Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Vícefaktorová autentizace a autorizace

Polívka Jan

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Polívka

Informatika

Název práce

Vícefaktorová autentizace a autorizace

Název anglicky

Multi-factor authentication and authorization

Cíle práce

Bakalářská práce je tématicky zaměřena na problematiku vícefaktorové autentizace a autorizace. Hlavním cílem práce je analýza využitelnosti vícefaktorové autentizace převážně v oblasti bankovnictví včetně analýzy a zhodnocení spokojenosti ze strany koncových uživatelů.
Dílčí cíle práce jsou:
- vypracování přehledu zpracovávané problematiky
- vypracování přehledu využitelnosti vícefaktorové autentizace v oblasti bankovnictví.

Metodika

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Teoretická část bude věnována využití vícefaktorové autentizace převážně v oblasti bankovnictví včetně přehledu o výhodách a úskalích autentizace. Vlastní práce spočívá v analýze a porovnání použitelnosti a úrovně spokojenosti koncových uživatelů. Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

40 – 50 stran textu

Klíčová slova

zabezpečení, autentizace, autorizace, bankovnictví, biometrie, tokeny

---

Doporučené zdroje informací

J.K. Mohsin, Liangxiu Han, Mohammad Hammoudeh and Rob Hegarty. Two Factor Vs Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. Manchester, 2017, UK. ISBN 978-145034844-7

MATYÁŠ, Vašek a Jan KRHOVJÁK. Autorizace elektronických transakcí a autentizace dat i uživatelů. Brno: Masarykova univerzita, 2008. ISBN 978-80-210-4556-9

MATYÁŠ, Vašek. Autentizace uživatelů a autorizace elektronických transakcí: příručka manažera = User authentication and electronic transaction authorization : manager's handbook. Praha: TATE International, 2007. Příručka manažera. ISBN 978-80-86813-14-1

Okpamen, Peter. Security of information systems in organization: A bank model. Ambrose Alli University, 2013, Ekpoma-Edo State, Nigeria. ISSN 20392117

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

Věra Motyčková, MA

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 03. 08. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Vícefaktorová autentizace a autorizace" jsem vypracoval(a) 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 15.3.2024 _____

Poděkování

Rád(a) bych touto cestou poděkoval(a) paní magistře Motyčkové za odborné vedení, trpělivost a ochotu, kterou mi v průběhu zpracování bakalářské práce věnovala.

Vícefaktorová autentizace a autorizace

Abstrakt

Tato bakalářská práce se zaměřuje na analýzu využitelnosti vícefaktorové autentizace, s důrazem na oblast bankovnictví, a zhodnocení spokojenosti koncových uživatelů. Hlavním cílem je posoudit, jak efektivně a spolehlivě je tato autentizační metoda využívána, přičemž se zkoumají přínosy a možná omezení. Dílčími cíli jsou vytvoření přehledu problematiky a zjištění úrovně přijetí MFA v bankovním sektoru. Vlastní výzkum spočívá v analýze a porovnání spokojenosti uživatelů pomocí dotazníkového šetření a v identifikaci optimálního autentizačního řešení pro banky na základě jejich potřeb a bezpečnostních požadavků.

Klíčová slova: zabezpečení, autentizace, autorizace, bankovnictví, biometrie, tokeny, heslo

Multi-factor authentication and authorization

Abstract

This bachelor's thesis focuses on analyzing the usability of multifactor authentication, with an emphasis on the banking sector, and evaluating the satisfaction of end users. The main objective is to assess how effectively and reliably this authentication method is utilized, while examining its benefits and potential limitations. Sub-goals include creating an overview of the issue and determining the level of acceptance of MFA in the banking sector. The research itself consists of analyzing and comparing user satisfaction through questionnaire surveys and identifying the optimal authentication solution for banks based on their needs and security requirements.

Keywords: security, authentication, authorization, banking, biometrics, tokens, password

Obsah

1 Úvod

V dnešní digitalizované společnosti, kde stále více našich životů a dat se odehrává online, je zabezpečení účtů a informací nezbytně důležité. Tradiční přístup k zabezpečení pomocí jednoduchého uživatelského jména a hesla už bohužel není dostatečný. Hesla mohou být snadno prolomena, což ohrožuje osobní bezpečnost a citlivá data.

Banky jsou již dlouho uznávány jako lídři při zavádění sofistikovaných bezpečnostních opatření na ochranu finančních aktiv a osobních informací zákazníků V digitálním věku, kdy se kybernetické hrozby stále vyvíjejí, se banky chopily příležitosti zavedením inovativních řešení, jako je vícefaktorová autentizace (multi-factor authentication, MFA), s cílem posílit svou bezpečnostní infrastrukturu. Technologie jsou ukázkovým příkladem odhodlání sektoru finančních služeb zůstat v čele trendu a zajistit nejvyšší úroveň ochrany svých zákazníků. MFA představuje jednu z nejefektivnějších metod, jak zvýšit zabezpečení online účtů a systémů. Vícefaktorová autentizace řeší tyto bezpečnostní výzvy tím, že vyžaduje od uživatele ověření prostřednictvím více nezávislých faktorů, jako jsou biometrická data (otisk prstu, rozpoznání obličeje), hardware tokeny, SMS nebo mobilní aplikace s jednorázovými kódy, poskytuje robustní a sofistikovanou ochranu. Pokud by se nějaký z faktorů stal kompromitovaným, zůstává zabezpečení stále pevné díky dalším nezávislým vrstvám. Banky mohou volit různé metody, aby co nejlépe odpovídaly potřebám a preferencím svých klientů. To zajišťuje, že finanční transakce jsou prováděny s vysokým stupněm bezpečnosti a minimalizují riziko finančních podvodů a zneužití platebních údajů. Organizace by měly MFA vnímat jako investici do bezpečnosti a ochrany důvěrných informací, která může chránit jak uživatele, tak i samotnou organizaci před nebezpečím kybernetických hrozeb a útoků.

V dané práci si detailněji probereme jednotlivé aspekty vícefaktorové autentizace a autorizace, včetně různých implementačních způsobů, výhod, nejnovějších technologií a zabezpečovacích postupů. Cílem je lépe pochopit, jak můžeme aktivně přispět k ochraně svých dat a zabezpečit své online účty proti stále sofistikovanějším hrozbám.

2 Cíl práce a metodika

Bakalářská práce je tématicky zaměřena na problematiku vícefaktorové autentizace a autorizace. Hlavním cílem práce je analýza využitelnosti vícefaktorové autentizace převážně v oblasti bankovnictví včetně analýzy a zhodnocení spokojenosti ze strany koncových uživatelů.
Dílčí cíle práce jsou:
- vypracování přehledu zpracovávané problematiky
- vypracování přehledu využitelnosti vícefaktorové autentizace v oblasti bankovnictví

Metodika řešené problematiky bakalářské práce je založena na studiu a analýze odborných informačních zdrojů. Teoretická část bude věnována autorizaci, využití vícefaktorové autentizace převážně v oblasti bankovnictví včetně přehledu o výhodách a úskalích. Vlastní práce spočívá v analýze a porovnání použitelnosti a úrovně spokojenosti koncových uživatelů pomocí dotazníku a zjištění ideální varianty autorizace pro banky na základě jejich požadavků, pomocí vícekriteriální analýzy. Na základě syntézy teoretických poznatků a výsledků praktické části budou formulovány závěry bakalářské práce.

3 Teoretická východiska

Teoretická část poskytne komplexní pohled na autorizaci, využití vícefaktorové autentizace v bankovnictví, zkoumající její výhody, výzvy a potenciální omezení, aby lépe porozuměla roli této metody v současném digitálním prostředí.

3.1 Autentizace

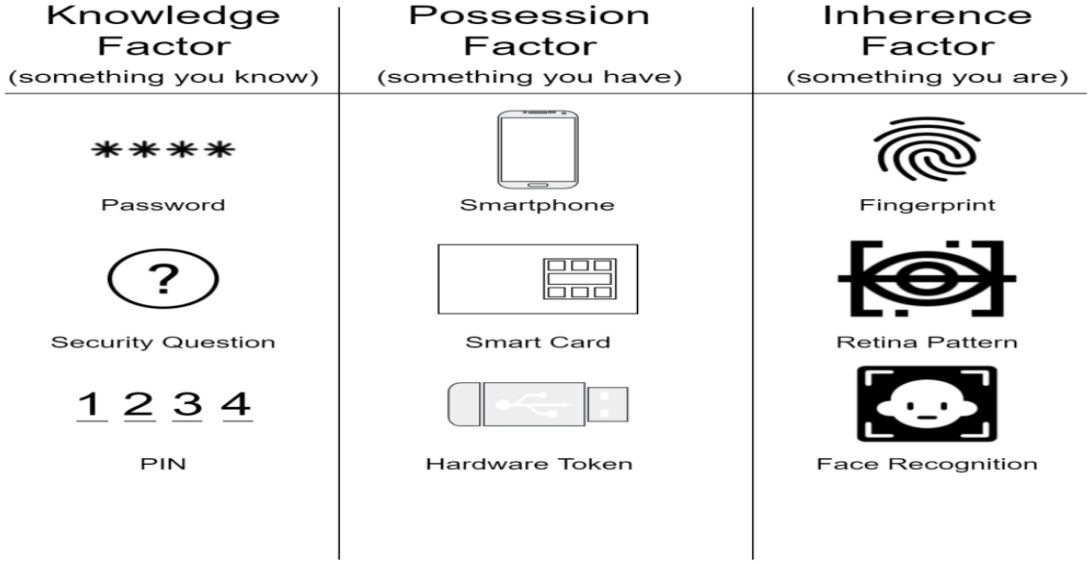
Autentizace je proces potvrzování identity uživatele, zařízení nebo entity pokoušející se o přístup k systému, aplikaci nebo službě. Jedná se o klíčový koncept kybernetické bezpečnosti a informačních technologií, který má zabránit neoprávněnému přístupu a zajistit bezpečnost dat.

Autentizace zajišťuje, že identita udávaná uživatelem je správná. To zabrání škodlivým uživatelům v přístupu k citlivým informacím nebo prostředkům. Pomocí různých faktorů se zajišťuje větší ochrana dat.

Tyto faktory spadají do tří hlavních kategorií:

1. Znalostní objekt: Cokoliv, co člověk ví, například hesla, PIN nebo odpovědi na bezpečnostní otázky.
2. Faktor vlastnictví: Uživatel vlastní něco jako smartphone, bezpečnostní token nebo čipovou kartu.
3. Genetický faktor: Něco jedinečného pro uživatele, jako jsou otisky prstů, skeny obličeje, vzory sítnice nebo rozpoznávání hlasu.

Obrázek 1 - Faktory autentizace



Zdroj:Rublon (2021)

Dále lze autentizační faktor klasifikovat jako transparentní nebo interaktivní:

- Transparetní autentizace probíhá v zákulisí bez interakce s uživateli. Příklady transparentních autentizačních faktorů jsou blízkost zařízení Bluetooth a geofencing. Geofencing je služba zaměřující polohu pomocí GPS nebo RFID, jako jsou Wi-Fi nebo Bluetooth či mobilní data.

- Interaktivní autentizace vyžaduje, aby uživatel něco udělal, například zadal PIN nebo vzorový kód. (Bedell 2018)

3.2 Autorizace

V oblasti bezpečnosti informací je autorizace klíčovým konceptem, který podporuje autentizaci. Zatímco autentizace vypadá, že je prováděna uživatelem nebo entitou, autorizace určuje, jaké činnosti nebo funkce má tato certifikovaná entita provádět. Pečlivým definováním a správou uživatelských oprávnění mohou organizace zajistit, aby jejich systémy a data zůstala bezpečná, a umožnit oprávněným uživatelům přístup k jejich základním službám. V podstatě jde o proces udělování nebo odpírání povolení založený na právech uznaných subjektů. (Okpamen 2013)

3.3 Vícefaktorová autentizace

V první řadě poskytuje MFA další vrstvu zabezpečení, která neoprávněným uživatelům ztěžuje přístup k citlivým informacím. Kromě toho tím, že vyžaduje alespoň dva nezávislé faktory ověřování, MFA vytvoří robustnější proces ověřování. V důsledku toho, i když je ohrožen jeden faktor, pravděpodobnost úspěšného porušení je stále snížena.

Nyní je pravda, že MFA není neomylná a v některých případech ji lze obejít. Složitost obcházení MFA však často působí jako odrazující prostředek pro potenciální útočníky. Úsilí a zdroje potřebné k obcházení MFA jsou výrazně vyšší než tradiční metody jednofaktorového ověřování. To je zvláště důležité při zvažování hodnoty chráněných informací. Čím cennější jsou data, tím atraktivnější se stávají jako cíl. MFA tedy zvyšuje náklady pro potenciální útočníky, kteří musí zvážit investici proti potenciální návratnosti.

Pro uživatele, společnosti a poskytovatele služeb mohou být důsledky narušení bezpečnosti zničující – od finančních ztrát až po poškození pověsti.

V neposlední řadě je důležité mít na paměti, že bezpečnost se neustále vyvíjí. Bezpečnostní opatření, jako je vícefaktorová autentizace, se musí přizpůsobit a zlepšit s tím, jak se objevují nové hrozby, aby zůstala účinná. V tomto neustále se měnícím prostředí není použití MFA zárukou absolutní bezpečnosti, ale spíše nástrojem, který pomáhá minimalizovat pravděpodobnost porušení.

3.3.1 Znalostní objekt

V oblasti autentizace hraje faktor „znalostní objekt“ důležitou roli při ověřování osob pokoušejících se o přístup k systému, aplikaci nebo službě. Tento faktor poskytuje informace založené na znalostech, které může použít pouze pro zákonné použití. Tato funkce ověřování vyžaduje, abyste poskytli znalosti, které by patřily pouze oprávněnému uživateli. Když se například budete přihlašovat k účtu, budete muset zadat heslo, PIN spojený s vaší kartou nebo otázku typu „Jak se jmenuje váš první mazlíček? Toto je způsob, jak vám umožnit přístup k programům, aplikacím nebo službám.

Heslo

V oblasti autentizace jsou hesla klíčovým způsobem, jak ověřit autenticitu uživatelů před udělením přístupu k digitálním platformám a službám. Jedná se o tajnou kombinaci znaků, které znají jen oprávnění, která funguje jako digitální klíč k odemknutí jejich zámku. Hesla se v systémech internetového bankovnictví běžně používají k ochraně citlivých finančních informací a transakcí před neoprávněným přístupem.

Tvorba silných hesel je nezbytná pro zachování bezpečnosti účtu. To často vyžaduje dodržování specifických parametrů nastavených poskytovatelem služby, jako je použití velkých a malých písmen, čísel a kombinací speciálních znaků a délka je také důležitá. Delší heslo je obecně bezpečnější. Cílem je udržet heslo složité a nezjistitelné a vyhnout se tak snadnému odhadu informací, jako je jméno, datum narození nebo běžná slova.

V bankovním sektoru, kde jsou transakce vysoké kvůli citlivosti finančních informací, hrají hesla důležitou roli při zajišťování bezpečnosti finančních prostředků klientů a osobních informací. Fungují jako spotřební mechanismus bývalého prostředku ochrany před neoprávněným přístupem. Zákazníkům se doporučuje, aby svá hesla uchovávali v tajnosti a nikomu je nesdělovali, protože by to mohlo ohrozit jejich účty.

Jakkoliv jsou hesla účinná, mohou být zranitelná vůči celé řadě hrozeb, včetně phishingových útoků, při kterých se kyberzločinci snaží obelstít jednotlivce, aby odhalili svá hesla prostřednictvím podvodných e-mailů a webových stránek. Aby banky tato rizika zmírnily, často své zákazníky vzdělávají o bezpečných on-line postupech a identifikují potenciální hrozby.

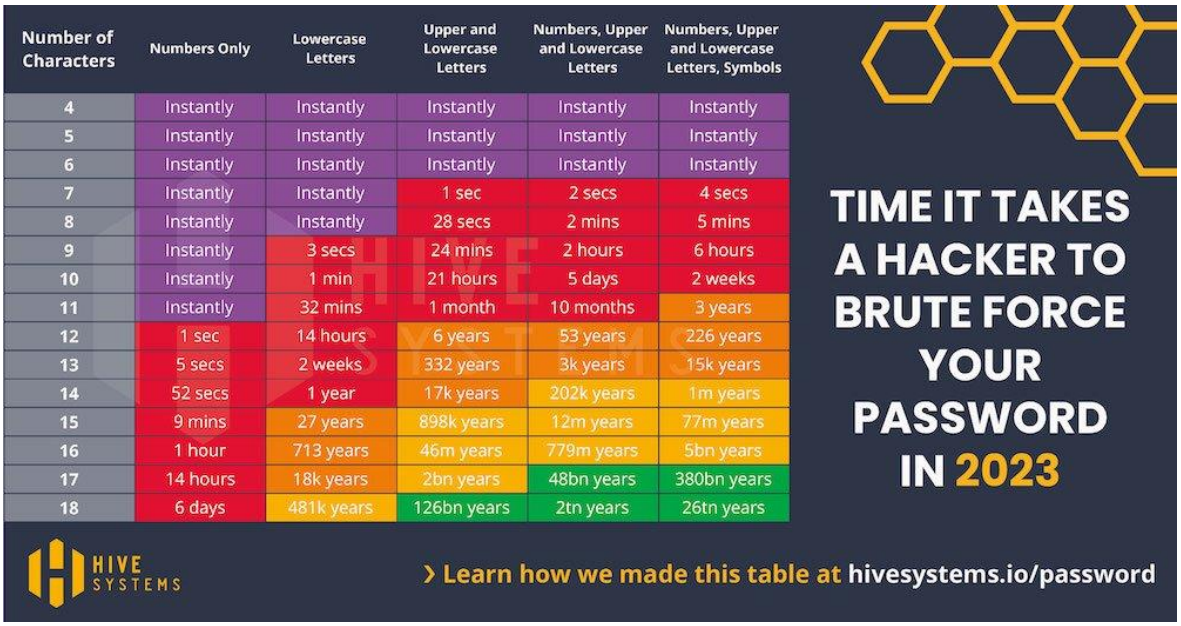
Heslo zůstává základním kamenem autentizace, zejména v kontextu internetového bankovnictví. V zájmu ochrany citlivých finančních informací je důležité zajistit, aby účty a transakce zákazníků byly důvěrné a bezpečné a aby byly řádně používány a vedeny.

Abychom byli spravedliví, hesla jsou nezbytná k tomu, aby naše digitální účty a informace byly bezpečné, ale všechny aplikace a služby, které používáme, mohou velmi ztížit jejich zapamatování. Podle vyjádření Kohouta (2016) *„často se pak stává, že uživatel rezignuje a u většiny webových služeb užívá stejné heslo. Toto je však jedna z nejhrubších chyb, které se uživatel může dopustit.“* Na základě délky a výběru znaků mohou počítače se speciálními

programy prolomit vaše zabezpečení a v případě využívání stejného hesla i na jiných portálech, má útočník možnost využít získané informace i zde. Samozřejmě čím složitější a delší heslo, tím menší šance zisku vašich údajů.

Rychlostí, jakou se informační technologie vyvíjejí, mohou dnešní neprolomitelná hesla, být za pár let velmi jednoduchým úkolem pro nové nebo aktualizované softwary na prolomení hesel. Proto je i doporučeno si hesla měnit na základě nejnovějších kritérií a požadavků.

Obrázek 2 - Čas na prolomení hesla na základě znaků



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years

Zdroj: Hive systems (2023)

Pro ochranu vašeho on-line účtu je důležité vytvořit silné a bezpečné heslo. Existuje mnoho návodů a rad, jak si vytvořit heslo. Zde pár možností jak na to:

- Délka: Použijte heslo, které má alespoň 12 až 16 znaků. Delší hesla jsou obecně bezpečnější, protože je pro útočníky těžší je uhodnout nebo prolomit.

- Složitost: Použijte směs velkých a malých písmen, čísel a speciálních znaků (například !, @, #, $, %). To činí heslo komplikovanějším a hůře uhodnutelným. Vyvarujte se používání obecných slov, frází nebo snadno odhadnutelných frází, jako je jméno, datum narození.

- Namátkovost: Vytvořte heslo, které se zobrazí náhodně a neřídí se předvídatelným vzorem. Vyhněte se postupným znakům, jako jsou „12345“ nebo „abcdef“.

- Žádné osobní informace: Nepoužívejte v hesle žádnou část svých osobních údajů, jako je jméno, příjmení nebo e-mailová adresa.

- Jedinečné heslo: Pro každý z vašich účtů použijte jedinečné heslo. Pokud je takto prozrazeno jedno heslo, zůstanou vaše ostatní účty v bezpečí.

- Pravidelně aktualizovat: Pravidelně si měňte heslo, zejména u důležitých účtů. Pokud služba, kterou používáte, způsobila narušení zabezpečení, změňte okamžitě heslo.

Vyvarujte se použití nejznámějších a nejpoužívanějších hesel, které i přesto, že jsou velmi známá a lehce prolomitelná, tak jsou i nadále uživateli využívaná ve velké míře po mnoho let a pouze se mění příčky.

Obrázek 3 - Nejvíce používaná hesla

Top 10 Worst Passwords - Historic Analysis

	2023	2015	2010	2005	2000
#1	123456	123456	123456	password	password
#2	123456789	password	password	123456	123456
#3	qwerty	12345	12345678	12345678	12345678
#4	password	12345678	qwerty	abc123	qwerty
#5	1234567	qwerty	abc123	qwerty	abc123
#6	12345678	1234567890	123456789	monkey	monkey
#7	12345	1234	111111	letmein	1234567
#8	iloveyou	baseball	1234567	dragon	letmein
#9	111111	dragon	iloveyou	111111	trustno1
#10	Covid	football	adobe123	baseball	dragon

Zdroj:Janco Associates (2021)

Pamatujte, že i když je důležité vytvořit silné heslo, je také důležité dávat pozor na phishingové pokusy a další techniky sociálního inženýrství, které mohou ohrozit váš účet. Právě vícefaktorová autentizace (MFA) je další nutnou ochranou.

Bezpečnostní otázka

Otázky zabezpečení jsou otázky používané v rámci procesu ověřování totožnosti uživatele, který se snaží získat přístup k účtu nebo službě. Jedná se o další zabezpečení, které podporuje hesla nebo jiné metody ověřování. Správným zodpovězením těchto otázek mohou uživatelé prokázat, že mají potřebné znalosti nebo osobní údaje o účtu. Otázky zabezpečení se často používají při problémech s obnovou účtů, například když uživatelé zapomenou svá hesla. Při vytváření bezpečnostních otázek je uživatelům často předkládán seznam předem definovaných otázek nebo je uživatelům povoleno vytvořit si vlastní. Typickými příklady bezpečnostních otázek jsou „Jaké je jméno vaší matky?“, „Jaká je vaše oblíbená barva?“, nebo „V jakém městě jste se narodil?“ Uživatel pak na tyto otázky odpoví.

O účinnosti bezpečnostních otázek se však diskutovalo kvůli možným rizikům. Odpovědi na tyto otázky může obvykle snadno uhodnout nebo analyzovat útočník, který zná osobní údaje cíle. Informace, jako je datum narození, oblíbené barvy nebo jména členů rodiny, lze nalézt na sociálních sítích nebo jiných veřejných místech. Tato zranitelnost vedla k některým obviněním, že útočníci jsou schopni obcházet bezpečnostní otázky a získat neoprávněný přístup k účtům. V reakci na tato omezení se některé podniky a platformy začaly odklánět od společných bezpečnostních otázek nebo nabízejí bezpečnější možnosti.

Závěrem lze říci, že bezpečnostní otázky jsou novou formou autentizace, jejímž cílem je zvýšení bezpečnosti účtu. Snadný přístup k osobním údajům však může narušit jejich účinnost. S tím, jak se digitální prostředí vyvíjí, je důležité zvážit bezpečnější metody, aby byla zajištěna vysoká úroveň bezpečnosti on-line účtů.

PIN

Osobní identifikační číslo (PIN) je číselný kód používaný v autentizačním procesu k ověření identity uživatele pokoušejícího se o přístup k systému, zařízení nebo účtu na rozdíl od hesla, což mohou být znaky, čísla a speciální znaky, PINy se obvykle skládají pouze z

matematických znaků. PINy se obvykle používají v situacích, kdy je potřeba rychlé a jednoduché ověření. Používání autentizačních PINů je běžné v různých kontextech. Často se používá například jako bezpečnostní mechanismus pro odemykání chytrých telefonů, přístup k bankovním účtům prostřednictvím bankomatů, provádění finančních transakcí a získávání přístupu do bezpečných míst. Díky jednoduchému kódu účtu je relativně snadné zapamatovat si PIN, čímž se snižuje pravděpodobnost, že jej uživatelé zapomenou. Pokud však jde o zabezpečení, je třeba mít na paměti některé věci. Vzhledem k tomu, že PINy jsou obvykle menší než složitá hesla, mohou být zranitelné vůči agresivním útokům, kdy útočník zkouší několik kombinací, dokud nenalezne tu správnou.

Z tohoto důvodu je důležité, aby uživatelé nezadávali snadno odhadnutelná čísla, jako je datum narození, sériové pořadí např. 1234, nebo opakující se číslice např. 1111. Pro zvýšení zabezpečení PINu lze implementovat několik akcí. Patří mezi ně volba sekvence znaků, která není snadno spojena s osobními údaji, vyhnutí se použití stejného PINu pro více účtů a pravidelná aktualizace, aby se snížilo riziko manipulace. (Kagan 2023)

V souhrnu je PIN číselný kód používaný pro autentizaci, který nastoluje rovnováhu mezi zranitelností a zabezpečením. I když zapamatovat si PIN je jednoduché a snadno použitelné, uživatelé by se měli mít na pozoru před výběrem PINu, které není snadné uhodnout, a zvážit dodatečná bezpečnostní opatření, jako jsou role dvou transakcí, k další ochraně svých účtů a informací. Z důvodu, že je PIN pouze malá kombinace čísel, využívá se převážně s dalším autentizačním prvkem, jako je například karta při výběru z bankomatu, nebo jiné při vstupu do bankovní aplikace, neboť při případném útoku musí útočník nejprve úspěšně odpozorovat PIN a pak ještě získat například právě platební kartu. (Matyáš 2008)

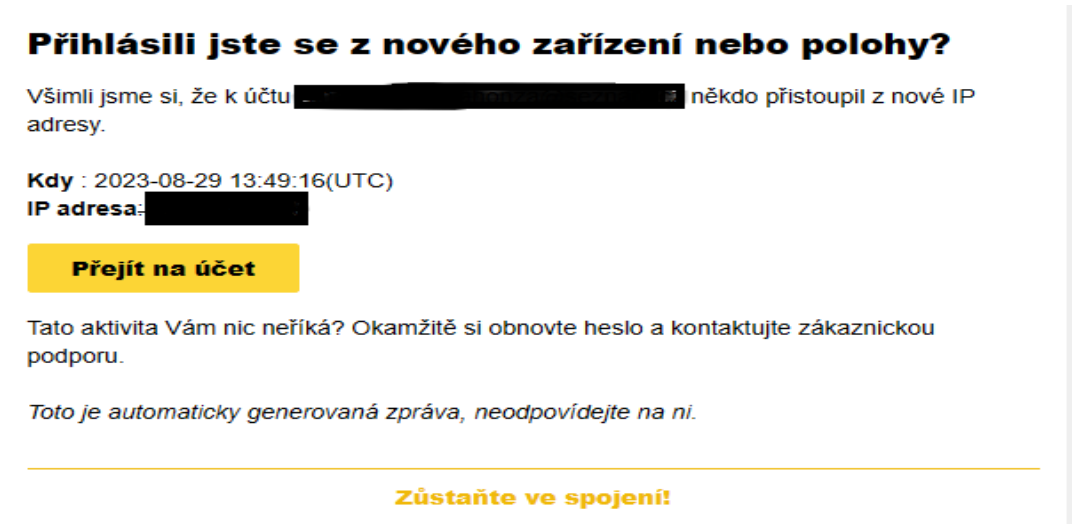
3.3.2 Faktor vlastnictví

Autentizace přidává proprietární faktor, který je stěžejní pro proces vytváření vlastní identity v digitální sféře. Tato funkce je vložena do hmotného nebo digitálního subjektu, který někomu patří, a tím posiluje bezpečnost nad tradičním heslem nebo PINem. Uzamykací mechanismus je důležitým zabezpečovacím zařízením, chránícím digitální majetek před neoprávněným přístupem. Přidává určitou úroveň bezpečnosti tím, že zajišťuje, aby přístup k citlivým systémům, aplikacím nebo informacím měli pouze autorizovaní jednotlivci.

Zařízení

Použití tohoto faktoru spočívá v přidružování certifikovaného zařízení ke konkrétní IP adrese. Je-li zařízení uživatele připojeno k síti, je IP adresa identifikátorem tohoto zařízení. Organizace mohou zvýšit bezpečnost autentizačních systémů tím, že zajistí, aby IP adresa odpovídala autorizovanému zařízení, které může být například počítač, nebo mobilní telefon. Telefon se pro vstup do bankovnictví, díky jeho pohodlnosti a rychlosti, využívá nejvíce, neboť se můžete přihlásit odkudkoliv. Zařízení uživatele může být spojené s konkrétní IP adresou, se kterou často komunikuje. Pokud pokus o ověření pochází z neznámé adresy IP, může systém vyzvat uživatele k dodatečné autentizaci, například k jednorázovému kódu z autentizační aplikace nebo k bezpečnostní otázce. Tato akce zvyšuje zabezpečení tím, že potvrzuje, že uživatel vlastní autorizované zařízení.
I když však IP adresy mohou poskytnout další loajalitu, nejsou neprůstřelné. IP adresy se mohou měnit v důsledku dynamické distribuce ze strany poskytovatelů internetových služeb, nebo využívání virtuálních privátních sítí (VPN). IP adresy mohou být útočníky zfalšovány nebo manipulovány. Je proto důležité podporovat autentizaci IP adres s dalšími prostředky. (GOV 2020)

Obrázek 4 - Oznaámení a příhlášení z jiné IP adresy



Zdroj: vlastní (2023)

Jedním z nejdůležitějších aspektů autentizace je vlastnický faktor, který zahrnuje držení něčeho fyzického nebo digitálního k ověření vlastní identity Jednou z nejběžnějších a

nejužitečnějších aplikací v této oblasti jsou smartphony, které jsou použity v procesu ověřování. Smartphony se staly všudypřítomnými společníky v našem každodenním životě a jejich integrace s autentizačními metodami přidává další úroveň bezpečnosti. Vlastnictví chytrých telefonů umožňuje uživatelům zjistit si identitu v digitálních interakcích.

Mobilní telefony také usnadňují distribuci ověřovacích kódů. Prostřednictvím SMS, hlasových hovorů nebo push notifikací uživatelé dostávají kódy, které následně zadají k ověření. Tato metoda maximalizuje ovládání smartphonu uživatele, což mu umožňuje okamžitě se identifikovat. To útočníkům znemožňuje vydávat se za uživatele z jiného zařízení, než který uživatel již použil. Smartphony navíc umožňují biometrickou autentizaci. Funkce, jako je snímání otisků prstů nebo rozpoznávání obličeje, využívají unikátní prvky uživatele.

V dnešním digitálním prostředí, kde jsou narušení bezpečnosti a neautorizované pokusy o přístup neustálým problémem, klade integrace chytrých telefonů jako vlastnického faktoru větší důraz na proces autentizace. Toto je příklad toho, že jde o neustále se měnící povahu kybernetické bezpečnosti a přizpůsobení se rychlému technologickému pokroku.

Chytrá karta

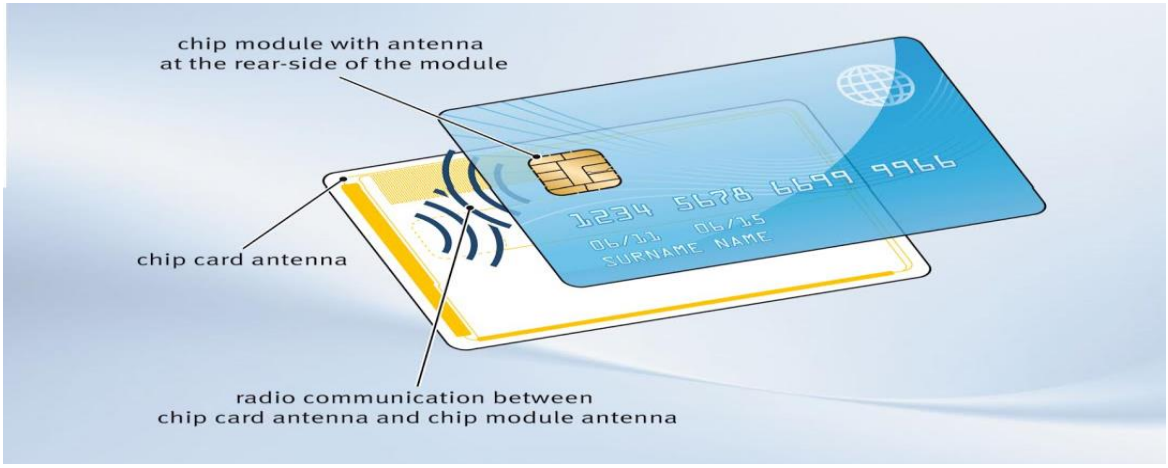
Tento přístup využívá fyzický objekt – čipovou kartu – k autentizaci a zavedení autorizovaného přístupu k digitálním systémům, aplikacím a soukromým datům. je malé přenosné zařízení, které obsahuje mikročip, který ukládá šifrovaná data. Tyto údaje mohou zahrnovat pověření a informace o ověření. Nošením této fyzické karty uživatelé zvyšují zabezpečení.
Používá se pro generování, ukládání a používání kryptografických klíčů. Ověřování čipovými kartami poskytuje uživatelům zařízení čipových karet pro ověření. Uživatelé připojují svou kartu ke stolnímu počítači. Software v přijímacím počítači ověřuje uživatele tím, že komunikuje s klíčem a dalšími údaji uloženými na čipové kartě. Aby čipová karta fungovala, musí ji uživatel odemknout uživatelským PINem.

Čipové karty se obvykle používají v zabezpečených prostředích, jako jsou firemní úřady, vládní úřady, kde je přísná kontrola. V tomto procesu je karta vložena do čtečky karet, která

komunikuje s vloženým mikročipem za účelem ověření uživatele. *„Obecně platí, že čipové karty jsou nejsilnější metodou ověřování.“* (Kružíková 2020)

Jedním z nejčastějších způsobů využití čipových karet jsou platební karty, jako jsou kreditní karty a debetní karty. Většina z těchto karet jsou „čipové a PIN“ karty, které vyžadují PIN, zatímco jiné jsou „čipové a podpisové“ karty, které vyžadují, aby se zákazníci k autentizaci podepisovali. Navíc lze tuto kartu použít jako „elektronickou peněženku“. Chytré karty nabízejí lepší řešení pro transakce elektronického obchodu, protože nabízejí lepší výsledky v oblasti bezpečnosti a soukromí než jiné finanční systémy.

Obrázek 5 - Popis čipové karty



Zdroj: KSEC Tagbase (2022)

Bezkontaktní platby zahrnují způsob transakce, při kterém čipová karta bezdrátově komunikuje s platebním terminálem za účelem dokončení platby. Transakční proces je rychlý a jednoduchý. Tato metoda se často používá při rychlých a levných transakcích, jako jsou jízdné ve veřejné dopravě nebo drobné nákupy potravin.

S přibývajícím trendem nenošení hotovosti se zvyšuje používání bezkontaktních plateb nejen pomocí karet, ale i chytrými hodinkami, telefonem nebo prstenem. Tato metoda se opírá o technologii identifikace na základě rádiové frekvence (RFID) nebo komunikace v blízkosti pole (NFC), která usnadňuje komunikaci mezi platební prvkem a místem platby. Bezkontaktní přiložení lze využít i při práci s bankomatem, a tudíž si můžete vybrat hotovost i bez karty. (Forbes 2024)

Jako každé bezpečnostní opatření se však neobejde bez problémů. Ztráta či krádež může ohrozit bezpečnost a je potřeba nahlášení ztracených karet a zavedení dodatečných bezpečnostních opatření. V dnešní době jde platit už i bezkontaktně. Obecně je nastaveno (národní limit), že do částky 500 korun není potřeba zadat PIN, čehož může být využito ve váš neprospěch. (ČSOB)

Čipovou kartu lze považovat za hardwarový token. Jde o fyzické zařízení, které kombinuje funkce tradiční kreditní nebo debetní karty s pokročilou počítačovou technologií. Dokáže bezpečně ukládat a zpracovávat data, čímž se stává účinným prostředkem autentizace, ukládání dat a zabezpečených služeb. Čipové karty se běžně používají jako hardwarové tokeny v celé řadě odvětví, včetně bankovnictví i mimo něj.

Hardware token

V bankovním odvětví, kde je bezpečnost dat a důvěra zákazníků prvořadá, používání hardwarové autentizace tokenů vydobylo pověst silného bezpečnostního mechanismu. Tento autentizační mechanismus kontroluje používání fyzických zařízení zvaných hardwarové tokeny za účelem zvýšení bezpečnosti kritických operací a výkonnosti služeb. Hardwarové tokeny jsou rozpoznatelná zařízení navržená tak, aby generovala jedinečný časově citlivý kód nebo heslo. Tyto tokeny jsou typicky malé a přenosné, jako třeba klíčenka, USB zařízení nebo již zmíněna čipová karta s vestavěnými mikročipy.

Obrázek 6 - Hardware token

Zdroj: Protectimus (2020)

Každá z těchto karet má své jedinečné vlastnosti a výhody. Některé hardwarové tokeny mají malý displej, který generuje jednorázová hesla (OTP), která se mění obvykle každých 30 sekund. Tento časově náročný kód se používá k autentizaci, což ztěžuje uživatelům se zlými úmysly znovu použít ukradená pověření. Hardwarové tokeny mohou být také součástí širšího systému známého jako infrastruktura veřejných klíčů (PKI). V takovém případě tokeny ukládají kryptografické klíče používané pro digitální podpisy a šifrování a další funkce. To je cenné zejména v korporátním prostředí, kde je bezpečné připojení a navazování kontaktů prvořadé. (Andress 2014)

Jednou z hlavních výhod hardwarových tokenů je jejich schopnost pracovat na internetu. I v případě, že systém, který vyžaduje autentizaci, nemá připojení k internetu, může token sloužit jako důležitý kód, který zajišťuje přístup ke kritickým systémům za různých okolností. Mnoho moderních hardwarových tokenů má zabezpečenou vrstvu, což je v podstatě hardwarový čip, který zajišťuje ukládání citlivých informací a vykonává kryptografické funkce. Tato bezpečná vrstva přidává velkou míru bezpečnosti, takže bude pro útočníky mimořádně získat uložená data. Hardwarové tokeny nacházejí uplatnění v nejrůznějších odvětvích a aplikacích. Běžně se používají v internetovém bankovnictví, korporátních sítích, řešeních vzdáleného přístupu, virtuálních privátních sítích, cloudových službách a dalších. Jejich hustota je zvláště vysoká v oblastech, kde je přístup k bezpečnosti kritický.

Uživatelé mohou tato dostupná zařízení špatně umístit nebo o ně přijít, což způsobuje problémy. Organizace musí řídit bezproblémový proces certifikace pro přidělování, výměnu a případné ztráty tokenů. Jak se technologie vyvíjí, vyvíjejí se i hardwarové tokeny. Některé tokeny nyní integrují biometrické senzory a přidávají tím tak dodatečnou autentizaci a bezpečnost uživatelů.
Hardwarové tokeny nejsou v podstatě jen zařízení; Jsou součástí finančního sektoru ke kybernetické bezpečnosti. Poskytováním lepší autentizace, šifrování, dodržování předpisů a předcházení podvodům tyto tokeny posilují důvěru mezi bankami a jejich zákazníky.

Velkým aktuálním tématem jsou i krypto peněženky, což je zařízení navržené tak, aby poskytovalo bezpečný a pohodlný způsob ukládání a správy kryptoměn. Poskytuje robustní řešení pro řešení bezpečnostních problémů spojených s digitálními aktivy, jako jsou Bitcoin, Ethereum a další kryptoměny. Tradiční banky, instituce se zavedeným regulačním rámcem a

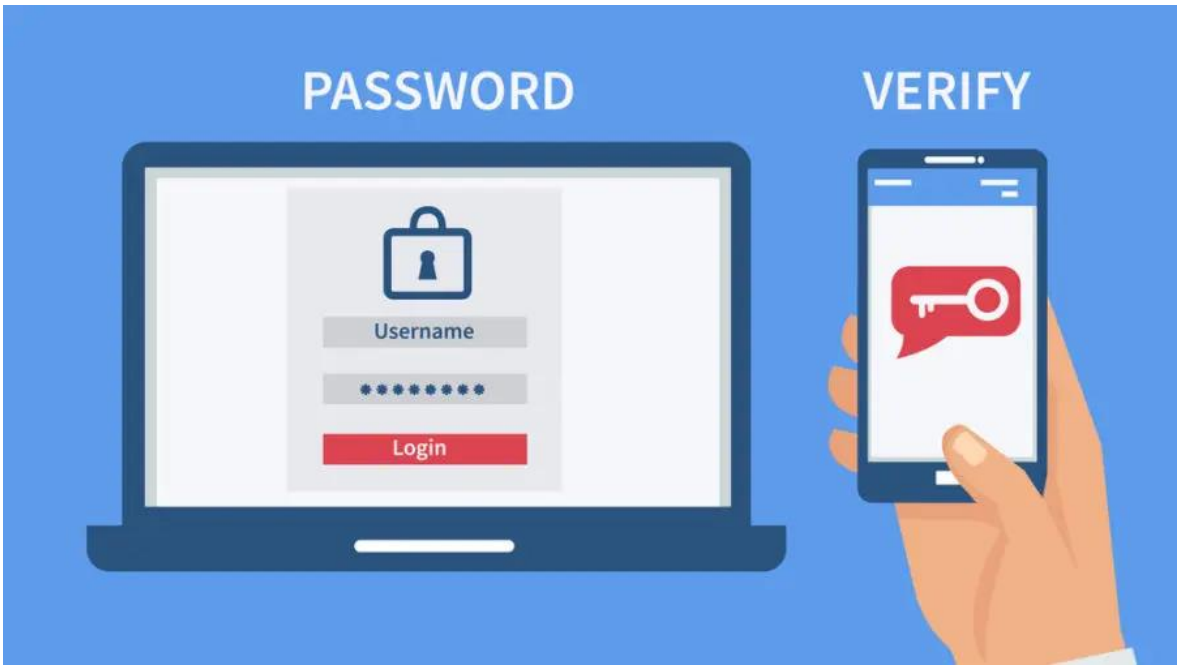
finanční strukturou, hrají roli ve vyvíjejícím se ekosystému kryptoměn. Banky sice nespravují přímo soukromé klíče pro kryptoměny, ale některé začaly nabízet integraci a podporu pro transakce s digitálními aktivy.

Software token

Softwarové tokeny jsou ve svém jádru softwarové aplikace, které generují časově citlivé dynamické autentizační kódy. Jinak řečeno využívá metodu OTP jako hardware token, ale pomocí aplikace na zařízení.
Když si uživatel nastaví softwarový token, obvykle ve svém zařízení používá autentizační aplikaci. Tato aplikace funguje jako platforma pro generování a zobrazování OTP. V prvním programu se vygeneruje unikátní kryptografický „seed“ neboli tajný klíč. Tento výsledek je znám pouze uživateli a programu důvěry. Když se uživatel pokusí o přístup do chráněného systému, služby nebo aplikace, zaznamenává jeho pravidelná přihlašovací pověření (jméno, heslo, biometrie atd.) spolu s aktuálním OTP. (EasyTechJunkie 2023)

Autentizační aplikace jsou velmi používanou funkcí pro přístup do internetového bankovnictví nebo práci v něm. Na mobilních telefonech vás banky mnohdy samy přesměrují na aplikaci třetí strany, nebo vám přijde notifikace, kde jen potvrdíte, že jste to opravdu vy, nebo že souhlasíte s daným úkonem a máte hotovo.

Obrázek 7 - Ověření soft tokenem



Zdroj: CyberHoot (2020)

Softwarové tokeny sice omezují přístup a zvyšují bezpečnost, ale nejsou tak bezpečné jako hardwarové tokeny. U hardwarových tokenů musí být samotný token fyzicky odcizen, pokud se někdo pokusí informace duplikovat, je token naprogramován k vymazání jeho paměti, pokud není digitální transportní metoda bezpečná, nebo pokud je stroj zaměstnance infikován virem. (Protectimus 2015)

Výhodou používání softwarových tokenů je, že jsou flexibilní a snadno se stahují. Pokud zaměstnanec potřebuje nový token, buď proto, že byl vymazán z paměti, nebo proto, že časový limit aktuálního tokenu je neplatný, může vydání nového tokenu zabrat pár sekund, zatímco hardwarové tokeny se obtížněji obnovují.

3.3.3 Genetický faktor

Genetický faktor, často označovaný jako „něco, čím jste“, je důležitým autentizačním faktorem založeným na jedinečných biologických vlastnostech člověka (biometrie) pro zajištění autenticity a je jednou ze tří hlavních složek autenticity.

Biometrie, zahrnuje jedinečné fyzikální vlastnosti, které jedince od sebe odlišují. Tyto vlastnosti jsou hluboce zakotveny v biologii člověka a je obtížné je napodobit. Mezi běžné

příklady biometrických údajů patří otisky prstů, rysy obličeje, vzory duhovky, hlasové znaky apod.

V posledních letech, kdy jsou aplikace pro mobilní bankovnictví stále populárnější, získávají biometrické metody ověřování, jako je snímání otisků prstů a rozpoznávání obličejů, na oblibě jako alternativy k tradičním heslům. Tyto metody nabízejí pohodlí a bezpečnost, protože spoléhají na jedinečné fyzické atributy a lze je využít již kdykoliv na mobilním zařízení.

Otisk prstu

Ověřování otisků prstů je sofistikovaná forma ověřování totožnosti, která využívá jedinečný otisk prstu každého člověka k zajištění bezpečného přístupu k systémům, zařízením a službám. Tato biometrická metoda se stala základním kamenem moderní bezpečnosti a nabízí bezproblémovou kombinaci komfortu a efektivity.

Autentizace otisků prstů se rychle vyvinula jako nedílná součást bankovní autentizace, která nově definuje, jak jednotlivci přistupují ke svým finančním účtům a transakcím. Tradiční metody, jako jsou hesla a PIN, jsou náchylné k narušení a neoprávněnému přístupu. Jedinečný otisk prstu činí výjimečně silnou bariéru proti krádeži a podvodům lidmi. Pokusy o kopírování nebo falšování otisků prstů je vysoce nepravděpodobné. Pouhým dotykem prstu na senzoru lze rychle a bezpečně ověřit identitu.

Obrázek 8 - Placení pomocí otisku prstu

Zdroj: Česká spořitelna (2021)

Banky mohou sledovat aktivitu otisků prstů a detekovat tak jakékoli nepravidelné vzory nebo podezřelé pokusy o přihlášení. Tento proaktivní přístup pomáhá identifikovat potenciální hrozby dříve, než přerostou v plnohodnotné narušení bezpečnosti.

Autentizace sítnice

Autentizace sítnice je sofistikovaná biometrická technika, která využívá unikátní cévy nalezené v lidské sítnici k ověření identity. Přesná a bezpečná metoda často používaná v extrémním bezpečnostním prostředí.

.

Ověřování sítnicového vzoru není běžnou metodou používanou v bankách. I když je autentizace sítnicového vzoru vysoce bezpečnou a přesnou biometrickou technikou, má několik praktických omezení a úvah, které mohou zkomplikovat její široké přijetí v bankách.

Rozpoznání obličeje

Rozpoznávání obličeje jako autentizace je sofistikovaná technologie, která využívá jedinečných vlastností obličeje člověka k potvrzení jeho identity. Tato metoda si díky své jednoduchosti a zabezpečení získala oblibu v oblasti bezpečnosti, ekonomiky, zdravotnictví a spotřební elektroniky. Analýzou obličejových charakteristik, jako je složení a symetrie, technologie vytváří jedinečný identifikační kód pro každou osobu.

Ověření rozpoznávání obličeje spočívá v zachycení obličeje osoby kamerou, zpracování obrazu tak, aby matematicky představoval obličej jako šablonu, a následném porovnání se šablonami uloženými v databázi. Tento proces zajišťuje, že je identita člověka přesně a účinně ověřena.

Obrázek 9 - Platba pomocí FaceID

Zdroj: Apple (2023)

Pokroky v umělé inteligenci a strojovém učení zpřesnily rozpoznávání obličejů, což z něj činí důležitý bezpečnostní nástroj. Jeho aplikace jsou různorodé, od odemykání chytrých telefonů po hraniční kontrolu. Jediné obavy mohou přibývat ohledně ochrany soukromý, což s rychle postupujícím se pokrokem v informačních technologiích a zabezpečení, se rizika zneužití budou stále snižovat.

4 Analytická část

Praktická část bakalářské práce se zabývá analýzou využití vícefaktorové autentizace převážně v oblasti bankovnictví včetně analýzy a zhodnocení případové studie v rámci ČZU.

Klíčovým faktorem provedení dané analýzy je aktuálnost tématu. V současné době je bezpečnost informací a ochrana před kybernetickými hrozbami stále naléhavějším problémem, zejména v bankovnictví, kde jsou údaje klientů a finanční transakce v ohrožení. Prozkoumání vícefaktorové autentizace v bankovním prostředí může poskytnout pohled na to, jaké bezpečnostní opatření jsou v současnosti v praxi a jak efektivní mohou být při ochraně citlivých dat.

4.1 Úvod

V této části je uvedena analýza výsledků dotazníku, zaměřeného na bezpečnost a spokojenost s online bankovnictvím. Cílem tohoto průzkumu bylo získat hlubší porozumění postojů a zkušeností respondentů v oblasti používání vícefaktorové autentizace a jejího vlivu na vnímanou bezpečnost a pohodlí při správě bankovních účtů online. Jinak řečeno: Jaké faktory přispívají k pozitivnímu vnímání nasazení vícefaktorové autentizace uživateli bankovnictví.

V rámci jednoho listopadového dne, na více místech budovy PEF na ČZU, se mohli studenti dobrovolně zúčastnit zodpovězení otázek a přispět k analýze výsledků zabezpečení internetového bankovnictví. Dotazník k vyplnění dostávali na chytrém zařízení s předem stanovenými otázkami.
Osoby ženského pohlaví byli stydlivější a nechtěli se zúčastnit analýzy i po případném oslovení, narozdíl od mužů.
Celkový počet získaných výsledků se vyšplhal na více než 166.

Dále bude ještě proveden výpočet vícekriteriální analýzy s váhami pro výběr nejlepší varianty autentizace z pohledu bank. (Soukopová 2013)

Stanovení vah lze vyjádřit pomocí vektoru vah kritérií v (přičemž platí, že čím je kritérium významnější (resp. důležitější), tím je i jeho váha větší):

$$v = (v1,v2,...,vk) , \sum = k \; i \; 1 \; vi = 1 , vi \geq 0.$$

Následně bude použita bodovací metoda.

V této metodě se vypočítá ohodnocení variant:

$$h_i = \sum_{j=1}^{k} v_j y_{ij}$$

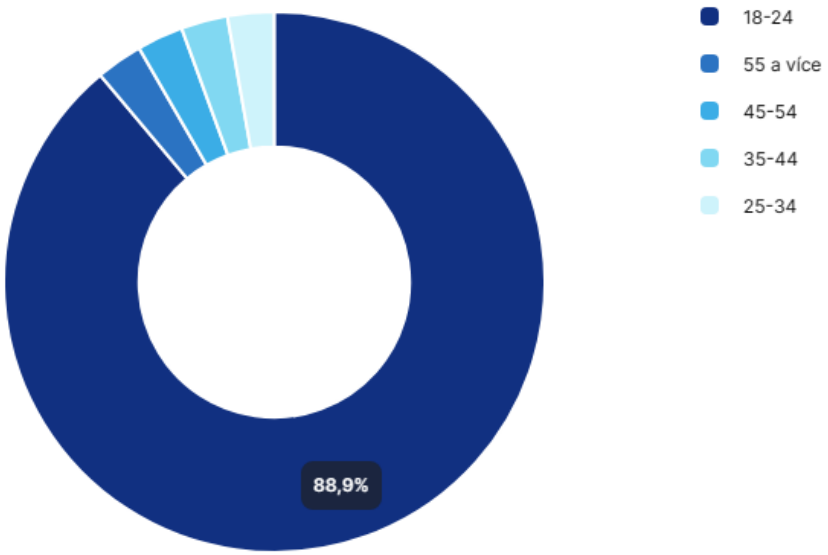
kde hi je ohodnocení i-té varianty, i = 1, 2, …, n ,
yij jsou hodnoty kriteriální matice Y,
vj je normovaná váha j-tého kritéria, j = 1,2, …, k

4.2 Základní údaje respondentů

V této kapitole je poskytován komplexní přehled klíčových výsledků dotazníku, které se zaměřují na věkovou strukturu, pohlaví a úroveň vzdělání respondentů. Tato základní analýza nám poskytuje pevný základ pro hlubší zkoumání vztahu mezi věkem, vzděláním a vnímáním pohodlí v online bankovnictví.

Výraznou většinu respondentů tvoří mladí jedinci ve věku 18-24 let. Tato skupina představuje klíčový segment, ze kterého můžeme získat podrobné informace o postojích mladší generace k bezpečnosti.

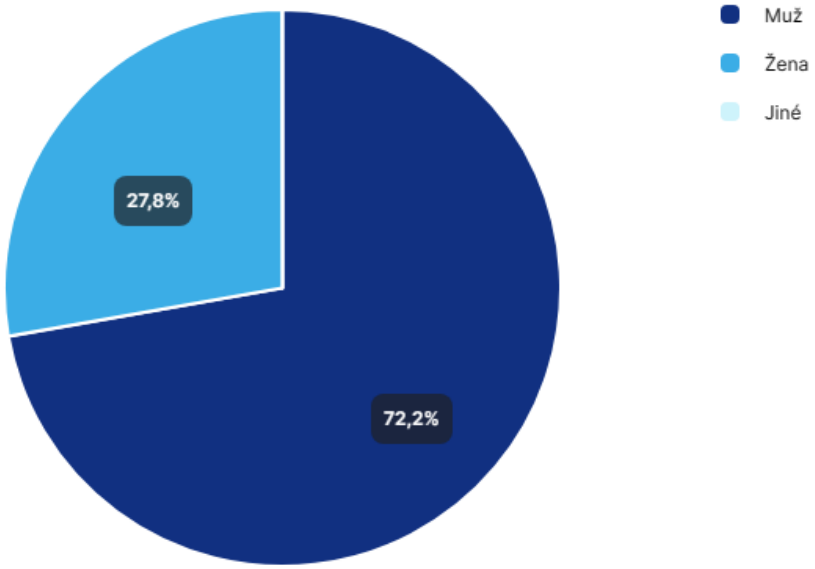
Graf 1 - Věkové rozmezí respondentů



Zdroj: vlastní zpracování

Rozložení pohlaví nám poskytuje další dimenzi pro analýzu výsledků. Zjišťujeme, že v našem vzorku bylo více mužů, což může ovlivnit dynamiku odpovědí v závislosti na pohlaví.

Graf 2 - Pohlaví respondentů



Zdroj: vlastní zpracování

Z výsledku je patrné, že většina respondentů má středoškolské vzdělání. To může ovlivnit jejich povědomí o bezpečnostních opatřeních.

Střední škola: 58. 3%
Vysoká škola/Bakalářský stupeň: 33. 3%
Vysoká škola/Magisterský stupeň: 8. 3%
Doktorát: 0%
Základní škola: 0%

Tyto základní údaje nám poskytují rámcový pohled na vzorek respondentů.

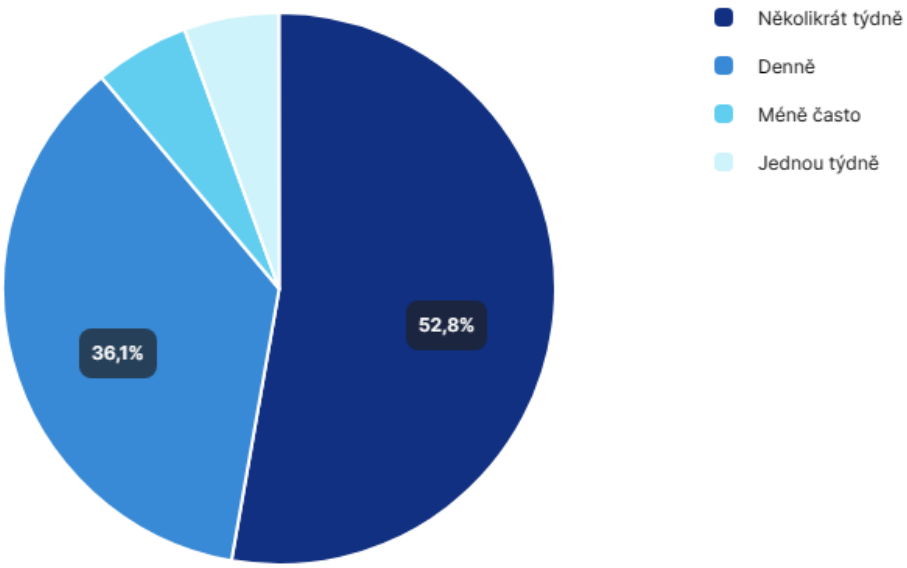
4.3 Používání internetového bankovnictví

Analýza frekvence používání internetového bankovnictví a mobilních bankovních aplikací poskytuje důležité informace o zvyklostech respondentů.
Jedním z klíčových faktorů pro pochopení angažovanosti respondentů v digitálním bankovnictví je četnost jeho používání. Z výsledků dotazníku vyplývá:

Několikrát týdně: 52.8%
Denně: 36.1%
Méně často: 5.6%
Jednou týdně: 5.6%
Tato analýza naznačuje, že většina respondentů využívá internetové bankovnictví pravidelně a často. Rostoucí trend používání digitálních finančních služeb poukazuje na rostoucí důvěru v tuto moderní formu bankovnictví.

Lidé dnes mají jedinečnou výhodu v podobě možnosti otevřít internetové bankovnictví prostřednictvím svých mobilních telefonů, a to kdykoliv a kdekoliv. Tato schopnost přináší nový rozměr pohodlí a flexibility v jejich finančním životě.

Graf 3- Návštěvnost internetového bankovnictví



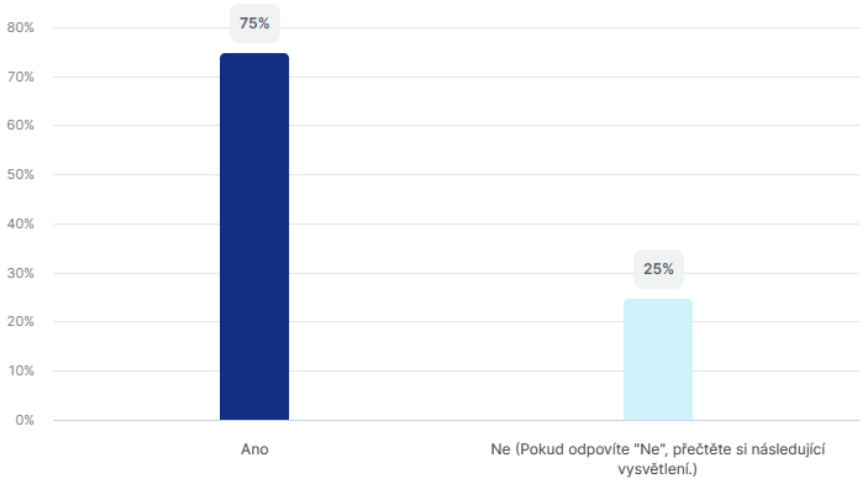
Zdroj: vlastní zpracování

Mobilní bankovnictví poskytuje mladým lidem flexibilitu při správě svých financí. Mohou jednoduše provádět platby, získávat informace o svých účtech a sledovat transakce, a to vše na dosah ruky. Tato nezávislost na místě a čase otevírá nové možnosti pro efektivní řízení financí.

S výhodami mobilního bankovnictví přicházejí i otázky bezpečnosti. Analyzujeme, jak mladí lidé vnímají bezpečnostní opatření, zejména v kontextu používání vícefaktorové autentizace. Tato skupina, která má pravděpodobně silné propojení s digitálními technologiemi, může poskytnout důležité informace o postojích k bezpečnosti v online prostředí.

Dalším klíčovým aspektem je povědomí respondentů o bezpečnostních opatřeních, konkrétně o vícefaktorové autentizaci.

Graf 4 - Znalost MFA



Zdroj: vlastní zpracování

Vysoký podíl respondentů, kteří znají termín "vícefaktorová autentizace", svědčí o relativně širokém povědomí o této bezpečnostní metodě. Tato znalost může ovlivnit postoj respondentů k bezpečnosti online bankovnictví a jejich schopnost ji plně využít.

Je skvělé vidět, že mladí lidé jsou seznámeni s pojmem MFA v bankovnictví, což naznačuje jejich povědomí o důležitosti bezpečnosti online transakcí a ochrany osobních účtů. Výsledky z dotazníku ukazují, že tato generace projevuje zvýšený zájem o moderní bezpečnostní opatření, která přinášejí vyšší úroveň ochrany v digitálním prostoru.

Vícefaktorová autentizace, jak ukazují odpovědi z dotazníku, je vnímána jako klíčový prvek v posilování bezpečnosti při práci s bankovními účty online. Mladí lidé jsou si pravděpodobně vědomi rizik spojených s používáním jednoduchých hesel a jednoúrovňových autentizačních metod. Tato povědomí mohou být důsledkem neustálých varování o kybernetických hrozbách, které jsou v dnešní digitální době stále pronikavější.

Dalším aspektem je četnost, s jakou jsou respondenti vyzváni k provedení vícefaktorové autentizace.

Vždy: 52.8%
Často: 16.7%
Občas: 13.9%
Zřídka: 11.1%
Nikdy: 5.6%

Vysoká četnost výzev k provedení MFA svědčí o tom, že organizace a poskytovatelé služeb si jsou vědomi potřeby zlepšit úroveň zabezpečení a chránit své uživatele před různými formami kybernetických hrozeb. Tento trend také odráží snahu přizpůsobit se dynamickému prostředí bezpečnosti a reagovat na neustále se vyvíjející techniky útoků.

Obrázek 10 - Využití šifrování a MFA v oborech

Zdroj: Eset (2022)

Pro uživatele může být inicializace vícefaktorové autentizace na první pohled považována za malou nepříjemnost, ale ve skutečnosti poskytuje významné zlepšení v oblasti bezpečnosti. V kombinaci s dalšími bezpečnostními opatřeními může MFA efektivně minimalizovat riziko úniku citlivých informací a ochránit uživatele před zneužitím účtů.

Lze konstatovat, že výzvy k provedení vícefaktorové autentizace jsou klíčovým prvkem moderního bezpečnostního paradigmatu a představují pozitivní krok směrem k ochraně digitálních identit a dat.

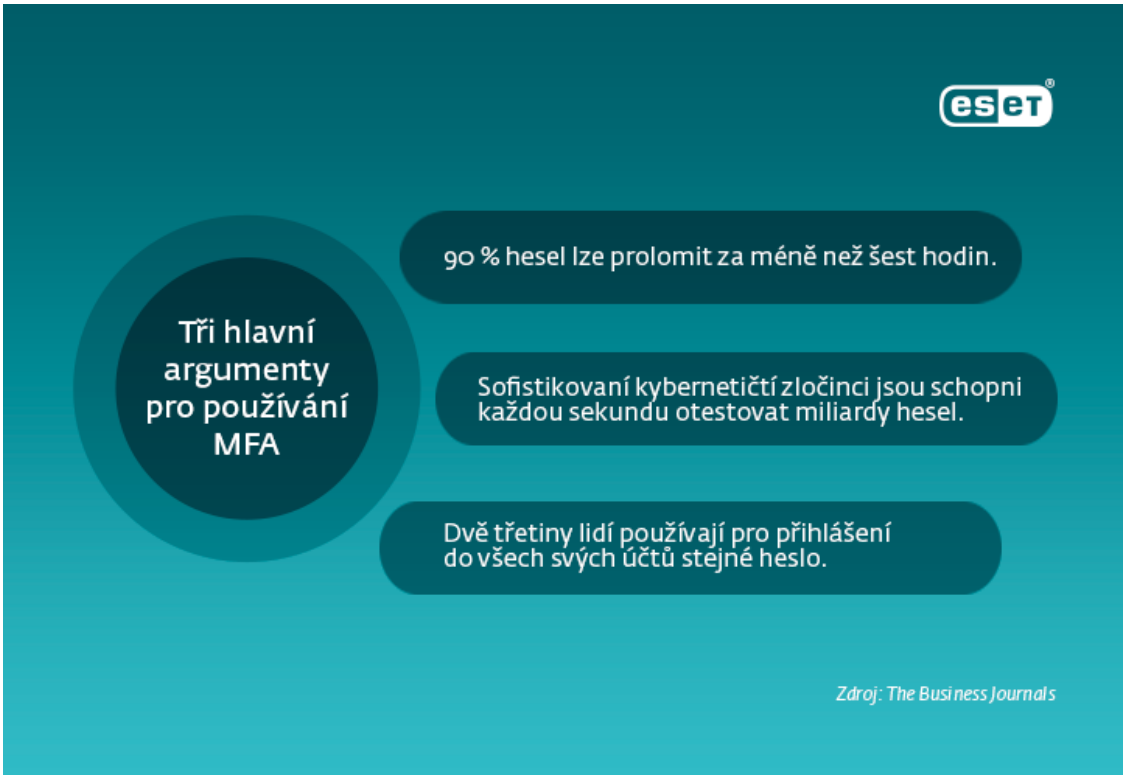
4.4 Hodnocení úrovně bezpečnosti

Respondenti byli také dotázáni, jak by hodnotili úroveň bezpečnosti vícefaktorové autentizace ve srovnání s používáním pouze uživatelského jména a hesla. Výsledky ukázaly následující rozložení:

Bezpečnější: 50%
Mnohem bezpečnější: 47.2%
Mnohem méně bezpečné: 2.8%

Jedním z klíčových faktorů je skutečnost, že MFA přidává další vrstvu ochrany, čímž ztěžuje neoprávněným osobám překonání bezpečnostních bariér. Použitím více nezávislých prvků pro ověření identity, jako jsou ověřovací kódy zasílané na mobilní zařízení nebo biometrická data, se zvyšuje bezpečnostní úroveň účtu.

Obrázek 11 - Argumenty využívání MFA



Zdroj: Eset (2022)

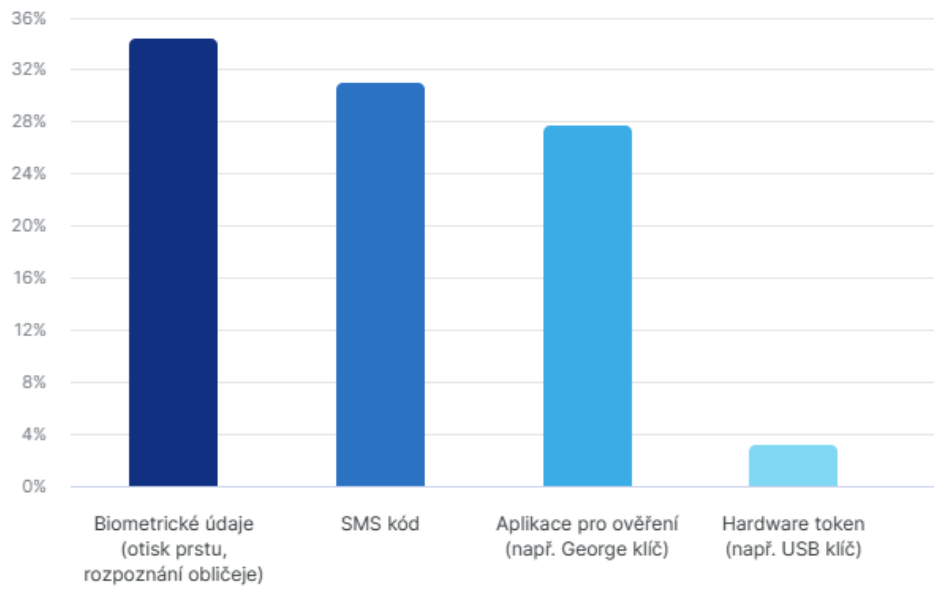
V rámci průzkumu, zaměřeného na vnímání schopnosti vícefaktorové autentizace (MFA) v ochraně bankovních údajů, se ukázalo, že respondenti převážně přisuzují této technologii vysokou úroveň bezpečnosti. Při hodnocení na škále od 1 do 5 vykázala více než polovina respondentů (54.3 %) důvěru na úrovni 4.

Není méně pozoruhodné, že zhruba třetina respondentů (28.6 %) udělila maximální hodnocení 5. Tato skupina jednotlivců vyjadřuje vysoký stupeň důvěry v účinnost MFA a považuje ji za klíčový nástroj pro zabezpečení svých finančních informací v digitálním prostoru.

Je zajímavé, že i když existuje určitý podíl respondentů (17.1 %), kteří udělují střední hodnocení 3, které může naznačovat mírný skepticismus nebo vnímání omezení MFA, žádný z účastníků nedosáhl hodnocení 2 ani nižšího hodnocení 1.

Dále byli respondenti dotázáni na typy vícefaktorové autentizace, které v minulosti používali.

Graf 5- Využívané typy MFA



Zdroj: vlastní zpracování

V rámci sledovaného průzkumu o preferencích využívaných typů vícefaktorové autentizace (MFA) se ukázalo, že biometrické údaje, konkrétně otisk prstu a rozpoznání obličeje, představují dominantní metodu s vysokým podílem 35.1 %. Tato statistika naznačuje rostoucí důvěru respondentů v bezpečnost a pohodlí spojené s biometrickými technologiemi. Otisk

prstu a rozpoznání obličeje jsou vnímány jako moderní, bezpečné a uživatelsky přívětivé možnosti ověření identity.

Druhým nejčastěji využívaným typem MFA jsou SMS kódy, které získaly podíl 31.7 %. Tato klasická metoda, která spočívá v přijímání ověřovacích kódů prostřednictvím krátkých textových zpráv, zdůrazňuje důvěru uživatelů ve snadnou dostupnost a rychlost této formy ověřování.

Aplikace pro ověření, jako je například George klíč, obsadily třetí místo s podílem 27.9 %. Tato skupina respondentů upřednostňuje využívání mobilních aplikací pro generování ověřovacích kódů, což může být spojeno s vysokou mobilitou a rychlým přístupem k ověřovacím údajům.

Obrázek 12 - Aplikace George klíč

Zdroj: Česká spořitelna (2021)

Naopak, hardware tokeny, zastoupené například USB klíči, jsou s podílem 3.8 % méně využívané. Nízký zájem o fyzické prvky MFA může odrážet snahu minimalizovat komplexitu a spoléhat se na pohodlnější metody ověření.

V průběhu zkoumání postojů respondentů k bezpečnosti v oblasti bankovnictví se ukazuje, že bezpečnostní otázky představují pro všechny účastníky průzkumu mimořádně důležitý aspekt. Tato jednotnost v hodnocení naznačuje, že bez ohledu na různorodost individuálních potřeb a

zkušeností sdílí všichni účastníci shodný zájem o ochranu svých finančních údajů a bankovních operací v digitálním prostoru.

Bankovní účty jsou často cílem kybernetických útoků, a proto je pro uživatele klíčové klást důraz na bezpečnostní opatření, která brání neoprávněnému přístupu nebo zneužití jejich finančních prostředků.

Další výsledky analýzy naznačují, že většina respondentů (91.7 %) očekává, že se vícefaktorová autentizace stane běžným standardem pro všechny online služby v budoucnosti. To svědčí o rostoucí důvěře ve vícefaktorovou autentizaci jako významný nástroj pro zajištění bezpečnosti v digitálním prostředí.

Při hodnocení pohodlí při používání vícefaktorové autentizace k přihlašování do bankovního účtu se ukázalo, že většina respondentů (74.3 %) vnímá tento proces pozitivně. Kombinace hodnocení 4 a 5 naznačuje, že více než tři čtvrtiny respondentů považují používání této bezpečnostní metody za relativně jednoduché a intuitivní.

Pohodlí hraje v moderním digitálním prostředí klíčovou roli, a to zejména v kontextu používání MFA. Přestože přidaná vrstva ověření může na první pohled působit jako zátěž, vývoj v oblasti MFA klade důraz na minimalizaci obtížnosti a zajištění co nejbezproblémovějšího přihlašovacího procesu.

Uživatelé, kteří jsou přesvědčeni o bezpečnosti svých účtů díky MFA, vnímají celý proces přihlašování jako méně obtížný. Důvěra ve spolehlivost a účinnost MFA přímo ovlivňuje to, jak jednotlivec vnímá pohodlí v rámci bezpečného přihlášení.

Moderní technologie umožňují rychlé generování ověřovacích kódů, ať už prostřednictvím SMS nebo ověřovacích aplikací, což minimalizuje čas potřebný pro dokončení přihlašovacího procesu. Rychlý a plynulý přístup k online účtům zvyšuje efektivitu MFA a snižuje jakýkoli nepříjemný pocit spojený s dlouhým čekáním.

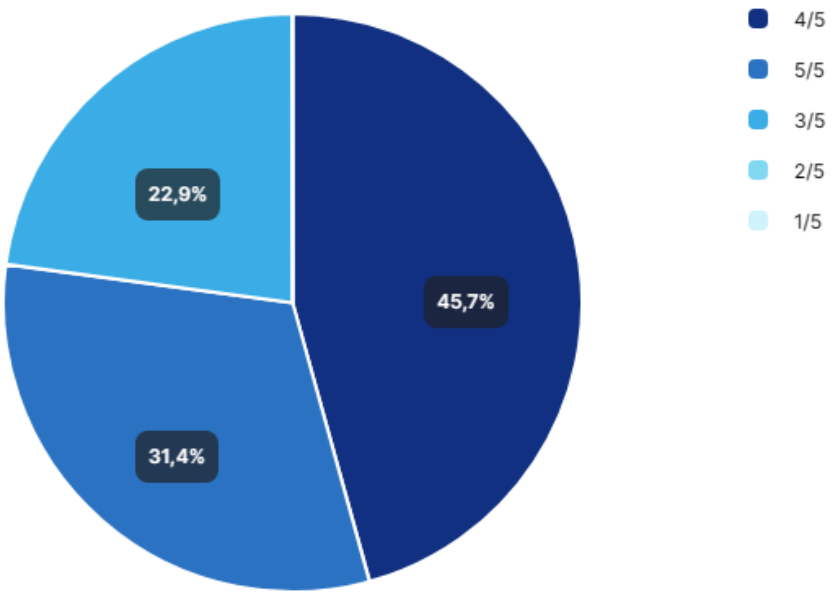
V neposlední řadě je důležitým faktorem pro pohodlí uživatelů podpora ze strany poskytovatelů služeb a firem implementujících MFA. Kvalitní uživatelské rozhraní, jasné

instrukce a případně i nápověda při nastavení MFA přispívají k bezproblémovému zavedení a užívání této bezpečnostní vrstvy.

Během analýzy byla klíčovým prvkem také otázka týkající se spokojenosti respondentů s aktuálním zabezpečením bankovnictví. Výsledky této části nabízejí zajímavý pohled na to, jak klienti hodnotí úroveň bezpečnosti ve svém bankovním prostředí.

V oblasti spokojenosti s aktuálním zabezpečením bankovnictví většina respondentů (77.1 %) vyjádřila svou důvěru hodnocením 4 nebo 5.

Graf 6 - Hodnocení spokojenosti zabezpečení bankovnictví



Zdroj: vlastní zpracování

Tato vysoká míra spokojenosti naznačuje, že klienti mají důvěru v bezpečnostní opatření, která banky implementují ke zabezpečení jejich finančních transakcí. Tato důvěra může být výsledkem efektivních preventivních opatření, jako jsou monitoring transakcí, šifrování dat a dalších bezpečnostních protokolů.

Zajímavým aspektem je, že vysoká spokojenost klientů s aktuálním zabezpečením bankovnictví je reflektována v úsilí bank informovat své klienty o bezpečnostních opatřeních

a procedurách, které chrání jejich citlivé údaje. Transparentnost a komunikace banky ohledně bezpečnosti mohou hrát klíčovou roli v budování důvěry mezi bankou a klienty.

Tato spokojenost klientů vytváří solidní základ pro udržení stávající klientely a přitahování nových klientů, kteří kladou vysoký důraz na bezpečnost svých finančních prostředků v digitálním bankovním prostředí.

4.5 Názor respondentů

V dotazníku byla položena i otázka, jak by se mohla vícefaktorová Autentizace zlepšit podle jejich názoru.

Několik názorů respondentů bylo systematicky rozděleno do tří klíčových typů, přičemž každý typ vyjadřuje specifický pohled.

Dle jednoho z názorů je současná úroveň bezpečnosti vícefaktorové autentizace považována za vysokou, s možností výběru mezi biometrickými údaji, SMS kódem nebo ověřením přes e-mail. Respondent vyjadřuje očekávání vylepšení této metody s nástupem umělé inteligence, avšak věří, že biometrické údaje, jako oční rohovka, budou obtížněji narušitelné než jiné technologické přístupy.

Obrázek 12 - Umělá inteligence

Zdroj: Generaliaeskaprofi (2023)

Další názor zdůrazňuje potřebu uživatelského přívětivosti, aby byla vícefaktorová autentizace nejen bezpečná, ale také pohodlná, a to nejen v bankovním sektoru. Tento přístup klade důraz na uživatelský komfort jako klíčový prvek pro popularizaci této bezpečnostní metody.

Poslední názor reflektuje spokojenost s aktuálním stavem vícefaktorové autentizace, konkrétně přihlašováním pomocí biometrických údajů, v tomto případě rozpoznání obličeje. Respondent věří, že biometrické ověření, jako je rozpoznání obličeje, je dostatečné pro

současnou dobu a zdůrazňuje jeho unikátnost a nemožnost jednoduchého napadení. Zároveň naznačuje, že do budoucna by dvojité biometrické ověření mohlo být vhodné pouze pro opravdu důležité aplikace.

4.6 Vícekriteriální analýza

Analýza s vypočtenými váhami je krokem k porovnání výsledků s na základě předem stanovených faktorů, které by pro banku mohli být důležitější než jiné, s výsledky dotazníku.

V tomto šetření byly vybrány čtyři nejvíce používané druhy autentizace. Biometrická autentizace, aplikační autentizace (např. generované kódy v mobilní aplikaci), Hardwarové tokeny a SMS ověření.
Jako faktory, které byly posuzovány pro přesnější vyhodnocení nejlepší varianty z pohledu bank jsou: bezpečnost, náklady na implementaci a provoz, uživatelská přívětivost, flexibilita a kompatibilita, dostupnost a spolehlivost.

Tyto faktory byly na základě získaných informací od zaměstnance České spořitelny bodově ohodnoceny, kde 5 je nejlepší a 1 je nejhorší, a následně seřazeny, v jakém pořadí jsou pro banku v jednotlivých faktorech nejdůležitější.

Tabulka 1 - Bodové ohodnocení jednotlivých faktorů

	Bezpečnost	Náklady na implementaci a provoz	Uživatelská přívětivost	Flexibilita a kompatibilita	Dostupnost a spolehlivost
Biometrická autentizace	5	2	4	2	2
Aplikační autentizace (např. generované kódy v mobilní aplikaci)	4	3	3	3	3
Hardwarové tokeny	4	3	2	2	4
SMS ověření	3	4	3	5	5

Zdroj: vlastní zpracování

Odůvodnění vybraných bodů:

Bezpečnost

- Biometrická autentizace: 5 bodů - Biometrická autentizace poskytuje vysokou úroveň bezpečnosti, protože využívá biometrické charakteristiky jednotlivců, jako jsou otisky prstů, rozpoznání obličeje nebo hlasu, což je obtížné podvrhnout nebo napodobit.
- Aplikační autentizace (např. generované kódy v mobilní aplikaci): 4 body - Pomocí generovaných kódů v mobilní aplikaci poskytuje dobrou úroveň bezpečnosti. Tyto kódy jsou generovány na základě unikátních faktorů, jako je čas nebo jednorázový kód, a jsou obtížné k napadení, pokud jsou správně implementovány.
- Hardwarové tokeny: 4 body - Poskytují vysokou úroveň bezpečnosti, protože vyžadují fyzickou přítomnost zařízení pro autentizaci. Nicméně, závisí na bezpečnosti samotného hardwarového zařízení a jeho schopnosti odolat útokům.
- SMS ověření: 3 body - Poskytuje nižší úroveň bezpečnosti ve srovnání s výše uvedenými metodami. Textové zprávy mohou být snadno odposlouchávány, zpracovány nebo přesměrovány útočníky, což zvyšuje riziko útoků na autentizační proces.

Náklady na implementaci a provoz

- Biometrická autentizace: 2 body - Implementační náklady biometrické autentizace mohou být vysoké kvůli pořízení specializovaných zařízení pro sběr biometrických dat a vývoji sofistikovaných algoritmů. Provozní náklady mohou být také významné kvůli údržbě a administraci biometrických systémů.
- Aplikační autentizace (např. generované kódy v mobilní aplikaci): 3 body - Mohou být střední až vysoké kvůli vývoji a implementaci mobilní aplikace. Avšak, provozní náklady jsou obvykle nižší než u biometrické autentizace, protože nevyžaduje fyzická zařízení a jejich údržbu.
- Hardwarové tokeny: 3 body - Náklady hardwarových tokenů jsou obvykle vysoké kvůli pořízení samotných zařízení a jejich distribuci. Provozní náklady mohou být nižší, ale stále zahrnují náklady spojené s údržbou a administrací tokenů.
- SMS ověření: 4 bod - Mohou být relativně nízké, ale provozní náklady jsou obvykle vyšší, protože zahrnují platby operátorům za odesílání SMS zpráv a licence pro použití služeb.

Uživatelská přívětivost

- Biometrická autentizace: 4 body - Může poskytovat vysokou úroveň uživatelské přívětivosti, protože uživatelé nemusí pamatovat nebo zadávat žádné hesla či kódy. Stačí jim pouze fyzická interakce se zařízením pro sběr biometrických dat, což může být považováno za jednodušší a přirozenější.
- Aplikační autentizace (např. generované kódy v mobilní aplikaci): 3 body - Pomocí generovaných kódů v mobilní aplikaci může být velmi uživatelsky přívětivá. Většina uživatelů používá své mobilní zařízení pravidelně, což znamená, že mají snadný přístup k autentizačním kódům. Navíc není potřeba pamatovat si složitá hesla, což může uživatelům zjednodušit proces přihlašování. Nicméně případné přeskakování mezi aplikacemi při přihlašování může být nepříjemné jako při SMS ověření.
- Hardwarové tokeny: 2 body - Přívětivost hardwarových tokenů může být střední. I když tyto tokeny poskytují jednorázové kódy, které mohou být snadno použity, uživatelé musí mít fyzický token u sebe, což může být nevýhoda, pokud je ztratí nebo zapomenou.
- SMS ověření: 3 body - Přívětivost SMS ověření může být průměrná. Přestože většina uživatelů má přístup k mobilním telefonům, proces ověření pomocí SMS může být vnímán jako zdlouhavý nebo obtěžující, zejména pokud není možné přijmout SMS okamžitě nebo pokud je nutné opakovaně zadávat kódy.

Flexibilita a kompatibilita

- Biometrická autentizace: 2 body - Může být omezená flexibilitou v různých situacích, například ve špatných světelných podmínkách nebo při změně biometrických charakteristik uživatele. Kompatibilita může také být omezená v závislosti na podporovaných zařízeních a platformách.
- Aplikační autentizace (např. generované kódy v mobilní aplikaci): 3 body - Obvykle nabízí dobrou flexibilitu a kompatibilitu, protože mobilní aplikace mohou být snadno aktualizovány a upravovány podle potřeb uživatele. Mohou být použity na široké škále mobilních zařízení a platforem.
- Hardwarové tokeny: 2 body - Mohou být méně flexibilní a kompatibilní, protože jsou obvykle vázané na konkrétní fyzické zařízení a mohou mít omezenou podporu na různých platformách.

- SMS ověření: 5 bodů – Mobilní telefon nosí u sebe prakticky každý a bez ohledu na chytrost zařízení lze využít SMS ověření téměř kdekoliv.

Dostupnost a spolehlivost

- Biometrická autentizace: 2 body - Může být spolehlivá pokud jsou použity spolehlivé biometrické senzory a algoritmy. Nicméně, může být ovlivněna různými faktory, jako je kvalita snímání biometrických dat nebo fyzický stav uživatele. Také může být problémem dostupnost zařízení pro sběr biometrických dat v určitých situacích (např. otisky prstů mohou být nečitelné na znečištěných nebo vlhkých površích).
- Aplikační autentizace (např. generované kódy v mobilní aplikaci): 3 body - Aplikační autentizace může být velmi spolehlivá a dostupná, pokud je správně navržena a implementována. Generování kódů v mobilní aplikaci je obvykle rychlé a spolehlivé, pokud je uživatel připojen k síti a má přístup k mobilní aplikaci. Nicméně, může být omezena v situacích, kdy uživatel nemá přístup k internetu nebo má problémy se zařízením.
- Hardwarové tokeny: 4 body - Hardwarové tokeny obvykle poskytují vysokou úroveň spolehlivosti a dostupnosti, protože jsou nezávislé na internetovém připojení a nemusejí být náchylné k výpadkům služeb. Uživatelé mohou používat tokeny k autentizaci bez ohledu na dostupnost internetu nebo jiných zařízení.
- SMS ověření: 5 bodů - Může být spolehlivé většinu času, pokud je uživatel připojen k mobilní síti, což je v téhle době dost pravděpodobné.

Následně bylo určené pořadí a stanovení vah kritérií:

Tabulka 2 - Stanovení vah kritérií

Stanovení vah kritérií						
	Pořadí		**váha (preference)**		**Body**	**váha (preference)**
Bezpečnost (B)	1.	5	0,31		10	0,33
Náklady na implementaci a provoz (N)	3.	3	0,19		5	0,17
Uživatelská přívětivost (U)	3.	3	0,19		5	0,17
Flexibilita a kompatibilita (F)	5.	1	0,06		2	0,07
Dostupnost a spolehlivost (D)	2.	4	0,25		8	0,27
	Součet	16	1		30	1

Zdroj: vlastní zpracování

Nejvíce důležitým faktorem pro banky je bezpečí pro své zákazníky, tudíž je právě bezpečnost na prvním místě a je k ní tedy přidělená nejvyšší váha. Na druhou stranu nejméně důležitým z nabídky je flexibilita a kompatibilita.

Tabulka 3 - Výpočet nejlepší varianty podle předem vypočtených vah

Matice bodování variant dle kritérií										
	Bezpečnost (B)	**Náklady na implementaci a provoz (N)**	**Uživatelská přívětivost (U)**	**Flexibilita a kompatibilita (F)**	**Dostupnost a spolehlivost (D)**		Bodovací metoda		Bodovací metoda s vahami	
Biometrická autentizace	5	2	5	3	2		17		3,89	1.
Aplikační autentizace (např. generované kódy v mobilní aplikaci)	4	4	4	4	3		19		3,77	2.
Hardwarové tokeny	4	4	2	3	4		17		3,76	3.
SMS ověření	2	5	4	5	5		21		3,35	4.
Charakter kriteria	max	max	max	max	max					
	0,51	0,11	0,10	0,04	0,23					

Zdroj: vlastní zpracování

Po výpočtu bodovací metody s váhami vyšlo, že nejlepší variantou autentizace je biometrická, i přesto, že například není výhodná, co se týče nákladů na implementaci a její provoz, neboť bezpečnost je pro banky hlavním faktorem. Nejen pro banky je bezpečnost hlavním faktorem, ale i pro zákazníky, kteří jsou si toho jistě vědomi.

5 Výsledky a diskuse

Výsledky analýzy naznačují, že většina respondentů projevuje vysokou spokojenost s vícefaktorovou autentizací (MFA) v oblasti bankovnictví. Tato pozitivní odezva je patrná jak z hlediska vnímané bezpečnosti, tak z pohledu uživatelského pohodlí.

Klíčovým aspektem, který ovlivňuje spokojenost respondentů, je vnímání bezpečnosti poskytované vícefaktorovou autentizací. Většina zúčastněných považuje tuto metodu za bezpečnější než tradiční přístup založený pouze na uživatelském jménu a heslu. Kombinace biometrických údajů, SMS kódu a dalších ověřovacích metod vytváří robustní bezpečnostní vrstvu, což vede k důvěře respondentů v ochranu svých finančních údajů.

Dále je zřetelný význam pohodlí při používání vícefaktorové autentizace. Mnoho respondentů vyjadřuje pozitivní názor na snadnost a rychlost, s jakou mohou ověřit svou identitu prostřednictvím biometrických údajů nebo SMS kódu. Tato uživatelská přívětivost je klíčovým faktorem pro širokou akceptaci MFA, zejména v době, kdy lidé očekávají efektivitu a rychlost v digitálních interakcích.
Přestože v některých případech může být zaznamenána mírná variabilita v názorech na pohodlí, obecně lze říci, že většina respondentů vnímá vícefaktorovou autentizaci jako pohodlný způsob zabezpečení svých bankovních účtů. Tato pozitivní zkušenost je podporována i tím, že většina respondentů uvádí, že bývají občas vyzváni k provedení vícefaktorové autentizace při přihlašování do svých účtů, což svědčí o běžném využívání této metody.

Lze konstatovat, že výsledky této analýzy naznačují, že vícefaktorová autentizace v oblasti bankovnictví získává širokou akceptaci a podporu mezi uživateli. Její schopnost kombinovat vysokou úroveň bezpečnosti s uživatelským pohodlím představuje klíčový prvek pro pozitivní přijetí a očekávání, že se tato bezpečnostní metoda stane běžným standardem v digitálním bankovnictví v budoucnosti.

Výsledky vícekriteriální analýzy jasně ukazují, že biometrická autentizace vychází jako preferovaná volba pro bankovní sektor, který klade nejvyšší důraz na bezpečnost. Tato analýza byla založena na vážení různých kritérií, která jsou klíčová pro banky při posuzování autentizačních metod.
Biometrická autentizace exceluje v této oblasti díky své schopnosti využít unikátní biometrické charakteristiky jednotlivce, jako jsou otisky prstů, rozpoznávání obličeje nebo hlasu. Tyto charakteristiky poskytují vysokou úroveň bezpečnosti, kterou banky vyžadují k ochraně citlivých bankovních dat a transakcí.
Další kritéria, jako je uživatelská přívětivost, náklady na implementaci a rychlost autentizace, byla také zohledněna, avšak jejich váha byla v analýze přizpůsobena dle požadavků na

bezpečnost. Zatímco biometrická autentizace může vyžadovat určité investice do infrastruktury a technologie, výhody v podobě vysoké úrovně bezpečnosti a pozitivní uživatelské zkušenosti zcela převážily nad těmito aspekty.

V rámci zkoumání výsledků dotazníku o vícefaktorové autentizaci v oblasti bankovnictví vyvstává několik aspektů, které mohou být předmětem diskuse. I přesto, že většina respondentů projevila pozitivní postoj k této bezpečnostní metodě, existují otázky, které by mohly být předmětem polemiky.

1. Nerovnováha ve věkovém rozpětí

Dominance mladší generace ve věkovém rozpětí 18-24 let vytváří obraz digitálního bankovnictví, který může být zkreslen. Mladší respondenti jsou pravděpodobně více otevření inovacím a technologiím, což může ovlivnit pozitivní vnímání vícefaktorové autentizace. Zde by se mohlo zaměřit na to, zda jsou výsledky reprezentativní pro celou populaci uživatelů bankovních služeb, zejména starší věkové skupiny.

Nicméně orientace na mladou generaci je velmi důležitá, a proto je možná právě tato cílová skupina ta, o kterou bychom se měli zajímat a případně vylepšovat nedostatky.

Že je tato skupina velmi důležitá si uvědomila i Air Bank, která začala cílit na mladé.

2. Genderová disproporce

Převažující počet mužských respondentů (72.2 %) v porovnání s ženskými respondentkami (27.8 %) ukazuje na určitou nerovnováhu a mohla by se nabídnout otázka, jak velký dopad na výsledek bude mít převaha odpovědí od mužů.

3. Očekávání od budoucnosti

I když většina respondentů očekává, že vícefaktorová autentizace bude standardem pro všechny online služby, může se vznést otázka, zda tato očekávání odpovídají realitě. Polemika by mohla zkoumat, zda jsou tato očekávání nadnesená a jaký bude skutečný rozsah implementace této bezpečnostní metody napříč různými odvětvími.

Je možné, že zabezpečení se bude v průběhu let měnit, aby reagovalo na budoucí aktuální hrozby. Například umělá inteligence může v budoucnu být na obou stranách zabezpečení, ať

už na té, která bude přispívat ke kontrole zabezpečení, nebo na té, která bude prolamovat již zavedená kritéria. Tím pádem nedokážeme s jistotou říct, zda bude MFA v budoucnosti standardem pro všechny online služby, nebo jsme dosáhli maximální úrovně.

4. Variabilita v používaných metodách

Přestože většina uvádí používání biometrických údajů, variabilita v používaných metodách (SMS kód, aplikace pro ověření) může naznačovat, že neexistuje jednotný standard. Polemika by se mohla zaměřit na to, zda různorodost používaných metod může způsobit komplikace v širším kontextu bezpečnosti.

Bezpečnost právě SMS kódu řeší i Bc. Pavel Břoušek ve své práci, kde z jeho slov můžeme vyčíst, že i přesto, jak je tato metoda velmi používaná, není natolik bezpečná. „*They are commonly used for 2FA and step-up authentication by large organizations including banks, although they face a number of security issues, and their use has been discouraged by NIST since 2017.“*

Nejen o těchto bodech lze vést diskuzi a rozvézt dané téma.

6 Závěr

Získané výsledky analýzy dotazníku poskytly vhled do postojů a preferencí respondentů ohledně vícefaktorové autentizace v rámci digitálního bankovnictví. Tato studie reflektuje širokou škálu pohledů, od očekávání budoucího vývoje po současnou spokojenost s existujícími bezpečnostními opatřeními.

V první řadě lze pozorovat dominanci mladší generace ve věku 18-24 let, která tvoří významnou většinu respondentů. Tato skupina prokazuje vysoký zájem o digitální bankovnictví, což naznačuje rostoucí trend směrem k moderním finančním technologiím. Přesto je důležité si být vědomi potřeby zvýšit genderovou rovnost v digitálním bankovnictví, neboť muži v této studii převažují.
Frekvence používání internetového bankovnictví odráží silnou angažovanost respondentů, kteří tuto službu využívají pravidelně. Tento trend naznačuje, že digitální nástroje pro správu financí jsou již pevnou součástí každodenního života.
Znalost a používání vícefaktorové autentizace jsou významnými prvky, které ukazují na povědomí respondentů o bezpečnostních opatřeních v digitálním bankovnictví.

Vnímání budoucnosti vícefaktorové autentizace je pozitivní, přičemž většina respondentů očekává, že se stane standardem pro všechny online služby. To podtrhuje rostoucí důvěru ve schopnost této metody chránit citlivé finanční údaje, a proto je. vícefaktorová autentizace vnímána jako pohodlný a bezpečný způsob přihlašování, což podporuje aktuální trend v oblasti finančních technologií.

Biometrické údaje jsou u respondentů preferovanou metodou, což svědčí o důvěře ve vysokou úroveň bezpečnosti, kterou tato autentizace poskytuje.
Vzhledem k tomu, že je bezpečnost důležitá nejen pro koncové uživatele, ale i pro banky, dospěli jsme k závěru, že autentizace biometrická se jeví jako nejlepší možnost pro bankovní sektor v kontextu zajištění vysoké úrovně bezpečnosti. Vícekriteriální analýza nám umožnila pečlivě zhodnotit různé typy autentizačních metod a jejich klíčové charakteristiky vzhledem k potřebám bank a bezpečnostním požadavkům.

Je založena na unikátních biometrických charakteristikách jednotlivce, jako jsou otisky prstů, rozpoznávání obličeje nebo hlasu, což poskytuje vysokou úroveň bezpečnosti a obtížně

napodobitelný identifikační faktor. Tato metoda také nabízí pohodlí a rychlost pro uživatele, což přispívá k celkové pozitivní uživatelské zkušenosti.

Vzhledem k neustále se zvyšujícím počtům kybernetických hrozeb a technologickým pokrokům je klíčové, aby banky využívaly autentizační metody, které poskytují nejvyšší možnou úroveň ochrany pro své klienty. Biometrická autentizace se ukázala jako efektivní nástroj pro prevenci podvodů a zajištění integrity bankovních dat a transakcí.

Lze tedy říct, že vícefaktorová autentizace, a převážně biometrická autentizace, hraje klíčovou roli v posilování bezpečnosti a důvěry v digitálním bankovnictví. S neustálým technologickým pokrokem a rostoucí digitalizací společnosti je zřejmé, že vícefaktorová autentizace bude hrát stále významnější roli v budoucnosti online bezpečnosti. Je nezbytné sledovat tyto trendy a přizpůsobovat bezpečnostní opatření tak, aby odpovídala dynamickému charakteru digitálního bankovnictví.

7 Seznam použitých zdrojů

AirBank. In: AirBank [online]. 2023. Dostupné z: https://www.airbank.cz/novinky/air-bank-predstavuje-novou-tvar-pro-komunikaci-s-generaci-z-v-online-spotech-se-objevi-popularni-moderator-a-sportovec-nikolaos-mach/

ANDRESS, Jason. The Basics of Information Security. 2nd Edition. Syngress, 2014. ISBN 9780128008126

BEDELL, Crystal a Michael THELANDER. In: Multi-Factor Authentication. 111 River Street, Hoboken,: John Wiley, 2018, s. 53. ISBN 978-1-119-45602-5.

České noviny. In: České noviny [online]. 2019. Dostupné z: https://www.ceskenoviny.cz/zpravy/1797371?_zn=aWQlM0Q0NDA3NTk1NzM3MzY3MTE1MTA2JTdDdCUzRDE3MTA0OTg4MzkuMDEwJTdDdGUlM0QxNzEwNDk4ODM5LjAxMCU3Q2MlM0RBNEIzNkQ5MzZDQUM0NjUwNEEyQjkyQ0RBRDUyODREQg%3D%3D

ČSOB [online]. Czech Republic: ČSOB,. Dostupné z: https://www.csob.cz/portal/documents/10710/25109/nejcastejsi-dotazy-platebni-karty.pdf

EasyTechJunkie. EasyTechJunkie [online]. San Francisco, CA, 2023. Dostupné z: https://www.easytechjunkie.com/what-is-a-software-token.htm

Forbes [online]. California: Forbes, 2023. Dostupné z: https://www.forbes.com/advisor/credit-cards/contactless-credit-cards/

GOV [online]GOV.UK, 2020. Dostupné z: https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services/giving-users-access-to-online-services

KAGAN, JULIA. Investopedia. Investopedia [online]. New York: Investopedia, April 26, 2023. Dostupné z: https://www.investopedia.com/terms/p/personal-identification-number.asp

KOHOUT Roman a Radek KARCHŇÁK. Bezpečnost v online prostředí [online]. Biblio Karlovy Vary z. s, 2016. ISBN 978-80-260-9543-9. Dostupné z: https://www.internetembezpecne.cz/wp-content/uploads/2017/03/Roman-Kohout-Bezpecnost-v-online-prostredi.pdf

OKPAMEN, Peter. In: Security of Information Systems in Organization: A Bank Model [online]. Mediterranean Journal of Social Sciences, 2013. ISBN ISSN 2039-2117. Dostupné z: https://www.researchgate.net/publication/271105062_Security_of_Information_Systems_in_Organization_A_Bank_Model

Kružíková, User Testing of Mobile Banking Authentication Methods [online]. Czech Republic: Faculty of Informatics Masaryk university, Brno, 2020. Dostupné z: https://irtis.muni.cz/media/3221965/usertesting_tacrreport_2020r.pdf

MATYÁŠ, Vašek, Jan KRHOVJÁK a kolektiv. Autorizace elektronických transakcí a autentizace dat i uživatelů. Masarykova univerzita, 2008. ISBN 978-80-210-4556-9.

Muni. In: BŘOUŠEK, Pavel. Muni [online]. 2019. Dostupné z: https://is.muni.cz/th/fah34/Multi_Factor_Authentication_in_Large_Scale_final-digital.pdf

Protectimus. Protectimus [online]. Dublin, 2015. Dostupné z: https://www.protectimus.com/blog/hardware-or-software-token-which-one-to-choose/

Vícekriteriální metody hodnocení. In: SOUKOPOVÁ, Jana. MUNI [online]. 2013. Dostupné z: https://is.muni.cz/el/econ/jaro2013/MKV_VZVP/um/33149329/Studijni_text_metody_vicekriterialniho_rozhodovani.pdf

7.1 Seznam obrázků

Apple. Apple [online]. Califronia: Apple, 2023 Dostupné z: https://support.apple.com/en-us/HT208109

CyberHoot. CyberHoot [online]. Portsmouth: CyberHoot, 2020. Dostupné z: https://cyberhoot.com/cybrary/two-factor-authentication/

ČS. Česká spořitelna [online]. Praha: Česká spořitelna, 2021. Dostupné z: https://www.csas.cz/cs/blog/dobre-vedet/nelze-ji-ukrast-ani-zneuzit-virtualni-george-karta-dokonale-chrani-vase-penize

Eset [online]. In: 2022. Dostupné z: https://digitalsecurityguide.eset.com/cz/proc-jsou-sifrovani-a-mfa-nezbytne-pro-vasi-firmu

Generaliceskaprofi. In: Generaliceskaprofi [online]. 2023. Dostupné z: https://www.generaliceskaprofi.cz/ze-zivota/kyberneticka-hrozba-umele-inteligence

Hive systems. In: Hivesystems [online]. Richmond, Virginia: 2023. Dostupné z: https://www.hivesystems.io/blog/are-your-passwords-in-the-green

Janco Associates, Inc. In: E-janco [online]. USA: Janco Associates, 2021. Dostupné z: https://e-janco.com/articles/2021/2021-04-17-worst-passwords-historic.html

KSEC Tagbase. KSEC Tagbase [online]. UK: KSEC Tagbase, 2022. Dostupné z: https://tagbase.ksec.co.uk/about/smart-cards/

Protectimus. Protectimus [online]. Protectimus, 2020. Dostupné z: https://protectimus.medium.com/hardware-tokens-for-azure-mfa-b71c51ad19d2

Rublon. Rublon [online]. Poland: Rublon Authors, 2021. Dostupné z: https://rublon.com/blog/what-are-the-three-authentication-factors/

7.2 Přílohy

Rozšířený výpočet vícekriteriální analýzy