VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

IDENTITY AND ACCESS MANAGEMENT VE SPOLEČNOSTI A NÁVRH NA JEHO ZLEPŠENÍ
CORPORATE IDENTITY AND ACCESS MANAGEMENT SUGGESTION FOR IMPROVEMENT

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — **Jiří Valtr**
AUTHOR

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

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání bakalářské práce

Ústav:	Ústav informatiky
Student:	**Jiří Valtr**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Manažerská informatika
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2019/20

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:

Identity and access management ve společnosti a návrh na jeho zlepšení

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:

Navrhnout management bezpečnosti.

Základní literární prameny:

ALDHIZER III, G. R., P. E. JURAS a D. R. MARTIN. Using Automated Identity and Access Management Controls. CPA Journal [online]. 78(9), 66-71 [cit. 2019-10-28]. 2008. ISSN 07328435. Dostupné z: Databáze EBSCOhost

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

ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

POŽÁR J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

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

YOUNG, D. Human Resources have a vital role to play within employee identity and access management. Network Security [online]. 2004(11), 5-7 [cit. 2019-10-28]. DOI: 10.1016/S1353-4858(04)00154-0. ISSN 13534858. Dostupné z: https://www-sciencedirec--com.ezproxy.lib.vutbr.cz/science/article/pii/S1353485804001540

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

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

ABSTRAKT

Tato bakalářská práce pojednává o problematice správy a řízení identit a přístupů ve společnosti. Jejím cílem je navrhnout možná řešení, která přispějí ke zlepšení celkového identity managementu firmy nebo jeho dílčím částem a tím i k celkové firemní IT bezpečnosti.

ABSTRACT

This bachelor thesis deals with the issue of control and management of identities and access in company. Its goal is to propose possible solutions that will contribute to the improvement of the overall identity management of the company or its parts and thus to the overal corporate IT security.

KLÍČOVÁ SLOVA

Správa a řízení přístupů a rolí, autorizace, autentizace, politika hesel, ICT bezpečnost

KEYWORDS

Identity and access management, authorization, authentization, password policy, ICT security

BIBLIOGRAFICKÁ CITACE

VALTR, J. *Identity and access management ve společnosti a návrh na jeho zlepšení*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2020. 48 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 11. května 2020 ……

podpis studenta

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu mé bakalářské práce Ing. Viktoru Ondrákovi, Ph.D. za jeho odborné vedení, rady a připomínky a dále všem, kteří mi jakoukoliv formou pomohli k tvorbě této práce.

OBSAH

ÚVOD

V posledních letech ve společnostech výrazně narůstá počet systémů napříč různými typy technologických platforem. Tento trend s sebou nese spoustu nevýhod. Jednou z nich je velké množství hesel do různých aplikací a systémů, které si musí uživatelé zapamatovat a které se stále vyššími požadavky na bezpečnost, vyžadují hesla stále složitější. To vede k riziku, že je uživatelé zapomenou, nebo si je někam zaznamenají, což bezpečnost výrazně snižuje. Navíc každý jednotlivý systém může mít odlišné způsoby řízení identit a jejich oprávnění a ve výsledku už se zdá být nemožným, řešit vše ručně. Manuální správa přístupů pak pro firmu představuje velké náklady na čas, zaměstnance a tím pádem i na finance.

Zavedení služby pro správu a řízení identit ve firmě se tedy stává stále častějším řešením. Identity and Access management (IAM) je dnes již klíčovou oblastí v IT bezpečnosti firmy. Představuje efektivní způsob řízení identit díky centralizaci firemních systémů a jejich účtů.

V mé bakalářské práci přednesu návrhy změn v oblasti řízení identit ve společnosti IFE – CR, a.s. Především se zaměřím na personální bezpečnost, firemní politiku hesel a organizační strukturu.

1 CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

1.1 Cíle práce

Cílem této práce je navrhnout úpravy a vylepšení pro systém správy a řízení přístupů a identit ve vybrané společnosti, které povedou k celkovému zlepšení firemní bezpečnosti ICT. Nejprve je třeba vysvětlit teoretické pozadí, nutné k porozumění problematiky identity managementu. Společnost bude podrobena analýze zaměřené na systém přístupů a následně bude vypracován návrh, sestávající se z dílčích návrhů na změny v jednotlivých oblastech bezpečnosti ICT.

1.2 Metody a postupy zpracování

Při zpracování jsem postupoval primárně dle doporučení odborníků z praxe. Klíčové byly především znalosti nabyté v teoretické části a výsledky analýzy společnosti, které odhalily nedostatky v její bezpečnostní struktuře. Metodika vypracování návrhů se odvíjela od každého problému zvlášť, ovšem s ohledem na celkový kontext zahrnující jak ekonomickou stránku řešení, tak důležitost, uskutečnitelnost nebo rizika spojená s metodou. Některé výsledky jsou prezentovány v podobě možných variant řešení s doporučením pro jednu z nich.

2 TEORETICKÁ VÝCHODISKA

V této části bakalářské práce Vás seznámím s jednotlivými teoretickými znalostmi, které budou využity v analýze současného stavu i při návrhu řešení.

2.1 Identity and access management

Identity and access management (IAM) je důležitá oblast především pro střední a větší firmy, která prostřednictvím řízení životních cyklů identit napomáhá se automatizováním a zrychlováním procesů, zvyšováním interní firemní bezpečnosti a umožňuje lepší přípravu na audity nebo jiné kontroly. Skládá se ze dvou stěžejních oblastí. První je oblast, zabývající se centrální správou a řízením identit a uživatelských účtů v organizaci, případně mimo organizaci u partnerů nebo prostřednictvím cloudu. Druhou nezbytnou součástí je správa a řízení rolí, přístupů a oprávnění, která se na identitu vážou. [1]

2.2 Identita

Identita je soubor atributů, přidružených k určité entitě. Nejčastěji k osobě, lze přiřadit i ke zvířeti, hardwaru, k právnické osobě atd. Tyto atributy musí entitu jednoznačně a nezaměnitelně charakterizovat. [5]

2.2.1 Životní cyklus identity

Každá identita během své existence projde životním cyklem. Dle tradičního modelu má životní cyklus identity 4 fáze. Založení, používání, upravování a zrušení. Vzhledem k neustále se rozvíjejícím metodikám identity managementu se založení rozděluje na dvě další části a upravování se stává méně častou činností. Důvodem je fakt, že většina firem dnes přístupy neuděluje napřímo identitě. Také se stává využívanou funkcí pozastavení. [1, 5]

2.2.1.1 Provisioning, vytvoření

Provisioning (zřizování, přidělování) znamená tvorbu verifikované identity, která tímto vstoupí do tzv. životního cyklu. Provádí se výhradně prostřednictvím informačního systému. Výstupem tohoto procesu je založení účtu identity v systému IAM a jeho následné promítnutí do ostatních systémů, v nichž je identita k řízení přístupu potřebná. [5]

Provisioning se skládá z několika dílčích kroků:

- Prokazování atributů mezi autoritami
- Vydávání ověřujících údajů (certifikát, klíč, atd.)
- Formování identity (z atributů, identifikátorů a ověřujících údajů) [5]

2.2.1.2 Provisioning zdrojů

Jedná se o přiřazení identity službám i systémům, ke kterým má na základě svých oprávnění přístup. Například místo na sdíleném disku, mailová schránka, přístup k intranetu, nebo i hardware, jako je přiřazení pracovního notebooku, auta, stolu nebo mobilního telefonu. [1, 5]

2.2.1.3 Používání

Jde o fázi samotného provozu. Identity se využívají při práci pouze jako nosiče atributů. Mají klíčovou funkci při přístupech do informačních systémů. V závislosti na modelu přiřazování přístupů se ale jejich využívání liší. Například, zda se na ně, v průběhu času, vážou různé role, či nikoliv. [1]

2.2.1.4 Úprava

Změny v identitě se provádějí zejména z důvodu potřeby změn údajů o osobě, (bydliště, rodinný stav, změna jména, vzdělání apod.) ale také z důvodů právních, organizačních nebo bezpečnostních (fúze společností, změna úrovně požadované důvěryhodnosti či podezření z podvodu). Aktualizací dat se zajistí jejich integrita. [1, 5]

2.2.1.5 De-provisioning

Musí být proveden pohotově hned po odchodu zaměstnance ze zaměstnání. De-provisioning znamená zrušení přiřazení identity přidruženým systémům a službám. Proces také případně zahrnuje relokaci uvolněných aktiv mezi volná aktiva. Umožňuje lepší využívání zdrojů a zabraňuje možnému zneužití identity. [1, 5]

2.2.1.6 Pozastavení / obnovení

Pozastavením se rozumí dočasné zastavení působení identity jako platného zdroje pro autorizaci vyplývající z jejich rolí / atributů. Využívá se například v době překládání pracovníka na jiný projekt, z důvodů vyšetřování nebo během úrazu, či dovolené. Obnovení je opačný proces pozastavení. [1, 5]

2.3 Řízení identit

Je potřebné pro monitorování všech identit i s jejich atributy a životními cykly, které v systému existují. Na základě řízení identit staví přidělování rolí. Identity se dají běžně rozdělit na interní a externí. [2]

2.3.1.1 Zaměstnanci

Pracovníci různých typů pracovních úvazků spadají pod interní identity. Jedná se o takzvaný B2E model (Business-to-Employee). Nejčastěji vznikají na základě činnosti personálního oddělení firmy. Kromě základního souboru oprávnění, které jim umožňují pracovat se základním informačním systémem společnosti jsou jejich přístupy typicky řízené pomocí přidělování rolí. O oprávnění si uživatelé žádají většinou prostřednictvím vedoucího pracovníka, nebo sami. [2]

2.3.1.2 Dodavatelé

Externí identity představují subjekty z B2B sféry (Business-to-Business). Dodavatelé, partneři a zákazníci. B2B identity jsou v interních systémech (např v LDAP serveru) organizačně odděleni od identit interních. Jejich oprávnění jsou spravovány kompetentní osobou na straně společnosti, která vyřizuje žádosti o oprávnění apod. Vzhledem k tomu, že se může stát, že identity zůstanou v systémech i po skončení projektu, jsou proto předmětem bezpečnostních auditů. [2]

2.3.1.3 Zákazníci

Zákazníci neboli B2C (Business-to-Customers) jsou druhou skupinou externích identit. Je pro ně specifické mít přístup pouze do jednoho izolovaného systému, kam se sami registrují. Tedy nejsou běžnou bezpečnostní hrozbou. Jsou ovšem případy, kdy zákazník dostává certifikát nezávisle na jeho registraci a teprve poté se páruje pro potřeby autentizace. Také se dnes čím dál hojněji využívá koncept BYOID (Bring Your Own Identity), kdy se zákazníci přihlašují do systému svou externí identitou například z Facebooku nebo Googlu. Proto je tedy model B2C také zohledňován v IAM. [2, 4]

2.4 Řízení oprávnění

Největší součástí je tzv. schvalování workflow, neboli proces, který předem definovaným způsobem umožní uživateli schválení žádosti o oprávnění. Do procesu vstupují linioví pracovníci (vedoucí) gestoři rolí a bezpečnost ICT. Linioví pracovníci v tomto případě představují jakýsi první stupeň filtru žádostí o oprávnění, kteří rozhodnou, zda je žádost relevantní či nikoliv. Gestoři rolí zase lépe znají význam dané role a jsou schopni lépe posoudit, zda má uživatel na přístup oprávnění nárok. Poslední pracovníci se zabývají otázkou, zda dané oprávnění může být přiděleno, aniž by ohrozilo bezpečnost ICT firmy. Důležitou součástí je i evidování a případně následné reportování přehledů o tom, kdo má kam přístup, kdo mu jej udělil a kdy. [2, 13]

2.5 Přidělování oprávnění

Existují tři známé způsoby, kterými lze identitě přiřadit oprávnění:

2.5.1 Přímé přidělování

Uživateli je přístup přidělen napřímo. Je svázán s jeho identitou a dokud není zažádáno o jeho odebrání, bude platný. V praxi to přináší jisté nevýhody. Přístupy každého jednotlivce zvlášť takto vyžadují individuální pozornost a v průběhu let, při kariérním postupu zaměstnance, pokud vystřídá několik pozic ve velké firmě, se takto velice snadno kumulují další a další přístupy. V praxi je totiž velice obtížné vyřešit předávání odpovědnosti za revalidating oprávnění uživatele (a případně za jejich rollback) z jednoho nadřízeného na jiného. Zvláště, pokud jde o nově vzniklá pracovní místa, nebo když se sám zaměstnanec stane oním nadřízeným. Ve výsledku má pak uživatel mnohem větší počet oprávnění, než kolik mu momentálně náleží. [3]

2.5.2 RBAC

(RBAC neboli Role Based Access Control) Řeší některé problémy přímého přidělování. V principu se k uživateli s identitou svážou role, kdy každá role nese svoji vlastní sadu oprávnění. Po změně pozice se uživateli automaticky role změní. Momentálně je RBAC nejvyužívanějším systémem ve společnostech. Tento systém má také svá úskalí. Při dlouhodobém nedůsledném využívání se ve velký společnostech nakumulují desetitisíce rolí, které se od sebe liší jen minimálně, Třeba jen různou kombinací atributů uživatele. Systém je pak nepřehledný. Podněcuje k vytváření dalších rolí, namísto hledání již existujících, v horším případě je zahlcen. Tento stav se musí řešit procesem zvaným Role Mining. [3, 16]

2.5.3 ABAC

(ABAC neboli Attribute Based Access Control) přiřazuje přístupy na základě atributů, které má každá identita. Například, kdyby pracovník pracoval na vytěžování dat z konkrétní firemní databáze, je v interním systému na řízení projektů zařazen do projektu datamining, což je atribut, jež mu povoluje mu přístup do databáze. V Identity Manageru můžeme stanovit i další podmínky, jako například, že aktuální datum musí být menší, než předpokládaný konec projektu, atp. Tyto podmínky stanovuje gestor. [3]

2.6 Řízení rolí

Ve většině případů, kdy firma řeší oprávnění pomocí přidělování rolí, je potřeba tyto role spravovat, monitorovat a někde uchovávat. V principu je můžeme uchovávat na jakémkoliv strukturovaném umístění, třeba i v excelové tabulce. Ovšem musíme zajistit, aby k nim IAM systém měl přístup. [3]

2.7 Řízení přihlášení

Nastává, jakmile už má uživatel svou identitu, správnou roli a chce vstoupit do systému. Řízení přihlášení obstarává distribucí potřebných údajů napříč systémem potřebným k provedení ověření uživatele. Tedy, aby mohla být provedena autorizace a autentizace. Využívá se nejčastěji heslo / pin / certifikát pro autentizaci a pro autorizaci pak role / skupina / atribut. Použita může být i identifikace uživatele u jiného poskytovatele, má-li firma tuto službu poskytovanou externě. [2] Existují však i jiné pokročilé metody řízení přihlášení. Například RAdAC (Risk-Adaptable Acces Control), který rozhodne o autorizaci na základě dynamického posouzení rizik. Posuzuje, kromě vpouštění uživatelů do systému, jaké podmínky pro vpouštění stanoví. Tedy jak se bude autentizovat, jaké parametry budou k přístupu potřeba atp. Po samotném přístupu se následně vytvoří záznam v log listu. [4]

2.7.1 Autentizace

Slouží k ověřování, zda uživateli opravdu patří daná identita. [13] Využívají se tři základní způsoby a často i jejich kombinace:

„Něco, co vím“ - heslo, pin, odpověď na verifikační otázku atd.
„Něco, co mám“ - klíč, karta, USB token, mobilní telefon atd.
„Něco, co jsem“ - biometriky postavy. Nejčastěji otisky prstů a skeny sítnic. Dají se ale využít i vzorky DNA, otisky rtů a zubů, sken stylu chůze a jiné pokročilé (experimentální) metody. [6]

V případě kombinace uvedených způsobů autentizaci pak hovoříme o MFA (Multi-Factor Authentization). V praxi se nejčastěji setkáváme s dvoufázovou autentizací v podobě hesla / pinu + klíče zaslaného na mobilní zařízení nebo USB tokenu. [4, 7]

V případě využívání pokročilých metod RAdAC (viz. 2.7) se způsob používané autentizace nazývá RBA (Risk Based Authentization). Tento systém může například

vyžadovat dodatečné požadavky autentizace v případě, že detekuje místo přihlášení odlišné od posledního místa. Například pomocí IP adresy. [7]

2.7.2 Autorizace

Je dle definice samotný proces získávání přístupu. Pojmem autorizace se typicky označuje vlastní získaný přístup. Tedy, jsem-li autorizován, mám povolení přístupu. Autorizace může podléhat nejen atributům / rolím či oprávnění identity, ale také vnějším podmínkám, jako například denní době, stavu systému (zda neprobíhá maintanance) nebo dle místa přístupu. (Např. zákaz přístupu z Číny.) [4]

2.7.3 Single sign-on

V důsledku narůstající početnosti systémů, ke kterým má uživatel přístup, postupně volí slabší, lehce zapamatovatelná hesla, nebo hesla opakuje. Tím se snižuje bezpečnost. Abychom předešli tomuto jevu a také pro zvýšení uživatelského komfortu byl navržen dnes již hojně využívaný koncept jednotného přihlášení Single Sign-on (SSO). Pomocí něj se dá přistupovat k více službám na základě jedné autentizace. SSO neslučuje přihlašovací údaje všech účtů, pouze vytvoří nadřazený účet, který slouží jako garant správné autentizace všech lokálních účtů. Opakem SSO je Single Sign-off. Jednotné odhlášení, kdy po automatickém odhlášení nadřazeného účtu se odhlásí i všechny přidružené aplikace. [4]

2.8 Active Directory

Active directory Domain Services je adresářová služba od společnosti Microsoft Corporation dostupna pro OS Windows 2000 a novější. Služba funguje na bázi klient – server a běží na LDAP protokolu, takže jednotlivé položky na serveru ukládá a uspořádává do stromové struktury (viz. níže). Ochranu dat zajišťuje protokol Kerberos. Hlavní součástí je autentizace a autorizace klienta. Active directory ověřuje uživatele a počítače vůči doméně a spravuje politiky členských počítačů. Existují i jiné adresářové

služby. Například eDirectory od firmy Novell nebo Open Directory od společnosti Apple. AD od Microsoftu je ale v současnosti výrazně nejpoužívanější adresářovou službou. [10]

2.8.1 DNS

Domain Name Systém (DNS) je pro funkci Active Directory klíčovou službou. Je to standart zahrnutý v TCP/IP a jeho funkce spočívá v překládání jmen objektů na IP adresy. Jména objektů se nazývají doménová jména a většinou jsou jimi jména hostitelů (hostname). DNS umí i opačnou funkci, tedy překlad IP adres na doménová jména, což se využívá například pro poštovní služby.
DNS služba většinou běží na dedikovaném DNS serveru a využívá tabulky IP adres a domén aktualizovanou téměř v reálném čase. [9]

2.8.2 Doménové řadiče

Domain controller (DC) je server zodpovědný za autentizaci požadavků v rámci domén. Je na něm uložený adresář služby AD DS a kontroluje veškeré interakce uživatelů a adresáře. Každá doména může pracovat s více řadiči, ale jednotlivé objekty jsou vždy řazeny pod jediný řadič. [8, 10]

2.8.3 Struktura active directory

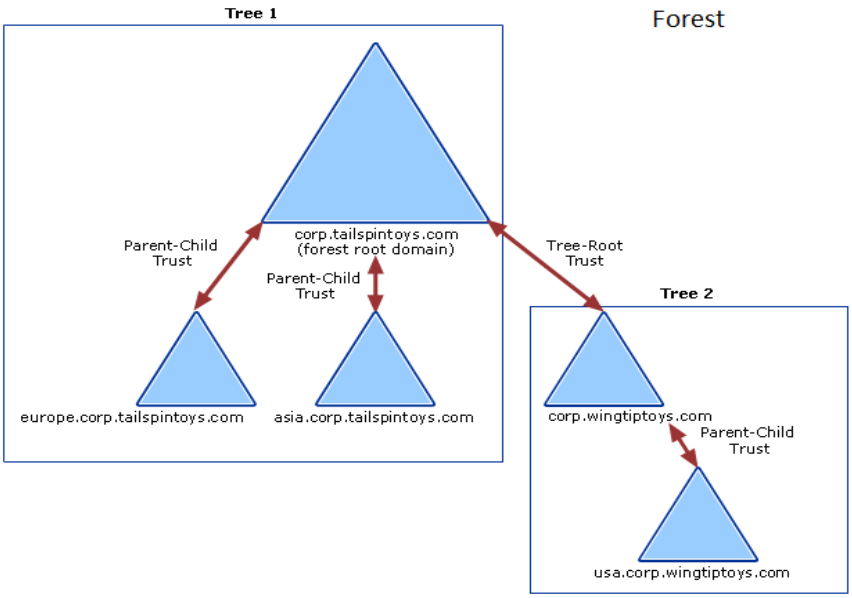
Active directory používá řízení síťových elementů několika úrovňovou strukturou, skládající se z domén, stromů a lesů.

Doména představuje logické seskupení objektů. Tvoří ji všechny v ní obsažené objekty, které sdílejí stejné umístění. Například počítače, uživatelé, tiskárny atd. Každá doména má název DNS (domena.local). Doména se může rozprostírat přes vícero fyzických míst. AD je tvořena jednou nebo více doménami. [8, 10]

OU (Organizational Unit) neboli Organizační jednotka je kontejner využívaný v rámci domény k seskupování / organizování objektů do skupin. Jejich vnořováním do sebe si tak lze vytvořit vlastní organizační strukturu. Ta je ale pouze lokální a neovlivňuje jiné domény, než ve které je hlavní OU umístěna. Obvykle je tvořena dle organizační struktury firmy a dle jejich potřeb. [8, 10]

Strom je jedna nebo více domén, spojených do logické hierarchické struktury. Lze jej chápat i jako prostor tranzitivních vztahů, ve kterém se sdílí informace o bezpečném připojení a důvěrnosti mezi jednotlivými doménami. Tedy pokud první doména důvěřuje druhé a druhá třetí, pak i první doména důvěřuje třetí. (Parent-child-trust) Hierarchická struktura domén ve stromu znamená, že má-li naše kořenová doména například jméno domena.local, budou všechny její podřazené domény toto jméno obsahovat. Podražená doména se pak může jmenovat například podrazena.domena.local. [8, 10]

Les je pak seskupení jednoho a více stromů, nebo kombinací stromů a domén. Skládá se ze sdílených globálních katalogů, adresářového schématu, a konfigurace domén. Schéma určuje třídy jednotlivým objektům v lese a globální katalog poskytuje výpis všech objektů v lese obsažených. Důvěrnost komunikace v rámci stromů je zajištěna opět tranzitivními důvěrnostními vztahy mezi kořenovými doménami jednotlivých stromů (tree-root-trust). [8, 10]



Obrázek 1: Příklad vztahu tree-root-trust v schématu domén, stromů a lesa

Paralelně vedle celé hierarchie je možné třídit objekty do skupin (Groups). Těm se přidělují pravidla (Policies) a usnadňují tak správu objektů v doméně. Skupiny můžou být s globálním nebo lokálním působením, tedy zda rozhodují o přístupech v rámci konkrétní domény, nebo celého lesa. [8]

2.8.4 Principal

V prostředí AD musí mít každý objekt svůj principal, aby bylo možné jej snadno rozpoznat. Jedná-li se o uživatele, mluvíme pak o User Principal Name (UPN). Podobu tohoto jména stanovil Microsoft záměrně jako předpona@kořenová.doména. [11]

3 ANALÝZA SOUČASNÉ SITUACE

V této části zanalyzuji aktuální stav řízení přístupů a identit ve firmě, ve které pracuji na stážích / praxích.

3.1 O společnosti

Základní informace

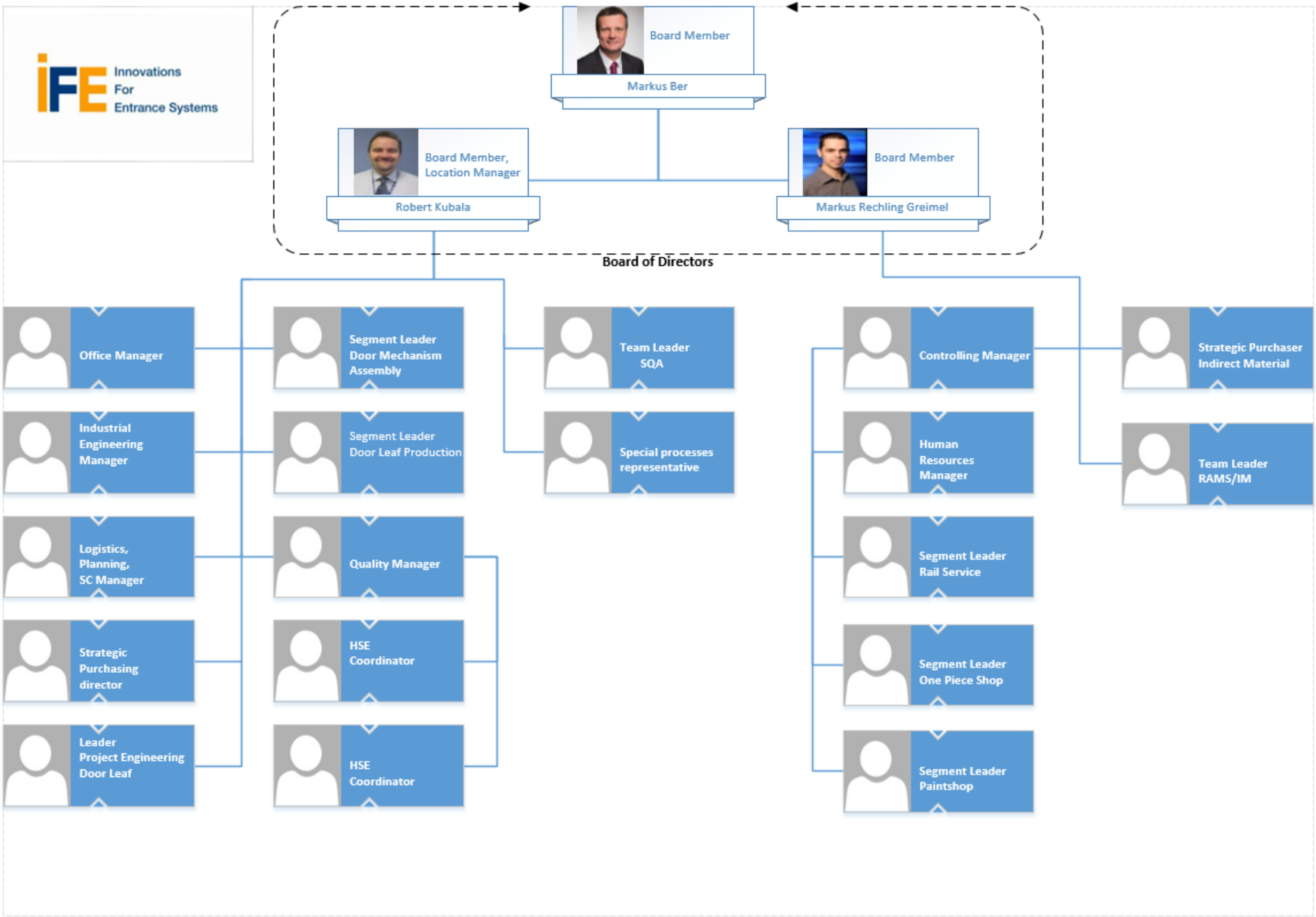
Společnost IFE se zabývá vývojem a výrobou automatických dveřních systémů pro všechny druhy kolejový vozidel. Její historie sahá až do roku 1947. Dnes patří ve svém oboru mezi světové lídry. Pobočkami v Česku, Německu, USA, Austrálii, Číně, Ekvádoru, Nizozemsku a s dalšími 13ti prodejními místy vytvořila silnou prodejní a servisní síť po celém světě.

Od roku 1997 je IFE součástí koncernu Knorr-Bremse s tradicí sahající do roku 1905. Knorr-Bremse se specializuje na výrobu a vývoj brzdových systémů pro kolejová vozidla a nákladní automobily.

V pobočce IFE – CR a.s. v Brně Modřicích, ve které analýzu provádím, pracuje více než 860 zaměstnanců. S ročním outputem 27 tisíc dveří, 19 tisíc pohonů a 3 tisíce schodů je Brněnská pobočka klíčovým výrobním závodem společnosti IFE.

Organizační struktura

Firemní organizační struktura je vyobrazena na obrázku níže. V čele společnosti stojí Markus Ber, Managing Director společnosti Knorr-Bremse pro divizi IFE – CR, řídící firmu z Německa. První úroveň manažerů představuje ředitel pro technickou část firmy a ředitel pro část ekonomickou. Jim se pak zodpovídají manažeři druhé úrovně - vedoucí dílčích částí firmy, kteří jsou zároveň pověřeni správou adresářů svých oddělení v Active Directory. Tu však mohou delegovat níže.



Obrázek 2: Organizační struktura společnosti IFE – CR pro Brno

3.2 Řízení přístupu

Společnost se již v minulosti snažila vlastními prostředky několikrát zavést systém řízení přístupu na základě rolí. (RBAC) Ovšem kvůli auditům a jiným faktorům, kterým se nedařilo vyhovět od této snahy upustila. Dnes už Knorr-Bremse, včetně svých 47 dceřiných společností, zaměstnává skoro třicet tisíc zaměstnanců po celém světě. Ve firmě o těchto rozměrech je implementace RBAC nebo ABAC velice nákladná.

Firma dnes funguje na bázi přímého přidělování přístupů. Každý uživatel si sám musí o jednotlivé přístupy zvlášť zažádat prostřednictvím Service Desku. Pokud jsou mu uděleny, jsou svázány přímo s jeho identitou až do jejich zrušení. V případě nástupu zaměstnance, úpravy údajů nebo jeho odchodu z firmy, je identita vytvořena / upravena / smazána pracovníkem na HR oddělení. Pro všechny ostatní požadavky musí uživatel vytvořit ticket pro IT support. Oprávněnost požadavků na přístup však IT technici nekontrolují, pouze přidělují práva. Schvalování provede vždy administrátor cílového adresáře. Manažer / nadřízený / zadavatel práce zaměstnance tedy do procesu vůbec nevstupuje, není-li žádáno o přístup do adresáře, jehož je sám správcem. Pro odebrání přístupu je třeba opět vyplnit ticket s požadavkem na zrušení přístupu uživateli. Tento ticket vyplňuje administrátor adresáře, nikoliv nadřízený zaměstnance nebo sám zaměstnanec.

3.2.1 Struktura Service Desku

SD slouží coby vstupní brána uživatelům k jejich kontaktu s IT supportem. Je nativně integrovaný s Active Directory a dalšími službami a slouží ke sledování životního cyklu všech jejich požadavků. Uživatelé k němu přistupují prostřednictvím webového prohlížeče. Základní firemní interface SD má následující strukturu:

Obrázek 3: Rozhraní pro kontakt IT supportu ve firmě

V rámci IAM nás nejvíce zajímá sekce „Žádost o přístupová práva“, která se následně dělí na 3 podsekce:

Požadavky o přístup do aplikací a systémů, dostupných ve zdejší lokalitě-jednotlivé služby zakoupené / využívané a držené na serverech v Brně. (Např. Lync, FirstSpirit, Black Berry, webové nebo databázové servery…)

Požadavky o přístup v jiné než zdejší lokalitě, například v rámci projektů na zahraničních pobočkách nebo prakticky všechny požadavky o přístup do adresářů v Active Directory (Domain Controller je totiž na centrále v Mnichově).

Ostatní požadavky-žádost o bezpečnostní výjimku, o povolení fotografování ve výrobě, o práva lokálního administrátora, přístup k WLAN a další…

Dokumenty, potřebné k doložení v papírové podobě, jsou u každého požadavku zvlášť přiloženy. Pro požadavky na přístupová práva v systému SAP je třeba kontaktovat lokálního SAP administrátora. Systémy SAP jsou izolovány.

3.2.2 Přístup na internet

Na všechny uživatele, využívající internet v práci, se vztahují stejná omezení. Existuje seznam webových stránek, ke kterým společnost zakázala přístup. Jsou to stránky nevztahující se k práci, jako například hry, sociální sítě atd. Nejedná se o blokování stránek přes firewall ani nejde o black list na DNS serveru. Webové stránky nepropustí firemní proxy server v Mnichově. Toto omezení nelze žádným požadavkem zrušit. Instalace jiného prohlížeče (např Firefoxu, který umí vynutit používání jiného proxy) je nemožná, vzhledem k bezpečnostní firemní politice. O každou nainstalovanou aplikaci se musí zažádat prostřednictvím Service Desku.

3.2.3 VPN

Zaměstnanci mají možnost pracovat z domu prostřednictvím VPN (Virtual private network). Pro připojení do sítě je třeba projít dvoufázovou autentizací. Do mobilní aplikace zadají čtyřmístný číselný PIN a aplikace zobrazí token kód, který je vyžadován VPN službou pro vytvoření šifrovaného TLS tunelu a následného připojení do privátní sítě.

3.3 Active Directory

Firma využívá služby Active Directory Domain Services od Microsoftu. Konkrétně verzi 2008. Na novější verzi zatím společnost přejít neplánuje. Všechna fyzická zařízení potřebná k chodu služby jsou umístěna na centrále v Německu v Mnichově a odtamtud je služba spravována. Je tam vše, včetně doménových řadičů, DNS serveru, DHCP serveru. Dále je centralizována proxy, mail server a velká část databázových serverů.

3.4 Bezpečnostní politika

Fyzický přístup

Každému zaměstnanci byla dle jeho skupiny přidělena kartička s čipem, určená pro vstup na pracoviště. Většina zaměstnanců spadá do základní skupiny s přístupem prakticky kamkoliv, kromě účtárny, HR, top managmentu, chemických laboratoří a server roomu. Pro přístup do těchto míst musí být zaměstnanec zařazen do příslušné skupiny. Neexistuje žádná skupina s přístupem všude. ID, nahrané na kartě, nejsou nijak svázané s žádnými jinými přístupy. Jsou téměř izolované od všech ostatních systémů s výjimkou možnosti využívat sdílené tiskárny (uživatel smí tisknout po přiložení kartičky k tiskárně) a s využíváním karty při platbě obědů v závodní kantýně. Systém plateb obědů je však spravován třetí stranou a firma dostává pouze seznam IDček s částkami, které za obědy dluží. Firma částky strhává zaměstnancům měsíčně z platu.

Do fyzického přístupu mohu zařadit i Bit-Locker. Zaměstnanci mají povinnost zvolit si osmimístné číselné heslo, které je potřeba při startu notebooku ještě před bootováním OS zadat k dešifrování pevného disku.

Single sign-on

Systém single sign-on ve společnosti defaultně zavedený není. Všichni uživatelé jsou povinni si všechna svá přístupová hesla pamatovat, což se stává bezpečnostním rizikem. Je zde ale možnost si individuálně zažádat přes Service Desk o zakoupení licence k libovolnému password manageru ze seznamu společností schválených. Zájem projevilo jen velice málo zaměstnanců.

Politika hesel

Na přístup do systému se vztahuje firemní politika hesel. Uživatelé se při volbě hesel musí řídit následujícími pravidly:

-heslo musí obsahovat minimálně 8 znaků
-heslo musí obsahovat minimálně 1 speciální znak, 2 číslice a 2 velká písmena
-heslo nesmí obsahovat uživatelské jméno ani jeho část
-heslo nesmí obsahovat 3 a více po sobě jdoucích číslic vzestupně či sestupně
-zaměstnanec nesmí své heslo nikomu sdělovat ani jej nikam zapisovat

Životnost hesla je nastavena na 3 měsíce. Systém si pamatuje posledních 8 hesel, které nesmí být znovu použity.

V některých případech však dodržování těchto předpisů nelze vynutit ani kontrolovat. Například téměř všichni kolegové používají jako heslo k Bit-Lockeru 12345678. Je to lehce zpozorovatelné a zneužitelné. Někteří si volí jako heslo své telefonní číslo. Taktéž PINem k vygenerování VPN tokencode je ve firmě běžně využívaná kombinace 1234. Tento trend výrazně snižuje bezpečnostní opatření a zvyšuje riziko zneužití.

3.5 Audit a reporting

Ačkoliv je Active Directory Domain Service klíčovou službou v Identity and Access Managementu firmy, neprovádí žádné audity. Historie požadavků není nikde zaznamenávána.

3.6 Požadavky Firmy

Společnost je spokojena se současným stavem informační bezpečnosti a neplánuje v blízké budoucnosti uvolňovat větší finanční prostředky na zlepšení v této oblasti. Slabin v podobě povědomí zaměstnanců o bezpečnosti přístupů si je vědoma, ovšem větší důraz klade na bezpečnost zaměstnanců při práci v dílnách, nežli odolnost ICT vůči vnitřním útokům. Souvisí to především s firemní analýzou a vyhodnocení rizik a také s faktem, že Brněnská pobočka nezahrnuje vývoj. Pouze výrobu a distribuci.
Návrhy na změny, které nijak výrazně nezasahují do chodu společnosti ovšem přijímá a vnímá jako potencionální zlepšení při nízkých nákladech. Jedná se o změny v podobě revitalizace politiky hesel a řízení přístupů, zavedení systému vzdělávání, případně zavedení podpůrné služby třetí strany (SSO, Password Manager atd.).

3.7 Shrnutí

Přístup společnosti k IAM shledávám velmi uvolněným. Na první pohled je zřejmé, že Active Directory je ve správě a řízení identit ve firmě klíčovou službou. Nevytváří a neukládá ovšem žádné záznamy o změnách. Z toho důvodu ani nebylo možné implementovat RBAC. Kupříkladu, bez historie není možné převést role bývalého zaměstnance na jeho nástupce a vyhovět tak auditům. Ve společnosti o desítkách tisíc zaměstnanců je ale zavedení nového způsobu řízení identit (vlastními silami nebo na zakázku) velice nákladná záležitost a v současné chvíli by za tu cenu ani nepřinesla nijak výrazné výhody. Všechny firmy koncernu Knorr-Bremse mají v této oblasti jednotné procesy, což omezuje pružnost a šanci na změnu v blízké budoucnosti. Proto bych se zaměřil ve snaze zlepšit IAM firmy na zpětnou kontrolu přístupů. Přímé přidělování přístupů k identitám je totiž charakteristické jednou výraznou nevýhodou, tedy, že identity mají lidským přičiněním tendenci svá oprávnění s časem kumulovat.

Všiml jsem si pár nedostatků také v jiných oblastech. Například centrální zavedení SSO nebo Password Managera by s malými náklady značně usnadnilo práci uživatelů. Pozornost by si jistě zasloužila také politika hesel.

Zároveň si myslím, že jednoúrovňový princip schvalování žádostí o přístup je nedostačující. Každý požadavek by měl mít ideálně dva filtry v podobě primární a sekundární kontroly, než jsou změny aplikovány IT technikem.

4 VLASTNÍ NÁVRHY

V této části popíšu vlastní návrh na zlepšení IAM ve firmě a ostatních bezpečnostních prvků. Zaměřím se především na první část, politiku hesel. Dále přehodnotím pravidla řízení přístupů, oprávnění a přednesu také návrh na vícestupňovou kontrolu oprávnění. Část práce věnuji i návrhu na zavedení systému pro vzdělání zaměstnanců ohledně bezpečnosti ICT. Budu vycházet především z výsledků analýzy prostředí.

4.1 Politika hesel

Přesto, že jsou ve společnosti nastavena přísná pravidla pro správu hesel, je všeobecný postoj k heslům mezi zaměstnanci dosti uvolněný. Politika hesel nutí zaměstnance vymýšlet komplexní hesla, vyhovující různým pravidlům každé 3 měsíce s tím, že nelze použít posledních 8 hesel. Čili minimálně dva a čtvrt roku nemůžou zaměstnanci rotovat svou sadu. V souvislosti s těžkou časovou vytížeností a přátelskou atmosférou na odděleních toto vedlo k porušování nařízení. Konkrétně k jedinému porušitelnému: „Zaměstnanec nesmí své heslo nikomu sdělovat nebo jej někam zapisovat“. Někteří si jej poznamenávají na papír u pracovního místa, na disk v nešifrované podobě nebo v některých případech jej přilepují na monitor.

Pro řešení tohoto problému přednesu dva návrhy. Obě varianty k problému přistupují protichůdně, čili reálně uplatnit lze pouze jednu z nich. Prvním návrhem je snaha o docílení dodržování bezpečnostních předpisů pomocí zmírnění požadavků na hesla. Aby se daly lépe pamatovat a potřeba poznamenávání hesel pak opadne. Druhým návrhem je rozšíření vybraného Password Manageru ve firmě a ukládání hesel v šifrované podobě.

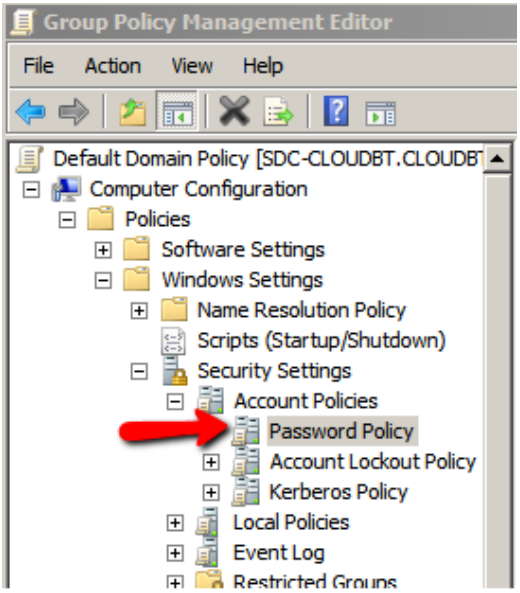
4.1.1 Varianta 1

Tlak na zaměstnance v podobě přísných opatření, kontrol pracovišť nebo postihů neshledávám jako účinnou metodu. Navrhuji pravidla naopak zmírnit:

- povinný počet číslic a velkých písmen bych snížil z 2 na 1.
- dobu životnosti hesla bych prodloužil z 3 měsíců na 1 rok.

Zmírnění pravidel sice sníží sílu hesel jako takových, ale zaměstnanci už nebudou nuceni pamatovat si stále nová a složitá hesla, která si pak někam poznamenávají. Spolu se školeními (viz. bod 4.3) paradoxně přispěje k celkově stabilnější firemní bezpečnosti. Bezpečnost hesla totiž nestojí pouze na jeho prolomitelnosti / uhodnutelnosti, ale zároveň na způsobu zacházení s ním. Proto je třeba vybalancovat tyto dva faktory, aby nebyl ani jeden slabinou pro druhý. Tato pravidla by musela být schválena managementem firmy, dána na vědomí ostatním zaměstnancům firmy a aktualizována v Active Directory pracovníky z IT pomocí Group Policy Management Editoru cestou:

Computer Configuration/Windows Settings/Security Settings/Account Policies/Password Policy/



Obrázek 4: Nastavení password policy v AD [12]

Ostatní předpisy týkající se délky hesla, nebo zda obsahuje uživatelovo ID nebo po sobě jdoucí číslice bych ponechal. Jejich zmírnění by nijak výrazně nepomohlo jejich zapamatovatelnosti, ale velice by hesla oslabilo.

4.1.2 Varianta 2

Směrnice společnosti umožňují uživatelům zažádat o proplacení / poskytnutí licence k podpůrnému programu, pokud jej k práci potřebuje a dostane schválení od příslušného nadřízeného. Zároveň musí být na seznamu schválených aplikací. Uživatel není oprávněn instalovat do počítače aplikaci, která není na tomto seznamu. Navrhuji tedy přidat do seznamu schválených aplikací vybraný Password Manager. V souvislosti se zavedením školení (viz. bod 3.) to přispěje k zodpovědnějšímu zacházení s hesly.

Na trhu se pohybují spousty programů zaměřených na bezpečnou úschovu a správu hesel. Uvedu z nich pět nejznámějších, porovnám jejich charakteristické slabé / silné stránky a vyberu ten nejvhodnější pro naši situaci.

Tabulka 1: Porovnání password managerů

SW	**Silné stránky**	**Slabé stránky**
Dashlane	- Nabízí VPN - Skenuje Dark Web, zda neunikly citlivé údaje	- Nákladný, navíc pokud už máte VPN - Omezená podpora pro Internet Explorer
Keeper	- Udržuje historii hesel	- Neaktualizuje si hesla automaticky - Nevyplňuje formuláře na webu
RoboForm	- Detekuje slabá hesla / duplikáty - Velice spolehlivé řešení pro „digitální dědění“ a sdílení souborů. - Spravuje hesla v aplikacích	- Omezené import funkce - Omezená dvoufázová autentizace
KeePass	- Kvalitní generátor hesel - Přes 100 plug-in funkcí - Umí odhalovat key-loggery - Kvalitní import dat	- Synchronizace napříč zařízeními je obtížná - Nepodporuje mobily
LastPass	- Automatické změny hesel - Funkce „dědění“ hesel	- Nepodporuje Operu a Explorer

Všechny uvedené programy využívají silnou šifrovací metodu AES, PBKDF2, využívající hash SHA1. Klíč je o velikosti 256 bit. Jedná se o standart, téměř 100% odolný vůči brute-force útokům. [15, 17] Všechny programy také disponují funkcí dvoufázové autentizace, generátorem silných hesel, jsou kompatibilní se všemi operačními systémy (Windows, macOS, iOS, Android, Linux a Chrome OS) a podporují většinu nejpopulárnějších internetových prohlížečů. Diverzita služeb tedy spočívá hlavně v kvalitě doprovodných funkcích a v ceně.

Po zvážení silných i slabých stránek jednoznačně doporučuji Password Manager KeyPass (v. 2.44). Konkurenční programy jsem nezvolil z následujících důvodů:

LastPass kvůli absenci podpory Exploreru, protože Explorer je defaultní prohlížeč na firemních zařízeních a jeden ze dvou povolených (2. je Edge). Také je jediný, na kterém běží firemní intraportál. Dashlane ztrácí význam kvůli VPN službě, kterou má už společnost centrálně zavedenou. Keeper nenabízí moc užitečných funkcí ve srovnání s KeyPass a RoboForm, ač je kvalitním programem s dlouholetým místem na trhu, zdá se být cílený spíše pro rodiny, než pro firmy.

Keypass je velice modulovatelný pomocí široké škály dostupných plug-inů a umí importovat data ze všech konkurenčních programů. Jeho rozhraní je přívětivé a intuitivní na ovládání, má pokročilejší funkci kontroly síly hesel. (Ostatní konkurenti se většinou řídí jednoduchými pravidly, jako je 8 znaků, velký symbol, číslice atd. a proto například heslo „Password1“ vyhodnotí jako velmi silné.) KeyPass je navíc distribuován jako open source (certifikovaný od OSI), což je pro firmu mnohem přívětivější, než platit okolo 20 € ročně za jednu licenci jiného konkurenčního programu, nebo téměř dvojnásobek v případě Dashlane. Absence podpory pro mobilní zařízení a složitost synchronizací nepovažuji za faktor ovlivňující výběr, protože zaměstnanci mají povoleno využívat pouze jeden služební laptop. Pro dvoufázové ověřování se budou využívat USB tokeny.

4.1.3 Výběr varianty + dodatečná opatření

Z dvou přednesených variant navrhuji uplatnění varianty 2, týkající se zavedení Password Managera. Důvodem je riziko, které Variantu 1 provází, že při nedostatečném apelu od společnosti na zaměstnance, se po čase vrátí zpět zvyky porušování pravidel. Výsledkem by pak byla, jak snížená síla hesel, tak i nadále nezodpovědná operace s nimi, což by znamenalo selhání. Varianta 1 by byla vhodná pouze v případě, kdy by management společnosti z různých důvodů variantu 2 zamítl a naznal, že jsou pravidla pro účely společnosti zbytečně přísná.

Dále, kromě přijetí varianty 2, navrhuji zavést dvě nová opatření:

- Nastavení počtu pokusů o zadání hesla na 5
- Nastavení následující prodlevy mezi pokusy:
    - Po třetím chybném zadání: prodleva 5 minut
    - Po čtvrtém chybném zadání: prodleva 30 minut
    - Po pátém chybném zadání: prodleva 1 hodina

Více chybných pokusů by vyústilo k zablokování účtu a k informování o incidentu IT oddělení. Zaměstnanec by v takovém případě musel prokázat svou totožnost a zažádat si o obnovení hesla.

4.1.4 Pin pro VPN Token

Prvotní nastavení hesel představuje velké bezpečnostní riziko v oblasti VPN. Zaměstnanci, pracující z domu, se musí přihlásit přes VPN do firemní sítě. K tomu potřebují TokenCode, vygenerovaný na mobilním zařízení v aplikaci SafeNet. Defaultní PIN do této aplikace je nastaven na „1234“. Nikdo ovšem zaměstnance neinformoval o tom, jak si jej změnit. Tato situace může usnadnit případným útočníkům přístup na firemní síť. Proto navrhuji přijmout toto opatření:

- Nastavit, aby si aplikace SafeNet pro generování Tokenů při druhém použití vynutila změnu PINu od zaměstnance.

4.2 Řízení přístupu

Veškeré řízení přístupů ve společnosti je spravováno pomocí přímého přidělování práv k identitám v Active Directory. V následující části přednesu 4 návrhy na opatření v této oblasti, které mohou zlepšit celkovou bezpečnost.

4.2.1 Zavedení systému revalidace

Navrhuji, aby každý rok obdrželi všichni vedoucí výzvu k revalidaci přístupových práv svých podřízených pracovníků. Aby nebylo možno tuto činnost opakovaně odkládat, systém odepře všechny nepotvrzené přístupy od určitého data. Nadřízený tedy musí překontrolovat přístupy podřízených a zhodnotit, zda je stále potřebuje. Pokud ne, musí vytvořit ticket pro jejich odstranění. Vzhledem k tomu, že přístupy nejsou přidělovány pomocí rolí, nýbrž napřímo, bude tato kontrola pracnější a časově náročnější. Ovšem je to klíčová činnost k zamezení efektu nechtěného kumulování přístupů v průběhu času.

4.2.2 Odebrání přístupů

Přestože je v mnoha případech člověk, zodpovědný za přístup do adresářů na oddělení, zároveň přímým nadřízeným zaměstnance, který je na odchodu, jedna a tatáž osoba, nemusí toto být pravidlem. Například v situaci, kdy vedoucí pověří spravováním adresářů jiného pracovníka, tomu tak není. Je proto důležité, aby člověk, odpovědný za odebrání přístupu zaměstnanci byl vždy jeho přímý nadřízený, nikoliv správce onoho adresáře, o který se jedná. Nadřízený tedy musí vyplnit a odeslat ticket přes Service Desk na IT oddělení. Workflow odebírání přístupů tak bude plynulejší a předejde se tím některým možným chybám.

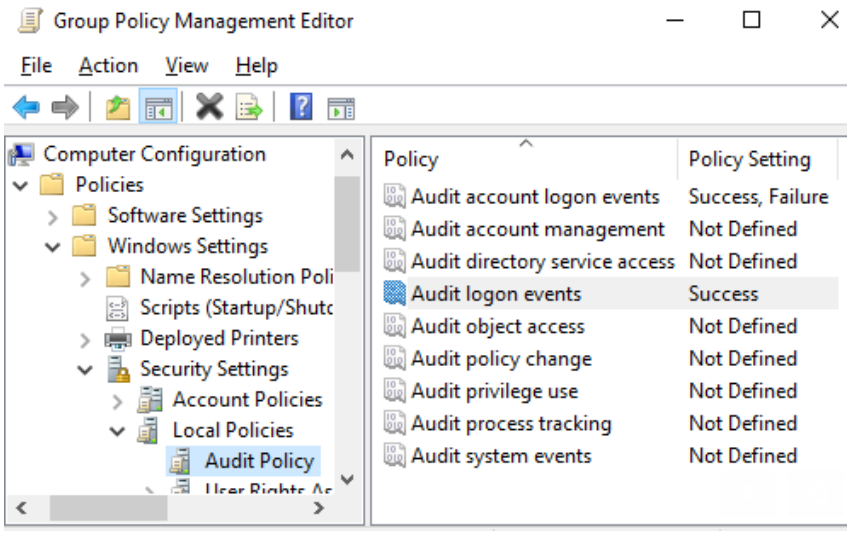
4.2.3 Dvou-úrovňové přidělování přístupů

Schválení přístupu pouze ze strany Service Desku je nedostačující. Každý požadavek o přístup k systému / aplikaci / adresáři nebo jakémukoliv nástroji potřebnému k práci by měl mít primární i sekundární filtr, aby se zamezilo faktoru lidské chybovosti. Požadavky by měly být primárně schváleny přímým nadřízeným zaměstnance, eventuelně manažerem projektu, v jehož rámci je přístup nutný. V případě požadavku o přístup do adresářové složky pak jejím správcem. Bez tohoto schválení nemůže být požadavek postoupen k sekundární kontrole, tedy na IT oddělení.

4.2.4 Reporting / Auditing

Zaznamenávání veškerých změn a událostí v systému z pohledu uživatelských přístupů a následné reportování / audit je jednou z nejdůležitějších funkcionalit IAM. Doposud však byla ve firmě upozaďována a prioritizovány byly spíše záznamy a reporting síťových a serverových událostí. Souvisí to s tím, že se firmě v minulosti nedařilo tuto funkcionalitu správně nastavit spolu s funkční RBAC metodou přidělování oprávnění. Po přechodu na přímé přidělování nastavení skupin by však měla být této oblasti věnována výrazně větší pozornost. Systém reportingu a auditů je nutno bezodkladně nastavit tak, aby v případě bezpečnostního incidentu byl schopen detekovat jeho příčinu. V nástroji Group Policy Management Editor jde o sekci Audit Policy s cestou:

> Computer Configuration/Policies/Windows Settings/Security Settings/Local Policies/Audit Policy/



Obrázek 5: Nastavení auditů v AD [12]

4.3 Systém školení zaměstnanců

Příčinou více než 90 % úspěšných kybernetických útoků na firmy bývá liknavý přístup zaměstnanců k ochraně citlivých dat. Během svých praxí jsem ovšem nezpozoroval snahu firmy o informování a vzdělání zaměstnanců v této oblasti. Proto navrhuji zavést následující opatření, aby se v budoucnu možným incidentům dařilo předcházet.

4.3.1 Externí vzdělávání

Navrhuji, aby firma pravidelně realizovala školení zaměstnanců externím odborníkem, který srozumitelnou formou provede zaměstnance oblastí informační bezpečnosti, přičemž se vždy zaměří na jednotlivé skupiny zaměstnanců (viz. 4.3.2). Zaměstnanci budou primárně informováni o rizicích spojených s nedodržováním bezpečnostních předpisů na jejich oddělení a zjistí, jak různé ochranné prvky skutečně fungují, jaké chování vyžadují ke svému chodu a jaké naopak snižuje jejich účinnost a mnohá další. Cílem je, aby se v povědomí zaměstnanců upevnilo, že IT bezpečnost je neoddělitelnou součástí společnosti.

Pro tyto účely navrhuji rozdělit zaměstnance do následujících skupin, a zajistit pro ně kurz přímo šitý na míru.

IT oddělení:

Skupina vyžadující odbornější kurz, zaměřený především na praktickou ochranu serverů a sítí v prostředí Windows Server, Troubleshooting a analýzu sítí, zabezpečení SQL serverů a na principy dnešních malwarů. Školení by mělo probíhat fyzickou formou v rozsahu minimálně dvanácti lekcí. Kurz zakončen ověřovacím testem, po němž zaměstnanec obdrží certifikát. Úroveň certifikátu, vyžadující společností, stanoví management firmy.

Účtárna, HR:

Pro tuto skupinu zaměstnanců je vhodné objednat kurz více zaměřený na hrozby v oblasti finančních podvodů a krádeže citlivých údajů. Rozeznávání phishingových bankovních zpráv atd. Kurz by měl být v rozsahu do 10 lekcí. Je možné jej absolvovat přes e-learning.

Ostatní provozní zaměstnanci:

Tato skupina zahrnuje všechny ostatní zaměstnance firmy využívající firemní ICT. Včetně, logistiky, prodeje, řízení výroby, laboratoří i managementu. Jejich kurz, také v rozsahu 10 lekcí přes e-learning, by měl být zacílen všeobecněji.

Uvedu seznam nejdůležitějších bodů, kterých by se školení mělo dotknout:

- Nebezpečnost sdílení účtů
- Bezpečné chování v síti
- Jak správně zacházet s Password Managerem
- Důležitost správného zacházení se laptopy, badgy, s hesly, PINy, USB Tokeny a podobnými klíčovými objekty
- Obezřetnost při vydávání guest-badges
- Social engineering (Phishing, tailgating, pretexting, baiting, atd.)
- Rizika spojená s pozdním odebíráním přístupů
- Opatření proti úniku údajů
- Správná reakce při incidentu

4.3.2 Ověřování znalostí

Absolvováním kurzů však nelze považovat otázku bezpečnosti za uzavřenou. Znalosti je potřeba pravidelně obnovovat a aktualizovat. Navrhuji takovéto školení celofiremně provádět v dvouletém, maximálně tříletém intervalu. Po každém školení projdou zaměstnanci znalostním testem. Výsledky testů poskytnuté od školící organizace lze využít pro analýzu, případně pro systém odměňování zaměstnanců.

4.3.3 Penetrační test

Dále navrhuji objednání penetračních testů. Jedná se o zkušební útoky, které jsou vedeny jak zevnitř, tak zvenčí. Tedy přes technické zabezpečení i přes organizační opatření i podvody. Cílem je především podat souhrnnou zprávu o úrovni a kvalitě celkového zabezpečení firmy proti široké škále útoků.

4.3.4 Falešné phishingové útoky

Pro udržení bdělosti zaměstnanců v oblasti internetové bezpečnosti doporučuji zavést po vzoru velkých IT firem takzvané „fake-phishing“ útoky. Jedná se o falešné phishingové útoky, tedy maily rozesílané globálně, nebo pouze do určitého firemního oddělení s cílem vymámit z uživatele přihlašovací údaje. Tyto maily jsou často téměř totožné s maily, které pracovníci v rámci firemní kultury běžně dostávají. Odkazují na stejné soubory nebo webové portály, ovšem s lehce pozměněnou necertifikovanou doménou. V reálném případě může po zadání ID a hesla od zaměstnance útočník ihned odcizit důležitá data, pozměnit je, smazat, nebo ukrást zaměstnanci celou pracovní identitu. Následky úspěšných phishingových útoků bývají fatální. Mnohé cílí na účetní oddělení / pokladnu a ve správný čas například zašlou falešnou fakturu od dodavatele, jen s pozměněným číslem účtu. Vznikají tak vysoké škody.

Zaměstnanci jsou tedy povinni tyto falešné útoky detekovat a nahlásit na příslušnou adresu podpory. Toto opatření má 3 přínosy:

1) V případě většího počtu nenahlášení to může firma analyzovat a zjistit, proč falešný útok prošel. S tím se dá dále pracovat, například v podobě informování, nebo dodatečného proškolení zaměstnanců. Jedná-li se o stále ty stejné jednotlivce, pak v podobě napomenutí.
2) Zvyšuje se tím obezřetnost a schopnost zaměstnanců detekovat tento sociální druh útoku.
3) Jakmile ve firmě proběhne skutečný phishingový útok, je celkem velká šance, že část zaměstnanců ho odhalí, nahlásí a support na něj může pohotově reagovat.

ZÁVĚR

Cílem této bakalářské práce bylo navrhnout úpravy v systému správy identit a přístupů ve vybrané společnosti, aby se zlepšila celková bezpečnost.

V první teoretické části byl zpracován teoretický podklad se všemi potřebnými informacemi k porozumění dané oblasti. Tato část se opírala o charakteristiky jednotlivých způsobů řízení přístupů identit, vysvětlila životnost identit, vysvětlila důležité pojmy jako RBAC, Autorizace, SSO atd. a nastínila základní znalosti potřebné k pochopení fungování systému Active Directory, který je v současnosti využíván většinou společností k IAM. Na tuto část navazovala část analytická, ve které byl zhodnocen současný stav ve společnosti. Během této analýzy byly nalezeny slabiny v bezpečnosti, především ve správě hesel a slabé snaze o poučení zaměstnanců o ICT bezpečnosti. Pozornost upoutaly i některé organizační procesy, které by mohly být optimalizovány.

Jako poslední následovala část praktická, ve které byly předneseny vlastní návrhy řešení. Pozornost byla směřována především na politiku hesel a na výběr vhodného podpůrného programu třetí strany pro schválení do interního seznamu povolených aplikací. Navrhnuty byly i úpravy pro schvalování přístupů. A pro udržení bezpečnostní obezřetnosti byl přednesen návrh na zavedení plošného školení zaměstnanců. Cíle mé práce byly tímto splněny.

SEZNAM POUŽITÉ LITERATURY

[1] BERTINO, E. a K. TAKAHASHI. *Identity management: Concepts, Technologies, and Systems*. Boston: Artech House, 2010. ISBN 978-1-60807-039-8.

[2] GAŠPARÍK, Petr. *Koho všechno můžeme řídit? – Seriál o IDM Část 2.* [online] 2015 [cit. 10.5.2020] Dostupné z: https://www.ami.cz/publikujeme/blog/koho-vsechno-muzeme-ridit-serial-o-idm-cast-2

[3] GAŠPARÍK, Petr. *Licence a delegace – seriál o IdM část 3.* [online] 2015 [cit. 10.5.2020] Dostupné z: https://www.ami.cz/publikujeme/blog/licence-a-delegace-serial-o-idm-cast-3

[4] GAŠPARÍK, Petr. *Access a key distribution management – seriál o IdM část 4.* [online] 2015 [cit. 10.5.2020] Dostupné z: https://www.ami.cz/publikujeme/blog/access-a-key-distribution-management-serial-o-idm-cast-4

[5] BALÁŽIK, Milan. *Principy řízení identit*. IT SYSTEMS [online]. 2012, (1-5) [cit. 2020-10-5]. ISSN 1802-615X. Dostupné z: https://www.systemonline.cz/itsecurity/principy-rizeni-identit.htm

[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, 2007 XVIII(1) [cit. 10.5.2020] ISSN 121-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/560.html#lit1

[7] MARTIN, A. James a John K. WATERS. *What is IAM? Identity and access management explained*. CSO [online] 2018 [cit 10.5.2020] Dostupné z: https://www.csoonline.com/article/2120384/what-is-iam-identity-and-access-management-explained.html

[8] BOUŠKA, Petr. *Active Directory komponenty – domain, tree, forest, site* [online] 2008 [cit. 10.5.2020] Dostupné z: https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/

[9] BOUŠKA, Petr. *DNS (Domain Name Systém) zaměřeno na Microsoft* [online] 2007 [cit. 10.5.2020] Dostupné z: https://www.samuraj-cz.com/clanek/dns-domain-name-system-zamereno-na-microsoft/

[10] COURSERA ve spolupráci s GOOGLE, *What is Active Directory?* In: video-courses, Coursera [video] 2018 [10.5.2020] Doustupné z: https://www.coursera.org/lecture/system-administration-it-infrastructure-services/what-is-active-directory-0BVxn

[11] BOUŠKA, Petr. *Kerberos část 2 – AD uživatelské účty a Service Principal Name*. [online] 2014 [cit. 10.5.2020] Dostupné z: https://www.samuraj-cz.com/clanek/kerberos-cast-2-ad-uzivatelske-ucty-a-service-principal-name/

[12] HINK, Tomáš. *Re: Dotaz - AD* [emailová komunikace] 27.4.2020 14:32 [cit. 10.5.2020]

[13] ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: CERM, 2013. ISBN 978-80-7204-872-4

[14] BÉBR, R. a P. DOUCEK. *Informační systémy pro podporu manažerské práce*. 1. vyd. Praha: Professional Publishing, 2005. ISBN 80-86419-79-7.

[15] POŽÁR, Josef, *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

[16] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

[17] MALINKA, Kamil. *12. Bezpečná zařízení, správa klíčů* [přednáška] Brno: VUT v Brně, Fakulta podnikatelská, 5.12.2018

SEZNAM TABULEK

SEZNAM OBRÁZKŮ