Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Implementace bezpečné autentizace ve vybraném systému

Vojtěch Kundela

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Vojtěch Kundela

Informatika

Název práce

Implementace bezpečné autentizace ve vybraném systému

Název anglicky

Implementation of secure authentication in a chosen system

Cíle práce

Cílem práce je návrh procesu implementace bezpečné autentizace ve vybraném systému.
Pro dosažení cíle bude zapotřebí splnit následující dílčí cíle:
-Analýza současné metody autentizace v systému a zhodnocení jejich bezpečnostních rizik.
-Výběr nových autentizačních metod s ohledem na požadavky majitele systému.
-Posouzení dopadu nového zabezpečení s ohledem na uživatelskou přívětivost a snížení bezpečnostních rizik.
-Vytvoření implementačního návrhu bezpečné autentizace.

Metodika

Na základě literární rešerše bude vybrána vhodná metoda pro novou bezpečnou autentizaci ve vybraném systému. Pro výběr nové metody se bude postupovat v následujících krocích:

-Studium odborných informačních zdrojů.

-Porovnání různých metod autentizace pro vytvoření přehledu o současné problematice a získání dalších relevantních informací.

-Výběr vhodné metody autentizace.

Na základě předchozích kroků bude vytvořen implementační návrh a budou formulovány závěry práce a její hodnocení.

Doporučený rozsah práce

35-45s.

Klíčová slova

bezpečnost, autentizace, ověřování, bezpečnostní rizika, návrh implementace, identifikace, ochrana přístupu

---

Doporučené zdroje informací

BALLAD, Bill, Tricia BALLAD a Erin K. BANKS. Access control, authentication, and public key infrastructure. Sudbury, MA: Jones & Bartlett Learning, 2011. Jones & Bartlett Learning information systems security & assurance series. ISBN 978-0763791285

KHAIRALLAH, Michael. Physical security systems handbook: the design and implementation of electronic security systems. Amsterdam: Elsevier Butterworth-Heinemann, 2006. ISBN 978-0750678506

NEWMAN, Robert M. Security and Access Control Using Biometric Technologies. Boston, MA: COURSE TECHNOLOGY CENGAGE Learning, 2010. ISBN 978-1435441057

RANKL, W. Smart card applications: design models for using and programming smart cards. Hoboken, NJ: John Wiley & Sons, 2007. ISBN 978-0470058824

XIANG, Yang. Cyberspace safety and security: 4th international symposium, CSS 2012, Melbourne, Australia, December 12-13, 2012 : proceedings. New York: Springer, c2012. LNCS sublibrary. ISBN 978-3-642-35361-1

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Martin Havránek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 9. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 14. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Implementace bezpečné autentizace ve vybraném systému" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3.2024 _____

Poděkování

Rád bych touto cestou poděkoval vedoucímu práce Ing. Martinu Havránkovi, Ph.D. za jeho pomoc a odborné znalosti. Zároveň děkuji i majiteli systému za spolupráci.

Implementace bezpečné autentizace ve vybraném systému

Abstrakt

Tato bakalářská práce je zaměřena na návrh procesu implementace nově zvolených autentizačních řešení ve vybraném systému, s cílem navýšení bezpečnosti. Tato řešení se budou zaměřovat jak na autentizaci fyzického, tak logického přístupu. Na základě seznámení se s aktuálními metodami autentizace v systému a požadavky jeho majitele bude provedena analýza různých způsobů navýšení bezpečnosti. Po získání výsledků a následné konzultaci s majitelem budou vybrány nové metody autentizace, které se poté ucelí do implementačního plánu.

Klíčová slova: bezpečnost, autentizace, ověřování, bezpečnostní rizika, návrh implementace, identifikace, ochrana přístupu

Implementation of secure authentication in a chosen system

Abstract

This bachelor thesis focuses on the design of the implementation process of newly selected authentication solutions in a chosen system, with the aim of increasing security. These solutions will focus on both physical and logical access authentication. Based on the familiarization with the current authentication methods in the system and the requirements of its owner, an analysis of different ways to increase security will be performed. After obtaining the results and subsequent consultation with the owner, new authentication methods will be selected and then consolidated into an implementation plan.

Keywords: security, authentication, verification, security risks, implementation design, identification, access protection

Obsah

1 Úvod

V dnešní době, kdy jsme propojeni digitálním světem, je zabezpečení systémů klíčové a závislé na spolehlivých autentizačních metodách. Únik citlivých dat, krádež majetku a výpadky systémů jsou potenciální hrozby, kterým čelíme. Tyto hrozby se neustále vyvíjejí, a tak je nezbytné přijímat opatření, pomocí kterých se jim budeme bránit. Nicméně s různými možnostmi zabezpečení přicházejí i různá řešení, a to, co funguje pro jednoho, nemusí být vhodné pro druhého. Je tedy klíčové hledat a implementovat efektivní bezpečnostní strategie, které budou odpovídat konkrétním potřebám a kontextu daného systému.

Z těchto důvodů se tato práce zaměří na návrh implementace pro nová autentizační řešení ve vybraném systému. V teoretické části budou rozvedeny jednotlivé metody autentizace, jejich komponenty, a také příklady hrozeb, které představují veliké riziko pro systém. V praktické části proběhne obeznámení se současným stavem systému, a hrozbami, které se v něm nachází. Po seznámení se s požadavky majitele bude provedena analýza různých metod autentizace, ze kterých bude na základě výsledků a následné konzultace s majitelem sepsán implementační návrh.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem práce je návrh procesu implementace bezpečné autentizace ve vybraném systému. Pro dosažení hlavního cíle je zapotřebí splnit několik dílčích cílů. Prvním dílčím cílem je analýza současných metod autentizace v systému a následné zhodnocení jejich bezpečnostních rizik. Následuje výběr nových autentizačních metod s ohledem na požadavky majitele systému. Dalším dílčím cílem je posouzení dopadu nového zabezpečení s ohledem na uživatelskou přívětivost a snížení bezpečnostních rizik. Na závěr je potřeba vytvořit implementační návrh bezpečné autentizace.

2.2 Metodika

V první části této bakalářské práce byla provedena literární rešerše, která umožnila seznámení se s problematikou bezpečnosti v rámci autentizace uživatelů. Na základě rešerše byly v praktické části vybrány vhodné metody pro novou bezpečnou autentizaci ve vybraném systému.

Pro výběr nové metody bylo nejprve zapotřebí se seznámit se současným stavem autentizace v systému. To umožnilo zhodnocení jejích existujících bezpečnostních rizika, která je zapotřebí opatřit. Dále proběhlo seznámení se specifickými požadavky majitele systému na nové autentizační metody. Pomocí analýzy různých způsobů autentizace v porovnání s požadavky majitele byly vybrány nové metody pro bezpečnou autentizaci, které následně byly s majitelem prokonzultovány. Po schválení nově zvolených metod zabezpečení byl vytvořen finální implementační návrh a proběhlo zhodnocení jeho dopadu v případě jeho implementace.

3 Teoretická východiska

Autentizace je proces ověřování identity uživatele nebo zařízení, při získání přístupu k prostředku nebo službě. Je nezbytná pro zajištění bezpečnosti a integrity dat a systémů. Přístup, jež se snažíme ochránit, se primárně dělí do dvou skupin: fyzický a logický.

Autentizace fyzického přístupu se týká metod, které omezují přístup na určité místo, například do budovy, nebo specifické místnosti. Jejím cílem je zabránění neoprávněného vstupu a manipulaci s fyzickými prostředky.

Autentizace logického přístupu obsahuje metody, které omezují přístup k datům uloženým na zařízeních nebo na síti, jako jsou databáze, soubory či aplikace. Cílem je zamezit možnost zneužití těchto dat. (Lutkevitch, 2022)

3.1 Způsoby autentizace

Existují 3 základní faktory pro ověření identity uživatele. Jedná se o prokázání znalosti, vlastnictví a vlastnosti. Tedy něco, co uživatel zná, co má fyzicky u sebe a jakou má unikátní vlastnost. Tyto faktory se dají využít jak pro autentizaci fyzického, tak logického přístupu. (Ballad, a další, 2010)

3.1.1 Znalost

Pro prokázání znalosti u fyzického přístupu se typicky používá zámek nebo trezor, pro jehož odemčení je potřeba zadat správný číselný kód. Pro logický přístup se nejčastěji používá heslo. Tato řešení jsou velmi jednoduchá na implementaci, ovšem mají několik zásadních problémů. Hlavním z nich je nutnost zapamatování jednotlivých kódů či hesel, což může být problém, pokud jsou ověřovací faktory velmi početné, například pokud se v objektu nachází velké množství dveří, jež každé požadují jiný číselný kód. Uživatel má pak tendenci volit jednoduchá hesla a kódy, které se snadno prolomí útoky typu brute force. Tyto druhy útoků obnáší opakované zkoušení často používaných hesel, popř. možné kombinace všech znaků pomocí počítačového programu. V případě, že jsou autentizační faktory předem nastavené, uživatel si je může poznamenat na papír či do mobilního zařízení, což umožní jejich ztrátu nebo krádež. (Kessler, 1996; Hanna, 2021)

Je tedy důležité zajistit, aby hesla a kódy splňovaly určité podmínky. Mezi ně může patřit minimální délka, existence speciálních znaků či nepovolení častých frází a číselných

kódů (např. nepovolit heslo „heslo123“ či číselný kód „1234“). Zároveň by uživatelé měli být školeni, aby si ověřovací faktory nikam nezapisovali a nesdíleli je s ostatními. (Kessler, 1996)

3.1.2 **Vlastnictví**

Nejzákladnější způsob pro ověření vlastnictví pro fyzický přístup se využívá už více jak 6000 let, a tím je klíč pro odemčení zámku. Dalším typickým příkladem je čipová karta, kterou při vstupu přiložíme ke čtečce u dveří, která zámek otevře. Pro logický přístup je také možnost použití čipové karty, je ovšem potřeba mít čtečky u každého zařízení, kde se tato autentizace využívá. V dnešní době se také často využívají mobilní zařízení, kde se autentizace provádí například pomocí jednorázového kódu přes SMS, nebo aplikace nainstalované na zařízení. U tohoto způsobu ověření ovšem hrozí, že uživatel daný předmět pro autentizaci ztratí. V případě, že systém nevyužívá žádnou jinou formu ověřování, může nastat situace, kdy nálezce bude schopen získat neoprávněný přístup do systému. (Jones, 2023)

3.1.3 **Vlastnost**

Prokázání vlastnosti funguje na stejném principu pro oba druhy přístupu. Uživatel musí mít unikátní tělesný rys, který je využit pro ověření jeho identity. Tomuto způsobu autentizace se říká biometrie. Typický příklad z běžného života je čtečka otisků prstů na mobilních zařízeních. Dalším častým řešením je snímek obličeje či očí. V závislosti na použité technologii se nejedná pouze o porovnání dvou fotografií, ale o hloubkové mapy, které jsou schopné otisk či obličej zaznamenat v 3D prostoru. Hlavní nevýhodou tohoto řešení jsou vysoké náklady, a náchylnost na falešně positivní a falešně negativní výsledky. Falešně positivní výsledek nastane, když projde neoprávněná osoba biometrickou kontrolou, například u rozpoznávání obličeje dvojčat či podobně vypadajících lidí. Falešně negativní výsledek je naopak zamítnutí oprávněného uživatele, k čemuž může dojít při znečištění senzoru, nebo při poranění snímané části těla. (Jones, 2023)

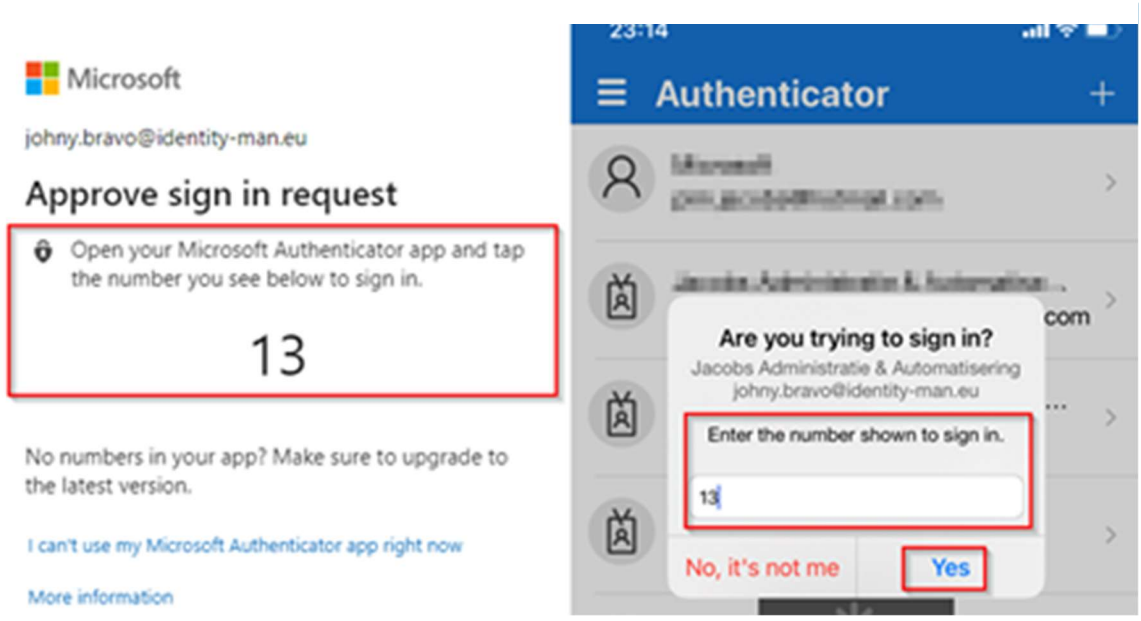
3.1.4 **Více faktorové ověřování**

Pro efektivnější zabezpečení systému se kombinuje více způsobů autentizace uživatele, například v případě krádeže či prolomení hesla. Zároveň je díky tomu možné

uživatele či správce systému varovat o potenciálním narušení bezpečnosti, pokud útočník splní pouze jeden z těchto faktorů. (Jones, 2023)

Dnes již běžně používaným systémem více faktorového ověřování je použití aplikací třetích stran na zasílání jednorázového, časově omezeného hesla. To se zobrazí na mobilním zařízení uživatele, který ho následně zadá zpět do přihlašovacího systému. Podobně se dá využít i QR kód zobrazený během přihlašování, který uživatel naskenuje v mobilní aplikaci, čímž prokáže, že je držitelem daného mobilního zařízení. Mezi nejvíce používané aplikace patří Google Authenticator či Microsoft Authenticator, který je vyobrazen na obrázku 1. Ten mimo jiné umožňuje přidat další vrstvu zabezpečení tím, že uživatel přiloží prst ke čtečce na mobilním zařízení při otevření aplikace či potvrzení přihlášení. Velikou výhodou tohoto řešení je fakt, že uživatel potřebuje pouze svůj mobilní telefon. (Lodha, 2018; Jacobs, 2021)

Obrázek 1 Proces autentizace v MS Authenticator



Zdroj: Jacobs (2021)

Biometrické údaje lze také ověřit externím zařízením připojeným přímo k počítači, jako je čtečka otisků prstu či skener obličeje nebo duhovky. Toto řešení je nákladnější na implementaci, ovšem předejde se problémům v případě, že daný uživatel sám takové zařízení nevlastní.

Dalším řešením jsou bezpečnostní tokeny, což jsou hardwarová zařízení nebo aplikace, které slouží pro ověření uživatele. V případě hardwarového zařízení se používá USB klíč, který po připojení k počítači ověří identitu uživatele. Token může být i bezdrátový, kde komunikace pro autentizaci probíhá přes Bluetooth. (Kirvan, 2023)

3.2 Komponenty autentizace fyzického přístupu

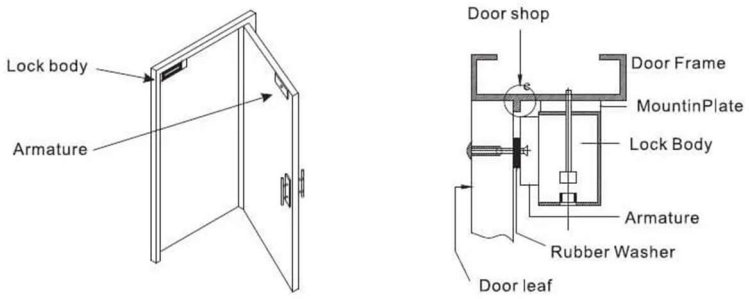
Autentizace fyzického přístupu se dělí do několika komponent, které spolu navzájem spolupracují pro navýšení bezpečnosti systému. Jedná se nejen o samotná zařízení omezující přístup, ale také o nastavení pravidel či rolí, podle kterých se rozdílná oprávnění rozdělují uživatelům.

3.2.1 Elektrické zámky

Elektrické zámky fungují pomocí elektromagnetů a slouží jako náhrada pro klasické zámky na klíč. Dvě hlavní kategorie, do kterých se elektrické zámky dělí, jsou fail-safe a fail-secure. Rozdílem je chování zámku v případě výpadku proudu. Fail-safe zámek se při výpadku proudu automaticky odemkne a umožní lidem opustit budovu nebo místnost. Je tedy vhodný pro hlavní vchody nebo kancelářské dveře, kde je bezpečí uživatelů prioritou. Fail-secure zámek zůstane ve stejné situaci zamčený, zabrání tak neoprávněnému vstupu do budovy nebo místnosti. Fail-secure zámek proto musí být možné odemknout manuálně. Je vhodný pro vysoce zabezpečené prostory, popř. požární dveře, aby se dalo zamezit rozšíření požáru. (Mehl, 2022)

Dále se elektrické zámky dělí podle principu samotného zamykání. Tím nejčastějším jsou elektromechanické, tedy zámky, které pomocí elektromagnetu aktivují mechanický zámek. Může se jednat například o klasický zámek, kde se závora zavře pomocí solenoidu. U magnetických zámků se využívá samotný magnetismus pro uzamčení. Na rám dveří se nainstaluje elektromagnet, a na dveře kovový plát. Při zavření dveří se mechanismus spustí, a elektromagnet se pevně drží plátu. Diagram pro instalaci magnetického zámku je vyobrazen na obrázku 2. (Norman, 2017)

Obrázek 2 Diagram instalace magnetického zámku



Zdroj: ShineACS (2019)

3.2.2 **Autentizační zařízení**

Každý přístupový bod musí být opatřen zařízením, přes které je možné provést autentizaci uživatele. Nejčastěji se jedná o klávesnici pro zadání číselného kódu, nebo čtečku čipových karet, které mají uživatelé u sebe. Může se také jednat o biometrická zařízení, jako skenery otisků prstů či obličeje. Dalším řešením je aplikace nainstalovaná v mobilním zařízení uživatele. Ta krom ověření, že daný uživatel zařízení vlastní, může pomocí Bluetooth komunikace s kontrolérem ověřit, že se uživatel skutečně nachází v dané lokaci. Na jednom zařízení je také možné ověřovat více způsoby najednou. (Maayan)

Obrázek 3 Autentizační zařízení na číselný kód a čipové karty

Zdroj: Palter (2020)

3.2.3 Kontrolní panel

Kontrolní panel je zařízení, které komunikuje mezi zámkem a zařízením pro ověření identity uživatele, například čtečkou karet či klávesnice. Pomocí interní paměti nebo komunikací se serverem je schopen ověřit, zda má daný uživatel dostatečná oprávnění a následně povolit nebo zabránit v přístupu. V případě chybné autentizace může tuto skutečnost zaznamenat a automaticky nahlásit. (Butchard, 2022)

3.2.4 Server na řízení přístupu

Ačkoliv je možné mít stejné ověřovací faktory pro více uživatelů, například jeden kód pro odemčení dveří uložen v interní paměti, není to ideální řešení. Správce systému bude mít přístup pouze k informacím, kdy byl kód použit, ne který specifický uživatel to byl. Problém též nastává v případě, kdy je potřeba uživateli oprávnění odebrat. Daný autentizační faktor je poté potřeba změnit pro všechny existující uživatele.

Při použití serveru jsou všechny informace ukládané do databáze. Zde se nachází informace o uživateli, jeho daná oprávnění, existující prostředky pro autentizaci (například čipová karta a informace o ní), popřípadě záznam, kdy a kde byl uživateli udělen nebo odepřen přístup. Daná oprávnění je možné jednoduše přidávat a odebírat dle potřeb správce a uživatelů. (Butchard, 2022)

3.2.5 Modely pro udělení přístupu

Tyto modely se využívají pro efektivní rozdělení oprávnění mezi uživatele s ohledem na požadavky majitele systému. Tyto modely se tradičně dělí do 5 kategorií. První je Discretionary Access Control. Zde existuje větší množství správců, kteří mohou udělovat oprávnění pro přístup. Tento model je jednoduchý na použití, ovšem má ze všech modelů nejmenší bezpečnost. (Rouse, 2023)

Druhým modelem je Mandatory Access Control. Zde je pouze jeden jediný správce, který má možnost udělovat a měnit oprávnění. Toto je velmi bezpečné řešení, díky čemuž se primárně využívá ve vládních zařízeních. Může ovšem dojít ke zpoždění přidávání oprávnění pro nové uživatele. (Awati, 2023)

Třetí model je Role-Based Access Control. V tomto modelu se každému uživateli přiřadí specifická role, která řídí jeho oprávnění. Každá role má jiná oprávnění v závislosti

na konkrétní potřebě, například vstup do serverové místnosti může být umožněn pouze technikům. Role-Based Access Control je velmi efektivní pro bezpečnost, zároveň nabízí možnost jednoduše upravovat oprávnění uživatelů podle jejich současné pozice. Nevýhodou tohoto modelu je jeho náročnost na počáteční implementaci, je nutné mít povědomí o všech možných rolích, které se v systému vyskytují, a jaká mají mít patřičná oprávnění. (Zhang, 2023)

Čtvrtým modelem je Rule-Based Access Control. Zde se daná oprávnění uživatelů mění s ohledem na předem nastavená kritéria. Je možné nastavit časové rozmezí, kdy je do prostor umožněn vstup. Dalším kritériem může být odepření přístupu do částí systému, pokud je zaznamenán neoprávněný přístup v jiné části. (McQuillan, 2022)

Posledním modelem je Attribute-Based Access Control. Tento model uděluje oprávnění na základě vlastností uživatele, akce, aplikace či prostředí. Toto řešení je velmi komplexní, jelikož udělení oprávnění přístupu se může lišit pro jednoho uživatele v závislosti na několika faktorech, např. čas přístupu, druh aplikace, ke které se snaží získat přístup, nebo také v závislosti na čase. Tento model je vyobrazen na obrázku 4. (Gašparík, 2014)

Obrázek 4 Model Atrribute-Based Access Control

Zdroj: Gašparík (2014)

3.2.6 **Alarmy**

Alarmy jsou důležitou součástí systémů ochrany fyzického přístupu. Jedná se o zařízení, která detekují neoprávněný vstup a upozorňují vybrané pracovníky na narušení systému. Alarmy mohou potenciální narušitele odradit hlukem nebo blikajícími světly, ale také upozornit ostrahu na narušení a pomoci jim rychle a účinně reagovat. Lze je také

přizpůsobit potřebám a preferencím systému, například nastavením různých úrovní poplachu, zón nebo časových plánů.

V případě, že se uživatel snaží dostat do části systému, do kterého nemá oprávnění, bude o tom notifikován správce. Ten se potom pomocí komunikačních kanálů může dotázat, zda se jednalo o pouhý omyl, či zda byl autentizační faktor uživatele odcizen. Při umístění senzoru do rámu dveří lze také zjistit, zda byly otevřené bez použití daného faktoru. Mimo jiné lze také upozornit uživatele a správce v případě, že dveře nebyly správně zavřeny, nebo jsou drženy moc dlouho. (Norman, 2017)

3.2.7 **Kamery**

Kamery neslouží jako aktivní prvky autentizace, stále jsou ale velmi důležitou částí bezpečnosti fyzického přístupu. V případě neoprávněného vniknutí do prostor systému je možnost, že pachatel odhalí svou identitu. Zároveň je možné sledovat pohyb jednotlivých uživatelů po systému, pro kontrolu, zda se nepohybují na místech, kam nemají oprávnění vstoupit. Kamery lze také napojit na alarm, který se spustí v případě zaznamenání pohybu v době, kdy mají být prostory prázdné. (Lewis-Rippington, 2021)

Aby bylo použití kamerového systému co nejefektivnější, je důležité mít dostatečný počet kamer umístěných v kritických lokacích. Vchody do budov jsou často vyhodnoceny jako nejdůležitější místo pro umístění kamer. Dále je dobré instalovat kamery do místností a chodeb, kde se pohybuje velké množství lidí. Tyto místnosti jsou často vstupní haly a pracoviště. Také je potřeba umístit kamery do místností, kde se nachází cenné předměty a zařízení důležitá pro chod firmy, jako jsou sklady serverovny. (Wilson, 2021)

3.3 **Komponenty autentizace logického přístupu**

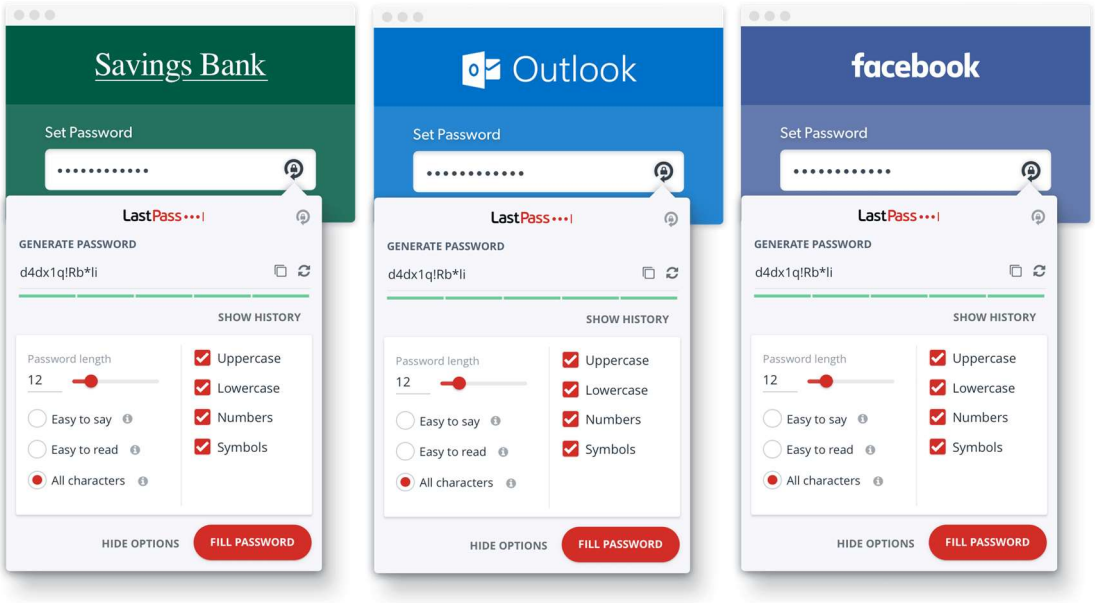
Komponenty pro autentizaci logického přístupu jsou z části stejné, jako pro fyzický přístup. Uživatel může například používat jednu čipovou kartu pro otevření dveří, i pro přihlášení do svého pracovního počítače. Stejně tak mohou být informace o uživateli a jeho oprávněních vedena na stejném serveru pro oba druhy přístupu. Na rozdíl od fyzického přístupu sem ovšem patří i jiné faktory, jako jsou dostatečně silná hesla či ochrana vzdáleného připojení.

3.3.1 **Hesla**

Hesla jsou velmi rozšířeným způsobem zabezpečování přístupu k datům. Ne ke všem zařízením je možné napojit čtečku karet či skener otisku prstů. Je ovšem velmi důležité praktikovat zásady výběru a používání vhodných hesel. Heslo uživatele má být dostatečně dlouhé, zároveň nemá obsahovat osobní informace či běžně používaná slova, která se dají snadno odhadnout.

Doporučuje se také nepoužívat stejné heslo pro přihlašování do více systémů a služeb. Pro pomoc se zapamatováním většího množství hesel se dají využít programy pro správu hesel. Ty daná hesla umožňují náhodně generovat pro každý účet a ukládat je, viz obrázek 5. (Jones, 2022)

Obrázek 5 Aplikace LastPass pro generaci a správu hesel



Zdroj: LastPass (2018)

3.3.2 **Ukládání hesel**

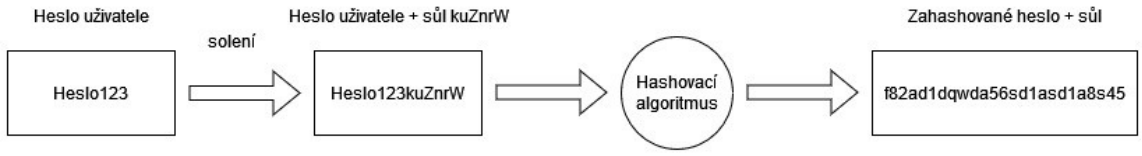
V případě, že se uživatelská hesla ukládají do samotného systému, je zapotřebí zajistit jejich správné zabezpečení. Hesla by se nikdy neměla ukládat jako prostý text, jelikož by v případě neoprávněného přístupu do databáze měl útočník okamžitý přístup ke všem heslům v systému. Místo toho se využívá hashování a solení.

Hashování hesel je technika, která transformuje heslo do jiné podoby, kterou je obtížné vrátit zpět. Používá se k bezpečnému ukládání hesel do databází, takže i když k ní někdo získá přístup, nemůže přečíst původní hesla. Při hashování hesel se používají speciální

algoritmy, jako je SHA-256 nebo Argon2, které jsou navrženy pro rychlý výpočet, ale obtížné prolomení.

Solení je technika, která zvyšuje zabezpečení hesla. Jedná se o proces, při kterém se ke každému heslu před jeho zahashováním přidá jedinečný náhodný řetězec znaků, tzv. sůl. Sůl je uložena společně s hashem, takže původní heslo nelze obnovit bez znalosti soli a hashe. Solení zvyšuje odolnost hashování hesel proti útokům, jako jsou slovníkové útoky nebo útoky duhovou tabulkou, které se snaží uhodnout hesla porovnáním hashů s předem vypočtenými tabulkami běžných hesel a jejich hashů. Solení zajišťuje, že i když mají dva uživatelé stejné heslo, jejich hashe se budou lišit, jelikož mají rozdílné sole. Jedním z příkladů solení je technologie SSHA, kde je před zahashováním hesla pomocí algoritmu SHA přidána sůl. (Stytch, 2022)

Obrázek 6 Funkce solení společně s hashovacím algoritmem



Zdroj: Vlastní zpracování (2023)

3.3.3 **VPN**

Vzdálené připojení k síti je v dnešní době běžné, zejména pro uživatele pracující primárně z domova. Virtual Private Network (virtuální privátní síť) pro vzdálené připojení je prostředek, pomocí kterého se vytvoří zabezpečený tunel mezi zařízením uživatele a firemní sítí přes internet. VPN umožňuje přístup k interním zdrojům společnosti, jako jsou soubory, aplikace nebo databáze, jako kdyby se uživatel nacházel v prostorách společnosti. Hlavním účelem použití VPN je skrytí komunikace mezi uživatelem a koncovou sítí, například pomocí šifrování dat. Dalším účelem je autentizace uživatele, kde koncový systém zamítne komunikaci se zařízeními, které nejsou přímo v lokální síti, nebo připojené přes VPN. (Spadafora, 2020)

3.4 **Propojení autentizace fyzického a logického přístupu**

Vzájemná integrace různých komponentů pro autentizaci fyzického a logického přístupu může zefektivnit proces ověřování. Po přidání nového uživatele může být

automaticky vyslán příkaz pro vytvoření nové čipové karty, pomocí které uživatel získá přístup do prostor, a zároveň pro přihlášení do systému. V případě využití jiných autentizačních faktorů, například biometrických vlastností, může být vyslán požadavek uživateli o přidání potřebných faktorů do systému. (Rightcrowd, 2023)

Propojení obou přístupů zároveň zlepší proces monitoringu všech uživatelů v systému. Velmi častou chybou zabezpečení fyzického přístupu je tzv. tailgaiting. V této situaci vejde uživatel do budovy poté, co jiný uživatel potvrdil svou identitu, aniž by se dveře zavřeli. Systém později může zaznamenat pokus o přihlášení k počítači nebo otevření dveří uvnitř prostor, aniž by měl záznam o vstupu uživatele do budovy. V tomto případě se uživateli může oprávnění odepřít, popřípadě tuto situaci nahlásit správci. Tímto se zvýší důraz na dodržování řádných procedur autentizace, zároveň se předejde potenciálnímu přístupu neoprávněné osoby k zařízením a prostorám uvnitř budovy. (Stallings, 2014; Managing access control – combining physical and logical security, 2007)

V kombinaci s kamerou je také možnost spustit záznam v případě, že uživatel vstoupí nebo opustí prostor. Záznam lze následně porovnat s další aktivitou uživatele pro zjištění, zda to opravdu byl daný oprávněný uživatel. (Lewis-Rippington, 2021)

3.5 Hrozby

Při návrhu bezpečné autentizace systému je nutné se nejprve obeznámit s hrozbami, které mohou integritu systému narušit.

3.5.1 Sociální inženýrství

Sociální inženýrství je typ útoku, který využívá lidské zranitelnosti, jako je důvěra, zvědavost nebo chamtivost, pro prolomení autentizačních systémů. Útoky sociálního inženýrství mohou využívat různé techniky pro oklamání nebo přesvědčení uživatele, aby prozradil své přihlašovací údaje, nebo umožnil útočníkovi přístup do budovy.

Při využití techniky phishing se útočník snaží, aby uživatel provedl akce, které ohrožují jeho bezpečnost, například kliknutí na škodlivé odkazy nebo přílohy. Dalším útokem může být záměna USB zařízení za falešné, které se po připojení k počítači chová normálně, ale na pozadí posílá data útočníkovi. Může se jednat o flash disk, nebo i klávesnici, která zaznamenává a ukládá stisknuté klávesy. (Copado, 2022; Creutzburg, 2017)

Těmto útokům může být velmi těžké předejít, jelikož neútočí na vadu v systému, ale na uživatele samotné. Proto je důležité vzdělávat uživatele o rizikách a příznacích sociálního inženýrství a o tom, jak se před takovými útoky chránit.

Obrázek 7 Proces útoku sociálního inženýrství

Zdroj: Sanders (2024)

3.5.2 **Ztráta a odcizení identifikačních faktorů**

Pokud systém nebo jeho části využívají jenom jeden identifikační faktor pro autorizaci, jeho ztráta či krádež představuje velké bezpečnostní riziko. I v případě, že přístup do logické části systému je chráněn dalšími faktory, pouhý přístup do budovy umožní útočníkovi nalézt tištěné dokumenty s citlivými informacemi, pokud nejsou řádně zabezpečeny. Dále si může udělat přehled o pohybu uživatelů a potenciální příležitosti pro další útok. (Ahola)

Opět je nutné poučit uživatele o správném zacházení s autentizačními faktory. Pokud uživatel zjistí, že daný faktor nemá, musí to okamžitě nahlásit správci systému. Také by měli mít přehled o ostatních uživatelích. Pokud se člověk v systému chová mimo normu, nebo není uživateli povědomý, ačkoliv ví, kdo se v dané části systému má pohybovat, měl by tuto skutečnost nahlásit.

3.5.3 **Návštěvníci**

Osoby, které se nacházejí v systému, aniž by se jednalo o uživatele, by stále měli mít formu autentizace. V případě zjištění neoprávněného přístupu do systému je zapotřebí zjistit, zda se dané osoby nacházeli v prostorách budovy, popřípadě v jakých. To se dá zajistit návštěvnickou čipovou kartou. Ta by zároveň měla mít pouze taková oprávnění pro přístup, která návštěvník potřebuje. (Khairallah, 2005)

3.5.4 **Malware**

Malware je hromadné označení pro škodlivý software, který má za cíl poškodit koncové zařízení či síť, nebo získat neoprávněný přístup k datům. Aby se předešlo ztrátě dat či poškození zařízení, je nutné poučit uživatele o správném zacházení při procházení internetu nebo stahování souborů. Dále je důležité aktualizovat jednotlivá zařízení, a zálohovat data do cloudu nebo na externí úložiště. V případě počítačů se také doporučuje mít nainstalovaný antivirový program, který je schopen kontrolovat webové stránky, na které uživatel vstoupil, stahované soubory či provést kontrolu celého zařízení. (Holmes, 2023)

4 Vlastní práce

V praktické části této práce je nejprve představen systém a požadavky jeho majitele ohledně nových metod autentizace fyzického a logického přístupu. Na základě zjištěných potřeb byly vybrány nové způsoby autentizace, které byly předneseny majiteli.

4.1 Seznámení se systémem

Systém, jímž se tato práce zabývá, je malý podnik, ve kterém se aktuálně pohybuje 32 uživatelů. Je zde nutno podotknout, že ne každý uživatel přistupuje do systému ve stejnou chvíli. Různá oddělení mají odlišné směny, zároveň malá část uživatelů pracuje dálkově z domova. Pro přístup do systému slouží hlavní vchod, krom toho se zde nachází i vedlejší vchod pro rychlý přístup do skladu.

Pro práci využívají uživatelé jak stolní počítače, tak firemní laptopy, které jsou připojené do dockovacích stanic. Zároveň laptopy využívají i uživatelé, kteří pracují dálkově. Dále se v systému nachází i místnost s vlastním serverem, na kterém jsou provozovány webové stránky firmy. Server též slouží pro interní funkce, jako je hostování ovládacích panelů a nástrojů pro uživatele v systému. Také se zde nachází firemní NAS pro ukládání a přístup k datům.

4.1.1 Současné metody autentizace v systému

Současné metody autentizace v systému jsou na relativně nízké úrovni. Samotný přístup do budovy je u obou vchodů zabezpečen pouze tradičním zámkem na klíč. Jednotlivé místnosti uvnitř systému jsou sice odděleny dveřmi se zámkem, většina z nich ovšem i po pracovních hodinách zůstává odemčená. Pouze dveře do skladu a místnosti s firemním serverem se zamykají.

V hale u hlavního vchodu se nachází detektor pohybu napojen na alarm. Při příchodu prvního uživatele do systému je pohyb zaznamenán, následně je nutné zadat během 15 vteřin číselný kód. Při opakovaném zadání špatného kódu či pokud není kód zadán včas, je spuštěn hlasitý alarm.

Přístup do počítačů a laptopů je ošetřen pouze nativním přihlašovacím systémem ve Windows. Při práci na počítačích využívají uživatelé Microsoft Office 365 Business Standard, pro přístup k aplikacím jako Word či Excel. Pro přihlášení do aplikací této služby

je krom přihlašovacích údajů využívána také mobilní aplikace Microsoft Authenticator, pro zajištění dvou faktorového ověření.

Pro vzdálený přístup z domova do firemní NAS je využíván protokol FTPS pomocí aplikace FileZilla. Uživatelé musí zadat správné přihlašovací údaje, aby byl přenos dat umožněn.

4.1.2 **Hrozby v aktuálním systému**

Jak je zřejmé z předchozí sekce, systém v současném stavu vykazuje značné zranitelnosti vyplývající ze zastaralých metod ověřování. Dveře zabezpečené jednoduchým zámkem na klíč představují značné riziko, protože tyto klíče lze snadno ztratit a mohou být odcizeny, nebo také duplikovány, což ohrožuje integritu prostor.

Ačkoliv je hlavní vchod opatřen alarmem napojeným na detektor pohybu, slouží primárně pro odstrašení potenciálního útočníka, jelikož pouze spustí zvukový signál. Není připojen k žádnému systému, který by ohlásil neoprávněný vstup majiteli, nebo na pult centrální ochrany bezpečnostní společnosti.

Co se autentizace logického přístupu týče, spoléhání se pouze na jednoduchou ochranu heslem pro přístup k počítači činí systém náchylným k neoprávněnému vstupu. Stejný problém má i využití FTPS pro přístup k NAS. Tento protokol je sice šifrovaný, ovšem kdokoli, kdo získá přístup k přihlašovacím údajům, může potenciálně ohrozit integritu a důvěrnost uložených dat. Absence více faktorového ověřování mimo přihlášení do Office 365 dále zvyšuje náchylnost systému ke zneužití. Tyto zranitelnosti zdůrazňují potřebu zavedení moderních a bezpečných ověřovacích mechanismů, které posílí obranu systému proti hrozbám.

4.2 **Seznámení se s požadavky majitele systému**

Majitel systému má tři hlavní požadavky ohledně nového řešení. Zvýšení bezpečnosti, jednoduchost, a flexibilita. Mimo tyto obecné požadavky by chtěl majitel v rámci logického přístupu využít více faktorové ověřování i při přihlašování do firemních zařízení. Na konečné ceně majiteli nezáleží, primárně z důvodu, že ceny poskytovatelů autentizačních služeb jsou velmi individuální dle přesných potřeb každého systému.

4.2.1 **Zvýšení bezpečnosti**

Prvním a zároveň nejdůležitějším požadavkem nového řešení je zvýšení bezpečnosti celého systému v rámci autentizace fyzického a logického přístupu. Co se fyzického přístupu týče, majitel si přeje, aby měl neustálý přehled o tom, kdo se aktuálně v systému nachází. Dále je důležité, aby do systému neměl přístup neoprávněný uživatel, popř. aby bylo případné neoprávněné vniknutí do prostoru rychle odhaleno. V rámci autentizace logického přístupu je potřeba zamezit možnosti neoprávněného přístupu do firemních zařízení a k citlivým datům, jak v prostorách systému, tak při práci z domova.

4.2.2 **Jednoduchost**

Požadavek pro jednoduchost se vztahuje jak k samotnému používání systému po implementaci nového řešení, ale také na proces implementace samotné. Vyšší míra zabezpečení by neměla bránit oprávněným uživatelům při výkonu práce, přístup má být udělen rychle a efektivně. Zároveň se tak sníží i potřeba pro nadměrné školení uživatelů ohledně samotného používání nového řešení, a bude možné se soustředit na školení ohledně hrozeb a bezpečnosti. V rámci implementace je potřeba se zaměřit na jednoduchost a rychlost instalace nových zařízení.

4.2.3 **Flexibilita**

Pod pojmem flexibilita si majitel systému představuje schopnost systému vyvíjet se a přizpůsobovat se v čase, zejména pokud jde o možnost modernizace. Flexibilní řešení by mělo být možno integrovat s novými technologiemi a přizpůsobit se budoucímu pokroku, aniž by vyžadovalo rozsáhlé opravy nebo narušení stávající infrastruktury. To znamená, že architektura nového řešení by měla být modulární a škálovatelná, což umožní snadné začlenění aktualizací, a vylepšení nových autentizačních faktorů, jakmile budou k dispozici.

4.2.4 **Více faktorové ověřování**

Ačkoliv se v současném systému využívá více faktorové ověřování pro přístup do služeb Office 365, pro přihlášení do firemních zařízení stačí pouze znalost hesla. Majitel požaduje, aby se i v těchto případech bylo nutné prokázat více faktory.

4.3 Výběr metod autentizace fyzického přístupu

4.3.1 Způsob řešení

Prvním krokem pro výběr metod autentizace fyzického přístupu bylo rozhodnutí, zda se bude implementovat vlastní řešení pro autentizaci, či řešení od poskytovatelů bezpečnostních služeb. Pro tento krok byla provedena vícekriteriální analýza variant pro obě řešení. Kritéria a jejich váhy pro analýzu jsou vzata z požadavků majitele systému.

Tabulka 1 Vícekriteriální analýza variant pro způsob řešení

			Vlastní řešení		Poskytovatel	
Kritéria	Pořadí	Váha	Body	Vážený průměr	Body	Vážený průměr
Bezpečnost	1.	0,5	7	3,5	8	4
Použitelnost	2.	0,2	6	1,2	7	1,4
Jednoduchost implementace	2.	0,2	5	1	7	1,4
Flexibilita	4.	0,1	8	0,8	6	0,6
Celkem		1		6,5		7,4

Zdroj: Vlastní zpracování (2023)

Každému kritériu bylo přiřazeno bodové ohodnocení od 0 do 10. V následujících podkapitolách jsou rozebrány jednotlivá ohodnocení všech kritérií pro obě varianty.

Bezpečnost

Tomuto kritériu bylo pro vlastní řešení přiřazeno 7 bodů. Vlastní řešení může být od základu navrženo s ohledem na bezpečnost a obsahovat pokročilé metody šifrování, jedinečné ověřovací protokoly a bezpečnostní funkce přizpůsobené konkrétním hrozbám, kterým systém čelí.

Existuje zde ovšem riziko bezpečnostních zranitelností, pokud není vlastní řešení správně implementováno, nebo pokud dojde k chybám v procesu vývoje. Toto riziko může vzniknout z několika důvodů, jako jsou nedostatečné odborné znalosti techniků,

nedostatečně důkladné testování nebo špatné dodržování osvědčených bezpečnostních postupů při implementaci.

Pro variantu od poskytovatele bylo bezpečnosti přiřazeno 8 bodů. Řešení od poskytovatele obvykle nabízejí standardizovaná bezpečnostní opatření a těží z rozsáhlého testování, osvědčených postupů v oboru a průběžných aktualizací zaměřených na nové hrozby. Ovšem ne všechna mohou být přizpůsobitelná konkrétním potřebám firmy.

Dále řešení od poskytovatele závisí na jejich odborných znalostech a pověsti. Přestože zavedení poskytovatelé mohou nabízet robustní bezpečnostní funkce, stále existuje určitá míra závislosti na schopnosti poskytovatele udržovat bezpečnostní standardy, včas řešit zranitelnosti a chránit před vnějšími hrozbami.

Použitelnost

Pro použitelnost bylo vlastnímu řešení přiděleno 6 bodů. Toto řešení nabízí výhodu přizpůsobení konkrétním potřebám firmy, také zajišťuje konzistenci se stávajícími systémy a umožňuje integraci rychlé zpětné vazby od uživatelů, čímž zvyšuje celkovou použitelnost a následné úpravy.

Vývoj vlastního řešení však vyžaduje specializované odborné znalosti a zdroje, a pokud vývojářský tým nemá zkušenosti s návrhem uživatelského rozhraní a zásadami použitelnosti, hrozí riziko komplikací. Pro uživatele může být nezbytné školení a zaškolení, aby se přizpůsobili novému řešení, a pro řešení problémů s použitelností a zajištění spokojenosti uživatelů je nezbytná průběžná údržba. Od majitele bylo zjištěno, že v oblasti použitelnosti nemá žádný z uživatelů v systému dostatečné odborné znalosti. Bodové ohodnocení je tedy nižší.

Řešení od poskytovatele obdrželo v použitelnosti 7 bodů. Často nabízí výhodu kompletních a uživatelsky přívětivých funkcí, takže je lze poměrně snadno nastavit a používat bez rozsáhlých úprav. Díky standardizovaným bezpečnostním opatřením a zdrojům podpory poskytovatele může řešení poskytnout uživatelům bezproblémové a intuitivní ověřování.

Řešení od poskytovatele však může postrádat možnosti přizpůsobení vlastního řešení vytvořeného na míru, což může omezit jeho schopnost splnit jedinečné požadavky firmy na použitelnost. I když jsou od poskytovatele k dispozici zdroje pro školení a podporu, systém může stále čelit problémům při funkčnosti nového řešení se stávajícími systémy

a pracovními postupy. Navíc spoléhání se na odborné znalosti a aktualizace poskytovatele přináší určitou míru závislosti a nejistoty ohledně budoucího vývoje a kompatibility.

Jednoduchost implementace

Pro jednoduchost implementace pro vlastní řešení bylo přiděleno 5 bodů. Díky možnosti přizpůsobit řešení konkrétním požadavkům a využití interní odborné znalosti o chodu systému lze proces implementace zefektivnit a optimalizovat z hlediska efektivity. Majitel má navíc kontrolu nad časovým plánem implementace a může upřednostnit klíčové vlastnosti a funkce, aby vyhověla okamžitým potřebám.

Jako u ostatních kategorií je zde však potřeba odborné znalosti a zdrojů. Pokud systém nemá dostatečný přehled o problematice, hrozí riziko komplikací. Je zapotřebí nakoupit veškeré nové vybavení a zajistit, aby daná zařízení šlo navzájem integrovat pro zajištění větší efektivity. Zároveň u této varianty hrozí riziko, že s nově nakoupeným vybavením vzniknou nečekané problémy. Je poté potřeba zjistit, která zařízení jsou problémová. V případě, že problém nelze vyřešit, je nutné objednat nová zařízení.

Druhé variantě bylo přiřazeno 7 bodů. Řešení od poskytovatele nabízí výhodu rychlé a snadné implementace díky předem připraveným metodám pro autentizaci a standardizovaným možnostem integrace. Díky hotovým funkcím může být proces implementace zjednodušený a efektivní, což minimalizuje narušení provozu. Dále se také poskytovatel postará o výběr a obstarání potřebných zařízení a softwaru.

Implementace řešení od poskytovatele však může vyžadovat, aby systém přizpůsobil své pracovní postupy novým funkcím. Zároveň možnosti nabízené poskytovatelem mohou být omezené, proto je zapotřebí prozkoumat, zda daný poskytovatel skutečně splňuje všechny požadavky majitele systému, aby nemuselo dojít ke kompromisu.

Flexibilita

Flexibilitě pro vlastní řešení bylo přiřazeno 8 bodů. Vzhledem k osobním zkušenostem uživatelů se systémem umožňuje vlastní řešení velikou míru flexibility, co se výběru metod autentizace týče. Nabízí také vyšší úroveň škálovatelnosti, což systému umožní navrhnout procesy ověřování podle toho, jak se vyvíjí, a zajistí se tak soulad s měnícími se požadavky a technologickým pokrokem. Systém také není závislý na technologiích jednoho poskytovatele, který nemusí vždy dodávat nejnovější zařízení a metody zabezpečení.

Vlastní řešení však může vyžadovat více času a zdrojů, jelikož současné řešení nemusí být kompatibilní s nejnovějšími technologiemi a metodami autentizace. V takovém případě je možné, že se velká část autentizačního systému bude muset navrhnout a implementovat znovu.

Pro řešení od poskytovatele bylo přiřazeno 6 bodů. V závislosti na vybraném poskytovateli může být flexibilita a škálovatelnost součástí jejich služeb, což velmi urychluje proces implementace nových technologií. Nemusí se jednat pouze o nová zařízení, ale také o aktualizace, které jsou schopny rozšířit funkcionalitu současného autentizačního systému.

Na druhou stranu je zde ovšem riziko, že se systém stane závislý na jednom poskytovateli. To může ohrozit bezpečnost systému, např. v případě, že poskytovatel přestane dodávat nejnovější aktualizace na vyvíjející se hrozby. Tato závislost také ztěžuje přechod na alternativní řešení nebo poskytovatele v budoucnu, pokud se tak majitel rozhodne.

Výsledek analýzy

Po přepočítání a součtu vážených průměrů vyšlo, že je pro majitele lepší zvolit řešení od poskytovatele bezpečnostních služeb. Výsledek a odůvodnění byly předneseny majiteli, který poté toto řešení odsouhlasil. Ačkoliv by vlastní řešení umožnilo vyšší míru flexibility, majitel se obává, že proces implementace by zabral moc času, spolu s větším rizikem nekompatibility jednotlivých komponent. Dále také v systému nejsou odborníci na použitelnost, výsledné řešení by tedy nemuselo být uživatelsky přívětivé.

4.3.2 Výběr služeb od poskytovatele

Na pokyn majitele byla jako poskytovatel bezpečnostního řešení vybrána společnost IMA s.r.o. Společnost nabízí širokou škálu možných produktů, které splňují všechny požadavky majitele. Produkty spolu umí navzájem komunikovat, implementace a jejich používání je jednoduché. Společnost také nabízí robustnější řešení pro případnou potřebu větších změn v bezpečnostním systému. Jeden nedostatek tohoto řešení je, že dodávaný software pro správu uživatelů je dostupný pouze na systému Windows. Toto ovšem majiteli systému nevadí, jelikož pro práci uživatelé používají právě tento operační systém. Může to však vést k problémům, pokud se zařízení s Windows budou nahrazovat, např. za MacOS.

V následujících podkapitolách budou představeny produkty, které byly vybrány na základě požadavků majitele. Informace o společnosti a produktech byly brány z webových stránek společnosti (IMA).

Přístupový systém

Pro autentizaci uživatele při vstupu do systému a při pohybu v jeho částech byl vybrán produkt IMAporter Basic. Databáze, která uchovává informace o oprávněných uživatelích, je přístupná přes software, který je určen pro platformu Windows. Správce systému má na starosti udělování a odebírání oprávnění, což umožňuje správu bez nutnosti kontaktování dodavatele. Uživatelé se mohou identifikovat buď pomocí karty s NFC čipem, nebo přes mobilní zařízení. Po úspěšné autentizaci bude uživateli umožněn vstup do budovy či specifické místnosti.

Docházkový systém

Komplexní docházkový systém od společnosti IMA umožňuje zaznamenání příchodu a odchodu zaměstnanců, mimo jiné ho lze také napojit na kamerový a přístupový systém. Další výhodou je, že pro docházkový systém lze použít stejný identifikátor jako pro přístup.

Kamerový systém

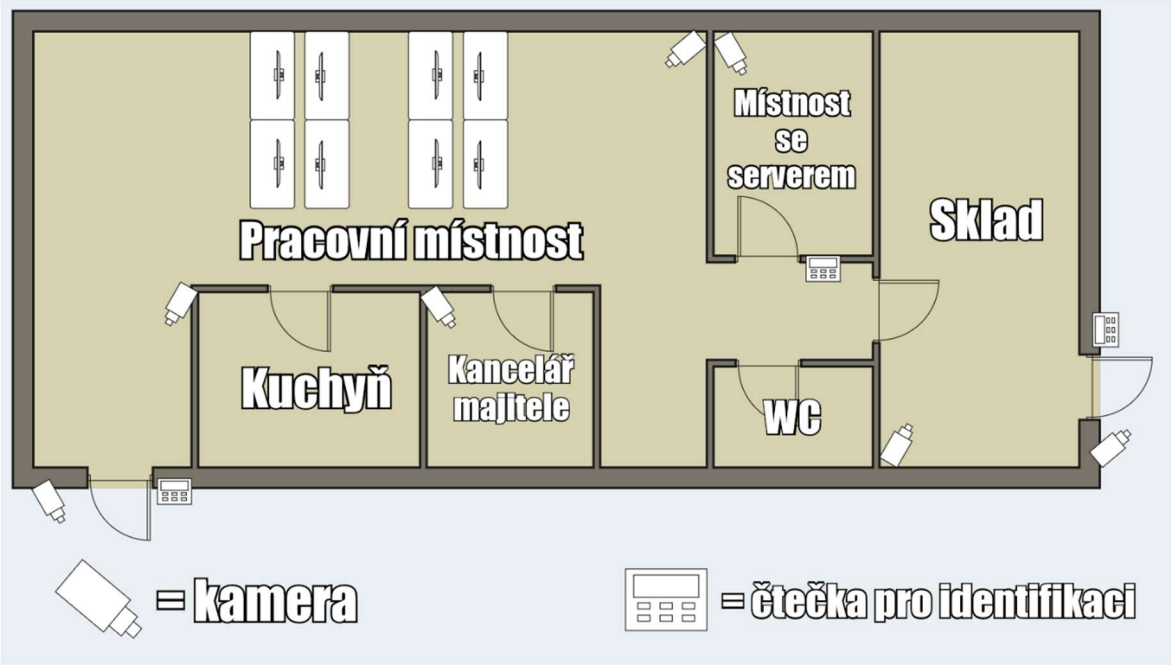
Kamery je možné sledovat živě, nebo zpětně ze záznamu. Spolu s výše zmíněnou integrací s přístupovým a docházkovým systémem je tak možné snadno dohledat, kde se který uživatel pohybuje, nebo pohyboval. Zároveň toto řešení nahradí čidlo pohybu, které je aktuálně implementováno v systému.

4.3.3 Umístění jednotlivých bezpečnostních prvků

Pro potřeby této práce byl vytvořen schematický nákres, který znázorňuje umístění bezpečnostních kamer a dveří, které je potřeba zabezpečit. Je nutno podotknout, že nákres neodpovídá skutečnému systému. Toto rozhodnutí bylo učiněno na žádost majitele s cílem

ochrany citlivých informací o skutečném fyzickém rozložení systému. Toto schéma však odpovídá skutečnosti natolik, aby se dalo využít pro vizualizaci a diskusi.

Obrázek 8 Schématický nákres umístění kamer a přístupového systému



Zdroj: Vlastní zpracování (2023)

V systému bylo vybráno několik kritických prostor, která je potřeba sledovat pomocí bezpečnostních kamer. Jedná se o venkovní prostory v blízkosti obou vchodů, místnost se serverem, sklad, vstupní halu u hlavního vchodu, pracovní prostor pro uživatele, a kancelář majitele systému.

Dále byly určeny dveře, které je potřeba zabezpečit pomocí přístupového systému. Zde se jedná o oba vchodu do prostor budovy, a zároveň také do místnosti se serverem. Do této místnosti mají oprávnění vstupu pouze technici, nikoliv uživatelé z jiných oddělení.

4.4 Výběr metod autentizace logického přístupu

V rámci výběru metod autentizace logického přístupu byla problematika rozdělena na dvě části. Prvně byla vybrána nová metoda pro přihlašování uživatelů do firemních zařízení při využití více faktorového ověřování, následně byl ošetřen bezpečný vzdálený přístup při práci z domova.

4.4.1 **Výběr metody více faktorového ověřování**

Pro výběr nového řešení byla použita vícekriteriální analýza variant. Kritéria a jejich váhy pro volbu nové autentizace logického přístupu jsou stejná, jako v kapitole 4.3.1 pro fyzický přístup. Po diskusi s majitelem systému byly pro analýzu vybrány varianty pro použití mobilní aplikace, konkrétně Microsoft Authenticator z důvodu, že jej uživatelé už aktuálně používají pro službu Office 365. Dalšími variantami jsou externí čtečky otisku prstů, a USB klíče. V následujících podkapitolách jsou opět rozebrána všechna ohodnocení.

Tabulka 2 Vícekriteriální analýza variant pro více faktorové ověřování

			MS Authenticator		Čtečka otisků prstů		USB klíč	
Kritéria	Pořadí	Váha	Body	Vážený průměr	Body	Vážený průměr	Body	Vážený průměr
Bezpečnost	1.	0,5	9	4,5	10	5	8	4
Použitelnost	2.	0,2	9	1,8	7	1,4	8	1,6
Jednoduchost implementace	2.	0,2	8	1,6	7	1,4	8	1,6
Flexibilita	4.	0,1	8	0,8	8	0,8	9	0,9
Celkem		1		8,7		8,6		8,1

Zdroj: Vlastní zpracování (2024)

Bezpečnost

Nejlepší bodové ohodnocení bylo uděleno pro čtečku otisků prstů. U moderních zařízení lze dosáhnout velmi vysoké úspěšnosti pro oprávněné uživatele, zároveň mají velice nízkou šanci udělit přístup neoprávněnému uživateli. Otisk prstu je také velmi obtížné zfalšovat pro potřeby neoprávněného vniknutí do systému.

MS Authenticator bylo uděleno 9 bodů. Ačkoliv je možné, aby byl telefon odcizen či ztracen, v systému mají všichni uživatelé přístup do telefonu ošetřen PIN kódem či biometrikou. Zároveň je mobilní telefon možné vzdáleně deaktivovat pomocí počítače. V aplikaci je také možné využít biometrické údaje i během potvrzení žádosti o přihlášení v aplikaci.

Nejméně bodů, konkrétně 8, bylo přiděleno USB klíči. Přestože poskytují silné bezpečnostní prvky, jako je hardwarové šifrování a kryptografické ověřovací protokoly, je

zde poměrně riziko ztráty či krádeže, což může ohrozit bezpečnost. Zároveň je zde šance, že uživatel omylem zapomene klíč v počítači. Je ovšem nutno podotknout, že na trhu existují USB klíče opatřené vlastní čtečkou otisků prstů, které bezpečnost navyšují.

Použitelnost

Nejvíce bodů pro toto kritérium bylo uděleno aplikaci MS Authenticator. Telefon je zařízení, které má každý z uživatelů systému neustále u sebe. Proces autentizace samotné je velice jednoduchý, stačí přepsat číselný kód uvedený na počítači do aplikace, popř. dodatečně použít biometrický údaj pro potvrzení identity.

USB klíč byl ohodnocen 8 body. Samotné používání klíče je snadné, stačí ho jednoduše zasunout do USB portu na počítači. Počítač ovšem nemusí mít volný USB port, v tom případě je nutné vypojit nějaké jiné zařízení. Zároveň musí uživatel USB klíč nosit s sebou, u velké části modelů je ale možné jej nosit na klíčence.

Čtečka otisků prstů byla ohodnocena 7 body. U čtečky může použitelnost ovlivnit navlhčení či poranění prstu. V tomto případě nebude uživateli umožněno se přihlásit. Pokud uživatel pracuje na laptopu z domova, je zapotřebí zajistit, aby měl ke čtečce přístup. To by pro něj znamenalo nošení čtečky s sebou, nebo aby majitel zajistil nové laptopy s integrovanou čtečkou.

Jednoduchost implementace

U tohoto kritéria bylo USB klíči uděleno 8 bodů. Majitel systému má na výběr vytvořit pomocí speciálního softwaru vlastní USB klíč, nebo ho zakoupit od poskytovatele, kteří také nabízejí vlastní software pro nastavení a autorizaci. Windows také nabízí možnost nastavení USB klíče pro přihlášení v rámci Windows Hello, je ovšem potřeba aby klíč splňoval standard FIDO2. Krom samotného USB klíče a softwaru je pro implementaci také potřeba volný USB port na firemním zařízení, zároveň musí být daný port kompatibilní s verzí USB na klíči.

Aplikace MS Authenticator byla ohodnocena 8 body. Pro implementaci je potřeba otevřít nastavení účtu Microsoft, a povolit režim Účet bez hesla. Při dalším přihlášení už bude potřeba provést autentizaci pomocí aplikace. Jelikož už účet nebude opatřen heslem, ztrácí takto tento způsob více faktorové ověřování. Tomu se dá ovšem předejít tím, že se pro použití aplikace nastaví potřeba ověření biometrikou.

Čtečce otisků prstů bylo přiděleno 7 bodů. Pro implementaci se dá využít funkce Windows Hello, daná čtečka s ní ovšem musí být kompatibilní. Pokud není, je zapotřebí použít software dodaný s čtečkou. Jedním z problémů tohoto řešení je, že musí být dostupné na všech firemních zařízeních. To může způsobit komplikace při implementaci na laptopech sloužících pro práci z domova. Zároveň je zde potřeba volný USB port pro připojení čtečky k zařízení.

Flexibilita

Pro kritérium flexibility bylo USB klíči uděleno 9 bodů. Jelikož je zapotřebí pouze volný USB port a software, dá se toto řešení snadno nahradit modernějšími verzemi nebo klíči, které mají zabudované funkce požadované při budoucím rozšiřování zabezpečení. Pokud se ovšem budou pořizovat nová firemní zařízení, nemusí vlastnit požadovaný port na USB. Pokud jsou současné klíče typu USB A, ale nově zakoupené laptopy mají pouze porty typu USB-C, bude potřeba zakoupit navíc redukce či kompletně nové klíče.

MS Authenticator byl ohodnocen 8 body. Zde se snížené hodnocení váže na obtížnost přestupu na nové mobilní zařízení. Na rozdíl od např. aplikace Google Authenticator se nelze pouze přihlásit na novém zařízení a získat přístup do aplikace. Je potřeba přejít do nastavení účtu a manuálně nastavit nové mobilní zařízení pro autentizaci.

Čtečce otisků prstů bylo přiděleno 8 bodů. S rozvojem nových technologií a metod identifikace mohou čtečky otisků prstů zastarávat a stávat se méně spolehlivými pro potřeby systému. To může znamenat nutnost jejich nahrazení novějšími modely nebo jinými biometrickými systémy, což by bylo časově náročné. Zároveň při výměně čteček otisků prstů je často nutné provést aktualizaci či instalaci nového softwaru, což může vést k dočasné nedostupnosti autentizace.

Výsledek analýzy

Po sečtení vážených průměrů z analýzy vyplývá, že je pro tento systém vhodné zvolit pro autentizaci přístupu k firemním zařízením aplikaci Microsoft Authenticator. Je ovšem nutno podotknout, že výsledky analýzy se znatelně neliší. Po přednesení výsledků majiteli se diskutovalo, zda by nebylo vhodné využít USB klíč s integrovanou čtečkou otisků prstů, jelikož toto řešení by spojilo přednosti obou variant. Toto řešení bylo finálně majitelem zamítnuto a byla vybrána varianta MS Authenticator. Ačkoliv s sebou nese rizika potíží při instalaci na nový telefon, aktuálně mají aplikaci všichni uživatelé nainstalovanou pro

přihlašování do Office 365. Zároveň je toto řešení jednoduše implementovatelné a uživatelsky přístupné. Bezpečnost může narušit ztráta či odcizení mobilního zařízení, dopad těchto situací se dá ovšem velmi zmírnit zamčením telefonu pomocí PIN kódu či biometrie. Ta se dá zároveň použít i při práci s aplikací samotnou pro zvýšení míry zabezpečení.

4.4.2 **Výběr metody pro vzdálený přístup**

Dle požadavku majitele bylo rozhodnuto, že se z aktuálního přístupu do NAS pomocí FTPS přejde na VPN. Tento přechod pro vzdálenou práci vychází z potřeby vyššího zabezpečení a zjednodušení řízení přístupu. Většina poskytovatelů VPN nabízí robustní šifrování a více faktorové ověřování, což zajistí, že data zůstanou důvěrná a přístupná pouze oprávněným uživatelům. Krom přístupu do NAS bude možné využít VPN i pro zabezpečený přístup na server, kde se nachází ovládací panely a nástroje potřebné pro uživatele při výkonu práce. Využití VPN tak poskytuje jednotné řešení pro bezpečný přístup ke všem potřebným síťovým zdrojům.

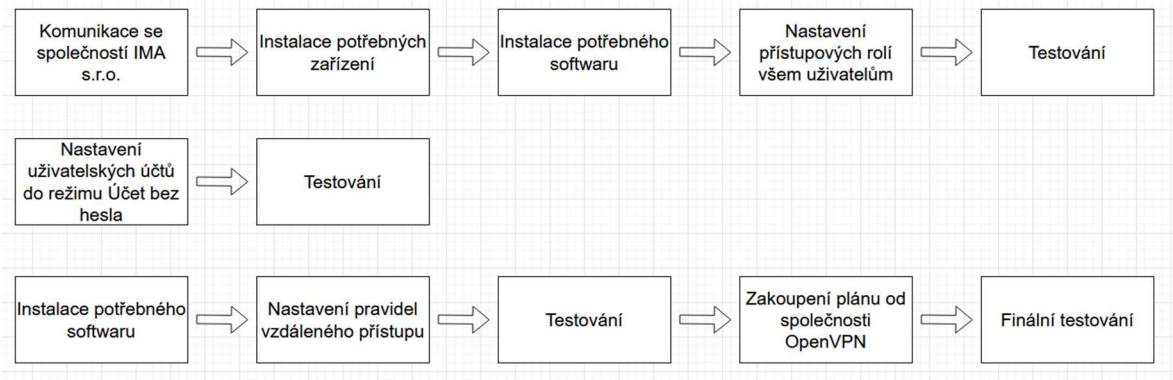
Vzhledem k výsledkům předchozí analýzy ohledně volby vlastního řešení v porovnání s řešením od poskytovatele bylo rozhodnuto, že i VPN bude zakoupena od poskytovatele. Po průzkumu existujících možností a následné konzultaci s majitelem systému se rozhodlo využít službu OpenVPN Access Server. Ta umožňuje hostování VPN na již existujícím serveru v systému za použití open-source OpenVPN protokolu. Toto řešení nabízí vysokou míru flexibility a přizpůsobení, což umožňuje konfiguraci na míru, aby splňovala požadavky na autentizaci vzdáleného přístupu do systému. Dále také společnost nabízí možnost otestovat službu zadarmo se všemi funkcemi, jako u placeného plánu. Jediným omezením je zde počet připojení.

Rozhodnutí zvolit OpenVPN bylo také ovlivněno rozsáhlou komunitní podporou tohoto protokolu. To zajišťuje průběžný vývoj, údržbu, podporu, a poskytuje přístup k bohatým zdrojům a odborným znalostem. Robustní bezpečnostní funkce OpenVPN, včetně silných šifrovacích protokolů, ověřování na základě certifikátů a komplexních funkcí auditu, odpovídají požadavkům majitele. Služba umožňuje i více faktorové ověřování mimo jiné pomocí aplikace Microsoft Authenticator, která už je v systému využívána. (OpenVPN, 2022)

4.5 Implementační plán

Po výběru potřebných metod autentizace bylo vytvořeno jednoduché schéma postupu při jejich implementaci, viz obrázek 9. Jelikož samotná implementace není součástí této práce, ve schématu nejsou zachyceny případné potíže, které mohou nastat při instalaci zařízení a potřebného softwaru. Tyto situace nelze předvídat v plném rozsahu, ovšem společnosti IMA s.r.o., OpenVPN, a Microsoft poskytují online podporu pro jejich zákazníky. V případě, že se vyskytne problém, který nelze jednoduše vyřešit v rámci systému, dá se na tyto společnosti obrátit.

Obrázek 9 Schéma procesu implementace



Zdroj: Vlastní zpracování (2024)

4.5.1 Implementace autentizace fyzického přístupu

Jelikož pro zabezpečení fyzického přístupu bylo zvoleno řešení přes poskytovatele bezpečnostních služeb, proces implementace zařízení je z technické stránky poměrně jednoduchý. Komunikace se společností IMA s.r.o. obnáší konzultaci o potřebných službách, dále také informace o přesném počtu a umístění jednotlivých zařízení.

Po instalaci kamer a elektronických zámků v souladu se schématickým návrhem je zapotřebí nainstalovat dodaný software, pomocí kterého se vytvoří databáze jednotlivých uživatelů a jejich oprávnění pro přístup. Za použití modelu Role-based access control jsou uživatelům přiřazeny role v závislosti na jejich potřebě. Je zde důležité, aby se ošetřil přístup do místnosti se serverem, kam mají mít oprávnění vstoupit pouze technikové. Dále je přístup do budovy mimo pracovní hodiny udělen pouze technikům a technické podpoře, v případě vyskytnutí akutního problému.

Posledním krokem je testování. Jedná se o zjištění, zda všichni uživatelé mají skutečně přístup do systému v souladu s rolí, která jim byla přidělena. Dále je potřeba se ujistit, že elektronické zámky na dveřích fungují bez problémů, např. zda je nelze otevřít bez ověření identity. Záznamy z kamer by měly být dobře viditelné a bezpečně uložené na firemní NAS, po dobu aspoň 30 dnů.

4.5.2 Implementace autentizace pro přístup k firemním zařízením

V prvním kroku této části implementačního plánu je potřeba nastavit účty všech uživatelů na režim Účet bez hesla. Po přihlášení do účtu Microsoft se v nastavení Zabezpečení účtu přejde do sekce Další možnosti zabezpečení. Zde se v části Účet bez hesla vybere možnost Zapnout, dále se postupuje podle pokynů na obrazovce. Nakonec se žádost schválí pomocí aplikace MS Authenticator. Dále je potřeba v aplikaci nastavit, aby pro udělení oprávnění bylo potřeba ověřit uživatele biometrickým údajem.

Proces implementace je jednoduchý, je ovšem důležité, aby byly takto nastaveny všechny účty uživatelů v systému. Zároveň je potřeba provést testování, zda autentizace funguje správně pro všechny uživatele.

4.5.3 Implementace autentizace pro vzdálený přístup

Prvním krokem pro implementaci služby OpenVPN Access Server je instalace potřebného softwaru a následné nastavení VPN. Toto prvotní nastavení je provedeno pomocí bezplatného plánu, aby šlo otestovat všechny funkce před zakoupením plné služby. VPN je potřeba nastavit tak, aby na ní uživatel musel být připojen pro vzdálený přístup. Dále je zapotřebí nastavit více faktorové ověřování přes aplikaci MS Auhtenticator.

Po otestování všech funkcí je zakoupen plán Standard, který umožní současné připojení ze všech zařízení v systému naráz. Zde je opět provedeno testování, že VPN funguje pro všechny uživatele, a že se k interním funkcím na serveru a NAS nelze připojit bez jejího použití.

4.5.4 Školení o bezpečnosti

V rámci implementačního plánu je i školení uživatelů ohledně používání nově implementovaných bezpečnostních řešení. Ačkoliv jsou vybrané metody autentizace uživatelsky přívětivé, je zapotřebí ověřit, zda všichni uživatelé vědí, jak s nimi správně

zacházet. Jedná se nejen o samotný proces autentizace, ale také o standardní postupy pro zamezení úniku citlivých dat a neoprávněnému vniknutí útočníka do systému.

Uživatelé musí být seznámeni s hrozbami, jako jsou různé metody sociálního inženýrství, a jak jim zamezit. Ztrátu identifikačního zařízení je nutno ihned ohlásit, zároveň by se měli vyvarovat pouštěním ostatních osob do systému, např. v situaci, kde jim podrží otevřené dveře, aniž by se druhá osoba identifikovala. Dalším rizikem je připojení neznámých USB zařízení, nejčastěji flash disky, do firemních zařízení. Uživatel nemůže vědět, zda je dané zařízení bezpečné, či zda neobsahuje škodlivý software.

I mimo systém je důležité brát ohled na bezpečnost. Uživatelům je doporučeno používat více faktorové ověření na všech účtech, zároveň i používat silná hesla. Dále je zapotřebí poučit uživatele o bezpečném pohybu na internetu, aby se vyvarovali nakažení zařízení malwarem. Zde se může jednat o stažení nakažených souborů z webové stránky či podvodné emailové zprávy. Z těchto důvodů je vhodné mít nainstalovaný antivirový software, který může případnému nakažení zařízení překazit.

5 Výsledky a diskuse

Bezpečnost je problematika, se kterou se potýká každý systém, který potřebuje zajistit, aby neoprávnění uživatelé neměli přístup k jeho zdrojům a prostorám. Tato problematika je ovšem velmi individuální a je ovlivněna vysokou škálou proměnných faktorů. Velikost budovy, ve které se systém nachází. Počet vchodů a místností, které je potřeba ochránit. Počet uživatelů, kteří se v systému pohybují. Nelze tedy určit jeden jediný plán, který by fungoval pro všechny systémy na světě.

Existují ovšem způsoby, jak takový plán vytvořit s ohledem na specifické požadavky daného systému. Výsledkem této práce je implementační návrh pro nové metody autentizace ve vybraném systému. V následujících podkapitolách budou zhodnoceny důsledky zavedení těchto nových metod ověřování v rámci systému, pokud se majitel rozhodne je skutečně implementovat. Výsledek této práce může také sloužit jako inspirace pro jiné systémy, které čelí podobným výzvám v oblasti autentizace.

5.1 Zvýšení bezpečnosti

Hlavním požadavkem pro nové metody autentizace v rámci této bakalářské práce bylo zvýšení bezpečnosti celého systému. Po provedení analýz a konzultace s majitelem systému byly do implementačního návrhu zavedeny nově vybrané autentizační metody, které by při jeho provedení měli za následek bezpečnější řešení.

5.1.1 Autentizace fyzického přístupu

Oproti současným metodám autentizace v systému nabízí nové řešení mnohem vyšší stupeň zabezpečení před neoprávněným přístupem do systému. Elektronické zámky nainstalované na oba vchody a místnost se serverem zajistí, že přístup bude udělen pouze ověřeným uživatelům, a to v daném čase. Nainstalované kamery umožní majiteli přehled o tom, kdy a kde se uživatelé pohybují. V případě vniknutí do systému neoprávněným uživatelem umožní záznam útočníka identifikovat, nebo dohledat, jak se do systému dostal. To umožní majiteli najít vadu v systému a následně ji opravit, aby se navýšila úroveň bezpečnosti.

5.1.2 Autentizace logického přístupu

Přijetí nástroje Microsoft Authenticator pro přihlašování k firemním zařízením a zavedení sítě VPN pro vzdálený přístup navýší bezpečnost sytému oproti současnému řešení. Obě metody využívají více faktorové ověřování, na rozdíl od nutnosti zadat pouze správné heslo. Tím by byl zabezpečen jak přístup k samotným počítačům a laptopům, ale také na server a NAS úložiště.

5.2 Uživatelská přívětivost

Navrhnutá řešení pro nové metody autentizace jsou zároveň více uživatelsky přívětivé. Pro přístup do navrhnutého systému, přihlašování k firemním zařízením, a připojení k síti VPN se využívá mobilní zařízení. Ta mají všichni uživatele neustále u sebe, takže se nemusí bát, že přijdou o přístup. Další výhodou je, že nemusí nosit jiný identifikační předmět navíc, jako jsou klíče či čipové karty.

Využití docházkového systému, který je napojen na bezpečnostní zařízení, zajistí jednak autenticitu příchodů a odchodů, ale zároveň i ulehčí práci samotným uživatelům. Ti nemusí sami hlídat a zapisovat čas jejich pohybu po systému, o všechno se postará software.

5.3 Jednoduchá implementace

Jelikož byla vybrána předem připravená řešení od poskytovatelů, samotná implementace je pro uživatele systému jednoduchá. Nemusí být vyhrazen čas na vývoj nového softwaru či na analýzu různých zařízení, zajištění jejich kompatibility, a následné instalaci. Zároveň každý z poskytovatelů nabízí technickou podporu v případě, že se během nebo po implementaci vyskytne problém.

5.4 Škálovatelnost a flexibilita

Díky volbě aplikace MS Auhtenticator lze autentizaci provést na všech moderních zařízeních s operačním systémem Android a iOS. To samé platí pro implementaci VPN klienta od OpenVPN, který je navíc dostupný na systémech Windows, Linux, MacOS a ChromeOS. Jeden potenciální problém při budoucím rozšiřování systému je, že počítačový software pro správu uživatelů v rámci přístupového systému od společnosti IMA s.r.o. je dostupný pouze pro platformu Windows. Tento nedostatek majiteli současného systému

nevadí, jelikož jinou platformu nevyužívají. Zároveň je možné systém spravovat přes aplikaci v mobilním zařízení. Ovšem ne každému systému musí toto řešení vyhovovat, proto je tuto informaci nutné vzít v úvahu.

6 Závěr

Cílem této práce bylo sestrojení implementačního návrhu pro implementaci nových metod autentizace ve vybraném systému. Pro splnění hlavního cíle bylo zapotřebí se seznámit s problematikou pomocí provedení literární rešerše. Nejprve byly vymezeny obecné způsoby autentizace. Poté následoval průzkum specifických metod autentizace jak pro fyzický, tak pro logický přístup. Poslední část literární rešerše se zabývala hrozbami, které představují pro systém riziko.

V praktické části bakalářské práce nejprve proběhlo seznámení se systémem a jeho aktuálními metodami autentizace. Dále proběhlo seznámení s požadavky majitele. Dalším krokem byl výběr druhu řešení pro autentizaci fyzického přístupu. Konkrétně se jednalo o otázku, zda vytvořit vlastní řešení, či řešení od poskytovatele. Na základě analýzy bylo vybráno řešení od společnosti IMA s.r.o. Poté následoval výběr metody autentizace pro logický přístup do firemních zařízení. Zde byla na základě výsledků zvolena aplikace Microsoft Authenticator. Pro autentizaci vzdáleného přístupu bylo zvoleno řešení OpenVPN Access Server. Posledním krokem byl samotný návrh implementačního procesu. Zde bylo předvedeno schéma postupu při implementaci, zároveň byl dán důraz na řádné školení uživatelů v rámci bezpečnosti.

Pokud se majitel systému rozhodne daná řešení implementovat, dosáhne tak mnohem vyššího stupně zabezpečení než v současném stavu systému. Dále jsou nově zvolené metody autentizace více uživatelsky přívětivé, jelikož pro kontrolu přístupu stačí pouze mobilní telefon, který má každý z uživatelů stále u sebe. Navrhnutá řešení jsou také z valné většiny jednoduše škálovatelná při budoucím rozvoji systému, a jsou dostatečně flexibilní pro potřeby majitele.

7 Seznam použitých zdrojů

Ahola, Micke. Top 5 Physical Security Risks - And How to Protect Your Business. *usecure.* [Online] [Citace: 22. Srpen 2023.] https://blog.usecure.io/physical-security-risks.

Awati, Rahul. 2023. What is mandatory access control (MAC)? *TechTarget.* [Online] Listopad 2023. [Citace: 15. Listopad 2023.] https://www.techtarget.com/searchsecurity/definition/mandatory-access-control-MAC.

Ballad, Bill, Balad, Tricia a Banks, Erin K. 2010. *Access Control, Authentication, and Public Key Infrastructure.* místo neznámé : Jones & Bartlett Learning, 2010. 978-0763791285.

Butchard, Kylie. 2022. Physical Access Control VS Logical Access Control. *Pacific Security Group.* [Online] 17. Listopad 2022. [Citace: 15. Srpen 2023.] https://pacificsecuritygroup.com.au/blog/physical-access-control-vs-logical-access-control/.

Copado. 2022. 12 Types of Social Engineering Attacks to Look Out For. *Copado.* [Online] 12. Prosinec 2022. [Citace: 22. Srpen 2023.] https://www.copado.com/resources/blog/12-types-of-social-engineering-attacks-to-look-out-for.

Creutzburg, Reiner. 2017. The strange world of keyloggers - an overview, Part I. *Electronic Imaging.* [Online] Leden 2017. [Citace: 22. Srpen 2023.] https://www.researchgate.net/publication/318228591_The_strange_world_of_keyloggers_-_an_overview_Part_I.

Gašparík, Petr. 2014. ABAC – řízení přístupu na základě atributů. *AMI.* [Online] 11. Srpen 2014. [Citace: 4. Prosinec 2023.] https://www.ami.cz/novinka/abac-rizeni-pristupu-na-zaklade-atributu/.

Hanna, Katie Terrell. 2021. What is a brute-force attack? *TechTarget.* [Online] 2021. [Citace: 12. Srpen 2023.] https://www.techtarget.com/searchsecurity/definition/brute-force-cracking.

Holmes, Josh. 2023. Malware Is A Threat To Businesses – Here's What You Need to Know. *Stanfield IT.* [Online] 13. Červenec 2023. [Citace: 22. Srpen 2023.] https://www.stanfieldit.com/malware/.

IMA. IMA s.r.o. *IMA s.r.o.* [Online] [Citace: 18. Prosinec 2023.] https://www.ima.cz/.

Jacobs, Pim. 2021. Improving the Microsoft Authenticator App Notifications with Number Matching, App name & Geographic location. *Identity Man.* [Online] 30. Listopad 2021. [Citace: 12. Říjen 2023.] https://identity-man.eu/2021/11/30/improving-the-microsoft-authenticator-app-notifications-with-number-matching-and-additional-context/.

Jones, Caitlin. 2023. Understanding the Three Factors of Authentication. *Expert Insights.* [Online] 28. Květen 2023. [Citace: 12. Srpen 2023.] https://expertinsights.com/insights/what-are-the-3-types-of-multi-factor-authentication/.

Jones, Catilin. 2022. How To Create A Secure Password Policy For Your Organization. *Expert Insights.* [Online] 24. Listopad 2022. [Citace: 16. Srpen 2023.] https://expertinsights.com/insights/how-to-create-a-secure-password-policy-for-your-organization/.

Kessler, Gary C. 1996. Passwords - Strenghts and Weaknesses. *Gary Kessler Associates* . [Online] Leden 1996. [Citace: 12. Srpen 2023.] https://www.garykessler.net/library/password.html.

Khairallah, Michael. 2005. *Physical Security Systems Handbook: The Design and Implementation of Electronic Security Systems.* místo neznámé : Butterworth-Heinemann, 2005. stránky 58-59. ISBN 978-0750678506.

Kirvan, Paul. 2023. Security Token. *Tech Target.* [Online] Červen 2023. [Citace: 12. Říjen 2023.] https://www.techtarget.com/searchsecurity/definition/security-token.

LastPass. 2018. What is a password manager? [Online] 2018. [Citace: 16. Srpen 2023.] https://www.lastpass.com/password-manager.

Lewis-Rippington, Luke. 2021. CCTV & Access Control: Everything You Need to Know. *Chris Lewis Group.* [Online] 5. Srpen 2021. [Citace: 16. Srpen 2023.] https://www.chrislewis.co.uk/blog/cctv-access-control-everything-you-need-to-know.

Lodha, Tilak. 2018. Google Authenticator and how it works? *Medium.* [Online] 17. Duben 2018. [Citace: 12. Srpen 2023.] https://medium.com/@tilaklodha/google-authenticator-and-how-it-works-2933a4ece8c2.

Lutkevitch, Ben. 2022. What is access control? *TechTarget.* [Online] Červenec 2022. [Citace: 12. Srpen 2023.] https://www.techtarget.com/searchsecurity/definition/access-control.

Maayan, Gilad David. 5 User Authentication Methods that Can Prevent the Next Breach. *ID R&D.* [Online] [Citace: 15. Srpen 2023.] https://www.idrnd.ai/5-authentication-methods-that-can-prevent-the-next-breach/.

Managing access control – combining physical and logical security. **Ting, David. 2007.** 2007, Card Technology Today, stránky 9-10.

McQuillan, Ronan. 2022. Rule-Based vs Role-Based Access Control. *Budibase.* [Online] Květen. 23 2022. [Citace: 15. Srpen 2023.] https://budibase.com/blog/app-building/difference-between-rule-based-role-based-access-control/.

Mehl, Bernhard. 2022. Fail Safe vs Fail Secure - and what most people get wrong. *Kisi.* [Online] 1. Prosinec 2022. [Citace: 15. Srpen 2023.] https://www.getkisi.com/blog/fail-safe-vs-fail-secure.

Norman, Thomas L. 2017. *Electronic Access Control.* místo neznámé : Butterworth-Heinemann, 2017. 978-0-12-805465-9.

OpenVPN. 2022. OpenVPN Access Server. *OpenVPN.* [Online] 2022. [Citace: 19. Prosinec 2023.] https://openvpn.net/access-server/.

Palter, Jay. 2020. Access Control Card Technology: Choose the Right One for Your Business. *Real Time Networks.* [Online] 13. Listopad 2020. [Citace: 26. Listopad 2023.] https://www.realtimenetworks.com/blog/choosing-access-control-card-technology.

Rightcrowd. 2023. The Convergence of Physical and Logical Access Control. *Rightcrowd.* [Online] 22. Únor 2023. [Citace: 21. Srpen 2023.] https://www.rightcrowd.com/2023/02/22/the-convergence-of-physical-and-logical-access-control/.

Rouse, Margaret. 2023. Discretionary Access Control. *Techopedia.* [Online] 23. Červen 2023. [Citace: 15. Srpen 2023.] https://www.techopedia.com/definition/229/discretionary-access-control-dac.

Sanders, Andrew. 2024. Co je sociální inženýrství a proč je to hrozba v roce 2024? *SafetyDetectives.* [Online] 2024. [Citace: 21. Leden 2024.] https://cs.safetydetectives.com/blog/co-je-socialni-inzenyrstvi-a-proc-je-to-takova-hrozba/.

ShineACS. 2019. What is a Maglock in door access control system? *ShineACS.* [Online] 13. Duben 2019. [Citace: 26. Listopad 2023.] https://www.shineacs.com/what-is-a-maglock/.

Spadafora, Anthony. 2020. Remote access VPN: what are they, how do they work and which are the best. *TechRadar.* [Online] 11. Březen 2020. [Citace: 21. Srpen 2023.] https://www.techradar.com/vpn/remote-access-vpn.

Stallings, William. 2014. *Physical Security Essentials.* místo neznámé : Syngress, 2014. 978-0-12-416681-3.

Stytch. 2022. What is password hashing? *Stytch.* [Online] 26. Červenec 2022. [Citace: 16. Srpen 2023.] https://stytch.com/blog/what-is-password-hashing/.

Wilson, Matt. 2021. Where is the best place to install security cameras? *A1 Security Cameras.* [Online] 21. Září 2021. [Citace: 5. Prosinec 2023.] https://www.a1securitycameras.com/blog/best-places-install-security-cameras-businesses.

Zhang, Ellen. 2023. What is Role-Based Access Control (RBAC)? Examples, Benefits, and More. *Digital Guardian.* [Online] 5. Květen 2023. [Citace: 15. Srpen 2023.] https://www.digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

NAS – Network Attached Storage, technologie pro ukládání a práci s daty v rámci jedné sítě
MS – Microsoft
VPN – Virtual Private Network, technologie pro zabezpečený přenos dat