

Nastavení bezpečnosti v prostředí SAP ve společnosti HP TRONIC

Bc. Jiří Trojan

Diplomová práce
2023



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Jiří Trojan
Osobní číslo:	A22538
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní technologie
Forma studia:	Kombinovaná
Téma práce:	Nastavení bezpečnosti v prostředí SAP ve společnosti HP TRONIC
Téma práce anglicky:	Security Settings of the SAP Environment in HP TRONIC Company

Zásady pro vypracování

1. Zpracujte literární rešerši zaměřenou na téma bezpečnosti IT a SAP prostředí.
2. Provedte analýzu současného stavu nastavení uživatelských rolí.
3. Navrhněte metodiku nastavení uživatelských rolí z pohledu bezpečnosti.
4. Realizujte navrženou metodiku v systému SAP.
5. Vytvořte program, pomocí kterého bude možné monitorovat dodržování těchto bezpečnostních standardů.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. MARKGRAF, Joe a Alessandro BANZER. SAP System Security Guide. SAP Press, 2018. ISBN 978-1-4932-1481-5.
2. CAVALLERI, Andrea a Massimo MANARA. Authorizations in SAP: 100 Things You Should Know About. SAP Press, 2012. ISBN 978-1-59229-803-7.
3. BANDARI, Kiran. Complete ABAP. SAP Press, 2022. ISBN 978-1-4932-2305-3.
4. DEGHANTANHA, Ali a Kim-Kwang RAYMOND CHOO. Handbook of Big Data and IoT Security. Springer Cham, 2019. ISBN 978-3-030-10542-6.
5. Security Administration Guide [online]. 2022-09-16, [cit. 2022-11-17]. Dostupné z: https://help.sap.com/doc/a6115f7abc2b1014bf21a063974f889e/16.0.4.3/en-US/Security_Administration_Guide_en.pdf
6. BUDKA, Marek. Analýza SoD (Segregation of Duties) konfliktů na platformě SAP Cloud Platform [online]. Praha, 2018 [cit. 2022-11-17]. Dostupné z: https://vskp.vse.cz/72563_analyza-sod-segregation-of-duties-konfliktu-na-platforme-sap-cloud-platform. Diplomová. Vysoká škola ekonomická v Praze. Vedoucí práce doc. Ing. Jan Pour, CSc.

Vedoucí diplomové práce: **doc. Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Konzultant diplomové práce: **Ing. Jakub Verbovský**
HP Tronic a.s.

Datum zadání diplomové práce: **2. prosince 2022**

Termín odevzdání diplomové práce: **1. června 2023**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 8. prosince 2022

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomové práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky. Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 30. 5. 2023

Bc. Jiří Trojan, v.r.

podpis studenta

ABSTRAKT

Tato diplomová práce se zaměřuje na problematiku nastavení bezpečnosti prostředí systému SAP z hlediska uživatelských oprávnění. Teoretická část práce se věnuje podnikovým informačním systémům, s důrazem na systém SAP ERP. V praktické části práce je provedena analýza současného stavu nastavení uživatelských oprávnění v systému. Na základě výsledků analýzy je navržena metodika pro nastavení uživatelských oprávnění. Navržená metodika je využita k úpravě stávajících rolí a vytvoření nových rolí podle stanovených kritérií.

Klíčová slova: podnikové informační systémy, bezpečnost, uživatelská oprávnění, rozdělení pravomocí, SAP, ERP, ABAP, databáze, transakce

ABSTRACT

This master's thesis deals with the issue of configuring security in the SAP environment from the perspective of user authorization. The theoretical part of the thesis focuses on enterprise information systems, with a particular emphasis on the SAP ERP system. In the practical part of the thesis, an analysis of the current state of user authorization settings in the system is performed. Based on the analysis results, a methodology for user authorization management has been proposed. The proposed methodology is used to modify existing roles and create new roles according to the defined criteria.

Keywords: enterprise information systems, security, user authorization, segregation of duties, SAP, ERP, ABAP, database, transaction

Rád bych touto cestou poděkoval panu děkanovi doc. Ing. Jiřímu Vojtěškovi, Ph.D., jakožto vedoucímu diplomové práce za cenné rady a připomínky, které mi během realizace této práce poskytl. Zároveň bych chtěl poděkovat konzultantům z oddělení správy a vývoje SAP společnosti HP TRONIC Zlín, spol. s r. o. za odborné rady při zpracování praktické části diplomové práce. Také bych rád poděkoval své rodině za neustálou podporu po celou dobu studia.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD	10
I TEORETICKÁ ČÁST	12
1 HP TRONIC ZLÍN.....	13
1.1 MALOOBCHODNÍ ZNAČKY	13
1.2 VELKOOBCHODNÍ ZNAČKY.....	14
2 PODNIKOVÉ INFORMAČNÍ SYSTÉMY	15
2.1 EKONOMICKÝ SOFTWARE.....	15
2.2 ENTERPRISE RESOURCE PLANNING	16
2.3 KLASIFIKACE INFORMAČNÍCH SYSTÉMŮ	16
2.4 KLASIFIKACE ERP SYSTÉMŮ PODLE FUNKČNÍHO ZAMĚŘENÍ	18
2.5 TŘÍVRSTVÁ ARCHITEKTURA	18
2.6 DODAVATELE ERP SYSTÉMŮ.....	19
2.6.1 Lídři	21
2.6.2 Vyzyvatelé	22
2.6.3 Vizionáři	22
2.6.4 Specializovaní hráči.....	22
3 PODNIKOVÝ INFORMAČNÍ SYSTÉM SAP	23
3.1 VÝVOJ SYSTÉMU SAP	23
3.2 MODULY SYSTÉMU SAP.....	24
3.2.1 Modul Finanční účetnictví a Vnitřní účetnictví	24
3.2.2 Modul Řízení kvality.....	26
3.3 TECHNOLOGICKÉ ZÁKLADY SYSTÉMU SAP	26
3.3.1 Měřítka výkonu SAPS.....	26
3.3.2 Servery.....	27
3.4 ARCHITEKTURA SYSTÉMU	27
3.4.1 SAP GUI.....	28
3.4.2 SAP Netweaver	29
3.4.3 Databáze SAP HANA	29
3.5 PROGRAMOVACÍ JAZYK ABAP.....	30
3.6 DYNPRO	30
3.7 TRANSAKCE	30
3.8 MOŽNOSTI PŘIZPŮSOBENÍ SYSTÉMU	31
3.8.1 Customizing.....	31

3.8.2	Rozšíření standardu SAP	31
3.8.3	Vlastní vývoj	31
3.8.4	Změna standardu	31
4	BEZPEČNOST PROSTŘEDÍ SAP	32
4.1	AUTENTIZACE UŽIVATELŮ	32
4.1.1	Single Sign-On	33
4.2	PRINCIP ROZDĚLENÍ PRAVOCOMÍ	34
4.3	PRINCIP MINIMÁLNÍCH PRAVOMOCÍ.....	35
4.4	SYSTÉMOVÉ PARAMETRY	35
4.5	SYSTÉMOVÉ PROFILY	35
4.6	ZAMYKÁNÍ TRANSAKcí	36
4.7	SPRÁVA UŽIVATELŮ	37
4.8	NASTAVOVÁNÍ AUTORIZACí.....	39
4.8.1	Uživatelské role	39
4.8.2	Uživatelské profily	40
4.8.3	Chyba autorizace.....	41
4.9	ZAZNAMENÁVÁNÍ ZMĚN	41
II	PRAKTICKÁ ČÁST	42
5	SYSTÉM SAP VE SPOLEČNOSTI HP TRONIC ZLÍN.....	43
5.1	MODULY VYUŽÍVANÉ VE SPOLEČNOSTI HP TRONIC.....	43
5.2	SAP S/4HANA A UŽIVATELSKÁ OPRÁVNĚNÍ.....	44
5.2.1	Zobrazení uživatelských oprávnění v transakci DBACOCKPIT .	44
6	ANALÝZA SOUČASNÉHO STAVU NASTAVENÍ UŽIVATEL- SKÝCH ROLÍ	46
6.1	STANDARDNÍ SAP TRANSAKCE UMOŽŇUJÍCÍ PŘEHLED UŽIVATELŮ	46
6.1.1	Transakce SUIM.....	46
6.1.2	Transakce PFCG	48
6.2	JEDNOTLIVÉ KROKY ANALÝZY	48
6.3	ANALÝZA POČTU SPUSTITELNÝCH TRANSAKcí DLE UŽIVATELE	49
6.4	ANALÝZA KRITICKÝCH OPRÁVNĚNÍ.....	51
6.5	ANALÝZA KRITICKÝCH UŽIVATELSKÝCH OPRÁVNĚNÍ U NEJPOU- ŽÍVANĚJŠÍCH ROLÍ.....	53
6.5.1	Role Z_HPT_USER	54
6.5.2	Role Z_USER_TEMPORARY	56
6.5.3	Seznam rolí obsahující kritická oprávnění	59

6.6	ANALÝZA NASTAVENÍ SoD	60
6.7	ANALÝZA NASTAVENÍ SYSTÉMOVÝCH PARAMETRŮ	60
6.7.1	Kontrola zakázaných hesel	61
6.7.2	Kontrola parametrů hesla	61
7	NÁVRH A REALIZACE NASTAVENÍ BEZPEČNOSTI	62
7.1	VYTVOŘENÍ TESTOVACÍHO UŽIVATELE.....	62
7.1.1	Vytvoření skupiny uživatelů	63
7.2	METODIKA NASTAVENÍ UŽIVATELSKÝCH ROLÍ	65
7.3	ÚPRAVA STÁVAJÍCÍ ROLE	65
7.3.1	Úprava role Z_HPT_USER	66
7.4	REALIZACE METODIKY U NASTAVENÍ NOVÝCH ROLÍ	67
7.4.1	Role pro změnu uživatelských oprávnění Z_HPT_ROLE.....	67
7.4.2	Role udělující obecná oprávnění Z_HPT_DEFAULT	69
7.4.3	Vytvoření odvozené role z Z_HPT_DEFAULT	70
7.4.4	Role zaměřená na finance Z_HPT_FINANCE	70
7.5	REALIZACE ROZDĚLENÍ PRAVOMOCÍ.....	71
7.5.1	Role umožňující založení a změnu rolí	71
7.5.2	Role umožňující generování rolí a profilů	72
7.6	NASTAVENÍ SYSTÉMOVÝCH PARAMETRŮ HESLA.....	72
7.7	ZAMKNUTÍ TRANSAKČÍ	73
8	VYTVOŘENÍ KONTROLNÍHO PROGRAMU.....	75
8.1	NÁVRH PŘEHLEDOVÉ TRANSAKCE ZHP_AUTH_VIEW	75
8.2	REALIZACE PROGRAMU ZHP_JT_AUT_VIEW	75
8.2.1	Realizace třídy ZCL_JT_AUT_VIEW	78
8.2.2	Metody pro získání dat z databáze	80
8.2.3	Vstupní obrazovka transakce ZHP_AUTH_VIEW	85
8.2.4	Customizační tabulka ZHP_AUTH_METHODS	85
8.2.5	Transportování objektů z vývojového prostředí	86
	ZÁVĚR.....	87
	SEZNAM POUŽITÉ LITERATURY	89
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	93
	SEZNAM OBRÁZKŮ	94
	SEZNAM TABULEK	96
	SEZNAM PŘÍLOH	97

ÚVOD

V dnešním dynamickém světě, charakterizovaném rychlým rozvojem a neustálým představováním nových technologií, se stává stěžejní skutečností, že téměř všechny společnosti, bez ohledu na jejich velikost, jsou klíčově závislé na specifických technologických řešeních. Jednou z nejčastěji využívaných technologií jsou podnikové informační systémy. Tyto systémy sehrávají klíčovou roli v prosperitě a fungování společnosti. Správné nastavení bezpečnostních opatření těchto systémů má zásadní vliv na provoz celé společnosti. Nesprávné nastavení bezpečnosti může velmi negativně ovlivnit konkurenceschopnost podniku. Proto je důležité klást velký důraz na zabezpečení těchto systémů proti vnějším i vnitřním hrozbám.

Jednou z celosvětově nejvýznamnějších společností poskytující systémy pro plánování podnikových zdrojů (ERP) je německá společnost SAP SE, která poskytuje stejnojmenný systém SAP. Diplomová práce se zabývá zabezpečením prostředí tohoto systému, neboť je využíván i ve společnosti HP TRONIC Zlín, spol. s r. o.

Hlavním tématem této diplomové práce je zabezpečení systému SAP proti vnitřním hrozbám. Zejména prostřednictvím analýzy a nastavení uživatelských rolí. Cílem je navrhnout nastavení, které zvýší odolnost systému vůči lidskému faktoru, ať už se jedná o úmyslné poškození společnosti nebo z nedorozumění. Systém SAP nabízí robustní možnosti nastavení bezpečnostních opatření a monitorovacích prvků. Společnost HP TRONIC Zlín využívá systém SAP pro zpracování téměř všech podnikových procesů, jako jsou objednávky, zakázky, faktury, reklamace nebo například k automatizaci všech pohybů na skladech. Jakákoli z těchto funkcionalit může být ohrožena v případě, že se systémem bude pracovat nezkušený uživatel, který bude mít příliš velké oprávnění a nebude si vědom možného dopadu jednotlivých úkonů. Zkušený uživatel by naopak mohl zneužít nadměrných pravomocí s úmyslem poškodit společnost nebo dosáhnout vlastního obohacení.

V úvodu teoretické části diplomové práce je stručně zmíněna historie a značky společnosti HP TRONIC Zlín. Následující kapitoly se zaměřují na hlavní témata práce. Nejdříve je popsána problematika podnikových informačních systémů, včetně jejich rozdělení, klasifikace a nejběžnější architektury. Kapitola je uzavřena stručným seznamem v současnosti největších dodavatelů ERP systémů. Následují dvě kapitoly zaměřené na systém plánování podnikových zdrojů SAP, který je klíčovou součástí praktické části diplomové práce. První z nich se zabývá podrobným seznámením se samotným systémem SAP. Jako je například jeho postupný vývoj, jednotlivé moduly, technologický základ, architektura a další detaily. Druhá z těchto kapitol je zaměřena na způsoby, kterými je možné zajistit zabezpečení systému SAP.

Praktická část se v úvodu zabývá bližším představením fungování systému SAP ve společnosti HP TRONIC. V navazující kapitole je zpracována analýza současného stavu nastavení uživatelských oprávnění u nejpoužívanějších rolí s částečným zaměřením na jeden z modulů systému, kterým je finanční a vnitřní účetnictví. Na základě výsledků analýzy dochází k provedení úprav kritických oprávnění u nejpoužívanějších rolí. U nejobsáhlejší z těchto rolí došlo ke změně, kdy byla nahrazena novou rolí. Jejím účelem byla redukce počtu autorizačních objektů, na co nejméně, při zachování potřebné funkcionality. V závěru diplomové práce došlo k vytvoření programu, který je možný využít pro analýzu uživatelských oprávnění v podobě přiřazených rolí, profilů a spustitelných transakcí.

I. TEORETICKÁ ČÁST

1 HP TRONIC ZLÍN

Firma HP TRONIC Zlín, spol. s r.o. byla založena v roce 1990 ve Zlíně panem Milanem Hradilem a panem Pastyříkem. Z iniciál jejich příjmení vychází i název společnosti. V době založení firmy se zaměřovala především na maloobchodní prodej domácích elektrospotřebičů a spotřebního zboží. [1]

V následujících letech došlo k rozšíření firmy o činnost velkoobchodního prodeje, kdy se začala budovat odběratelská síť po celé České republice. [1]



Obrázek 1.1 Logo společnosti HP TRONIC [2]

Společnost se dále orientuje i na cestovní ruch a gastronomii. Příkladem může být restaurace Bistrotéka Valachy ve Zlíně nebo síť hotelů ve Velkých Karlovicích.

V současné době firma zaměstnává přes 3000 zaměstnanců. Hlavní sídlo společnosti je na Obchodním domě ve Zlíně.

1.1 Maloobchodní značky

Klíčovými maloobchodními značkami jsou Datart, ETA a Kasa.cz v České republice. Slovenskou alternativou webu Kasa.cz je web Hej.sk. [3]

Dlouhou dobu byla pro HP TRONIC nejdůležitější maloobchodní značkou EURONICS. V roce 2017 došlo ke spojení společností DATART INTERNATIONAL, a.s. a HP TRONIC Zlín, spol. s r.o., čímž započalo postupné nahrazování všech prodejen EURONICS prodejny Datart. Jedná se o síť internetových a kamenných prodejen zaměřených na elektroniku.

Jednotlivé prodejny nemají za úkol pouze prodej elektroniky, ale jsou využívány také, jako prostory pro skladování zboží či výdej nakoupeného zboží přes internet. Celkový počet maloobchodních prodejen ETA a Datart v České a Slovenské republice je více než 180. [3]

Kasa.cz a Hej.sk jsou výhradně internetové obchody, zabývající se prodejem především bazarového zboží. [3]

1.2 Velkoobchodní značky

Velkoobchod HP TRONIC Zlín, spol. s r. o. je exkluzivním velkoobchodním distributorem značek ETA, Hyundai, GoGEN, JVC, Gallet. [3]

Přední z těchto značek je česká značka ETA, založená v roce 1943 pod jménem Elektrotechnická akciová společnost ESA. Společnost se původně zaměřovala na výrobu elektrických žehliček a dalších spotřebičů pro domácnost. Majitelem společnosti ETA se společnost HP TRONIC Zlín stala v roce 2011. [7]



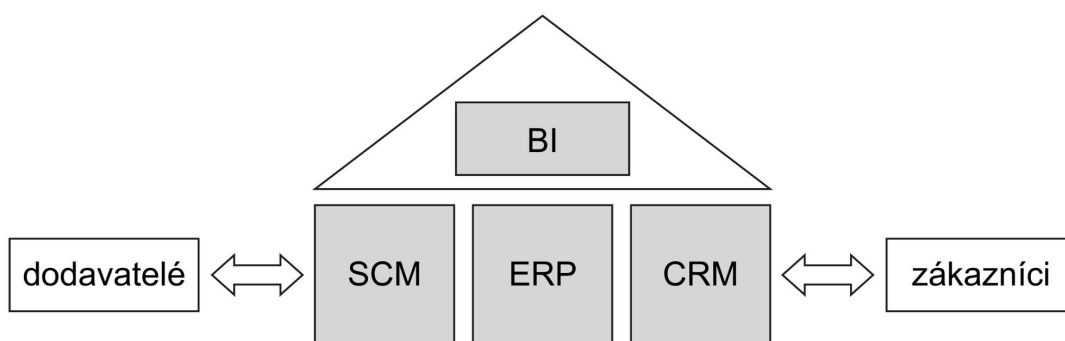
Obrázek 1.2 Logo značky ETA [4]

2 PODNIKOVÉ INFORMAČNÍ SYSTÉMY

Podnikové informační systémy jsou kombinací nástrojů, softwaru a personálu, které shromažďují, zpracovávají a ukládají podniková data. Tato data jsou využívána k vytváření informací, které slouží k řízení podnikových operací, plnění podnikových cílů a přijímání manažerských rozhodnutí. [5]

Podle holisticko-procesní klasifikace je podnikový informační systém sestaven z následujících modulů:

1. SCM - Systém, který řídí dodavatelský řetězec. Jeho součástí bývá systém sloužící k plánování výroby (APS).
2. ERP - Jádro podnikových informačních systémů, které lze rozdělit do dvou skupin, a to na ekonomický software a enterprise resource planning (ERP), v českém jazyce plánování podnikových zdrojů.
3. CRM - Systém řídící procesy směřované zákazníkům.
4. BI - Sbírá specifická data z jednotlivých modulů a externích zdrojů. Z těchto dat vytváří výstupy, které využívá podnikový management. [6]



Obrázek 2.1 Schéma podnikových informačních systémů [6]

2.1 Ekonomický software

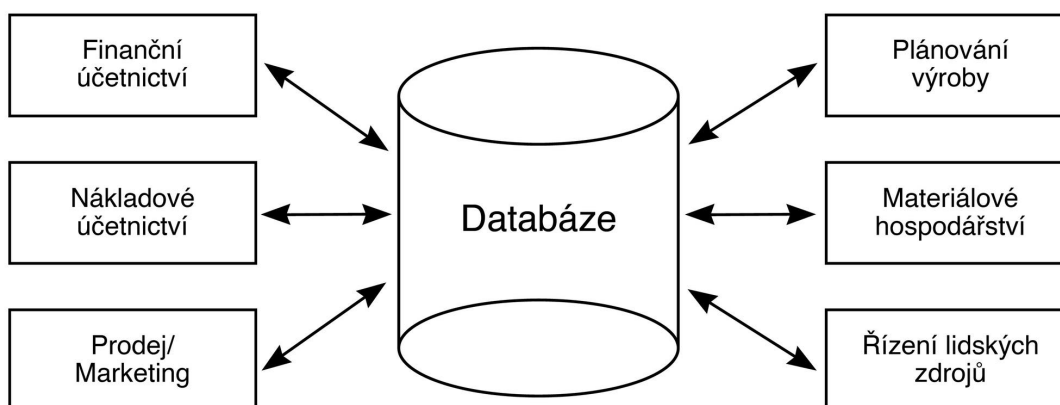
Ekonomický software je obvykle zaměřen na řízení podnikové agendy z některé oblasti v podobě ekonomiky, logistiky, výroby nebo řízení lidských zdrojů. Avšak nemají dostatečný rozsah systému, hloubku funkcionality nebo míru technologické vyspělosti, aby je bylo možné považovat za ERP systémy. [5]

Aplikace POHODA od české firmy STORMWARE s.r.o. je typickým příkladem ekonomického a účetního softwaru. [8]

2.2 Enterprise resource planning

ERP jsou systémy skládající se z množiny aplikací, které mají rozdílné účely, avšak sdílejí stejnou databázi a systém. Tato vlastnost jim umožňuje zajistit podporu pro všechny procesy související s podnikovou ekonomikou. Mezi tyto činnosti obvykle patří finanční účetnictví, nákup, logistika, prodej, expedice, plánování a řízení výroby nebo řízení lidských zdrojů. [6]

Díky sdílené databázi všechny aplikace v systému sdílejí stejná data. Tato data lze zobrazovat, dále zpracovávat nebo rozšiřovat o údaje specifické pro jednotlivá oddělení, což je jeden z charakteristických rysů ERP systémů. Přímé propojení všech obchodních procesů je největším plusem integrace těchto systémů. [7]



Obrázek 2.2 Způsob integrace dat v ERP systémech [5]

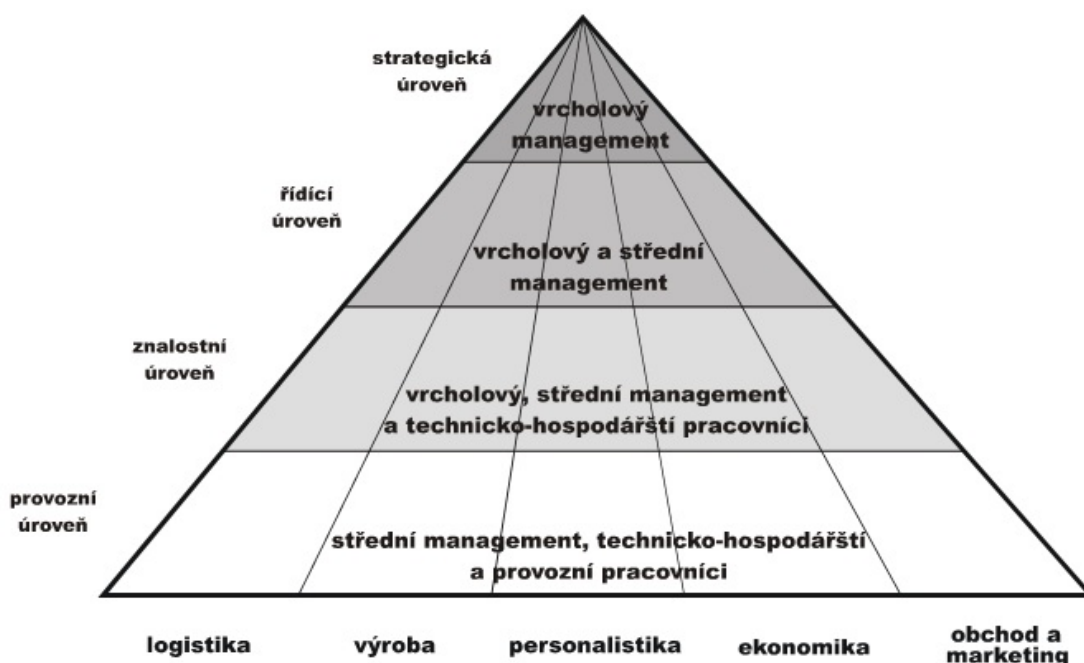
Většina aplikací ERP systémů sdílí podobnou koncepci vývoje, která umožňuje začlenění samostatně vyvinutých funkcí do systému jako celek. Tento vývojový koncept aplikace je založen na vrstveném modelu. Příkladem lze uvést systém SAP používající specifický programovací jazyk ABAP, který spolu s datovým slovníkem využívají i všechny ostatní softwarové moduly k provádění obecných služeb potřebných pro všechny další dílčí funkce. Tento výchozí systém je nejnižší úroveň a obsahuje všechny potřebné obecné služby. Integrované systémy mimo jiné pracují s jednotnými standardy, které zaručují konkrétní vzhled. [7]

Aby informační systém mohl být označen kategorie ERP, tak musí být schopen pokrytí všech hlavních interních podnikových procesů na všech organizačních úrovních. [5]

2.3 Klasifikace informačních systémů

Organizační úrovně informačních systémů se rozdělují do čtyř základních úrovní a to na provozní, znalostní, řídicí a strategickou. Samostatné úrovně neposkytují

všechny informace, které management potřebuje. Žádná z těchto úrovní zároveň nepředstavuje samostatnou celistvou entitu.



Obrázek 2.3 Informační pyramida podle organizačních úrovní podniku [5]

- Provozní úroveň se zabývá zpracováním informace týkající se běžné podnikové agendy jako například realizace nákupu a prodeje, příjmy plateb a výplat.
- Znalostní úroveň se zaměřuje na rozšiřování znalostní báze organizace, osobní informatiku a tok dokumentů. Jsou zde obsaženy nejen klientské aplikace podnikových informačních systémů, ale také veškeré kancelářské aplikace.
- Řídící úroveň vyžaduje informace k podpoře rozhodování středního a vrcholového managementu a k plnění administrativních úkolů.
- Na strategické úrovni se identifikují dlouhodobé trendy, jak uvnitř, tak vně organizace. Její hlavní úlohou je poskytovat vrcholovému managementu informace o možných změnách a posoudit, zda je schopen adekvátně reagovat na tyto změny. [5]

Jednotlivé úrovně se vždy zabývají některým z několika interních procesů: logistiky, výroby, personalistiky, ekonomiky, obchodu nebo marketingu. Z nichž jsou první čtyři klíčové. Každá úroveň vyžaduje specifický druh informací a také způsob nakládání s nimi. [5]

2.4 Klasifikace ERP systémů podle funkčního zaměření

ERP systémy jsou klasifikovány do tří skupin podle toho, jak dobře dokáží pokrýt všechny čtyři klíčové interní procesy podniku.

Tabulka 2.1 Klasifikace ERP systémů podle funkčního zaměření [5]

ERP Systém	Charakteristika	Výhody	Nevýhody
All-in-One	Systémy, které zahrnují všechny klíčové interní podnikové procesy.	Vysoká úroveň propojení dílčích aplikací v systému.	Méně detailní funkcionality, nákladná úprava na míru.
Best-of-Breed	Systémy orientující se pouze na některé z klíčových procesů.	Obsažené procesy mají velmi detailní funkcionality.	Potenciálně obtížnější integrace podnikových procesů.
Lite ERP	Odlehčená verze ERP systému. Je zaměřený na trh malých firem.	Nízká cena.	Omezená funkcionality, počet uživatelů nebo bez možnosti rozšíření.

2.5 Třívrstvá architektura

Třívrstvá architektura nebo také tříúrovňová architektura je známý a zavedený design softwarových aplikací, který je rozděluje do tří vrstev.

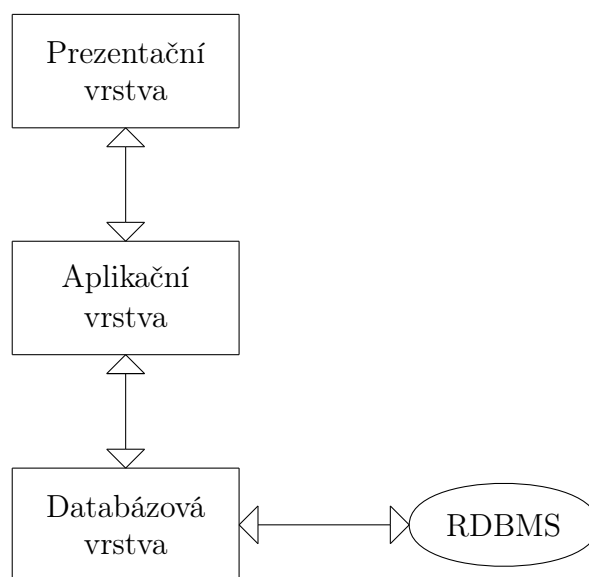
- Prezentační vrstva má na starosti uživatelské rozhraní a komunikační vrstvu aplikace. Což je místo, kde koncoví uživatelé pracují se softwarem. Jejím hlavním cílem je zobrazování informací uživateli a sběr vstupních dat od něj. Tato vrchní vrstva může fungovat například v desktopové aplikaci, webovém prohlížeči nebo grafickém uživatelském rozhraní (GUI).
- Aplikační vrstva, také někdy označovaná jako logická vrstva, je jádrem aplikace. V této vrstvě se data shromážděná v prezentační vrstvě zpracovávají pomocí obchodní logiky nebo určité sady obchodních pravidel. Často ve srovnání s daty shromážděnými v datové vrstvě. Data v datové vrstvě mohou být také přidávána, odebírána nebo upravována aplikační vrstvou.
- Datová vrstva (databázová vrstva) - v této vrstvě se ukládají data zpracovávané v aplikační vrstvě. Může to být databázový server NoSQL (MongoDB), nebo relační systém správy databází jako například PostgreSQL, MySQL, Oracle, SAP HANA nebo Microsoft SQL Server. [9]

Hlavní výhodou tříúrovňové architektury je to, že každá úroveň má svou vlastní logickou a fyzickou funkcionality. Každá úroveň může běžet na rozdílném operačním systému a serveru podle toho, co je k dané úrovni nejvhodnější. Díky tomu,

že každá úroveň běží na vlastní infrastruktuře, tak jednotlivé úrovně mohou být optimalizovány a rozšiřovány bez toho, aby byly ovlivněny ostatní. [9]

Další výhody oproti jedno či dvou úrovňové architektuře jsou následující:

- Lepší škálovatelnost: jakákoli vrstva může být rozšířena nezávisle na ostatních dle potřeb.
- Lepší spolehlivost: výpadek jedné vrstvy neovlivní výkon ostatních vrstev.
- Lepší bezpečnost: z důvodu, že prezentační a datová vrstva mezi sebou nemohou komunikovat na přímo. Správně navržená aplikační vrstva může fungovat jako interní firewall. Je tedy schopna bránit útokům, kterými jsou například tzv. SQL injections. [9]



Obrázek 2.4 Schéma třívrstvé architektury [25]

2.6 Dodavatelé ERP systémů

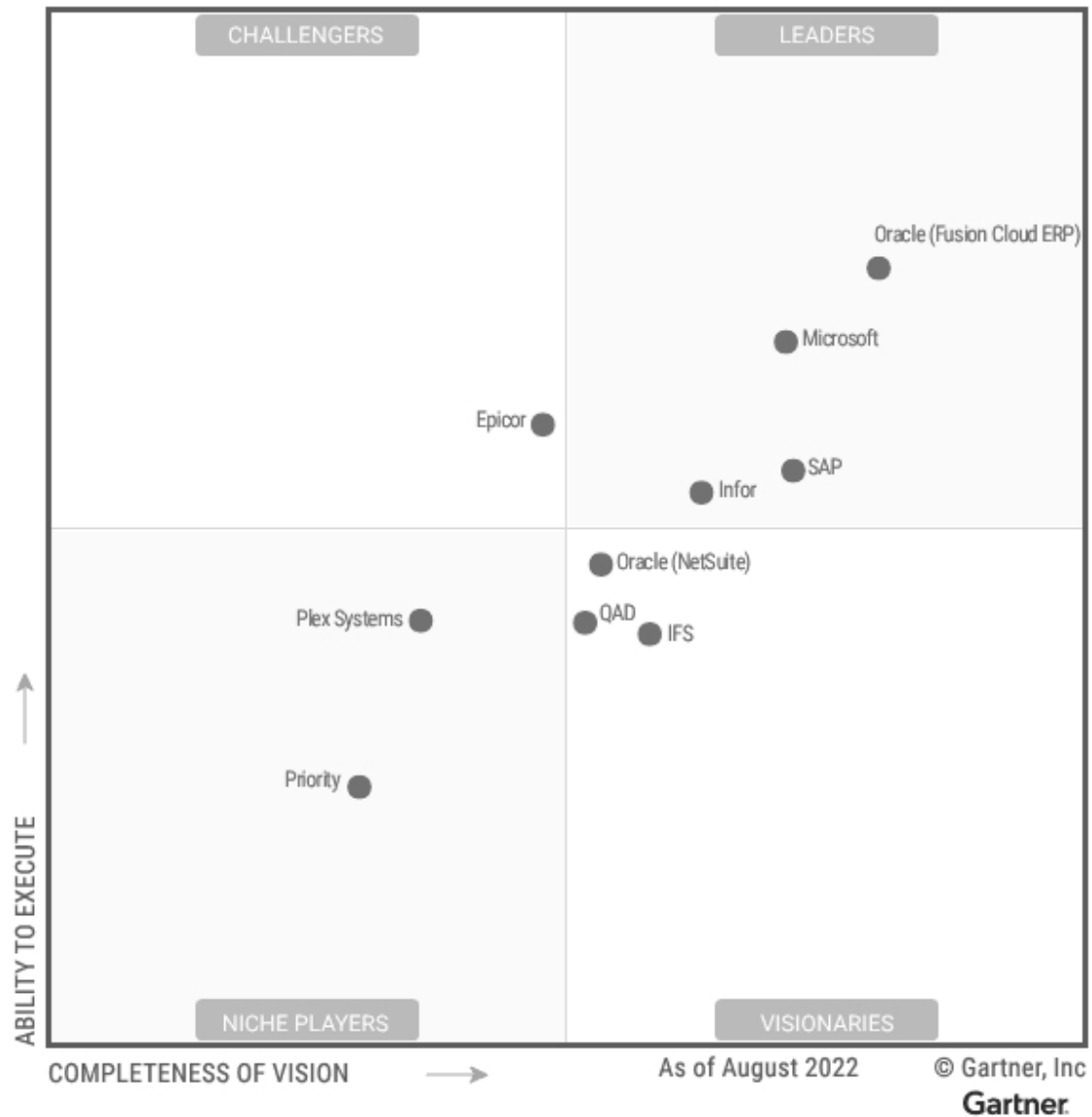
Existuje velká škála společností poskytujících systémy ERP. V roce 2022 provedla americká společnost Gartner, specializující se na výzkum a poradenství v oblasti IS/ICT technologií, výzkum mezi předními dodavateli ERP systémů pomocí svého vlastního hodnotícího modelu Magic Quadrant (česky Magický Kvadrant). [10]

Techniku průzkumu a analýzu trhu známou jako Magický kvadrant vyvinula a patentovala společnost Gartner. Pomocí magického kvadrantu se vizualizuje a porovnává relativní postavení různých společností na určitém trhu. [11]

Magický kvadrant se skládá ze čtyř kvadrantů, které jsou rozděleny do dvou os. Horizontální osy představují „úplnost řešení“ (anglicky „completeness of vision“)

a vertikální osy představují „schopnost vykonávání“ (anglicky „ability to execute“). Tyto dvě osy umožňují porovnat různé společnosti v oblastech, jako jsou například IT řešení, firemní software nebo služby cloud computing. Kvadranty jsou označeny jako „lídři“, „vyzyvatelé“, „vizionáři“ a „specializovaní hráči“. [11]

V roce 2022 byly společnostmi Gartner provedeny celkem dva výzkumy v oblasti systémů ERP, a to na ERP systémy pro podniky, které jsou zaměřené na produkty a na služby. Tato kapitola bude zaměřena na studii první zmíněné oblasti.



Obrázek 2.5 Vizualizace dodavatelů ERP pomocí metodologie Magic Quadrant [10]

Gartner definuje trh systémů plánování podnikových zdrojů u podniků, jenž jsou zaměřené na výrobky jako trh aplikačních technologií, které podporují automatizaci provozních a finančních činností při výrobě, distribuci, dodávkách a servisu zboží. Systémy ERP považuje za základní technologii pro fungování podniků. [10]

Gartner udává, že hlavní schopnosti ERP balíčků zaměřených na produkty jsou:

- Provozní systém ERP: řízení poptávky, řízení objednávek, plánování materiálových potřeb, řízení zásob, dodavatelský řetězec/přímé nákupy, možnosti řízení výroby a distribuce/logistika.
- Funkce správy financí: finanční účetnictví, dílčí účetnictví, konsolidace a finanční výkaznictví. [10]

Mezi volitelné funkce produktově orientovaných ERP balíčků patří:

- Pořízení a nákupy zboží: správa požadavků a nákupních objednávek na nepřímé zboží, služby a investiční vybavení.
- Řízení lidského kapitálu.
- Specializované, oborově specifické moduly nebo aplikace: jedná se mimo jiné o moduly používané pro konfigurace na zakázku, výrobu na zakázku a komplexnější aplikační řešení, jako jsou moduly pro správu podnikových aktiv nebo správu životního cyklu produktu. [10]

2.6.1 Lídři

Lídři nabízejí nejmodernější služby, které splňují současné požadavky trhu. Tito poskytovatelé služeb navíc disponují vizí, která je potřebná k tomu, aby si udrželi dominantní postavení v závislosti na změnách trhu. Lídři věnují pozornost zboží, které v současnosti nabízejí a zároveň do něj investují, aby ovlivnili celkový směr trhu. [11]

- Oracle (Fusion Cloud ERP) - jedná se o vysoce konfigurovatelné řešení pro střední a velké podniky s globálními klienty. Poskytuje integrovanou sadu administrativních a logistických provozních funkcí podpořenou společným datovým modelem. Je vhodné pro podniky, které potřebují komplexní sadu funkcí pro složité obchodní procesy dodavatelského řetězce, výroby a financí. Oracle Fusion Cloud ERP je spravován v datových centrech společnosti Oracle.
- SAP - v tomto hodnocení byl zvolen model nasazení S/4HANA Cloud, který ve srovnání s lokální verzí (on-premise) má mírně odlišnou sadu funkcí. Pro organizace, které potřebují kompletní sadu funkcí pro složité obchodní operace v oblasti dodavatelského řetězce, výroby a financí, je S/4HANA Cloud ideálním produktem. [10]

Systém SAP je mnohem podrobněji popsán v následujících kapitolách diplomové práce.

2.6.2 Vyzyvatelé

Vyzyvatelé mají dobrou pozici pro implementaci, ale nemusí mít dostatečně robustní strategii, aby byli schopni i nadále nabízet produkty nebo služby se dostatečnou přidanou hodnotou v dlouhodobém horizontu. Často mají dostatek lidských a finančních zdrojů, ale mohou postrádat potřebnou vizi, invenci nebo celkovou znalost trhu. Vyzyvatelé mohou příležitostně poskytovat zboží, které ovládá značnou část trhu, jehož význam časem slábne. Rozšířením své vize mají šanci dostat se do kvadrantu lídrů. [11]

2.6.3 Vizionáři

Vizionáři se shodují s pohledem společnosti Gartner ohledně budoucího vývoje trhu, ale není jasné, zda budou schopni poskytnout trhu řešení odpovídající jejich vizi. Tato situace je typická pro rozvíjející se trhy. Na rozvinutějších trzích může takový postoj představovat konkurenční strategii menšího dodavatele (prodávajícího například inovace před hlavní vlnou poptávky) nebo většího poskytovatele, který se chce odlišit od konkurence. Vizionáři patří do skupiny, jež v očích prodejců a zákazníků může přinést větší odměnu, pokud podstoupí větší riziko. Často nabízejí nové technologie, služby nebo obchodní modely, ale obvykle jim chybí finanční zdroje, pokročilé služby, podpora prodeje a distribuční síť. [11]

2.6.4 Specializovaní hráči

Vzhledem k omezené schopnosti nebo kapacitě inovovat a překonávat ostatní dodavatele uspějí pouze v určité tržní mezeře. Může tomu tak být proto, že se jedná o nové účastníky trhu nebo se soustředí pouze na určitou vlastnost nebo zeměpisnou oblast (např. zavedené technologické startupy). Hodnocení specializovaných účastníků je často obtížnější než hodnocení dodavatelů v ostatních kvadrantech. Zatímco někteří mohou expandovat, jiní nemusí být schopni držet krok s potřebami trhu, protože nedosahují dobrých výsledků. [11]

3 PODNIKOVÝ INFORMAČNÍ SYSTÉM SAP

Systém SAP není klasickou desktopovou aplikací, jako je například Microsoft Excel nebo Word, které jsou používány k provádění jednotlivých úkolů. Na rozdíl od nich SAP představuje aplikaci pro podnikové účely. Jedná se o ERP systém klasifikace All-in-One. Lze jej využívat nejen ke všem klíčovým interním podnikovým procesům, ale i k mnoha dalším. [7]



Obrázek 3.1 Logo společnosti SAP [15]

Systém SAP je produktem stejnojmenné německé společnosti SAP sídlící ve Walldorfu v Německu. Název SAP je zkratkou německého názvu Systemanalyse und Programmentwicklung, což se nejčastěji překládá do anglického jazyka jako Systems, Applications and Products in data processing. [14]

Společnost byla založena v roce 1972 bývalými zaměstnanci firmy IBM. Jejich vizí bylo vyvinout balík aplikací obsahující všechny možné podnikové funkce. V té době firmy používaly běžně více než deset různých podnikových aplikací. [14]

V současné době zaměstnává přes 110 000 zaměstnanců v 160 zemích světa. SAP uvádí, že 99 ze 100 největších společností světa používá některý z produktů společnosti SAP. [12]

3.1 Vývoj systému SAP

Vize se zakladatelům částečně podařila uskutečnit již v roce 1973, kdy byl vydán software s označením SAP R/1. Ovšem až jeho nástupce SAP R/2, který vyšel o šest let později, bylo možno označit za první ERP systém. K provozu tohoto systému bylo nutné použití sálového počítače. Systém zaznamenal velký úspěch v osmdesátých letech a začátkem let devadesátých. [14]



Obrázek 3.2 Historie verzí produktu SAP [15]

Velkým skokem bylo vydání systému SAP R/3 roce 1992, který již využíval třívrstvou architekturu klient-server. V roce 2004 byla vydána novější verze systému s názvem SAP ECC (či SAP ERP). Hlavním rozdílem mezi SAP R/3 a SAP ECC je to, že ECC je založeno na technologické platformě Netweaver. Ovšem podoba mezi R/3 a ECC je téměř totožná. Tato verze systému nabyla v průběhu let postupně rozšiřována a je v mnoha společnostech je využívána do dnes. [7]

V současné době je tomu tak i ve společnosti HP TRONIC Zlín, která plánuje přechod na nejnovější verzi systému SAP v roce 2024.

Dalším důležitým milníkem byl rok 2010, ve kterém byla vydána in-memory databáze SAP HANA (High-performance ANalytic Appliance). V současné době je nejaktuálnější verzí systém SAP S/4HANA, který plně využívá výhody databáze HANA. Na rozdíl od předchozích verzí systému neumožňuje využití žádné jiné databáze, než je právě HANA. Jedná se o největší skok systému od roku 1992, kdy byl vydán systém SAP R/3. [17]

Systém SAP S/4HANA poskytuje různé možnosti implementace v podobě lokálního prostředí, cloudu a hybridního systému. Hybridní systém kombinuje výhody soukromí a kontroly lokálního systému s nižšími náklady, větší pamětí a rozsáhlejším přístupem prostředí v cloudu. Jeho nasazení lze přizpůsobit podle potřeb daného podniku. Díky schopnosti efektivně zpracovávat velké objemy dat je systém snadno škálovatelný, takže se může přizpůsobit růstu firmy bez ohrožení bezpečnosti nebo stability. [19]

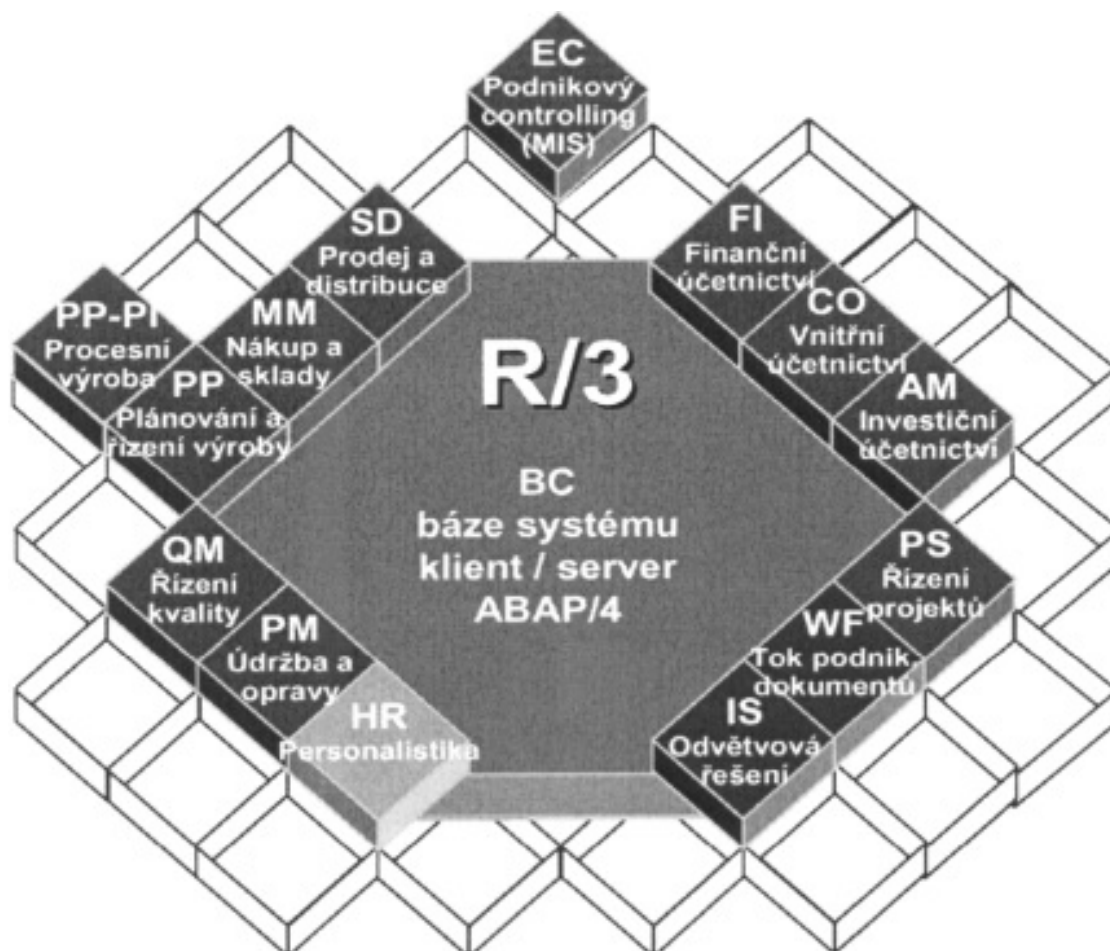
Za zmínku také stojí vlastnost, že veškeré vytvořené aplikace jsou a budou kompatibilní ve všech budoucích verzích systému. Ovšem pokud byla aplikace vytvořena na některé novějších verzích SAP, tak zpětná kompatibilita nemusí být možná.

3.2 Moduly systému SAP

Obrázek 3.3 zobrazuje všechny moduly systému SAP R/3. Přestože systém SAP od této verze prošel značným vývojem, tak hlavní moduly zůstávají stejné. Četnost a množství používání jednotlivých modulů záleží na každé organizaci. Podniky zabývající se výrobou budou hojně využívat modul PP, který například podniky zaměřující se na elektronický prodej vůbec nevyužijí. Ovšem ostatní moduly budou používat v podobné míře.

3.2.1 Modul Finanční účetnictví a Vnitřní účetnictví

SAP FI/CO je jedním ze základních funkčních modulů komponent SAP ERP, které pomáhají organizaci spravovat veškerá finanční data. Hlavním účelem SAP FI/CO je podporovat organizaci při vytváření a zpracování všech finančních výkazů pro



Obrázek 3.3 Funkční moduly produktu SAP R/3 [6]

analýzu a výkaznictví a také pomáhat při efektivním plánování a rozhodování podniku. Modul SAP FI/CO se skládá ze dvou modulů, tj. modulu Finanční účetnictví (FI) a Vnitřní účetnictví (CO), přičemž každý z těchto modulů slouží k provádění specifických finančních procesů. Modul SAP FI se zaměřuje na kompletní finanční výkaznictví a účetnictví, zatímco SAP CO klade důraz na plánování a sledování nákladů. Moduly SAP FI a SAP CO byly původně vydány jako samostatné moduly, ale nyní jsou tyto moduly tak silně integrovány, že je většina lidí označuje jako jeden modul. [20]

Finanční účetnictví je jedním ze základních modulů systému SAP ERP. Slouží k ukládání finančních údajů organizace. Pomáhá analyzovat finanční podmínky společnosti na trhu. Může se integrovat s dalšími moduly SAP, jako jsou SD, PP, MM, QM atd. [20]

Vnitřní účetnictví v každé společnosti pomáhá při sledování, obhajobě a plánování obchodních procesů. Modul CO je přímo propojen s finančním účetnictvím. Organizuje související výdaje do jednoho pohledu. Dále slouží ke zpracování

a nastavení kmenových dat, která evidují údaje o interních zakázkách, ziskových střediscích, nákladových prvcích a mnoho dalších věcí. Modul SAP CO dohlíží na řízení výdajů, úpravy produktů a kalkulaci nákladů. Zahrnuje také prvky spojené s účtováním nákladových středisek, účtováním interních zakázek, analýzou ziskovosti, řízením režijních nákladů atd. [20]

3.2.2 Modul Řízení kvality

Modul SAP Quality Management (QM) pomáhá organizacím při nastavování a řízení postupů kontroly kvality. Jeho cílem je vytvořit dlouhodobé programy řízení kvality, umožnit neustálé zlepšování procesů a předcházet vadám. Možnými výhodami pro společnost jsou nižší provozní náklady, zvýšení spokojenosti zákazníků a dodržování předpisů o kvalitě výroby. [21]

Nákup a sklady (MM), Údržba a opravy (PM), Plánování a řízení výroby (PP), Prodej a distribuce (SD), Finance (FI) a Controlling (CO) jsou jen některé z komponent ECC, se kterými SAP QM spolupracuje. Díky této integraci mohou úlohy z těchto ostatních komponent ECC integrovat úlohy SAP QM. [21]

3.3 Technologické základy systému SAP

Základním prvkem systému SAP je hardware. Hardware se skládá z několika částí, kterými jsou servery, disková úložiště a síťová zařízení. Všechny tyto části musí společně pracovat, aby mohl systém SAP fungovat efektivně. [14]

3.3.1 Měřítka výkonu SAPS

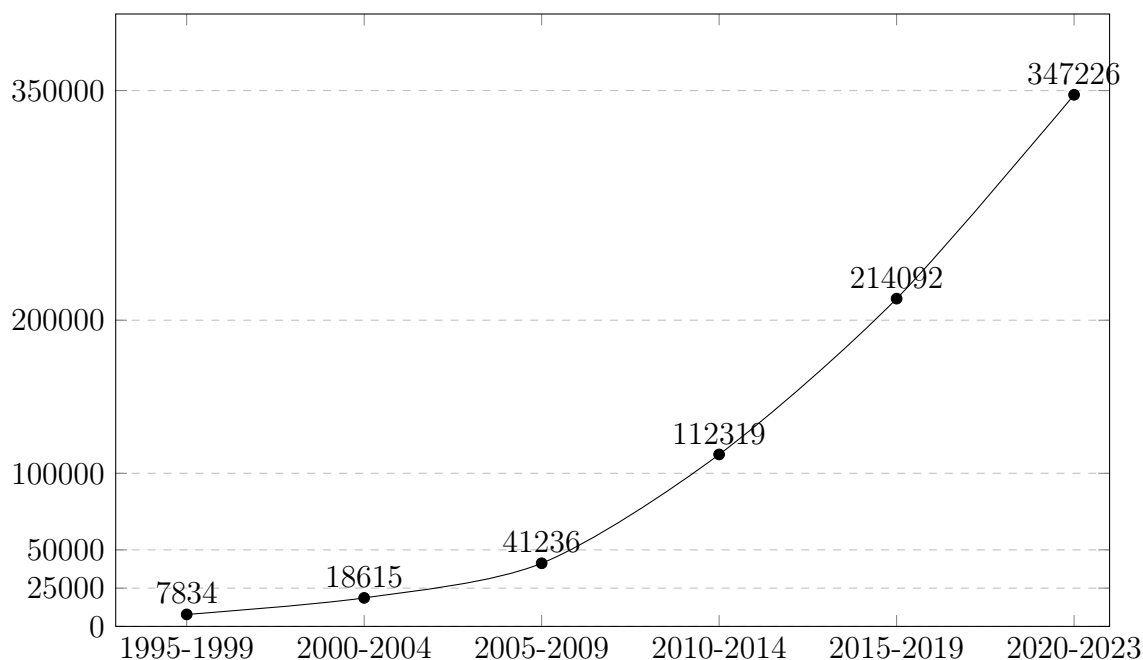
Pomocí jednotek SAPS se hodnotí výkon celého systému SAP, včetně konfigurace softwaru a hardwaru, nikoliv výpočetní výkon samotného hardwaru. Organizace mohou plánovat nákupy a zlepšovat výkon svých systémů SAP pomocí SAPS, aby vyhodnotily výkon, který mohou očekávat od různých konfigurací a hardwaru. Jednotka SAPS je jedinečná pro platformu SAP a její výpočet je postaven na modulu SD softwaru SAP ERP. Jedná se o nejpoužívanější ukazatel efektivity systému SAP. [14]

Podle definice dokáže 1 SAPS zpracovat 20 kompletních zákaznických zakázek za hodinu s maximálním počtem pěti položek na objednávku. Je důležité si uvědomit, že v obchodním procesu, který je základem tohoto ukazatele výkonnosti je 6 různých transakcí. Zmíněných 20 kompletně zpracovaných zákaznických objednávek tedy odpovídá přibližně 60 různým obrazovkám. [14]

3.3.2 Servery

Hardware serverů může běžet přímo ve vlastním datovém centru podniku, či u tradičního poskytovatele outsourcingu nebo v současné době velmi často používanou službou cloud computingu. Ovšem stále platí, že se servery třídí do kategorií daných cenou a výkonem. [14]

Výkon v SAPS



Obrázek 3.4 Graf vývoje průměrného výkonu v SAPS

Výkon technologií prochází neustálým rozvojem. Dle dat, které poskytuje přímo společnost SAP byl ještě před několika lety server s výkonem přesahující sto tisíc SAPS jedním z nejvýkonnějších. V současné době se jedná spíše o podprůměrný server. [22]

Společně s rostoucím výkonem se začala velmi zvyšovat efektivita serverů v podobě Watt/SAPS, kde v současné době výkon jednoho Wattu odpovídá téměř 100 SAPS. [22]

3.4 Architektura systému

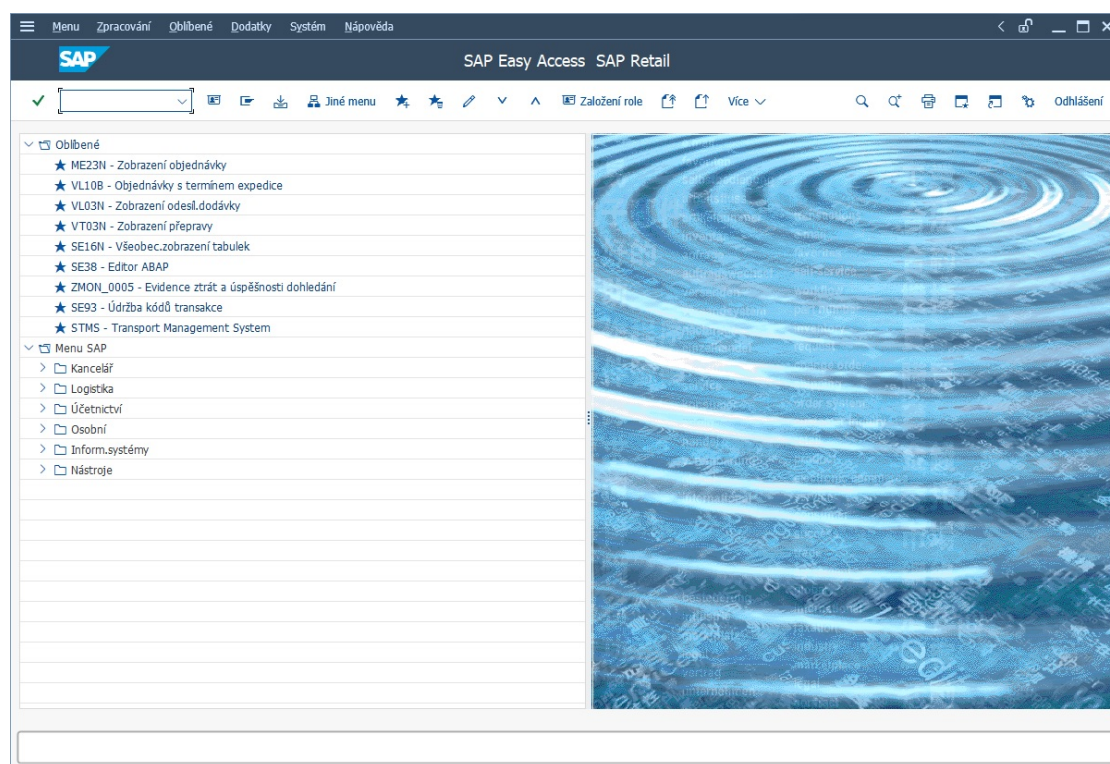
Jak již bylo v úvodu kapitoly zmíněno, tak od verze R/3 je systém SAP založen na třívrstvé architektuře klient-server. Architektura umožňuje kooperativní zpracování informací u úkolů, ke kterým je potřeba více softwarových komponent. Výhodou je to, že tyto komponenty nemusejí být nainstalovány na jednom počítači. [7]

Za jednotlivé vrstvy třívrstvé architektury od verze SAP ECC lze považovat SAP GUI, SAP Netweaver a Databáze.

3.4.1 SAP GUI

SAP GUI je desktopový klient, který umožňuje uživatelům přistupovat k různým aplikacím a modulům v rámci systému SAP. Jedná se o jednoduché a intuitivní uživatelské rozhraní, které umožňuje uživatelům pracovat s různými funkcemi SAP. Uživatelé mohou pracovat s aplikacemi a moduly SAP prostřednictvím grafických ikon, nabídek a oken, což umožňuje snadnou navigaci a intuitivní používání aplikace. [14]

V SAP GUI si uživatel může vybrat jeden z celkem šesti různých motivů, které byly postupem času vytvořeny. U většiny z těchto motivů je možné si navíc vybrat barevný pod motiv v podobě tmavé či světlé.



Obrázek 3.5 SAP GUI v motivu Quartz

Spuštění transakce se nejčastěji provádí použitím příkazového pole v levém horním rohu SAP GUI. Do tohoto pole stačí napsat název transakce. V případě, že si uživatel název transakce nepamatuje, tak může použít uživatelské menu v levé části obrazovky. Uživatel si může jakoukoliv transakci přidat do seznamu oblíbených, aby k ní mohl přistupovat rychle a zároveň si nemusel pamatovat její přesný název.

3.4.2 SAP Netweaver

SAP Netweaver je technologie, jež je klíčovým prvkem pro integraci a optimalizaci jednotlivých částí podnikových informačních systémů (SCM, ERP, CRM a BI) v rámci jediného systému. Jedná se o aplikační vrstvu sloužící jako základní technologický kámen pro produkty SAP. [16]

SAP NetWeaver také umožňuje vývoj aplikací pomocí programovacích jazyků jako je Java nebo ABAP. Vývojáři mohou využít velké škály nástrojů a funkcí, které platforma poskytuje. [16]

3.4.3 Databáze SAP HANA

Každý systém SAP se skládá z centrální databáze, kde jsou uložena všechna data. SAP R/3 a ECC podporují širokou škálu databází například: SAP HANA, Oracle, MSSQL, IBM Db2. Ovšem systém SAP S/4HANA je navržen a optimalizován pouze pro databázi SAP HANA. Na rozdíl od předchozích verzí tedy není možné používat jiné databáze. [25]

Více modelová databáze SAP HANA uchovává data v paměti RAM, nikoli na disku. Sloupcový design databáze in-memory umožňuje provádět pokročilé analýzy a rychlé transakce ve stejném systému. Díky tomu umožňuje podnikům okamžitě provádět dotazy na data a zpracovávat obrovské objemy dat s téměř nulovou odezvou. SAP HANA se od ostatních systémů pro správu databází (DBMS) na současném trhu liší tím, že integruje systémy OLAP a OLTP do jednoho samostatného systému. [18]

- OLAP je systém optimalizovaný pro analýzu a vyhodnocení velkých objemů dat.
- OLTP je systém optimalizovaný pro co nejvyšší rychlost zápisu. [25]

In-memory databáze (IMDB) je druh databáze, která ukládá data do hlavní paměti počítače (RAM) namísto na tradiční disky nebo SSD. Ačkoli většina dnešních databází přidala další možnosti ukládání v paměti, stále se jedná především o databázi založenou na disku. SAP HANA byla od základu vytvořena tak, aby pracovala s daty nejprve in-memory a podle potřeby využívala další úložné mechanismy, aby vyvážila výkon a náklady. Vyhledávání z paměti je řádově rychlejší než z disku nebo SSD, což vede k odezvám ve zlomcích sekund. [18]

Hlavní vlastnosti databáze HANA dle IBM jsou následující:

- Vylepšení databáze: většina databázových systémů je postavena na jediném datovém modelu, který omezuje způsob uspořádání, ukládání a zpracování

dat. Více modelová databáze SAP HANA podporující více datových modelů umožňuje snadno vytvářet vztahy mezi datovými body.

- Zlepšení správy dat: všechny procesy probíhají v reálném čase díky technologii IMDB, která odstranila pracné dávkové zpracování a zachovala extrémní dostupnost všech dat bez zpoždění. [19]

3.5 Programovací jazyk ABAP

ABAP je zkratka pro „Advanced Business Application Programming“. Jedná se o objektově orientovaný programovací jazyk využívaný v prostředí SAP. ABAP byl původně vyvinut společností SAP v roce 1980 pro tvorbu interních aplikací pro řízení podnikových procesů a je stále používán jako primární jazyk pro vývoj a údržbu SAP aplikací. [25]

3.6 Dynpro

SAP Dynpro je technologie pro tvorbu uživatelských rozhraní v prostředí SAP. Dynpro umožňuje vytvářet interaktivní obrazovky pro uživatele, které umožňují vstup, zobrazení dat a spouštění akcí v SAP aplikacích. Dynpro se skládá z různých prvků, kterými jsou vstupní pole, tlačítka, seznamy, grafické prvky a další. Dynpro umožňuje vytvářet uživatelská rozhraní, která jsou přizpůsobena potřebám uživatelů a poskytují jim efektivní nástroje pro práci s daty. [25]

Dynpro je součástí SAP GUI a je stále používán v mnoha SAP aplikacích. Ovšem v poslední době je stále více nahrazován modernějšími technologiemi jako SAPUI5 a SAP Fiori. [26]

3.7 Transakce

Transakce umožňují uživatelům jednodušší spuštění aplikace. Téměř každá SAP aplikace má určitý transakční kód, pomocí kterého se přistupuje k programu. Propojení programů a transakcí se provádí v transakci SE93 (Údržba transakce). Poté, co je program propojený s transakcí, tak jej uživatel může spustit napsáním kódu transakce do příkazového pole. [25]

SAP se řídí standardními konvencí pojmenovávání většiny standardních SAP aplikací. Transakční kódy končící číslem „1“ se obecně používají pro vytváření či zakládání, transakční kódy končící číslem „2“ slouží pro úpravu a transakční kódy končící číslem „3“ jsou pro zobrazování. [25]

Transakce končící znakem „N“ se nazývají „enjoy“ transakce. Tyto transakce byly vydány společně se systémem SAP ECC. Jedná se o transakce, které nahra-

zují staré transakce z pohledu vizuální a přehledové stránky. Ovšem zachovávají základní funkcionalitu transakce staré. Příkladem může být transakce SE16N (zobrazení tabulek), která je „enjoy“ transakcí transakce SE16. [25]

3.8 Možnosti přizpůsobení systému

Systém SAP umožňuje zpracování standardizovaných podnikových procesů. Ovšem každý podnik může mít určitá specifika, u kterých je potřeba úprava SAP standardu. Standard lze upravovat několika způsoby: customizing, rozšíření standardu, vlastní vývoj a změna standardu. [7]

3.8.1 Customizing

Customizing je přístup, který se pro přizpůsobení systému doporučuje nejčastěji. K přizpůsobení standardních funkcí k potřebám firmy lze použít tento nástroj. Customizing se provádí pomocí seznamu nastavitelných parametrů. Tento seznam, který má stromovou strukturu, je známý jako implementační příručka. Různé možnosti nastavení jsou tak rozděleny do kategorií podle témat. Touto úpravou se mění pouze parametry, které již byly v systému nastaveny, nikoli program samotný. [7]

3.8.2 Rozšíření standardu SAP

Rozšíření standardu je možné provést pomocí tzv. Customer Exit nebo User Exit. Jedná se o úmyslně vytvořená prázdná místa ve zdrojovém kódu programu, do kterých lze vložit vlastní kód nebo místa odkud je možné spuštění vlastního programu. [7]

3.8.3 Vlastní vývoj

Vlastní vývoj umožňuje vytvoření funkcionalit, které nejsou základem SAPu. Mohou to být pouze programy pro zobrazení určitých dat. Dále se mohou vytvářet úplně nové funkcionality nebo programy využívající funkcionalitu standardu. Možný je i vývoj vlastních datových prvků a databázových tabulek. [7]

3.8.4 Změna standardu

Mimořádně invazivní způsob změny představuje zásah do samotného standardu. Pokud je to možné, doporučuje se od tohoto druhu úpravy upustit. Takové změny vyžadují důkladnou znalost systému, architektury databáze a systémových tabulek. U tímto způsobem provedených změn může při zveřejnění nové verze systému dojít k jejich smazání. [7]

4 BEZPEČNOST PROSTŘEDÍ SAP

Vzhledem k tomu, že podnikový informační systém je jádrem každého podniku, tak jeho zabezpečení je klíčovou součástí nastavení bezpečnosti ve společnosti.

Zajištění úrovně bezpečnosti ERP systémů závisí od následujících základních požadavků:

- Autentizace uživatelů jménem a heslem.
- Správa uživatelů je v rukou pověřených osob.
- Dostatečné zabezpečení komunikace mezi klientskou aplikací a serverem.
- Sledování historie vytvoření a změn jednotlivých záznamů.
- Pro zjednodušení řešení chybových stavů je možné detekovat, sledovat a následně hlásit jejich výskyt. [5]

Na specifikované funkce nebo bezpečnostní požadavky systému ERP je třeba pohlízet jako na komplex specifikací a kontrolních mechanismů v kontextu celkové bezpečnostní politiky organizace. [5]

4.1 Autentizace uživatelů

Autentizace uživatelů by se dala považovat za jednu z prvních forem zabezpečení systému. Jedná se o předem definovaný proces, podle kterého uživatel prokazuje svoji identitu. Autentizace může být klasickým způsobem jménem a heslem nebo některým sofistikovanějším způsobem, jako je třeba dvou-faktorová autentizace. [28]

Klíčová nastavení pro přístup uživatelů lze v systému SAP definovat několika způsoby:

- Dostatečně bezpečné heslo - lze nastavit jeho délka, požadovaný počet znakových sad a nebo také životnost.
- Maximální počet neúspěšných pokusů o přihlášení.
- Automatické odhlášení neaktivního uživatele.
- Zamezení přístupu neaktivního uživatele do systému.
- Ukládání hesel v zahashovaném formátu. [31]

Tabulka 4.1 Doporučené základní parametry hesla [29]

Parametr	Popis	Hodnota
login/min_password_lng	Minimální délka hesla	10
login/min_password_lowercase	Minimální počet malých znaků	1
login/min_password_uppercase	Minimální počet velkých znaků	1
login/min_password_letters login/min_password_digits login/min_password_specials	Minimální počet znaků, číslic a speciálních znaků v hesle	2
login/password_history_size	Počet různých hesel tak, aby stejné heslo nemohlo být použito znovu.	20

Každá společnost může mít požadavky na bezpečnost hesla rozdílné, ovšem doporučené parametry jsou zobrazeny v tabulce 4.1.

V systému SAP existuje opravdu velká škála parametrů, které se zabývají oblastí autentizace uživatelů. Při nastavování bezpečnosti by bylo vhodné se zabývat i následujícími parametry:

- Počet rozdílných nových hesel tak, aby stejné heslo nemohlo být použito znovu.
- Počet znaků, které musí být u nového hesla rozdílné oproti původnímu.
- Nastavení celkové doby platnosti hesla. [29]

Za zmínku také stojí tabulka USR40, jež je možná upravovat v transakci SM30. V této tabulce lze nastavit hesla, či určitá posloupnost znaků, které se v hesle nesmí použít. Aby se nemusely nastavovat všechny možné kombinace hesla, tak se dají do tabulky USR40 vložit dva zástupné znaky, kde:

- ? - znamená jeden znak.
- * - znamená sekvenci libovolné kombinace znaků libovolné délky. [29]

4.1.1 Single Sign-On

Single Sign-on (SSO) je technologie, která umožňuje uživatelům přihlásit se jedním přihlašovacím jménem a heslem k více různým aplikacím. Uživatel si tedy nemusí pamatovat hesla ke každé aplikaci, ale stačí mu pouze jedno, které tím pádem může být silnější. [29]

SSO funguje tak, že uživatel se přihlásí pouze jednou, obvykle na hlavní portál, aplikaci nebo do systému. V systému Windows to může být například pomocí

protokolu Kerberos SSO. Uživatel po přihlášení do systému obdrží tokeny pomocí domény Active Directory, jež je použita jako autorizační autorita protokolu Kerberos. Tyto tokeny jsou poté využitelné k přihlášení do ostatních aplikací, kterým je například systém SAP. [29]

SSO je nejlepším způsobem k zabezpečení systému SAP. U systému SAP se jedná o placenou funkcionalitu, která v současné době bohužel není v systému SAP u společnosti HP TRONIC přítomná.

4.2 Princip rozdělení pravomocí

Segregation of Duties (SoD) je koncept rozdělení úkolů mezi více osob. V systému SAP se SoD může týkat nejen obchodních procesů, ale také procesů administrativních, jako je tvorba uživatelů, přiřazování rolí atd. [31]

V případě nastavení SoD by jednotlivec teoreticky neměl mít přístup k více než jedné funkci pro úkol, ve kterém by bylo možné rozdělení použít. [31]

Příklady úkolů, jenž se skládají ze dvou více funkcí mohou být následující:

- Spravovat uživatele a jejich role.
- Vytvářet dodavatele a zpracovávat platby.
- Objednávat a evidovat přijaté zboží.
- Měnit hlavní údaje o zaměstnancích a provádět mzdové účetnictví. [29]

Rozdělení rolí není vždy možné dosáhnout. Může to být kvůli omezeným personálním zdrojům v organizaci nebo jednoduše proto, že by to proces rozšířilo, a tím zpomalilo organizaci. [29]

Průběh SoD u správy uživatelů a jejich rolí by se mohl rozdělit na dvě role, a to na správce uživatelů a správce autorizace. Správce uživatelů spravuje záznam o hlavním uživateli a přiřazení rolí k uživatelům, zatímco správce autorizace spravuje role, vytváří autorizace a jejich profily. V případě, že by jeden uživatel spravoval oba úkoly, tak by mohl potenciálně vytvořit roli s neomezeným oprávněním a mohl by ji přiřadit ji sám sobě. [29]

Předchozí příklad zobrazuje princip dvojité kontroly. Nicméně k dosažení ještě vyšší úrovně bezpečnosti v organizaci může být implementován i princip trojitě kontroly. To znamená, že k dokončení celých úkolů je potřeba zapojení nejméně tří osob. V příkladu by se mohlo jednat o rozdělení role správce autorizace na dvě další role. Jeden ze správců autorizace by neměl práva k vytvoření profilu autorizace role. K vytvoření profilu autorizace by bylo potřeba zásahu ještě třetího administrátora. [29]

Důležité je si uvědomit, že SoD přichází za cenu, ať už zvýšenou složitostí jednotlivých úkonů a zvýšením času potřebného k dokončení úkolu. [29]

4.3 Princip minimálních pravomocí

Princip minimálních pravomocí je bezpečnostní koncept, podle kterého by každému uživateli mělo být uděleno pouze minimální množství oprávnění potřebných k provádění příslušných úkolů. Například uživatelský účet určený k zobrazení načtených dat z databáze nevyžaduje stejný rozsah oprávnění jako zadavatel objednávek nebo správce systému. Dodržování konceptu nejmenších oprávnění je osvědčeným postupem v oblasti zabezpečení informací. [30]

Princip minimálních pravomocí funguje tak, že se uděluje pouze přístup nezbytný k dokončení daného úkolu. Při dodržování principu nejmenších oprávnění v prostředí SAP se snižuje rozsah dopadů v případě, že by došlo k nežádoucímu jednání. [30]

Princip minimálních pravomocí je aplikovatelný i v systému SAP. Nicméně složitost jeho nastavení pro zachování bezproblémového běhu je velmi časově náročné a vyžaduje důkladnou znalost celého systému.

4.4 Systémové parametry

Obecná pravidla v systému SAP lze nastavit v systémových parametrech. Systémové parametry si lze představit jako soubor základních provozních pokynů pro systém SAP NetWeaver. [29]

Tyto instrukce určují systému například to, kolik paměti má být přiděleno pracovnímu procesu, minimální délku hesla nebo kolik pokusů o zadání hesla smí uživatel provést, než je jeho účet uzamčen. Některé z těchto pokynů lze vyhodnocovat za běhu systému, jiné lze číst při spuštění. [29]

Systémové parametry jsou uloženy v operačním systému i databázi. To se dělá proto, aby se v případě selhání systému mohl správce do systému přihlásit. Mohlo by se stát, že by chybná konfigurace nebo chybový stav bránili správci přihlásit se do systému. Jestliže by nemohl systémové parametry upravit na úrovni operačního systému, tak by nebylo možné se do systému přihlásit. Ačkoli je tento postup v případě nouze přijatelný, pro správné sledování a kontrolu změn by měl správce ke změně parametrů vždy používat systém SAP. [29]

4.5 Systémové profily

Skupinu parametrů určenou pro určitý rozsah lze označit profilem systému. Do této kategorie patří jedna instance, aplikační server, všechny servery, server zpráv,

plánovač a další možnosti. Toto rozlišení bylo provedeno proto, aby nebylo potřeba zadávat stejné hodnoty v každém jednotlivém profilu. V případě, že se nebudou měnit v závislosti na systému. Použití správného profilu dále umožňuje nastavit určitou hodnotu pouze v jediné instanci. [29]

V systému SAP jsou nejčastěji používány dva systémové profily, kterými jsou:

- **Profil instance** obsahuje parametry, které se vztahují pouze na instanci (například aplikační server), pro kterou je profil určen. Každá instance systému SAP NetWeaver by měla mít svůj vlastní profil instance.
- **Výchozí profil** poskytuje hodnoty parametrů všem instancím, které nemají položky pro daný parametr. To znamená, že pokud je parametr nastaven ve výchozím profilu, tak každý profil instance zdědí tuto hodnotu, jako by byla nastavena v jejím profilu. [29]

Pro zobrazení a úpravu profilových parametrů lze použít některou z transakcí. Přehledné zobrazení všech profilových parametrů je vhodné využít report RSPARAM. Program RSPARAM nemá ve standardu SAP přidělen transakční kód. Tento program je tedy nutné spustit v transakci SE38. [31]

Pro zobrazení či změnu jednotlivých parametrů je určena transakce RZ10. Zobrazení dokumentace k jednotlivým parametrům slouží transakce RZ11. [29]

4.6 Zamykání transakcí

Zamykání transakcí je prvním nástrojem, který se používá k tomu, aby bylo zabráněno uživatelům prohlížet transakce v systému SAP. Možnost zabránit všem uživatelům v provedení určitého kódu transakce se nazývá uzamčení transakce. K uzamčeným transakcím nemůže přistupovat žádný uživatel v systému. [29]

Uzamčení transakcí je možné v závislosti na klientovi či nezávisle na klientovi. Zámek nezávislý na klientovi je vytvořen ve všech klientech, na rozdíl od zámku závislého na klientovi, který je vytvořen pouze v jednom konkrétním klientu. [29]

Zamykání transakcí se tradičně provádělo v transakci SM01. Společnost SAP však považuje transakci SM01 za zastaralou a od verze SAP Net-Weaver 7.5 ji nahradila transakcí SM01_DEV a transakcí SM01_CUS. Tato změna byla provedena za účelem přidání dalších funkcí pro zamykání transakcí a zaznamenávání změn. [29]

Volba, které transakce uzamknout, či k nim zamezit přístup, závisí na řadě obchodních a technických proměnných, podobně jako mnoho dalších rozhodnutí

o zabezpečení v systému SAP. Seznam transakcí, které je třeba uzamknout, může správci zabezpečení předat jeho auditor nebo bezpečnostní oddělení podniku. [29]

V tabulce 4.2 je zobrazen stručný seznam obecných transakcí, které by bylo vhodné na produkčním klientovi zamknout.

Tabulka 4.2 Seznam vhodných transakcí k uzamknutí [29]

Kód transakce	Název transakce
SCC5	Výmaz klienta
SE11	ABAP Dictionary
SE37	Editor funkcí
SE38	Editor ABAP
SU10	Hromadná údržba uživatelů
SM30	Údržba tabulek
F110	Automatický platební styk
MIRO	Založení došlé faktury

Existuje i další řada transakcí, které je vhodné zamknout v závislosti na požadavcích společnosti. Jednalo by se například o robustní personální nebo finanční transakce, které by při nesprávném použití mohly vést k problémům. [29]

4.7 Správa uživatelů

Každý uživatel má své unikátní User ID neboli uživatelské jméno, které je uloženo v tabulce USR02. Každé User ID je závislé na klientu SAP. Maximální možná délka uživatelského jména je dvanáct znaků. [31]

Existuje několik metodik pojmenovávání uživatelů. Nejčastější je celé jméno plus první písmeno křestního jména. [31]

Seznam transakcí, které jsou pro správu uživatelů a jejich pravomocí nejčastěji používány:

- PFCG - transakce pro zpracování rolí a profilů.
- SU01 - transakce pro správu uživatelů.
- SU02 - transakce pro zpracování profilů (doporučuje se použití novější transakce PFCG).
- SU03 - transakce pro údržbu a oprávnění profilů.
- SU10 - transakce pro hromadnou údržbu uživatelů.

Správa uživatelů se provádí v transakci SU01. V této transakci je možné u jednotlivých záložek nastavovat obecné informace uživatele a vytvářet, přiřazovat

Obrázek 4.1 Úvodní obrazovka při zobrazení uživatele v transakci SU01

a nastavovat určité bezpečnostní parametry. Jednotlivé záložky mají následující použití:

- Adresa - informace o uživateli (jméno, příjmení a kontakt).
- Přihlašovací údaje - zde je možné nastavit či obnovit heslo.
- Parametry - umožňují nastavit základní uživatelské parametry. Příkladem může být nastavení pobočky, která by se uživateli doplňovala automaticky při používání programu.
- Role - v této záložce je možné uživateli přiřadit jednotlivé role. Po přidání role se uživateli přidá i k ní vygenerovaný profil. Další možností je nastavení referenčního uživatele. Od tohoto uživatele zdědí všechny jeho role. Pro vytváření rolí slouží transakce PFCG.

- Profily - zde je možné uživateli přiřadit některý z již dříve vytvořených profilů. Generování profilů se stejně jako vytváření rolí provádí v transakci PFCG.
- Skupiny - v této záložce lze přidávat uživatele do určitých skupin. Největší výhodou těchto skupin je možnost hromadné údržby uživatelů dané skupiny v transakci SU10. Tyto skupiny nehrají žádnou roli v zabezpečení. [31]

Pro přístup k jednotlivým transakcím a jejich funkcím je nutné mít patřičná oprávnění. Obecně by uživatel měl být schopen spustit transakci SU01. Ovšem měl by mít možnost pouze pro zobrazení účtu, nikoli pro úpravu či vytváření. Autorizace pro provádění určitých operací se určují hodnotou u pole ACTVT u daného typu oprávnění. Seznam všech činností a jim přiřazených hodnot je možný dohledat v tabulce TACT, kde:

- Hodnota 01 - vytváření
- Hodnota 02 - upravování
- Hodnota 03 - zobrazení
- Hodnota 04-XX - další možnosti

4.8 Nastavování autorizací

Autorizace řídí funkce, které může uživatel provádět, a která data lze zobrazovat, měnit, zadávat, mazat atd. Díky robustním možnostem nastavení oprávnění lze zajistit, aby byl systém SAP v souladu s běžnými praktikami a předpisy, a tímto jej ochránil před podvodným jednáním. [31]

V podnikovém prostředí se oprávnění používají k regulaci přístupu na aplikační úrovni. Při nastavování autorizací podnikových uživatelů se bere v úvahu řada věcí. Obecně je důležité zabránit podvodům a obstrukcím v procesech. Na druhou stranu to může být i například legislativa týkající se ochrany dat a soukromí. Podnik musí být schopen tato pravidla dodržovat, aby byl v souladu s platnými zákony. Také je třeba najít rovnováhu mezi náklady a přínosy rozsáhlého zabezpečení. [31]

4.8.1 Uživatelské role

V systému SAP existují uživatelské role, které definují soubor oprávnění a funkcionalit, jenž jsou přiděleny uživatelům. Tyto role určují, jaké úkoly a funkce může uživatel v systému SAP provádět. [27]

Každá role v systému SAP může obsahovat sadu oprávnění, která umožňují uživatelům přistupovat k určitým funkcím a datům v systému. Mezi běžná oprávnění patří například přístup k transakcím, prohlížení a úprava dat v určitých oblastech systému, vytváření a úprava záznamů a práce s reporty a formuláři. [27]

V systému SAP existují především dva typy rolí: jednoduché role a složené role. Jednoduchá role by mohla být dále odvozena do role odvozené.

- Jednoduchá role obsahuje všechny autorizační objekty a hodnoty polí potřebné pro provedení transakce. Jednoduché role jsou nejpoužívanějším typem rolí v prostředí SAP. [27]
- Odvozená role je ze své technické podstaty stále jednoduchou rolí, která dědí svá funkční oprávnění od hlavní role. Odvozená role je užitečná, pokud se potřebuje zrcadlit přesně stejná funkcionality, jako má hlavní role, ale je třeba manipulovat s organizačními úrovněmi. [27]
- Složená role je kolekce dvou a více jednoduchých a odvozených rolí, které je možné seskupit do jedné společné role. Účelem složených rolí je zjednodušení přiřazování rolí uživatelům. Složené role neobsahují žádné autorizační údaje, pouze jiné role. [27]

Jakmile role obsahuje alespoň jeden objekt oprávnění a je vygenerována, systém automaticky vytvoří profil oprávnění pro tuto roli. Vztah mezi rolí a profilem je 1:n, což znamená, že jedna role může mít více profilů. Jeden profil je omezen na maximálně 150 autorizačních objektů. Po dosažení tohoto limitu se automaticky generují další profily. Vygenerované profily pro jednotlivé role a jejich autorizační objekty lze zobrazit v tabulce AGR_1016. [29]

4.8.2 Uživatelské profily

V systému SAP se profilem obvykle rozumí soubor nastavení a oprávnění, které jsou přiřazeny jednomu uživateli nebo skupině uživatelů. Profily v systému SAP definují, jaké činnosti a transakce může uživatel provádět, jaké údaje může zobrazovat a jaké změny může provádět v rámci systému SAP. [27]

Profily existovaly dlouho před rolemi. Před systémem R/3 byli uživatelé v systému autorizováni prostřednictvím profilů. Při generování role se vytváří profil, který obsahuje skutečné objekty oprávnění a jejich hodnoty. Profily lze stále použít k autorizaci uživatelů. [29]

Příkladem profilu může být profil SAP_ALL, který danému uživateli dává všechny systémové autorizace.

4.8.3 Chyba autorizace

Po počátečním nastavení rolí a profilů může dojít k tomu, že uživatel nebude schopen provádět určité transakce nebo při provádění určité části transakce začne docházet k selhání autorizace. Transakce SU53 (Kontroly oprávnění) je místo, kde začíná většina vyšetřování problémů s autorizací konkrétního uživatele. Transakce SU53 umožňuje identifikovat pouze neúspěšné autorizační kontroly, což je také její největší nevýhoda, protože neuvádí, které autorizační kontroly byly provedeny úspěšně. [31]

4.9 Zaznamenávání změn

Zaznamenávání změn nebo také logování změn umožňuje administrátorovi sledovat téměř všechny změny provedené v systému. Rozsah těchto logů závisí na nastavení systému, typu změny či nastavení samotné tabulky, ve které byla změna provedena. Administrátor může zjistit, jaký řádek tabulky byl změněn, ale ne vždy je schopen rozpoznat, jaké hodnoty se změnily.

Klasické změny nad tabulkou (například v transakci SM30) je možné sledovat v transakci SCU3 (Historie tabulky). Aby ve zmíněné transakci bylo možné změny sledovat, tak musí být v příslušné tabulce zapnuté logování.

Jestliže by logování zapnuté nebylo a nastal by požadavek vypátrat, kdo změnu provedl. Je možné použít transakci STAD (sledování statistiky zatížení napříč transakcemi). Jedná se o transakci, která zobrazuje veškeré zatížení systému SAP. Vzhledem k tomu, že se jedná o obrovský objem dat, tak se tato data většinou ukládají pouze po krátkou dobu (hodiny, případně jednotky dní).

Existuje i další speciální případ změny tabulky zvaný sap_edit v transakci SE16. Jedná se o možnost přímé změny dat v jakékoli tabulce. Jedná se o velký zásah do systému, kde v případě změn určitých polí může docházet k velkým diskrepancím v systému. Změny tímto způsobem se zaznamenávají do tabulek SE16N_CD_KEY a SE16N_CD_DATA. V první zmíněné tabulce jsou pouze hlavičky záznamu o změně a druhá obsahuje bližší informace o změněných datech.

II. PRAKTICKÁ ČÁST

5 SYSTÉM SAP VE SPOLEČNOSTI HP TRONIC ZLÍN

Systém SAP byl ve společnosti HP TRONIC implementován v roce 2009 prostřednictvím české poradenské společnosti MIBCON, a. s., již je partnerskou společností SAP.

Jednalo se o systém SAP R/3 nad databází Db2 od IDB. V roce 2020 došlo za účelem zvýšení výkonu a efektivity systému k přechodu na databázi SAP HANA, u které se nepředpokládá, že bude minimálně v následující dekádě nahrazena. Systém SAP EPR již tak velkým rozšířením neprošel. Došlo pouze k postupné aktualizaci verze SAP Netweaveru, jenž má v současnosti verzi 7.4. Velkým milníkem bude rok 2024, ve kterém se předpokládá nasazení systému SAP S/4HANA, který nahradí stávající systém SAP ECC.

Systém SAP je ve společnosti HP TRONIC provozován na několika prostředích, kterými jsou vývojové, testovací a produkční. Následující seznam blíže popisuje funkcionalitu jednotlivých prostředí:

- Vývojové prostředí - jak již název vypovídá, tak toto prostředí slouží především k vývoji. Ovšem probíhá zde i nastavování určitých customizačních parametrů a tabulek, které je nemožné na testovacím či produkčním prostředí upravovat. Nastavení těchto parametrů na těchto prostředích probíhá transportem customizačního požadavku z vývojového prostředí.
- Testovací prostředí slouží k testování vyvinutých programů či upravených parametrů. Toto prostředí by se mělo nastavením co nejvíce blížit produkčnímu prostředí, aby bylo možné téměř s jistotou říci, že budoucí nasazení úprav neohrozí funkcionalitu produkčního prostředí.
- Produkční prostředí - na tomto prostředí se pracuje s reálnými daty v reálném čase. Vývoj by nikdy neměl probíhat v produktivním prostředí, proto je to SAPem znemožněno a technicky téměř nemožné.

Vzhledem k tomu, že je nastavení uživatelských oprávnění nezávislé na prostředí, tak je nutné nastavení provádět na každém prostředí samostatně. Proto, aby se neohrozila funkcionalita produkčního prostředí, tak většina nastavení a testování oprávnění bude provedeno na testovacím či vývojovém prostředí.

5.1 Moduly využívané ve společnosti HP TRONIC

Jak již bylo v úvodu diplomové práce zmíněno, tak systém SAP je ve společnosti využíván téměř ve všech klíčových firemních procesech kromě personálního oddě-

lení (HR). Mezi tyto klíčové procesy i patří modul FI/CO, na jehož nastavení se praktická část diplomové práce částečně zaměřuje.

Výsledkem praktické části by měla být analýza současného stavu nastavení nej-používanějších uživatelských rolí. Na základě výsledku analýzy dojde k vytvoření obecné role, která bude použitelná pro všechny uživatele. Součástí analýzy i návrhu je část zaměřená na modul FI/CO, u kterého dojde k návrhu metodiky SoD u jedné z aktivit. Tato metodika bude v budoucnu aplikovatelná pro nastavení i ostatních modulů.

5.2 SAP S/4HANA a uživatelská oprávnění

Plánovaný přechod na SAP S/4HANA v roce 2024 bude u některých procesů v systému vyžadovat změnu nastavení či funkcionality. Změny ve všech modulech popisuje SAP v dokumentu Simplification List for SAP S/4HANA [36]. Dle tohoto dokumentu by k žádným zásadním změnám u uživatelských oprávnění dojít nemělo. Tudíž jakékoli role a profily nastavené v systému SAP ECC by tedy měly být kompatibilní i v systému SAP S/4HANA.

Společně s přechodem dojde ke zlepšení procesu přehledu uživatelů a jejich rolí. Příkladem může být to, že v systému přibude nová tabulka PUSERROLE, která umožňuje jednoduché zobrazení všech rolí, které má uživatel přiřazen. Ve verzi SAP ECC je možné stejný seznam také zobrazit. Ovšem je potřeba propojení alespoň dvou tabulek. Propojení těchto tabulek a následné grafické zobrazení výstupu bude jednou z funkcionalit přehledového programu, který je součástí praktické části diplomové práce.

5.2.1 Zobrazení uživatelských oprávnění v transakci DBACOCKPIT

SAP umožňuje přímý dotaz do databáze v transakci DBACOCKPIT v záložce SQL Editor. V SQL editoru se používá obecná syntaxe SQL dotazu, kterou zobrazuje kód 1.

Kód 1. SQL dotaz pro získání seznamu rolí a jejich popisu pro určitého uživatele

```
SELECT DISTINCT TXT.LINE, USR.AGR_NAME AS Nazev, TXT.TEXT
FROM AGR_USERS AS USR
JOIN AGR_TEXTS AS TXT ON USR.AGR_NAME = TXT.AGR_NAME
WHERE USR.UNAME = 'TROJANJ'
AND USR.MANDT = '500'
AND TXT.SPRAS = 'C'
ORDER BY Nazev, LINE
```

V jazyce ABAP je syntaxe SQL dotazu mírně rozdílná. Příklady těchto SQL dotazů jsou součástí kapitoly 8.

Při jakémkoli SQL dotazu v SAP se doporučuje používat číslo klienta, ze kterého je požadavek získat data. Ve společnosti je pouze jeden klient u každého SAP serveru, jehož číslo je 500. Dotaz by tedy bylo možné i bez použití podmínky `USR.MANDT = '500'`. Pole MANDT (klient) je primárním klíčem u všech databázových tabulek.

Podmínka `TXT.SPRAS = 'C'` určuje, který jazyk se má použít v případě, že by měla role popisy ve více jazycích. Tento příklad nastává převážně u rolí a profilů, které byly vytvořeny společností SAP.

Každá role může obsahovat několik řádků popisu. Z toho důvodu dotaz obsahuje dodatečný parametr LINE (řádek) a jeho seřazení od nejnižší hodnoty po hodnotu nejvyšší. Tímto způsobem je zaručeno, že se uživatelům zobrazí jednotlivé popisy role v posloupnosti dle pořadí zápisu.

LINE	NAZEV	POPIŠ
00000	Z_BC_UNLOCKUSER_TY	Role - blokování a odblokování uživatelů - skupiny '012_TY
00001	Z_BC_UNLOCKUSER_TY	SIK 3.12.2008 - menu OK,
00000	Z_DUZP_1000	Aktualizace DUZP 1000
00000	Z_DUZP_3000	Aktualizace DUZP 3000
00000	Z_DUZP_3200	Aktualizace DUZP 1000
00000	Z_HPT_USER	Role - společná oprávnění pro všechny uživatele
00001	Z_HPT_USER	7.8.08 10:57 - založení + základní nastavení
00002	Z_HPT_USER	8.8.08 10:23 - přidání transakce SM37 a nastavení pro ni
00003	Z_HPT_USER	27.8.08 12:04 - přidání transakce SE93 (ale ne do menu!!!) a nastavení pro ni,
00004	Z_HPT_USER	pouze pro tlení
00005	Z_HPT_USER	5.9.2008 10:20 - přidání transakce SP01 (ne do menu!!!) nastavení pro ni
00006	Z_HPT_USER	10.12.2008 15:00 - přidání pro práva zobrazit základní data z personalistiky
00007	Z_HPT_USER	29.12.2008 14:00 - přidání práva pro import (mj. obilíbené)
00000	Z_MM_DOD_RO_MASTER	Role - pro údržbu kmenových dat dodavatelů, RO
00001	Z_MM_DOD_RO_MASTER	SIK 9.10.2008 menu OK - nutná konzultace, zda jsou ty transakce nutné, nejsou
00002	Z_MM_DOD_RO_MASTER	abecedně
00000	Z_MM_DOD_RW_MASTER	Role - pro údržbu kmenových dat dodavatelů, RW
00001	Z_MM_DOD_RW_MASTER	SIK 9.10.2008 menu OK - nutná konzultace, zda jsou ty transakce nutné

Obrázek 5.1 Vzhled výstupu v transakci DBACOCKPIT

Na obrázku 5.1 je zobrazen výstup předchozího SQL dotazu přímo v prostředí SAP. Výstup záznamů je zobrazen formou ALV (ABAP List Viewer). Jedná se o standardní nástroj pro zobrazení výstupu tabulek a seznamů v systému SAP. ALV je nejběžnější formou zobrazování výstupních tabulek uživateli. Umožňuje uživatelům interaktivně manipulovat s daty, jako je například seřazení záznamů, vyhledávání, filtrování a nebo vytvoření .xlsx souboru na základě aktuální úpravy ALV.

6 ANALÝZA SOUČASNÉHO STAVU NASTAVENÍ UŽIVATELSKÝCH ROLÍ

Prvním krokem v analýze nastavení uživatelských rolí bylo potřeba zjistit několik základních informací. Na základě těchto informací bude umožněno provést efektivní analýzu současného stavu nastavení uživatelských oprávnění. Mezi tyto informace patří:

1. Určení modulu pro který bude analýza stavu rozdělení pravomocí provedena.
2. Vytvoření seznamu uživatelů, jež využívají daný modul na denní bázi.
3. Určit požadovaná oprávnění dle pracovní pozice uživatele ve společnosti.
4. Zjištění nepoužívanějších rolí ve společnosti.
5. Vytvoření seznamu oprávnění patřících do skupiny kritických oprávnění.

Jak již bylo v předchozí kapitole 5.1 zmíněno, tak byl zvolen modul SAP FI/CO. Na základě tohoto rozhodnutí byl vytvořen seznam celkem dvaceti devíti uživatelů využívající tento modul. Jedná se o uživatele od obecných účetních, kteří vyžadují pouze základní oprávnění až po hlavní účetní či finančního ředitele společnosti HP TRONIC.

Tato kapitola se zabývá analýzou současného nastavení oprávnění u rolí nebo uživatelů splňující tyto podmínky. Na základě výsledku analýzy je v kapitole 7 proveden návrh nové metodiky nastavení bezpečnosti a její následná realizace.

6.1 Standardní SAP transakce umožňující přehled uživatelů

Přehled uživatelů se v systému nejčastěji provádí v transakci SUIM, která je standardním nástrojem pro správu uživatelů a autorizací. Další transakcí, ve které je možné využít omezený přehled je transakce PFCG.

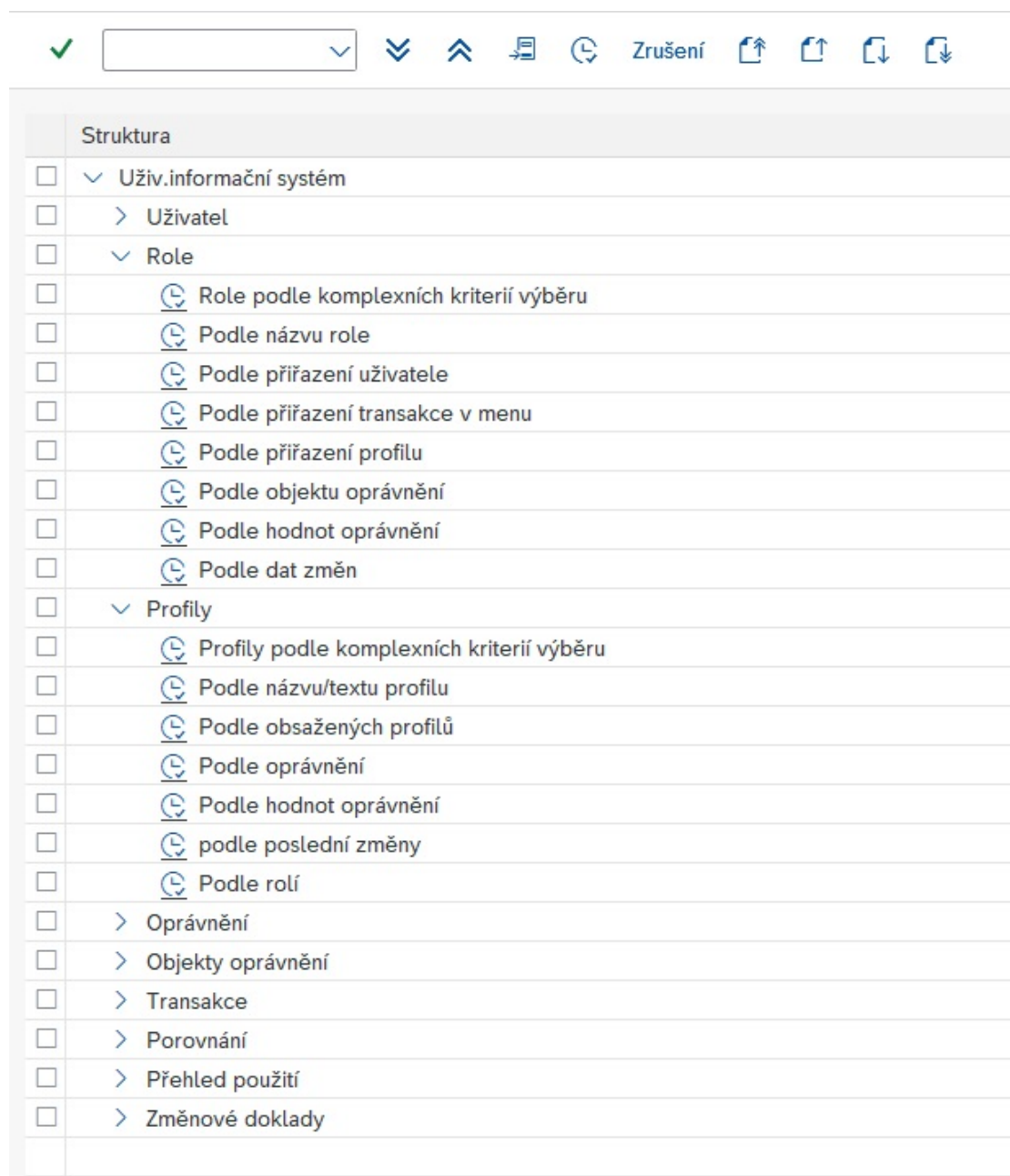
6.1.1 Transakce SUIM

Transakce SUIM (SAP User Information System) je nejobsáhlejší nástrojem pro správu uživatelů a autorizací v SAP. SUIM poskytuje různé funkce pro správu uživatelských účtů, rolí a oprávnění v SAP. Mezi některé z funkcí SUIM patří:

- Zobrazení seznamu všech uživatelů v systému SAP a jejich atributů.
- Správa rolí uživatelů a přidávání nebo odebrání rolí uživatelům.

- Kontrola oprávnění uživatelů a jejich přístupu k různým funkcím a datům v SAP.
- Kontrola záznamů o přihlášení uživatelů a sledování jejich aktivit v systému SAP. [29]

Transakce SUIM je velmi užitečným nástrojem pro správu uživatelů a autorizací v systému SAP. Následující obrázek 6.1 zobrazuje vstupní obrazovku transakce SUIM s rozvinutým výběrem vstupu pro role a profily.



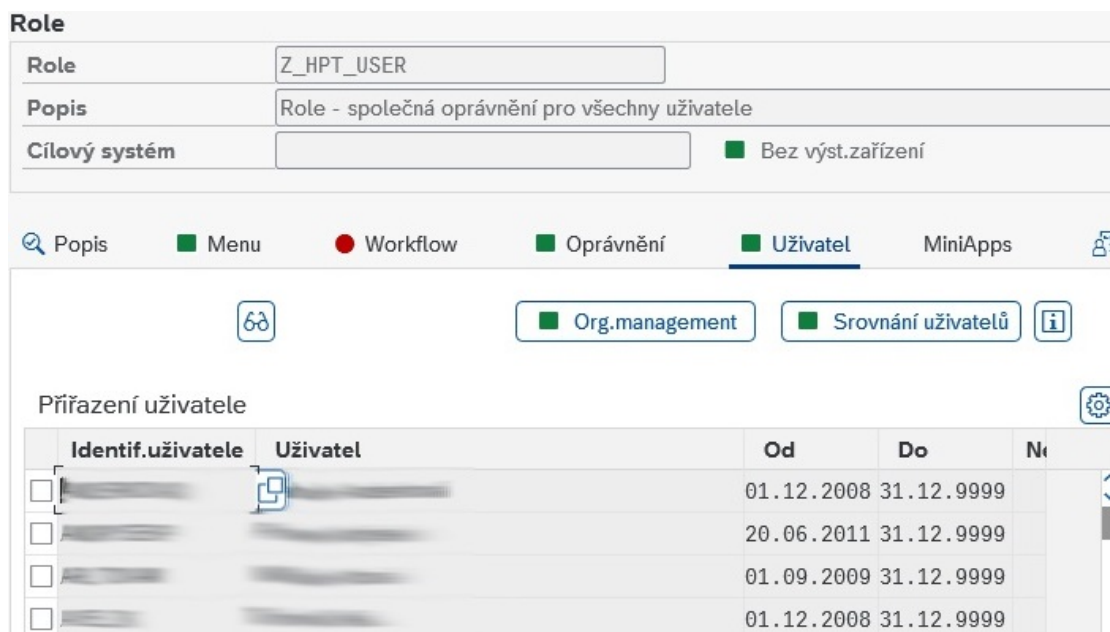
Obrázek 6.1 Vstupní obrazovka transakce SUIM

Výstupem transakce může být například zobrazení všech rolí, které jsou přiřa-

zeny zvolenému uživateli. Ovšem v této transakci není možnost zobrazit všechny uživatele, kteří mají určitou roli. Tento výsledek je naopak možný v transakci PFCG.

6.1.2 Transakce PFCG

Transakce pro údržbu rolí PFCG umožňuje nastavení oprávnění jednotlivých rolí, ale také zobrazení seznamu uživatelů, kteří mají přiřazenou vybranou roli. Seznam uživatelů je možný zobrazit v záložce Uživatel. Následující obrázek 6.2 zobrazuje vzhled transakce PFCG v prostředí SAP.



Obrázek 6.2 Seznam uživatelů majících roli Z_HPT_USER v transakci PFCG

Z důvodu práce s osobními údaji, jako je uživatelské jméno a celé jméno (případně telefonní číslo či emailová adresa), tak dojde u všech výstupů k jejich rozmazání.

6.2 Jednotlivé kroky analýzy

Úvodní analýza se zabývá jednoduchým přehledem počtu spustitelných transakcí u celkem 29 vybraných uživatelů z modulu FI/CO. Na základě tohoto výsledku bude možné získat základní představu o nastavení oprávnění. Následující kroky jsou již zaměřeny na specifické parametry jako spustitelné kritické transakce nebo analýza nejpoužívanějších rolí v systému, kterými jsou Z_HPT_USER a Z_USER_TEMPORARY. V závěru kapitoly je provedena analýza nastavení SoD a systémových parametrů zaměřených na uživatelská hesla. Přestože systémové parametry již nejsou součástí nastavení uživatelských oprávnění, tak hrají důležitou roli v zabezpečení systému SAP.

Značná část analýzy je prováděna pomocí základních funkcionalit transakce SUIM a PFCG.

6.3 Analýza počtu spustitelných transakcí dle uživatele

Prvním krokem analýzy byla kontrola počtu spustitelných transakcí v systému. Jedná se o opravdu základní analýzu, dle které lze jednoduše zjistit, kteří uživatelé mají všechna oprávnění a kteří nikoli. Tato metoda může být vhodná jako statistika toho, zda uživatelé na stejné pozici mají stejná oprávnění.

Jedním z výstupů analýzy je tabulka 6.1, která zobrazuje počet uživatelů a jejich pracovních pozic dle počtu spustitelných transakcí.

Tabulka 6.1 Počty uživatelů dle počtu spustitelných transakcí a pracovních pozic

Počet uživatelů	Množství transakcí	Pracovní pozice
8	126772	finance (1), účetní (7)
4	126778	účetní (4)
3	(vše) 127579	controlling (1), finance (1), analytik (1)
2	126940	účetní
	126929	účetní
	126855	účetní
1	126856	finance
	126840	analytik
	126813	účetní
	126788	účetní
	126721	účetní
	126711	controlling
	121578	účetní
	121536	účetní

V tabulce jsou zobrazeny již sloučené pozice do skupin bez ohledu na jejich zaměření. Jednotlivé pozice a jejich zaměření jsou následující:

- Účetní - souhrn všech účetních od hlavních, maloobchodních, zbožíových, saldových a ostatních
- Finance - finanční ředitel, finance
- Analytik - účetní analytik

Tabulka nezobrazuje naprosto přesné výsledky, protože došlo ke sloučení několika účetních zaměření do jedné skupiny.

Tabulka 6.2 je obdobou předchozí tabulky ovšem obsahuje detailnější informace o tom, které transakce mohou uživatelé provádět dle zaměření pracovní pozice.

Tabulka 6.2 Počty uživatelů dle počtu spustitelných transakcí a zaměření pracovních pozic

Pracovní pozice	Množství transakcí	Zaměření - Počet uživatelů
účetní	126940	hlavní (1), ostatní (1) - 2
	126929	ostatní (2) - 2
	126855	maloobchod (1), ostatní (1) - 2
	126772	salda (4), zboží (3) - 7
	126813	hlavní - 1
	126788	hlavní - 1
	126721	salda - 1
	121578	zboží - 1
	121536	maloobchod - 1
controlling	(vše) 127579	1
	126711	1
finance	(vše) 127579	finanční ředitel - 1
	126856	1
	126772	1
účetní analytik	(vše) 127579	1
	126840	1

Dle analýzy jde poznat, že uživatelé, kteří mohou spustit všechny transakce (tři uživatelé, kteří mohou spustit 127579 transakcí) mají s největší pravděpodobností přiřazený profil SAP_ALL.

Analýza umožnila identifikovat, že není nastavena přesná definice nastavení oprávnění dle pracovní pozice. Zatím nelze přesně určit, zda rozdíly v počtu spustitelných transakcí nejsou z důvodu již částečně nastavené metodiky SoD nebo jiných interních pravidel. Je tedy nutné provést podrobnější porovnání uživatelů.

Srovn...	Objekt	Označení objektu oprávnění
●○○	B_NOTIF_EX	Rozšířená změna druhu zprávy
●○○	F_IDFIVAT	Elektronický ledger DPH
●○○	F_KNA1_AEN	Odběratel: Oprávnění ke změně pro určitá pole
●○○	F_LFA1_AEN	Dodavatel: Oprávnění ke změně určitých polí
●○○	P_RUNTIME	
●○○	S_ALV_LAYO	ALV Standardní layout
●○○	S_SCD0_OBJ	Změnové doklady objektu změnových dokladů
●○○	S_TABU_NAM	Přístup k tabulce via generické standardní nástroje
●○○	ZHP_AMT_PD	Povolení změnit částku při uznání požadavku na dbp
●○○	ZRTL_ORDE...	Retail objednávka
●○○	ZTR_ORDER	Převodka
○○■	/CWM/C_ACT	Activate Catch Weight Management in Client

Obrázek 6.3 Rozdíly oprávnění mezi dvěma uživateli

U uživatelů s rozdílným počtem spustitelných transakcí byla využita funkce

transakce SUIM pro porovnání dvou uživatelů, jako je zobrazeno na obrázku 6.4, ze kterého lze vyčíst, že uživatel č. 2 na rozdíl od uživatele č. 1 nemá dostatečné oprávnění k úpravě některých polí u zákazníků a dodavatelů (transakce XD02 a XK02), a také nemá přístup ke stejným tabulkám.

Transakce dále umožňuje se dvojklikem přesunout do detailu porovnání. Tímto způsobem je možné zjistit, že uživatel č. 2 nemá přístup k úpravě tabulky T001B (povolená účetní období) v transakci SM30. Dále je zde informace o tom, která role tento přístup umožňuje.

Analýzou bylo dále zjištěno, že jsou všichni uživatelé správně přiřazeni v odpovídajících skupinách. Hlavní výhodou tohoto přiřazení je možnost hromadné úpravy všech uživatelů, nichž jsou ve skupině. Tímto je umožněno přiřazení nové role nebo odebrání staré role u všech uživatelů zároveň.

6.4 Analýza kritických oprávnění

Transakce SUIM umožňuje využití kontroly kritických oprávnění podle vstupní varianty. Variantu kritických oprávnění je možné vytvořit v transakci SU_VCUSRV-AR_CHANGE. V této transakci byla vytvořena varianta ZTROJAN_DP. Varianta je v podstatě seznam kontrol, které se mají provádět.

Aby bylo možné variantu používat, tak bylo nutné vytvořit seznam transakcí a operací, u kterých by bylo vhodné sledovat, zda je uživatel může spustit či nikoli. Seznam transakcí je založen na tabulce 4.2 a dále došlo k rozšíření i o operace:

- transakce: SU01, SE37, SE38, SE14, SCC5, SE11, SU10, SM30, F110, MIRO
- operace: úprava uživatelských rolí a profilů, debugování (sledování běhu programu) a zakládání či změna rolí v transakci PFCG

Popis			
Uživatel	TESTC1	Neúspěšné kontroly od	30.04.2023 11:46:12
Systém	HED	Klient	500
Datum	30.04.2023	Čas	14:46:12
Instan.	hedci_HED_00	Parametry profilu opr./nové - buffer	4

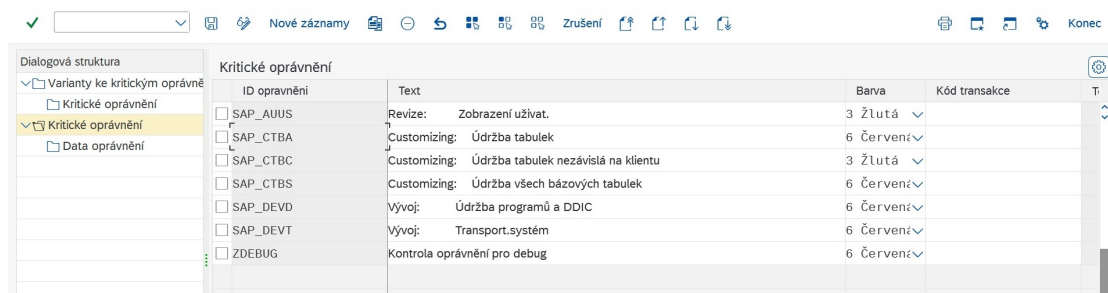
⚡ Kontrola oprávnění se nezdařila			
▼ Datum 30.04.2023 Čas 14:46:06 Transakce			
▼ Objekt oprávnění S_DEVELOP ABAP Workbench			
Pole oprávnění	ACTVT	Činnost	
Pole oprávnění	DEVCLASS	Paket	
Pole oprávnění	OBJNAME	Název objektu	
Pole oprávnění	OBJTYPE	Typ objektu	
Pole oprávnění	P_GROUP	Skupina opráv. programu ABAP/4	

Obrázek 6.4 Neúspěšná kontrola oprávnění pro debugování

Oprávnění byly nastavovány pomocí dvou účtů SAP. Prvním byl účet, který má přístup do transakce SU53 (Kontroly oprávnění) a druhým účtem byl testovací

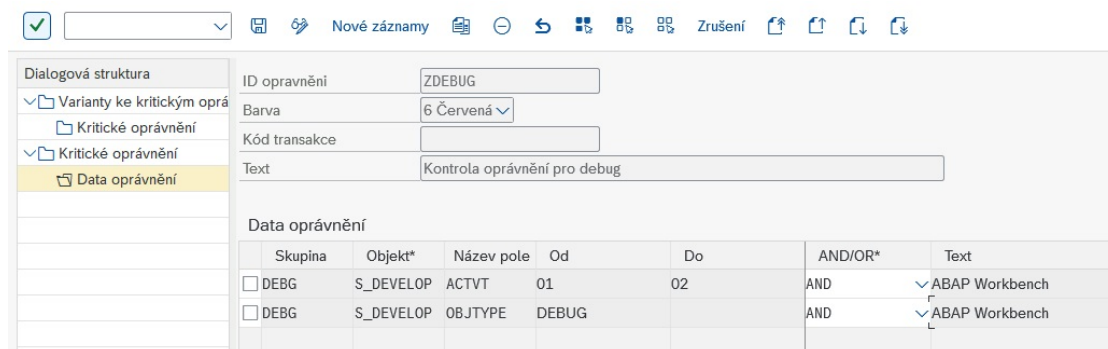
účet bez jakéhokoli oprávnění. Tímto je zajištěno, že uživatel bez oprávnění nebude moci spustit žádnou transakci a půjde jednoduše zjistit, které kontroly oprávnění se nezdařily, jako je zobrazeno na obrázku 6.4.

Na obrázku 6.5 je zobrazeno přidání nově vytvořeného oprávnění do seznamu kritických oprávnění nazvané ZDEBUG. Toto oprávnění je následně potřeba zahrnout do vytvořené varianty ZTROJAN_DP. Při názvu čehokoli se stále vychází z doporučení společnosti SAP o pojmenovávání zákaznických úprav znaky „Z“ nebo případně „Y“.



Obrázek 6.5 Vytvoření kritického oprávnění ZDEBUG

Po přidání oprávnění je nutné ještě nastavení parametrů zvolením záložky „Data oprávnění“. Bez tohoto kroku by oprávnění nemělo žádnou funkcionalitu. Přidání je zobrazeno na následujícím obrázku 6.6. Nastavení umožňuje i kombinaci kontrol několika oprávnění. Bylo by tedy možné všechny kontroly oprávnění zahrnout pouze do jednoho prvku oprávnění. Ovšem z důvodu přehlednosti výstupu je vhodnější pro každou kontrolu vytvořit nový prvek oprávnění.



Obrázek 6.6 Nastavení kritického oprávnění ZDEBUG

Při spouštění transakce se provádí více kontrol než pouze jedna. První kontrolou je spustitelnost transakce pro daného uživatele. V případě, že uživatel transakci spustit může, tak stále musí splnit podmínky pro jednotlivé úkony. U těchto úkonů dochází ke kontrole oprávnění (hodnota pole ACTVT). Na základě této hodnoty se určují oprávnění uživatele. Všechny činnosti u jednotlivých autorizačních objektů jsou obsaženy v tabulce TACTZ.

Bylo by tedy možné uživatele nechat spustit transakce, jako jsou MIRO, F110 nebo SCC5, ale neumožnit mu vytvářet či upravovat záznamy nastavením pouze aktivity s hodnotou 03.

Počet nalezených objektů pro kritická oprávnění: 13

Systém HED Klient 500 Zkontroloval TROJANJ 01.05.2023 13:22:37

Kritéria výběru:
 Kritická oprávnění X
 Varianta ZTROJAN_DP
 Uživatel I EQ

ID	CA	Text kritického oprávnění (CA)	Uživatel	DI	Jméno	Skupi...	Platí od	Platí do	ČísloZú...	Typ
SAP_AUPM		Administrace: Údržba profilu					01.08.2022	31.12.9999		A Dialog
SAP_CTBA		Customizing: Údržba tabulek					01.08.2022	31.12.9999		A Dialog
SAP_CTBC		Customizing: Údržba tabulek nezávislá na klientu					01.08.2022	31.12.9999		A Dialog
SAP_CTBS		Customizing: Údržba všech bazových tabulek					01.08.2022	31.12.9999		A Dialog
SAP_DEVD		Vývoj: Údržba programů a DDIC					01.08.2022	31.12.9999		A Dialog
SAP_DEVT		Vývoj: Transport systém					01.08.2022	31.12.9999		A Dialog
ZDEBUG		Kontrola oprávnění pro debug					01.08.2022	31.12.9999		A Dialog
ZF110		Kontrola spustitelnosti transakce F110					01.08.2022	31.12.9999		A Dialog
ZMIRO		Kontrola spustitelnosti transakce MIRO					01.08.2022	31.12.9999		A Dialog
ZROLECREATE		Oprávnění zakládat role					01.08.2022	31.12.9999		A Dialog
ZROLEEDIT		Oprávnění upravovat role					01.08.2022	31.12.9999		A Dialog
ZSCC5		Kontrola spustitelnosti transakce SCC5					01.08.2022	31.12.9999		A Dialog
ZTAB_GDPR		Oprávnění zobrazovat tabulky obsahující osobní data					01.08.2022	31.12.9999		A Dialog

Obrázek 6.7 Výsledek kontroly kritických oprávnění v transakci SUIM

Obrázek 6.7 zobrazuje výsledek použití kontroly oprávnění v transakci SUIM pro nově vytvořenou variantu u uživatele, jenž má profil SAP_ALL. Na obrázku lze vidět, že transakce správně vyhodnotila, že uživatel má všechny z kritických oprávnění.

6.5 Analýza kritických uživatelských oprávnění u nejpoužívanějších rolí

Mezi nejpoužívanější role ve společnosti HP TRONIC Zlín patří:

- Z_HPT_USER - role, která by měla uživateli přidávat základní oprávnění pro práci se systémem SAP.
- Z_USER_TEMPORARY - mělo se jednat o dočasnou roli, která byla vytvořena v roce 2009 a je stále hojně používána i v současnosti.

Tato kapitola je zaměřena právě na tyto dvě role z pohledu kritických oprávnění a dalších oprávnění, u kterých by bylo vhodné vytvořit samostatnou roli.

Testování těchto oprávnění opět probíhalo za využití kontroly kritických oprávnění v transakci SUIM. Ovšem místo uživatelského jména byl na vstupu vyplněn název role.

6.5.1 Role Z_HPT_USER

První zvolenou rolí je role Z_HPT_USER, která obsahuje přibližně 100 autorizačních objektů. Roli má na produktivním prostředí přiděleno celkem 964 aktivních uživatelů z celkového počtu 1200 uživatelů.

Kód 2. Zjištění počtu aktivních uživatelů s rolí Z_HPT_USER

```
SELECT COUNT(DISTINCT UNAME) FROM AGR_USERS AS A
  INNER JOIN USR02 AS U ON U.BNAME = A.UNAME
 WHERE A.AGR_NAME = 'Z_HPT_USER'
 AND A.FROM_DAT < '2023-01-04'
 AND A.TO_DAT > '2023-01-05'
 AND U.GLTGV < '2023-01-04'
 AND U.GLTGB > '2023-01-05'
 AND U.UFLAG = 0
"UFLAG - informace důvodu blokace: 0 = OK,
"32/64 = lokální/globální blokování administrátorem,
"128 = chybné přihlášení (několik neúspěšných pokusů).
"U více důvodů blokace dochází k součtu těchto čísel.
```

První krok analýzy je kontrola kritických oprávnění v transakci SUIM. Obrázek 6.8 poskytuje informace o výstupu u role Z_HPT_USER.

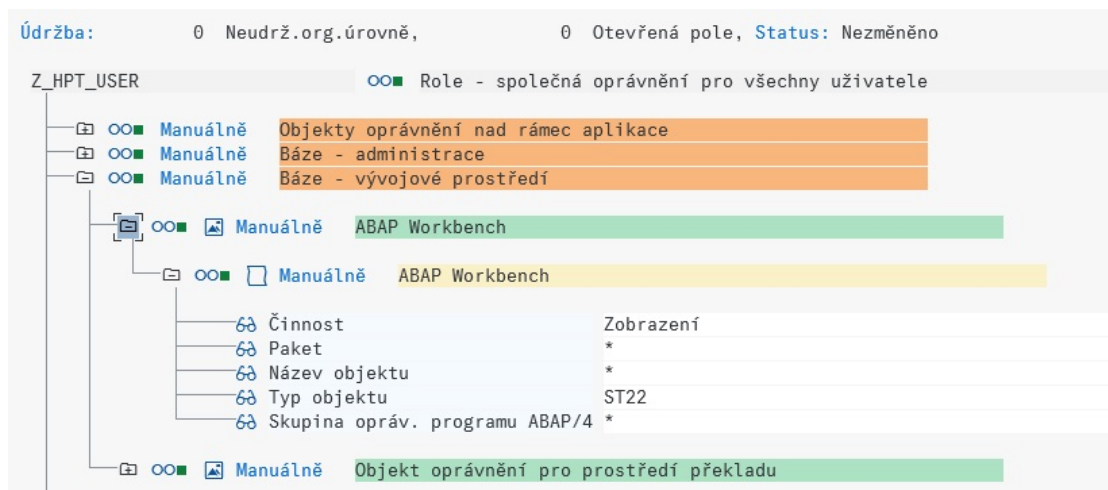
Počet nalezených objektů pro kritická oprávnění: 1					
Systém	HEP	Klient	500	Zkontroloval	TROJANJ 02.05.2023 12:41:17
Kritéria výběru:					
Kritická oprávnění		X			
Varianta		ZTROJAN_DP			
Role	I	EQ	Z_HPT_USER		
ID CA	Text kritického oprávnění (CA)	Role	T...	Označení role	
SAP_AUAM	Administrace: Údržba oprávnění	Z_HPT_USER			
SAP_AUPM	Administrace: Údržba profilu				
SAP_AUUM	Administrace: Údržba uživatelů				
SAP_CTBA	Customizing: Údržba tabulek				
SAP_CTBC	Customizing: Údržba tabulek nezávislá na klientu				
SAP_CTBS	Customizing: Údržba všech bázových tabulek				
SAP_DEVD	Vývoj: Údržba programů a DDIC				
SAP_DEVT	Vývoj: Transport systém				
ZDEBUG	Kontrola oprávnění pro debug				
ZF110	Kontrola spustitelnosti transakce F110				
ZMIRO	Kontrola spustitelnosti transakce MIRO				
ZROLECREATE	Oprávnění zakládat role				
ZROLEEDIT	Oprávnění upravovat role				
ZSCC5	Kontrola spustitelnosti transakce SCC5				

Obrázek 6.8 Kontrola kritického oprávnění u role Z_HPT_USER

Výsledek vypisuje všechny objekty kontroly. Avšak pouze u objektů, jenž mají vyplněný text ve sloupcích „Role“ a „Označení role“ bylo nalezeno hledané oprávnění.

Jediné kritické oprávnění, které bylo nalezeno je údržba profilu uživatele. Toto oprávnění samo o sobě problematické nijak není. Problematické by mohlo být pouze v případě, že by měl uživatel zároveň možnost údržby uživatelů.

Přestože nedošlo k vyplnění kritického oprávnění SAP_DEVD, tak je stále vhodné provést dodatečnou kontrolu v transakci PFCG. Důvodem je to, že základní kontrola vytvořená společností SAP kontroluje, zda je u autorizačního objektu S_DEVELOP pouze hodnota činnosti 01, ale nekontroluje ostatní hodnoty.



Obrázek 6.9 Nastavení autorizačního objektu S_DEVELOP

Obrázek 6.9 ukazuje, že uživatelé s přiřazenou rolí Z_HPT_USER mohou pouze zobrazovat informace v transakci ST22 (zobrazení chyby běhu programu). Nejedná se o nijak kritické oprávnění, ale právě naopak umožňuje uživateli případnou chybu vyfotit a zaslat ji vývojáři.

Provedení kontroly autorizačního objektu S_DEVELOP (ABAP Workbench) je obecně velmi důležité. Příkladem může být oprávnění použití ladění (ladění neboli debug lze zavolat z jakékoli obrazovky použitím funkčního kódu /h), jenž je nejmocnějším samostatným oprávněním, které uživatel může mít k dispozici. Zkušený uživatel s tímto oprávněním dokáže obejít téměř veškeré autorizace. Toto oprávnění mu například dává možnost upravovat tabulky v transakci SE16N na datábázové úrovni (známé jako SAP_EDIT), kde navíc může obejít samotné uložení informace o změně (logování) do databáze. [37]

Možnost spuštění ladění (s hodnotami oprávnění 01 a 02) je ve výstupu transakce SUIM odhaleno nově vytvořeným kritickým oprávněním ZDEBUG. Možnost spuštění ladění pouze s hodnotou 03 nijak nebezpečné není, protože uživatel nemůže měnit výstup programu.

Vhodné je také zkontrolovat možnost spuštění jednotlivých tříd (transakce SE24), funkčních modulů (transakce SE37) či programů (transakce SE38). Jestliže by uži-

vatel měl možnost spouštět funkční moduly, tak by mohl například spustit funkční modul umožňující uživateli měnit data v jakékoli tabulce na databázové úrovni (SE16N_INTERFACE). Jedná se v podstatě o stejný typ změny jako v případě použití ladění. Ovšem stále zde probíhá kontrola oprávnění upravovat záznamy v tabulkách a není možné přeskočit krok ukládání informace o změně.

Role Z_HPT_USER se na základě analýzy dá považovat za téměř bezpečnou. Jestliže dojde k odebrání oprávnění vytváření a změny u údržby profilu bude možné tuto roli i nadále používat.

6.5.2 Role Z_USER_TEMPORARY

Druhou nejpoužívanější rolí je Z_USER_TEMPORARY, která má dle stejného SQL dotazu přiřazeno aktivních 709 uživatelů. Role obsahuje přibližně 2400 autorizačních objektů.

Pro tuto roli byla opět provedena kontrola kritických oprávnění.

Počet nalezených objektů pro kritická oprávnění: 7

Systém

HEP

Klient

500 Zkontroloval TROJANJ 02.05.2023 12:41:47

Kritéria výběru:

Kritická oprávnění

X

Varianta

ZTROJAN_DP

Role

I EQ Z_USER_TEMPORARY

ID CA	Text kritického oprávnění (CA)	Role	T...	Označení ro...
SAP_AUAM	Administrace: Údržba oprávnění			
SAP_AUPM	Administrace: Údržba profilu			
SAP_AUUM	Administrace: Údržba uživatelů			
SAP_CTBA	Customizing: Údržba tabulek	Z_USER_TEMPORARY		Dočasná role
SAP_CTBC	Customizing: Údržba tabulek nezávislá na klientu	Z_USER_TEMPORARY		Dočasná role
SAP_CTBS	Customizing: Údržba všech bazových tabulek	Z_USER_TEMPORARY		Dočasná role
SAP_DEVD	Vývoj: Údržba programů a DDIC			
SAP_DEVT	Vývoj: Transport systém	Z_USER_TEMPORARY		Dočasná role
ZDEBUG	Kontrola oprávnění pro debug			
ZF110	Kontrola spustitelnosti transakce F110	Z_USER_TEMPORARY		Dočasná role
ZMIRO	Kontrola spustitelnosti transakce MIRO	Z_USER_TEMPORARY		Dočasná role
ZROLECREATE	Oprávnění zakládat role			
ZROLEEDIT	Oprávnění upravovat role			
ZSCC5	Kontrola spustitelnosti transakce SCC5	Z_USER_TEMPORARY		Dočasná role

Obrázek 6.10 Kontrola kritického oprávnění u role Z_USER_TEMPORARY

Výsledek kontroly kritických oprávnění zobrazuje celkem 7 kritických oprávnění. Z nichž jsou celkem čtyři výstupem kontrol oprávnění společnosti SAP a zbylé tři jsou možnosti spustit transakci.

Kód transakce	SCC5	Uloženo					
Objekty oprávnění							
Objekt Hodnoty polí Sledování							
Status	Objekt	Označení objektu	TST...	KonZn	Návrh	Paket	Zkratka komponenty
☐	S_BTCH_JOB	Dávkové zpracování: Operace v dávkových jobech		Kontrola	Ne	SBTC	BC-CCM-BTC
☐	S_DEVELOP	ABAP Workbench		Kontrola		SEU	BC-DWB-UTL-BRR
☐	S_PRO_AUTH	IMG: Nová oprávnění pro projekty		Kontrola		SCSC	BC-CUS-TOL-IMG
☐	S_SPO_DEV	Spooler: Oprávnění pro zařízení		Kontrola		SPO...	BC-CCM-PRN
☐	S_TABU_DIS	Údržba tabulky (pomocí stand.nástr.- např.SM30)		Kontrola		SVIM	BC-CUS-TOL-TME
☐	S_TCODE	Kontrola kódu transakce při spuštění transakce		Kontrola		SUSR	BC-SEC-USR-ADM
☐	S_TRANSPRT	Transport Organizer		Kontrola		SCT...	BC-CTS-ORG
☐	S_CLNT_IMP	Import dat při kopírování klienta		Kontrola	Ano	STRM	BC-CTS-CCO
☐	S_DATASET	Oprávnění pro přístup k souboru		Kontrola		SECC	BC-SEC
☐	S_TABU_CLI	Údržba tabulek nezávislých na klientu		Kontrola		SVIM	BC-CUS-TOL-TME
☐	S_USER_AG...	Oprávnění: Kontrola rolí		Kontrola		S_P...	BC-SEC-AUT-PFC
☐	S_USER_G...	Údržba km.souboru uživ.: Skupiny uživatelů		Kontrola		SUSR	BC-SEC-USR-ADM
☐	S_USER_PR...	Údržba kmen.soub.uživatelů: Profil oprávnění		Kontrola		SUSR	BC-SEC-USR-ADM

Dvojklikem na název objektu je možné zobrazit, jaké hodnoty jsou k provedení transakce třeba. Obrázek 6.12 zobrazuje potřebné hodnoty u autorizačního objektu S_USER_AGR. Jedná se o autorizační objekt kontroly rolí, u kterého musí být vyplněna činnost 01 a 06 (výmaz).

Navrhované hodnoty oprávnění (S_USER_AGR)

Objekt	Název pole	Zobraz...	Od	Hodnota do
S_USER_AGR	ACT_GROUP	68	*	
	ACTVT	68	01	
		68	06	

Oprávnění u transakcí F110 a MIRO jsou u role Z_USER_TEMPORARY zcela v pořádku. Při kontrole autorizačních objektů u transakce SCC5 bylo zjištěno, že

Tabulka 6.3 Hodnoty autorizačních objektů u role Z_USER_TEMPORARY

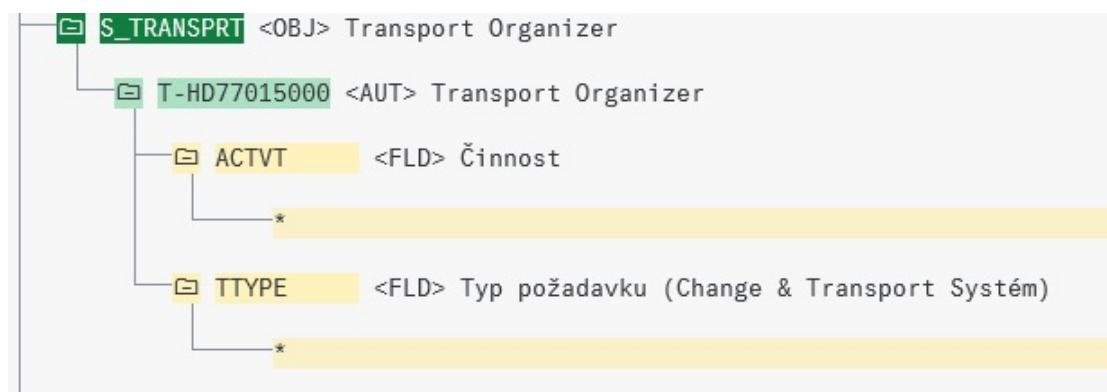
Název transakce	Požadované autorizační objekty	01	02	03-XX
F110	F_REGU_BUK	-	-	-
	F_REGU_KOA	-	-	-
MIRO	M_RECH_AKZ	-	-	-
	M_RECH_WRK	-	-	-
SCC5	S_CLNT_IMP	✓	✓	✓
	S_DATASET	✓	✓	✓
	S_TABU_CLI	✓	✓	✓
	S_USER_AGR	-	-	✓
	S_USER_GRP	-	-	✓
	S_USER_PRO	-	-	✓

autorizační objekty S_CLNT_IMP, S_DATASET a S_TABU_CLI požadavky pro vykonání transakce splňují. Naopak u zbylých autorizačních objektů jsou třeba oprávnění s hodnotou 01, ale tyto objekty mají pouze hodnotu 03, případně 08 (zobrazení změn).

Výmaz klienta je hlubokým zásahem do systému a je možné, že by akce nebyla proveditelná ani, kdyby uživatel měl všechna požadovaná oprávnění. Je velmi důležité se na tyto oprávnění v návrhu zabezpečení zaměřit. U transakce SCC5 není žádný pádný důvod, proč by nemohla být uzamčena.

Kontroly oprávnění vytvořené společností SAP zabývající se údržbou tabulek (SAP_CTB*) by na produkčním prostředí nemuselo být potřeba řešit, protože systémové parametry takovou změnu zakazují. Nicméně k zvýšení bezpečnosti by mohlo být vhodné toto oprávnění od běžně používané role oddělit.

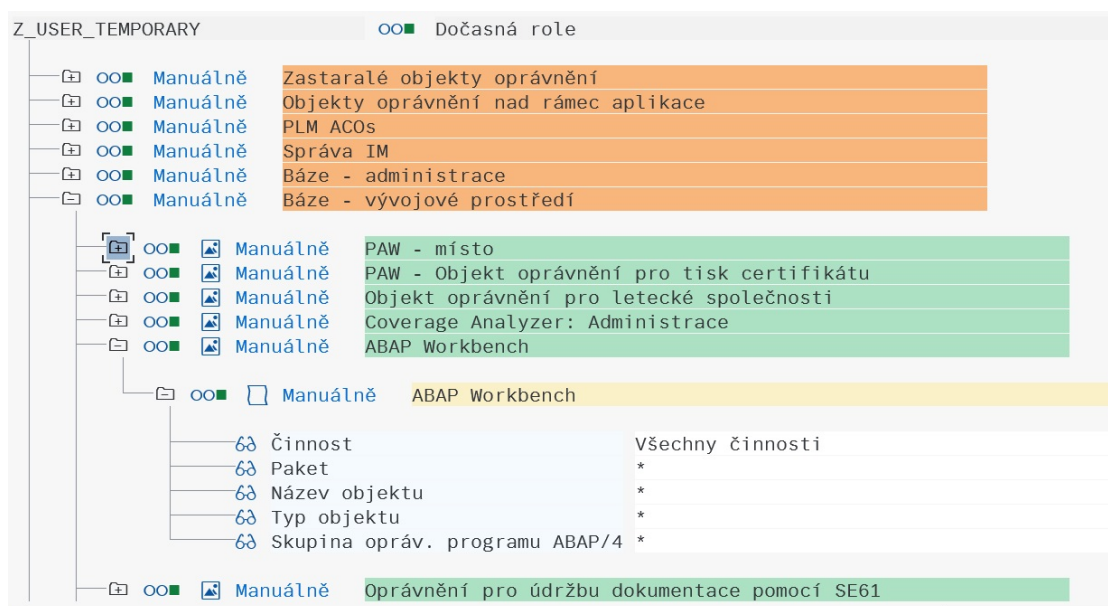
Každopádně tito uživatelé mají oprávnění pro používání transportního systému (SAP_DEVT). Mohou tedy provést změny na vývojovém prostředí a tyto změny mohou obratem transportovat na produkční prostředí. Důležité je tedy opět v transakci PFCG zkontrolovat, jaké transportní oprávnění mají.



Obrázek 6.13 Nastavení autorizačního objektu S_TRANSPRT

Obrázek 6.13 zobrazuje informaci o tom, že všichni uživatelé, kteří mají roli Z_USER_TEMPORARY mohou provádět všechny transportní akce. Od vytvoření transportního požadavku až po jeho transportování (transakce SE10, STMS). Oprávnění transportovat úpravy by v ideálním případě mělo mít pouze několik osob zabývajících se především těmito záležitostmi.

Důležité je zmínit, že jednotlivé role nejsou na všech vývojových prostředích totožné. Například na vývojovém prostředí má role Z_USER_TEMPORARY dle obrázku 6.14 všechna oprávnění v autorizačním objektu S_DEVELOP.



Obrázek 6.14 Nastavení autorizačního objektu S_DEVELOP

Možnost transportovat a zároveň vyvíjet různé objekty je kritickou kombinací oprávnění. Eventuálně může velmi negativně ovlivnit produkční prostředí.

6.5.3 Seznam rolí obsahující kritická oprávnění

Po vytvoření kontrolního programu v kapitole 8, který umožňuje hromadnou kontrolu bylo zjištěno, že všechny odvozené role od role Z_USER_TEMPORARY mají neomezená oprávnění v autorizačním objektu S_DEVELOP. Jedná se o příklad z obrázku 6.14., který je ovšem na produkčním prostředí nikoli pouze na vývojovém. Od této role je odvozeno celkem jedenáct rolí, které jsou rozděleny dle organizací (účetních okruhů). U těchto rolí došlo k odvození pravděpodobně v době, když role Z_USER_TEMPORARY měla neomezené práva v autorizačním objektu S_DEVELOP. Přestože toto oprávnění je z rodičovské role již zcela odebráno, tak u odvozených rolí stále přetrvává.

Tyto role má přiřazeno velké množství uživatelů a je důležité, aby došlo k jejich důkladné revizi.

Tabulka 6.4 zobrazuje přehled kontrolovaných rolí a nalezených kritických oprávnění a jejich hodnot, jež obsahují.

Tabulka 6.4 Seznam kontrolovaných rolí a nalezených kritických oprávnění

Název role	Kritické autorizační objekty	Hodnoty
Z_HPT_USER	S_USER_PRO	*
Z_HPT_USER_2100	-	-
Z_USER_TEMPORARY	S_TABU_CLI	*
	S_TABU_DIS	*
	S_TRANSPORT	*
Z_USER_TEMPORARY_2100	S_DEVELOP	*
	S_TABU_CLI	*
	S_TABU_DIS	*
	S_TRANSPORT	*
Z_USER_TEMPORARY_FI	-	-
Z_USER_TEMPORARY_FI_2100	S_TABU_CLI	*
	S_TABU_DIS	*

6.6 Analýza nastavení SoD

Analýza současného nastavení SoD v modulu FI/CO byla provedena pomocí porovnávání uživatelů mezi sebou. Ukazatelem jakékoli formy nastavení SoD by bylo to, že jeden uživatel může určité dokumenty zakládat, ale nemá přístup ke změně. Zatím co druhý má přesně opačné oprávnění. Druhou možností detekce SoD je přístup k rozdílným transakcím a autorizačním objektům.

O SoD se nejedná v případě, že jeden uživatel má stejné základní pravomoce jako druhý uživatel, ale zároveň má ještě několik pravomocí navíc. Stejným případem může být i to, že budou mít uživatele pravomoci rozdílné, které mezi sebou nijak nesouvisí.

Analýza SoD vychází ze stejného principu porovnávání dvou uživatelů, jak již bylo zobrazeno v kapitole 6.3.

Výsledkem analýzy bylo zjištěno, že u všech 29 uživatelů žádné rozdělení pravomocí nastaveno není. Ve většině případů se jednalo o možnost provádět určité transakce navíc. V kapitole 7 budou vytvořeny návrhy uživatelských rolí umožňující použití SoD.

6.7 Analýza nastavení systémových parametrů

Závěrem kapitoly je kontrola současného nastavení systémových parametrů. Jsou to parametry zabývající se nastavením bezpečnosti hesla, na které je tato kapitola

změřena. Bezpečnost hesla jde nastavovat dvěma způsoby: zakázané hesla a parametry hesla.

6.7.1 Kontrola zakázaných hesel

Seznam zakázaných hesel je uložen v tabulce USR40. Úpravu této tabulky je možné provádět v transakci SM30. V současné době je tabulka zcela prázdná a bylo by vhodné posloupnosti znaků „*123*“ nebo „*heslo*“ zakázat.

6.7.2 Kontrola parametrů hesla

Hodnoty parametrů hesla je možné zobrazit v programu RSPARAM (zobrazení parametrů profilu). Na základě tohoto výstupu byla vytvořena tabulka 6.5.

Tabulka 6.5 Parametry hesla v programu RSPARAM

Parametr	Aktuální	Přednastavená	Doporučená
login/min_password_diff	1	1	1
login/min_password_digits	1	0	2
login/min_password_letters	1	0	2
login/min_password_lng	8	4	10
login/min_password_lowercase	1	0	1
login/min_password_specials	0	0	2
login/min_password_uppercase	0	0	1
login/password_history_size	5	5	20
login/min_password_diff	1	1	4

Výsledkem kontroly bylo zjištěno, že by bylo vhodné se zamyslet nad zvýšením délky hesla na minimálně 10 znaků, a také nad zvýšením minimálního počtu použitých znakových sad. Hesla jsou do databáze ukládány v bezpečné - zahashované podobě (včetně použití saltu).

7 NÁVRH A REALIZACE NASTAVENÍ BEZPEČNOSTI

Z výsledku analýzy vyšlo, že role Z_HPT_USER až na možnost údržby profilu nijak nebezpečné oprávnění neobsahuje. Vzhledem k tomu, že se jedná o obecnou roli, kterou mají téměř všichni uživatelé, tak by bylo vhodné toto oprávnění z role odebrat a vytvořit novou roli. Nová role bude mít přiděleny pouze autorizační objekty pro upravování uživatelských oprávnění.

Hlavní částí této kapitoly je provedení návrhu nových rolí, které budou mít za cíl nahradit často používané a velmi obsáhlé dočasné role Z_USER_TEMPORARY a Z_USER_TEMPORARY_FI. Na základě tohoto návrhu bude provedeno vytvoření nových rolí. U nově vytvořených rolí musí být jistota, že budou zachovány všechny potřebné funkcionality, aby nedošlo k narušení produkčního prostředí. Z nově vytvořené role budou moci opět být odvozeny další role, které budou omezeny jen na určité účetní okruhy.

Poté co budou všechny obecné role vytvořeny, tak dojde k vytvoření rolí umožňujících rozdělení pravomocí. Jednou z těchto rolí je role, která bude umožňovat přidělování oprávnění pouze vybrané skupině uživatelů (modul FI/CO). Zároveň s tímto omezením budou omezeny role a profily, které mohou být uživatelům ve zmíněné skupině přiděleny.

Přestože při návrhu nových rolí, bude brán velký důraz na zachování hlavní funkcionality oprávnění, tak by stále bylo vhodné, aby došlo k jejich důkladnému otestování na testovacím prostředí. Role by na produkční prostředí byly nasazeny, jakmile bude možné s jistotou říci, že funkcionality byla zachována. V diplomové práci dojde na produkčním prostředí pouze ke změnám kritických oprávnění, které by mohly narušit chod podniku.

Závěr kapitoly se zaměřuje na nastavením systémových parametrů zabývajících se hesly.

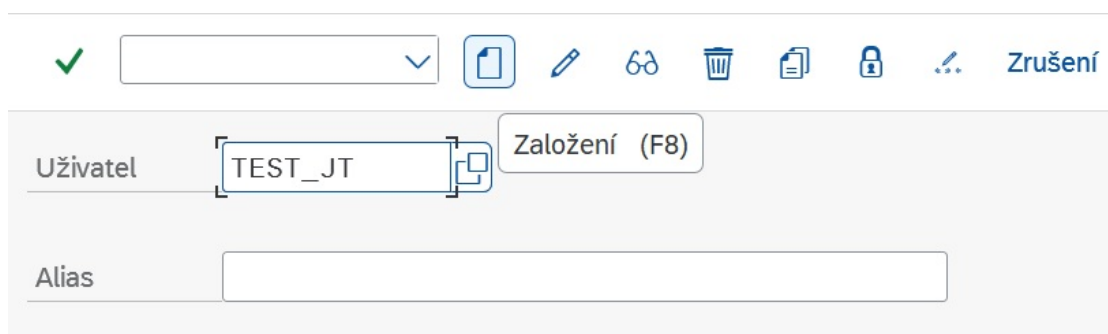
7.1 Vytvoření testovacího uživatele

Účelem testovacího uživatele je možnost si prakticky otestovat správnou funkčnost změněných rolí. Na základě testování doplnit či upravit chybějící oprávnění.

Vytváření, úprava a zobrazení uživatelů se provádí v jedné transakci. Jedná se opět o transakci SU01 (případně SU10 pro hromadnou údržbu), která již byla několikrát zmíněna v předchozích kapitolách.

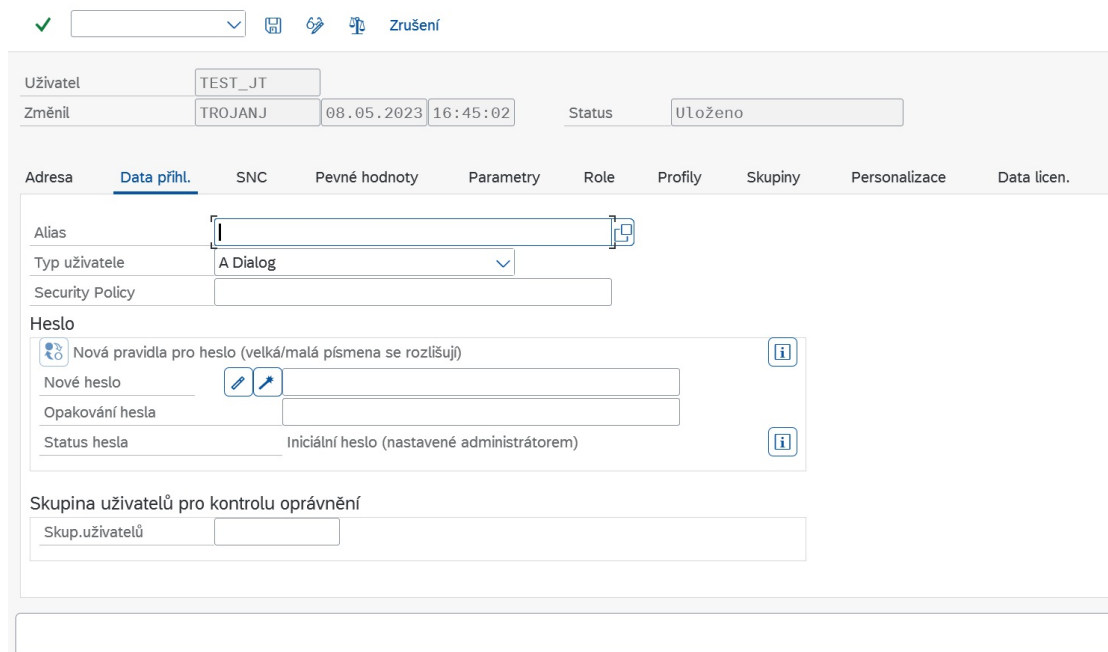
Pro založení uživatele stačí do pole „Uživatel“ napsat požadované uživatelské jméno a stisknout tlačítko pro založení. V případě diplomové práce se jedná o uživatele s názvem TEST_JT. U klasických uživatelů ve společnosti HP TRONIC

se používá příjmení plus první znak křestního jména. Pro vytváření testovacího uživatele není určena přesná jmenná konvence.



Obrázek 7.1 Založení uživatele TEST_JT

Po založení uživatele je potřeba vyplnit pouze jediné povinné pole, kterým je příjmení. Nutné je také nastavit uživateli iniciální heslo, aby se uživatel mohl do systému přihlásit.



Obrázek 7.2 Vytvoření iniciálního hesla pro prvotní přihlášení

Po úspěšném prvním přihlášení je uživatel upozorněn na nutnost provést změnu hesla, které bude známo pouze jemu. Uživatel tak má možnost vytvořit si vlastní unikátní heslo, které bude sloužit jako osobní identifikace při přístupu k systému.

7.1.1 Vytvoření skupiny uživatelů

Pro rozpoznání testovacích uživatelů byla vytvořena samostatná skupina uživatelů. Vytváření nových skupin uživatelů a případné přidání uživatelů do nich se provádí

v transakci SUGR. V této transakci došlo k vytvoření skupiny uživatelů TESTUSR. Přidání uživatele do skupiny uživatelů je možné přímo v transakci SUGR nebo v záložce „Skupiny“ v transakci SU01. Tato skupina je čistě organizační a slouží pro lepší přehlednost či hromadnou údržbu využitím transakce SU10.

Obrázek 7.3 Přidání uživatele do skupiny uživatelů

Nicméně existuje ještě jedna skupina, kterou může mít každý uživatel vyplněnou pouze jednou. Jedná se o skupinu uživatelů pro kontrolu oprávnění (viz. obr. 7.2). Tato skupina je kontrolována u autorizačního objektu S_USER_GRP. Příkladem využití může být hlavní účetní, který by mohl měnit uživatelská oprávnění pouze u uživatelů, kteří jsou ve skupině spadající pod účetnictví (skupina ZL_FI). Na obrázku 7.4 je zobrazen příklad nastavení autorizačního objektu, který umožní provádět změny pouze u uživatelů, kteří jsou ve skupině TESTUSR (nebo nejsou v žádné).

Obrázek 7.4 Příklad nastavení autorizačního objektu S_USER_GRP

7.2 Metodika nastavení uživatelských rolí

V návrhu metodiky nastavení uživatelských oprávnění jsou zohledněna některá základní pravidla. Jedním z hlavních principů je, že žádná potenciálně kritická oprávnění by neměla být přiřazena k rolím, které jsou široce využívány. Dále následují další pravidla:

1. Stanovení hierarchie rolí: Vytvoření hierarchie rolí umožní přehlednější a strukturovanější organizaci oprávnění. Každá role by měla být jasně definována a měla by být přiřazena pouze nezbytná oprávnění pro danou úroveň. Toto pravidlo platí například pro roli Z_HPT_FINANCE v rámci diplomové práce.
2. Pravidla pro přiřazování oprávnění: Definování pravidel pro přiřazování oprávnění může zabránit nadměrnému nebo neoprávněnému přístupu. Například, aby bylo možné přiřadit kritická oprávnění, musí existovat důvodová zpráva a schválení nadřízeného.
3. Pravidelné revize oprávnění: Zavedení pravidelných revizí oprávnění umožní aktualizovat a ověřit platnost přidělených oprávnění pro každou roli. Revize by měly být prováděny pravidelně a měly by zahrnovat kontrolu a odstranění nepotřebných nebo zastaralých oprávnění. Tím se zajistí, že uživatelé mají pouze oprávnění, která skutečně potřebují pro svou práci.

Zahrnutí těchto prvků do metodiky by přineslo další úroveň zabezpečení a zjednodušilo správu uživatelských oprávnění.

Při vytváření nových rolí v budoucnosti je důležité dodržovat tuto metodiku. Tím se dosáhne vyšší úrovně bezpečnosti a lepšího přehledu nad uživatelskými oprávněními.

7.3 Úprava stávající role

Kapitola zobrazuje postup při změně kritického oprávnění u role Z_HPT_USER, u které dojde k úplnému odebrání autorizačního objektu S_USER_PRO.

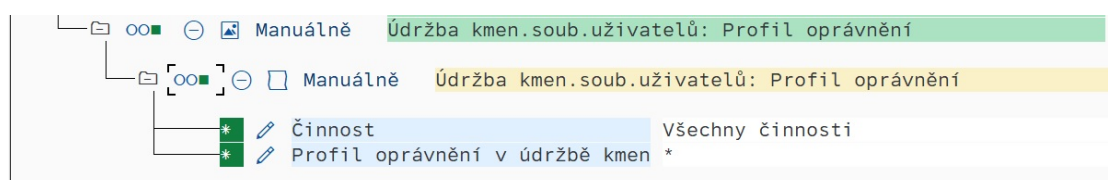
Úpravy jsou nejdříve prováděny na testovacím prostředí, na kterém by nijak nevadila případná nefunkčnost role. Při generování aktualizovaného profilu se může stát, že uživatelé dočasně přijdou o všechna oprávnění, které profil uděluje. Pro obnovení funkcionality stačí restartovat SAP GUI. Další výhodou nastavení role nejdříve na testovacím prostředí je následná možnost přenesení role na produkční prostředí, čímž bude zajištěno to, že na obou prostředí budou role stejně nastavené.

Odstraní se tím potenciální problém s rozdílnými výstupy programů z důvodu nedostatečných oprávnění.

Pro zajištění konzistence rolí mezi testovacím a produkčním prostředím bylo provedeno kopírování role z produkčního prostředí do testovacího prostředí. Toto kopírování bylo provedeno stažením role z produkčního prostředí a jejím nahráním do testovacího prostředí. Alternativně je také možné vytvořit kopii role pomocí transportního požadavku. Tímto způsobem je zajištěno, že role jsou identické a připravené k provádění změn ve všech prostředích.

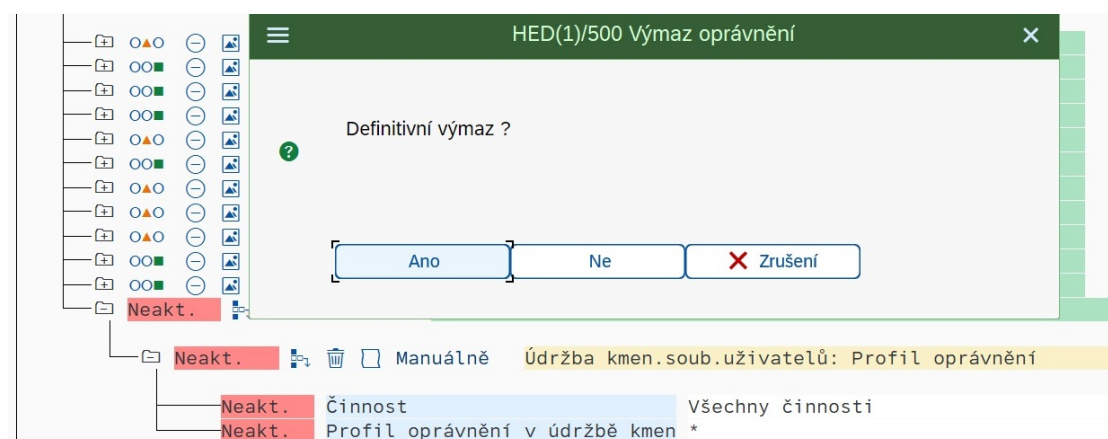
7.3.1 Úprava role Z_HPT_USER

U obecně používané role je dle metodiky vhodné, aby neobsahovala žádné kritické oprávnění. Z toho důvodu dojde k jeho odebrání. Odebírání autorizačních objektů probíhá ve dvou krocích. Prvním krokem je deaktivace autorizačního objektu.



Obrázek 7.5 Deaktivace autorizačního objektu S_USER_PRO

Po deaktivaci autorizačního objektu je možné provést jeho definitivní odstranění z role. Po úspěšném vymazání autorizačního objektu lze roli znovu vygenerovat, čímž se úprava role stane aktivní. Deaktivace a následné vymazání nežádoucích autorizačních objektů pomáhá udržovat role čisté a efektivně spravované.



Obrázek 7.6 Vymazání autorizačního objektu S_USER_PRO

Po provedení úprav neobsahuje upravená role žádné oprávnění, které by mohlo představovat riziko. Všechna kritická oprávnění byla odstraněna z role. Role byla upravena tak, aby vyhovovala bezpečnostním standardům a nastavené metodice.

V následující kapitole 7.4 zabývající se návrhem nových rolí, bude návrh role obsahující autorizační objekty zaměřené přímo na změnu uživatelských oprávnění.

7.4 Realizace metodiky u nastavení nových rolí

Tato kapitola se zaměřuje na implementaci nových rolí a definování jejich funkcionalit na základě navržené metodiky. Budou vytvořeny tři klíčové role, které budou sloužit jako základ pro odvození dalších rolí.

1. Z_HPT_ROLE - role umožňující u uživatelů měnit pouze ty role a profily, které byly vytvořeny ve společnosti HP TRONIC Zlín (role začínající znakem Z*).

 - Z_HPT_ROLE_ALL - role umožňující měnit všechny role a profily u všech uživatelů.
 - Z_HPT_ROLE_FI - role umožňující měnit jen určité role a profily u uživatelů spadajících do skupiny ZL_FI.

2. Z_HPT_DEFAULT - role přidávající oprávnění k provádění všech obecných funkcionalit v systému SAP.

 - Z_HPT_DEFAULT_* - role přidávající oprávnění k provádění všech obecných funkcionalit v systému SAP. S omezením na jednotlivé organizace.

3. Z_HPT_FINANCE - role přidávající oprávnění k provádění požadovaných funkcionalit v modulu FI/CO.

 - Z_HPT_FINANCE_* - role přidávající oprávnění k provádění požadovaných funkcionalit v modulu FI/CO. S omezením na jednotlivé organizace.

V následujících kapitolách jsou podrobně popsány jednotlivé fáze a kroky procesu vytváření všech rolí, jenž jsou klíčové pro úspěšnou implementaci tohoto procesu.

7.4.1 Role pro změnu uživatelských oprávnění Z_HPT_ROLE

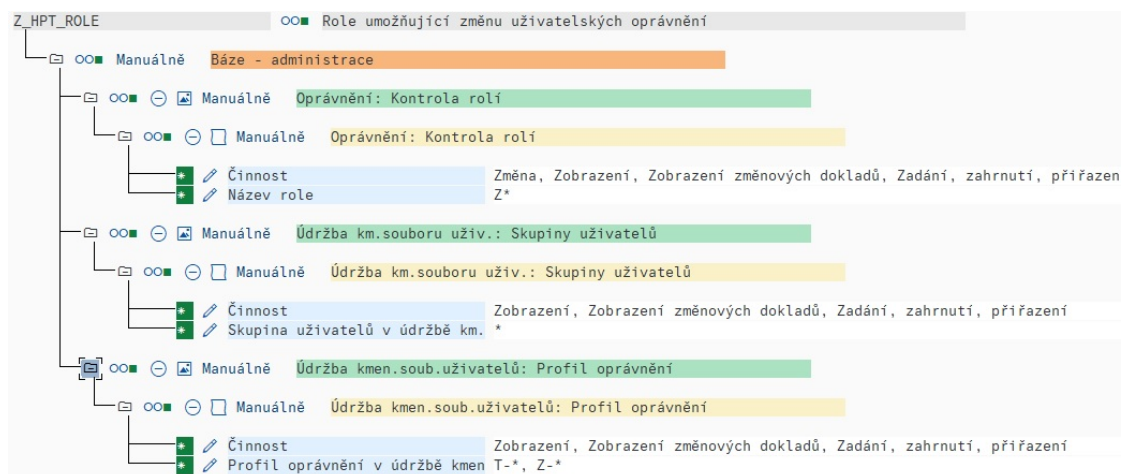
Aby uživatel mohl přidávat či odebírat role a profily u uživatelů, tak je nutné, aby měl celkem tři autorizační objekty. Seznam, popis a potřebné hodnoty jsou zobrazeny v tabulce 7.1.

U jednotlivých autorizačních objektů je možné navíc specifikovat název skupiny uživatelů, rolí nebo profilů. Ukázku nastavení obecné role Z_HPT_ROLE

Tabulka 7.1 Potřebné autorizační objekty pro změnu oprávnění

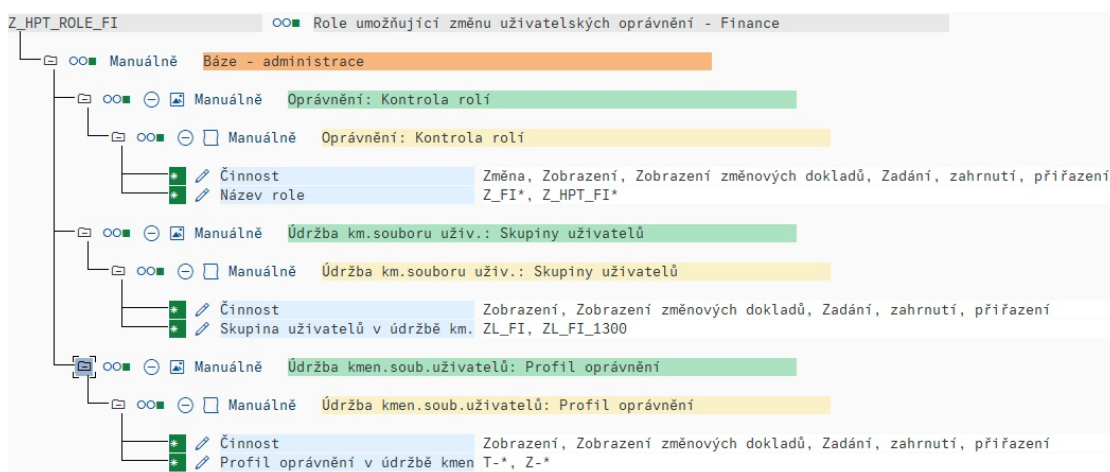
Aut. objekt	Popis	Hodnoty činnosti
S_USER_AGR	Oprávnění: Kontrola rolí	03, 08, 22
S_USER_PRO	Údržba kmen.soub.úživatelů: Profil oprávnění	03, 08, 22
S_USER_GRP	Údržba km.souboru uživ.: Skupiny uživatelů	*

zobrazuje obrázek 7.7. Zde je umožněno nastavení rolí Z*, což by se mělo rovnat pouze zákaznickým rolím. Skupiny uživatelů je možno upravovat všechny. Profily lze upravovat pouze ty, které začínají písmeny „T-“ (automaticky nastavené názvy profilu) a případně „Z-“ (profily se specifikovaným názvem).



Obrázek 7.7 Nastavení role Z_HPT_ROLE

Role Z_HPT_ROLE_FI je nastavena specificky na role a uživatele z FI/CO. Dovoluje přiřazovat pouze role zaměřené na finance uživatelům ve skupině ZL_FI.



Obrázek 7.8 Nastavení role Z_HPT_ROLE_FI

Role Z_HPT_ROLE_ALL umožňuje přidělení všech rolí a profilů všem uživatelům. Má tedy v těchto polích přiřazen znak * (vše). Hodnoty aktivit má totožné s předchozími rolemi.

Uživatel, jenž má tyto oprávnění, může pouze role uživatelům přidělovat či odebírat. Nemůže provádět jakékoli změny u jednotlivých rolí. Tato možnost je dána hodnotou činnosti 02. Dále by pro takové změny potřeboval ideálně další autorizační objekty S_USER_VAL, S_USER_AUT a případně S_USER_TCD. Tímto způsobem by se dalo přistupovat k rozdělení pravomocí. Jedná se o příklad z teoretické části diplomové práce, jehož realizace je součástí kapitoly 7.5.

7.4.2 Role udělující obecná oprávnění Z_HPT_DEFAULT

Tato role by měla být nástupcem role Z_USER_TEMPORARY. Role by měla stále obsahovat všechny funkcionality jejího předchůdce. Snahou při jejím vytváření bude odstranění co nejvíce oprávnění, které v produktivním prostředí nejsou vyžadovány nebo nejsou potřeba. Bližším zaměřením projdou autorizační objekty spadající pod modul FI/CO, kde zůstanou zachovány pouze ty objekty, které jsou nejvíce používány.

V ideálním případě by bylo možné roli Z_USER_DEFAULT přidat přesně ty autorizace, které uživatelé k obecných úkonům potřebují vždy. Ostatní oprávnění by byly přidány na základě pracovní pozice a požadovaného modulu.

Bohužel z důvodu zákaznického vývoje toto rozdělení není zcela možné. Některé z vyvinutých transakcí potřebují oprávnění modulu FI/CO (nejen tohoto modulu). Uživatel, u kterého by se na první pohled mohlo zdát, že oprávnění k modulu nepotřebuje, tak úkony běžící na pozadí mohou některé z funkcionalit modulu využívat. Chyba oprávnění by se nemusela projevit ani v transakci SU53. Nastavení takové funkcionality by vyžadovalo absolutní znalosti systému, která k dosažení vyžaduje mnoho let a v rámci diplomové práce ji nelze dosáhnout.

Pro modul FI/CO bude v následující kapitole proveden alespoň základní návrh oddělení oprávnění mezi obecnou rolí a rolí zaměřenou na finance.

Proces vytváření role Z_USER_DEFAULT probíhal ve dvou hlavních krocích.

1. Odvození role z Z_USER_TEMPORARY, která byla již částečně upravena.
2. Postupná analýza všech 2415 autorizačních objektů. V případě, že lze s vysokou pravděpodobností říci, že se nejedná o potřebné oprávnění, tak bude objekt oprávnění odebrán nebo upraven pouze na možnost zobrazení.

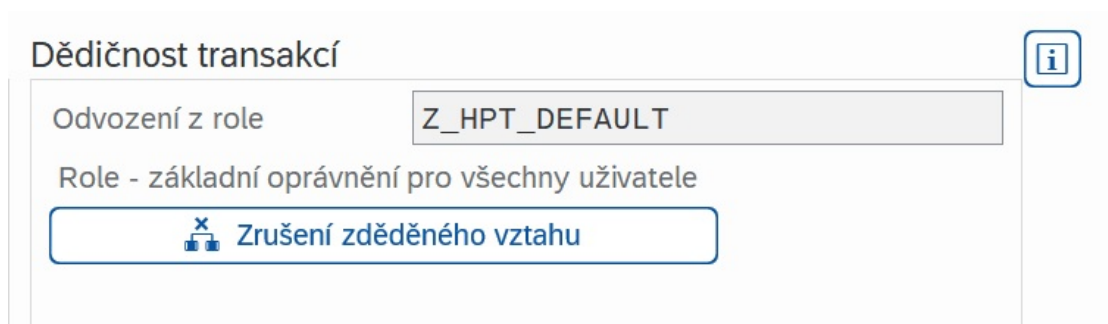
Výsledná role má celkem 1194 autorizačních objektů (o 1221 méně než měla role původní). Velká část z nich byla odebrána úplně z důvodu, že se jednalo o objekty z modulů, které se nijak nepoužívají. Zlomek těchto objektů byl stále potenciálně kritických. Některé z nich byly odebrány a u některých došlo pouze ke změně

aktivity na zobrazení. Část objektů zaměřených na modul FI/CO byla odebrána, protože se již nachází v roli Z_HPT_FINANCE nebo došlo k jejich přidání do ní.

7.4.3 Vytvoření odvozené role z Z_HPT_DEFAULT

Systém SAP umožňuje v transakci PFCG odvození všech autorizačních objektů transakce do dalších transakcí. Tato funkcionality bude zobrazena na odvození role Z_HPT_DEFAULT do role, která bude přidělovat stejnou funkcionality, jenž bude omezena pouze na organizaci 1000 (HP TRONIC).

Odvození role od jiné je možné až po jejím vytvoření v záložce „Obecné“.



Obrázek 7.9 Odvození role od Z_HPT_DEFAULT

Jakmile je role odvozena, tak je nutné provést převzetí dat při její úpravě. Tímto dojde k vytvoření přesné kopie odvozované role. Organizační úroveň je možné změnit hromadně. Nastavení, které bylo použito pro odvození organizace 1000 obsahuje tabulka 7.2

Tabulka 7.2 Parametry odvození role pro organizaci 1000

Organizační úroveň	Hodnota OD	Hodnota DO
Účetní okruh	1000	
Nákupní organizace	1000	
Pracovní úsek	1000	1999
Prodejní organizace	1000	
Pobočka	1000	1999

Toto odvození bylo provedeno i pro další organizace, kterými jsou 2100 (ETA) a 3000 (Elektrosped).

7.4.4 Role zaměřená na finance Z_HPT_FINANCE

Při vytváření role byl proveden stejný proces, jako u role Z_HPT_DEFAULT.

U role Z_HPT_FINANCE došlo k odebrání obecných autorizačních objektů, jenž jsou součástí rolí Z_HPT_DEFAULT nebo Z_HPT_USER. Dále došlo k roz-

šíření role o autorizační objekty spadající do skupin: Treasury, Treasury management, Controlling, Financials Basis a Účtování leasingu. Tato skupina byla zároveň odebrána z role Z_HPT_DEFAULT.

Výsledné role a seznam všech změněných autorizačních objektů je v příložených souborech k diplomové práci. Součástí seznamu jsou i autorizační objekty, u kterých by bylo vhodné v budoucnu provést detailnější analýzu. Tento seznam byl vytvořen manuálně při vytváření rolí.

Seznam odebraných autorizačních objektů u obou nových rolí lze zobrazit i pomocí SQL dotazu:

Kód 3. SQL dotaz pro dohledání odebraných autorizačních objektů

```
SELECT A1.OBJECT, A1.ATEXT FROM AGR_1250 AS A1
LEFT JOIN AGR_1250 AS A2 ON A1.OBJECT = A2.OBJECT
                        AND A2.AGR_NAME = 'Z_HPT_FINANCE'
WHERE A1.AGR_NAME = 'Z_USER_TEMPORARY_FI'
AND A2.OBJECT IS NULL
```

Výstup SQL dotazů je součástí příložených .xlsx souborů. Dále i všechny hlavní role, včetně rolí k nim odvozených, jsou součástí příložených souborů k diplomové práci.

7.5 Realizace rozdělení pravomocí

V kapitole 7.4.1 byla vytvořena role Z_HPT_ROLE, která lze považovat za první třetinou rozdělení pravomocí. V této kapitole bude vytvořena ještě druhá a třetí role způsobu přístupu k SoD. Jedná se o princip trojitě kontroly pro úpravu a vytváření nových rolí, jenž byl představen v kapitole 4.2 teoretické části.

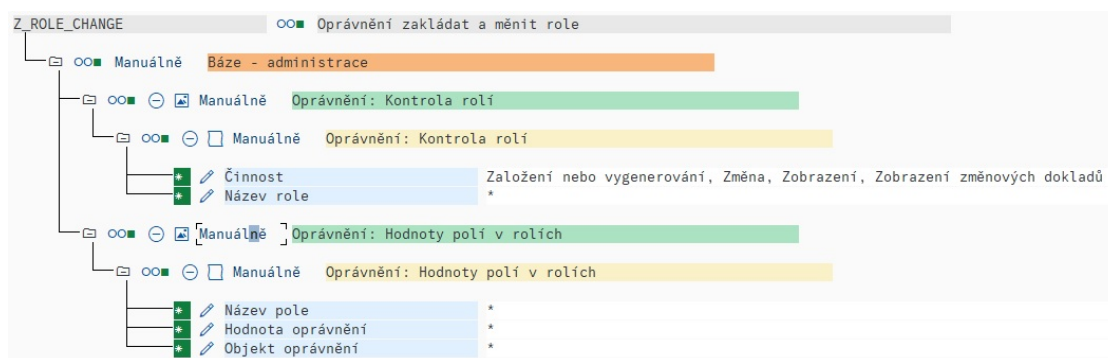
7.5.1 Role umožňující založení a změnu rolí

Druhá třetina rozdělení pravomocí spočívá v tom, že dojde k vytvoření role umožňující změnu a vytvoření nové role. Nikoli její generování (aktivita 64). Tabulka 7.3 zobrazuje autorizační objekty a jejich hodnoty, které jsou pro tuto funkcionalitu potřeba.

Tabulka 7.3 Autorizační objekty umožňující vytváření a úpravu role

Název autorizačního objektu	Hodnoty činnosti
S_USER_AGR	01, 02, 03, 08
S_USER_VAL	*

Na základě hodnot z tabulky byla vytvořena role s názvem Z_ROLE_CHANGE. Nastavení role v systému SAP je zobrazeno na obrázku 7.8.



Obrázek 7.10 Nastavení role Z_ROLE_CHANGE

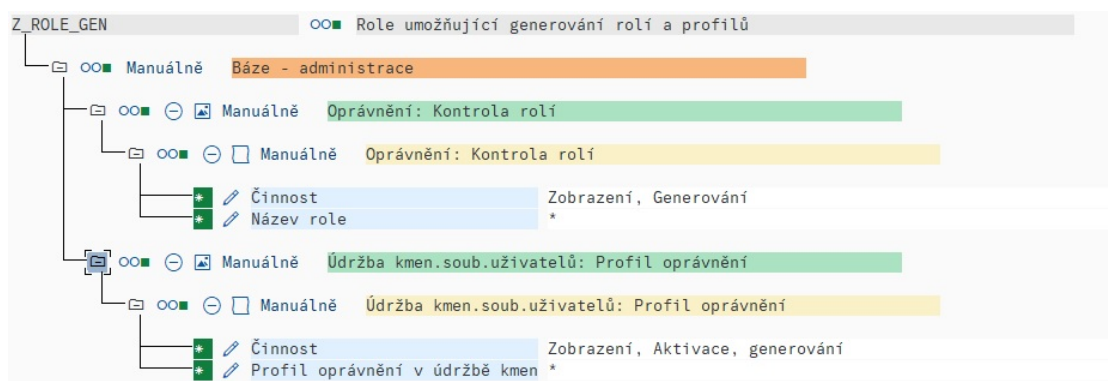
7.5.2 Role umožňující generování rolí a profilů

Posledním krokem ve vytváření principu trojitě kontroly uživatelských oprávnění je role, která má za účel pouze generovat (aktivovat) vytvořené role a k nim přiřazené profily. Každou roli co je vytvořena nebo upravena, je potřeba vygenerovat, jinak se neprojeví žádné provedené změny. Pro to, aby tato akce mohla být provedena, tak uživatel musí mít přiřazenou autorizační objekty a hodnoty, minimálně jako jsou zobrazeny v následující tabulce.

Tabulka 7.4 Autorizační objekty umožňující generování role

Název autorizačního objektu	Hodnoty činnosti
S_USER_AGR	03, 64
S_USER_PRO	03, 07

Tato role obdržela název Z_ROLE_GEN a její nastavení v úpravě rolí transakce PFCG vypadá následovně:



Obrázek 7.11 Nastavení role Z_ROLE_GEN

7.6 Nastavení systémových parametrů hesla

Vzhledem k tomu, že by jakákoli změna v parametrech, jež přímo mění požadavky na heslo, nemusela být uživatelsky přívětivá, tak k takové změně při vytváření

diplomové práce nedošlo. Jediné parametry zabývající se heslem, které mohou být změněny jsou login/password_history_size a login/min_password_diff.

Na testovacím prostředí došlo v transakci RZ10 u systémového profilu DEFAULT verze 0002 ke změně těchto parametrů na doporučenou hodnotu dle tabulky 6.5.

✓ [dropdown] Převzetí [edit icon] + Řádka - Řádka ^ PARAM+ v PARAM- [copy icon] [paste icon] [undo icon] [redo icon]

Náz.parametru:	Status	Poř.č.
login/password_history_size	Aktiv.	1

Hodn.parametru:

20

Nenahrazená standard.hodnota:

5

Nahrazená standard.hodnota:

5

Komentář:

1	#parameter created	by: TROJANJ	16.05.2023 10:51:13
	#		

Obrázek 7.12 Změna systémových parametrů

Nejvhodnějším časem k provedení větších změn parametrů hesla by mohlo být společně s přechodem všech uživatelů na systém S4HANA. Avšak naprosto nejlepší variantou by byl přechod na přihlašování pomocí SSO.

7.7 Zamknutí transakcí

Zamykání transakcí je především pojistkou vůči situaci, kdy by potenciálně kritickou transakci chtěl provádět (a měl oprávnění) neoprávněný či neznalý uživatel. Informace o tom, že je transakce zamknutá by mohlo být pro uživatele upozorněním, že transakci není vhodné používat. Aby uživatel mohl transakci uzamknout či odemknout, tak potřebuje mít roli s autorizačním objektem S_ADMI_FCD, jenž má hodnotu TLCK nebo *. U všech běžně používaných rolí došlo ke kontrole zda tento autorizační objekt obsahují či nikoli.

Na testovacím prostředí došlo k uzamknutí několika transakcí, které jsou zobrazeny v tabulce 7.5, která vychází přesně z tabulky 4.2.

Tabulka 7.5 Transakce, u kterých došlo k jejich uzamčení

Kód transakce	Název transakce	Uzamčeno
SCC5	Výmaz klienta	✓
SE11	ABAP Dictionary	×
SE37	Editor funkcí	×
SE38	Editor ABAP	×
SU10	Hromadná údržba uživatelů	✓
SM30	Údržba tabulek	✓
F110	Automatický platební styk	×
MIRO	Založení došlé faktury	×

Pověřený uživatel má schopnost kdykoli odemknout uzamčené transakce, pokud je to nezbytné. S ohledem na tuto možnost je vhodné zvážit, které další transakce jsou potenciálně kritické a zároveň se používají velmi zřídka nebo vůbec. Tyto transakce by mohly být uzamčeny.

8 VYTVOŘENÍ KONTROLNÍHO PROGRAMU

Systém SAP umožňuje sledování uživatelů a jejich oprávnění v několika transakcích již ve svém standardu. Ovšem využívání těchto transakcí je časově náročnější a uživatelsky méně přívětivé než užití programu, jenž je specificky zaměřen na zobrazení vybraných parametrů. Mezi tyto parametry patří uživatelské jméno, název role nebo profilu a seznam uživatelů, kteří mají oprávnění provádět určitou transakci.

Stále platí pravidlo, že jakýkoli vlastní vývoj, ať už se jedná o program, transakci, tabulku či datový prvek, se z pravidla značí počátečním znakem Z.

8.1 Návrh přehledové transakce ZHP_AUTH_VIEW

Program má být alternativou k transakci SUIM. Transakce SUIM umožňuje výrazně obsáhlejší analýzu uživatelských oprávnění, ovšem za cenu nižší přehlednosti a relativně vyšší časové náročnosti.

Jedná se o program sloužící k zobrazení informací dle vstupních požadavků. Uživatel bude mít možnost zvolení jednoho z několika výstupů:

- Zobrazení rolí: zobrazí všechny role pro zvoleného uživatele či množinu uživatelů.
- Zobrazení profilů: zobrazí všechny profily pro zvoleného uživatele či množinu uživatelů.
- Zobrazení všech uživatelů, kteří mají určitou roli.
- Zobrazení všech uživatelů, kteří mají určitý profil.
- Kontrola zda vstupní uživatelé mohou provádět určitou transakci. V případě, že nesplňují všechny autorizační požadavky, tak jsou tyto požadavky a jejich hodnoty zobrazeny na výstupu.
- Zobrazení všech uživatelů, kteří mají přístup k vybrané transakci.

Program byl navržen tak, aby jej bylo možné dle ohlasu uživatelů jednoduše rozšiřovat o nové funkcionality.

8.2 Realizace programu ZHP_JT_AUT_VIEW

Tato kapitola obsahuje úryvky kódu programu ZHP_JT_AUT_VIEW a jejich popis. Program slouží především pro zobrazení vstupní a výstupní obrazovky. Po

spuštění programu je vytvořen objekt třídy ZCL_JT_AUT_VIEW, ve které probíhá zpracování vstupu k možnému zobrazení.

Kód 4. Parametry vstupní obrazovky

```
SELECTION-SCREEN BEGIN OF BLOCK b1 WITH FRAME TITLE text
-001.

SELECT-OPTIONS:
so_bname FOR usr02-bname NO INTERVALS MODIF ID usr,
so_pnam FOR agr_define-agr_name NO INTERVALS MODIF ID rol.

PARAMETERS:
p_tcode TYPE zhp_auth_methods-name MODIF ID trn,
p_name TYPE zhp_auth_methods-name AS LISTBOX VISIBLE LENGTH
30 USER-COMMAND cm1.

SELECTION-SCREEN END OF BLOCK b1.
```

Vstupní parametry mohou být deklarovány dvěma způsoby: parametr a select-option. Parametr je definován jako proměnná, jež může nabývat pouze jedné hodnoty. V případě vstupu programu ZHP_JT_AUTH_VIEW jsou ideálními parametry název metody (p_name) a název transakce (p_tcode).

Druhou možností vstupních parametrů je select-option. Jedná se o proměnné typu range. Tyto proměnné mohou nabývat více hodnot, rozmezí mezi hodnotami nebo například vyloučení určitého intervalu. Vzhledem k tomu, že by uživatel mohl mít požadavek zobrazování informací pro více uživatelů či názvů profilů a rolí současně, tak jsou vstupní proměnné jako uživatelská jména (so_bname) a název role nebo profilu (so_pnam) typu select-option.

Kód 5. Vytvoření listboxu

```
INITIALIZATION.
DATA: vrm_values TYPE vrm_values,
vrm_value LIKE LINE OF vrm_values.
"seznam metod a jejich popisů
SELECT name, dscr FROM zhp_auth_methods
INTO TABLE @vrm_values.
"funkční modul pro vytvoření listboxu
CALL FUNCTION 'VRM_SET_VALUES'
EXPORTING
id = 'P_NAME'
values = vrm_values
EXCEPTIONS
id_illegal_name = 1
OTHERS = 2.
```

Při spuštění programu se pro parametr p_name vytvoří listbox s názvy metod a jejich popisů uložených v databázové tabulce ZHP_AUTH_METHODS.

Kód 6. Příklad skrývání polí na vstupní obrazovce

```

AT SELECTION-SCREEN OUTPUT.
  LOOP AT SCREEN.
    "podmínka pro skrytí vstupního pole: název transakce
    IF p_name NS 'TCODE' AND screen-group1 = 'TRN'.
      screen-invisible = 1.
      screen-active = 0.
    ENDIF.
    "podmínka pro skrytí vstupního pole: uživatelské jméno
    IF p_name CS 'LIST' AND screen-group1 = 'USR'.
      screen-invisible = 1.
      screen-active = 0.
    ENDIF.

    MODIFY SCREEN.
  ENDLOOP.

```

Úryvek kódu 6. zobrazuje práci se vstupní obrazovkou, kde dochází ke skrytí vstupních parametrů podle vybrané výstupní metody. Každý vstupní parametr je přiřazen do skupiny, podle které se určuje, jestli má být zobrazen nebo ne.

Kód 7. Část kódu po spuštění programu

```

START-OF-SELECTION.
  CLEAR o_auth.
  "kontrola zda byly vyplněny vstupní select-options
  IF so_bname IS INITIAL AND so_prnam IS INITIAL AND p_tcode
    IS INITIAL.
    MESSAGE i001(zhp_auth) DISPLAY LIKE 'E'.
    EXIT.
  ENDIF.
  "inicializace objektu třídy
  o_auth = NEW #( i_bname = so_bname[]
                  i_prnam = so_prnam[]
                  i_tcode = p_tcode
                  i_mname = p_name ).

  IF o_auth->check_error( ) IS INITIAL.
    CALL SCREEN 0100.
  ENDIF.

```

Po spuštění programu dojde ke kontrole, zda bylo vyplněn alespoň jeden vstupní parametr. V případě, že ano, tak program pokračuje k vytvoření objektu třídy ZCL_JT_AUTH_VIEW. Jestliže žádný vstup naplněn nebyl, tak dojde k vypsání zprávy číslo 001 ze skupiny zpráv zhp_auth, kterou je: „Vyplňte alespoň jeden vstupní parametr.“

Většina programu je spouštěna přímo v konstruktoru zmíněné třídy. Tento kód je popsán až v následující kapitole 8.2.4. Poté co je kód ve třídě proveden dojde

k volání obrazovky 0100 (dynpra), na které dojde k zobrazení výstupu ALV.

Kód 8. Moduly dynpra 0100

```
"část kódu před zobrazením obrazovky 0100
MODULE status_0100 OUTPUT.
  SET TITLEBAR 'TITLE_0100'. "nastavení titulku
  SET PF-STATUS 'STATUS_0100'. "nastavení statusu
ENDMODULE.

"část kódu reagující na uživatelský vstup
MODULE user_command_0100 INPUT.
  CASE sy-ucomm.
    WHEN 'BACK'.
      LEAVE TO SCREEN 0. "vrácení se na úvodní obrazovku

    WHEN 'EXIT' OR 'END'.
      LEAVE PROGRAM. "ukončení programu
  ENDCASE.
ENDMODULE.
```

Modul user_command_0100 umožňuje tlačítkům přidat funkcionalitu. V současné verzi programu je nastavena pouze funkcionalita k vrácení se na původní obrazovku či k vypnutí programu. V případě, že by tato funkcionalita nastavena nebyla, tak by nebylo možné program jednoduše vypnout.

8.2.1 Realizace třídy ZCL_JT_AUT_VIEW

Veškerá hlavní funkcionalita je zprostředkována třídou ZCL_JT_AUT_VIEW, ve které je jednotlivými metodami zajištěno získání požadovaných dat a příprava k jejich zobrazení.

Kód 9. Constructor třídy ZCL_JT_AUTH_VIEW

```
METHOD constructor.
  me->r_bname = i_bname. "uživatelské jméno
  me->r_prnam = i_prnam. "název role/profilu
  me->v_tcode = i_tcode. "kód transakce
  me->v_name = i_mname. "typ metody
  CALL METHOD me->(me->v_name). "volání metody
ENDMETHOD.
```

Constructor je část kódu, která je spuštěna vždy, když je inicializován objekt třídy. Při inicializaci objektu třídy je třeba předat vstupní parametry constructoru, kterými jsou: i_bname, i_prnam, i_tcode a i_mname.

Tyto vstupní parametry jsou uloženy do globálních proměnných třídy. Pro lepší rozlišení lokálních a globálních proměnných je u všech globálních proměnných třídy použita předpona me->.

Kód 10. Metoda pro vytvoření fieldcatalogu dle datových prvků interní tabulky

```
METHOD create_fcat.
  DATA: lr_tbdscr TYPE REF TO cl_abap_structdescr,
        lr_data   TYPE REF TO data,
        lt_dfies   TYPE ddfields,
        ls_dfies   TYPE dfies,
        ls_fcat    TYPE lvc_s_fcat.

  CREATE DATA lr_data LIKE LINE OF i_tab.

  lr_tbdscr ?= cl_abap_structdescr=>describe_by_data_ref(
    lr_data ).
  lt_dfies = cl_salv_data_descr=>read_structdescr( lr_tbdscr
    ).

  LOOP AT lt_dfies INTO ls_dfies.
    CLEAR ls_fcat.
    MOVE-CORRESPONDING ls_dfies TO ls_fcat.
    APPEND ls_fcat TO me->t_fieldcat.
  ENDLOOP.

  DELETE me->t_fieldcat WHERE fieldname = 'MANDT'.
  rename_fields( ).
ENDMETHOD.
```

Tato metoda vytváří fieldcatalog (v českém jazyce katalog polí), který je roven jakékoli vstupní interní tabulce. Další možnosti vytváření fieldcatalogu je na základě struktury, jež je součástí systému.

Fieldcatalog poskytuje ALV gridu informaci, která data interní tabulky náleží jakým sloupcům. Dále umožňuje nastavení popisu sloupců, jejich případné zabarvení, šířku, přidání ikony a další možnosti vizualizace.

Kód 11. Metody pro nastavení layoutu a varianty

```
METHOD set_layout.
  me->s_layout-cwidth_opt = 'X'.
  me->s_layout-zebra = 'X'.
ENDMETHOD.

METHOD set_variant.
  me->s_variant-report = sy-repid. "název programu
  me->s_variant-variant = |/{ me->v_name }|. "název varianty
ENDMETHOD.
```

Layout ALV gridu slouží především k lepší přehlednosti výstupu. Hodnota proměnné struktury `s_layout`, kterou je **cwidth_opt** udává, zda má dojít k dynamickém rozšíření sloupců dle délky nejdelšího textu sloupce. Tímto je zajištěno to, že nebude docházet k zakrytí výstupních informací. Druhá hodnota **zebra** zlepšuje

čitelnost mezi řádky, u kterých se bude střídát odstín jejich pozadí.

Varianta udává, jak by měl vypadat výstup oproti základnímu vzhledu. V případě, že by uživatel v budoucnu chtěl změnit vzhled výstupu v podobě skrytí určitých polí či změněním pořadí polí, tak uložením varianty v podobě /název metody docílí toho, že bude tato varianta nastavena vždy automaticky.

Kód 12. Metoda pro zobrazení ALV gridu

```
METHOD display_alv.

    me->set_layout( ). "nastavení layoutu
    me->set_variant( ). "nastavení varianty
    me->create_fcat( c_tab ). "vytvoření fieldcatalogu

    "inicializace objektu třídy ALV gridu
    me->alv_grid = NEW #( cl_gui_container=>default_screen ).

    "připravení ALV gridu k~zobrazení
    me->alv_grid->set_table_for_first_display(
        EXPORTING
            is_variant      = me->s_variant
            is_layout       = me->s_layout
            i_save           = 'A' "možnost uložení varianty
        CHANGING
            it_outtab       = c_tab
            it_fieldcatalog = me->t_fieldcat ).

ENDMETHOD.
```

Vstupním parametrem této metody je proměnná `c_tab`, která může mít typ jakékoli vstupní tabulky. Před vytvořením dojde na základě této interní tabulky k vytvoření příslušného fieldcatalogu.

8.2.2 Metody pro získání dat z databáze

Jakmile došlo k vytvoření hlavních metod pro a byla zajištěna správná funkčnost programu, tak se mohlo začít s vytvářením jednotlivých metod. Jedná se o celkem šest metod, které byly již zmíněny v kapitole 8.1.

Všechny metody obsahují základní SQL dotazy do databáze za pomoci Open SQL v jazyce ABAP. Metody, které kontrolují spustitelnost transakce vyžadují dodatečnou práci s daty. Vracená data se ukládají do globálních tabulek třídy. Tabulky jsou definovány v části definice třídy. Typ těchto tabulek je určen dle jednotlivých metod výběru a SQL dotazu.

Výstupem těchto metod je vždy uživatelské jméno (případně celé jméno uživatele). Poté následují parametry závislé na typu metody. Může to být název metody,

název profilu či název transakce a jejich případný popis.

Kód 13. Metoda pro získání profilů uživatele

```
METHOD user_profiles.  
  SELECT DISTINCT ust04~bname, name_text, profile, ptext  
  FROM ust04  
    INNER JOIN usr11 ON usr11~profn = ust04~profile AND  
  langu = @sy-langu "pouze názvy profilu v jazyce systému"  
    INNER JOIN usr21 ON usr21~bname = ust04~bname  
    INNER JOIN adrp ON usr21~persnumber = adrp~persnumber  
  INTO TABLE @me->t_out  
  WHERE ust04~bname IN @me->r_bname  
  ORDER BY ust04~bname, profile.  
  
DELETE ADJACENT DUPLICATES FROM me->t_out COMPARING  
  name_text prnam.  
display_alv( CHANGING c_tab = me->t_out ).  
ENDMETHOD.
```

Kód 13. zobrazuje SQL dotaz vracející seznam všech uživatelů, jejich celých jmen a jim přidělených profilů na základě vstupního seznamu uživatelů.

Tabulka UST04 obsahuje informace o tom, jaké profily mají uživatelé přiřazeny. Názvy jednotlivých profilů jsou uloženy v tabulce USR11.

Vzhledem k tomu, že v systému SAP neexistuje tabulka, která by obsahovala uživatelské jméno společně s celým jménem, tak je potřeba využít propojení dvou tabulek. Těmito tabulkami jsou USR21 a ADRP, které lze propojit pomocí pole PERSNUMBER.

Open SQL umožňuje dynamické určení jazyka textu. Není tedy nutné zadávat český jazyk ('C'), ale místo toho je možné použít jazyk přihlášení uživatele sy-langu.

Kód 14. Metoda pro získání seznamu uživatelů, kteří mají daný profil

```
METHOD profile_user_list.  
  SELECT DISTINCT ust04~bname, adrp~name_text, profile,  
  ptext FROM ust04  
    INNER JOIN usr11 ON usr11~profn = ust04~profile AND  
  langu = @sy-langu "pouze názvy profilu v jazyce systému"  
  LEFT JOIN usr21 ON usr21~bname = ust04~bname  
  LEFT JOIN adrp ON usr21~persnumber = adrp~persnumber  
  INTO TABLE @me->t_out  
  WHERE profile IN @me->r_prnam  
  ORDER BY ust04~bname, profile.  
  
DELETE ADJACENT DUPLICATES FROM me->t_out COMPARING  
  name_text prnam.  
display_alv( CHANGING c_tab = me->t_out ).  
ENDMETHOD.
```

SQL dotaz v metodě `profile_user_list` vychází z předchozího příkladu. Jediný rozdíl je v podmínce `WHERE`, kde je místo seznamu uživatelů dosazen seznam názvů profilů. Pro tyto profily je zobrazen seznam všech uživatelů a jejich celých jmen, jež mají daný profil přiřazený.

Kód 15. Metoda pro získání rolí uživatele

```
METHOD user_roles.  
  
SELECT DISTINCT uname, name_text, usr~agr_name, text FROM  
agr_users AS usr  
  INNER JOIN agr_texts AS txt ON usr~agr_name = txt~  
agr_name  
  LEFT JOIN usr21 ON usr21~bname = usr~uname  
  LEFT JOIN adrp ON usr21~persnumber = adrp~persnumber  
INTO TABLE @me->t_out  
WHERE usr~uname IN @me->r_bname  
AND txt~spras = @sy-langu  
ORDER BY uname, usr~agr_name.  
  
DELETE ADJACENT DUPLICATES FROM me->t_out COMPARING  
name_text prnam.  
display_alv( CHANGING c_tab = me->t_out ).  
  
ENDMETHOD.
```

Obdobně, jako při získávání profilů uživatele, je možné postupovat i u získávání rolí. V podstatě jediným rozdílem jsou názvy tabulek se seznamem rolí, jež má uživatel přiřazený (`AGR_USERS`) a tabulkou s texty k jednotlivým rolím (`AGR_NAME`).

Kód 16. Metoda pro získání seznamu uživatelů, kteří mají danou roli

```
METHOD role_user_list.  
  
SELECT DISTINCT uname, name_text, usr~agr_name, text FROM  
agr_users AS usr  
  INNER JOIN agr_texts AS txt ON usr~agr_name = txt~  
agr_name  
  LEFT JOIN usr21 ON usr21~bname = usr~uname  
  LEFT JOIN adrp ON usr21~persnumber = adrp~persnumber  
INTO TABLE @me->t_out  
WHERE usr~agr_name IN @me->r_prnam  
AND txt~spras = @sy-langu  
ORDER BY uname, usr~agr_name.  
  
DELETE ADJACENT DUPLICATES FROM me->t_out COMPARING  
name_text prnam.  
display_alv( CHANGING c_tab = me->t_out ).  
  
ENDMETHOD.
```

Stejným případem je kód 16. pro získání seznamu uživatelů jenž mají přiřazenou určitou roli.

Následující úryvek kódu zobrazuje hlavní funkcionalitu metody pro vytvoření seznamu chybějících oprávnění, které uživateli chybí k úspěšnému provedení transakce.

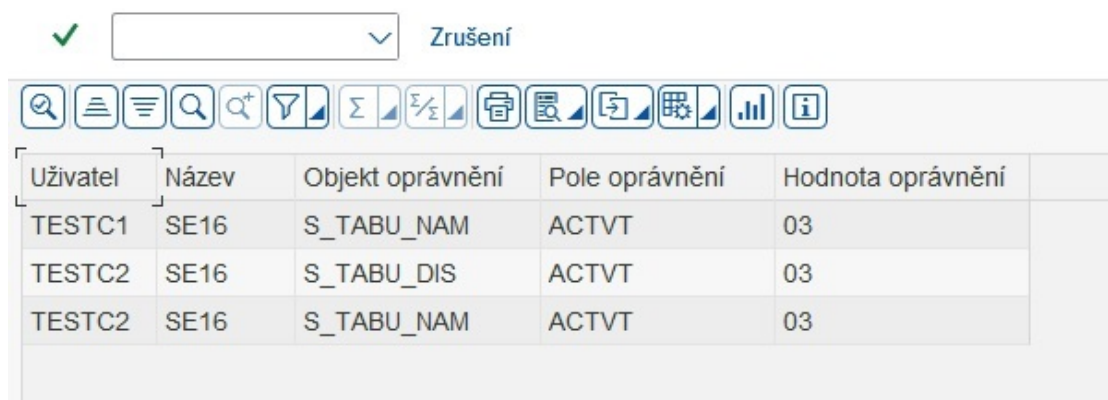
Kód 17. Zjištění chybějících oprávnění uživatele

```
METHOD user_tcode_check.  
  DATA lt_usobt TYPE STANDARD TABLE OF ty_auth.  
  
  LOOP AT me->r_bname INTO DATA(wa_bname).  
    SELECT name AS tcode, object, field, low FROM usobt  
      INTO CORRESPONDING FIELDS OF TABLE @lt_usobt  
      WHERE name = @me->v_tcode  
      AND low <> ''  
      AND type = 'TR'.  
    SELECT ust04~bname, profile FROM ust04  
      INTO TABLE @DATA(lt_profiles)  
      WHERE ust04~bname = @wa_bname-low.  
    IF lt_profiles IS NOT INITIAL.  
      LOOP AT lt_profiles ASSIGNING FIELD-SYMBOL(<row>).  
        <row>-profile = |{ <row>-profile }00|.  
      ENDLOOP.  
      LOOP AT lt_usobt INTO DATA(wa_usobt).  
        SELECT COUNT( * ) FROM ust12  
          FOR ALL ENTRIES IN @lt_profiles  
          WHERE objct = @wa_usobt-object  
          AND field = @wa_usobt-field  
          AND ( von = @wa_usobt-low OR von = '*' )  
          AND auth = @lt_profiles-profile.  
        IF sy-subrc = 0.  
          DELETE lt_usobt.  
        ENDIF.  
      ENDLOOP.  
    ENDIF.  
  
    LOOP AT lt_usobt ASSIGNING FIELD-SYMBOL(<name>).  
      <name>-uname = wa_bname-low.  
      APPEND <name> TO me->t_objects.  
    ENDLOOP.  
  ENDLOOP.  
  IF me->t_objects IS NOT INITIAL.  
    display_alv( CHANGING c_tab = me->t_objects ).  
  ELSEIF lt_profiles IS NOT INITIAL.  
    MESSAGE i002(zhp_auth) DISPLAY LIKE 'S'.  
    "Všichni uživatelé mají dostatečná oprávnění.  
    me->v_error = 'X'.  
  ENDIF.  
ENDMETHOD.
```

Jedná se již o obsáhlejší metodu, protože informace o proveditelnosti transakce není možné získat pouze za použití SQL dotazu, ale je nutné dodatečně pracovat se získanými daty.

Prvním krokem je zjištění seznamu všech oprávnění a hodnot, jež jsou potřeba k provedení transakce. Tato informace je obsažena v tabulce USOBT. Následně je nutné zjistit seznam všech profilů, které má uživatel přiřazen (tabulka UST04). Poté je nutné zjistit, zda jednotlivé profily obsahují dostatečné hodnoty u objektů oprávnění. Tato informace lze zjistit dle hodnot v tabulce UST12.

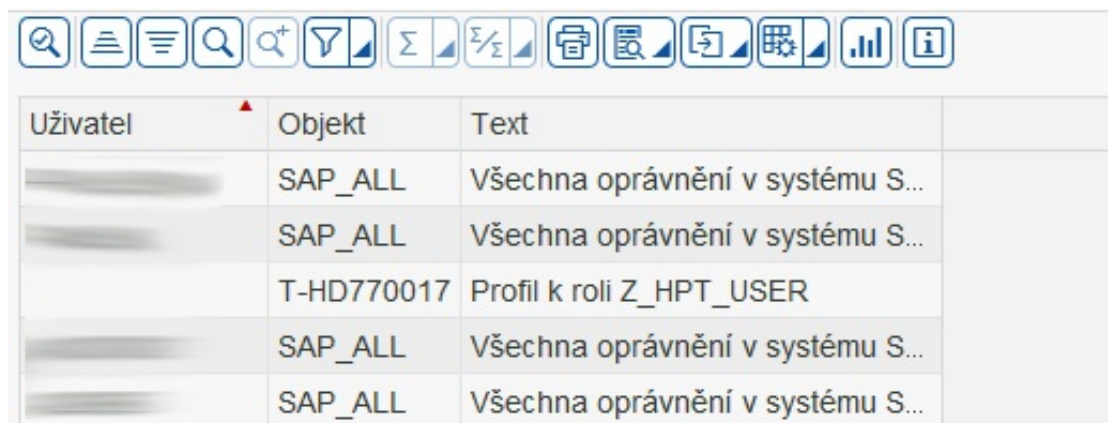
Výstupem je seznam oprávnění a jejich hodnot, které uživateli chybí, aby mohl provádět obecné funkcionality transakce.



Uživatel	Název	Objekt oprávnění	Pole oprávnění	Hodnota oprávnění
TESTC1	SE16	S_TABU_NAM	ACTVT	03
TESTC2	SE16	S_TABU_DIS	ACTVT	03
TESTC2	SE16	S_TABU_NAM	ACTVT	03

Obrázek 8.1 Seznam chybějících oprávnění k provedení transakce SE16

Na základě této metody byla vytvořena poslední metoda, která dohledá seznam uživatelů, kteří mají oprávnění provádět všechny operace ve vstupní transakci. Jedná se o metodu s názvem TCODE_CHECK. Výstupem transakce je seznam všech uživatelů, jenž mohou provádět vstupní transakci včetně zobrazení profilů, které mu toto oprávnění dávají.



Uživatel	Objekt	Text
	SAP_ALL	Všechna oprávnění v systému S...
	SAP_ALL	Všechna oprávnění v systému S...
	T-HD770017	Profil k roli Z_HPT_USER
	SAP_ALL	Všechna oprávnění v systému S...
	SAP_ALL	Všechna oprávnění v systému S...

Obrázek 8.2 Seznam uživatelů a jejich profilů, které jim umožňují provedení transakce

Syntaxe metody TCODE_CHECK je zobrazena v příloze č. 1 v seznamu příloh.

Syntaxi hlavního programu a třídy obsahující všechny metody lze zobrazit v příložených souborech k diplomové práci. Součástí zobrazených kódů byly hlavně úryvky hlavní části kódu. Mnohdy byly tyto úryvky bez zobrazení definice proměnných a jejich typů, které jsou definovány v definici třídy. ALV výstupy jednotlivých metod jsou do příloh zahrnuty taktéž. Jedná se o celkem šest obrázků zobrazujících jednotlivé výstupy programu.

8.2.3 Vstupní obrazovka transakce ZHP_AUTH_VIEW

Následující obrázek 8.3 zobrazuje vstupní obrazovku s rozvinutým listboxem se seznamem použitelných metod.

Vstupní parametry	
Uživatel	TROJANJ
Název transakce	SM01
Název metody	USER_TCODE_CHECK Metoda pro
PROFILE_USER_LIST	Seznam uživatelů, kteří mají daný profil
ROLE_USER_LIST	Seznam uživatelů, kteří mají danou roli
USER_PROFILES	Metoda pro načtení profilů pro vstupní uživatele
USER_ROLES	Metoda pro načtení rolí pro vstupní uživatele
USER_TCODE_CHECK	Metoda pro zobr. oprávnění uživatele ve vybrané transakci
TCODE_CHECK	Seznam uživatelů, kteří mohou provádět transakci

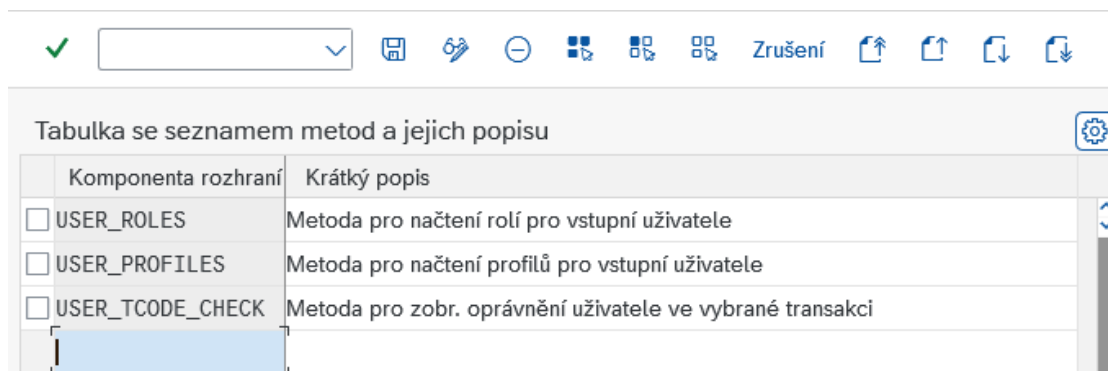
Obrázek 8.3 Úvodní obrazovka transakce ZHP_AUTH_VIEW

Na základě názvu zvolené metody dochází ke změně vstupních parametrů. U metody USER_ROLES pro zobrazení všech rolí, které má uživatel přiřazen na vstupní obrazovce zůstává pouze uživatelské jméno. Naopak u metody pro zobrazení všech uživatelů, kteří mohou spustit vybranou transakci se na obrazovce zobrazí pole pro zadání názvu transakce.

8.2.4 Customizační tabulka ZHP_AUTH_METHODS

Seznam jednotlivých metod a jejich popisů, které jsou v listboxu zobrazeny je uložen v customizační tabulce ZHP_AUTH_METHODS. Customizační tabulka je klasickou databázovou tabulkou, kterou je ovšem možno jednoduše uživatelsky upravovat v transakci SM30.

Tímto způsobem je zajištěno jednodušší rozšíření funkcionality v případě budoucí potřeby. Na následujícím obrázku 8.4 je zobrazeno přidávání názvů metod a jejich popisů do tabulky ZHP_AUTH_METHODS v transakci SM30.



Obrázek 8.4 Údržba tabulky v transakci SM30

8.2.5 Transportování objektů z vývojového prostředí

Všechny vývoj byl proveden na vývojovém prostředí systému SAP. Proto, aby tyto funkcionality byly možné využít i na testovacím či produkčním prostředí, tak je třeba transportování požadavku.

Požadavek obsahuje všechny vytvořené objekty, které zobrazuje obrázek 8.5.

Krátký popis	ID prog	Typ objektu	Název objektu	Funk	Status blok./importu	Já
Paket	R3TR	DEVC	ZAUTORIZACE		Objekt blokován	
Program	R3TR	PROG	ZHP_JT_AUTH_VIEW		Objekt blokován	
Třída (objekty ABAP)	R3TR	CLAS	ZCL_JT_AUTH_VIEW		Objekt blokován	
Tabulka	R3TR	TABL	ZHP_AUTH_METHODS		Objekt blokován	
Technické vlastnosti tabulky	LIMU	TABT	ZHP_AUTH_METHODS		Objekt blokován	
Definice tabulky	LIMU	TABD	ZHP_AUTH_METHODS		Objekt blokován	
View	R3TR	VIEW	Z_METHODNAME_W		Objekt blokován	
Nápořádá vyhledávání	R3TR	SHLP	Z_METHODNAME_H		Objekt blokován	
Skupina funkcí	R3TR	FUGR	ZHP_AUTH_METHODS		Objekt blokován	
Definice objektu údržby a	R3TR	TOBJ	ZHP_AUTH_METHODSS		Objekt blokován	
Obsah tabulky	R3TR	TABU	TVDIR			
Obsah tabulky	R3TR	TABU	TDDAT			
Třída zpráv	R3TR	MSAG	ZHP_AUTH		Objekt blokován	

Obrázek 8.5 Seznam vytvořených objektů

Poté co jsou objekty úspěšně odtransportovány, tak je možné jejich využívání i na ostatních prostředích. Části programu byly použity při analýze a návrhu uživatelských oprávnění v předchozích kapitolách.

ZÁVĚR

V teoretické části byla představena společnost HP TRONIC Zlín, spol. s r. o., která je zadavatelem tématu diplomové práce a dále byly prezentovány podnikové informační systémy, jejich členění, nejčastěji používaná architektura a dodavatelé. Zvláštní pozornost byla věnována systému SAP, jehož podrobnosti jsou důkladně rozebrány nejen v teoretické části, ale i v praktické části.

V praktické části je nejprve podrobněji popsán systém SAP ve společnosti HP TRONIC. Následující kapitoly se zaměřují na nastavení bezpečnosti systému SAP. První kapitola obsahuje analýzu současného stavu zabezpečení, zatímco druhá kapitola se zabývá metodikou, která slouží jako podklad pro úpravy stávajících uživatelských rolí a vytvoření nových. Na konci této kapitoly je popsán proces vytvoření programu pro sledování oprávnění na základě vstupních parametrů.

Analýza současného stavu zabezpečení odhalila mnoho potenciálně kritických oprávnění, které by dle navržené metodiky neměly být součástí obecně používaných oprávnění. Současně bylo u analýzy zjištěno, že by bylo vhodné se zamyslet nad změnou systémových parametrů zabývajících se bezpečností hesla.

Na základě výsledků analýzy byly v kapitole 7 dle metodiky odstraněny nepotřebné kritické oprávnění z běžně používaných rolí. Dále došlo k vytvoření nové obecné role Z_HPT_DEFAULT, která by měla zachovat všechny vyžadované funkcionality role předchozí, kterou byla role Z_USER_TEMPORARY. U nové role došlo k odebrání přibližně poloviny autorizačních objektů, které měla předchozí role. Jednalo se především o objekty, které jsou pro běžného uživatele nepotřebné nebo se v průběhu let staly zastaralé a byly nahrazeny jinými autorizačními objekty.

Obecná role nebyla jedinou rolí, jež byla vytvořena. Vzhledem k tomu, že praktická část byla zaměřena i na modul FI/CO, tak pro tento modul došlo k vytvoření nové obecné role Z_HPT_FINANCE. Tato role byla odvozena z dočasné role Z_USER_TEMPORARY_FI, která však musela být upravena, protože nebyla v souladu s nastavenou metodikou.

V závěru vytváření rolí došlo k vytvoření soustavy rolí umožňující princip trojitě kontroly rozdělení pravomocí. Jednotlivé role umožňují vždy pouze jednu část pro přidělení, úpravu nebo aktivování uživatelských oprávnění.

V rámci úprav byly provedeny také změny v systémových parametrech týkajících se hesel a zamykání transakcí. U systémových parametrů byla provedena nastavení týkající se historie hesla, jako počet změn hesla před použitím původního hesla a rozdílný počet znaků od předchozího hesla. Při zamykání transakcí

byly zamčeny pouze tři transakce s doporučením zamknout několik dalších.

V poslední kapitole diplomové práce byl vytvořen program pro kontrolu oprávnění. Tento program je založen především na jednoduchém uživatelském rozhraní ve srovnání se standardní transakcí SUIM, která je sice podrobnější, ale méně uživatelsky přívětivá.

Nejnáročnější částí praktické části bylo správné nastavení oprávnění s cílem co nejvíce se přiblížit principu minimálních pravomocí. Ve společnosti se používá mnoho zákaznických transakcí, u kterých nelze přesně určit, jaká oprávnění jsou nezbytná pro správnou funkčnost. Je tedy téměř nemožné přesně přiřadit uživatelům pouze ta oprávnění, která potřebují k výkonu své práce.

Téměř celá praktická část byla realizována pouze v testovacím prostředí systému SAP. Jedinou výjimkou bylo vytvoření kontrolního programu, který byl vyvíjen v prostředí pro vývoj a byl transportován do produkčního prostředí, přičemž jeho funkcionality nemohla ohrozit běh společnosti.

SEZNAM POUŽITÉ LITERATURY

- [1] ČECHUROVÁ, Hana. Analýza spokojenosti zaměstnanců ve firmě HP TRONIC Zlín, spol. s.r.o. Zlín: Univerzita Tomáše Bati ve Zlíně, 2011, 66 s. (72 816 znaků). Dostupné také z: <http://hdl.handle.net/10563/16265>. Univerzita Tomáše Bati ve Zlíně. Fakulta managementu a ekonomiky, Vyšší odborná škola ekonomická. Vedoucí práce Vrdlovec, Ladislav.
- [2] HP Tronic - O nás [online]. [cit. 2023-04-02]. Dostupné z: <https://www.hptronic.cz/o-nas>.
- [3] HP Tronic - Značky [online]. [cit. 2023-04-02]. Dostupné z: <https://www.hptronic.cz/znacky>.
- [4] ETA - Logo ke stažení [online]. [cit. 2023-04-02]. Dostupné z: <https://www.eta.cz/logo-ke-stazeni/>.
- [5] SODOMKA, Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi: Petr Sodomka, Hana Klčová. 2., aktualiz. a rozš. vyd. Brno: Computer Press, 2010, 501 s. ISBN 978-80-251-2878-7.
- [6] BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 2. Praha: Grada, 2008. Management v informační společnosti. ISBN 978-80-247-2279-5.
- [7] CÁPÍK, Josef. Nákupní modul ve vývojovém prostředí SAP. Zlín: Univerzita Tomáše Bati ve Zlíně, 2017, 103 s. (102 948 znaků). Dostupné také z: <http://hdl.handle.net/10563/41536>. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav informatiky a umělé inteligence. Vedoucí práce Šilhavý, Radek.
- [8] HORKÁ, Marie. Podnikové informační systémy. Zlín: Univerzita Tomáše Bati ve Zlíně, 2014, 63 s. (9 030 znaků). Dostupné také z: <http://hdl.handle.net/10563/30054>. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav počítačových a komunikačních systémů. Vedoucí práce Šilhavý, Petr.
- [9] IBM. What is three-tier architecture? [online]. IBM. 28. 10. 2020 [cit. 2023-02-10]. Dostupné z: <https://www.ibm.com/topics/three-tier-architecture>.
- [10] VAN DECKER, John, Denis TORII, Anderson ROBERT a Faith TIM. Magic Quadrant for Cloud ERP for Service-Centric Enterprises [online]. 12. červenec

- 2022 [cit. 2023-02-18]. Dostupné z: <https://www.gartner.com/doc/reprints?id=1-2AKVNBGX&ct=220713&st=sb>.
- [11] KPC GROUP. Jak fungují magické kvadranty? [online]. In: . [cit. 2023-02-19]. Dostupné z: <https://kpc-group.cz/blog/metodika/magicky-kvadrant>.
- [12] SAP Company Information [online]. [cit. 2023-02-12]. Dostupné z: <https://www.sap.com/corporate/en/company.html>.
- [13] MAASSEN, André. SAP R/3: kompletní průvodce. Brno: Computer Press, 2007. Informační systémy. ISBN 978-80-251-1750-7.
- [14] ANDERSON, George W. Naučte se SAP za 24 hodin. Brno: Computer Press, 2012. ISBN 978-80-251-3685-0.
- [15] SAP logo [online]. In: . [cit. 2023-02-26]. Dostupné z: https://logos-download.com/wp-content/uploads/2016/08/SAP_logo.png.
- [16] SAP NetWeaver [online]. [cit. 2023-02-18]. Dostupné z: <https://www.sap.com/products/technology-platform/netweaver.html>.
- [17] ROY, Mrinal Kanti. S/4HANA and its differences with ECC [online]. 2016 [cit. 2023-02-18]. Dostupné z: <https://blogs.sap.com/2016/05/16/s4-hana-and-its-differences-with-ecc/>.
- [18] SAP. What is SAP HANA? [online]. [cit. 2023-03-07]. Dostupné z: <https://www.sap.com/products/technology-platform/hana/what-is-sap-hana.html>.
- [19] IBM. What is SAP HANA? [online]. IBM. 28. 10. 2020 [cit. 2023-02-10]. Dostupné z: <https://www.ibm.com/topics/sap-hana>.
- [20] ANTO, Alvera. What is SAP FICO [online]. 13. května 2019 [cit. 2023-03-07]. Dostupné z: <https://www.zarantech.com/blog/what-is-sap-fico/>.
- [21] O'DONNELL, Jim. SAP Quality Management (QM) [online]. [cit. 2023-03-07]. Dostupné z: <https://www.techtarget.com/searchsap/definition/SAP-Quality-Management-QM>.
- [22] SAP Standard Application Benchmarks [online]. [cit. 2023-02-28]. Dostupné z: <https://www.sap.com/dmc/exp/2018-benchmark-directory>.
- [23] KÜHNHAUSER, Karl-Heinz. ABAP: výukový kurz. Brno: Computer Press, 2007. ISBN 978-80-251-2117-7.

- [24] KROENKE, David a David J. AUER. Databáze. Brno. ISBN 978-80-251-4352-0.
- [25] BANDARI, Kiran. Complete ABAP. SAP Press, 2022. ISBN 978-1-4932-2305-3.
- [26] SOUVIK, Roy, Aleksandar DEBELIC a Gairik ACHARYA. SAP Fiori: Implementation and Development. 1. 2022. ISBN 978-1-4932-2204-9.
- [27] JURAN, Tracy. Beginner's Guide to SAP Security and Authorizations. 2016. ISBN 978-1508635390.
- [28] TROJAN, Jiří. Výukový modul pro předmět Mikropočítače a PLC: elektronický zámek. Zlín: Univerzita Tomáše Bati ve Zlíně, 2021, 56 s. Dostupné také z: <http://hdl.handle.net/10563/46617>. Univerzita Tomáše Bati ve Zlíně. Fakulta aplikované informatiky, Ústav bezpečnostního inženýrství. Vedoucí práce Dostálek, Petr.
- [29] MARKGRAF, Joe a Alessandro BANZER. SAP System Security Guide. SAP Press, 2018. ISBN 978-1-4932-1481-5.
- [30] LORD, Nate. What is the Principle of Least Privilege (POLP)? A Best Practice for Information Security and Compliance [online]. 2020 [cit. 2023-05-05]. Dostupné z: <https://www.digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance>.
- [31] CAVALLERI, Andrea a Massimo MANARA. Authorizations in SAP: 100 Things You Should Know About. SAP Press, 2012. ISBN 978-1-59229-803-7.
- [32] DEHGHANTANHA, Ali a Kim-Kwang RAYMOND CHOO. Handbook of Big Data and IoT Security. Springer Cham, 2019. ISBN 978-3-030-10542-6.
- [33] BUDKA, Marek. Analýza SoD (Segregation of Duties) konfliktů na platformě SAP Cloud Platform [online]. Praha, 2018 [cit. 2022-11-17]. Dostupné z: <https://vskp.vse.cz/72563-analyza-sod-segregation-of-duties-konfliktu-na-platforme-sap-cloud-platform>. Diplomová. Vysoká škola ekonomická v Praze. Vedoucí práce doc. Ing. Jan Pour, CSc.
- [34] Security Administration Guide [online]. 2022-09-16, [cit. 2022-11-17]. Dostupné z: https://help.sap.com/doc/a6115f7abc2b1014bf21a063974f889e/16.0.4.3/en-US/Security_Administration_Guide_en.pdf.

- [35] GHAVAMI, Peter. BIG DATA GOVERNANCE: Modern Data Management Principles for Hadoop, NoSQL & Big Data Analytics. 1. CreateSpace, 2015. ISBN 978-1519559722.
- [36] Simplification List for SAP S/4HANA 2022 Initial Shipment [online]. 1390 [cit. 2023-04-16]. Dostupné z: https://help.sap.com/doc/59bf7d0f62d24af78f87c560da8f18ce/2022/en-US/SIMPL_OP2022.pdf.
- [37] MANS, Ivan. SAP DEBUGGER, POWERFUL YET DANGEROUS! [online]. 1. srpna 2022 [cit. 2023-05-01]. Dostupné z: <https://securitybridge.com/security-news/sap-debugger-powerful-yet-dangerous/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ABAP	Advanced Business Application Programming
ALV	ABAP List Viewer
APS	Advanced Planning System
BI	Business Intelligence
CO	Controlling
CRM	Customer Relationship Management
DYNPRO	Dynamic program
ERP	Enterprise resource planning
FI	Financial Accounting
GUI	Graphical user interface
HANA	High-performance ANalytic Appliance
HR	Human Resources
IMDB	In-Memory Database
MM	Material Management
OLAP	Online Analytical Processing
OLTP	Online Transaction Processing
POLP	Principle of Least Privilege
PP	Production Planning
QM	Quality Management
RDBMS	Relational Database Management System
RAM	Random Access Memory
SAP	Systemanalyse und Programmentwicklung
SAP	Systems Applications Products
SCM	Supply Chain Management
SD	Sales & Distribution
SNC	Secure Network Communication
SOD	Separation Of Duties & Segregation Of Duties
SSO	Single Sign-On

SEZNAM OBRÁZKŮ

Obr. 1.1.	Logo společnosti HP TRONIC [2]	13
Obr. 1.2.	Logo značky ETA [4]	14
Obr. 2.1.	Schéma podnikových informačních systémů [6]	15
Obr. 2.2.	Způsob integrace dat v ERP systémech [5]	16
Obr. 2.3.	Informační pyramida podle organizačních úrovní podniku [5]	17
Obr. 2.4.	Schéma třívrstvé architektury [25]	19
Obr. 2.5.	Vizualizace dodavatelů ERP pomocí metodologie Magic Quadrant [10]	20
Obr. 3.1.	Logo společnosti SAP [15]	23
Obr. 3.2.	Historie verzí produktu SAP [15]	23
Obr. 3.3.	Funkční moduly produktu SAP R/3 [6]	25
Obr. 3.4.	Graf vývoje průměrného výkonu v SAPS	27
Obr. 3.5.	SAP GUI v motivu Quartz	28
Obr. 4.1.	Úvodní obrazovka při zobrazení uživatele v transakci SU01	38
Obr. 5.1.	Vzhled výstupu v transakci DBACOCKPIT	45
Obr. 6.1.	Vstupní obrazovka transakce SUIM	47
Obr. 6.2.	Seznam uživatelů mající roli Z_HPT_USER v transakci PFCG... ..	48
Obr. 6.3.	Rozdíly oprávnění mezi dvěma uživateli	50
Obr. 6.4.	Neúspěšná kontrola oprávnění pro debugování	51
Obr. 6.5.	Vytvoření kritického oprávnění ZDEBUG	52
Obr. 6.6.	Nastavení kritického oprávnění ZDEBUG	52
Obr. 6.7.	Výsledek kontroly kritických oprávnění v transakci SUIM	53
Obr. 6.8.	Kontrola kritického oprávnění u role Z_HPT_USER	54
Obr. 6.9.	Nastavení autorizačního objektu S_DEVELOP	55
Obr. 6.10.	Kontrola kritického oprávnění u role Z_USER_TEMPORARY	56
Obr. 6.11.	Vyžadované autorizační objekty k provedení transakce SCC5	57
Obr. 6.12.	Vyžadované hodnoty u autorizačního objektu S_USER_AGR	57
Obr. 6.13.	Nastavení autorizačního objektu S_TRANSPRT	58
Obr. 6.14.	Nastavení autorizačního objektu S_DEVELOP	59
Obr. 7.1.	Založení uživatele TEST_JT	63
Obr. 7.2.	Vytvoření iniciálního hesla pro prvotní přihlášení	63
Obr. 7.3.	Přidání uživatele do skupiny uživatelů	64
Obr. 7.4.	Příklad nastavení autorizačního objektu S_USER_GRP	64
Obr. 7.5.	Deaktivace autorizačního objektu S_USER_PRO	66
Obr. 7.6.	Vymazání autorizačního objektu S_USER_PRO	66
Obr. 7.7.	Nastavení role Z_HPT_ROLE	68

Obr. 7.8.	Nastavení role Z_HPT_ROLE_FI.....	68
Obr. 7.9.	Odvození role od Z_HPT_DEFAULT.....	70
Obr. 7.10.	Nastavení role Z_ROLE_CHANGE	72
Obr. 7.11.	Nastavení role Z_ROLE_GEN	72
Obr. 7.12.	Změna systémových parametrů.....	73
Obr. 8.1.	Seznam chybějících oprávnění k provedení transakce SE16.....	84
Obr. 8.2.	Seznam uživatelů a jejich profilů, které jim umožňují provedení transakce	84
Obr. 8.3.	Úvodní obrazovka transakce ZHP_AUTH_VIEW	85
Obr. 8.4.	Údržba tabulky v transakci SM30	86
Obr. 8.5.	Seznam vytvořených objektů.....	86

SEZNAM TABULEK

Tab. 2.1.	Klasifikace ERP systémů podle funkčního zaměření [5]	18
Tab. 4.1.	Doporučené základní parametry hesla [29]	33
Tab. 4.2.	Seznam vhodných transakcí k uzamknutí [29]	37
Tab. 6.1.	Počty uživatelů dle počtu spustitelných transakcí a pracovních pozic	49
Tab. 6.2.	Počty uživatelů dle počtu spustitelných transakcí a zaměření pra- covních pozic	50
Tab. 6.3.	Hodnoty autorizačních objektů u role Z_USER_TEMPORARY ..	58
Tab. 6.4.	Seznam kontrolovaných rolí a nalezených kritických oprávnění	60
Tab. 6.5.	Parametry hesla v programu RSPARAM	61
Tab. 7.1.	Potřebné autorizační objekty pro změnu oprávnění	68
Tab. 7.2.	Parametry odvození role pro organizaci 1000	70
Tab. 7.3.	Autorizační objekty umožňující vytváření a úpravu role	71
Tab. 7.4.	Autorizační objekty umožňující generování role	72
Tab. 7.5.	Transakce, u kterých došlo k jejich uzamčení	74

SEZNAM PŘÍLOH

- P I. Metoda tcode_check
- P II. Seznam rolí uživatele TESTC1
- P III. Seznam uživatelů, kteří mají roli Z_HPT_USERS
- P IV. Seznam profilů uživatele TESTC1
- P V. Seznam uživatelů, kteří mají profil T-HD770372

PŘÍLOHA P I. METODA TCODE_CHECK

```
METHOD tcode_check.  
DATA: r_values TYPE ty_r_value,  
      wa_values LIKE LINE OF r_values,  
      lt_auth TYPE STANDARD TABLE OF auth,  
      r_auth TYPE ty_r_auth,  
      wa_auth LIKE LINE OF r_auth,  
      len TYPE i.  
  
SELECT object, field, low FROM usobt  
      INTO TABLE @DATA(lt_usobt)  
      WHERE name = @me->v_tcode  
      AND low <> ''.  
  
LOOP AT lt_usobt INTO DATA(wa_usobt).  
  CLEAR: wa_values, r_values.  
  wa_values-sign = 'I'.  
  wa_values-option = 'EQ'.  
  wa_values-low = wa_usobt-low.  
  APPEND wa_values TO r_values.  
  
  SELECT auth FROM ust12  
    INTO TABLE @DATA(lt_auth_temp)  
    WHERE objct = @wa_usobt-object  
    AND field = @wa_usobt-field  
    AND ( von IN @r_values OR von = '*' ).  
  
  SORT lt_auth_temp BY auth.  
  
  IF lt_auth IS INITIAL.  
    APPEND LINES OF lt_auth_temp TO lt_auth.  
  ELSE.  
    LOOP AT lt_auth INTO DATA(temp).  
      READ TABLE lt_auth_temp INTO DATA(temp2) WITH KEY auth  
      = temp BINARY SEARCH.  
      IF sy-subrc <> 0.  
        DELETE lt_auth.  
      ENDIF.  
    ENDLOOP.  
  ENDIF.  
  
ENDLOOP.  
  
SORT lt_auth.  
DELETE ADJACENT DUPLICATES FROM lt_auth.
```

```

LOOP AT lt_auth ASSIGNING FIELD-SYMBOL(<row>).
    wa_auth-sign = 'I'.
    wa_auth-option = 'EQ'.
    IF <row>(3) = 'T-H'.
        len = strlen( <row> ).
        len = len - 2.
        wa_auth-low = <row>(len).
    ELSEIF <row>(2) = '&_'.
        wa_auth-low = <row>+2.
    ELSE.
        wa_auth-low = <row>.
    ENDIF.
    APPEND wa_auth TO r_auth.
ENDLOOP.

SELECT bname AS uname, profile AS object, ptext FROM ust04
LEFT JOIN usr11 ON usr11~profn = ust04~profile AND langu =
    @sy-langu
    INTO CORRESPONDING FIELDS OF TABLE @me->t_users
    WHERE profile IN @r_auth.

SORT me->t_users BY uname.
IF me->t_users IS NOT INITIAL.
    display_alv( CHANGING c_tab = me->t_users ).
ELSE.
    me->v_error = 'X'.
ENDIF.

ENDMETHOD.

```

< System Nápořádá SAP > 250 ms INS [] — X

Zrušit

Konec

Uživatel	Úplné jméno	Název	Označení role
TESTC1	Test Číslo 1	Z_HPT_USERS	Revize uživatelských rolí 2023
TESTC1	Test Číslo 1	Z_HPT_USER_2100	Obscená práva pro uživatele

PŘÍLOHA P III. SEZNAM UŽIVATELŮ, KTERÍ MAJÍ ROLI Z_HPT_USERS

[illegible]

SAP

Konec

	Označení role
TESTC1 Test Číslo 1 T-HD770372	Profil k roli Z_HPT_USERS
TESTC1 Test Číslo 1 T-HP770124	Profil k roli Z_HPT_USER_2100

Systém

Nápověda

<

SAP

SAP

> 250 ms

INS

📄

—

🖨️

✕

✓ [] Zrušení

🔍

☰

≡

🔍

Q+

🔍

Σ

½

📦

📦

🔄

📊

📈

ℹ️

Konec

⚙️

📄

Uživatel	Úplné jméno	Název	Označení role
TESTC1	Test	Číslo 1 T-HD770372	Profil k roli Z_HPT_USERS
TESTC2	TESTC2	T-HD770372	Profil k roli Z_HPT_USERS
TROJANU Jiří Troján	T-HD770372	T-HD770372	Profil k roli Z_HPT_USERS