikaci s nimi,
- **řízení obchodní komunikace**,
- **řízení nabídek v reálném čase**.

2.6.3 SAP Product Lifecycle Management *PLM*

Pomáhá řešit problematiku řízení životního cyklu produktů. Je základem pro proces vývoje nových produktů a jejich uvedení na trh. PLM umožňuje seskupení partnerů, dodavatelů, externích poskytovatelů služeb a zákazníků pro vývoj lepších produktů. Zahrnuje technické, výrobní i marketingové údaje o daném produktu.

2.6.4 SAP Supply Chain Management *SCM*

Podniky tuto komponentu využívají k modelování dodavatelského řetězce podniku, který se skládá z nákupu, výroby a distribuce. Díky SAP SCM jsou podniky schopny flexibilně reagovat na měnící se poptávku a nabídku, mohou přizpůsobovat své procesy měnícímu se konkurenčnímu prostředí.

2.6.5 SAP Supplier Relationship Management *SRM*

Nabízí metody pro řízení a zefektivnění obchodních procesů mezi podnikem klíčovými dodavateli. Díky SAP SRM lze předpovídat nákupní chování či spolupracovat s partnery v reálním čase. To umožňuje vytvářet dlouhodobé vztahy se všemi osvědčenými partnery.

2.7 Řešení pro malé a střední podniky

Vedle SAP Business Suite společnost dále vyvíjí a dodává tři různá řešení pro malé a středně velké podniky. Tato řešení vychází ze SAP Business Suite. Jsou však přizpůsobená procesům malých a středně velkých podniků. Jsou cenově dostupnější a snadněji implementovatelná [3].

SAP Business One je navržen pro podniky s méně než 100 zaměstnanci v maximálně pěti pobočkách. Podporuje klíčové podnikové procesy, jako jsou finanční řízení, řízení skladu, nákup, řízení zásob, výrobu, bankovnictví a CRM. Nabízí téměř okamžitý přístup ke všem podnikovým informacím v jednom sytému. Výhodou tohoto řešení je krátká doba nasazení [32].

SAP BusinessByDesign je řešení pro malé a středně velké podniky. Řešení vychází z předpokladu, že bude poskytováno způsobem SaaS *Software as a Service*. SAP Business ByDesign je řešení pro podniky do 500 zaměstnanců [32].

SAP Business All-In-One je navrženo pro střední podniky do 2500 zaměstnanců. Jde o úplné podnikové řešení vycházející z ERP, jeho součástí je vlastní CRM řešení [32].

2.8 Práce se systémem

Po přihlášení uživatel systému SAP zadá konkrétní transakční kód do SAP menu. Systém otevře dialogové okno s výběrovou obrazovkou, kde uživatel specifikuje parametry pro běh konkrétního programu, po zadání všech povinných parametrů může být program spuštěn.

Příkladem je transakce `su01` sloužící pro vytvoření nového uživatele systému. Uživatel zadá do SAP menu transakční kód `su01` (obrázek B.1), zobrazí obrazovku, kde vybere název uživatele a klikne na tlačítko vytvořit, systém zkontroluje zda uživatel se stejným jménem již v systému neexistuje (obrázek B.2) a zobrazí se obrazovka s dalšími selekčními parametry. Pokud je vše vyplněno správně po kliknutí na tlačítko uložit je vytvořen nový uživatel, v případě chybných vstupů se zobrazí chybová hláška ve spodní části obrazovky (obrázek B.3). Stejná akce může být provedena přes Web Dynpro aplikaci což je webový front-end SAP systému [26].

Kapitola 3

Hodnocení bezpečnosti informačních systémů

Z hlediska bezpečnosti informačního systému je nejdůležitějším úkolem zajistit bezpečnost informací vytvářených, zpracovávaných nebo ukládaných v daném informačním systému [2]. Bezpečností informací rozumíme dle ISO/IEC 27001:2005 [13] zajištění základních bezpečnostních cílů - důvěrnosti, integrity a dostupnosti informací.

Pro oblast bezpečnosti informačních systémů jsou důležité následující pojmy definované normou ISO/IEC 27001:2005 [13] využívané dále v této práci:

- **Aktivum *asset*** je cokoliv, co má pro organizaci hodnotu.
- **Integrita *integrity*** je zajištění správnosti a úplnosti informací.
- **Důvěrnost *confidentiality*** znamená zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
- **Dostupnost *availability*** je zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
- **Nepopiratelnost *non-repudiation*** znamená zajištění, že subjekt, který inicioval nějakou operaci, nebude moci tuto skutečnost popřít.
- **Riziko *risk*** je kombinace pravděpodobnosti, že dojde k nechtěné události a následků, které by z takové události mohly vzniknout.
- **Hrozba *threat*** je potenciální příčina nechtěného incidentu, která může vyústit v poškození systému nebo organizace.
- **Zranitelnost *vulnerability*** je slabina aktiva nebo skupiny aktiv, která může být využita jednou nebo více hrozbami.
- **Politika *policy*** je celkový záměr a směr formálně vyjádřený vedením organizace.
- **Opatření *control*** je prostředek řízení rizik zahrnující politiky, směrnice, metodické pokyny, praktiky nebo organizační struktury, které mohou být povahy administrativní, technické řídící nebo legislativní.

- **Bezpečnostní událost *information security event*** je identifikovaný stav systému, služby nebo sítě, ukazující na možné porušení bezpečnostní politiky, nebo selhání bezpečnostního opatření. Může se jednat o jinou předtím nenastalou situaci, která može být důležitá z pohledu bezpečnosti informací.
- **Bezpečnostní incident *information security incident*** je jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací.
- **Akceptace rizika *risk acceptance*** je rozhodnutí příjmout riziko.
- **Zbytkové riziko *residual risk*** je riziko, které zůstane po implementaci bezpečnostních opatření.
- **Analýza rizik *risk analysis*** je systematické používání informací k odhadu rizika a k určení jeho zdrojů.
- **Hodnocení rizik *risk assessment*** je celkový proces analýzy vyhodnocení rizik.
- **Vyhodnocení rizik *risk evaluation*** je proces porovnávání odhadnutého rizika vůči daným kritériím pro určení jeho významu.

Bezpečnost informačního systému minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí. Bezpečnosti informací můžeme dosáhnout implementací soustavy opatření, která mohou existovat ve formě pravidel, postupů, procedur, organizační struktury a programových či hardwarových funkcí. Tato opatření musí být ustavena, zavedena, provozována, monitorována a přezkoumávána, aby bylo dosaženo specifických bezpečnostních cílů organizace [14]. Pro zabezpečení informačního systému je dle [10] třeba zajistit:

- **Komunikační bezpečnost** týkající se působení hrozeb na aktiva v době jejich přenosu. Zabývá se ochranou dat proti modifikaci při přenosu, ochranou proti škodlivému kódu, ochranou před neoprávněným průnikem z internetu a ochranou proti nežádoucímu síťovému provozu.
- **Fyzickou bezpečnost** zahrnující ochranu informačního systému a jeho částí proti neoprávněnému vniknutí osob, ochranu proti přírodním živlům. Definuje způsoby zničení již nepotřebných důvěrných informací uložených na záznamových médiích. Fyzická aktiva musí být chráněna před neautorizovaným přístupem a enviromentálními vlivy.
- **Personální bezpečnost** zabývající se eliminací hrozeb způsobených lidským faktorem. Úkolem je definovat pravomoci a zodpovědnosti jednotlivých zaměstnanců organizace.
- **Logickou bezpečnost** týkající se působení hrozeb na aktiva nezbytná pro fungování informačního systému z hlediska řízení přístupu k informacím. Zabývá se tím, aby byla zabezpečena kontrola přístupu, identifikace a autentizace uživatelů, rozdělení práv uživatelům, sledování a záznam činností v systému.
- **Počítačovou bezpečnost** zahrnující působení hrozeb na fyzická aktiva potřebná pro zpracování, ukládání a přenos informací. Typickou hrozbou v této kategorii je selhání pevného disku. Základním ochranným opatřením proti zničení nebo znehodnocení dat je systematické zálohování.

3.1 Analýza rizik

Analýza rizik je základní předpoklad pro vytvoření efektivního systému ochrany informačních systémů. V kontextu bezpečnosti informačních systémů analýza rizik zahrnuje analýzu aktiv, analýzu hrozeb a analýzu zranitelností a ochranných opatření. Způsob dosažení bezpečnosti a bezpečnostní vlastnosti určuje bezpečnostní politika, což je soubor norem, pravidel a praktik, definující způsob správy, ochrany a distribuce citlivých dat a jiných aktiv v rámci činnosti informačního systému. Obecně tedy bezpečnostní politika vymezuje co je třeba chránit, proti jakým hrozbám a jak to chránit [10].

3.1.1 Analýza aktiv

V rámci analýzy aktiv musíme identifikovat kritická aktiva a určit jejich hodnotu. Sestavujeme inventářní seznam aktiv a subaktiv s jejich relativní hodnotou a důležitostí, na základě kterých je určena úroveň ochrany. Z hlediska podnikového informačního systému aktivy chápeme data a programy v systému.

3.1.2 Analýza hrozeb

Z hlediska analýzy hrozeb se soustředíme na jednotlivé hrozby působící na aktiva a přiřazujeme většinou číselnou hodnotu ke každé identifikované hrozbě. Kritérii k ohodnocení mohou být otázky [20]:

- Existuje zdroj hrozby?
- Existuje případ z minulosti?
- Existuje motivace, záměr či příčina hrozby?
- Které základní atributy informací jsou ohrožené?

Informační systémy jsou vystavovány hrozbám z nejrůznějších zdrojů. Příkladem výstupu ohodnocení hrozeb dle otázek výše je tabulka 3.1. Hrozby využívají zranitelných míst informačních systémů k útoku na hardware, software nebo data systému. Lze je dle [4] rozdělit do čtyř generických tříd: neautorizovaný přístup k informacím *disclosure*, podvržení dat *deception*, narušení operace *disruption*, neautorizované využití částí systému *usurpation*. Dále můžeme hrozby kategorizovat z hlediska jednotlivých částí informační bezpečnosti - logické bezpečnosti, počítačové bezpečnosti, komunikační bezpečnosti, personální bezpečnosti a fyzické bezpečnosti [20].

Hrozba	Existence zdroje hrozby	Existence případů v minulosti	Existence motivace záměru, příčiny	Integrita	Dostupnost	Důvěrnost	Hodnocení hrozby
1	X	X	X	X	X	X	5
2	X	X		X	X		2
3							0

Tabulka 3.1: Příklad tabulky pro ohodnocení hrozeb, zdroj [20].

3.1.3 Analýza zranitelností a ochranných opatření

Při analýze zranitelností a ochranných opatření zkoumáme slabá místa vznikající chybami při analýze, návrhu či implementaci a definujeme ochranná opatření. Cílem organizací je, aby byla přijata opatření snižující riziko minimálně na úroveň akceptovatelného rizika. Navrhovaná ochranná opatření vyplývají z bezpečnostních požadavků. Jeden ze způsobů hodnocení zranitelností nabízí standard Common Vulnerability Scoring System *CVSS* blíže popsaný v kapitole 3.3.3.

Výsledným krokem analýzy rizik je zjištění hodnoty rizika vyjadřujícího stupeň hrozby pro dané aktivum. Rizika můžeme hodnotit kvalitativně nebo kvantitativně. Kvantitativní hodnocení vyjadřuje pravděpodobnost výskytu bezpečnostního incidentu P a číselné vyjádření škody vzniklé tímto incidentem C, vypočte se jako $R = P * C$ [9].

Kvalitativně se riziko ohodnocuje pomocí expertního hodnocení vyplývajícího z jednotlivých faktorů. Pro kvalitativní ohodnocení existuje několik standardních metodik, například *CRAMM*, *COBIT* či *CORAS* [20].

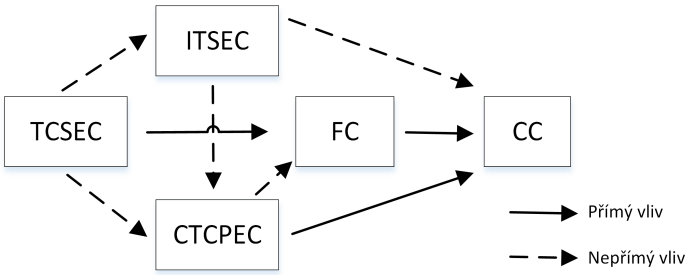
3.2 Standardy a metody pro ohodnocení stavu bezpečnosti informačních systému

Prvním široce používaným standardem pro zhodnocení bezpečnostního stavu systému byla Kritéria hodnocení důvěryhodných výpočetních systémů *TCSEC*[1] označována kvůli barvě obalu často jako Oranžová kniha. Byla vytvořena Národním střediskem počítačové bezpečnosti USA v roce 1983 a byla vydána roku 1985 jako norma Ministerstva obrany USA. Od té doby tvoří základ pro soubor norem a doporučení označovány jako Duhová série *Rainbow Series*. Série zahrnuje desítky publikací a stanovuje základní požadavky pro hodnocení efektivnosti počítačové bezpečnosti systému, počítačových sítí, systémů řízení báze dat a podobně. Oranžová kniha sloužila k posuzování bezpečnosti systémů ve státní správě USA, ale pronikla i do komerční sféry [7].

Další standardy berou *TCSEC* jako základ, ze kterého vycházejí, vylepšují jej či doplňují. V Evropě vznikla v roce 1990 norma nazývaná Kritéria hodnocení bezpečnosti informačních systémů *ITSEC*[2] převzata celou Evropskou unií. V Kanadě vznikla Kanadská kritéria hodnocení bezpečnosti počítačových produktů. Nedostatky *TCSEC* vedly k přepracování americké normy. V roce 1992 byla vydána Federální kritéria pro bezpečnost informačních technologií *Federal Criteria FC*) organizacemi *National Institute of Standards and Technology NIST* a *National Security Agency NSA* [8]. V polovině devadesátých let vznikla Všeobecná kritéria *CC*[3] akceptována jako standard mezinárodně. Vývoj a vztahy kritérií jsou ilustrovány na obrázku 3.1.

Pro hodnocení bezpečnosti informací a informačních systémů jsou dnes hojně využívány standardy z rodiny ISO/IEC 27000 a dále pak i projekty ze skupiny *Open Web Application Security Project OWASP*, zejména projekt *Top Ten* či začínající projekt *OWASP Enterprise Security Project* soustředící se na bezpečnost podnikových systémů.

[1] Zkratka TCSEC pochází z anglického Trusted Computer System Evaluation Criteria.
[2] Zkratka ITSEC vznikla z anglického Information Security Evaluation Criteria.
[3] Zkratka CC pochází z anglického Common Criteria, ISO/IEC 15 408 1-3.



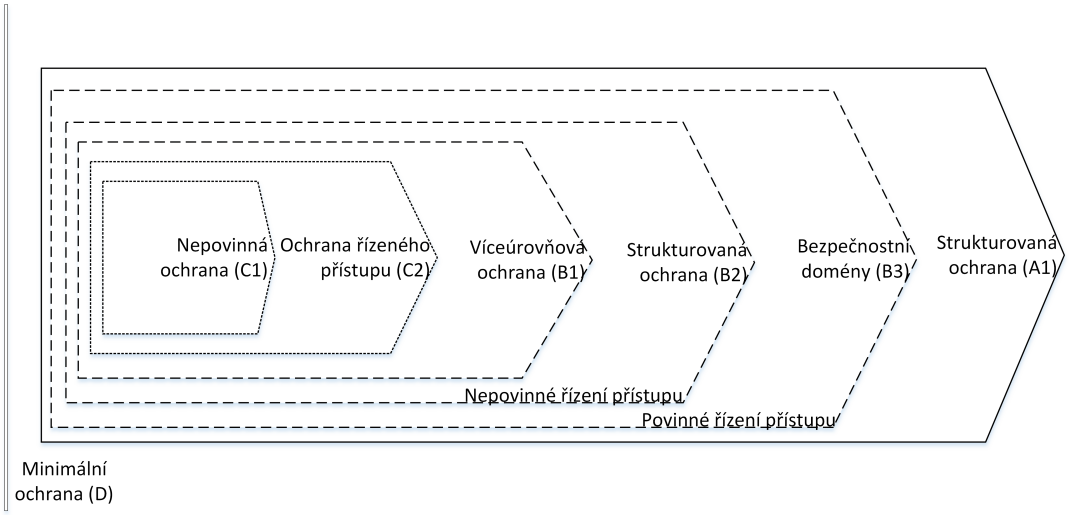
Obrázek 3.1: Vývoj a vztahy kritérií hodnocení bezpečnosti, zdroj: [8]

3.2.1 Kritéria hodnocení důvěryhodných výpočetních systémů *TCSEC*

Míra bezpečnosti dle *Trusted Computer Security Evaluation Criteria TCSEC* je hodnocena dle míry splnění požadavků, které jsou rozděleny do čtyř částí [8]:

- politika *policy* kladoucí důraz na způsoby řízení přístupu k datům a označování stupně jejich utajení,
- odpovědnosti *accountability* soustředící se na zjištění identity uživatele a sledování jeho činností v informačním systému.
- zaručitelnost *assuarance* stanovující potřebu nezávislého hodnocení a nepřetržité funkčnosti bezpečnostních mechanismů,
- dokumentace *documentation*

Systémy jsou na základě *TCSEC* děleny do sedmi hierarchických tříd, popsaných níže. Pro informační systém vyšší třídy se předpokládá vždy splnění všech požadavků ze třídy nižší. TCSEC uplatňuje principy řízení přístupu k aktivům – *Discretionary Access Control DAC* a *Mandatory Access Control MAC*, hierarchie tříd je ilustrována na obrázku 3.2.



Obrázek 3.2: Hierarchie tříd TCSEC, zdroj: [9]

Požadavky jednotlivých úrovní [7]:

- **D** – minimální ochrana *Minimal Protection* systém nemusí splnit žádná kritéria, zabezpečení je minimální nebo vůbec žádné.
- **C1** – ochrana výběrovým přístupem *Discretionary protection* definuje minimální funkční požadavky, je zde povinná pouze identifikace a autentizace uživatelů pracujících se systémem. Systém jim musí přidělovat prostředky dle pravidel nepovinného řízení přístupu (DAC). Požadavky na zabezpečení jsou také minimální.
- **C2** - ochrana řízeným přístupem *Controlled Access Protection* definuje jemnější řízení přístupu, a řeší opětovné použití objektů (uživatel nedostane spolu s přidělenou pamětí zbytky dat zanechané v ní jiným uživatelem). Jednotlivé procesy od sebe musí být bezpečně odděleny. Jde o nejvíce používanou třídu pro komerční produkty.
- **B1** - ochrana bezpečnosti návěštím *Labeled Security protection* pro tuto třídu je povinné řízení přístupu pro některé objekty, požadavky na bezpečnostní testy jsou přísnější. Je vystavěna na neformálním modelu bezpečnostní politiky.
- **B2** - strukturovaná ochrana *Structured Protections* požaduje existenci formálního modelu řízení bezpečnosti. Je přijatelná pro některé vládní aplikace. povinné řízení přístupu je vyžadováno pro všechny objekty. Systémy musí nabízet důvěryhodnou cestu pro přihlášení. Bezpečnostní požadavky zahrnují analýzu skrytých kanálů, přísnější dokumentaci a správu konfigurace.
- **B3** - bezpečnostní domény *Security Domains* zvyšuje požadavky na důvěryhodnost cesty, definuje omezení při vytváření kódu jako je modularita, jednoduchost, vrstvy či skrývání dat. Zahrnuje veškeré bezpečnostní požadavky z B2 a dále zpřísňuje požadavky na testování a design dokumentaci.
- **A1** - verifikovaná ochrana *Verified protection* vyžaduje významné použití formálních metod pro analýzu, specifikaci návrhu a verifikaci. U všech částí systému musí být proveden formální matematický důkaz. Požaduje důvěryhodnou distribuci.

TCSEC klade důraz na důvěrnost, směšuje však v jednom dokumentu různé úrovně abstrakce. Nedefinuje jak přistupovat k integritě dat. Kombinuje funkčnost a zaručitelnost do jedné lineární stupnice. Z dnešního pohledu je *TCSEC* již zastaralá norma s nízkou schopností přizpůsobovat se novým podmínkám. Zformulovala však některá zásadní platná východiska.

3.2.2 Kritéria hodnocení bezpečnosti informačních systémů *ITSEC*

Information Technology Security Evaluation Criteria ITSEC byla vytvořena z národních kritérií Velké Británie, Německa, Francie a Holandska. Jako doporučení byla schválena roku 1995. Roku 1993 byl vydán doplňující dokument, manuál *Information Technology Security Evaluation Manual ITSEM*, což je metodika pro hodnocení bezpečnosti informačních systémů [10]. Rozděluje požadavky do dvou nezávislých částí, kterými jsou míra zaručitelnosti a funkčnost.

ITSEC přichází s konceptem *Target of Evaluation TOE*, což je předmět hodnocení odkazující na hodnocený produkt či systém.

Kritéria *ITSEC* definují sedm tříd míry zaručitelnosti bezpečnosti IT reprezentujících vzrůstající úroveň důvěry. Třídy míry zaručitelnosti kladou požadavky na proces vývoje systému, prostředí vývoje systému, provozní dokumentaci systému a provozní prostředí

systému [8]. *ITSEC* jsou mnohem obecnější než *TCSEC* a pokrývají částečně požadavky na integritu a dostupnost informací.

Požadavky *ITSEC* na míru zaručitelnosti bezpečnosti:

- **Třída E0** do této třídy spadají systémy nesplňující požadavky *ITSEC*, hodnocení nelze provést.
- **Třída E1** požaduje neformální zadání modelu bezpečnosti a popis návrhu architektury. Testy dokazují, že systém splňuje bezpečnostní cíl.
- **Třída E2** požaduje neformální popis detailního návrhu hodnoceného předmětu a dokumentované testování.
- **Třída E3** hodnotí zdrojové kódy bezpečnostních funkcí. Požaduje jejich detailní návrh.
- **Třída E4** formální model bezpečnostní politiky a poloformální popis architektury a návrhu hodnoceného předmětu .
- **Třída E5** požaduje úzkou vazbu mezi detailním návrhem bezpečnosti a zdrojovým kódem a provedení analýzy zranitelnosti na úrovni zdrojových textů.
- **Třída E6** požaduje formální specifikaci návrhu bezpečnostní architektury hodnoceného předmětu, který musí být konzistentní s formálním modelem bezpečnostní politiky.

Třídy bezpečnostní funkčnosti *ITSEC* definují zásady. Třídy F-C1, F-C2, F-B1, F-B2, F-B3 odpovídají příslušným třídám z *TCSEC*. Dalších 5 tříd nemá přesně definovanou hierarchickou strukturu, definují zvýšené požadavky na některou specifickou oblast [8]:

- **F-IN** – zvýšené požadavky na integritu,
- **F-AV** – zvýšené požadavky na dostupnost dat,
- **F-DI** – integrita dat při přenosu,
- **F-DC** – zajištění důvěrnosti při přenosu,
- **F-DX** – důvěrnost a integrita při přenosu.

ITSEC přinesla vyjádření výsledku hodnocení ve více rozměrech.

3.2.3 Všeobecná kritéria *CC*

Common Criteria CC je norma pro hodnocení bezpečnosti uznána mezinárodně. První verze CC vznikla v roku 1996 [10]. Roku 1999 byla schválena další verze jako mezinárodní norma ISO/IEC 15408. Nejnovější verze 3.1 byla převedena do ISO/IEC 15408 roku 2008. Celou normu tvoří tři části:

- ISO/IEC 15408-1 definuje globální koncepci a principy hodnocení bezpečnosti informačních technologií. Je zde popsána konstrukce základních používaných struktur a vysvětlena používaná terminologie.
- ISO/IEC 15408-2 obsahuje katalog funkčních komponent a popis jednotlivých funkčních tříd.

- ISO/IEC 15408-3 definuje požadavky na bezpečnostní záruky. Obsahuje úrovně hodnocení záruky *Evaluation Assurance Levels EAL*.

Common Criteria umožňují porovnávat výsledky nezávisle prováděných hodnocení bezpečnosti, stanovují obecně platné požadavky na bezpečnostní funkce a míry zaručitelnosti bezpečnosti udělované bezpečnostním funkcím. *CC* definují hierarchicky uspořádané úrovně zaručitelnosti bezpečnosti. Výsledkem hodnocení je výrok, říkající kterou úroveň zaručitelnosti bezpečnosti daný produkt nebo systém splňuje [10].

Bezpečnostní funkce jsou rozděleny do tříd, každá třída se skládá z rodin a rodina se skládá z komponent, které plní požadavky rodiny s různou mírou ochrany. Katalog obsahuje tyto třídy [16]:

- Třída FAU - bezpečnostní audit,
- Třída FCO - komunikace,
- Třída FCS – kryptografická podpora,
- Třída FDP – ochrana uživatelských dat,
- Třída FIA – identifikace a autentizace,
- Třída FMT – správa bezpečnosti,
- Třída FPR – soukromí,
- Třída FPT – ochrana bezpečnostní funkcionality,
- Třída FRU – využití zdrojů,
- Třída FTA - přístup,
- Třída FTP – důvěryhodné cesty/kanály.

Kritéria jsou orientována na ochranu informací před neautorizovanou modifikací, ztrátou či neautorizovaným přístupem. Zaručitelností rozumíme důvody a příčiny opravňující důvěřovat, že systém splňuje své bezpečnostní plány. Zaručitelnost bezpečnosti systému se odvozuje z výsledků získaných hodnocením systému. Mezi typické hodnotící techniky můžeme zahrnout analýzu a kontrolu procesu, ověřování důkazů, analýzu dokumentů s návody, nezávislé testování funkcí či analýzu zranitelných míst.

3.2.4 Řada norem ISO/IEC 27000

ISO/IEC 27000 je mezinárodně platný soubor norem zabývajících se informační bezpečností, jejichž úkolem je sjednotit doporučení, požadavky a návody vyskytující se v různých normách. Roku 2005 byla zveřejněna první norma ISO/IEC 27001 vycházející z britského předchůdce BS 7799-2. Soubor zahrnuje více než třicet norem, jejichž detaily jsou popsány v [12], pro tuto práci jsou důležité následující normy:

- ISO/IEC 27000 slouží jako slovník a definice pravidel pro všechny ostatní normy ze série.
- ISO/IEC 27001 je základní normou používanou při certifikacích obsahující požadavky na systém řízení bezpečnosti informací ISMS.

- ISO/IEC 27002 je sbírkou nejlepších bezpečnostních praktik sloužící jako kontrolní seznam správnosti bezpečnosti informací. Jedenáct oddílů definuje množství doporučených základních bezpečnostních opatření. Cílem není implementovat vše, co norma popisuje ale naplnit všechny aplikovatelné cíle.
- ISO/IEC 27004 poskytující doporučení zaměřená na vývoj a používání metrik a měření za účelem hodnocení účinnosti zavedeného systému řízení bezpečnosti informací a účinnosti opatření nebo skupin opatření z ISO/IEC 27001.

3.2.5 Open Web Application Security Project

Open Web Application Security Project OWASP [1] je komunita zabývající se bezpečností webových aplikací. Projekty *OWASP* můžeme rozdělit do dvou kategorií na vývojářské a dokumentační projekty. Do vývojářských projektů se řadí například aplikace pro testování zranitelností webových aplikací, uměle děravá webová aplikace sloužící jako simulátor bezpečnostních chyb a další. Příklady dokumentačních projektů jsou *Top Ten*, což je dokument zaměřující se na nejkritičtější problémy webových aplikací, projekt *Metrics* definující metriky zabezpečení aplikací či projekt *Enterprise Security Project* definující problémy pro podnikové aplikace.

3.3 Bezpečnostní metriky

Informace jsou pro podniky důležitá aktiva a jakékoliv narušení, či zničení jsou pro podnik kritické. Spousta společností je schopna na vylepšování bezpečnosti utratit mnoho. Bezpečnost nemá žádné přirozené hranice, některé společnosti do „vylepšování“ bezpečnostních opatření investují zbytečně mnoho či investují na špatných místech, proto se zavádějí bezpečnostní metriky pomáhající kvalitativně, statisticky či matematickou analýzou měřit efektivitu bezpečnostních opatření a kvantifikovat data [18]. Využití metrik spadá do několika širokých tříd [17]:

- Strategická podpora – posouzení vlastností zabezpečení může být využito na podporu různých druhů rozhodování, jako programového plánování či přidělování zdrojů.
- Zajištění kvality – bezpečnostní metriky mohou být využity v životním cyklu vývoje software pro eliminaci zranitelností objevujících se především během vytváření kódu.
- Přehled za provozu – monitorování a reportování stavu zabezpečení je prováděno za účelem ověření souladu s požadavky na bezpečnost (s bezpečnostní politikou, procedurami, regulemi).

Metriky umožňují lépe porozumět bezpečnostním rizikům, odhalit včas vznikající problémy či porozumět slabým místům v bezpečnostní infrastruktuře. Obecně by měly určit, do jaké míry organizace naplňuje své bezpečnostní cíle. Správná metrika by měla obecně splňovat následující kritéria [18]:

1. Metrika je měřitelná dle objektivních kritérií, různí lidé by měli být schopni aplikovat metodu na stejná data se stejným výsledkem.
2. Dosažení výsledku je jednoduché, ideálně automatizované.
3. Výsledek je vyjádřený číslem nebo procenty.

4. Výsledek má jednotku.

5. Metrika je kontextově specifická.

3.3.1 Dělení metrik

Různé standardy a metodiky definují rozdělení metrik různě. Například dle NIST [17] můžeme metriky rozdělit do tří kategorií vycházejících z úrovní zralosti bezpečnostního programu organizace *Capability Maturity Model* na:

- **Implementační metriky**, odpovídající fázi zavádění systémů řízení IT bezpečnosti a opatření měřící procentuální pokrytí stanic, systémů a podobně konkrétními kontrolami.
- **Výkonnostní metriky** hodnotí efektivitu bezpečnostního systému.
- **Dopadové metriky** se uplatňují tehdy, kdy jsou bezpečnostní procesy integrovány. Využívají se pro analýzu dopadů.

Bezpečnostní metriky můžeme dále dle [11] rozdělit na tvrdé metriky a měkké metriky. **Tvrdé metriky**, neboli kvantitativní, usilují o poskytnutí kvantitativního objektivního základu pro zajištění bezpečnosti a jsou většinou snadno měřitelné. **Měkké metriky**, neboli kvalitativní, jsou ukazatele, které nejsou objektivně měřitelné, vstupuje do nich subjektivní hodnocení. Získání těchto ukazatelů bývá složitější.

Metriky pro diagnostiku bezpečnostních problémů informačních systémů lze dle [18] rozdělit do čtyř kategorií:

- **Metriky perimetru** zkoumající hranice informačního systému, které oddělují síť organizace od sítí ostatních subjektů. Zjišťujeme kdo má přistup má přístup k systému a za jakých podmínek. Typickou aktivitou je zkoumání efektivity antivirového softwaru, antispamových systémů, firewallů a systémů pro detekci průniků *IDS* v sítě uvnitř bezpečnostního perimetru.
- **Metriky pokrytí opatření**, kdy pokrytím rozumíme do jaké míry byla aplikována bezpečnostní opatření na cílové prostředky, které by z toho mohly mít prospěch. Pro tuto skupinu typicky zkoumáme procentuální míru pokrytí stanic a serverů antivirovým a antispywarovým softwarem, identifikujeme a měříme počet záplat systému aplikovaných v dané periodě, počet neaplikovaných záplat systému pro jednotlivé uzly, kontrolujeme zda pracovní stanice a servery jsou konfigurovány tak, aby dovolovaly dosažení bezpečnostních cílů organizace.
- **Metriky dostupnosti a spolehlivosti** - systémy na kterých stojí zisk společnosti musí běžet bez výpadků kvůli neočekávaným bezpečnostním incidentům. Zkoumáme, co se stane při výpadku části systému. Patří sem metriky jako *Mean Time To Recover MTTR*.
- **Metriky pro aplikační rizika** jsou metriky zkoumající kvalitu a komplexitu kódu a s nimi spojené zranitelnosti na úrovni aplikací, jejichž využití může ohrozit integritu, dostupnost či důvěrnost. Typickými útoky, které využívají aplikačních zranitelností jsou SQL injection, command injection, cross-site scripting a další.

3.3.2 Měření dle normy ISO/IEC 27004

Norma ISO/IEC 27004:2016 [15] poskytuje doporučení pro vývoj a použití metrik a měření za účelem hodnocení bezpečnostních opatření a účinnosti systému řízení bezpečnosti informací. Měření se dle ISO/IEC 27004 dělí na čtyři části:

- **Vývoj metrik a měření**, kdy je třeba specifikovat požadavky, prováděné kontroly a cíle měření. Spadají sem úkoly jako identifikace rozsahu měření, identifikace informační potřeby, identifikace objektu měření, volba a vývoj metriky či specifikace konceptu měření.
- **Provádění měření** zahrnující činnosti pro sběr, ukládání a ověřování dat.
- **Analýza dat a reporting**, kdy jsou sebraná data analyzována za účelem získání výsledků měření.
- **Vyhodnocení a zlepšování programu měření**.

3.3.3 Metriky pro ohodnocení zranitelností

Common Vulnerability Scoring System CVSS poskytuje framework pro zkoumání a charakteristiku dopadů zranitelností. Definuje jednotlivé metriky a dělí je do tří skupin: základní temporální a environmentální [5]. Základní metriky jsou pro hodnocení dle *CVSS* povinné a reprezentují základní charakteristiky konstantní v průběhu času a nezávislé na prostředí. Kombinují výpočet metriky zneužití *Exploitability metrics* odrážející složitost zneužití zranitelnosti a metriky dopadů *Impact metrics* reflektující přímé důsledky úspěšného zneužití zranitelnosti. Temporální a environmentální metriky doplňují a rozšiřují základní, jejich použití je však volitelné. Výsledkem je vždy číselné skóre od 0 do 10, rozdělené do pěti kategorií zobrazených v tabulce 3.2 a vektor hodnocení, což je textová reprezentace metrik použitých pro ohodnocení zranitelnosti. Příkladem vektoru hodnocení je řetězec CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:L, říkající, že pro hodnocení bylo použito *CVSS* verze 3.0 s hodnotami Attack Vector = Network, Attack Complexity = Low, Privileges Required = High, PUser Interaction = Required, Scope = Changed a Confidentiality, Integrity, Availability = Low.

skóre	závažnost
0	žádná
0.1 - 3.9	nízká
4.0 - 6.9 - 3.9	střední
7.0 - 8.9	vysoká
9.0 - 10.9	kritická

Tabulka 3.2: Kategorie závažností dle CVSS. Zdroj: [5]

Základní metriky zneužití

- **Vektor útoku** *Attack Vector* definuje odkud může být využita daná zranitelnost – z internetu, z lokální sítě či zda útočník musí mít fyzický přístup k danému systému. Může nabývat čtyř hodnot - *Network*, *Adjacent*, *Local*, *Physical*.

- **Komplexita útoku** *Attack Complexity* definuje podmínky, za kterých může být využito zranitelnosti, podmínky mohou vyžadovat více informací o cíli, například o různých konfiguračních nastaveních. Nabývá dvou hodnot - *Low* a *High*.
- **Požadovaná oprávnění** *Privileges Required* definují zda je třeba mít v systému účet k zneužití zranitelnosti. Může nabývat tří hodnot - *None*, *Low*, *High*.
- **Uživatelská interakce** *User Interaction* definuje zda může být zranitelnost zneužita bez součinnosti ze strany uživatele systému, například kliknutí na odkaz. Může nabývat hodnoty *None* a *Required*.
- **Rozsah** *Scope* definuje zda zneužití zranitelnosti postihuje i jiné komponenty. Základní skóre je vyšší v pokud je postižena i jiná komponenta. Nabývá hodnot *Unchanged* a *Changed*.

Základní metriky dopadu

Všechny tři metriky dopadu mohou nabývat tří hodnot - *High*, *Low* a *None*.

- **Dopad na důvěrnost** *Confidentiality Impact* je metrika definující do jaké míry mohou být zneužity důvěrné informace při využití zranitelnosti.
- **Dopad na dostupnost** *Availability Impact* popisuje do jaké míry budou znepřístupněná data či služby po využití zranitelnosti.
- **Dopad na integritu** *Integrity Impact* říká, do jaké míry dojde při využití zranitelnosti k znehodnocení dat.

Výpočet skóre

Celkové základní skóre využívá vypočteného subskóre zneužití 3.1 a subskóre dopadu, které se počítá rozdílně pro případ nezměněného rozsahu 3.3 a v případě změněného rozsahu 3.4. Základní skóre je poté vypočteno dle 3.5, pokud rozsah nabývá hodnoty Unchanged či 3.6 v opačném případě. Výpočty byly převzaty z [6].

$$ES = 8.22 \times AV \times AC \times PR \times UI \tag{3.1}$$

Kde:
ES ... Subskóre zneužití *Exploitability Subscore*
AV ... Vektor útoku *Attack Vector*
AC ... Komplexita útoku *Attack Complexity*
PR ... Požadovaná oprávnění *Privilege Required*
UI ... Uživatelská interakce *User Interaction*

$$ISC_{base} = 1 - [(1 - IC) \times (1 - II) \times (1 - IA)] \tag{3.2}$$

Kde:
IS_{base} ... Základ subskóre dopadu
IC ... Dopad na důvěrnost *Confidentiality Impact*
II ... Dopad na integritu *Integrity Impact*
IA ... Dopad na dostupnost *Availability Impact*

$$IS = 6.42 \times IS_{base} \tag{3.3}$$

$$IS = 7.52 \times (IS_{base} - 0.029) - 3.25 \times (IS_{base} - 0.02)^1 5 \tag{3.4}$$

Kde:
IS ... Subskóre dopadu *Impact Subscore*
IS_{base} ... Základ subskóre dopadu vypočtený dle 3.2

$$BS = RoundUp(Minimum[(IS + ES), 10]) \tag{3.5}$$

$$BS = RoundUp(Minimum[1.08 \times (IS + ES), 10]) \tag{3.6}$$

Kde:
BS ... Výsledné základní skóre
IS ... Subskóre dopadu *Impact Subscore*
ES ... Subskóre zneužití *Exploitability Subscore*

3.3.4 Vlastní metodika pro ohodnocení kritičnosti

Pro ohodnocení kritičnosti jednotlivých bezpečnostních požadavků byla vytvořena vlastní metodika. Bere v potaz dopad na jednotlivé bezpečnostní cíle a pravděpodobnost zneužití neaplikovaného bezpečnostního požadavku. Při jejím využití může auditor využít své expertní znalosti daného systému, znalost hodnoty daných aktiv a vlastní úsudek. Metodika definuje následující čtyři stupně kritičnosti:

Kritický *Critical* Jako kritický hodnotíme nález s přímým vážným dopadem na integritu, dostupnost či důvěrnost. Kritické problémy jsou typicky ty, které umožňují útočníkovi provádět kritické zásahy v systému. Zneužití zranitelností v této kategorii vede přímo k tomu, že není naplněn některý z bezpečnostních cílů. Tyto nálezy vyžadují okamžitou aplikaci bezpečnostních opatření.

Vysoký *High* Jako vysoce závažný nález hodnotíme ten, který má vysoký dopad na na bezpečnost systému. Zneužití zranitelností v této kategorii vede k částečnému narušení některého z bezpečnostních cílů. Bezpečnostní opatření je nutné aplikovat do jednoho týdne od nálezu.

Střední *Medium* Využití zranitelnosti se střední závažností k napadení umožňuje průnik do systému když jsou splněny určité doplňující se podmínky. Provedení napadení tedy vyžaduje vyšší úsilí a je méně pravděpodobné než zneužití zranitelností z předchozích kategorií. Nemá dopad na kritickou funkcionalitu systému. Tyto nálezy vyžadují aplikaci bezpečnostních opatření do měsíce od nálezu.

Nízký *Low* Nízkou závažností hodnotíme nálezy s akceptovatelným málo významným dopadem. Nejsou pro ně typicky vyžadována žádná speciální bezpečnostní opatření, je dobré pouze zvážit náklady na případné řešení. Nálezy této kategorie však většinou zůstávají v systému ve formě residuálních rizik.

Kapitola 4

Bezpečnostní analýza SAP platformy

Pro analýzu byla vybrána nejnovější verze platformy *SAP NetWeaver 7.5* s aplikačním serverem ABAP. Běží na ní v dnešní době nejrozšířenější produkt společnosti SAP ERP. Jednotlivé kategorie byly tvořeny na základě požadavků *OWASP Enterprise Application Security Project*, standardů z rodiny ISO/IEC 27000 a známých potenciálních zranitelností systému SAP popsaných ve vydaných *SAP Security Notes*. Z hlediska podnikový aplikací je dle *OWASP* [1] nutné se soustředit na bezpečnost:

- operačního systému,
- databáze,
- aplikační bezpečnost.

4.1 Bezpečnost operačního systému a databáze

Dle [34] a *Product Availability Matrix* [30] může *SAP NetWeaver ABAP 7.5* běžet na různých databázových strojích a operačních systémech. Jejich výčet spolu s požadavky na nejnižší podporované verze jsou uvedeny v tabulkách 4.1 a 4.2. Cílem práce není hodnotit bezpečnost databázové platformy ani operačních systémů, v tabulkách je tedy zároveň uvedeno, na základě jakých požadavků je možné je ohodnotit. Většinou se jedná o *CIS benchmarks*[1].

databáze	minimální verze	hodnocení
SAP MaxDB	7.9	
IBM DB2	10	CIS IBM DB2 10 Benchmark v1.1.0
MS SQL Server	2012	CIS Microsoft SQL Server 2012 Benchmark v1.3.0
Oracle	12	CIS Oracle Database 12c Benchmark v2.0.0
HANA DB	1.00 SP8	SAP HANA Security Checklists and Recommendations[31]

Tabulka 4.1: Podporované verze databází a jejich bezpečnostní ohodnocení

[1] Center for Internet Security je nezisková organizace posuzující bezpečnost. Slouží jako klíčový zdroj informací v oblasti počítačové bezpečnost. Publikuje takzvané benchmarks sloužící pro prověření bezpečnosti systémů. Jednotlivé benchmarks je možné získat z: https://www.cisecurity.org/cis-benchmarks.

systém	minimální verze	hodnocení
AIX	7.1	CIS IBM AIX 7.1 Benchmark v1.1.0
HP-UX	11.3	CIS HP-UX 11i Benchmark v1.5.0
SUSE Linux	11	CIS SUSE Linux Enterprise 11 Benchmark v2.0.0
Redhat Linux	6	CIS Red Hat Enterprise Linux 6 Benchmark v2.0.2
Oracle Solaris	10	CIS Oracle Solaris 10 Benchmark v5.2.0
Windows Server	2012	CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.1

Tabulka 4.2: Podporované verze operačních systémů a jejich bezpečnostní ohodnocení

4.1.1 Oracle databáze

Nejvyužívanější databází pro SAP řešení je databáze Oracle nabízející pro zákazníky SAP od verze 11 zajímavé zabezpečující mechanismy. SAP řešení samo o sobě nenabízí žádné zabezpečení komunikace mezi aplikačním serverem a databází.

Pokud chce uživatel číst a zapisovat data s využitím SAP rozhraní, je všechen přístup k datům řízen v rámci SAP systému pouze nastavením uživatelských rolí. Nicméně privilegovaní databázoví uživatelé mohou přímo přistupovat k databázi a obejít tak autorizace v rámci SAP systému. Tento problém neřeší ani šifrování databáze, neboť privilegovaný uživatel může vytvořit dotaz do databáze a databáze považuje dotaz za validní a vrátí výsledek v dešifrovaném stavu. K řešení tohoto problému slouží *Oracle Database Vault*, což je nástroj umožňující zavést systém pro přidělování autorizací na úrovni databáze. Administrátor má defaultně přidělena systémová privilegia a běžný uživatel může přistupovat přímo k objektům. V případě, že existuje důvod aby administrátor přistupoval k datům jsou mu přidělena práva explicitně [25].

Druhým zajímavým řešením z pohledu SAP zákazníků je *Oracle Advanced Security* nabízející šifrování databáze a šifrování přenosu mezi Oracle databázovým serverem a aplikačním serverem SAP. Podporuje zároveň i kontrolní součty pro zajištění integrity dat. Pro šifrování přenosu jsou využívány algoritmy AES256 či AES128, pro zajištění integrity dat jsou využívány algoritmy SHA1, SHA256, SHA384 či SHA512 [35]. Defaultně je šifrování komunikace mezi SAP aplikačním serverem a databází deaktivované. Je možné jej aktivovat přidáním konfiguračního souboru `SQLNET.ORA` na straně databázového serveru nebo SAP aplikačního serveru. Data v databázi je možné šifrovat buď po jednotlivých sloupcích či jako celé tabulky. Šifrování dat po sloupcích zabezpečuje pouze nejvíce citlivá data, tento přístup nabízí však rovnováhu mezi bezpečnostními požadavky a zatížením z hlediska výkonnosti [25].

4.2 Správa záplat a aktualizace aplikační platformy

Dle ISO/IEC 27002:2013 [14] mají být po zjištění potencionální technické zranitelnosti provedena nápravná opatření jako záplatování. Jestliže je dostupná záplata, mělo by být ohodnoceno riziko spojené s její instalací a porovnáno s rizikem plynoucím z neaplikování záplaty. Dříve než jsou opravy aplikovány do produkčního systému, je vhodné funkcionalitu otestovat a vyhodnotit na testovacím prostředí.

Aplikace bezpečnostních záplat je jedna z důležitých věcí udržujících bezpečnost SAP systému. Každé druhé úterý v měsíci SAP vydává novou sérii *SAP Security Notes* s detailním popisem zranitelností a stupněm jejich závažnosti dle CVSS[2]. Po zveřejnění *Security*

[2]SAP Security Notes jsou dostupné na: https://support.sap.com/securitynotes.

Notes se stávají zranitelnosti veřejně známé a pozdní implementace zvyšuje riziko jejich zneužití pro získání přístupu k citlivým datům a podobně, proto je nezbytné provádět pravidelné kontroly implementací bezpečnostních záplat. Je silně doporučováno bez prodlení aplikovat záplaty s prioritou 1 a 2, jedná se o záplaty pro kritické zranitelnosti většinou nalezené externí stranou. *Security Notes* s prioritou 3 a 4 doporučuje společnost SAP aplikovat nejdéle do třiceti dní od zveřejnění.

Pro implementaci *SAP Security Notes* slouží nástroj *SAP Solution Manager* kontrolující všechny chybějící bezpečnostní záplaty pro daný systém. Nástroj pro vyhodnocení relevantních *SAP Notes* bere v potaz aktuální softwarovou konfiguraci, instalované komponenty, nainstalovaný *Support Package* a implementované *SAP Notes* [37].

Vedle *SAP Solution Manager* je možné využít transakci `SPAM` přímo z tlustého klienta SAP GUI spouštějící nástroj *SAP Patch Manager*, který umožňuje stažení a aplikaci *Support Package*. Transakce `SNOTE` zase nabízí seznam všech *SAP Notes* pro konkrétní systém a možnost jejich implementace. Z hlediska Patch Managementu jsou pro SAP systémy důležité dále takzvané *Kernel Patches*, což jsou záplaty opravující vysoce kritické zranitelnosti týkající se dispečeru aplikačního serveru, Gatewaye či Message Serveru. Verzi posledního aplikovaného Kernel Patche je možné zjistit v systému v menu `System/Status/Kernel Info`, stažení a aplikace těchto záplat je prováděna opět pomocí *SAP Solution Manager*. Navržené kontroly týkající se správy záplat a aktualizací jsou uvedeny v dotazníku pod kategorií Správa záplat a aktualizací.

4.3 Řízení přístupu

Řízení přístupu k aktivům zahrnuje čtyři části:

- Identifikaci
- Autentizaci
- Autorizaci
- Logování

V rámci procesu řízení přístupu je kontrolováno kdo má přístup k jakým zdrojům. Řízení přístupu je fyzické, což zahrnuje například fyzické zabezpečení zařízení a podobně, a logické. Dále se budeme soustředit na logické řízení přístupu z hlediska informačního systému.

Prvním bodem řízení přístupu je identifikace, kdy uživatel zadává do systému své unikátní uživatelské jméno či identifikační číslo. Je důležité, aby měl každý uživatel systému svůj unikátní identifikátor a aby nedocházelo ke sdílení jednoho identifikátoru mezi více uživateli, jen tak mohou být všechny provedené akce v systému spojeny se specifickým uživatelem.

Dalším krokem je autentizace, kdy dochází k ověření identity subjektu. Typicky je identita ověřována zadáním správné kombinace uživatelského jména a hesla. Vedle hesla může být identita uživatele ověřena i dle toho, co má – například přístupová karta, co je – využívají se biometrické vlastnosti, co umí – odpověď na vygenerovaný kontrolní dotaz. Pro zabezpečení systémů s kritickými daty se často využívá vícefaktorová autentizace díky níž lze snížit pravděpodobnost útoků.

Poskytnutí zabezpečeného mechanismu pro ověřování uživatelů přihlašovacím jménem a heslem je složité, zneužití hesla vede většinou k širokému rozsahu škod. Vyzrazení a zneužití přihlašovacích údajů má dopad na důvěrnost, neboť neautorizovaná osoba má přístup

ke všem datům jako uživatel. Tato data může měnit či mazat, což znamená dopad na integritu i dostupnost. Existuje mnoho faktorů, kterým je třeba zabránit, mezi nejkritičtější patří:

- únik hesel u klienta, po cestě od klienta na server, na samotném serveru či z databáze kde je informace uložena,
- existenci hesel, která mohou být jednoduše rozlousknuta například útoky brute-force či dictionary attacks,
- manipulace hesel administrátorem bez logování.

4.3.1 Identifikace

V rámci SAP systému jsou uživatelé identifikováni unikátním uživatelským jménem skládajícím se z písmen a číslic. Uživatelské jméno není case-sensitive, což odpovídá požadavkům dle *OWASP*.

4.3.2 Autentizace

Identita uživatele je ověřena zadáním hesla. Heslo by mělo dle *OWASP* splňovat následující požadavky:

- je vždy case-sensitive,
- má alespoň než 10 znaků,
- maximální délka je 128 znaků,
- požaduje alespoň jedno velké písmeno, jedno malé písmeno, jedno číslo a jeden speciální znak,
- heslo má omezenou platnost, po jejím vypršení musí být obnoveno,
- systém drží historii hesel, která nemohou být znovupoužita,
- je specifikován počet neúspěšných pokusů o přihlášení, po určeném počtu pokusů je účet uzamčen na určitou dobu,
- heslo se při přihlašování nezobrazuje v plain textu,
- heslo není ukládáno do databáze v plain textu, je zahashováno schválenou hashovací funkcí,
- při změně hesla uživatelem musí být zverifikováno staré heslo a nové musí být zadáno dvakrát,
- administrátor systému může vygenerovat uživateli nové heslo, tato aktivita musí být logována pro zamezení manipulace hesla administrátorem, nové heslo je uživateli zasláno e-mailem a po prvním použití musí být změněno,
- hesla nejsou zapisována do žádných logů,
- zpráva o chybě během přihlášení neukazuje detaily zda je zadáno chybně jméno či heslo.

Většina požadavků výše může být nastavena super administrátorem přímo v konkrétním SAP systému v transakci `RZ10`. Detaily ohledně nastavení a kontroly pravidel pro hesla jako jsou minimální délka hesla, minimální počet číslic, speciálních znaků, velkých či malých písmen a další jsou uvedena v dotazníku pod kategorií Autentizace, Identifikace. Uživatelské jméno a heslo jsou defaultním mechanismem pro autentizaci z prohlížeče i SAP GUI. Heslo je hashované algoritmem SHA-1 a je ukládané a přenášené pouze v této podobě. Heslo musí splňovat interní požadavky nastavené administrátorem v SAP systému.

Uživatelská jména a zahashovaná hesla jsou ukládány v tabulkách `USR02`, `USH02` a `USRPWDHISTORY`. Přístup k těmto tabulkám musí být omezen nastavením autorizací.

4.3.3 Defaultní uživatelé

SAP NetWeaver aplikační server ABAP vytváří během instalačního procesu standardně tři klienty 000, 001, 066 s defaultními uživateli s kritickým autorizačním profilem, kteří mají defaultní veřejně známá hesla uvedená v tabulce 4.3.

Uživatel	Heslo	Klient
SAP⋆	06071992, PASS	všichni
DDIC	19920706	000, 001
TMSADM	PASSWORD, $1Pawd2&	000
SAPCPIC	ADMIN	000, 001
EARLYWATCH	SUPPORT	066

Tabulka 4.3: Tabulka defaultních uživatelů, zdroj [36]

Defaultní dialogový uživatel SAP⋆

Tento uživatel je vytvořen po instalaci ve všech klientech systému s autorizačním profilem `SAP_ALL`, může tedy provádět libovolné akce v systému. Je nutné na každém klientu SAP systému vytvořit nového uživatele s novým heslem a přiřadit mu autorizační profil `SAP_ALL`, nového uživatele deaktivovat a následně uživateli `SAP⋆` změnit heslo, nastavit autorizační profil `SUPER` a také jej deaktivovat. Jeho existence je nutná pro běh ABAP aplikačního serveru, v případě, že je smazán, je znovu vytvořen s defaultním heslem `PASS` a všemi autorizacemi.

Defaultní uživatel DDIC

Uživatel DDIC je vytvořen v klientu 000 a 001 během instalace s autorizačním profilem `SAP_ALL`. V klientu 000 je dialogovým typem uživatele, v ostatních klientech může být systémový, jsou přes něj prováděny akce na pozadí a interakce se systémem. Má oprávnění provádět obnovy, instalovat balíčky záplat a konfigurovat systém, jeho smazání by způsobilo ztrátu těchto možností. Je doporučeno mu změnit autorizační profil na `SUPER`, deaktivovat jej a aktivovat jen když je to nezbytné, v systému 000 je doporučováno dle [36] nastavit typ uživatele na `SYSTEM` a změnit mu defaultní heslo.

SAPCPIC a TMSADM uživatelé

Tito dva uživatelé jsou oba komunikační typ uživatele, přes kterého může útočník provádět RFC požadavky. Je dobré oba uživatele smazat a vytvořit nové uživatele s jiným jménem a stejnou autorizační skupinou.

EARLYWATCH uživatel

Dialogový typ uživatele je využívaný společností SAP AG pro podporu. Jeho defaultní heslo je veřejně známe, je doporučováno toto heslo změnit a uživatele deaktivovat a znovu je aktivovat pouze v případě potřeby.

4.3.4 Autorizace

Bezpečný autorizační koncept by měl omezit přístupová práva na nutné minimum. Systém by měl mít dle ISO/IEC 27002:2013 [14] oddělený přístup z hlediska vývoje, nasazení, administrace, konfigurace, podpory, auditu a produktivního používání. Pro některé části by měl být umožněn režim pouze pro čtení. Administrátoři by neměli mít přístup k citlivým datům pokud to není nezbytně nutné. Administrativní oprávnění by měla být rozdělena mezi více administrativních rolí (například systémový administrátor, databázový administrátor, administrátor uživatelů a podobně).

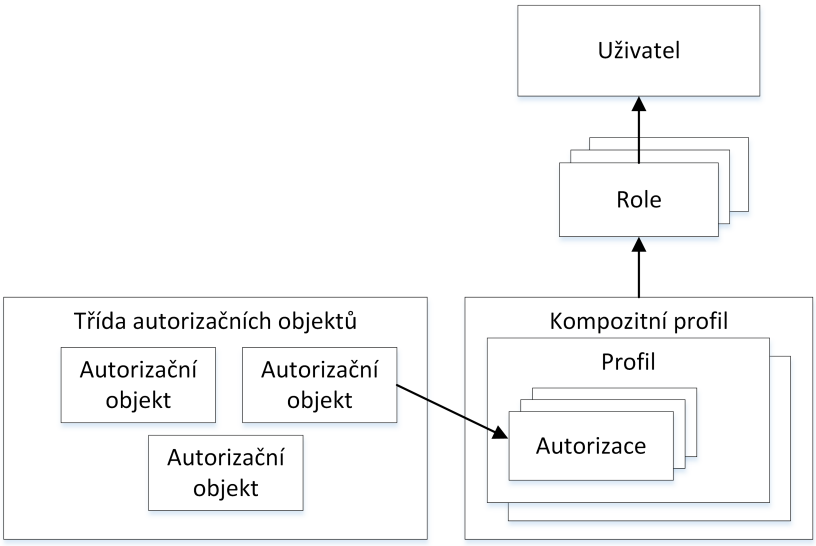
V podnikových aplikacích bývají autorizace velice sofistikované proto, aby operace splňovaly právní požadavky a zároveň zamezovali zneužití dat a podvodům. Dle *OWASP* má být zajištěna podpora principu *Segregation of Duties* pro kritickou kombinaci autorizací a principu *Least Privilege*, kde je cílem omezit přístup subjektu k datům a funkcím tak, aby mohl plnit svůj účel a nic víc.

Autorizační koncept SAP systému umožňuje chránit transakce, programy, služby a tabulky před neautorizovaným přístupem. Autorizace jsou kombinovány do autorizačního profilu asociovaného s rolí. Přiřazování rolí má na starosti systémový administrátor.

Obrázek 4.1 ukazuje autorizační komponenty a jejich vztahy:

- **Autorizační pole** je spojeno s datovým elementem uloženým v ABAP Dictionary.
- **Autorizační objekt** seskupuje až deset autorizačních polí.
- **Autorizace** umožňuje provést konkrétní aktivitu v SAP systému na základě skupiny autorizačních objektů.
- **Kompozitní profil** se skládá z jakéhokoliv počtu autorizačních profilů.
- **Autorizační profil** je zaveden z důvodu snížení úsilí při správě autorizací, seskupuje množství autorizací.
- **Role** je asociována s autorizačním profilem a je přiřazována uživateli.

Seggregation of Duties SoD je bezpečnostní metoda pro vyhnutí se přidělení dvou přístupový práv, která mohou dohromady způsobit riziko. *SoD* pomáhá rozdělit zodpovědnosti, umožňující jednotlivci dohromady provést kritickou aktivitu. *SoD* je založena na business procesech každé společnosti. Z hlediska *SoD* principu nemá kompozitní profil `SAP_ALL` se všemi oprávněními žádné praktické využití. Uživatel s touto rolí může provádět jakékoliv aktivity v systému.



Obrázek 4.1: Autorizace v SAP systému, zdroj: [39]

Uživatelská práva by měla být specifikována na základě principu *Least Privileges*. Dle tohoto principu by `SAP_ALL` profil by měl být používán pouze v případě nouze. Měl by být vytvořen pouze jeden uživatel s tímto profilem. Namísto profilu `SAP_ALL` by mělo být vytvořeno více uživatelů s distribuovanými oprávněními.

V SAP systému je několik autorizačních objektů, díky kterým mohou uživatelé neomezeně spouštět jakékoliv programy, upravovat zdrojové kódy, nahlížet do tabulek a upravovat je a podobně. Kritické autorizační objekty, pro které má být kontrolováno, zda jsou přiřazeny správným uživatelům jsou uvedené v dotazníku v sekci Autorizace. Kontrola potřebných autorizací může být deaktivována transakci `su24` nebo `su25` pro všechny objekty v systému.

V transakci `SUIM` možné kontrolovat přidělení kritických autorizací a jejich kombinací. Společností SAP je definována řada kontrol ověřovaných spuštěním varianty `SAP_RSUSR009`. Mohou být rozšířeny o nejrůznější další kontroly.

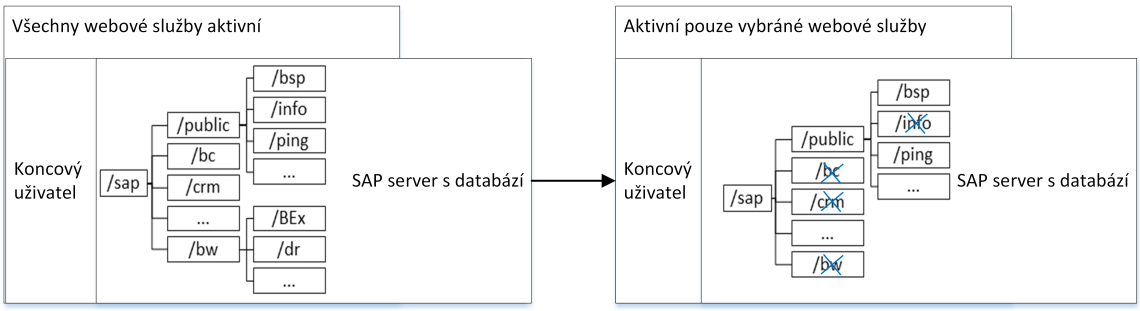
4.4 Deaktivace nepoužívaných kritických funkcionalit

SAP systémy nabízí přístup k webovému obsahu. Přístup k němu je spravován *Internet Communication Managerem ICM*. Některé *ICM* služby mohou být potenciálně zneužity k neautorizovanému přístupu k SAP systému. Dle [38] je vhodné aktivovat pouze služby, které jsou nezbytné pro požadovaný obchodní scénář. Většina funkcionalit je defaultně aktivována. Čím více funkcionalit je aktivováno, tím je větší pravděpodobnost výskytu zranitelností.

Kontrola se týká především webových služeb typicky umístěných v `/sap/public`, které jsou dostupné přes internet pro uživatele s malými oprávněními nebo i pro anonymní uživatele. Standardní instalace obsahuje asi 1500 různých webových služeb dostupných vzdáleně pro registrované uživatele. Vedle toho existuje asi 40 služeb dostupných anonymním uživatelům.

Přístup k RFC funkčním přes SOAP rozhraní umožňuje služba `/sap/bc/soap/rfc`. S aktivní službou a dostatečnými oprávněními může uživatel přistupovat a provádět RFC

funkce na ABAP platformě přes internet. Zároveň klasický uživatel s jakýmikoliv oprávněními může provést DoS útok s nesprávným SOAP požadavkem. Dle [33] je vhodné tuto službu v případě, že není používána, deaktivovat v transakci `SICF`. Pokud je služba nezbytná, musí mít v transakci `SICF` nastavená pouze nejnutnější autorizační pravidla. Aktivace a deaktivace všech webových služeb jsou prováděny v této transakci. Kompletní seznam webových služeb vhodných pro deaktivaci dle [29], pokud nejsou nezbytné z hlediska funkcionality, je uveden v dotazníku v sekci Kritická funkcionalita. Deaktivací nepotřebných webových služeb se zmenší možný attack surface na systém, což je ilustrováno obrázkem 4.2.



Obrázek 4.2: Zmenšení možného attack surface po deaktivaci vybraných webových služeb, zdroj: [29]

Dále je dle [27] na produkčním systému vhodné deaktivovat v každém případě množství kritických transakcí pro správu databázových tabulek, mazání uživatelů, správu autorizací a podobně, které nejsou v produkčním systému potřeba. Detailní seznam transakcí je opět uveden v dotazníku v sekci Kritická funkcionalita.

4.5 Omezení přístupu k rozhraním vzdálené správy

SAP NetWeaver ABAP platforma zahrnuje služby dispečeru zodpovědného za uživatelský přístup ze SAP GUI, ale i velké množství jiných služeb umožňujících vzdálený administrativní přístup a technický přístup služeb jako je například *message server*. Tyto služby mohou být dostupné přes korporátní síť či přes internet a mohou být nastaveny nezabezpečeně, mohou umožňovat přístup bez jakékoliv autentizace. Je třeba se soustředit na zabezpečení následujících služeb:

4.5.1 Přístup k funkcím SAPControl služby

SAP Start Service je spouštěna automaticky na Windows jako `sapstartsrv.exe` v UNIX jako `sapstartsrv` při startu instance SAP aplikačního serveru. Tato služba poskytuje SAP řešení monitorování aktivního stavu, čtení logů a konfiguračních souborů, technické informace o síťových portech a podobně. Tyto služby jsou přístupné přes *SAPControl SOAP Web Service*. Služba používá tyto porty:

- HTTP port 5<xx>13, kde <xx> je číslo instance,
- HTTPS port 5<xx>14, kde <xx> je číslo instance.

Proces dovoluje číst různá systémová data bez uživatelského souhlasu, může vyžadovat autentizaci pro takzvané chráněné operace, které jsou v seznamu pod systémovým parametrem `service/protectedwebmethods` v transakci `rz10`. Jiným řešením zvýšení bezpečnosti je omezení vzdáleného přístupu přes síť k portům 5<xx>13 a 5<xx>14 na minimum prostřednictvím Access Control Listu v parameterech `service/http/acl_file` a `service/https/acl_file` v transakci `rz10`.

4.5.2 Přístup k servisním funkcím Message Serveru

SAP Message Server je systémová komponenta starající se o komunikaci mezi aplikačními servery v rámci jednoho SAP systému a vyrovnávající zátěž distribuováním požadavků přicházejících ze SAP GUI. Z důvodů kontroly adres, které se mohou spojit s Message Serverem je třeba aktivovat Access Control List nastavením parametru `ms/acl_info` s cestou ke konfiguračnímu souboru pro message server. V případě že ACL soubor chybí může se kdokoliv připojit k Message Serveru, zaregistrovat vlastní aplikační server a provést man-in-the-middle útok pro získání citlivých dat či přihlašovacích údajů právoplatných uživatelů připojujících se k Message Serveru.

4.5.3 Přístup k SAP Gateway

SAP Gateway je technická komponenta pro komunikaci mezi SAP systémy. Přistup externích programů k SAP Gateway je řízen a kontrolován souborem `reginfo`, definovaným systémovým parametrem `gw/reg_info` a `secinfo` definovaným systémovým parametrem `gw/sec_info`. Tyto soubory je doporučováno měnit ze SAP GUI, neboť je kontrolována syntaktická správnost záznamů. Při změně souborů v textovém editoru může být do souborů zanesená syntaktická chyba způsobující nefunkčnost SAP Gateway.

Reginfo slouží ke specifikaci registrovaných služeb a pro řízení přístupu k nim, rušení jejich registrace, určení externích služeb, které mohou být zaregistrovány na Gateway. Pokud soubor `reginfo` není definován, může se k SAP Gateway zaregistrovat kdokoliv, stejně tak pokud je v `reginfo` záznam kde `HOST` je nastaven na *. V takovém případě může kdokoliv získat přístup k SAP Gateway a zaregistrovat jakoukoliv službu se škodlivou funkcionalitou například pod stejným názvem jako již existující služba spouštěna právoplatnými uživateli.

Secinfo soubor je využíván pro předcházení neautorizovaného startu externího programu. Bez tohoto souboru může systém spustit jakékoliv externí programy, pokud je tento soubor prázdný, není možné spustit žádnou externí službu. V případě chybějícího secInfo může kdokoliv spustit službu registrovanou v SAP Gateway a získat tím neautorizovaný přístup k SAP serveru.

4.6 Bezpečnost přenosu dat mezi prezentační a aplikační vrstvou

Pro komunikaci mezi tlustým klientem SAP GUI a aplikačním serverem je používán proprietární protokol *Dynamic Information and Action Gateway DIAG* nepodporující autentizaci a šifrování během přenosu dat. Bez přídavného zabezpečení může útočník pomocí programu Wireshark bez problému zjistit přihlašovací jméno a heslo.

4.6.1 Přenos mezi tlustým klientem a aplikačním serverem

Řešením pro zabezpečení komunikace mezi SAP GUI a aplikačním serverem je využití softwarové vrstvy *Secure Network Communication SNC*, zabezpečující *DIAG* komunikaci mezi SAP GUI a aplikačním serverem a RFC volání používané pro komunikaci mezi více SAP NetWeaver aplikačními servery. *SNC* nemůže být využito pro komunikaci mezi databází a aplikačním serverem, proto je doporučeno mít databázi a aplikační server ve stejné síti. *SNC* nabízí tři úrovně ochrany:

- Pouze autentizaci – systém verifikuje identitu komunikujících stran, jedná se o nejnižší úroveň bezpečnosti nabízené *SNC*.
- Autentizaci a ochrany integrity – systém detekuje změny dat, které se mohou vyskytnout během komunikace.
- Autentizaci, ochranu integrity a důvěrnosti - systém nabízí kryptování zpráv mezi komunikujícími stranami, jedná se o nejvyšší stupeň ochrany nabízený *SNC*.

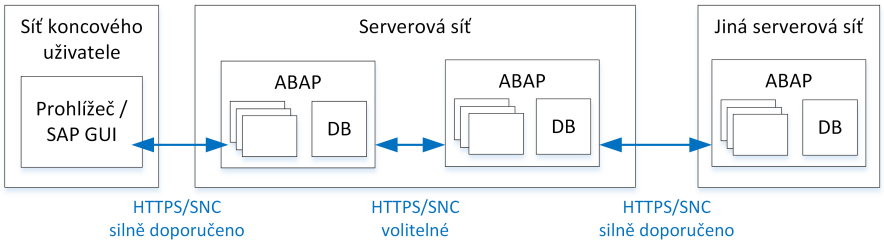
SNC je defaultně deaktivováno a je možné jej aktivovat nastavením systémového parametru `snc/enable` na hodnotu 1. Deaktivované *SNC* může vést k neautorizovanému získání dat, která jsou přenášena protokoly RFC nebo DIAG. Tyto protokoly nabízí pouze nezabezpečené kompresní algoritmy bez šifrování. Proto data mohou být jednoduše dekódována.

SAP systémy se mohou připojovat k jiným SAP systémům přes SAP Gateway s využitím RFC. RFC funkce mohou přes RFC protokol přenášet důvěrná data, bez šifrování je může útočník zachytit spoofing útokem. Nastavení *SNC* pro RFC spojení je nastavováno v transakci `sm59`.

4.6.2 Přenos mezi webovým rozhraním a aplikačním serverem

Internet Communication Manager dovoluje komunikaci mezi SAP systémem a internetem s využitím HTTP a HTTPS. Defaultně je využíván protokol HTTP, což je samo o sobě bezpečnostní riziko, jméno a heslo jsou posílány jako textový řetězec zakódovaný Base64 v HTTP požadavku. Metoda je snadná na implementaci, ale počítá s bezpečným spojením mezi klientem a serverem. Při tomto přístupu mohou být navíc uživatelské autentizační informace vloženy do logovacího souboru, kde se logují hlavičky HTTP požadavků. Pro přepnutí na HTTPS je nutné nastavit parametr `icm/server_port` v transakci `rz10` v systému.

Šifrovací klíče jsou ukládány v *Personal Security Environment PSE* souborech na serveru a v databázové tabulce `SSF_PSE_D`. Přístup k těmto klíčům musí být chráněný, pro přístup k tabulce musí být vyvořena speciální autorizační skupina.



Obrázek 4.3: Doporučené použití SNC a HTTPS, zdroj: [29]

4.7 Logování bezpečnostních událostí

Důležitým aspektem pro zajištění bezpečnosti SAP systémů je logování bezpečnostních událostí, což jsou události, které mohou mít dopad na důvěrnost, integritu či dostupnost systému. SAP systém nabízí kolem třiceti logů. Dle [28] jsou čtyřmi nejdůležitějšími logy *Security Audit Log*, log HTTP požadavků, log udržující změny tabulek a log aktivit SAP Gateway. Dle doporučení Národního centra kybernetické bezpečnosti by měly logy zahrnovat informace o času události, uživateli, zdrojové IP adrese a případné další informace o detailech události. Měla by být zajištěna dostatečná kapacita pro logování, pravidelná analýza logů v log managementu, bezpečnost a integrita záznamů v logu a dostupnost logů i v případě poruchy [24]. Bez logování událostí vyvstává riziko pozdní reakce na potenciální útok.

Auditní log

Security Audit Log je doplňkovým logem pro systémový log. Na rozdíl od něj může být neaktivní. Jedná se o detailní log pro všechny události v SAP systému:

- události spojené s bezpečností v SAP systému, například úprava účtu primárních uživatelů,
- informace pro větší transparentnost přístupů - úspěšné a nevalidní pokusy o přístup,
- informace pro rekonstrukci řetězce událostí - úspěšné a neúspěšné spuštění transakcí.

Transakce `sm19` slouží ke správě událostí, které mají být logovány. Udržuje seznam všech událostí rozdělených dle kritičnosti. Pro revizi logu se využívá transakce `sm20`. Soubory jsou umístěny na aplikačních serverech. Defaultně je auditní logování vypnuté, zapíná se parametrem `rsau/enable` nastaveným na 1 v transakci `rz10`.

Logování HTTP požadavků

Logování HTTP požadavků je také defaultně deaktivované, může být aktivováno nastavením parametru `icm/http/logging` v transakci `rz10`.

Logování změn v tabulkách

Jakékoliv akce s tabulkami je vhodné zaznamenávat do logů. Logován je nastavováno parametrem `rec/client` v transakci `rz10` a mělo by být zapnuté na všech produkčních klientech. Existují klientské tabulky obsahující data pro jednoho klienta a takzvané klient nezávisle tabulky obsahující data validní pro všechny klienty systému. Změny tabulek nejsou logovány defaultně. Z kapacitních důvodů není doporučené zapnutí logování na testovacích klientech. Záznamy všech tabulek nastavených pro logování jsou udržovány v tabulce `DD09L`.

Logování SAP Gateway aktivit

Logování aktivit na SAP Gateway se nastavuje parametrem `gw/logging` parameter v `rz10`. Gateway zajišťuje interakci mezi workprocesy a externími programy a mezi workprocesy z různých SAP systémů. Každá SAP instance má SAP Gateway zajišťující interakci mezi workprocesy a externími programy a interakci mezi instancemi SAP systému.

Kapitola 5

Dotazník pro evaluaci platformy SAP

Metodika evaluace platformy bude vycházet z normy ISO/IEC 27002:2013 [15], podle které měřící proces zahrnuje čtyři základní části:

- tvorbu metrik,
- provádění měření,
- analýzu metrik a reporting,
- vyhodnocení měření.

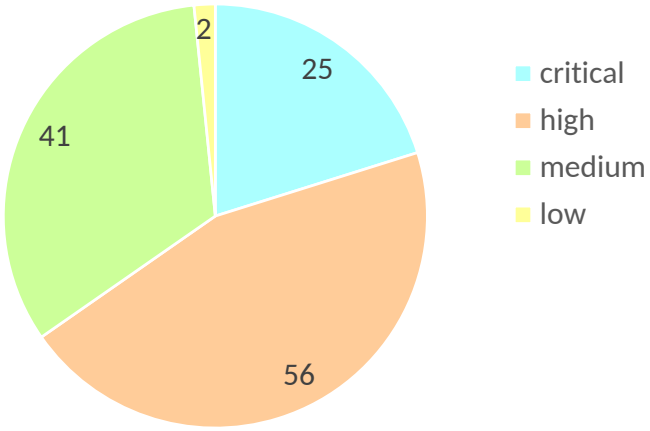
Metriky jsou vytvořeny v podobě dotazníku. Dokumentování měření je prováděno přímo v samotném dotazníku. Na analýzu výsledků a jejich vyhodnocení se soustředí kapitola 6. Byla vytvořena sada celkem 124 kontrol rozdělených do kategorií přímo vycházejících z kapitoly 4 s tím rozdílem, že kapitola Řízení přístupu 4.3 byla rozdělena do dvou kategorií Autentizace, identifikace a Autorizace. Bylo tedy vytvořeno celkem osm kategorií:

1. operační systém a databáze (2 kontroly),
2. správa záplat a aktualizací (4 kontroly),
3. autentizace, identifikace (27 kontrol),
4. autorizace (24 kontrol),
5. kritická nepotřebná funkcionalita (32 kontrol),
6. otevřená rozhraní (11 kontrol),
7. přenos (11 kontrol),
8. logování bezpečnostních událostí (13 kontrol).

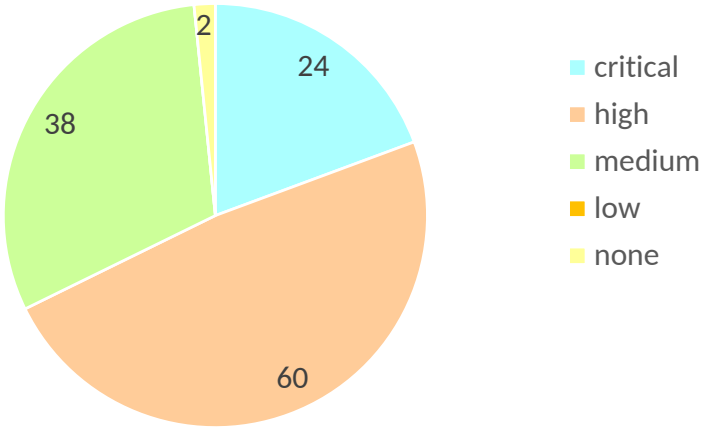
Pro přehlednost a možnost detailnější filtrace v dotazníku jsou jednotlivé kategorie rozděleny dále do podkategorií. Každá skupina obsahuje sadu požadavků označených unikátními identifikátory *ID* ve tvaru *1.2.3.4*, kde 1 je číslo kategorie, a 2 je číslo závislé podkategorie nebo samotného požadavku, 3, 4 jsou nepovinné identifikátory určující další závislé podkategorie či požadavky.

Jednotlivé požadavky jsou ohodnoceny dle kritičnosti kritičnosti skórem *CVSS* detailněji popsaného v kapitole 3.3.3 a vlastní metodikou definovanou v kapitole 3.3.4. Pro výpočet *CVSS* existuje oficiální online nástroj, kde uživatel zadá hodnocení jednotlivých metrik a je mu vypočítáno *CVSS* skóre a zobrazen hodnotící řetězec. Pro zjednodušení hodnocení a možnou úpravu *CVSS* skóre je výpočet prováděn přímo v dotazníku a není zobrazován hodnotící řetězec, neboť charakteristiky, ze kterých je odvozeno výsledné skóre, jsou viditelné také v dotazníku. Ve sloupcích *CVSS* ohodnocení uživatel zadá hodnocení jednotlivých metrik (sloupce K – R) a na základě pomocných výpočtů ve skrytých sloupcích (S - AF) je vypočítáno výsledné *CVSS* skóre (sloupec J), které je pak ve sloupci AG převedeno na textovou reprezentaci dle tabulky 3.2 z kapitoly 3.3.3. Dotazník uvažuje pouze základní metriky *CVSS*, neboť hodnocené požadavky jsou neměnné vzhledem k času a prostředí.

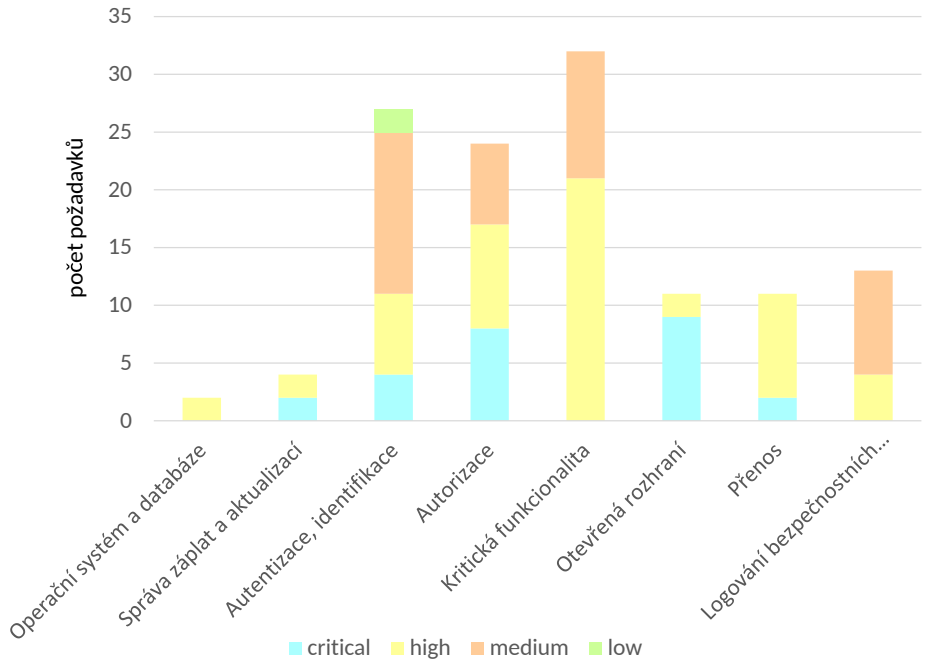
Rozdělení požadavků na základě kritičnosti dle *CVSS* a vlastní metodiky je znázorněno na grafech 5.1 a 5.2. Rozdělení dle kritičnosti do jednotlivých kategorií je pak znázorněno na grafu 5.3 pro vlastní metodiku a 5.4 pro *CVSS*.



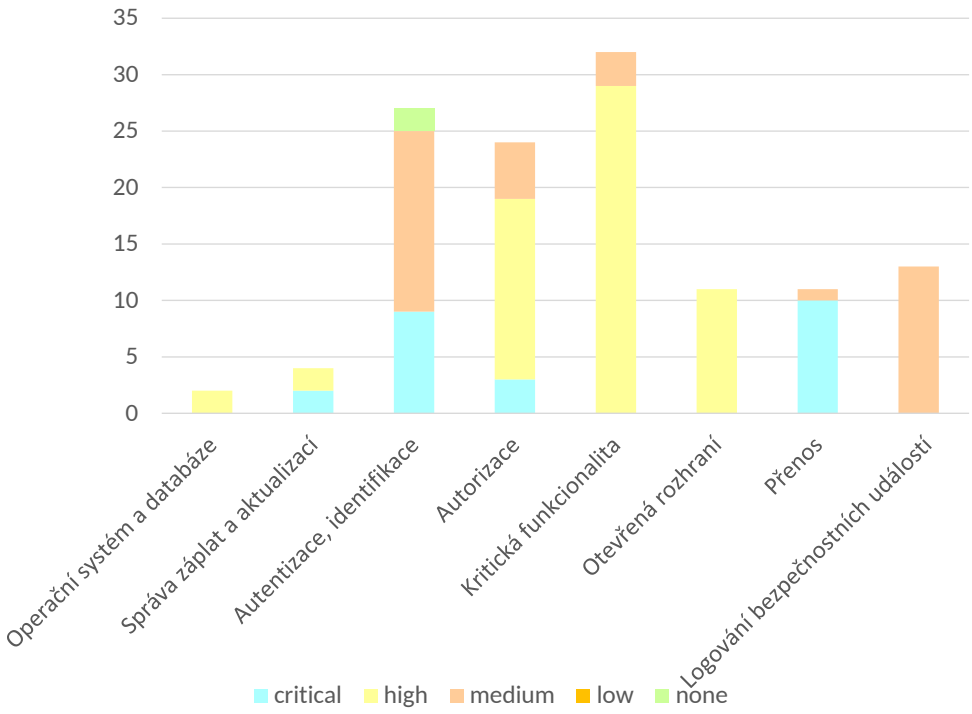
Obrázek 5.1: Rozdělení požadavků na základě kritičnosti dle vlastní metodiky.



Obrázek 5.2: Rozdělení požadavků na základě kritičnosti dle CVSS.



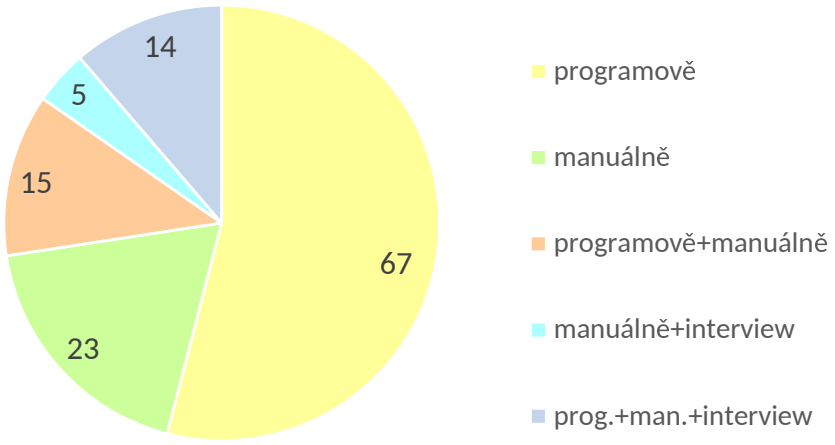
Obrázek 5.3: Rozdělení požadavků do skupin dle vlastní metodiky.



Obrázek 5.4: Rozdělení požadavků do skupin dle CVSS.

V dalších sloupcích je uvedeno jakým způsobem je požadavek zajišťován v SAP systému (sloupec AI), jakým způsobem je prováděno ověření a detailní návod jak ověřit, zda je požadavek splněn. Způsob ověření může nabývat šesti typů, jejich četnost v dotazníku je znázorněna grafem na obrázku 5.5:

- Programově, kdy ověření vyžaduje spuštění programu uvedeného ve sloupci postup ověření na testovaném systému a nakopírování hodnot do sloupce Výsledek ověření. Celkem je využíváno šest vlastních programů a řada standardních ověřujících celkově 69 kontrol.
- Manuálně, kdy ověření vyžaduje manuální vyhledání výsledku v některé ze SAP programů.
- Interview, kdy ověření vyžaduje pouze interview se zodpovědným administrátorem systému.
- Programově + manuálně, kdy je třeba vytvořit určitý testovací scénář v systému a poté spustit daný program.
- Manuálně + interview, kdy ověření vyžaduje manuální vyhledání výsledku a interview se zodpovědným administrátorem systému.
- Programově + manuálně + interview, kdy ověření zahrnuje spuštění programu, manuální vyhodnocení a interview se zodpovědným administrátorem.



Obrázek 5.5: Rozdělení požadavků dle způsobu ověření.

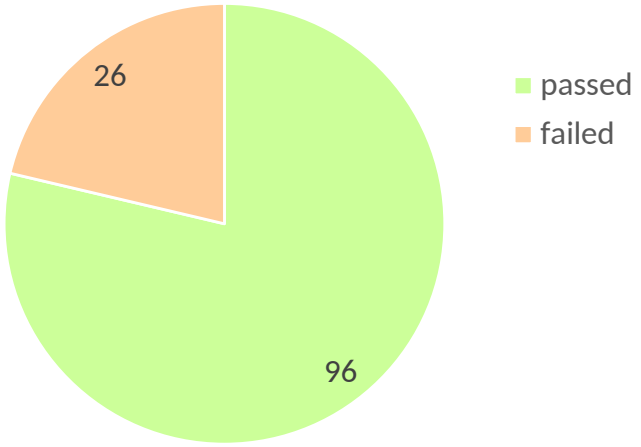
Jednotlivé kontroly mohou nabývat hodnot *passed*, v případě že byla kontrola úspěšná, a *failed* pro případ, že systém nesplňuje daný požadavek. V případě, že je výsledkem ověření hodnota *failed*, je přenesena hodnota *CVSS* do sloupce *Riziko dle CVSS* a stejně tak i hodnota *Vlastní metodiky* je přenesena do sloupce *Riziko dle vlastní metodiky*. Pro vyhodnocení kontrol v dotazníku je vytvořený report blíže popsaný v kapitole 6.

Kapitola 6

Testování

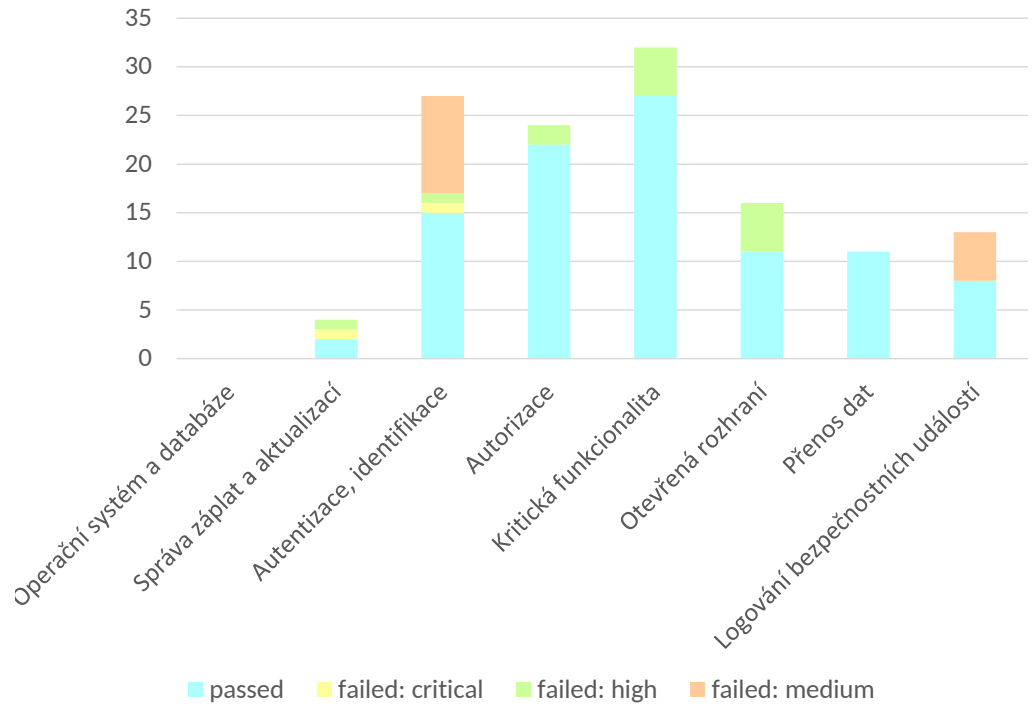
Testování probíhalo na testovacím systému nejmenované společnosti s řešením SAP ERP běžícím na SAP NetWeaver 7.5 s aplikačním serverem ABAP. Testovací systém by měl mít již stejná nastavení jako produkční. Pro testování bylo předpokládáno, že požadavky dle CIS pro databázi a operační systém z první kategorie jsou již splněny. Celkem bylo tedy provedeno 122 ověření rozdělených do kategorií *critical*, *high*, *medium* a *low* respektive *none*. Testování probíhalo dle pokynů v dotazníku manuálně, programově i s využitím interview se systémovým administrátorem. Výsledky byly zaneseny do dotazníku do sloupce *Výsledek ověření*. Dotazník následně vygeneroval výsledné statistiky do záložky *Report*.

Celkově nebylo splněno 26 požadavků, což je 21 procent z celkového počtu všech ověření. Poměr *passed* a *failed* je znázorněn obrázkem 6.1.



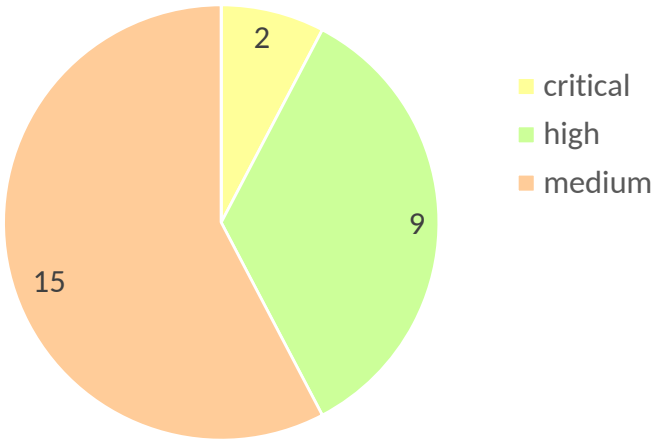
Obrázek 6.1: Poměr úspěšných a neúspěšných ověření.

Rozdělení splněných a nesplněných požadavků v rámci jednotlivých kategorií je ilustrováno na obrázku 6.2. Z grafu je patrné, že nejvíce nesplněných požadavků spadá do kategorie Autentizace, identifikace, kde bylo odhaleno, že není aplikována politika hesel a chybělo zabezpečení jednoho z defautních uživatelů. Naopak všechny bezpečnostní požadavky byly splněny v kategorii Přenos dat. *Secure Network Communication SNC* a HTTPS byly nakonfigurovány správně.

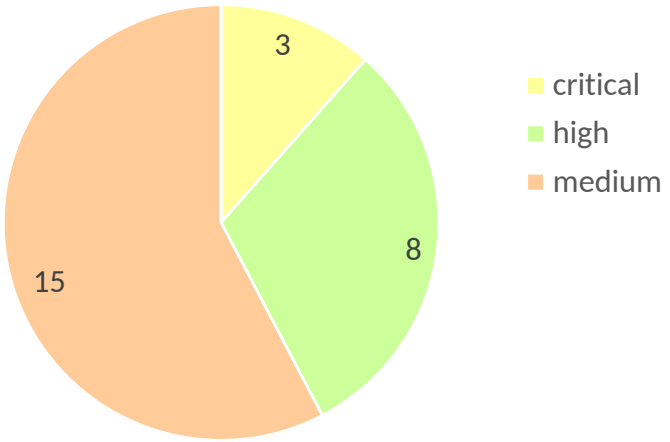


Obrázek 6.2: Poměr úspěšných a neúspěšných ověření v rámci jednotlivých kategorií.

Poměr ohodnocení nesplněných požadavků dle CVSS a vlastní metodiky je ilustrováno obrázky 6.3 a 6.4. Nesplněné kritické požadavky dle CVSS i vlastní metodiky spadají do kategorií Správa záplat, kde byl nalezen problém s chybějící aktualizací kernelu a Autentizace, Identifikace, kde nebyl správně zabezpečen defaultní uživatel EARLYWATCH.



Obrázek 6.3: Rozdělení kritičnosti neúspěšných kontrol dle vlastní metodiky.



Obrázek 6.4: Rozdělení kritičnosti neúspěšných kontrol dle CVSS.

Pro kategorii *High* nebyly splněny některé požadavky ze sekce Kritická funkcionalita, konkrétně deaktivace kritických transakcí a ze sekce Autorizace pro zabezpečení uživatele EARLYWATCH. Dále bylo zjištěno, že není nastavena jakákoliv politika hesel a jsou deaktivované některé logy. Tyto požadavky spadají do kategorie *Medium*. Přehled všech požadavků se statusem failed je uveden v tabulce C.1.

Kapitola 7

Závěr

Cílem práce bylo prostudovat existující standardy, postupy a metodiky pro ohodnocení stavu bezpečnosti informačních systémů a následně navrhnout metriky a metodiku pro bezpečnostní zhodnocení systémů založených na platformě SAP.

Pro evaluaci byla vybrána platforma SAP NetWeaver s aplikačním serverem ABAP, neboť je v dnešní době nejrozšířenější platformou mezi zákazníky společnosti. Práce analyzuje možná rizika působící na platformu a identifikuje nejrůznější zranitelnosti. Vytvořený dotazník rozděluje jednotlivé bezpečnostní požadavky do osmi kategorií – operační systém a databáze, správa záplat a aktualizací, autentizace a identifikace, autorizace, kritická nepotřebná funkcionalita, otevřená rozhraní, přenos dat a logování bezpečnostních událostí. Jednotlivé bezpečnostní požadavky jsou v dotazníku ohodnoceny dle kritičnosti skórem CVSS a vlastní metodikou definující čtyři úrovně kritičnosti. Každý požadavek zahrnuje přesný postup ověření v systému SAP. Pro případy, které je možné vyhodnotit programově, byly vytvořeny programy v jazyku ABAP spouštěné přímo v testovaném systému. Na základě výsledků hodnocení jsou v dotazníku automaticky generovány grafy vyhodnocující stav systému. Dotazník byl testován na reálném testovacím systému nejmenované společnosti s řešením SAP ERP běžícím na SAP NetWeaver 7.5, který by měl být konfigurován identicky s produkčním systémem. Výsledky poskytly ohodnocení bezpečnosti systému, ze 122 testovaných bezpečnostních kontrol nebylo naplněno 26 požadavků, což je 21 procent z celkového počtu. Dotazník odhalil i kritické nálezy, konkrétně nebyly aplikovány poslední kriticky důležité záplaty a chybělo správné zabezpečení jednoho z defaultních uživatelů systému. Celkově se jednalo o lehce odstranitelné chyby. Díky dotazníku byla zavedena nastavení pro kontrolu politik hesel a zavedeny pravidelné kontroly dostupnosti nových kritických záplat.

V práci jsem využila znalosti získané vysokoškolským studiem a svou prací ve společnosti SAP. Tyto znalosti jsem si zároveň prohloubila a to zejména v oblasti architektury samotného systému SAP, bezpečnosti informačních systémů a bezpečnosti z hlediska SAP systémů.

Do budoucna je možné rozšířit způsoby ohodnocení kritičnosti bezpečnostních požadavků o další metody, jako je například *OWASP Risk Rating Methodology*. Je možné vytvořit druhý dotazník analyzující aplikační platformu SAP NetWeaver s aplikačním serverem Java. Jako další zajímavé vylepšení vidím tvorbu dotazníku ve formě webové aplikace.

Literatura

[1] The Open Web Application Security Project. [Online; navštíveno 17.05.2017].
URL https://www.owasp.org/index.php/Main_Page

[2] Alexander, P.: Audit bezpečnosti informačních systémů: Klíčový krok k eliminaci zranitelností. [Online; navštíveno 10.04.2017].
URL http://www.itbiz.cz/clanky/audit-bezpecnosti-informacnich-systemu-klicovy-krok-k-eliminaci-zranitelnosti

[3] Anderson, G. W.: *Naučte se SAP za 24 hodin*. Brno: Computer Press, první vydání, 2012, ISBN 978-80-251-3685-0.

[4] Bishop, M.: *Introduction to computer security*. Boston: Addison-Wesley, 2005, ISBN 978-0321247445.

[5] Common Vulnerability Scoring System v3.0: Specification Document. [Online; navštíveno 17.04.2017].
URL https://www.first.org/cvss/cvss-v30-specification-v1.7.pdf

[6] CVSS v3.0 Preview 2: Metrics / Formula / Examples.

[7] Doseděl, T.: *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, vyd. 1. vydání, 2004, ISBN 80-251-0106-1.

[8] Doucek, P.: *Řízení bezpečnosti informací*. Praha: Professional Publishing, druhé vydání, 2011, ISBN 978-80-7431-050-8.

[9] Hanáček, P.: Bezpečnost informačních systémů - Kritéria hodnocení bezpečnosti IS, slidy k předmětu BIS. Brno: FIT VUT v Brně, 2007.

[10] Hanáček, P.; Staudek, J.: *Bezpečnost informačních systémů*. Praha: Úřad pro státní informační systém, první vydání, 2000, ISBN 80-238-5400-3.

[11] Hayden, L.: *IT security metrics*. New York: McGraw Hill, 2010, ISBN 978-0071713405.

[12] Řada norem ISO/IEC 27000. [Online; navštíveno 06.04.2017].
URL http://www.iso27000.cz/

[13] *ČSN ISO/IEC 27001:2005, Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací - Požadavky*. Praha, 2005.

[14] *ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls*. Geneva, 2013.

[15] *ISO/IEC 27004:2016, Information technology - Security techniques - Information security management - Monitoring, measurement, analysis and evaluation*. Geneva, 2016.

[16] ISO/IEC 15408-1:2009 Preview Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. 2009.

[17] Jansen, W.: *Directions in Security Metrics Research [online]*. DIANE Publishing Company, 2010, ISBN 9781437924510.
URL https://books.google.cz/books?id=fXgyeLTsinQC

[18] Jaquith, A.: *Security metrics*. Upper Saddle River, NJ: Addison-Wesley, 2007, ISBN 03-213-4998-9.

[19] Lawlor, W.: *Common SAP R/3 functions manual*. New York: Springer, první vydání, 2004, ISBN 18-523-3775-3.

[20] Loveček, T.: *Bezpečnostné systémy*. Žilina: Žilinská univerzita v Žiline, první vydání, 2007, ISBN 978-80-8070-767-5.

[21] Maassen, A.; Schoenen, M.; Frick, D.; aj.: *SAP R/3*. Brno: Computer Press, první vydání, 2007, ISBN 978-802-5117-507.

[22] Markandeya, S.; Roy, K.: *SAP ABAP*. Apress, přepracované vydání vydání, 2014, ISBN 978-1-4302-4803-3.

[23] Mereddy, R.: *SAP Basis administration handbook*. New York: McGraw-Hill, první vydání, 2012, ISBN 978-0071663489.

[24] Doporučení na minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů. Národní bezpečnostní úřad, [Online; navštíveno 22.04.2017].
URL https://www.govcert.cz/download/doporuceni/container-nodeid-1259/logmngmntfinal.pdf

[25] Oracle Database Security for SAP Applications. [Online; navštíveno 12.04.2017].
URL http://www.oracle.com/us/products/database/nl20-database-security-396167.pdf

[26] Polyakov, A.: Introduction to SAP. [Online; navštíveno 29.03.2017].
URL http://resources.infosecinstitute.com/sap-security-for-beginners-part-two-introduction-to-sap/

[27] Polyakov, A.: SAP NetWeaver ABAP security configuration part 4: Unnecessary functionality. [Online; navštíveno 04.05.2017].
URL https://blogs.sap.com/2015/05/18/sap-netweaver-abap-security-configuration-part-4-unnecessary-functionality/

[28] Polyakov, A.: SAP NetWeaver ABAP Security Configuration Part 9: Security Events Logging. [Online; navštíveno 04.05.2017].
URL https://blogs.sap.com/2015/06/22/sap-netweaver-abap-security-configuration-part-9-security-events-logging/

[29] SAP Audit Guide for Basis. [Online; navštíveno 10.05.2017].
URL https://layersevensecurity.com/wp-content/uploads/2014/07/SAP-Audit-Guide-Basis.pdf

[30] Product Availability Matrix. [Online; navštíveno 29.04.2017].
URL https://support.sap.com/en/release-upgrade-maintenance/product-availability-matrix.html

[31] SAP HANA Security Checklists and Recommendations. SAP SE, 2016, [Online; navštíveno 15.04.2017].
URL https://assets.cdn.sap.com/sapcom/docs/2016/08/3031581b-867c-0010-82c7-eda71af511fa.pdf

[32] SAP Help Portal. [Online; navštíveno 15.02.2017].
URL https://help.sap.com

[33] Access to RFC-enabled modules via SOAP. [Online zákaznická sekce; navštíveno 17.04.2017].
URL https://launchpad.support.sap.com/#/notes/1394100/E

[34] Minimal DB system platform requirements for SAP NetWeaver 7.5. [Online zákaznická sekce; navštíveno 27.04.2017].
URL https://launchpad.support.sap.com/#/notes/2158828/E

[35] Oracle network encryption and data integrity. [Online zákaznická sekce; navštíveno 27.04.2017].
URL https://launchpad.support.sap.com/#/notes/973450/E

[36] SAP NetWeaver ABAP Security Configurations. Default Passwords for Access to the Application. 2014, [Online; navštíveno 06.05.2017].
URL https://erpscan.com/press-center/blog/sap-netweaver-abap-security-configuration-part-2-default-passwords-for-access-to-the-application/

[37] SEC204 – Live on Stage: Monthly Security Patch Webinar. SAP Teched, [Online; navštíveno 11.05.2017].
URL https://support.sap.com/content/dam/library/SAP%20Support%20Portal/support-programs-services/support-services/security-optimization-service/media/SEC204_updated.pdf

[38] Secure Configuration of SAP NetWeaver Application Server Using ABAP. [Online; navštíveno 10.05.2017].
URL https://www.sap.com/documents/2015/07/c06ac591-5b7c-0010-82c7-eda71af511fa.html

[39] Spalding, G.: Authorization Objects – A Simple Guide. 2006, [Online; navštíveno 02.04.2017].
URL http://sapstory.tistory.com/attachment/ik0.pdf

[40] Zendulka, J.; Rudolfová, I.: Databázové systémy IDS, studijí opora. Brno: FIT VUT v Brně, 2006.

Přílohy

Příloha A

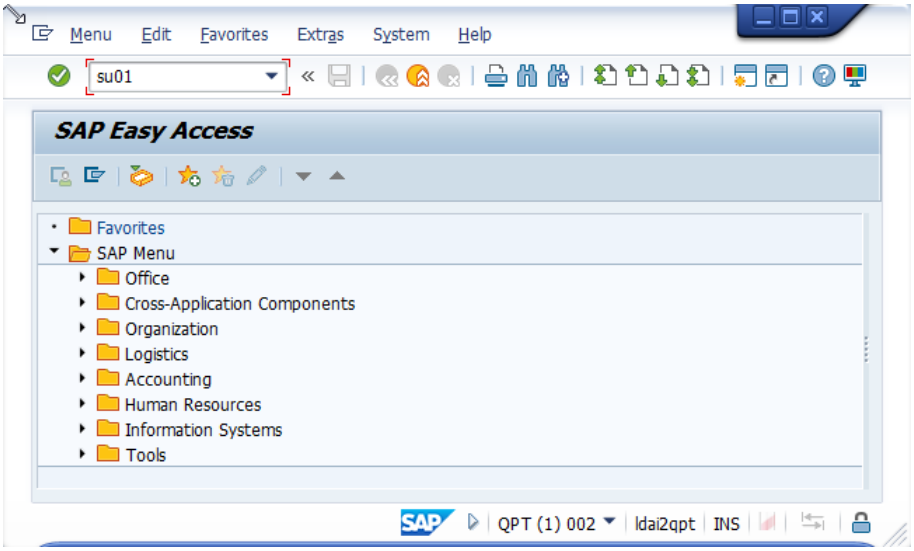
Obsah přiloženého CD

Přiložené CD obsahuje čtyři adresáře:

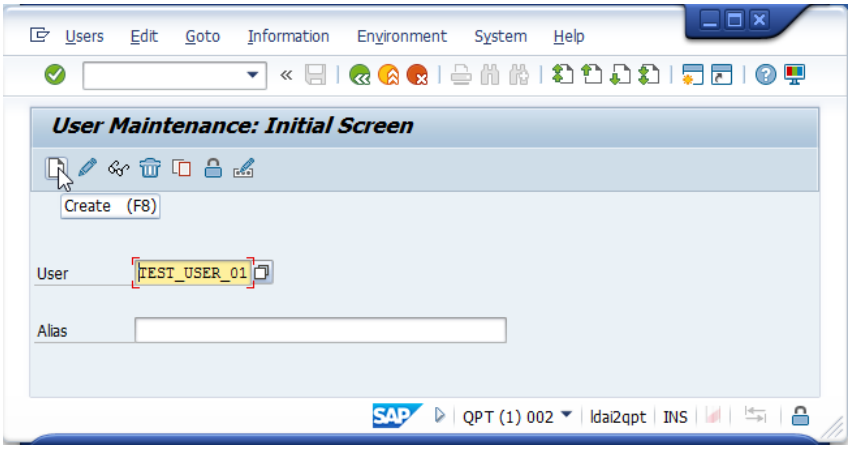
- text - zdrojove soubory textu práce a z nich vygenerovaný soubor pdf,
- abap - zdrojové kódy exportované ze SAP GUI,
- excel - výsledný dotazník ve formátu excel.

Příloha B

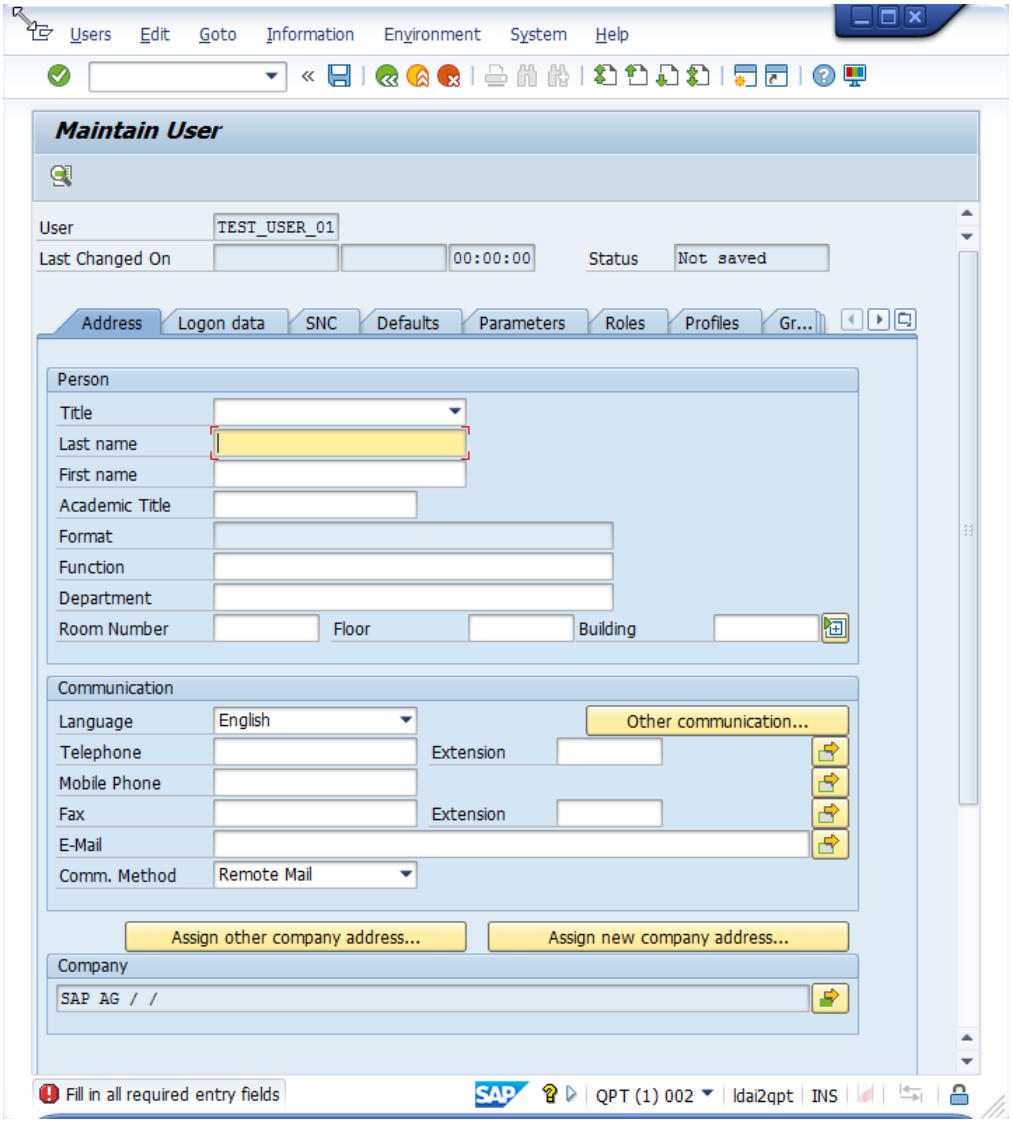
Práce se systémem



Obrázek B.1: Práce se systémem - zadání transakce, zdroj: autor - screenshot obrazovky



Obrázek B.2: Práce se systémem - tvorba uživatele, zdroj: autor - screenshot obrazovky



Obrázek B.3: Práce se sytémem - tvorba uživatele (detail), zdroj: autor - screenshot obrazovky

Příloha C

Příklad dotazníku

Na obrázku C.1 je přehled nesplněných kontrol z Testování. Některé sloupce byly pro přehlednost vynechány, celý dotazník je k dispozici na přiloženém CD.

ID	Kategorie	Požadavek		CVSS	CVSS text	Vlastní	Způsob ověření	Výsledek ověření	Riziko dle vlastní	Riziko dle CVSS
2	Správa záplat a aktualizací									
2.2	Správa záplat a aktualizací	Je aplikován poslední Kernel Patch		9,6	critical	critical	manuálně	failed	critical	critical
2.3	Správa záplat a aktualizací	Jsou aplikovány Security Notes s prioritou 3 a 4		7,1	high	high	manuálně	failed	high	high
3	Autentizace, identifikace									
3.4	Autentizace, identifikace	Formát hesla splňuje požadavky		5	medium	medium	manuálně	failed	medium	medium
3.4.2	Autentizace, identifikace		minimální délka	5	medium	medium	programově	failed	medium	medium
3.4.3.1	Autentizace, identifikace		výskyt velkých písmen	5	medium	medium	programově	failed	medium	medium
3.4.3.2	Autentizace, identifikace		výskyt malých písmen	5	medium	medium	programově	failed	medium	medium
3.4.3.3	Autentizace, identifikace		výskyt čísilc	5	medium	medium	programově	failed	medium	medium
3.4.3.4	Autentizace, identifikace		výskyt speciálních znaků	5	medium	medium	programově	failed	medium	medium
3.5	Autentizace, identifikace	Je zapnutá kontrola zadávaného hesla dle specifikovaného formátu hesla, pokud heslo nesplňuje pravidla, je vynucena		5	medium	medium	programově	failed	medium	medium
3.6	Autentizace, identifikace	Je specifikována doba platnosti hesla		5	medium	medium	programově	failed	medium	medium
3.7	Autentizace, identifikace	Systém nedovoluje nastavit stejné heslo, jako pět posledních hesel v minulosti		5	medium	medium	programově	failed	medium	medium
3.8	Autentizace, identifikace	Je specifikován počet neúspěšných pokusů o přihlášení po kterých dojde k uzamčení systému pro uživatele		5	medium	medium	programově	failed	medium	medium
3.14.1	Autentizace, identifikace	Uživatel EARLYWATCH	Nemá defaultní heslo	9,6	critical	critical	programově+manuálně	failed	critical	critical
3.14.2	Autentizace, identifikace		Je deaktivován ve všech klientech	9,6	critical	high	programově+manuálně	failed	high	critical
4	Autorizace									
4.6.1	Autorizace	V produkčním systému nejsou přiřazeny žádné role a autorizační objekty pro ABAP workbenchi (Workbench, Customizing, Transport Organizer)	žádný uživatel s autorizačním objektem S_DEVELOP	8,8	high	high	programově+manuálně	failed	high	high
4.6.2	Autorizace		žádný uživatel s autorizačním objektem S_TRANSPRT	8,8	high	high	programově+manuálně	failed	high	high
5	Kritická funkcionalita									
5.1.12	Kritická funkcionalita		Přístup ke konfiguraci SAP Gateway: SMGW	8,3	high	high	programově	failed	high	high
5.1.13	Kritická funkcionalita		Přístup ke konfiguraci RFC: SM59	8,3	high	high	programově	failed	high	high
5.1.14	Kritická funkcionalita		Přístup ke správě ICM služeb: SICF	8,3	high	high	programově	failed	high	high
5.1.15	Kritická funkcionalita		Konfigurace ICM portů: SMICM	8,3	high	high	programově	failed	high	high
5.1.16	Kritická funkcionalita		Konfigurace message serveru: SMMS	8,3	high	high	programově	failed	high	high
8.2	Logování bezpečnostních událostí	log HTTP požadavků	Je aktivován	5,9	medium	medium	programově	failed	medium	medium
8.3	Logování bezpečnostních událostí	log udržující změny tabulek	Je aktivován	5,9	medium	medium	programově	failed	medium	medium
8.4	Logování bezpečnostních událostí	log aktivit SAP Gateway	Je aktivován	5,9	medium	medium	programově	failed	medium	medium
8.5	Logování bezpečnostních událostí	logování provozu ICM		5,9	medium	medium	programově	failed	medium	medium
8.6	Logování bezpečnostních událostí	logování aktivit message serveru		5,9	medium	medium	programově	failed	medium	medium

Obrázek C.1: Příklad dotazníku, nesplněné požadavky z Testování.