VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH SYSTÉMU SPRÁVY IDENTIT VE FIRMĚ
CORPORATION IDENTITY MANAGEMENT SYSTEM DESIGN

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Dominik Nop**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Viktor Ondrák, Ph.D.**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Dominik Nop**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Návrh systému správy identit ve firmě

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je navrhnout systém správy identit ve společnosti.

Základní literární prameny:

BERTINO, E. a K. TAKAHASHI. Identity management: concepts, technologies, and systems. London, UK: ARTECH, 2011. ISBN 16-080-7039-5.

DOSTÁLEK, L., M. VOHNOUTOVÁ a M. KNOTEK. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. 2., aktualiz. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2619-6.

HANSEN, M., A. PFITZMANN a S. STEINBRECHER. Identity management throughout one's whole life. Information Security Technical Report [online]. 0805, 13(2), 83-94 [cit. 2016-09-28]. DOI: 10.1016/j.istr.2008.06.003. ISSN 1363-4127.

KRHOVJÁK, J. a V. MATYÁŠ. Autentizace a identifikace uživatelů. Zpravodaj ÚVT MU: bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě [online]. Brno: Masarykova univerzita, 2011, XVIII(1). ISSN 1212-0901.

STAMP, Mark. Information security principles and practice [online]. Hoboken, N.J: Wiley-Interscience, 2005. s. 153-176. ISBN 978-04-717-44191.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Předmětem této bakalářské práce je navrhnout novou podobu systému správy identit ve firmě. V úvodní části se práce zabývá teoretickými poznatky z oblasti správy identit, od základních pojmů a definic po podrobný popis jednotlivých komponent systému. Součástí práce je analýza současného stavu systému správy identit ve firmě ABC. Na základě této analýzy i teoretických poznatků je v práci sestaven návrh na vylepšení systému. Závěr obsahuje zhodnocení a možnosti vylepšení nového návrhu v budoucnu.

Abstract

This bachelor thesis' main task is development of a new variation of the corporal identity management system. Firstly, this thesis deals with theoretical knowledge related to the subject of identity management. Secondly, it analyses the current status of the identity management system in a company ABC. A plan for system improvement in this work is based on this analysis and theoretical knowledge as well. Finally, the work contains an evaluation and suggests possible improvements of the new system for the future time.

Klíčová slova

Správa identit, autentizace, autorizace, doména, přístup, SSO, ICT bezpečnost

Keywords

Identity management, authentication, authorisation, domain, access, SSO, ICT security

Bibliografická citace

NOP, D. *Návrh systému správy identit ve firmě.*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 63 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D..

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2017

……

podpis studenta

Poděkování

Děkuji vedoucímu mé práce Ing. Viktoru Ondrákovi, Ph.D. za veškeré rady, připomínky a čas věnovaný této práci. Také děkuji zaměstnanci společnosti ABC za poskytnuté informace o společnosti a četné konzultace, které byly pro vznik této práce zásadní.

OBSAH

ÚVOD

S nástupem moderních ICT technologií se počet identit na každou osobu zvětšuje každým rokem. Ve společnostech tomu není výjimkou a je pro ně proto zásadní, aby byly schopny tyto identity efektivně spravovat s pomocí systémů, jejichž zavedení ušetří práci zaměstnanců a tím i náklady společnosti.

Identity také vyžadují patřičnou úroveň zabezpečení, aby nemohlo dojít k jejich zneužití. To klade při rostoucím množství identit stále větší nároky na zaměstnance. Při příliš vysokých nárocích může ze strany zaměstnance dojít k obcházení bezpečnostních předpisů, což může mít pro společnost fatální následky. Systémy na správu identit mohou poskytnout efektivní řešení v podobě centralizace řízení přístupů. Snižováním nároků na zaměstnance se tak optimalizuje stav informační bezpečnosti ve společnosti, což vede ke snížení nákladů způsobených bezpečnostními incidenty. I proto se tyto systémy řadí do oblasti informační bezpečnosti.

V této bakalářské práci se budu zabývat návrhem nové podoby systému správy identit ve společnosti ABC s cílem zvýšit úroveň zabezpečení a zefektivnit některé procesy.

1 CÍL A METODIKA PRÁCE

Cílem této práce je navrhnout vylepšení v systému správy identit společnosti ABC. Požadavkem firmy je zvýšení bezpečnosti a pokud možno zjednodušení nebo automatizace některých procesů ve společnosti. Pro vytvoření návrhu bude v rámci práce provedena analýza současného stavu, s cílem najít bezpečnostní slabiny a zbytečně pomalé procesy.

2 TEORETICKÁ VÝCHODISKA PRÁCE

V teoretické části uvedu základní pojmy související s návrhem řešení v praktické části.

2.1 ISMS

ISMS je zkratka pro Information Security Management System, česky Systém řízení bezpečnosti informací. Jde o systematický přístup ke správě citlivých firemních informací tak, aby tyto informace zůstaly zabezpečeny. ISMS zahrnuje osoby, procesy a IT systémy [1].

2.2 Řada norem ISO/IEC 27000

Mezinárodní organizace pro standardizaci (ISO) vydala mezinárodně platnou řadu norem pro ISMS. Pro tuto řadu rezervovala sérii ISO 27000. Firmy nejsou povinny se touto řadou norem řídit, ale jejich dodržování vede k získání a udržení vysoké úrovně zabezpečení dat a ke standardizaci systémů. Základními normami, které v teoretické části stručně zmíním, jsou normy ISO/IEC 27000:2016, 27001:2013 a 27002:2013 [2].

2.2.1 ISO/IEC 27000:2016

„ISO/IEC 27000 Information technology - Security techniques - Information security management systems - Overview and vocabulary obsahuje definici pojmů a terminologický slovník pro další normy z této série“ [2].

2.2.2 ISO/IEC 27001:2013

Celým názvem ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements. Tato norma poskytuje firmám doporučený postup při aplikaci, udržování i zlepšování ISMS. Kombinuje pojmy z oblasti informatiky a managementu a doporučuje např. zavedení zlepšovacího modelu PDCA (plan-do-check-act) pro aplikaci ISMS ve firmě [2].

V příloze této normy jsou také uvedeny hlavní části ISO/IEC 27002 [2]. Více zmíním v samotném popisu normy 27002.

2.2.3 ISO/IEC 27002:2013

V normě „ISO/IEC 27002:2013 Information technology – Security techniques - Code of practice for information security management“ jsou definovány nejlepší bezpečnostní postupy z oblasti informační bezpečnosti. Tyto základní postupy se dále rozpadají na specifičtější opatření a umožňují tak detailně posoudit úroveň zabezpečení dat ve firemním informačním systému. Hlavní části této normy jsou zmíněny v příloze předcházející normy. Zatímco ISO/IEC 27002 pomáhá firmám odhalit slabiny v zabezpečení, ISO/IEC 27001 pomáhá s výběrem vhodné sady opatření pro tyto slabiny [2].

2.3 Identita a její složení

M. Bishop [3] definuje identitu jako souhrn atributů, které jednoznačně identifikují subjekt v dané množině subjektů. Důležitým aspektem této definice je, že se nevztahuje pouze na osoby. Ty jsou nejčastějšími nositeli identit, ale za nositele lze na základě této definice považovat i např. softwarové agenty nebo hardware.

M. Bishop [3] také zmiňuje možnost přidělení identit umělým objektům, např. stroje, budovy, předměty denní spotřeby atd. Dalšími nositeli mohou být přírodní objekty, např. plodiny a dobytek. To vše díky neustále se zrychlujícímu rozvoji informačně-komunikačních technologií.

Tato teorie je shrnuta v doporučení organizace ITU [4], která identitu definuje jako informace o entitě. Tyto informace jsou samy o sobě dostatečné pro identifikaci této entity v konkrétním kontextu. Dále uvádí 3 druhy informací, ze kterých se každá identita skládá: identifikátory, atributy a ověřovací údaje

2.3.1 Identifikátory

Identifikátor je v ITU-T Y.2720 [4] definován jako libovolná forma dat (číslice, písmena, symboly atd.), užívaná pro identifikaci entity. Typickými příklady jsou čísla dokladů (občanský průkaz, cestovní pas atd.), telefonní čísla, uživatelská jména, nebo URI.

2.3.2 Atributy

Podle ITU-T Y.2720 [4] jsou atributy informacemi, které jsou vázány k dané entitě, a které specifikují její charakteristiky. Příkladem u osob je pohlaví, rodné příjmení nebo záznamy aktivit. Atributy mohou být i výstupem činností dané entity, např. tituly, role nebo záznamy aktivit.

2.3.3 Credentials – ověřovací údaje

ITU-T Y.2720 [4] definuje ověřovací údaje jako množinu dat, která umožňuje autentizaci a autorizaci entity. Těmto dvěma pojmům se budu věnovat v následujících podkapitolách.

Mezi ověřovací údaje patří hesla, PIN kódy, digitální certifikáty, Kerberos tickety apod.

2.4 Autentizace

Pojem autentizace úzce souvisí s pojmem identifikace. Identifikace je proces zjištění identity entity, autentizace identitu ověřuje. Existuje-li množina identifikátorů entit a jejich ověřovacích údajů, je potřeba vyhledat identifikátor entity v databázi. Pro autentizaci entity je potřeba pouze identita dané entity. Ověřuje se správnost předložených ověřovacích údajů srovnáním s údaji v databázi [5].

Existují 3 základní metody autentizace: něčím, co máme, co víme a čím jsme. Každá z metod má své výhody a nevýhody [5].

2.4.1 Autentizace něčím, co máme

Tato metoda je založena na vlastnictví předmětů (tzv. tokenů). Tyto tokeny „*mají buď specifické fyzické vlastnosti (tvar, elektrický odpor, elektrickou kapacitu apod.), nebo obsahují specifické tajné informace (např. kvalitní heslo nebo kryptografický klíč), nebo jsou dokonce schopny provádět specifické (obvykle kryptografické) výpočty"* [6].

Výhodou této metody jsou většinou nízké požadavky na uživatele, kteří nejsou nuceni si pamatovat jakékoli údaje. Největším rizikem je ztráta, případně krádež a zneužití tokenu, proto je kladen důraz na fyzické zabezpečení tokenu [6].

2.4.2 Autentizace něčím, co víme

Tato forma autentizace se spoléhá na to, že si je uživatel schopen zapamatovat informaci, na kterou je následně v případě potřeby autentizace dotázán. Do této skupiny patří hesla, nejrozšířenější nástroj pro autentizaci. Hesla se rozšířila díky své všestrannosti a snadno pochopitelnému principu fungování pro uživatele jakékoli věkové kategorie [7].

Velkou slabinou hesel je, že se spoléhají na schopnosti uživatele. Realita je taková, že velká část uživatelů na webu stále volí jednoduchá hesla kvůli pohodlí, např. kombinaci po sobě jdoucích čísel či písmen (12345, abc123 qwertz apod.), nebo univerzální výrazy (heslo, password, pass, password123 apod.). Tato hesla jsou tak často používána, že je útočník obvykle zkusí zadat jako první. Existují programy, které již obsahují seznam nejpoužívanějších frází (tzv. slovník) a zkouší je do systému automaticky zadávat. Tento typ útoku je znám jako „Slovníkový útok“ [8].

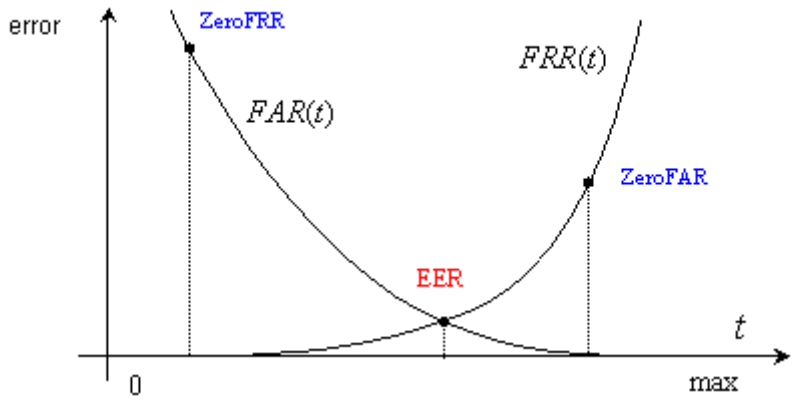
Pod tuto metodu spadají i další druhy autentizace, např. grafická hesla. Ta jsou založena na tendenci uživatele volit jednoduše zapamatovatelné ověřovací údaje. V případě grafických hesel je tato vlastnost velmi subjektivní, proto neexistuje jednoznačný postup pro uhádnutí hesla. Nevýhodou je snadné vypozorování metodou tzv. shoulder surfingu, stejně jako nepoužitelnost pro uživatele se zrakovým postižením [9].

2.4.3 Autentizace něčím, čím jsme

Každá forma života disponuje nepřeberným množstvím biologických informací. Tato metoda využívá ty, které jsou u většiny populace této formy života jedinečné. Tato metoda rozvíjí především pro autentizaci osob. Příklady jsou autentizace s pomocí otisků prstů, snímků rohovky a záznamu hlasu. Autentizovat osobu lze i podle tvaru ucha, obličeje, nebo stylu chůze [6].

Každá autentizace s pomocí biometriky musí řešit četnost výskytu 2 typů chyb – četnost nesprávných odmítnutí (false rejection rate - FRR) a četnost nesprávných přijetí (false acceptance rate - FAR). Oba problémy současně vyřešit nelze, snížení četnosti výskytu jednoho druhu chyby vede ke zvýšení četnosti výskytu toho druhého [10].

K nesprávnému odmítnutí dojde v případě, že je odmítnut přístup osobě, která by přístup měla získat. V takovém případě stačí, když se odmítnutá osoba autentizuje opakovaně.



Obr. 1: Graf vztahu FRR a FAR. [10]

Nesprávné přijetí je chyba, kdy je do systému vpuštěna osoba, která by přístup získat neměla. Vysoká FAR je bezpečnostním rizikem, proto bývá kladen mnohem větší důraz na snížení výskytu této chyby, za cenu vyššího FRR [9].

Výhodou biometrických skenů je, že veškeré údaje jsou součástí uživatele samotného. Není potřeba, aby si uživatel pamatoval jakékoli údaje, nebo je nosil s sebou v podobě fyzického tokenu. Nevýhodou jsou vysoké náklady na pořízení kvalitních forenzních systémů, nemluvě o vysokých časových nárocích na provedení všech výpočtů (až několik dní). Levnější komerční systémy provádí sken s velkou chybovostí, což má velký dopad na funkčnost i bezpečnost autentizačního systému [9].

2.4.4 Vícefaktorová autentizace

Každá ze zmíněných metod má své slabiny. Řešením je použít více metod pro jednu autentizaci, aby jedna metoda pokryla slabé stránky druhé. Tento princip je běžně využíván v oblastech s vysokými nároky na zabezpečení, např. v bankovnictví. Klient se při platebních transakcích v kamenném obchodě autentizuje pomocí platební karty (token) a PIN kódu (znalost). Různé banky užívají různé kombinace metod, od PIN a jednorázových TAN kódů, přes USB a HW tokeny, až po biometrické skenery [9].

.

2.5 Životní cyklus identity

Systém správy identit se identitami zabývá od jejich vzniku, až po zánik. V této podkapitole uvedu všechny části životního cyklu identity – vznik, užívání, aktualizace a revokace [11].

2.5.1 Vznik

Samotný vznik identity je dále dělen na 3 dílčí části. V první fázi jsou potvrzeny atributy autoritami, důvěryhodnými pro příjemce identity. Příkladem může být předložení občanského průkazu při zakládání bankovního účtu, zadání a ověření e-mailové adresy při registraci na stránkách e-shopu apod. Tento krok není proveden při každém zakládání identity. Při zakládání e-mailové schránky nemusí být vyžadovány žádné údaje [11].

Ve druhé fázi dochází k přidělení ověřovacích údajů, kterými se bude uživatel autentizovat. Jde např. o přidělení platební karty a PIN kódu bankou. Dnes si tyto atributy může jejich budoucí vlastník často vytvořit sám, např. přístupová hesla do účtů na webu [11].

Ve třetí fázi dochází podle [11] k vytvoření identity, složené z potvrzených atributů, ověřovacích údajů a přidělených identifikátorů.

2.5.2 Užívání

Nově vytvořená identita je následně využívána pro získání přístupů k požadovaným službám. Je nezbytné, aby identita byla využívána bezpečně a diskrétně. Za účelem splnění těchto podmínek bývají nasazovány do provozu různé funkce, které přiblížím v následujících odstavcích [11].

Důležité je zajištění důvěryhodné komunikace. To je možné jen v případě, že se odesilatelé i příjemci zpráv jsou schopni navzájem vyhledat, rozlišit a autentizovat. Stejně nutné je klást důraz i na zabezpečení služeb pro vyhledávání identit [11].

Další nasazovanou funkcí je tzv. Single Sign-On (SSO). Za normálních okolností je potřeba jedna sada přihlašovacích údajů pro autentizaci a přístup k jedné službě. SSO umožňuje výsledky autentizace znovu využít k získání přístupu k dalším službám [12]. Jednotlivé architektury SSO, včetně výhod i nevýhod, rozeberu v následujících podkapitolách.

Dále lze využít i funkci sdílení atributů. Sdílení probíhá mezi poskytovateli identit a poskytovateli služeb, čímž dochází k zamezení vzniku redundancí a zajištění integrity atributů, které jsou rozptýleny mezi službami napříč sítí. Sdíleny by měly být pouze ty atributy, na kterých se dohodne poskytovatel identity s jejím nositelem [11].

2.5.3 Údržba

Údaje identity se během doby její existence mění. Z bezpečnostních důvodů dochází k obměně ověřovacích údajů – digitální certifikáty i hesla mívají omezenou platnost.

Některé údaje se mění přirozeně, např. zdravotní stav. Jiné závisí na činnostech nositele identity – bydliště, pracovní pozice apod. Proto dochází k aktualizaci údajů. [13].

Všechny změny musí být zaznamenávány a být dohledatelné pro potřeby auditu. Zároveň by nemělo docházet k rozsáhlejším změnám v klíčových identifikátorech, proto při zakládání identity je tyto identifikátory potřeba vhodně zvolit, např. rodné číslo osoby [13].

2.5.4 Revokace

Identita by měla existovat jen po dobu, kdy je její existence potřebná. Je-li např. ukončena spolupráce se zaměstnancem ve firmě, stává se z pohledu zaměstnavatele existence identity této osoby ve firemních systémech bezpečnostní hrozbou, která může způsobit krádež interních dat, nebo sabotáž projektů. Proto dochází k revokaci identity. Tím jsou bývalému zaměstnanci odebrána všechna oprávnění a přístupy [13].

2.6 Identity management – správa identit

Martin Lízner [14] popisuje správu identit jako: „*informační systém, který dokáže z jednoho místa ovládat životní cyklus všech uživatelských účtů v organizaci a zároveň sledovat jejich změny díky auditu.“*

Systém správy identit je složen z různých technologií, přizpůsobených potřebám prostředí, ve kterém funguje. Existují 3 základní technologie – adresářová služba, systém řízení přístupů a provisioning systém [15].

2.6.1 Adresářová služba a LDAP

Adresář je srdcem systému správy identit, jde o databázi údajů o identitách. Tyto údaje jsou využívány dalšími komponentami systému správy identit. Adresářová služba má za úkol v adresářích ukládat a organizovat informace o uživatelích. U menších podniků a organizací se lze nejčastěji setkat s Active Directory Domain Services (AD DS) od Microsoftu, zatímco ve společnostech, vyžadujících větší a komplexnější řešení, je využíváno více databází [16, 17]. AD DS rozeberu podrobněji v samostatné podkapitole.

Prioritou pro adresářové služby je maximalizace dostupnosti. V případě neuspokojivé dostupnosti lze přidat dodatečné servery. Adresářové služby běžně využívají alespoň dva. Tyto servery svůj obsah vzájemně replikují [16, 17].

Nevýhodou systému je nízká datová kapacita a omezené množství operací, které je možné s daty provádět. Např. standardní SQL příkaz JOIN není možné v adresářové službě použít, stejně jako transakce nebo indexy. Údaje v adresářích ale slouží nejčastěji ke čtení, proto je nejdůležitější rychlost čtení, která je v případě těchto databází vysoká [16].

V současnosti většina adresářových služeb využívá protokol LDAP, který vznikl zjednodušením standardu X.500 z 80tých let. LDAP je zkratka pro Lightweight Directory Access Protocol [16, 17]. Jde o „*aplikační protokol pro dotazování a modifikaci adresářových služeb nad TCP/IP*“ [17]. Důležitou modifikací je možnost autentizace uživatele. Díky tomu se z adresářové služby stává jednoduchý autentizační server. Jde o jednoduché řešení, které nepodporuje SSO, proto je vhodné pouze pro menší podniky [16, 17].

2.6.2 Systém řízení přístupů

Identita slouží uživateli k získání přístupu ke službám, kterých potřebuje využít v rámci své role. Oprávnění každého uživatele by nemělo přesahovat tento rámec, uživatel by měl mít přístup pouze k těm službám, které skutečně potřebuje využívat. K tomu slouží systém řízení přístupů [13].

Dalším důležitým úkolem systému řízení přístupů je sjednotit autentizační mechanismy a oddělit je od aplikací. Zajištění autentizace pro každou aplikaci samostatně je plýtváním zdrojů, nemluvě o komplikovanějším prostředí pro uživatele [18].

V prostředí správy identit se používá několik různých řešení. Prvním je již dříve zmíněný SSO – Single Sign-On [18]. Pro toto řešení jsem se rozhodl vyhradit samostatnou podkapitolu, z důvodů obsáhlosti tématu. V této části práce uvedu systém řízení přístupů na základě rolí – RBAC.

RBAC – Role Based Access Control je založen na existenci opakovaně přidělitelných objektů – tzv. rolí. Ty mají v rámci RBAC přiděleny oprávnění a přístupy. Systém tyto role přiděluje identitám. Díky tomu není potřeba přidělovat každé identitě zvlášť jednotlivá oprávnění, stačí ji přiřadit některou z rolí [14].

RBAC má možnost řídit na úrovni rolí funkci Segregation of Duties (SoD). S její pomocí zajišťuje, aby žádný zaměstnanec nemohl disponovat všemi rolemi potřebnými pro provedení celé transakce samostatně. *„Uživatel nemůže mít například roli, která jej opravňuje k vydávání faktur společně s rolí, která faktury kontroluje“* [14].

2.6.3 Provisioning

S každou personální změnou v podniku je potřeba identity měnit – vytvářet nové, rušit staré, měnit stávající. Pokud jsou tyto změny prováděny ručně, dochází ke zpožděním, které mohou mít pro firmu katastrofální důsledky – např. nespokojený zaměstnanec propuštěný okamžitou výpovědí může svého přístupu zneužít, není-li včas připraven o

svá oprávnění. K zajištění co nejrychlejší úpravy dat vznikly systémy na správu účtů, tzv. provisioning systémy [19].

Změny mohou být v provisioning systému prováděny automaticky. Jsou-li provedeny změny např. v HR systému, provisioning převede během následující automatické synchronizace údaje do dalších systémů, aby v nich mohlo dojít k potřebným změnám. Mezi výhody patří i možnost uložit do paměti vazby identit na zaměstnance. V případě odchodu zaměstnance je provisioning schopen zrušit všechny jeho identity, včetně přístupů a oprávnění. Stejným způsobem může postupovat při úpravě některých údajů, např. při převedení zaměstnance na jinou pozici. Systém tak šetří práci administrátorům a brání chybovosti [19].

2.7 Active Directory Domain Services

AD DS je serverovou rolí adresářové služby Active Directory od firmy Microsoft, která je součástí systémů Windows Server od verze 2000 až po současnost. *„AD v sobě zahrnuje řadu služeb. Jeho primární role je poskytování centrálních služeb pro autentizaci a autorizaci, tedy správa uživatelů (přesněji správa účtů, protože to může být i třeba počítač). Ale různé části poskytují mnoho dalších funkcí, například Group Policy umožňuje spravovat politiky jednotlivých počítačů (co je na nich povoleno) a instalovat hromadně (a vzdáleně) aplikace.“* [20].

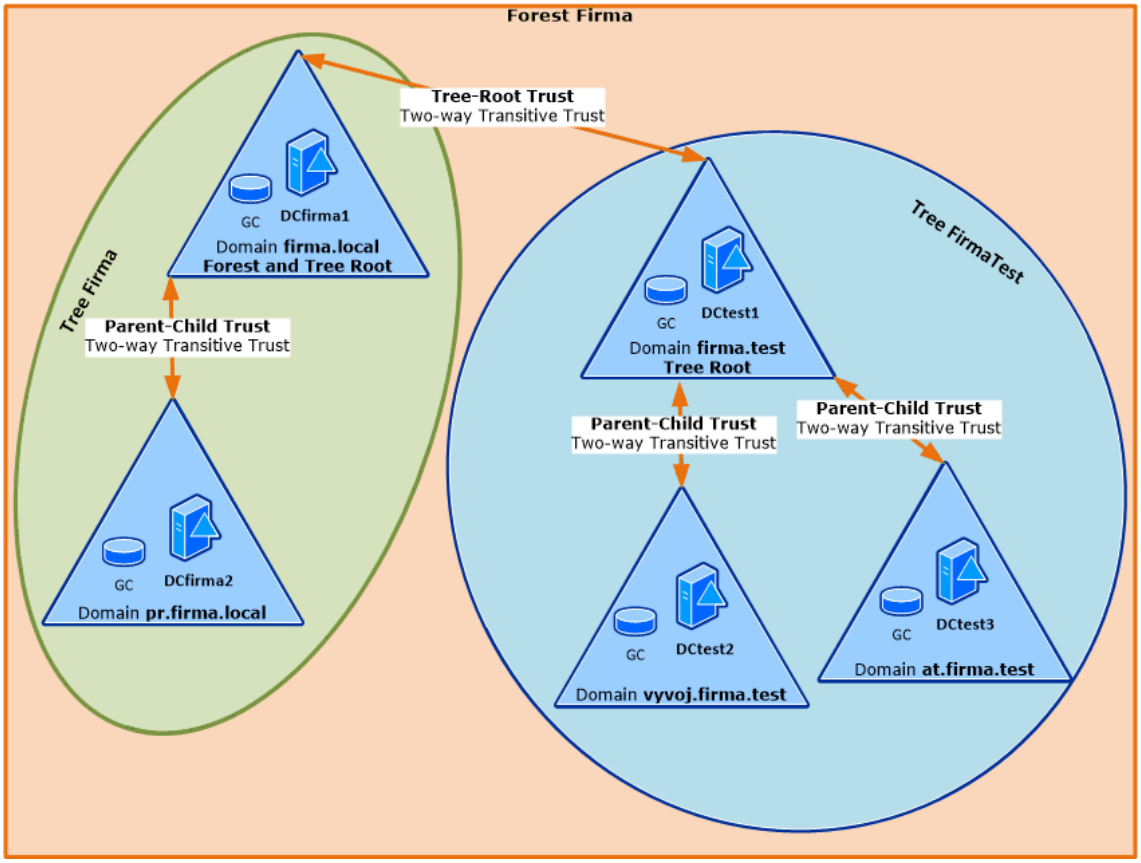
2.7.1 Doména, strom, les

Základním kamenem struktury AD je doména (Domain). Tvoří ji všechna zařízení, která sdílí stejný adresář. Doménu mohou tvořit zařízení z více sítí, nacházející se v různých

lokalitách. Každá doména musí mít své jedinečné jméno. To může být složeno z písmen, číslic, případně pomlčky. Jednotlivé komponenty jména jsou odděleny tečkou [21].

Máme-li více domén, spojených hierarchickými vazbami, mluvíme o tzv. stromu (Tree). V rámci stromu stojí nejvýše kořenová doména, která sdílí svůj jmenný prostor s ostatními doménami. Pokud má kořenová doména jméno např. example.local, budou jména všech podřazených domén toto jméno obsahovat. Další částí bude jejich vlastní relativní jméno. Jméno podřazené domény pak může být např. test.example.local [21].

Pokud je potřeba zajistit komunikaci mezi stromy, je možné je seskupit do lesa (Forest). Domény v lese mají stejné schéma a sdílí globální katalog (více uvedu v další části podkapitoly), ale nesdílí obsah databází ani nejsou na sobě závislé, co se týče pojmenování. Komunikace mezi stromy je zajištěna vzájemnou důvěrou mezi kořenovými doménami daných stromů (Tree-Root trust). Stejně jako v případě stromu je i v lese jedna z domén kořenovou [21].



Obr. 2: Příklad schématu doménových vazeb [21]

2.7.2 Lokality

Lokality (Sites) v AD DS reprezentují fyzickou topologii sítě. V prostředí AD DS jsou lokality využívány za účelem co nejefektivnější replikace mezi DC. Jejich zavedením je také zajištěno, že se uživatel bude autentizovat vůči nejbližšímu DC. To snižuje nároky na přenos dat ve WAN síti i zpoždění autentizace. V logické struktuře nehrají lokality žádnou roli, proto se zde nezobrazují [20].

2.7.3 Doménový řadič

Doménový řadič (Domain Controller – DC) je server, na kterém je nainstalován AD DC a který obsahuje repliku doménového adresáře (doménovou databázi). Jedna doména může mít více doménových řadičů a každé zařízení je v rámci domény řazeno pod jeden z nich. Přes DC je možné provádět změny v adresářích, přičemž změny jsou automaticky replikovány do ostatních DC v doméně [21].

2.7.4 Globální katalog

Globální katalog (Global Catalog – GC) je nejdůležitější služba fungující v rámci lesa. Obsahuje základní informace o každém objektu v lese. Každá doména má alespoň jeden GC server a zařízení z jakékoli domény je díky jeho službám schopné dohledat zařízení v jiné doméně stejného lesa. GC server musí vždy být DC [20].

2.7.5 Skupiny, zásady skupin

Pro usnadnění správy uživatelských účtů i zařízení v doméně je možné tyto objekty rozdělit do skupin (Groups). Těmto skupinám je následně možné přidělovat tzv. zásady (Policies), které by jinak musely být nastavovány pro každý objekt zvlášť [22].

„Ve službě AD DS existují dva typy skupin: distribuční skupiny a skupiny zabezpečení. Distribuční skupiny lze použít k vytvoření distribučních seznamů pro e-maily. Skupiny zabezpečení slouží k přiřazení oprávnění ke sdíleným prostředkům“ [22].

Dále lze dělit skupiny podle jejich rozsahu, tedy podle oblasti působení. Existují 3 typy rozsahu skupin – místní doménová, globální a univerzální [22].

U místních doménových skupin (Domain Local Groups) lze rozhodovat o přístupu k zařízením a službám, nacházejícím se ve stejné doméně [22].

Globální skupiny (Global Groups) řeší přístup k prostředkům jakékoli domény v rámci stejného lesa. Výhodou globálních skupin je, že nejsou replikovány mimo doménu. Díky tomu jejich změny nezatěžují replikační komunikaci [22].

Univerzální skupiny (Universal Groups) jsou využívány ke sloučení globálních skupin a slouží ke zjednodušení přístupu k prostředkům ve větších prostředích s více doménami v rámci lesa. Vzhledem k jejich vlastnostem jsou vhodnější do rozsáhlejších doménových struktur. V případě univerzálních skupin je vhodné neprovádět mnoho změn, kvůli nutnosti replikovat změny do dalších DC [22].

2.7.6 Principal

Aby bylo možné v rámci domény rozpoznat jednotlivé uživatele i služby (např. pro využití protokolu Kerberos), musí mít každá služba i uživatel svůj principal [23].

V případě uživatele mluvíme o tzv. User Principal Name (UPN). Toto jméno se skládá ze dvou částí – uživatelského přihlašovacího jména, které tvoří tzv. UPN prefix a DNS jména domény, tzv. UPN suffix, přičemž jméno domény bývá v rámci pojmenování DNS serverem převedeno z malých na velká písmena. Obě části UPN jsou od sebe odděleny zavináčem. V případě, že uživatelským jménem bude „userexample“ a jméno domény bude „domain.test,“ bude UPN tohoto uživatele userexample@DOMAIN.TEST [23].

U UPN je zřejmá podobnost s e-mailovou adresou. Tato podobnost není náhodná. Microsoft zavedl UPN v této podobně ve snaze usnadnit uživatelům zapamatování si tohoto jména [23].

Pro identifikaci služby v rámci lesa slouží tzv. Service Principal Name (SPN). Zpravidla se skládá ze dvou částí. První částí je identifikátor třídy služby, druhou doménové jméno zařízení, na kterém služba běží. Případně může být součástí jména i číslo portu, na kterém se v rámci daném zařízení služba nachází a jméno služby. Číslo portu je potřeba specifikovat v případě, že se služba nenachází na defaultně určeném portu. V případě, že máme službu na webovém serveru (třída služby HTTP) s doménovým jménem serverexample.domain.test, bude SPN služby HTTP/serverexample.domain.test [23].

2.8 Single Sign-On

Ve firmách, využívajících větší množství systémů a služeb, je pro zaměstnance časově (v případě autentizace heslem i znalostně) náročné zadávat opakovaně přihlašovací údaje. Zaměstnanec v důsledku volí slabá hesla a snižuje tak úroveň zabezpečení svých účtů. Pro vyšší komfort i úroveň zabezpečení vznikl systém jednotného přihlášení, Single Sign-On (SSO). Ten umožňuje uživateli přístup k více službám a systémům na základě jediné autentizace, bez dalších požadavků na autentizaci [12].

SSO nesjednocuje přihlašovací údaje (identifikátory a ověřovací údaje) u všech účtů daného uživatele. Místo toho vytváří účet, který „zastřeší“ lokální účty a při přihlášení do tohoto účtu je může namapovat a zajistit autentizaci uživatele automaticky [11].

Elisa Bertino a Kenji Takahashi [11] rozeznávají 3 druhy SSO:

1) podnikové – fungující v rámci jednoho podniku

2) multidoménové – fungují v rámci několika podniků

3) webové – pro uživatele, komunikující přes prohlížeč s webovými aplikacemi.

Centralizace SSO bývá terčem kritiky, kvůli vyššímu rozsahu škod v případě úspěšného útoku na centrální prvek [9]. Zastánci SSO argumentují tvrzením, že uživatel se autentizuje méně často a nepotřebuje znát více než jednu sadu přihlašovacích údajů, proto má vyšší předpoklady pro zvolení silnějšího hesla [24].

Single sign-on technologie může být implementována v závislosti na různých typech architektur, přičemž SSO řešení může kombinovat prvky těchto architektur. Existuje několik typů architektur [12].

2.8.1 Broker-based architektura a protokol Kerberos

V broker-based architektuře existuje jeden server pro centrální autentizaci a správu uživatelských účtů. Tento „broker“ přiděluje uživatelům identity, které mohou být využity pro získání dalších přístupů [12].

Do tohoto typu architektury spadá protokol Kerberos, který je nejznámějším příkladem broker-based SSO architektury [12]. Tento protokol je integrován do služby Active Directory a je založen na existenci třetí strany – distribučního centra (Key Distribution Centre – KDC). Toto centrum má 2 části, fungující nezávisle na sobě – autentizační server

(Authentication server – AS) a server přidělující tickety (Ticket Granting Server – TGS) [24].

Základ procesu autentizace je následující [24]:

- Klient se přihlásí do počítače zadáním svých přihlašovacích údajů (identifikátor a ověřovací údaj – pro zjednodušení předpokládejme heslo).

- Klient si vytvoří tajný klíč aplikací hashovací funkce na své heslo, tento klíč nikam neodesílá, ponechává si jej u sebe.

- Klient odešle žádost na AS společně se svým identifikátorem. Zpráva není nijak zašifrována

- AS vyhledá podle doručeného identifikátoru ve svém adresářovém systému klientovy přihlašovací údaje, včetně hesla. Ty jsou v adresáři uloženy od první registrace klienta do systému. Pokud je klient zaregistrován a údaje jsou uloženy v adresáři, AS vytvoří klientův tajný klíč z hashe klientova hesla.

- AS pošle klientovi session key, zašifrovaný pomocí klientova tajného klíče, současně odešle Ticket-Granting Ticket (TGT), zašifrovaný vlastním klíčem, který klient nezná a nemůže tak tuto zprávu dešifrovat. Zpráva je totiž určena TGS a klient ji pouze přepošle (viz následující kroky).

- Klient dešifruje session key s pomocí svého tajného klíče. TGT nemůže dešifrovat.

- Klient pošle žádost o service ticket na TGS. Service ticket slouží k přístupu ke konkrétní službě. Klient odešle dvě zprávy – první obsahuje TGT, který zašifroval AS a ID služby. Druhá se skládá z uživatelova identifikátoru a časového razítka. Druhou zprávu klient zašifruje s pomocí session key, který obdržel od AS.

- TGS dešifruje zprávu, obsahující TGT. Ten obsahuje mimo jiné session key, které pro TGS nachystal AS. S pomocí tohoto klíče dešifruje druhou zprávu, kterou zašifroval uživatel. Je-li operace úspěšná, má TGS ověřenou identitu klienta, protože ví, že on i klient získal od AS stejný session key a byl schopen jej dešifrovat s pomocí svého hesla.

- TGS odešle odpověď, opět ve dvou zprávách. V první je nový session key, který tentokrát poslouží ke komunikaci klienta a serveru. Tato zpráva je zašifrována starým session key. Ve druhé zprávě odesílá service ticket a informace o klientovi, vše zašifrované tajným klíčem serveru. Klient tuto zprávu nemůže dešifrovat, bude ji pouze přeposílat.

- Klient dešifruje první zprávu s novým session key a použije jej k zašifrování zprávy, určené serveru. Tato zpráva bude obsahovat klientův identifikátor a časové razítko. Současně přepošle serveru i zašifrovaný service ticket, který obdržel od TGS.

- Server dešifruje service ticket, díky čemuž obdrží nový session key. S ním je schopen dešifrovat i klientův identifikátor a časové razítko. Tak ověří identitu uživatele stejným způsobem, jako ji ověřil TGS v bodě 8.

- Server se ještě musí autentizovat vůči klientovi, tudíž pošle klientovi zpět časové razítko, s hodnotou navýšenou o 1, zašifrované pomocí nového session key.

- Klient dešifruje časové razítko a porovná hodnoty. Pokud server byl schopen razítko dešifrovat, navýšit o 1 a opět zašifrovat, pak se u klienta odesláním razítka autentizoval, protože prokázal, že byl schopen dešifrovat zprávu od TGS, která byla zašifrována jeho tajným klíčem. V tomto okamžiku si obě strany věří a je navázána relace.

Výhodou této architektury je, že nikdy nedochází k přenosu hesla, s výjimkou registrace nového uživatele, kdy je potřeba heslo uložit do AD. Jako tajné klíče slouží hashe hesel, KDC jimi šifruje odeslané zprávy. Klient zadává heslo pouze lokálně. Další výhodou je

vzájemná autentizace komunikujících stran [24]. Broker-based architektura také velmi usnadňuje administraci – jedinou centrální databázi je jednodušší spravovat [12].

Centrální databáze je zároveň jednou z nevýhod systému. Útočník má v případě úspěšného proniknutí do databáze k dispozici všechny přihlašovací údaje. Další nevýhodou je nutnost přizpůsobení systémů, užívajících odlišné autentizační metody. Proces přizpůsobování těchto aplikací se nazývá kerberizace [12].

2.8.2 Agent-based architektura

Základem tohoto řešení je tzv. agent. Je to program, který může být použit jako nosič seznamu ověřovacích údajů. Tyto údaje pak užívá pro automatickou autentizaci uživatele. Agent také může působit jako prostředník mezi klientem a autentizačním systémem na serveru. V takovém případě je schopen plnit roli překladatele mezi koncovými uzly, užívajícími různé autentizační metody. Aplikace díky tomu není nutno přizpůsobovat [12].

Nevýhodou architektury je zvýšení nároků na administraci. Na rozdíl od broker-based architektury nejsou v agent-based architektuře údaje nijak centralizovány, proto je z administrativního pohledu potřeba řešit stejné množství prvků a k tomu navíc zabezpečení agenta, který může být zneužit, nebo nahrazen škodlivým software [12].

2.8.3 Agent a Broker-based architektura

Obě již zmíněné architektury mají své výhody i nevýhody. Broker-based usnadňuje administraci, ale nepodporuje různé metody autentizace. Agent-based je sice více flexibilní, ale decentralizovaný, správu nijak neusnadňuje. Proto vznikl návrh na jejich

sloučení do jedné hybridní architektury. Modely, řadící se do této architektury, staví na podobných základech, jako Kerberos, doplněných o agenta, který může být nainstalován na různých platformách [12].

2.8.4 Gateway-based architektura

V tomto řešení klient naváže spojení s tzv. branou (gateway), která funguje jako autentizační server. Uživatel se tak autentizuje ještě před vstupem do sítě. Brána ukládá do své paměti identity uživatelů a je schopna dohledat služby pomocí jejich IP adres. Může tak uživatelům po prvním přihlášení poskytovat veškeré služby dané sítě bez nutnosti opakované autentizace [12].

Jelikož brána kontroluje veškerý tok dat ke službám, může být využita i pro zaznamenávání těchto toků. Další výhodou je centralizace dat, podobně jako u broker-based architektury. Veškerá data o uživatelích jsou ukládána na autentizačním serveru [10]. Jelikož se ale brána nachází na pozici, kterou by měl zaujímat firewall, může být napadena DoS útoky, např. SYN-floodingem. Tento problém lze vyřešit ochranou brány samostatným firewallem [12].

3 Analýza současného stavu

V této kapitole analyzuji současný stav podniku a zmíním požadavky firmy.

3.1 O společnosti

V této kapitole se budu zabývat aktuálním stavem systému správy identit ve firmě. Společnost, kterou jsem oslovil, si nicméně nepřála být jmenována, proto ji budu dále označovat jako společnost ABC.

3.1.1 Základní informace

Společnost ABC působí na Českém trhu od roku 1992. Zabývá se vývojem, výrobou a distribucí ekonomických a právních informačních systémů a aplikací. Mezi poskytované služby patří aktualizace i servis zakoupených produktů. Sídlo společnosti se nachází v Ostravě.

Pro společnost v současné době pracuje přibližně 80 stálých zaměstnanců. Výhradním obchodním zastoupením firmy je její dceřiná společnost. Ta má své pobočky umístěny v Praze, Brně a v Ostravě. Tržby dceřiné společnosti se pohybují v řádu desítek milionů Kč ročně.

3.1.2 Organizační struktura

Společnost ABC má funkční organizační strukturu a je rozdělena na 4 základní části – divizi informačních systémů, divizi ekonomicko-personální, administrativní budovu ABC a samostatně je vyčleněn i manažer kvality, Organizační strukturu společnosti ABC přikládám do přílohy 2.

3.1.3 Certifikace, ocenění

Společnost ABC se zavázala vytvořit, udržovat a zlepšovat systém managementu kvality dle normy ČSN EN ISO 9001:2001 s účinností od 31.10.2007 pro hlavní obor své činnosti vývoj, příprava a distribuce právních a ekonomických informačních systémů a aplikací. Společnost úspěšně prošla všemi recertifikacemi a pravidelným externím dozorovým auditem, naposled realizovaným v roce 2016.

Za dobu svého působení na Českém trhu se společnost zatím nesnažila získat žádnou certifikaci v oblasti informační bezpečnosti.

3.2 Autentizace

Ve společnosti jsou zaměstnanci autentizování dvěma různými způsoby.

3.2.1 Fyzický přístup

Každý zaměstnanec se autentizuje s pomocí čipu, a to jak při vstupu do budovy, tak při vstupu na patro. Zaměstnancům je povolován přístup pouze na ta patra, ve kterých vykonávají svou běžnou pracovní činnost. Většina zaměstnanců tak má přístup pouze do jednoho z pater 2-4. Výjimku tvoří IT podpora a většina manažerů. Další výjimky jsou možné, ale pouze po schválení příslušného nadřízeného. První patro (resp. přízemí) je přístupné všem, s výjimkou několika místností.

V případě ztráty nebo zcizení čipu, musí zaměstnanec tento problém nahlásit na recepci, aby došlo k zablokování tokenu. Zaměstnanec pak obdrží dočasný čip, než mu bude

vydán nový. Svoji identitu musí na recepci prokázat předložením platného dokladu, nejčastěji občanského průkazu, aby mohl čip obdržet.

3.2.2 Přístup k aplikacím

Pro přístup ke klientským stanicím a k aplikacím se zaměstnanci autentizují s pomocí uživatelského jména a hesla. V pracovních postupech firmy je stanoveno, že heslo pro přihlášení do klientských stanic musí mít alespoň 8 znaků a musí obsahovat alespoň jednu číslici a velké písmeno. Síla hesel, sloužících k přístupu k aplikacím ale není pracovními postupy nijak řešena. Stejně tak neexistuje pro zaměstnance povinnost pravidelně si měnit kterékoli z hesel.

3.3 Adresářové služby

Společnost používá Active Directory Domain Services na starší platformě Windows Server 2003. Zařízení jsou součástí domény abc.cz (název domény obsahuje jméno firmy). Má k dispozici servery s nainstalovaným systémem Windows Server 2008, které plánuje využít pro vytvoření nové domény. Plány struktury nové domény má společnost vypracované.

3.4 Řízení přístupů

Tato podkapitola se věnuje systémům řízení přístupů ve firmě.

3.4.1 Single Sign-On

Do služby AD DS je integrován protokol Kerberos, společnost ale nemá všechna zařízení přizpůsobena k jeho používání.

3.4.2 Řízení přístupů na základě rolí – RBAC

Přístupy do aplikací a systémů jsou řízeny na základě rolí. Pro usnadnění přidělování rolí slouží CSO – Centrální Správa Oprávnění. Jde o systém, který obsahuje údaje o všech zaměstnancích, a v němž nadřízení podávají zaměstnancům žádosti o přidělení oprávnění pro příslušné aplikace a oblasti. Veškerá jména zaměstnanců jsou převáděna z informačního systému Helios.

V případě jakékoli změny v oprávněních je automaticky generován e-mail, který je odeslán správcům aplikací. Ti provedou změny a potvrdí jejich realizaci. Potvrzovací e-mail je následně opět poslán automaticky. Tím je žadatel o provedení okamžitě informován [26].

Každá pozice ve firmě má standardní sadu oprávnění, která jsou v systému vybrána automaticky. Tato oprávnění jsou označena modře, pro snazší orientaci v případě úprav jednotlivých účtů. Další, rozšířená oprávnění, která jsou pro danou pozici dostupná a počítá se s případnou potřebou jejich přidělení, jsou značena zeleně. Tato oprávnění nejsou přidělována automaticky, ale může je zaměstnanci přidělit jeho nadřízený [26].

Potřebuje-li zaměstnanec speciální oprávnění nad rámec předdefinované i rozšířené sady, které byly jeho roli určeny, musí nadřízený tohoto zaměstnance nejprve kontaktovat vlastního nadřízeného a požádat jej o schválení a předání informací HR oddělení. Až poté jsou generovány e-maily správcům aplikací. V databázi jsou tato oprávnění značena černě [26].

3.5 Provisioning

Propisování informací o uživatelích do jejich účtů je pro většinu systémů prováděno automaticky. Mezi výjimky patří např. intranet.

Změny poprvé do systému zaznamená personalistka v systému Helios, odkud se, většinou s pomocí SQL skriptů, informace dále propisují do dalších systému, včetně C.S.O.

SQL skript pro přenos aktualizovaných informací ze systému Helios do C.S.O. je automaticky spouštěn v pravidelných intervalech. Propisovány jsou všechny informace, s výjimkou oprávnění, která jsou přidělována ručně. Pro zvýšení přehlednosti systému C.S.O. je automaticky označována standardní a rozšířená sada oprávnění pro daného uživatele podle šablony. Za definici šablon je odpovědná personalistka. Podrobnější informace o fungování systému lze najít v příloze 3.

3.6 Požadavky firmy

Společnost plánuje na volném serveru vybudovat novou doménu, na kterou po jejím vytvoření přejdou všechna zařízení ve firmě – klientské stanice i servery. Společnost dále potřebuje navrhnout nový systém jednotného přihlášení a zajistit jeho funkčnost.

V souvislosti se zavedením SSO pak je potřeba také upravit pracovní postupy společnosti (pracovní řád), aby ze strany zaměstnanců nedocházelo k zanedbávání zabezpečení nového systému.

3.7 Shrnutí

Situaci ve společnosti vnímám velmi znepokojivě. Společnost se sice snaží plnit podmínky normy ČSN EN ISO 9001, o certifikace z oblasti informační bezpečnosti ale nejeví zájem. Velký problém ale vidím především v chybějících pracovních postupech, týkajících se volby hesel do aplikací a jejich pravidelné obměny. Zaměstnanci mohou zvolit libovolné heslo do jakékoli aplikace, díky čemuž pravděpodobně většina užívá pro všechny aplikace stejné heslo, případně malé množství jednoduchých hesel.

Zmíněný problém souvisí s dalším – nevyužívání SSO. S tímto systémem by každému zaměstnanci stačilo zapamatovat si jediné silné heslo pro přístup ke všem aplikacím a službám v doméně. Bez tohoto systému je v podstatě nemožné zajistit, aby každý zaměstnanec užíval silná hesla pro každý svůj účet, protože pouhé zavedení pravidel pro minimální sílu všech hesel by vedlo k jejich častému zapomínání, což by vedlo k zahlcení IT oddělení žádostmi o resetování hesel.

Pozitivně hodnotím C. S. O., nicméně pouze ze strany manažera, nikoli správce aplikací. Tomu systém nepřináší téměř žádné usnadnění práce, správce musí oprávnění stále zadávat ručně. C. S. O. pouze šetří čas manažera automatickým odesíláním e-mailů v případě, že manažer v systému provede změny.

4 Návrh řešení

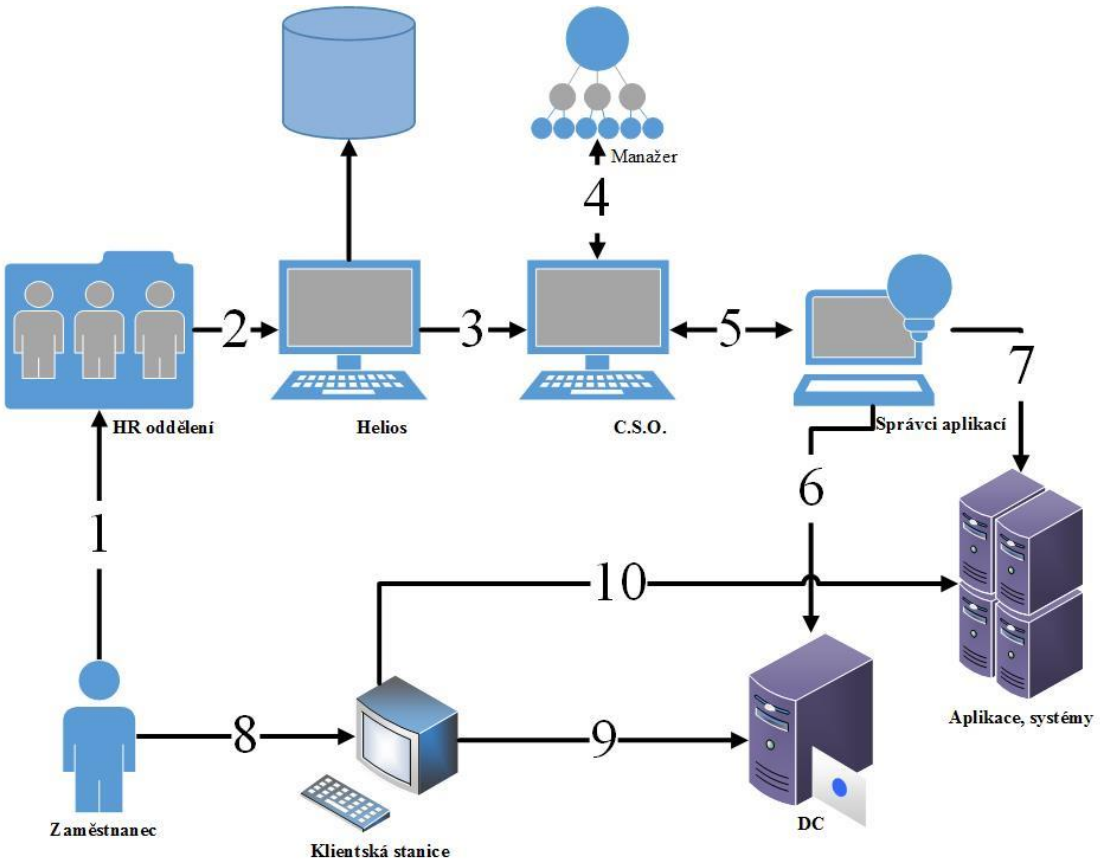
V této kapitole představím svůj návrh na vylepšení systému správy identit ve firmě ABC. V první části navrhnu podobu systému ve firmě a rozeberu role a odpovědnosti. Dále vyberu vhodný systém SSO a určím postup jeho implementace. Na závěr navrhnu změny v pracovních postupech firmy, v oblasti politiky hesel.

4.1 Návrh systému správy identit

Pro sestavení systému správy identit je potřeba navrhnout schéma systému, včetně popisu procesů probíhajících mezi jednotlivými prvky. Dále je potřeba přiřadit role a odpovědnosti zaměstnancům, kteří budou mít na starost správu jednotlivých systémů.

4.1.1 Schéma procesů systému správy identit

Fungování systému ve společnosti popíši s pomocí následujícího schématu:

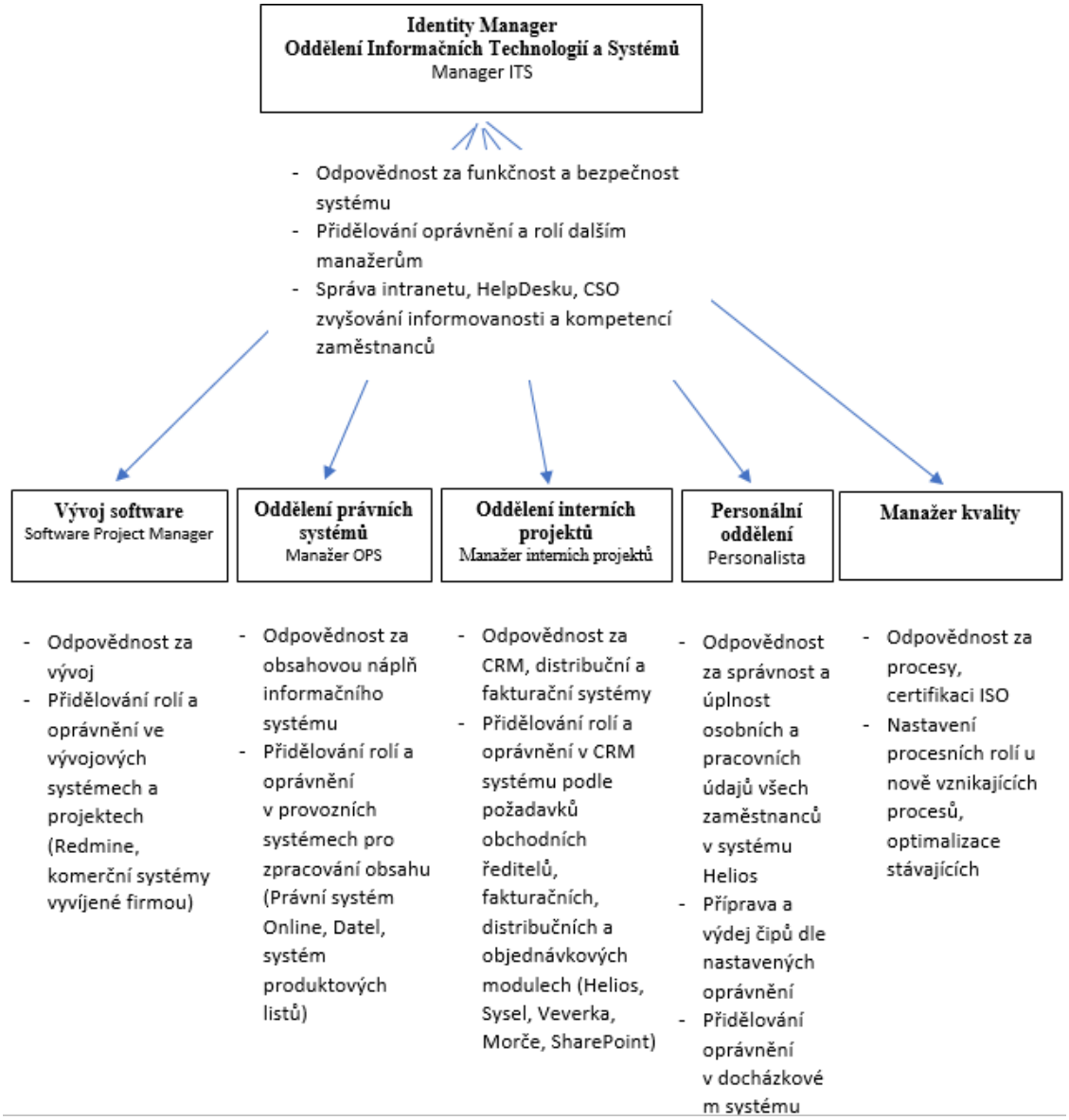


Obr. 3: Schéma průběhu základních procesů IdM ve společnosti [vlastní zpracování]

Krok 1 v této podobě platí v případě, že zaměstnanec nastupuje do firmy. V takovém případě předá HR oddělení své údaje. V případě změny údajů zaměstnance nebo jejich odebrání ze systému předává v kroku 1 informace manažer. HR oddělení nové údaje navede do systému Helios (2). Z něj se informace s pomocí společností zavedených skriptů převedou do C.S.O. (3). V kroku 4 dojde k e-mailové notifikaci příslušného nadřízeného a v případě přidělení nových práv je příslušný nadřízený upozorněn, že má přidělení schválit (v takovém případě začne krok 5 až po schválení nadřízeného). Následně je zaslán e-mail správcům aplikací o provedení patřičných změn v aplikacích a systémech (5). Ti změny provedou v krocích 6 a 7. V tuto chvíli jsou změny provedeny a zaměstnanec při dalším přihlášení do počítače (8) se může autentizovat vůči DC (9, v případě, že je to potřeba) a díky nově zavedenému systému SSO stanice zajistí autentizaci uživatele vůči požadovaným systémům a aplikacím (10), vše s novými údaji. V případě odebrání práv zaměstnanec v procesu nefiguruje a kroky 8-10 neprobíhají, resp. zaměstnanec v danou chvíli nemá přístup.

4.1.2 Role a odpovědnosti v rámci systému

V současném organizačním schématu je potřeba vyčlenit pravomoci a odpovědnosti za prvky systému správy identit a přístupů. Jako vhodné se jeví toto nastavení:



Obr. 4: Role a odpovědnosti v oblasti IdM [vlastní zpracování]

4.1.3 Návrh dokumentu

Společnost má své závazné postupy kodifikované v systému Pracovních postupů, které je každý zaměstnanec povinen prostudovat a potvrdit seznámení s nimi. Proto považuji za vhodné zanést i jednotlivé povinnosti, lhůty a odpovědnosti v systému správy identit do nového Pracovního postupu, a to v následující podobě:

SYSTÉM SPRÁVY IDENTIT

- Systém správy identit zaměstnanců přináší vyšší zabezpečení firemních systémů, zjednodušuje práci zaměstnanců a definuje jednoznačné povinnosti, lhůty a odpovědnosti v přidělování a správě oprávnění a přístupů do aplikací jednotlivým zaměstnancům.

ÚČASTNÍCI PROCESU

- Proces správy identit má následující účastníky:
    - Zaměstnanec
    - Personalista
    - Manažer ITS
    - Manažer interních projektů
    - Manažer kvality
    - Manažer oddělení právních systémů
    - Všichni další manažeři s podřízenými zaměstnanci
    - Správci aplikací

ROLE A ODPOVĚDNOST ÚČASTNÍKŮ PROCESU

Zaměstnanec

- Při nástupu do zaměstnání uvede správné a úplné osobní údaje
- Při nastavení či změně hesla postupuje dle nastavené firemní politiky hesel
- Je povinen nakládat se svým heslem dle zásad bezpečnosti, tak, aby nedošlo k jeho prozrazení
- V případě prozrazení hesla nebo podezření na neoprávněný přístup neprodleně změnit heslo a informovat manažera ITS
- Je povinen oznámit zaměstnavateli jakékoliv změny v osobních údajích, zadaných při vytváření jeho identity

Personalista

- Odpovídá za zadání správných a úplných údajů každého zaměstnance do systému Helios při nástupu a zadání změn v průběhu životního cyklu zaměstnance.
- Přiděluje, schvaluje a odebírá oprávnění pro náhled na jednotlivce/tým/oddělení v docházkovém systému, oprávnění pro editaci, údržbu výjimek v docházce
- Ruší identitu zaměstnance při jeho odchodu z firmy
- Přeřazuje zaměstnance při přechodu na jinou pozici, změně kompetencí apod.

Manažer ITS

- Odpovídá za funkčnost a bezpečnost celého systému správy firemních identit
- Přiděluje, schvaluje a odebírá role a oprávnění dalším manažerům s podřízenými zaměstnanci

- Odpovídá za informovanost zaměstnanců o pravidlech bezpečnosti a nakládání s hesly

- V rámci své gesce za tým ITS přiděluje, schvaluje a odebírá oprávnění a přístupy ve spravovaných aplikacích (Intranet, HelpDesk, CSO)

- V případě nečinnosti či nepřítomnosti některého z účastníků procesu má oprávnění vstoupit do kterékoliv části procesu a rozhodnout o dalším postupu (přesměrování na delegovaného zástupce, nadřízeného nekonajícího zaměstnance, sám rozhodnout o oprávnění)

Manažer interních projektů

- Odpovídá za přidělování, schvalování a odebírání oprávnění v CRM systémech, definovaných obchodními řediteli

- Odpovídá za přidělování, schvalování a odebírání přístupů a oprávnění pro fakturační, distribuční a objednávkové systémy

- Odpovídá za přidělování, schvalování a odebírání přístupů v systému Share Point

Manažer kvality

- Odpovídá za procesní mapy, popis realizovaných procesů a přidělených rolí

- V případě vzniku nového procesu vytváří ve spolupráci s jeho vlastníkem popis, mapu, definice a nastavení rolí v procesu, včetně potřebných aplikací a přístupů do nich.

Manažer oddělení právních systémů

- Odpovídá za přidělování, schvalování a odebírání přístupů v provozních systémech pro zpracování obsahu (Právní systém online, Datel, systém produktových listů)

Manažer s podřízenými zaměstnanci

- Ve spolupráci se správci aplikací odpovídá za definice rolí, pozic a oprávnění pro podřízené zaměstnance a jejich zařazování do tohoto systému

- V případě vytvoření nové pozice iniciuje definici rolí a oprávnění pro tuto pozici

- Neprodleně, nejpozději do 3 dnů, schvaluje oprávnění pro podřízené zaměstnance na základě e-mailové notifikace

- Pro případy, kdy nemůže sám schválit potřebná oprávnění, deleguje svého zástupce, který po přesměrování IT managerem příslušnou žádost ve stejné lhůtě schválí či zamítne

- Potvrzuje personalistovi odebrání identity odcházejícího zaměstnance či změnu při přechodu do jiné role (zaměstnanec x externista apod.).

Správce aplikace

- Ve spolupráci s liniovými manažery se podílí na definici rolí, pozic a oprávnění ve spravovaném systému a zařazování zaměstnanců do tohoto systému

- Neprodleně, nejpozději do 24 hodin, realizuje nastavení přístupů do spravované aplikace na základě notifikace o schválení definovaného přístupu ze strany nadřízeného manažera

- Pro realizaci požadavků na přístupy do svěřené aplikace v případě své nepřítomnosti deleguje svého zástupce.

NEDODRŽENÍ ZÁSAD A POVINNOSTÍ STANOVENÝCH TÍMTO PP

- V případě nečinnosti příslušného zaměstnance v daných lhůtách oznamuje tuto skutečnost Manažer ITS nadřízenému tohoto zaměstnance a v případě urgentních záležitostí, nebezpečí z prodlení vstupuje do procesu s oprávněním nekonajícího zaměstnance

- Porušení zásad bezpečného nakládání s hesly ohrožuje firemní data a systémy a bude považováno za závažné porušení povinnosti vyplývající z právních předpisů vztahujících se k zaměstnancem vykonávané práci dle §52 písm.g) Zákona č. 262/2006 Sb., Zákoník práce, se všemi z toho vyplývajícími důsledky.

Vypracovaný dokument je také možné najít v příloze č. 4

4.2 Výběr modelu SSO

Společnost má k dispozici řešení v podobě protokolu Kerberos. Zaměstnanci IT oddělení jsou dobře obeznámeni s fungováním tohoto protokolu a mohou být využiti pro jeho implementaci i správu bez nutnosti zaškolení. Na trhu ale existuje více druhů SSO a některé jsou schopny nabídnout více funkcí oproti protokolu Kerberos. V této podkapitole uvedu a zhodnotím použitelnost nejvýznamnějších konkurentů na trhu.

4.2.1 SESAME

Jedním z hlavních konkurentů protokolu Kerberos na evropském trhu je SESAME. Název je zkratkou pro „The Secure European System and Applications in a Multivendor Environment" [28].

Cílem vývoje SESAME bylo pokrýt slabá místa Kerberos. Tvůrci se zaměřili především na kontrolu oprávnění, pro která má SESAME vlastní databázi, a pro které vydává Autentizační Server (AS) vlastní certifikát (obdoba ticketu v Kerberos) [28].

Dalším vylepšením je užití asymetrické kryptografie pro distribuci klíčů a pro zvýšení bezpečnosti využívá hashovací funkce [28].

4.2.2 IBM KryptoKnight

KryptoKnight od firmy IBM je dalším řešením vycházejícím z modelu Kerberos. Proces získávání ticketu zůstává stejný, následná komunikace probíhá odlišně Zatímco v Kerberos komunikuje s AS pouze klient, v KrptoKnight využívají obě strany (KryptoKnight místo klienta a serveru využívá pojmy iniciátor a respondent) aplikačního rozhraní (API) k ověření údajů, zasílaných protistranou a pro získání tajného klíče pro šifrovanou komunikaci. KryptoKnight používá také odlišné metody šifrování, užívá rozdílné algoritmy a liší se i zprávy, zasílané iniciátorovi a respondentovi [29].

Za jednu z výhod protokolu KryptoKnight je považována kompaktnost zpráv, zasílaných v rámci SSO, včetně možnosti rozdělení zprávy na menší části a optimalizovat tím tok dat. KryptoKnight také může přidělit iniciátorovi i respondentovi stejná oprávnění v rámci SSO, není tedy pevně postaven na modelu klient-server. To může být výhodou v případě, že je potřeba zacházet s některou z entit oběma způsoby, každým v jiné situaci [29].

4.2.3 Zhodnocení

Přestože SESAME a KryptoKnight jsou vylepšenými verzemi modelu Kerberos a snaží se řešit některé nedostatky tohoto systému, nepovažuji je za vhodné pro zavedení do této firmy. V tabulce jsou shrnuty vlastnosti jednotlivých řešení.

	Kerberos	SESAME	KryptoKnight
Základní požadavky firmy			
Kompatibilita	•••	••	•
Vícefaktorová autentizace	•	•	•
Další vlastnosti			
Šifrování komunikace	•	••	•
Objem datových toků*	•	•	••
Uživatelské rozhraní	••	•	
Podpora aplikací	••	•	•
Cena projektu	•••	•	•
Znalosti zaměstnanců	•••		
Celkové hodnocení	••	•	•
**vyšší hodnocení = nižší zatížení sítě*			

Tabulka 1: Porovnání řešení SSO [vlastní zpracování]

Většina vylepšení KryptoKnightu i SESAME dává firmě oproti protokolu Kerberos jen minimální, nebo žádnou přidanou hodnotu. Za jedinou výraznější výhodu lze považovat vyšší kvalitu šifrování u SESAME. Co se týče výhody KryptoKnightu, každá entita ve společnosti má již nyní určenou svoji roli (klient, server) a není potřeba některé z nich roli měnit pro různé druhy komunikace.

Přestože řešení nejsou určena výhradně pro specifický OS ani stanici a jejich implementace na Windows Server by tedy byly možné (i když minimálně v případě KryptoKnight nevhodné), je zkušenost zaměstnanců s oběma protokoly prakticky nulová. I to je důvodem, proč by se celý projekt ve výsledku prodražil příliš na to, aby jeho zavedení a provoz byl dlouhodobě výhodnější oproti implementaci protokolu Kerberos.

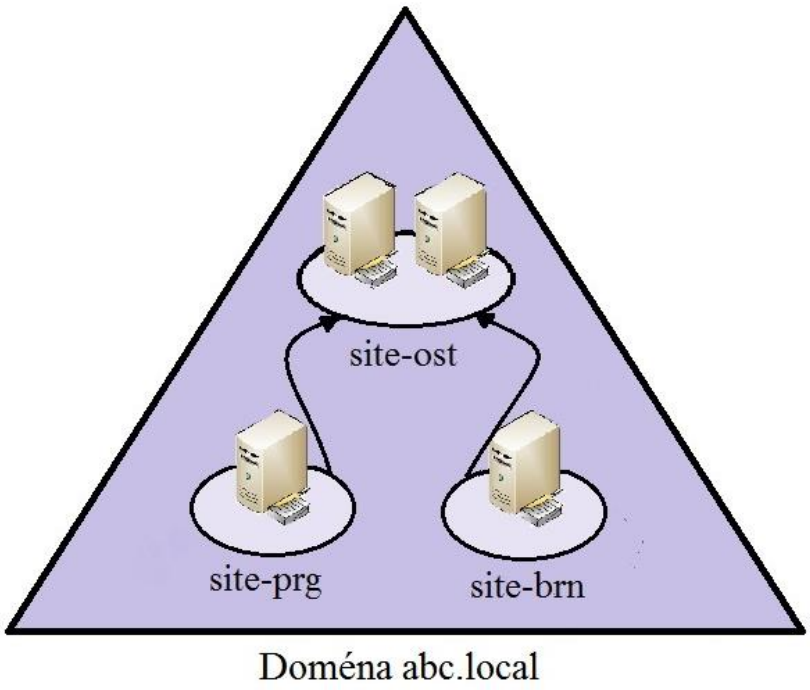
4.3 Návrh domény Active Directory

V následující podkapitole navrhnu základní strukturu nové domény, která bude zaváděna do společnosti ABC.

4.3.1 Struktura a jméno domény

Vzhledem k relativně nízkému počtu zaměstnanců a tím i počtu používaných zařízení bude prostředí společnosti tvořeno jedinou doménou abc.local, spravovanou 4 doménovými řadiči ve 3 lokalitách. Přípona local byla zvolena z důvodů oddělení interní domény.

Největší lokalita site-ost bude spravována 2 DC, zbylé lokality budou mít po jednom. Řadiče umístěné v lokalitě site-ost, budou hlavními DC.



Obr. 5: Struktura domény abc.local [vlastní zpracování]

4.3.2 Globální katalog

Funkce GC bude aktivována na všech řadičích při jejich instalaci do domény.

4.3.3 Pravidla pro pojmenování objektů

Pro jednodušší vyhledávání objektů v rámci domény je vhodné stanovit si pravidla pro pojmenování těchto objektů.

Objekt	**Šablona pro jméno**	**Max. počet znaků**
Uživatel	Příjmení uživatele + první 2 písmena jména uživatele	9 + 2
Počítač	Příjmení uživatele + první 2 písmena jména uživatele + pořadové číslo přiřazeného zařízení danému uživateli	9 + 2 + 1
Lokalita	″Site″ +″-″ + zkratka lokace	4 + 1 + 3
Server	Zkratka lokace serveru +″-″ + zkratka funkce serveru + pořadové číslo	3 + 1 + 4 + 2

Tabulka 2: Návrh pravidel pro pojmenování objektů [vlastní zpracování]

4.4 Implementace protokolu Kerberos

V této podkapitole rozeberu jednotlivé části procesu implementace protokolu Kerberos

4.4.1 Instalace Active Directory Domain Services a vytvoření domény

Společnost má k dispozici servery s nainstalovaným systémem Windows Server 2008 R2 Enterprise. Pro zajištění plného fungování systému jednotného přihlášení bude potřeba na servery nainstalovat Active Directory Domain Services (AD DS). Ke spuštění průvodce slouží příkaz dcpromo.exe. V něm bude vytvořena nová doména abc.local. Další informace o procesu instalace přikládám do přílohy 5.

Po provedení instalace je vytvořena nová doména a server se stává prvním DC v rámci této domény.

Pro instalaci AD DS je potřeba v síťovém prostředí mít dostupnou službu DNS. Jelikož společnost v tuto chvíli službu dostupnou nemá, její instalace bude provedena přímo na DC. V takovém případě je instalace DNS možná v rámci instalačního průvodce pro AD DS.

Přidání dalších DC proběhne podobným způsobem. Podrobný popis lze najít v příloze 5.

4.4.2 Vytvoření účtů a přidání zařízení do domény

Všechna zařízení, která budou protokol Kerberos využívat, musí být součástí domény. Před jejich samotným přidáním je potřeba vytvořit v rámci domény uživatelské účty, skupiny a organizační jednotky. Vytvořeny budou na serveru v Active Directory Users and Computers. Podrobně je proces rozebrán v příloze 6

Následně budou zařízení přidána do domény. Přidání bude provedeno přímo na zařízeních. Podrobný postup pro vytvoření účtů i přidání zařízení do domény je obsahem přílohy 7.

4.4.3 Vytvoření keytab souboru

Keytab soubor slouží pro zajištění šifrované komunikace mimo doménu. Pro vytvoření souboru lze využít řádkový příkaz ktpass. Toto je návrh šablony pro vytvoření souboru:

C:>ktpass –princ principalname -ptype KRB5_NT_PRINCIPAL -mapOp set –mapuser userexample –pass passexample –out userexample.keytab

Popis jednotlivých parametrů lze najít v příloze 8.

4.4.4 Konfigurace prohlížečů

Na závěr je potřeba nakonfigurovat prohlížeče na klientských stanicích.

Internet Explorer povoluje autentizaci pouze na adresy, které jsou součástí lokálního intranetu. Není ale schopen adresy sám rozeznat – jakákoli adresa, obsahující tečku, je v IE považována za internetovou. Proto je potřeba přidat lokální adresy ručně. V našem případě bude do Internet Options zadáno *.abc.local pro povolení autentizace v rámci celé domény. ***** je zástupný znak pro libovolné množství znaků.

Změny v nastavení IE se následně projeví i v Google Chrome, je-li nainstalován. Pro tento prohlížeč proto platí stejný postup

Prohlížeč Mozilla Firefox je defaultně nastaven na podporu protokolu Kerberos, ale stejně jako v IE je potřeba zadat adresy, pro které bude protokol využíván.

Podrobný postup konfigurace prohlížečů lze najít v příloze 9.

4.5 Návrh změn pracovního řádu

Zavedení systému jednotného přihlášení je založeno na použití jednoho hesla pro všechny doménové služby. Z tohoto důvodu by mělo být pro firmu prioritou přimět zaměstnance, aby kvalita jejich jediné formy zabezpečení byla co nejvyšší. V současných pracovních postupech firmy stojí, že:

„Heslo musí mít alespoň 8 znaků a musí obsahoval alespoň jedno malé a velké písmeno a alespoň jednu číslici“ [30].

Při použití velkých i malých písmen základní abecedy + číslic lze při výběru hesla počítat s 62 znaky. Při síle 8 znaků to znamená 62^8 (cca 10^{14}) možností. Takové heslo lze považovat za silné. Pokud by společnost chtěla zajistit solidní ochranu před v současné době nejmodernějšími metodami lámání hesel, které jsou schopny vyzkoušet až 180 miliard kombinací za vteřinu [31], doporučuji zvýšit povinný minimální počet znaků na 10.

4.5.1 Nastavení zásad skupin

Pro zajištění dodržování nových pracovních postupů je vhodné nastavit novou politiku hesel do zásad skupin. Nové hodnoty budou nastaveny následovně:

Minimum password length	10 characters
Password must meet complexity requirements	**Enabled**

Tabulka 3: Nastavení zásad skupin – hesla [vlastní zpracování]

4.6 Ekonomické zhodnocení

Společnost pro zavedení nové domény využívá vlastních zdrojů. Nenese tedy žádné náklady na pořízení potřebného hardware, ani licencí. Stejně tak nebude potřeba školit zaměstnance, jelikož jsou s fungováním AD DS obeznámeni velmi dobře. Uvedení nové domény do plného provozu a přizpůsobení prostředí protokolu Kerberos ale jsou časově náročnými operacemi. Zvláště přizpůsobování prostředí nemusí být zcela úspěšné napoprvé. Společnost musí z tohoto důvodu počítat s patřičným finančním ohodnocením zaměstnanců, kteří budou na projektu pracovat, viz následující tabulka

Činnost	**Doba (č-h)**	**Sazba (Kč/č-h)**	**Hrubá mzda (Kč)**	**Odvody (zdr.+soc.) (Kč)**	**Celkové náklady (Kč)**
vybudování nové domény	24	200	4 800	1 632	6 432
konfigurace serverů	24	200	4 800	1 632	6 432
test komunikace	40	100	4 000	DPP	4 000
přesun uživatelů do nové domény	80	200	16 000	5 440	21 440
nastavení zásad skupin	4	100	400	DPP	400
test funkčnosti protokolu Kerberos	40	100	4 000	DPP	4 000
konfigurace klientských stanic pro použití protokolu Kerberos	80	200	16 000	5 440	21 440
Celkem	292		50 000	14 144	64 144

Tabulka 4: Ekonomické zhodnocení [vlastní zpracování]

Vzhledem k ziskům firmy bych z krátkodobého hlediska tyto náklady ale neviděl jako výrazný problém. Z dlouhodobého hlediska vidím tuto investici jako velmi výhodnou, protože přísnější politika hesel v kombinaci s SSO může v budoucnu předejít vzniku nákladných bezpečnostních incidentů.

ZÁVĚR

Cílem této bakalářské práce bylo navrhnout novou podobu správy identit ve společnosti ABC tak, aby došlo ke zvýšení bezpečnosti, případně zjednodušení některých procesů ve společnosti. Na základě analýzy současného stavu byla nalezena slabina v zabezpečení společnosti v její politice hesel a absenci systému SSO.

V praktické části byla nejprve vypracována struktura systému správy identit v jeho nové podobě a byly přiděleny oprávnění a odpovědnost příslušným zaměstnancům. Na základě plánů společnosti byl dále vytvořen návrh struktury nové domény. Díky návrhu na změnu pracovního řádu společnosti dojde k výraznému zvýšení zabezpečení v oblasti politiky hesel. Přísnější pravidla ale zvyšují nároky na zaměstnance. Tento problém řeší přizpůsobení prostředí Active Directory použití protokolu Kerberos, což zjednoduší procesu autentizace. Kombinace využití SSO a přísnější politiky hesel tak zvyšuje úroveň zabezpečení při stejném, nebo jednodušším (v závislosti na dosavadní volbě hesel jednotlivých zaměstnanců) procesu autentizace.

Náklady na zavedení nové domény a přizpůsobení prostředí jsou velmi nízké, především díky tomu, že společnost již vlastní potřebné prostředky pro nové řešení. Problém vidím ve využití dnes již relativně zastaralého OS Windows Server 2008 R2 Enterprise na doménových řadičích. I když je zde zlepšení oproti původnímu Windows Server 2003, stále tento systém postrádá některé funkce svých nástupců, nebo je není schopen poskytovat na stejné úrovni (např. omezená podpora Windows Defender, nástroje pro správu serverů apod.). V budoucnu bych doporučoval nešetřit na nákladech a při dalším vylepšení systému zavést server s nejnovější verzí OS Windows Server (momentálně Windows Server 2016).

SEZNAM POUŽITÝCH ZDROJŮ

[1] ISO/IEC 27001 - Information security management. *ISO – International Organization for Standardization* [online]. Geneva: International Organization for Standardization, 2014 [cit. 2017-01-17]. Dostupné z: http://www.iso.org/iso/iso27001

[2] *RAC – Řada norem ISO/IEC 27000* [online]. Praha: Risk Analysis Consultants, 2016 [cit. 2017-01-18]. Dostupné z: http://www.iso27000.cz/

[3] BISHOP, Matt. *Computer security: art and science*. Boston: Addison-Wesley, c2003. ISBN 02-014-4099-7.

[4] *NGN Identity Management Framework: Recommendation Y.2720*. Paris: International Telecommunication Union, 2009.

[5] STAMP, Mark. *Information security principles and practice* [online]. Hoboken, N.J: Wiley-Interscience, 2005, s. 153-176 [cit. cit. 2016-10-5]. ISBN 9780471744191. Dostupné z: http://onlinelibrary.wiley.com.ezproxy.lib.vutbr.cz/doi/10.1002/0471744190.ch7/pdf

[6] KRHOVJÁK, Jan a Václav MATYÁŠ. Autentizace a identifikace uživatelů. *Zpravodaj ÚVT MU: bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě* [online]. Brno: Masarykova univerzita, 2011, **XVIII**(1) [cit. cit. 2016-10-5]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/560.html#lit1

[7] Jak je na tom Vaše heslo? ÚSTAV VÝPOČETNÍ TECHNIKY MU. *CSIRT-MU* [online]. 2014 [cit. 2016-10-6]. Dostupné z: https://security.ics.muni.cz/18-Jak-je-na-tom-vase-heslo

[8] Most common passwords list. *Passwordrandom* [online]. Nikolaev: Koshevoy, 2016 [cit. 2016-10-8]. Dostupné z: http://www.passwordrandom.com/most-popular-passwords

[9] BONNEAU, Joseph, Cormac HERLEY, Frank STAJANO, Paul C. VAN OORSCHOT. *The quest to replace passwords: a framework for comparative evaluation of Web authentication schemes*. Cambridge, 2012. Dostupné také z: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf. Technical report. University of Cambridge, Computer Laboratory.

[10] Biometrika: Basics of fingerprint recognition technology and biometric systems. BIOMETRIKA S.R.L. *Biometrika* [online]. 2012, 2015 [cit. 2016-11-17]. Dostupné z: http://www.biometrika.it/eng/wp_biointro.html

[11] BERTINO, Elisa a Kenji TAKAHASHI. *Identity management: concepts, technologies, and systems*. Boston: Artech House, 2011. Artech House information security and privacy series. ISBN 16-080-7039-5.

[12] HURSTI, Jani. *Single Sign-On* [online]. Helsinki, 1997 [cit. 2016-11-24]. Dostupné z: http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/single_sign-on.html. Helsinki University of Technology, Department of Computer Science.

[13] BALÁŽIK, Milan. Principy řízení identit. *IT SYSTEMS* [online]. 2015, (1-2) [cit. 2016-11-5]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/it-security/principy-rizeni-identit.htm

[14] LÍZNER, Martin. Identity management: centrální správa uživatelských účtů. *Computerworld* [online]. Praha, 2010 [cit. 2016-11-26]. Dostupné z: http://computerworld.cz/securityworld/identity-management-centralni-spravauzivatelskych-uctu-47568

[15] SEMANČÍK, Radovan a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (1. díl): Základy správy identit a přístupů. *IT SYSTEMS* [online]. 2015, (1-2) [cit. 2016-11-20]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-identity-managementu-1-dil.htm

[16] SEMANČÍK, Radovan a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (2. díl): Adresářové systémy. *IT SYSTEMS* [online]. 2015, (3) [cit. 2016-11-12]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-identity-managementu-2-dil.htm

[17] BOUŠKA, Petr. Adresářové služby a LDAP. *www.samuraj-cz.com* [online]. 2010 [cit. 2016-11-20]. Dostupné z: http://www.samuraj-cz.com/clanek/adresarove-sluzby-a-ldap/

[18] SEMANČÍK, Radovan, Katarína VALALIKOVÁ a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (4. díl): Řízení přístupů. *IT SYSTEMS* [online]. 2015, (3) [cit. 2016-11-26]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/it-security/cesta-k-efektivnimu-identity-managementu.htm

[19] NORIS, Ivan a Stanislav GRÜNFELD. Cesta k efektivnímu identity managementu (4. díl): Provisioning. *IT SYSTEMS* [online]. 2015, (5) [cit. 2016-11-27]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-idm-provisioning.htm

[20] BOUŠKA, Petr. Active Directory komponenty – domain, tree, forest, site. *www.samuraj-cz.com* [online]. 2008 [cit. 2017-05-10]. Dostupné z: http://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/

[21] BOUŠKA, Petr. *Kerberos část 1: Active Directory komponenty* [online]. 2014, (1) [cit. 2017-05-21]. Dostupné z: http://www.samuraj-cz.com/clanek/kerberos-cast-1-active-directory-komponenty/

[22] Principy skupin. *Microsoft Technet: Windows Server* [online]. Microsoft, 2009 [cit. 2017-05-21]. Dostupné z: https://technet.microsoft.com/cs-cz/library/dd861330(v=ws.11).aspx

[23] BOUŠKA, Petr. *Kerberos část 2: AD uživatelské účty a Service Principal Name* [online]. 2014, (2) [cit. 2017-05-21]. Dostupné z: http://www.samuraj-cz.com/clanek/kerberos-cast-2-ad-uzivatelske-ucty-a-service-principal-name/

[24] MADSEN, Paul, Yuzo KOGA a Kenji TAKAHASHI. Federated identity management for protecting users from ID theft. *Proceedings of the 2005 workshop on Digital identity management - DIM '05: Proceedings of the 2005 workshop on Digital identity management*. New York, New York, USA: ACM Press, 2005, , 77-. DOI: 10.1145/1102486.1102500. ISBN 1595932321. Dostupné také z: http://portal.acm.org/citation.cfm?doid=1102486.1102500

[25] BOUŠKA, Petr. Kerberos protokol a Single sign-on. *www.samuraj-cz.com* [online]. 2010 [cit. 2016-11-20]. Dostupné z: http://www.samuraj-cz.com/clanek/kerberos-protokol-a-single-sign-on/

[26] *Návod k použití C. S. O. pro manažery* Ostrava, 2014.

[27] *C.S.O. – stav k 14. 4. 2015* Ostrava, 2015

[28] VANDENWAUVER, Mark, René GOVAERTS a Joos VANDEWALLE. KATHOLIEKE UNIVERSITEIT LEUVEN, DEPT. ELEKTROTECHNIEK. *Overview of Authentication Protocols*. Heverlee, 2000, 6 s. Dostupné také z: https://www.cosic.esat.kuleuven.be/sesame/papers/carnahan.pdf

[29] MOLVA, Refik, Gene TSUDIK, Els VAN HERREVEGHEN a Stefano ZATTI. *KryptoKnight Authentication and Key Distribution System*. Valbonne: EURECOM Institute, 2002, 20 s. Dostupné také z: http://www.eurecom.fr/~nsteam/Papers/kryptoknight.pdf

[30] *Pracovní postup č. 12* Ostrava, 2012

[31] GOODIN, Dan. 25-GPU cluster cracks every standard Windows password in <6 hours. *Ars Technica* [online]. 2012 [cit. 2017-05-20]. Dostupné z:

https://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

[32] *Organizační struktura společnosti* Ostrava, 2011

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

AD Active Directory – adesářová služba od společnosti Microsoft

AD DS Active Directory Domain Services – serverová role služby Active Directory

API Application Programming Interface – aplikační programovací rozhraní

AS Authentication Server – autentizační server, součást protokolu Kerberos

DC Domain Controller – doménový řadič, centrální prvek domény

DNS Domain Name System – systém doménových jmen, realizovaný s pomocí DNS serverů

FAR False Acceptance Rate – četnost nesprávných přijetí u biometrických skenerů

FRR False Reject Rate – četnost nesprávných odmítnutí u biometrických skenerů

GC Global Catalog – globální katalog, součást lesa v prostředí Active Directory, umožňující dohledání zařízení z jiné domény v lese

HR Human Resource – lidské zdroje

ICT Information and Communication Technologies – informačně-komunikační technologie

IdM Identity Management – správa identit

IE Internet Explorer – webový prohlížeč

ISMS Information Security Management Systém – systém řízení bezpečnosti informací

ISO International Organization for Standardization – Mezinárodní organizace pro standardizaci

ITU International Telecommunication Union – Mezinárodní telekomunikační unie

KDC Key Distribution Centre – součást protokolu Kerberos

LDAP Lightweight Directory Access Protocol – protokol k ukládání a přístup k datům na adresářovém serveru

PIN Personal Identification Number – osobní identifikační číslo

RBAC Role-Based Access Control – řízení přístupů na základě rolí

SPN Service Principal Name – unikátní identifikátor instance služby

SQL Structured Query Language – strukturovaný dotazovací jazyk, určný pro práci s daty v relačních databázích

SSO Single Sign-On – metoda jednotného přihlášení do více služeb

TAN Transaction Authentication Number – autentizační číslo pro transakce

TGS Ticket-Granting Server – server, poskytující tickety, součást protokolu Kerberos

TGT Ticket Granting Ticket – ticket udělovaný v rámci autentizace v protokolu Kerberos

UPN User Principal Name – unikátní identifikátor uživatele

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH