VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH IDENTITY MANAGEMENTU VE SPOLEČNOSTI
IDENTITY MANAGEMENT DESIGN IN COMPANY

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE
AUTHOR

Lukáš Sladovník

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Viktor Ondrák, Ph.D.

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Lukáš Sladovník**
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 identity managementu ve společnosti

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 pro společnost zavedení identity managementu.

Základní literární prameny:

BERTINO, E. a K. TAKAHASHI. Identity management: Concepts, Technologies, and Systems. Boston: Artech House, 2011. ISBN 978-1-60807-039-8.

DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

OSMANOGLU, T. Ertem. Identity and access management: business performance through connected intelligence. Amsterdam, [Netherlands]: Syngress, an imprint of Elsevier, 2013. ISBN 978-012-40-1-406.

OSMANOGLU, T. E., R. ALLEN a A. G. LOWE-NORRIS. Active Directory: implementace a správa Microsoft Active Directory. Praha: Grada, 2005. ISBN 80-247-0973-2.

POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-8--7251-250-8.

STANEK, William R. Active Directory: kapesní rádce administrátora. Brno: Computer Press, 2009. ISBN 978-80-251-2555-7.

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

Bakalářská práce se zaobírá problematikou identity managementu ve společnosti. Analyzuje stav, jakým způsobem společnost řídí identity a spravuje přístupy, a jakým způsobem přistupuje k auditu dat. Následně podává návrhy na zlepšení včetně zavedení softwaru pro monitorování a audit.

Abstract

The bachelor's thesis deals with the issue of identity management in a company. It analyzes how the company manages identities and access and how the company audits data. Then it suggests proposals for improvement including software implementation for auditing and reporting.

Klíčová slova

identity management, identita, přístup, autentizace, autorizace, audit, role, heslo

Key words

identity management, identity, access, authentication, authorization, audit, role, password

Bibliografická citace

SLADOVNÍK, L. *Návrh identity managementu ve společnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 66 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 panu vedoucímu práce Ing. Viktoru Ondrákovi, Ph.D. za jeho vedení, rady a připomínky a všem dalším, kteří nějakou formou přispěli ke vzniku této bakalářské práce.

OBSAH

ÚVOD 11

1 CÍL A METODIKA PRÁCE 12

2 TEORETICKÁ VÝCHODISKA PRÁCE 13

2.1 Identity management 13

2.2 Životní cyklus identity 15

2.2.1 Vytvoření 15

2.2.2 Používání 16

2.2.3 Úprava 16

2.2.4 Zánik 16

2.2.5 Řízení 16

2.3 Autentizace 17

2.3.1 Single sign-on 17

2.4 Autorizace 18

2.4.1 Role based access control (RBAC) 18

2.5 Provisioning systém 18

2.6 Adresářový systém 19

2.7 Active Directory 20

2.7.1 Domény DNS 22

2.7.2 Řadiče domény 22

2.7.3 Objekty služby Active Directory 22

2.7.4 Schéma služby Active Directory 23

2.7.5 Logické součásti 24

3 ANALÝZA SOUČASNÉHO STAVU 26

3.1 Charakteristika společnosti 26

3.1.1 Organizační struktura 26

3.2 Řízení přístupu 28

3.2.1 Uživatelské role 28

3.2.2 Přístup na internet 29

3.3 Active Directory 30

3.3.1 Zásady účtu/Zásada hesel 30

3.3.2 Zásady účtu/Zásada uzamčení účtu 30
3.4 Autentizace 32
3.4.1 Politika hesel 32
3.4.2 Způsob nakládání s hesly 33
3.4.3 Uzamčení účtu 34
3.4.4 Single sign-on 35
3.5 Audit a reporting 35
3.6 Školení zaměstnanců 35
3.7 Požadavky investora 36
3.8 Shrnutí analýzy současného stavu ve společnosti 36
3.9 ADAudit Plus 37
3.9.1 Funkce a výhody ADAudit Plus 37
3.9.2 Dostupné edice a cenotvorba 38
3.9.3 Podpora 39
4 VLASTNÍ NÁVRHY ŘEŠENÍ 40
4.1 Politika hesel 40
4.1.1 Složitost hesla 40
4.1.2 Životnost hesla 41
4.2 Řízení přístupu 41
4.2.1 Odpovědnost a povinnosti 42
4.2.2 Uživatelské role 42
4.2.3 Schvalování rolí a přístupových práv 42
4.2.4 Odebírání přístupových práv 42
4.2.5 Kontrola uživatelských účtů a rolí 43
4.3 Systém vzdělávání zaměstnanců 44
4.4 ADAudit Plus 44
4.5 Časová náročnost a plán 46
4.6 Finanční zhodnocení 47
4.7 Přínosy zavedení návrhů 48
ZÁVĚR 49
SEZNAM POUŽITÝCH ZDROJŮ 50

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ 54
SEZNAM OBRÁZKŮ 55
SEZNAM TABULEK 56
SEZNAM PŘÍLOH 57

ÚVOD

Identity management neboli správa identit a přístupů je klíčová oblast pro zaručení bezpečnosti a efektivity téměř jakékoliv společnosti. Podnikové prostředí nedokáže efektivně existovat bez těchto technologií.

Základem porozumění celé této oblasti je, že identity management není jedna konkrétní technologie, ale soubor několika spolupracujících technologií. Jednotlivé prvky řešení se dají kombinovat podle potřeb daného prostředí. Existují však tři technologie, které by se měly nacházet v každém řešení. První z nich je adresářová služba, která udržuje centrální databázi uživatelů. Dále je to systém řízení přístupů, který zajišťuje autentizaci, základní autorizaci, zaznamenávání přístupů, a nakonec je to provisioning systém, který zabezpečuje správu databáze uživatelů, její synchronizaci, řídí bezpečnostní politiku atd.

V praxi se však můžeme setkat s tím, že systém řízení přístupů nahrazuje adresářová služba, synchronizaci databází neprovádí provisioning systém, ale synchronizuje se ručně. Takováto řešení jsou pomalá, chybová a otevírají velká bezpečnostní rizika.

Uživatelé jsou mnohdy povinni pamatovat si mnoho uživatelských jmen a hesel do několika různých aplikací a systémů. Avšak do těchto aplikací potřebují přístup nejen zaměstnanci dané společnosti, ale také její dodavatelé, zákazníci atd. Tuto problematiku řeší systém jednotného přihlášení, single sign-on, který však není vždy nasazen. Pokud má společnost jen částečné řešení systému řízení identit a přístupů, zvyšují se tím náklady na správu a zvyšují se bezpečnostní rizika. IT pracovníci musí mnohdy nastavovat ručně přístupová práva, hesla, v některých případech si uživatelé tyto hesla nalepují na klávesnici nebo ukládají do počítačů v nešifrované podobě. Smyslem identity managementu je tyto problémy vyřešit, místo toho, aby aplikace prováděly svou vlastní autentizaci a autorizaci, správa se centralizuje.

1 CÍL A METODIKA PRÁCE

Tato bakalářská práce se zaobírá problematikou identity managementu ve společnosti. Analyzuje stav, jakým způsobem společnost řídí identity a spravuje přístupy, a jakým způsobem přistupuje k auditu dat. Cílem je navrhnout řešení na zlepšení včetně zavedení softwaru pro monitorování a audit dat.

Bakalářská práce obsahuje část teoretických východisek, kterou je důležité znát pro pochopení dalších částí této práce. Na teoretická východiska navazuje analýza současného stavu, ve které se budu věnovat analýze dané problematiky ve společnosti. A následně v části návrhy na řešení se věnuji návrhům na zlepšení nedostatků a také zavedením softwaru pro monitorování a audit dat.

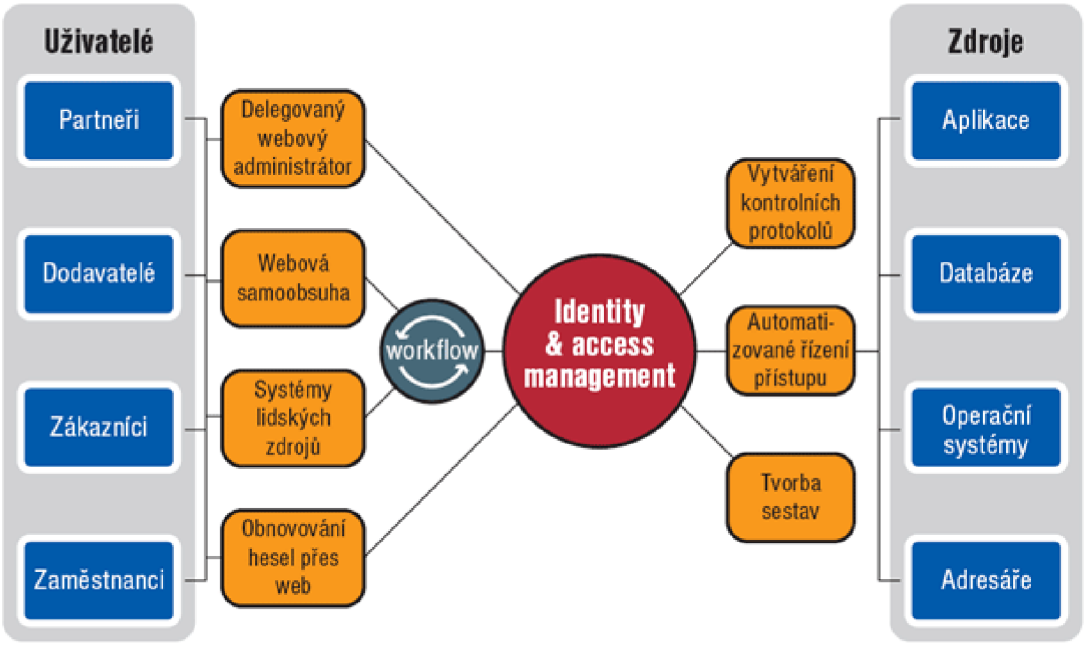
2 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole budou popsána jednotlivá teoretická východiska, která budou potom dále využita v analýze současného stavu a v návrhu řešení.

2.1 Identity management

Identity management nebo také identity and access management je informační systém, který dokáže z jednoho místa ovládat životní cyklus všech uživatelských účtů v dané společnosti a zároveň sledovat jejich změny díky auditu (20).

Identity and access management je soubor procesů a technologií používaných k řízení digitálních identit a jejich přístupů k prostředkům (12).



Obr. 1: Centrální správa uživatelských účtů a přístupů (17)

Identity management se odkazuje na lidi, procesy a technologie potřebné pro správu celého životního cyklu digitálních identit. Funkce identity managementu zahrnují následující:

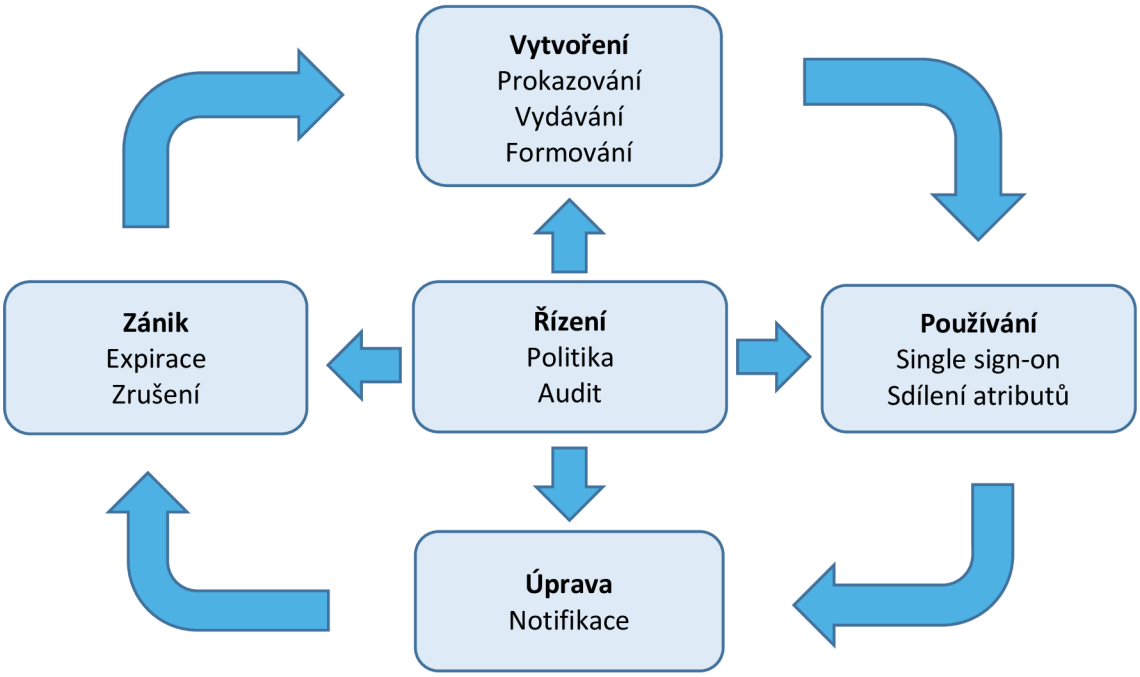
- zakládání jedinečných identit s příslušnými ověřovacími údaji,
- zavedení těchto identit do cílových aplikací, systémů a platforem,
- provisioning a de-provisioning nových uživatelských účtů,
- správa identit a uživatelských přihlašovacích údajů (např. automatické resetování hesla),
- vytváření workflow pro schvalování vytváření a modifikace účtů,
- poskytování možnosti k úpravě, deaktivování nebo odstranění účtů,
- audit a tvorba reportů (1).

Access management se odkazuje na procesy a technologie používané k řízení přístupů k určitým informačním aktivům poskytnutých určité identitě. Oprávnění je sada atributů, která určuje přístupová práva a privilegia autentizované identity. Například bezpečnostní skupiny a přístupové práva jsou oprávnění. Role, logické seskupení oprávnění, jsou definovány pracovními funkcemi, které mohou být trvale spojeny s definovaným souborem přístupových práv. Funkce access managementu zahrnují následující:

- poskytování možnosti požádat o určité oprávnění nebo roli,
- implementaci workflow pro schvalování udělení oprávnění nebo role identitě,
- poskytování možnosti upravit nebo odebrat oprávnění nebo role přiřazené uživateli,
- správu oprávnění vzhledem k rolím,
- asociace oprávnění a rolí k pracovním funkcím,
- poskytování možnosti posoudit, odebrat, schválit a ověřit oprávnění a role přiřazené uživatelům,
- poskytování možnosti prověrek a auditu historických přístupů spojených s identitou (1).

2.2 Životní cyklus identity

Správa životního cyklu identit zahrnuje procesy a technologie potřebné pro distribuci a odebírání zdrojů, správu a synchronizaci digitálních identit. Patří zde nástroje pro tvorbu digitálních identit, správu atributů, synchronizace identit, jejich agregace a odstraňování (14).



Obr. 2: Životní cyklus identity (8)

2.2.1 Vytvoření

Vytvoření identity se skládá z následujících dílčích kroků:

- prokazování atributů – mezi autoritami,
- vydávání ověřovacích údajů – po prokázání atributů autorita vydá ověřovací údaje (např. digitální certifikát, heslo),
- formování identity – z atributů, identifikátorů a ověřovacích údajů se vytvoří identita (8).

2.2.2 Používání

Identity mohou být využívány v různých službách, avšak jejich informace musí být chráněny. Běžně se používají tyto funkce:

- důvěryhodná komunikace – pro důvěryhodné transakce mezi komunikujícími stranami je potřebná důvěryhodnost identity,
- single sign-on – umožňuje přístup k více aplikacím a službám na základě jedné autentizace,
- sdílení atributů – mezi jednotlivými poskytovateli (8).

2.2.3 Úprava

Data identity je třeba neustále upravovat a aktualizovat, aby se zachovala jejich integrita a aktuálnost (8).

2.2.4 Zánik

Pokud identitě nebo jejím ověřovacím údajům vyprší platnost, jsou ukradeny nebo narušeny, je třeba je zrušit. Zrušení je důležité pro zajištění správné autentizace a autorizace (8).

2.2.5 Řízení

Celý životní cyklus identity je třeba řídit podle platných politik v dané společnosti. K řízení patří autentizace, autorizace a audit. Životní cyklus identity by měl být zaznamenáván v centrálním úložišti dat (8).

2.3 Autentizace

Autentizace je proces ověření identity nějakého subjektu. Existují tři základní způsoby:

- něco, co subjekt má (USB token, čipová karta, mobilní telefon),
- něco, co subjekt zná (heslo, PIN),
- něco, čím subjekt je (biometrické informace – např. otisky prstů, struktura duhovky, hlas).

V praxi se mohou tyto způsoby kombinovat. Na základě kombinace se potom jedná o autentizace dvoufaktorovou, třífaktorovou apod. (16).

2.3.1 Single sign-on

Single sign-on (SSO) je autentizační proces umožňující uživateli, který chce v rámci jedné relace přistupovat k více aplikacím, zadat přihlašovací údaje pouze jednou. Provedení procesu SSO se vyžádá při zahájení relace. Proces autentizuje uživatele pro přístup ke všem aplikacím, ke kterým mu bylo vydáno na serveru přístupové právo a eliminuje tím všechny budoucí výzvy k autentizaci, které by byly jinak aktivovány kdykoliv by se uživatel v rámci relace přepojil mezi aplikacemi. Výhodou je kromě uživatelského komfortu zvýšení bezpečnosti – omezuje se počet případů, kdy uživatel musí zadávat přihlašovací údaje (17).

Systémy SSO bývají obvykle budovány na bázi předávání pověřovacích dokladů (tokenů), aplikace musí tvořit homogenní systém. Např. když se použije jako pověřovací doklad standardizovaný certifikát a systém SSO je vybudovaný na bázi PKI, všechny aplikace musí být schopny spolupracovat s PKI (6).

Zavedení technologie SSO požaduje implementovat speciální infrastrukturu, ve které se obvykle nachází autentizační server, který nejprve ověří identitu uživatele a jeho přístupová práva, a až poté mu umožní přístup k požadované aplikaci (7).

2.4 Autorizace

Autorizaci je možné popsat jako proces přidělení privilegií, specifikaci povolené aktivity (16).

2.4.1 Role based access control (RBAC)

Role Based Access Control (RBAC) je rozšířený princip v řízení oprávnění, který využívá opakovaně přidělitelné objekty – role. Uživatel získá oprávnění přes přidělenou roli. Role může obsahovat další atributy, název, vlastníka role, jejího schvalovatele nebo popis. Identity management reprezentuje dílčí oprávnění v koncovém systému pomocí aplikační role (9).

Uživatel může mít mnoho různých aplikačních rolí, které se sdružují do skupin. Skupiny se nazývají business role a mohou odkazovat na více oprávnění v různých koncových systémech společnosti. Business role může být odvozena od organizační struktury, kdy obsahuje všechna oprávnění, která pracovník potřebuje pro příslušnou pozici ve společnosti. Business role mohou být také vázané na procesy nebo projekty (3).

2.5 Provisioning systém

Úlohou provisioning systému je spravovat účty a jejich přístupová práva ve všech systémech. Správa se provádí na základě požadavku administrátora i automaticky. Při automatické pravidelné synchronizaci se vytvoří identita v provisioning systému, adresářovém systému pro řízení přístupů a v ostatních informačních systémech a přidělí se příslušná přístupová práva podle připravených politik. Provisioning systém vytváří globální pohled na identitu pracovníka ve všech systémech. Při odchodu pracovníka je proto možné zrušit přístupy na jediném místě – v provisioning systému a synchronizovat změny do ostatních informačních systémů (10).

Synchronizace umožňuje i transformaci údajů na základě pravidel, vygenerování e-mailové adresy na základě jména, vygenerování jedinečného přihlašovacího jména nebo odstranění diakritiky pro některé atributy. Provisioning systém zabezpečuje konzistenci databází, údaje o uživatelích jsou tak konzistentní ve všech připojených systémech (2).

Provisioning systém poskytuje samoobslužné rozhraní, kdy si uživatel může na jednom místě změnit heslo pro kterýkoli účet, požádat o přístup do nového systému nebo vykonat přímou změnu předem definovaných atributů, což snižuje zatížení správců a administrátorů (15).

2.6 Adresářový systém

Adresářový systém slouží k efektivnímu ukládání a zpřístupnění údajů o identitách, které jsou využívány ostatními komponenty IAM řešení i samotnými aplikacemi. Standardem u adresářových služeb se stal protokol LDAP (13).

Adresářový systém bývá navrhován na vysokou dostupnost a škálovatelnost, umožňuje lehkou replikaci a distribuci dat. Adresářové služby jsou charakteristické pomalým zápisem dat a vysokou rychlostí při čtení. Adresářový systém je možné popsat jako rychlou, škálovatelnou a vysoce dostupnou databázi identit, která je zdrojem pro autentizační a autorizační rozhodnutí (5).

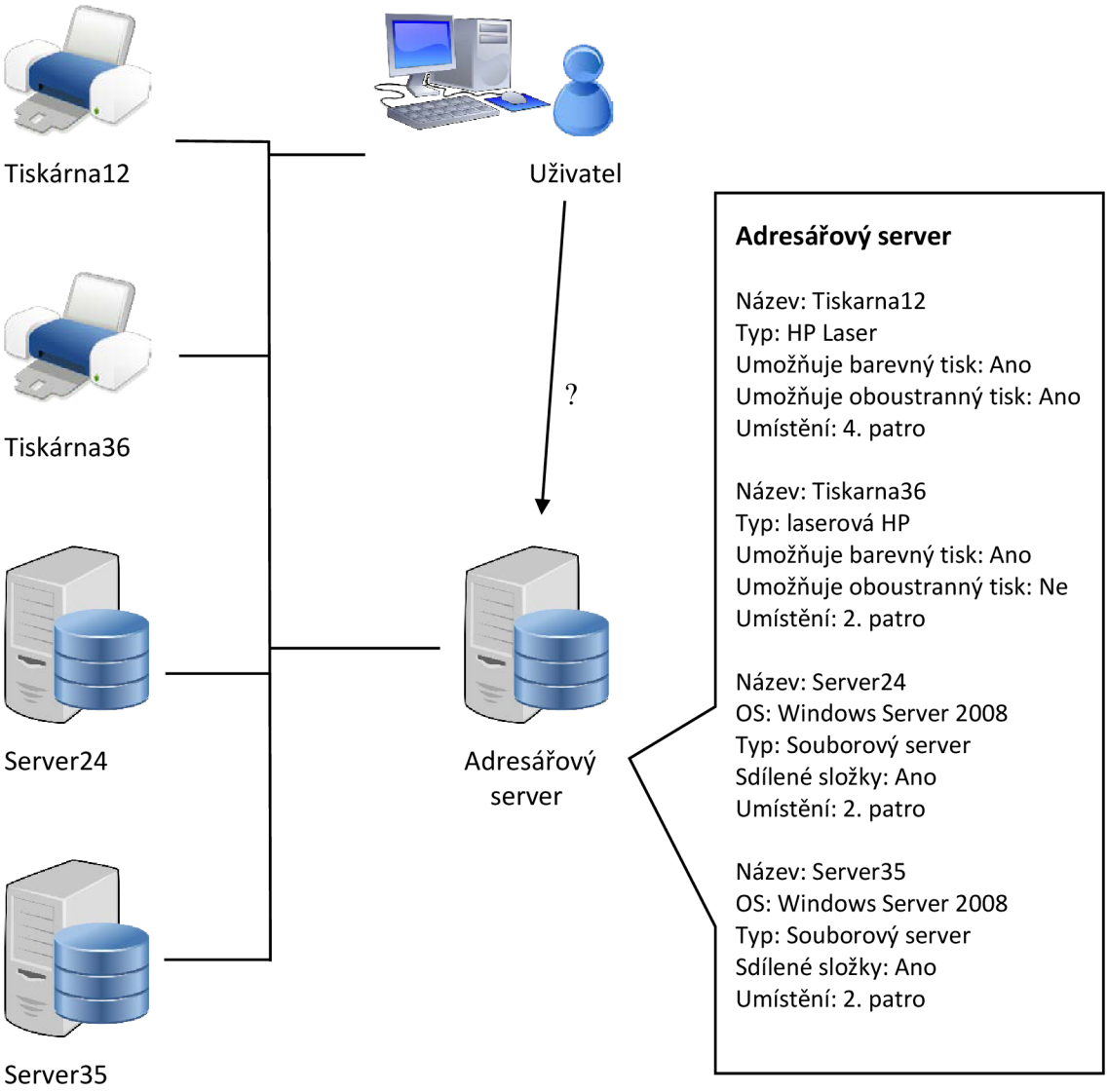
Mnoho aplikací podporuje autentizaci pomocí protokolu LDAP, proto je možné adresářovou službu využít i jako jednoduchý autentizační server, avšak pouze v rámci jednoduchého a omezeného řešení správy identit. Adresářové servery neudržují informace o uživatelské relaci (session), nemohou proto poskytovat službu SSO (2).

2.7 Active Directory

Active Directory je rozšiřitelná adresářová služba, která umožňuje centralizovanou správu síťových prostředků. Umožňuje snadno přidávat, odebírat nebo přemisťovat účty pro uživatele, skupiny, počítače a další typy prostředků. Je založena na standardních internetových protokolech (4).

Adresářová služba AD je obsažená v systému Windows Server. Poskytuje potřebnou infrastrukturu pro vytváření adresáře, který plní potřeby dané společnosti. Adresář je uloženou kolekcí informací o různých typech prostředků (11).

Služba AD ukládá veškeré informace, které jsou potřebné k používání a správě distribuovaných prostředků na jednom místě a umožňuje jejich spolupráci. Je zodpovědná za správu identit, ověření přístupu a kontrolu vztahů mezi prostředky. Umožňuje také vyhledávání prostředků podle různých charakteristik (4).



Obr. 3: Práce s adresářovými službami (4)

Služba AD vzájemně spolupracuje s dalšími adresářovými službami a je navržena tak, aby akceptovala požadavky od různých klientů, kteří využívají různé rozhraní. Standardním protokolem pro adresářové služby je protokol LDAP (Lightweight Directory Access Protocol), který primárně služba AD využívá. Ochrana dat je zajištěna protokolem Kerberos a také standardním podepisováním a šifrováním veškeré komunikace, která používá protokol LDAP (11).

2.7.1 Domény DNS

Služba AD používá službu DNS (Domain Name System), což je standardní internetová služba. Služba DNS i AD mají stejnou hierarchickou strukturu. DNS identifikují jednotlivé počítače a jejich vztahy, které jsou vyjádřeny pomocí domén. Domény používané v organizacích jsou organizačními doménami (4).

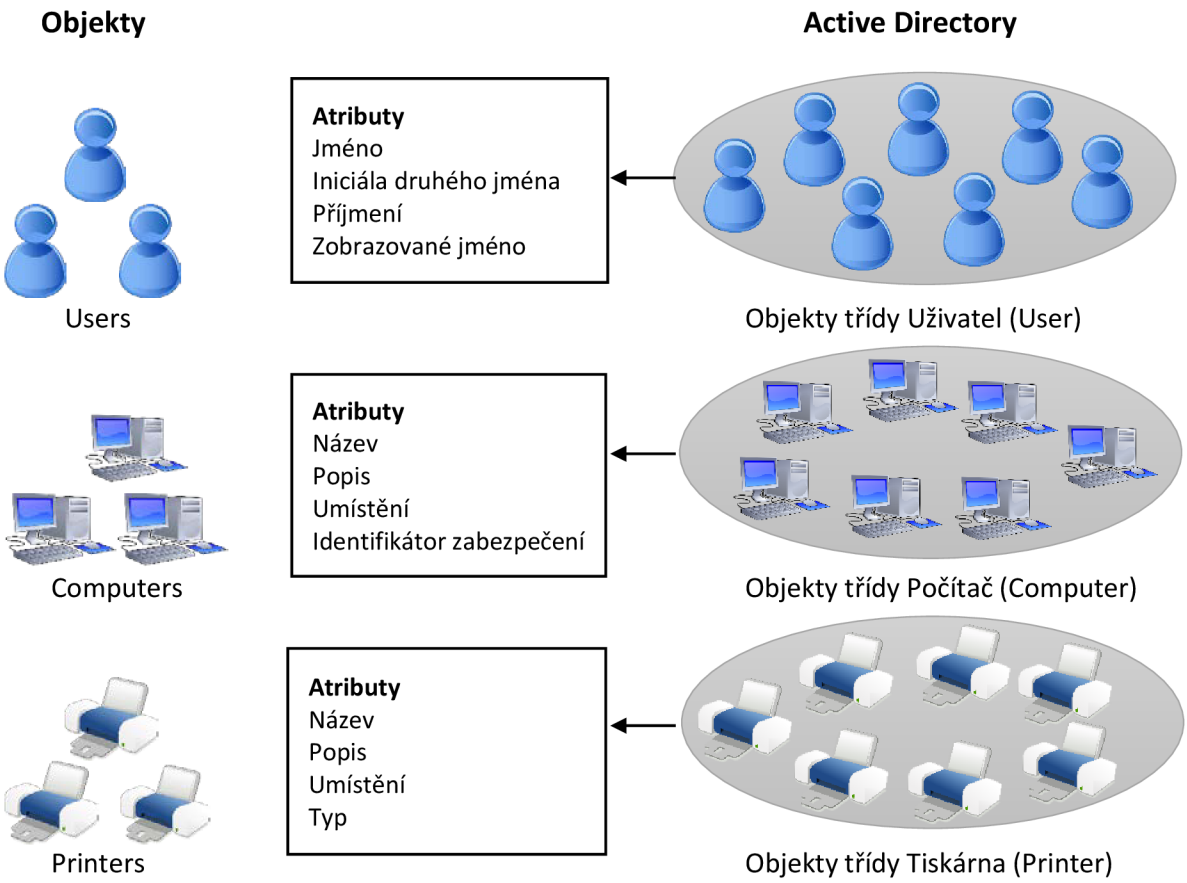
Služba DNS je používána k nalezení prostředků, překládá názvy hostitelů na adresy protokolu IP (11).

2.7.2 Řadiče domény

Řadič domény je počítač, na kterém je uložen adresář služby AD. Řadiče domény řídí všechny aspekty uživatelské interakce s doménami služby AD. Vyhledávají objekty, ověřují pokusy o přihlašování uživatelů a další. Řadiče domény jsou určeny pro čtení a pro zápis nebo jen pro čtení. Na řadičích jen pro čtení nejsou, až na výjimky, uložena žádná hesla. Jsou vhodné zejména tam, kde nelze zaručit fyzické zabezpečení (4).

2.7.3 Objekty služby Active Directory

Prostředky v AD jsou uložené jako objekty, které obsahují charakteristické atributy. Objekty se dělí na kontejnery a listy podle toho, zda mohou obsahovat jiné objekty (11).



Obr. 4: Objekty a atributy ve službě Active Directory (4)

2.7.4 Schéma služby Active Directory

Schéma definuje dostupné třídy objektů a stanovuje pravidla určující způsob vytváření a používání objektů. Mezi dostupné třídy objektů patří Uživatel, Skupina, Počítač a Tiskárna. Schéma určuje typy informací o třídách objektů, které mohou být v adresáři uloženy. Samotné schéma je uložené jako objekt tříd schématu nebo jako objekt atributů schématu (11).

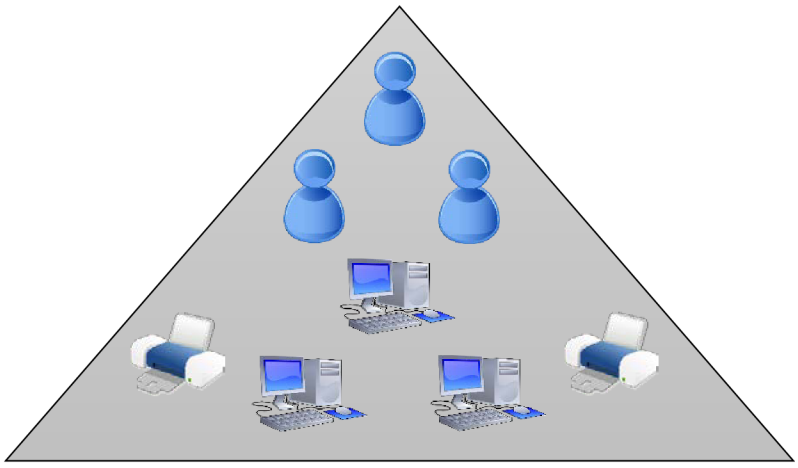
Objekty tříd schématu slouží jako šablony pro vytváření nových objektů. Atributy schématu uchovávají informace popisující příslušné objekty. Služba AD obsahuje základní třídy schématu a atributy, které je možné dále rozšiřovat (4).

2.7.5 Logické součásti

Mezi logické součásti se řadí domény, stromy domén, doménové struktury a organizační jednoty (OU). Tyto součásti tvoří logickou strukturu, která je prezentována uživatelům (4).

Domény

Domény jsou logickými seskupeními objektů, představují objekty kontejneru. V doméně lze vytvářet účty pro uživatele, počítače, skupiny, tiskárny a složky. Doména může obsahovat velké množství objektů, o kterých uchovává informace, avšak přístup k těmto objektům je kontrolován oprávněními zabezpečení (11).



Obr. 5: Doména služby Active Directory (4)

Stromy

Stromy domén jsou logickými seskupeními domén. Stromová struktura znázorňuje vzájemné vztahy nadřazených a podřízených objektů (4).

Doménové struktury

Doménové struktury jsou logickými skupinami stromů domén. Doménová struktura umožňuje komunikaci mezi členy domén. Mezi těmito doménami existují implicitní obousměrné přenositelné vztahy důvěryhodnosti. Výchozím používaným protokolem je Kerberos (11).

Organizační jednotky

Organizační jednotky (OU) jsou logickými kontejnery, které se používají k uspořádání objektů v doméně. Organizační jednotky usnadňují správu účtů pro uživatele, skupiny, počítače, tiskárny a sdílené složky (4).

3 ANALÝZA SOUČASNÉHO STAVU

Následuje analýza současného stavu ve společnosti, na kterou potom navazují vlastní návrhy řešení.

3.1 Charakteristika společnosti

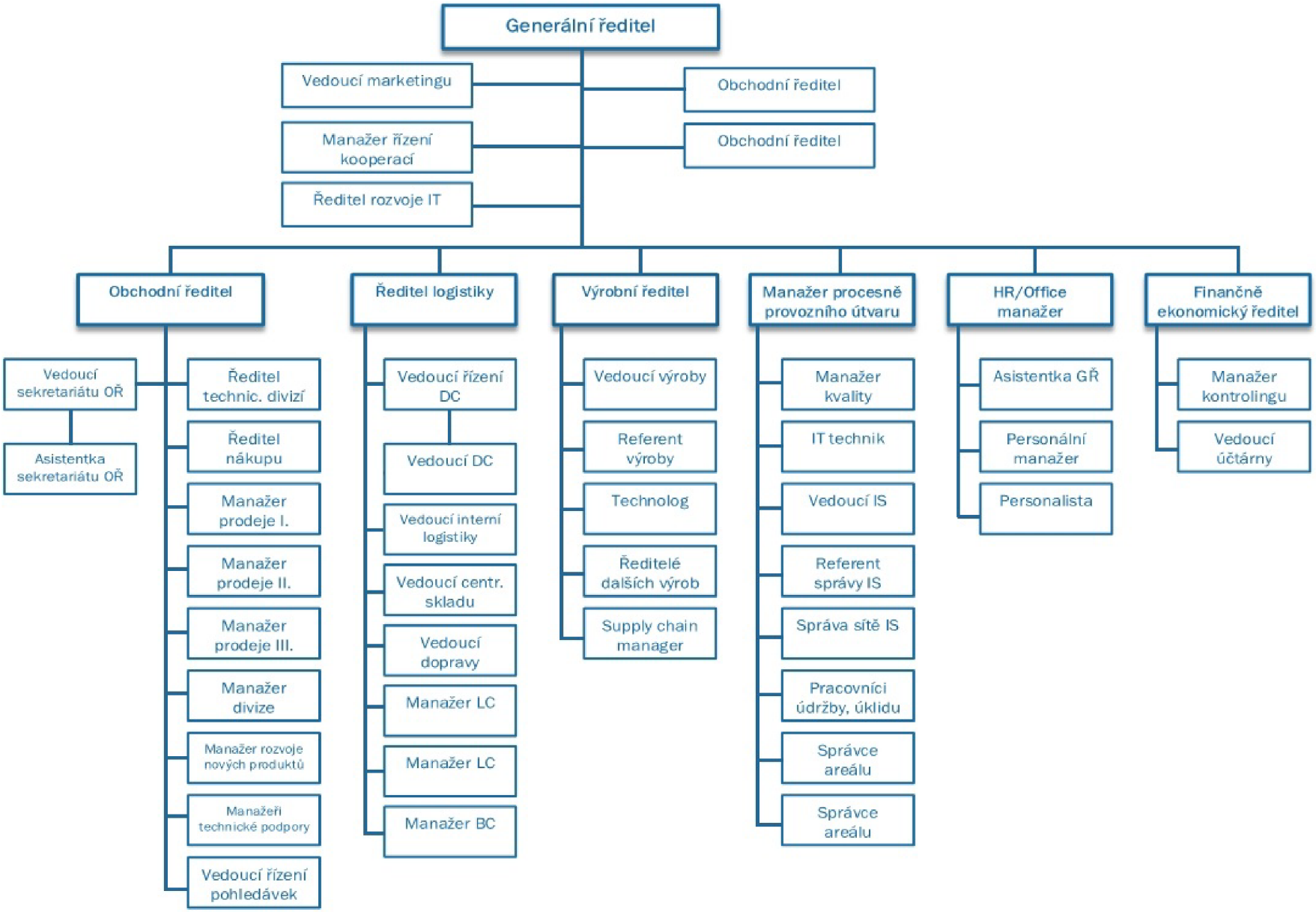
Společnost si z důvodu citlivosti údajů nepřála být jmenována. Společnost je českým výrobcem a dodavatelem obalových materiálů a balicích strojů pro Českou republiku a Evropu. Cílem společnosti je vycházet zákazníkům vstříc v jejich požadavcích na spolehlivost, kvalitu dodávek a profesionální poradenský servis v oblasti balicích strojů a obalových materiálů pro skupinová, přepravní a ochranná balení.

Společnost vlastní několik výrobních závodů a distribučních center po celé České republice a počet zaměstnanců je do pěti set. Vlastní certifikaci systému managementu kvality ČSN EN ISO 9001 a systému enviromentálního managementu ČSN EN ISO 14001.

Analýzu budu provádět v areálu sídla společnosti, které se nachází v Brně. Počet zaměstnanců se zde pohybuje okolo dvou set. Nachází se zde několik stolních počítačů a přenosných notebooků s operačním systémem MS Windows. Je zde také zavedena centrální IT podpora, se kterou uživatelé komunikují především prostřednictvím aplikace Service Desk.

3.1.1 Organizační struktura

Organizační struktura je vyobrazena na následujícím obrázku. V jejím čele stojí Generální ředitel, který má pod sebou další ředitele jednotlivých útvarů. Ředitel rozvoje IT je přímým podřízeným Generálního ředitele, avšak ostatní IT pracovníci jsou podřízeni Manažerem PPÚ.



Obr. 6: Organizační struktura

3.2 Řízení přístupu

Společnost má vypracované dokumenty politiky řízení přístupu, avšak tyto dokumenty jsou zastaralé a momentálně se připravují nové verze těchto dokumentů. Certifikaci ISO/IEC 27001 systému řízení informační bezpečnosti společnost nevlastní. Většinu procesů a činností v oblasti identity managementu provádí IT technik a schvaluje jeho nadřízený, Manažer PPÚ.

3.2.1 Uživatelské role

Přístupy jsou udělovány na základě rolí v AD. Role se zaměstnanci přiřazuje při jeho nástupu na pozici, kdy pracovník HR zadá požadavek přes Service Desk, což je nástroj pro sledování celého životního cyklu požadavků. Service Desk je nativně integrovaný s AD, který slouží jako zdroj informací o uživatelích a také řídí uživatelské role a oprávnění v Service Desku. Do Service Desku mají přístup pouze někteří pracovníci, zejména vedoucí a manažeři. Pokud zaměstnanec svým nástupem nahradil bývalého pracovníka, je mu přiřazena jeho původní role. V tomto případě IT technik v AD přepíše účet původního zaměstnance. V jiném případě mu přiřadí roli na základě nové pozice. Roli musí schválit Manažer PPÚ. HR oddělení následně přijde vyrozumění, že požadavek je vyřešen. V politice AD je nastaveno 5 následujících rolí:

- Obchodní zástupce,
- Manažer,
- Člen porady vedení,
- Referent,
- Pracovník skladu výroby.

Na podobném principu funguje také odebírání rolí. Role určuje rozsah přístupů. Každý pracovník má takovou roli, která je adekvátní jeho pracovní pozici a která ho neomezuje při běžných pracovních činnostech. Navíc má každý pracovník různá oprávnění zapisovat a nahlížet do složek podle toho, na jakém oddělení pracuje.

Přístupy a oprávnění se mohou individuálně povolovat a zakazovat. Řeší se to zadáním požadavku přes Service Desk. Pokud nemá žádající pracovník přístup do Service Desku, požádá svého nadřízeného. Změnu provádí IT technik a schvaluje Manažer PPÚ. Service Desk dokumentuje komunikaci a způsob řešení a archivuje splněné požadavky.

Role a oprávnění se kontrolují pouze namátkově IT technikem a dalšími pracovníky IT oddělení, celkové kontroly neprobíhají. Je to dáno především tím, že pracovníci IT jsou velmi zaneprázdněni a na takové kontroly nemají dostatek času. Kontroly se nedokumentují.

3.2.2 Přístup na internet

Zaměstnanci mohou na svých pracovních počítačích využívat internet. Určité webové stránky jsou zablokované. Jsou zavedené 3 skupiny pro používání internetu:

- Referenti,
- Manažeři,
- Členové porady vedení.

Zaměstnanci se při nástupu na určitou pozici přidělí příslušná skupina, která určuje seznam blokovaných webových stránek. Také jsou určeny webové stránky, které jsou blokované pro všechny zaměstnance bez ohledu na přidělenou skupinu. Seznam blokovaných webových stránek sestavil generální ředitel společnosti.

Webové stránky se třídí podle kategorií a každá skupina má nastavené blokované kategorie. Zaměstnanec může požádat o změnu skupiny, ve které je zařazený, změnu kategorie nebo povolení pro určitou webovou stránku zadáním požadavku přes Service Desk. Požadavek následně zpracuje IT technik. Pokud je požadavek oprávněný, podléhá schválení Manažera PPÚ. Manažer přes Service Desk požadavek schválí nebo zamítne. Pokud je požadavek schválen, IT technik podle druhu požadavku buď změní skupinu pro zaměstnance, změní kategorii nebo povolí zadanou webovou stránku. Zaměstnanec je o způsobu vyřízení informován přes Service Desk.

Ve společnosti je také zavedené Wifi připojení. Síť Intranet mohou využívat pouze zaměstnanci a zabezpečení je přes registrovanou MAC adresu a heslo. Síť Guests je veřejná, slouží pro návštěvy a je zabezpečena heslem. Firemní zařízení mají doménovou politikou nastaveno, že tahle síť pro ně není dostupná.

3.3 Active Directory

Společnost používá k řízení přístupu AD. Momentálně vlastní verzi 2008. Na následujícím obrázku je vyobrazen Group Policy Management neboli správa zásad skupiny. Je zde vidět jeden strom s názvem ipp.loc, který obsahuje jednu doménu ipp.loc. Doména obsahuje řadiče domény (Domain Controllers), doménové servery (Domain Servers), organizační jednotky, Microsoft Exchange skupiny zabezpečení a objekty zásad skupiny (Group Policy Objects). Na obrázku jsou rozkliknuty výchozí zásady domény, nastavení zabezpečení. Nastavení zabezpečení popisují následující podkapitoly a jsou platné pro stolní počítače. Pro přenosné notebooky platí určité rozdíly (viz obr. 9).

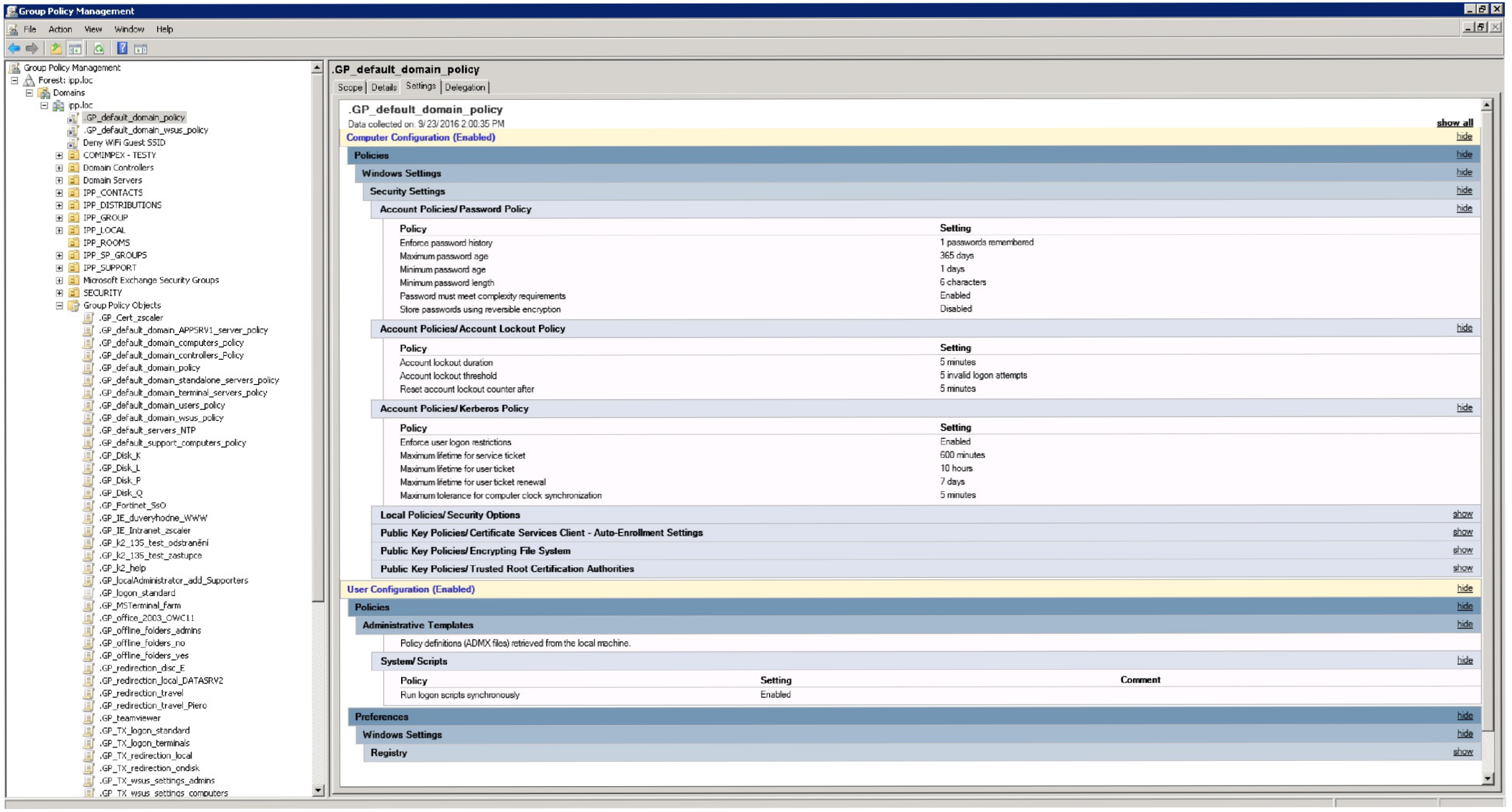
3.3.1 Zásady účtu/Zásada hesel

Z obrázku č. 7 lze vyčíst, že historie hesel je nastavena pouze na jedno heslo, maximální životnost hesla je 365 dní, minimální životnost jeden den. Heslo musí být dlouhé alespoň šest znaků a musí obsahovat požadavky, které jsou popsány v kapitole Politika hesel. Ukládání hesel pomocí reverzibilního šifrování je zakázáno.

3.3.2 Zásady účtu/Zásada uzamčení účtu

Účet je uzamčen po 5 neplatných pokusech o přihlášení. Resetování čítače je nastaveno na 5 minut, stejně tak jako doba trvání uzamčení účtu.

Dále lze z obrázku vyčíst zásady modulu Kerberos. Všechny nastavené hodnoty jsou v AD výchozí.



Obr. 7: Správa zásad skupiny (18)

3.4 Autentizace

V roce 2010 byla ve společnosti zavedena dvoufaktorová autentizace. Zaměstnanci se do svých PC přihlašovali pomocí USB tokenu a hesla. Společnost si tím slibovala především zvýšení bezpečnosti. Po čase se však ukázalo, že tento způsob s sebou přinesl spoustu problémů. Největším problémem byla poruchovost tokenů. Průměrná životnost jednoho zařízení byla asi dva měsíce. Dále to byla nepraktičnost. Tokeny byly pro zaměstnance příliš velké. Zapomínali je v PC, vůbec je nevyndávali, a to i přesto, že v bezpečnostní politice bylo stanovené, že při každém opuštění pracovního místa u PC musí token z PC vytáhnout a vzít ho s sebou. Zároveň bylo s tímto řešené šifrování. Šifrování probíhalo po jednotlivých souborech. Občas se stalo, že se nějaký soubor zašifroval dvakrát – soubor již nešel obnovit. Z těchto důvodů společnost USB tokeny zrušila a zaměstnanci se k PC přihlašují pouze na základě hesla. Zároveň společnost přešla na variantu šifrování celého disku. Tato varianta je bezpečnější, celý disk je v případě odcizení zašifrovaný.

3.4.1 Politika hesel

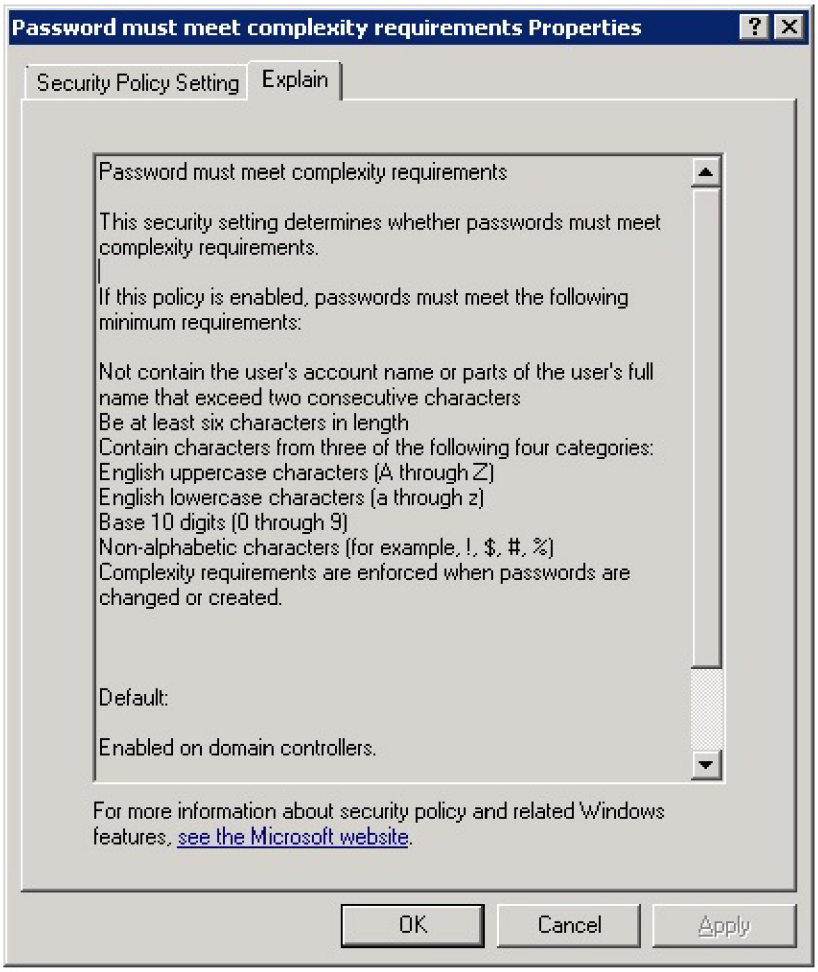
V současné době je politika hesel následující:

- heslo nesmí obsahovat uživatelovo přihlašovací jméno,
- heslo nesmí obsahovat část uživatelova jména a příjmení, která je delší než dva po sobě jdoucí znaky,
- délka hesla musí činit minimálně šest znaků,
- heslo musí obsahovat znaky minimálně tří z následujících čtyř kategorií:
    - velká písmena (A-Z),
    - malá písmena (a-z),
    - číslice (0-9),
    - nealfanumerické znaky (např. !, $, #, %).

Politika hesel je obsažena jak ve směrnici, tak v AD a všichni zaměstnanci jsou povinni ji dodržovat.

U stolních počítačů je životnost hesla nastavena na 365 dní a AD si pamatuje pouze jedno heslo, tudíž může uživatel střídat dvě hesla pořád dokola (viz obr. 7).

U přenosných notebooků je historie hesel nastavena na 10, avšak heslo nikdy nevyprší, tudíž mají uživatelé pořád jedno (viz obr. 9).



Obr. 8: Politika hesel (18)

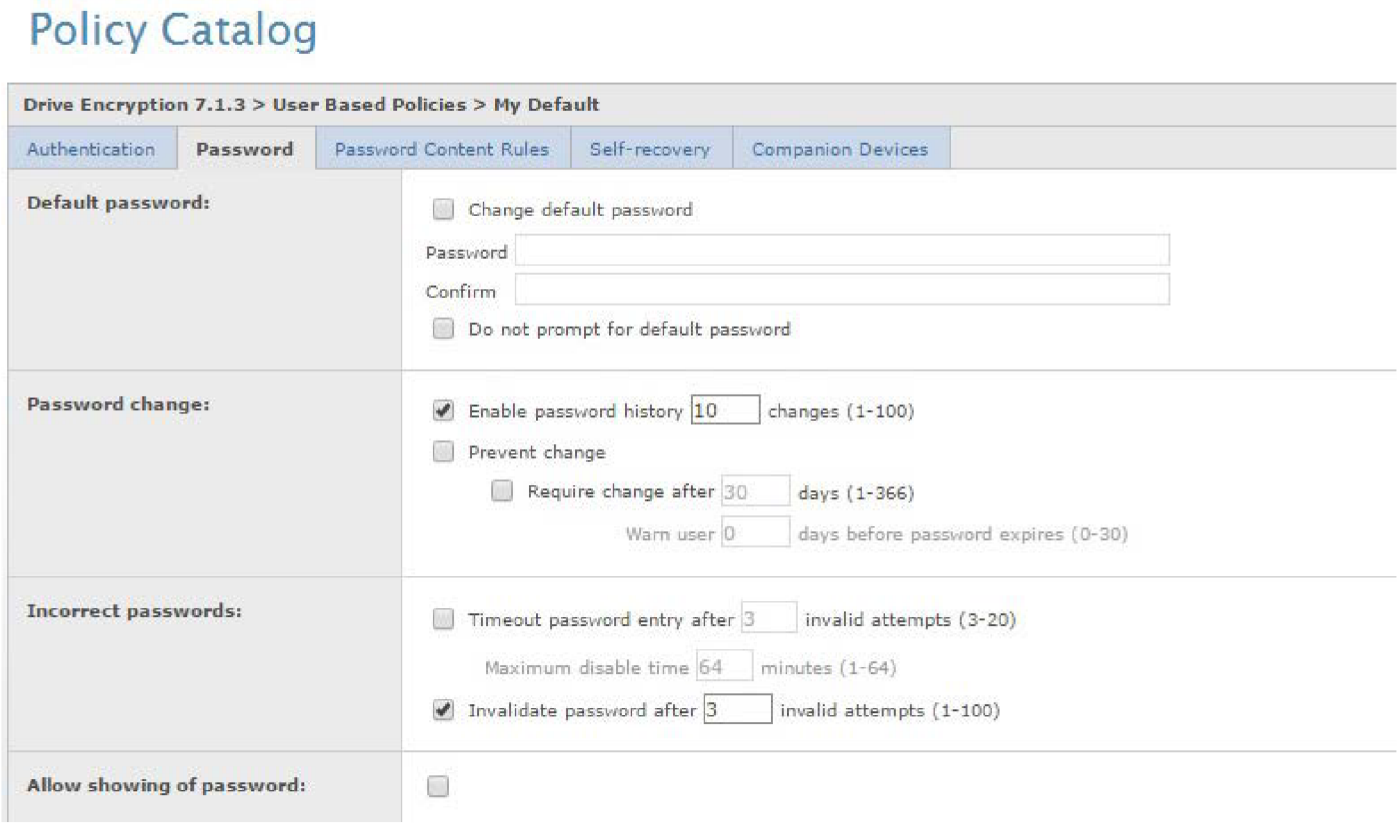
3.4.2 Způsob nakládání s hesly

Způsob nakládání a používání hesel je uveden ve směrnici. Zaměstnanci jsou povinni udržovat heslo v tajnosti. Všichni zaměstnanci jsou povinni tuto směrnici dodržovat.

3.4.3 Uzamčení účtu

V případě stolních počítačů platí výchozí zásady domény v AD (viz obr. 7). Počet pokusů o přihlášení je stanoven na 5, poté musí uživatel čekat 5 minut na dalších 5 pokusů nebo se obrátit na IT podporu. U přenosných notebooků je počet pokusů o přihlášení nastaven na tři. Pokud uživatel zadá třikrát špatné heslo, počítač se uzamkne (viz následující obrázek). Tento případ bývá nejčastěji způsoben zapomenutím hesla. Následně uživatel volá IT technikovi. Uživateli se vygeneruje 28 znakový kód, který nadiktuje IT technikovi do telefonu. Na základě tohoto kódu se mu vygeneruje jiný 28 znakový kód, který zase zpětně nadiktuje uživateli. Uživatel tento kód zadá do počítače, kde si následně může zobrazit původní heslo nebo nastavit nové.

Rozdělení počtu pokusů o přihlášení je z důvodu bezpečnosti. Riziko, že se útočník dostane do kanceláře k počítači a nikdo ze zaměstnanců si ho nevšimne je menší, než když se útočník dostane k notebooku, který si odnesl zaměstnanec domů.



Obr. 9: Zabezpečení pro notebooky

3.4.4 Single sign-on

Systém single sign-on společnost zavedený nemá. Zaměstnanci jsou stále povinni pamatovat si několik desítek hesel. To s sebou přináší některé rizika, např. zapisování hesel na papír a následné nalepování na klávesnici nebo ukládání hesel do počítačů v nešifrované podobě.

V dohledné době společnost se zavedením SSO nepočítá. Důvody jsou především ekonomické – nasazení a správa SSO vyžaduje nemalé finanční prostředky. Avšak s růstem společnosti a nárůstem počtu zaměstnanců je možné, že SSO bude jednou ve společnosti zaveden.

3.5 Audit a reporting

AD hraje v identity managementu společnosti velkou roli. AD však není nastavený, aby prováděl jakýkoliv audit. Veškeré aktivity a procesy se nikde zaznamenávají.

3.6 Školení zaměstnanců

Školení zaměstnanců probíhá nepravidelně. Zaměstnanci bývají školeni při nástupu do společnosti a dále pak podle individuálních potřeb a podle potřeb společnosti.

Školení v oblasti informační bezpečnosti probíhá individuálně při nástupu na pozici v rámci přebírání počítače. Zaměstnanec je poučen o způsobu nakládání s hesly, pravidlech přihlašování a odhlašování a dalších bezpečnostních opatřeních. Školení zpravidla nepřesahuje dobu jedné hodiny.

Dále probíhají velká školení, kdy jsou zaměstnanci školeni v oblasti různých témat, které se za dobu od posledního takového školení nashromáždily. Obvykle se do těchto školení

zahrne i oblast IT (např. školení na MS Excel), méně často pak oblast informační bezpečnosti. Taková školení probíhají obvykle jednou až dvakrát za rok.

3.7 Požadavky investora

Management společnosti potřebuje monitorovat činnosti uživatelů v souvislosti s identity managementem a AD. Dosáhne toho zavedením softwaru pro monitorování a audit dat. Management společnosti se rozhodl pro nástroj ADAudit Plus, jelikož v minulosti již probíhala snaha IT oddělení o jeho zavedení. Dále s tímto nástrojem mají již pracovníci IT zkušenosti, a proto management společnosti trvá na zavedení právě tohoto nástroje.

Dále by chtěl zhodnotit politiku hesel a nastavit novou.

3.8 Shrnutí analýzy současného stavu ve společnosti

Z analýzy současného stavu vyplynulo, že AD hraje v identity managementu společnosti velkou roli. Problém spočívá v absenci auditu dat. Jakékoliv aktivity, konfigurace a změny nejsou hlášeny a nikde se nezaznamenávají.

Další problémy se týkají politiky hesel. Požadavky na složitost hesla jsou nastaveny optimálně, až na minimální délku šest znaků. Problém spočívá v životnosti hesla. V případě stolních počítačů používají uživatelé stejné heslo po celý rok, v případě notebooků nemají povinnost si heslo měnit vůbec, tudíž používají pořád stejné.

Další nedostatky se týkají školení uživatelů a řízení přístupu. V současné době jsou uživatelé školeni při nástupu do společnosti a pak již nepravidelně nebo vůbec. Role určující přístupová práva, které jsou nastaveny v politice AD, a také individuální změny přístupových práv se kontrolují pouze namátkově nebo vůbec. Je zde absence směrnic, které by určovaly povinnosti a odpovědnosti.

3.9 ADAudit Plus

ADAudit Plus představuje nástroj pro audit, monitorování a reporting všech operací týkajících se objektů AD (Uživatel, Skupina, GPO, Počítač, OU, DNS, AD Schéma, Konfigurace) s možností aktivních upozornění oprávněných uživatelů na nestandardní či nebezpečné akce (22).

3.9.1 Funkce a výhody ADAudit Plus

ADAudit Plus je kompletně webově založený a umožňuje přístup odkudkoliv v doméně. To umožňuje centrální sledování a reporting všech změn auditu. Dále nabízí intuitivní uživatelské rozhraní a archivování auditních dat (21).

ADAudit Plus poskytuje více než 100 přednastavených reportů pokrývajících širokou škálu požadavků auditu AD ve společnosti. Reporty jsou rozděleny do těchto kategorií:

- uživatelské přihlášení,
- místní přihlášení – odhlášení,
- management účtů,
- management uživatelů,
- management skupin,
- management počítače,
- změny zásad domény (Domain Policy Changes),
- management OU,
- management GPO (21).

Podrobný rozpis reportů je uveden v příloze. ADAudit Plus umožňuje grafické znázornění různých událostí auditu pomocí grafů, umožňuje upozornění v reálném čase a upozornění emailem. Upozornění na události lze nakonfigurovat, což lze provést buď pomocí profilů nebo na jakéhokoliv vybraného nebo vybrané uživatele (21).

Dále poskytuje možnost nastavit si vlastní reporty, možnost exportování různých reportů do požadovaných formátů - csv, html, pdf nebo xls.

ADAudit Plus umožňuje vícenásobný přístup**.** Pracovníci helpdesku se mohou přihlašovat pomocí delegovaných operátorských rolí nebo rolí administrátorů. Pomocí administrátorské role mohou spravovat konfigurace, pomocí operátorské role mohou pouze zobrazovat reporty (21).

ADAudit Plus umožňuje aplikovat bezpečnostní certifikáty organizace a umožňuje aplikaci spustit zabezpečeným připojením.

ADAudit Plus audituje každou změnu v Active Directory. Tyto změny lze popsat jako čtyři dimenze: kdo, co dělal, odkud a kdy to dělal.

ADAudit Plus poskytuje detekci a prevenci incidentů – díky okamžitému upozornění na anomálii lze zabránit vzniku případného incidentu. Nabízí také organizované archivování a prevenci incidentů – lze se dostat až k jádru problému a zabránit tím jeho opakovanému vzniknutí (21).

3.9.2 Dostupné edice a cenotvorba

ADAudit Plus je dostupný ve čtyřech edicích. Edice Free a Trial jsou bezplatné, edice Standard a Professional jsou placené. Licencování je založeno na počtu řadičů domén, souborových serverů, členských serverů a pracovních stanic. Licence je založena na XML a dodávána prostřednictvím e-mailu. Tabulka popisující jednotlivé edice je uvedena v příloze.

Pro všechny edice je k dispozici na stažení jeden soubor. Při instalaci se nainstaluje edice Professional a bude bezplatně fungovat po dobu třiceti dní. Poté je třeba zakoupit edici Standard nebo Professional, jinak se produkt vrátí do Free edice, kterou je možné dále bezplatně používat. Je možné stáhnout 32 bit nebo 64 bit verzi.

3.9.3 Podpora

Uživatelský online manuál je dostupný na adrese: https://www.manageengine.com/products/active-directory-audit/help/index.html. Lze si ho také stáhnout v souboru Zip. Manuál je nápomocný v případě různých problémů, které mohou nastat při konfiguraci nebo provozu ADAudit Plus. K dispozici je také online podpora, a to prostřednictvím živého chatu 24/5 nebo prostřednictvím e-mailu: support@adauditplus.com.

4 VLASTNÍ NÁVRHY ŘEŠENÍ

U vlastních návrhů řešení budu vycházet z analýzy současného stavu. Zaměřím se na změnu politiky hesel a na změnu řízení přístupu. Zde se budu věnovat odpovědnostem a povinnostem za jednotlivé činnosti a procesy, uživatelským rolím, schvalováním rolí a přístupových práv, odebíráním přístupových práv a kontrolou uživatelských účtů a rolí. Dále na systém vzdělávání pracovníků a na nástroj ADAudit Plus pro monitorování a audit dat.

4.1 Politika hesel

Politika hesel by měla být nastavena tak, aby z bezpečnostního hlediska nebylo možné heslo jednoduše uhodnout, mělo by být odolné proti slovníkovému útoku. Zde se kladou nároky na délku, složitost a obsah. Na druhou stranu v případě přísné politiky roste riziko zapisování hesla uživatelem např. na klávesnici nebo ukládání do počítače v nešifrované podobě. Roli zde hraje i školení, jak si takové heslo vytvořit. Zodpovědný za politiku hesel bude Manažer PPÚ.

4.1.1 Složitost hesla

Do směrnice obsahující politiku hesel doporučuju doplnit:

- minimální délka hesla činí osm znaků,
- zaměstnanec nesmí své heslo nikomu sdělovat a nesmí si ho nikam zapisovat.

Implementace by měla zahrnovat:

- schválení managementu společnosti a IT oddělením změny složitosti hesla,
- informování uživatelů o budoucí změně politiky hesel,
- nastavení v AD minimální délku hesla na osm znaků IT oddělením,
- doplnění změn do směrnice politiky hesel,

- informování managementu společnosti IT oddělením o provedených změnách.

4.1.2 Životnost hesla

Aktuálně nastavená životnost hesla není optimální. V případě stolních počítačů používají uživatelé stejné heslo po celý rok, v případě notebooků nemají povinnost si heslo měnit vůbec a většina uživatelů proto používá pořád stejné.

V případě stolních počítačů bych doporučil snížit maximální životnost hesla na 190 dní. Jelikož si AD pamatuje pouze jedno minulé heslo, neměla by to být pro uživatele příliš velká zátěž. V případě notebooků bych doporučil nastavit maximální životnost hesla taktéž na 190 dní a současně přenastavit historii hesel z deseti na tři. Tyto doporučení je třeba doplnit do směrnice a zároveň aktualizovat v AD.

Implementace by měla zahrnovat:

- schválení managementu společnosti a IT oddělením změny životnosti hesla,
- informování uživatelů o budoucí změně politiky hesel,
- nastavení v AD maximální životnost hesla na 190 dní IT oddělením,
- nastavení maximální životnosti hesla 190 dní pro notebooky IT oddělením,
- nastavení historie hesel pro notebooky na tři hesla IT oddělením,
- doplnění změn do směrnice politiky hesel,
- informování managementu společnosti IT oddělením o provedených změnách.

4.2 Řízení přístupu

V této části se budu věnovat odpovědnostem a povinnostem za jednotlivé činnosti a procesy, uživatelským rolím, schvalováním rolí a přístupových práv, odebíráním přístupových práv a kontrolou uživatelských účtů a rolí. Zodpovědný za politiky řízení přístupu bude Manažer PPÚ, který může některé činnosti delegovat na svého podřízeného IT technika, který mu bude reportovat.

4.2.1 Odpovědnost a povinnosti

Jednotlivé činnosti a procesy v oblasti identity managementu by se měly rozdělit a přidělit tak, aby každý zaměstnanec věděl, co je jeho povinnost a za co je zodpovědný. S tímto pomůže zavedení nástroje ADAudit Plus, který bude veškeré změny auditovat a reportovat. Aplikace Service Desk bude dokumentovat komunikaci, schvalování a workflow. Jednotlivé workflow by měly být nastavené a měly by se správně používat.

4.2.2 Uživatelské role

V politice AD je nastaveno 5 následujících rolí, které určují přístupová práva: Obchodní zástupce, Manažer, Člen porady vedení, Referent a Pracovník skladu výroby. Zde bych doporučil přístupové práva rolí a také jednotlivé role zkontrolovat, zda odpovídají aktuálním potřebám společnosti. Takováto kontrola by se měla opakovat v intervalu jedenkrát za rok.

4.2.3 Schvalování rolí a přístupových práv

Při nástupu zaměstnance na pozici se role přiřazuje na základě požadavku pracovníka HR oddělení. Roli přiřazuje IT technik a schvaluje Manažer PPÚ. Do toho procesu bych doporučil zahrnout ještě nadřízeného příslušného zaměstnance, který bude muset roli také schválit. Tímto se zamezí případnému nesouladu mezi pracovní pozicí a přidělenou rolí. Workflow by se mělo implementovat do aplikace Service Desk.

4.2.4 Odebírání přístupových práv

Zde je důležité, aby byla pracovníkovi odebrána přístupová práva k informacím hned po ukončení pracovního poměru. Uživatelský účet by měl být odstraněn nebo deaktivován. Prostřednictvím Service Desku dá pracovník HR oddělení pokyn IT technikovi, který účet

deaktivuje nebo zruší. Kontrolu bude provádět Manažer PPÚ. Deaktivace nebo zrušení účtu bude reportováno a auditováno nástrojem ADAudit Plus.

4.2.5 Kontrola uživatelských účtů a rolí

Každému uživateli byla při jeho nástupu na pozici přidělena jedna z pěti rolí v AD. Avšak role se mohla během jeho pracovního poměru změnit. Taktéž přístupy a oprávnění se mohou individuálně povolovat a zakazovat, což se navíc nikde neauditуje. Z těchto důvodů doporučuji provést kontrolu všech uživatelských účtů v AD. Každý uživatel by měl mít roli odpovídající jeho aktuálním pracovním činnostem. Přístupy a oprávnění by měl mít pouze takové, které potřebuje pro výkon pozice, na druhou stranu by ho neměly omezovat.

Kontrola bude provedena po implementaci a zaběhnutí nástroje ADAudit Plus, jelikož by měl veškeré tyto činnosti auditovat. Kontrolu provedou pracovníci IT oddělení. Pokud si nebudou v některých případech jistí, je třeba konzultace s příslušným uživatelem, jeho nadřízeným a také s Manažerem PPÚ, který by měl spolu s příslušným nadřízeným všechny změny schválit. Taková kontrola by se měla opakovat v intervalu jedenkrát za rok.

Veškeré tyto opatření včetně jednotlivých rolí, které jsou nastavené v AD by se měly zavést do směrnice. O dokumentaci komunikace, řešení, schvalování a workflow se postará aplikace Service Desk. Veškeré provedené změny v AD budou reportovány a archivovány nástrojem ADAudit Plus. Směrnice by se měly v intervalu jedenkrát za rok přezkoumávat, zda odpovídá aktuálním potřebám. Každou změnu je třeba vždy schválit managementem společnosti a také uživatelé by měli být o každé změně informováni.

4.3 Systém vzdělávání zaměstnanců

Doporučuji zavést nový systém vzdělávání zaměstnanců v oblasti informační bezpečnosti. V současné době jsou zaměstnanci školeni při nástupu do společnosti a pak již nepravidelně nebo vůbec. Odpovědnost za školení ponese HR/Office manažer, který spolu s dalšími pracovníky HR bude školení evidovat, sledovat a zanese jej do směrnice. Školení budou provádět pracovníci IT oddělení a Manažer PPÚ. Tito pracovníci rozdělí zaměstnance do skupin podle úrovně nutných znalostí a každé této skupině přizpůsobí obsah školení. Dále vypracují veškeré potřebné studijní podklady. Zodpovědnost za rozdělení a přizpůsobení obsahu ponese Manažer PPÚ.

Zaměstnanci by měli být proškoleni v oblasti informační bezpečnosti, měli by být seznámeni se směrnicemi a politikami organizace v této oblasti. Z pohledu identity managementu by školení mělo obsahovat: novou politiku hesel, zásady správného používání hesel, způsoby, jak si vytvořit lehce zapamatovatelné heslo v souladu s politikou hesel, způsoby a pravidla odhlašování a přihlašování, dále zdůraznit, že heslo nesmí zaměstnanci sdělovat nikomu jinému a nesmí si ho nikam zapisovat, a že jsou povinni se odhlašovat při každém opuštění svého pracoviště. S odstupem několika dní je třeba ověřit znalosti pracovníků testem. V případě prokázání, že pracovník nedisponuje znalostmi, které by měl znát, by měl školení opakovat.

Školení by se mělo provádět vždy při nástupu nových zaměstnanců a mělo by se opakovat v intervalu jedenkrát za rok.

4.4 ADAudit Plus

Nástroj ADAudit Plus je popsán v analýze současného stavu a v příloze. Vlastníkem tohoto nástroje bude Manažer PPÚ, který bude zodpovědný za celý jeho životní cyklus. Instalaci, nastavení a provoz bude provádět IT technik, jehož přímým nadřízeným bude Manažer PPÚ, kterému bude reportovat. Následující tabulka popisuje, co všechno bude ADAudit Plus auditovat a monitorovat.

Tab. 1: ADAudit Plus – audit a monitoring

Název	Počet
Doménový řadič	3
Členský doménový server	3
Členský souborový server	1
Členský aplikační server	3
Členský databázový server	1
Členský terminálový server	3
Členský certifikační server	1
Členský zálohovací server	1
Pracovní stanice	230

Monitorovat se bude AD v reálném čase, uživatelé, skupiny, počítače, OU a GPO. Dále se bude auditovat přihlášení a odhlášení na stanici, vytvoření, změny, výmaz, přístup k souborům, budou se sledovat systémové události, události tiskáren a USB zařízení. Veškeré data se budou archivovat.

Upozornění na události se po nainstalování nakonfigurují v prostředí ADAudit Plus. Upozornění budou zasílány elektronickou poštou na firemní e-mail Manažera PPÚ a IT technika. IT technik bude e-maily studovat, reagovat na události a reportovat Manažerovi PPÚ. V případě nestandardní události se předpokládá spolupráce obou těchto pracovníků a příp. i dalších pracovníků IT oddělení. Doporučuji zakoupit edici Standard, která nabízí více než 200 předkonfigurovaných reportů.

Po nainstalování je třeba spustit ověřovací provoz, který bude trvat po dobu jednoho měsíce. V průběhu této doby by měla být věnována pozornost e-mailům a reportům a měly by být provedeny případné úpravy tak, aby nebylo reportováno a posíláno velké množství nerelevantních informací. Na druhou stranu by měly být posílány takové údaje, aby bylo možné v případě nestandardní události ihned reagovat. ADAudit Plus by měl být zanesen do směrnice. V případě nedostatku paměťové kapacity v důsledku ukládání reportů a auditních dat je doporučeno kapacitu rozšířit.

4.5 Časová náročnost a plán

Časová náročnost a plán slouží jednak k přehledu jednotlivých opatření a také určuje pořadí zavádění, aby jednotlivé opatření na sebe logicky navazovaly. Následující tabulka zobrazuje počty člověkohodin, které jsou potřebné na zavedení a dále na roční provoz.

Tab. 2: Časové náklady na zavedení

Název opatření	Jednorázový počet člh při zavedení	Roční počet člh
Školení uživatelů	26	24
ADAudit Plus	60	53
Politika hesel	2	1
Odpovědnosti a povinnosti	4	2
Uživatelské role	4	2
Kontrola uživatelských účtů a rolí	50	30
Odebírání přístupových práv	2	4
Schvalování rolí a přístupových práv	2	4
Celkem	150	120

U opatření školení uživatelů není započtená doba jednotlivých uživatelů, kteří budou školeni. U každého uživatele se předpokládá malé množství počtu hodin za rok, kdy se tato doba může zahrnout do jejich běžné pracovní doby.

Celkový odhadovaný čas vychází na 150 hodin jednorázově v rámci implementace a dále 120 hodin každoročně.

Opatření by měly být implementovány v pořadí, v jakém jsou uvedeny v tabulce. Jelikož pracovníci IT oddělení, kteří se jednotlivým opatřením budou primárně věnovat, nemají v rámci své pracovní doby dostatek potřebného času, doporučuji najmout dalšího pracovníka. Pracovníka doporučuju najmout v rámci dohod o pracích konaných mimo

pracovní poměr. Dohody jsou výhodné z hlediska nízkého počtu hodin potřebného na jednotlivá opatření.

Pracovník by měl mít IT vzdělání a alespoň krátkou praxi. Tento pracovník se po zaučení bude moci věnovat jednoduchým činnostem na IT oddělení, čímž sníží zatížení ostatních IT pracovníků. IT pracovníkům se následně uvolní potřebná doba na implementaci a provoz navržených opatření. Lze předpokládat náklady na nového pracovníka ve výši 225 Kč na hodinu, což v rámci jednorázového zavedení odpovídá 33750 Kč a dále 27000 Kč za rok. Nabízí se také varianta přesčasových hodin IT pracovníků, avšak zde by byla částka vyšší.

Po najmutí a zaškolení nového pracovníka se může začít s implementací. Předpokládá se, že pracovník nebude pracovat každý pracovní den. V případě rozvržení implementace na dva měsíce připadá na jeden pracovní týden přibližně 17 člověkohodin. Po dokončení implementace může pracovník dále pokračovat v občasném docházení do firmy tak, aby se pokryla poptávka ročního pracovního času potřebného na provoz návrhů, což odhadem vychází na 120 hodin.

4.6 Finanční zhodnocení

Kromě nákladů na lidské zdroje, které jsou uvedeny výše, je zde ještě nutno počítat s cenou licence Standard ADAudit Plus. Tu popisuje následující tabulka.

Tab. 3: Cena licence ADAudit Plus

Název	Počet	Roční poplatek v Kč
Doménový řadič	3	18 800
Souborový server	1	7 500
Členský server	13	16 300
Pracovní stanice	230	11 500
	Celkem	54 100

Následující tabulka zobrazuje celkové náklady na zavedení. Uvádí jak jednorázové náklady potřebné na implementaci, tak každoroční náklady.

Tab. 4: Celkové náklady na zavedení

	Jednorázové náklady v Kč	Roční náklady v Kč
Licence ADAudit Plus	54 100	54 100
Náklady na lidské zdroje	33 750	27 000
Celkem	87 850	81 100

Vzhledem k tomu, že obrat společnosti překračuje jednu miliardu Kč, vychází náklady na 0,009 % a 0,008 % obratu společnosti. Finanční částky jsou pro společnost přijatelné.

4.7 Přínosy zavedení návrhů

Mezi hlavní přínosy patří zvýšení informační bezpečnosti ve společnosti. Díky auditu a reportingu, který nabízí nástroj ADAudit Plus, získají pracovníci IT oddělení a management společnosti daleko větší přehled o aktivitách uživatelů. Zvýší se informovanost o tom, co, kdo a kdy dělal, čímž se zlepší kontrola v různých činnostech a procesech a také efektivita práce. Rozdělení povinností a odpovědností a nastavení správného workflow pomůže předcházením omylů a chyb a také díky jednotlivým kontrolám bude mít každý uživatel přesně taková oprávnění a přístupová práva, jaká potřebuje k výkonu své pozice.

ZÁVĚR

Cílem této bakalářské práce bylo navrhnout řešení na zlepšení v oblasti identity managementu.

V první části jsem zpracoval teoretická východiska, na které navazovala analýza současného stavu. V analýze jsem se věnoval tomu, jakým způsobem společnost řídí identity a spravuje přístupy, a jakým způsobem přistupuje k auditu dat. Na základě analýzy současného stavu byla navržena jednotlivá opatření.

Po analýze následovala část vlastní návrhy řešení. V návrhu změny politiky hesel jsem se věnoval jak složitosti, tak životnosti hesla. V návrhu změn řízení přístupu jsem se věnoval odpovědnostem a povinnostem za jednotlivé procesy, uživatelským rolím, schvalováním rolí a přístupových práv, odebíráním přístupových práv a kontrolou uživatelských účtů a rolí. Také byl navržen nový systém vzdělávání zaměstnanců v oblasti informační bezpečnosti a bylo navrhnuto, co by měl obsahovat z hlediska identity managementu. Nakonec jsem se věnoval zavedením nástroje ADAudit Plus pro monitorování a audit dat.

Návrhy řešení uzavíral časový plán a náročnost, finanční zhodnocení a přínosy zavedení návrhů. Mezi hlavní přínos se řadí zvýšení informační bezpečnosti.

SEZNAM POUŽITÝCH ZDROJŮ

(1) OSMANOGLU, T. Ertem. *Identity and access management: business performance through connected intelligence.* Amsterdam, [Netherlands]: Syngress, an imprint of Elsevier, 2013. ISBN 978-012-4081-406.

(2) SEMANČÍK, Radovan. Cesta k efektivnímu identity managementu (1. díl). *IT SYSTEMS* [online]. 2015, 1-2 [cit. 2016-09-14]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-identity-managementu-1-dil.htm

(3) LÍZNER, Martin. Identity management – centrální správa uživatelských účtů. *ComputerWorld* [online]. 2010 [cit. 2016-09-14]. Dostupné z: http://computerworld.cz/securityworld/identity-management-centralni-spravauzivatelskych-uctu-47568

(4) STANEK, William R. Active Directory: kapesní rádce administrátora. Brno: Computer Press, 2009. ISBN 978-80-251-2555-7

(5) SEMANČÍK, Radovan. Cesta k efektivnímu identity managementu (2. díl). *IT SYSTEMS* [online]. 2015, 3 [cit. 2016-09-14]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-identity-managementu-2-dil.htm

(6) HANÁČEK, P. a J. STAUDEK. Správa identity. Brno, 2005.

(7) SEMANČÍK, R. a K. VALALIKOVÁ. Cesta k efektivnímu identity managementu (3. díl). *IT SYSTEMS* [online]. 2015, 4 [cit. 2016-09-14]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/it-security/cesta-k-efektivnimu-identity-managementu.htm

(8) BERTINO, E. a K. TAKAHASHI. Identity management: Concepts, Technologies, and Systems. Boston: Artech House, 2011. ISBN 978-1-60807-039-8.

(9) LÍZNER, Martin. Identity management zjednodušuje správu uživatelských účtů (3). *ComputerWorld* [online]. 2010, 4 [cit. 2016-09-14]. Dostupné z: http://computerworld.cz/securityworld/identity-management-zjednodusujespravu-uzivatelskych-uctu-3-47977

(10) NORIS, Ivan. Cesta k efektivnímu identity managementu (4. díl). *IT SYSTEMS* [online]. 2015, 5 [cit. 2016-09-14]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-idm-provisioning.htm

(11) OSMANOGLU, T. E., R. ALLEN a A. G. LOWE-NORRIS. Active Directory: implementace a správa Microsoft Active Directory. Praha: Grada, 2005. ISBN 80-247-0973-2.

(12) VOHNOUTOVÁ, Marta. Identity a access management. *IT SYSTEMS* [online]. 2008, 11 [cit. 2016-09-14]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/identity-a-access-management-1.htm

(13) SEMANČÍK, Radovan. Cesta k efektivnímu identity managementu (5. díl). *IT SYSTEMS* [online]. 2015, 6 [cit. 2016-09-14]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/cesta-k-efektivnimu-idm-architektura-iam-reseni.htm

(14) WATERS, J. K. a P. KHUDHUR. Správa identit pod lupou. *ComputerWorld* [online]. 2009 [cit. 2016-09-14]. Dostupné z: http://computerworld.cz/securityworld/sprava-identit-pod-lupou-45276

(15) SEMANČÍK, R. a I. NORIS. Cesta k efektivnímu identity managementu (6. díl). *IT SYSTEMS* [online]. 2015, 7-8 [cit. 2016-09-14]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/it-security/cesta-k-efektivnimu-idm-pokrocile-technologie.htm

(16) MALINKA, K. *Kryptografie* (přednáška). Brno: VUT v Brně, Fakulta podnikatelská, 20. 10. 2015.

(17) KREJČÍ, Jan. Správa identity. *IT SYSTEMS* [online]. 2008, 1-2 [cit. 2016-09-14]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/sprava-it/sprava-identity.htm

(18) MICROSOFT. *Active Directory* [přístup 25. října 2016].

(19) ManageEngine: ADAudit Plus. ManageEngine: ADAudit Plus [online]. [cit. 2016-11-07]. Dostupné z: https://www.manageengine.com/products/active-directory-audit

(20) WATERS, J. K. a P. KHUDHUR. Abeceda identity managementu. *CIO Business World* [online]. 2008 [cit. 2016-09-17]. ISSN 1803-7321. Dostupné z: http://businessworld.cz/bezpecnost-a-rizeni-rizik/abeceda-identitymanagementu-1390

(21) Reports, Features and benefits of ManageEngine ADAudit Plus. ManageEngine: ADAudit Plus [online]. [cit. 2016-11-07]. Dostupné z: https://download.manageengine.com/products/active-directory-audit/ad-audit-plus-features-reports.pdf

(22) ManageEngine ADAudit Plus: A detailed walkthrough. ManageEngine: ADAudit Plus [online]. [cit. 2016-11-07]. Dostupné z: https://download.manageengine.com/products/active-directory-audit/ADAuditPlus-a-detailed-walkthrough.pdf

(23) ADAudit Plus Quick Start Guide [online]. [cit. 2017-04-12]. Dostupné z: https://download.manageengine.com/products/active-directory-audit/adaudit-plus-quick-start-guide.pdf

(24) DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

(25) POŽÁR J. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

(26) ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 369790.

(27) ČSN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017. Třídící znak 369790.

(28) ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 369797.

(29) ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017. Třídící znak 369797.

(30) ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 369798.

(31) ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.* Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017. Třídící znak 369798.

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

AD	Active Directory
ČLH	Člověkohodina
DNS	Domain Name System (Systém doménových jmen)
GPO	Group Policy Objects (Objekty zásad skupiny)
HR	Human Resources (Lidské zdroje)
IAM	Identity and Access Management (Management identit a přístupů)
IP	Internet Protocol (Protokol IP)
IT	Information Technology (Informační technologie)
LDAP	Lightweight Directory Access Protocol (Protokol LDAP)
OU	Organizational Unit (Organizační jednotka)
PKI	Public Key Infrastructure (Infrastruktura veřejných klíčů)
PPÚ	Procesně provozní útvar
RBAC	Role Based Access Control (Řízení přístupu založené na rolích)
RPC	Remote Procedure Call (Vzdálené volání procedur)
SSO	Single Sign-On (Systém jednotného přihlášení)

SEZNAM OBRÁZKŮ

Obr. 1: Centrální správa uživatelských účtů a přístupů 13
Obr. 2: Životní cyklus identity 15
Obr. 3: Práce s adresářovými službami 21
Obr. 4: Objekty a atributy ve službě Active Directory 23
Obr. 5: Doména služby Active Directory 24
Obr. 6: Organizační struktura. 27
Obr. 7: Správa zásad skupiny 31
Obr. 8: Politika hesel 33
Obr. 9: Zabezpečení pro notebooky 34

SEZNAM TABULEK

Tab. 1: ADAudit Plus – audit a monitoring.....45
Tab. 2: Časové náklady na zavedení.....46
Tab. 3: Cena licence ADAudit Plus.....47
Tab. 4: Celkové náklady na zavedení.....48

SEZNAM PŘÍLOH

Příloha 1: Audit a reporty ADAudit Plus……...……..i
Příloha 2: Dostupné edice ADAudit Plus……..……..v
Příloha 3: Systémové požadavky, instalace a nastavení ADAudit Plus……...……vii

Příloha 1: Audit a reporty ADAudit Plus

ADAudit Plus poskytuje celou řadu reportů, které jsou zařazeny do 9 kategorií.

Reporty uživatelských přihlášení

Tato kategorie reportů poskytuje informace o všech přihlášeních, které jsou zaznamenány v nakonfigurovaných řadičích domén.

Reportovány jsou přihlašovací informace konkrétního uživatele v doméně, přihlášení do konkrétního počítače a poslední přihlášení z pracovní stanice. Patří zde:

- chybné přihlášení,
- přihlašovací aktivita na řadiči domény,
- přihlašovací aktivita na členském serveru,
- přihlašovací aktivita na pracovní stanici,
- přihlašovací aktivita uživatele,
- nedávná přihlašovací aktivita uživatele,
- poslední přihlášení na pracovních stanicích,
- poslední přihlášení uživatele (21).

Místní přihlášení a odhlášení

Tato kategorie zobrazuje reporty, které jsou závislé na místních přihlašovacích auditních datech. ADAudit Plus poskytuje místní přihlašovací údaje pro řadiče domény a členské servery. Patří zde:

- doba trvání přihlášení,
- chybné přihlášení,
- historie přihlášení,
- aktivita terminálových služeb (21).

Management účtů

Tato kategorie reportů audituje administrátorské činnosti. Patří zde:

- management uživatele,
- management skupiny,
- management počítače,
- management OU,
- management GPO (21).

Management uživatelů

Tato kategorie reportů umožňuje audit všech nedávno vytvořených, odstraněných nebo modifikovaných uživatelů v doméně. Patří zde:

- nedávno vytvoření uživatelé,
- nedávno odstranění uživatelé,
- nedávno povolení uživatelé,
- nedávno zakázaní uživatelé,
- nedávno uzamčení uživatelé,
- nedávno odemčení uživatelé,
- nedávná změna uživatelských hesel,
- nedávná nastavení uživatelských hesel,
- nastavení uživatelů trvale platných hesel,
- nedávno modifikovaní uživatelé,
- poslední změna v uživatelích,
- uživatelské administrativní činnosti,
- historie uživatelských objektů (21).

Management skupin

Tato kategorie umožňuje auditovat vytváření, odstraňování a modifikaci všech skupin zabezpečení a distribučních skupin v doméně. Zahrnuto je zde také přidávání a odstraňování členů do a z těchto skupin. Patří zde:

- nedávno vytvořené skupiny zabezpečení,
- nedávno vytvořené distribuční skupiny,
- nedávno odstraněné skupiny zabezpečení,
- nedávno odstraněné distribuční skupiny,
- nedávno modifikované skupiny,
- nedávno přidaní členové do skupin zabezpečení,
- nedávno přidaní členové do distribučních skupin,
- nedávno odstranění členové ze skupin zabezpečení,
- nedávno odstranění členové z distribučních skupin,
- historie objektů skupin (21).

Management počítačů

Tato kategorie se zabývá auditem počítačových objektů v síti. Reportována je každá akce od vytvoření počítačového objektu až k jeho odstranění. Dokonce i provedené změny na počítačovém objektu jsou zaznamenávány a reportovány. Do této kategorie spadá kompletní historie modifikací provedených na jednom nebo více počítačových objektů. Patří zde:

- nedávno vytvořené počítače,
- nedávno odstraněné počítače,
- nedávno modifikované počítače,
- nedávno povolené počítače,
- nedávno zakázané počítače,
- historie počítačových objektů (21).

Změny zásad domény

Auditovány a reportovány jsou změny v politice účtů a změny v politice hesel. Patří zde:

- změny zásad domény (21).

Management OU

Auditována a reportována je každá změna vztahující se k vytvoření, odstranění nebo modifikaci organizační jednotky. Reportovány jsou také auditní data v historii změn organizačních jednotek. Patří zde:

- nedávno vytvořené organizační jednotky,
- nedávno odstraněné organizační jednotky,
- nedávno modifikované organizační jednotky,
- historie organizačních jednotek (21).

Management GPO

Vytvoření Objektů zásad skupiny, jejich odstranění a modifikace mohou být auditovány včetně reportů spadajících do této kategorie. Reportovány jsou také auditní data v historii změn Objektů zásad skupiny. Patří zde:

- nedávno vytvořené GPO,
- nedávno odstraněné GPO,
- nedávno modifikované GPO,
- historie GPO (21).

Příloha 2: Dostupné edice ADAudit Plus (19)

Verze a cena	Popis
Free od 0 USD za rok	bez časového omezení
	25 pracovních stanic
	reporty mohou být generovány jen po dobu trial periody
Trial od 0 USD za rok	všechny funkce edice Professional po 30 dní bez omezení
	Možnost auditovat: 5 řadičů domény 2 souborové servery 1 NetApp Filer/1 EMC souborový server 10 serverů 100 pracovních stanic
Standard od 495 USD za rok	200+ předkonfigurovaných reportů
	monitoring Active Directory v reálném čase
	monitoring uživatelů, skupin, počítačů, OU a GPO
	audit přihlášení/odhlášení na stanici
	vytvoření/změny/výmaz/přístup k souborům
	sledování systémových událostí
	audit událostí tiskáren a USB zařízení
	reporty souladu s legislativními předpisy
	archivace dat

Professional od 795 USD za rok	všechny funkce Standard edice
	audit změn GPO
	sledování původních a nových hodnot změněných atributů AD
	změny přístupových práv k AD
	analyzátor zamčení účtů
	audit událostí DSN serveru, schématu AD, kontaktů a změn konfigurace
	podpora databáze MS SQL

Příloha 3: Systémové požadavky, instalace a nastavení ADAudit Plus (23)

Systémové požadavky

ADAudit Plus může být nainstalován na jakémkoliv zařízení v doméně s následujícími systémovými požadavky:

Doporučené hardwarové požadavky:

- procesor: P4 - 1.5 GHz nebo lepší,
- RAM: 2 GB nebo vyšší,
- místo na disku: 20 GB.

Další místo na disku využité databází se bude lišit v závislosti na počtu uživatelů, souborů a zachycování auditních událostí.

Softwarové požadavky

Podporované operační systémy

ADAudit Plus může být nainstalován a spuštěn na následujících verzích OS Windows: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 2003 Server, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012 a Windows Server 2012 R2.

Podporované prohlížeče

ADAudit Plus požaduje jeden z následujících prohlížečů k nainstalování v systému: Internet Explorer 6 a vyšší, Firefox 2.0 a vyšší nebo Chrome. Preferované rozlišení obrazovky 1024 x 768 pixelů nebo vyšší.

Podporované platformy

Active Directory 2003 a vyšší, Windows File Server 2003 a vyšší, NetApp Filer - Data ONTAP 7.2 a vyšší, Windows Failover Cluster se SAN.

ADAudit Plus může být nainstalován na jakémkoliv počítači v síti a lze k němu přistupovat z jakéhokoliv klientského počítače v síti použitím webového prohlížeče.

Instalace a nastavení

ADAudit Plus je dodáván ve formátu exe a lze si ho stáhnout prostřednictvím tohoto webového odkazu: https://www.manageengine.com/products/active-directory-audit/download.html?topMenu. Po stáhnutí a nainstalování edice Trial, která nabízí veškeré funkce edice Professional po dobu třiceti dní a zakoupení edice Standard bude licence dodána prostřednictvím e-mailu ve formátu XML.

Spuštění ADAudit Plus jako službu Windows:

- Stop ADAudit Plus (Start -> Všechny programy -> ADAudit Plus -> Stop ADAudit Plus),
- otevřít příkazový řádek (Pravým kliknutím -> Spustit jako správce - v případě Windows server 2008),
- jít do instalační složky ADAudit Plus\Bin (např: C:\Program Files (x86)\ManageEngine\ ADAudit Plus\bin),
- spustit "InstallNTService.bat",
- otevřít services.msc -> "ManageEngine ADAudit Plus" Service -> Pravým kliknutím -> Properties,
- kliknout na "Log on" záložku and vybrat "This Account" a poskytnout přihlašovací údaje (pokud je to možné, použít administrátorský účet),
- začít s ADAudit Plus.

Potřebné otevřené porty

Pro sběr událostí:

- port 389 pro komunikaci s protokolem LDAP,
- port 135 pro komunikaci s RPC,
- port 445 a 135 pro komunikaci s NetBioS Session Service.

Pro přístup k ADAudit Plus:

- http: 8081,
- https: 8444.

Konfigurace zásad auditu

Zásady auditu musí být nakonfigurovány v jakémkoliv prostředí AD. Tím je zajištěno, že jsou zaznamenávány relevantní auditní data do bezpečnostních logů požadovaných počítačů nebo řadičů domén. ADAudit Plus bude schopen shromažďovat a reportovat auditní data pouze pro počítače dle zásad auditu.

K auditování AD:

- musí být nakonfigurován výchozí řadič domény,
- mělo by být povoleno objektové auditování.

K auditování souborových serverů:

- zásady auditu musí být nakonfigurovány pro konkrétní souborové servery, odkud je vyžadován audit dat,
- mělo by být povoleno objektové auditování.

K auditování členských serverů: zásady auditu musí být nakonfigurovány pro konkrétní členské servery, odkud je vyžadován audit dat.