UNIVERZITA PARDUBICE

EKONOMICKO-SPRÁVNÍ FAKULTA

BAKALÁŘSKÁ PRÁCE

2023 KAROLÍNA NĚMCOVÁ HROMÁDKOVÁ

Univerzita Pardubice

Ekonomicko-správní fakulta

Testování použitelnosti a bezpečnosti webu

Karolína Němcová Hromádková

Bakalářská práce

2023

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2022/2023

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Karolína Němcová Hromádková**
Osobní číslo:	**E20588**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Testování použitelnosti a bezpečnosti webu**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je navrhnout řešení zjištěných nedostatků použitelnosti a bezpečnosti vybraného webu na základě výsledků jeho testování.

Osnova:

0. Popis vzájemného vztahu použitelnosti a bezpečnosti webů.
1. Popis metod testování a hodnocení použitelnosti a bezpečnosti webů.
2. Otestování vybraného webu.
3. Formulovace nedostatků vybraného webu z hlediska jeho použitelnosti a bezpečnosti.
4. Navržení řešení zjištěných nedostatků.

Rozsah pracovní zprávy: **Cca 35 stran.**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

DUMAS, J. S., REDISH, J. C. *A Practical Guide to Usability testing*. Exeter, England: Intellect Books, 1999. ISBN: 1-84150-020-8.
KRUG, S. *Web design: nenuťte uživatele přemýšlet!*. Brno: Computer Press, 2003. ISBN 80---7226-892-9.
RUBIN, J., CHISNELL, D. *Handbook of usability testing: how to plan, design, and conduct effective tests*. 2nd ed. Indianapolis: Wiley Pub., c2008. ISBN 978-0-470-18548-3.
SELECKÝ, M. *Penetrační testy a exploitace*. Brno: Computer Press, 2012. ISBN 978-80-251--3752-9.

Vedoucí bakalářské práce: **doc. Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2022**
Termín odevzdání bakalářské práce: **30. června 2023**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2022

Prohlašuji:

Práci s názvem Testování použitelnosti a bezpečnosti webu jsem vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 27.2.2023

Karolína Němcová Hromádková v. r.

ABSTRAKT

Tato bakalářská práce se zabývá testováním a hodnocením použitelnosti části webu Univerzity Pardubice a jeho bezpečností. Jsou zde popsány hlavní metody testování použitelnosti a bezpečnosti, souvislost mezi použitelností a bezpečností. Pomocí definovaných metod je realizováno testování použitelnosti multifaktorové autentizace. V závěru práce je uveden seznam doporučení, jak eliminovat nedostatky nalezené při testování.

KLÍČOVÁ SLOVA

autentizace, bezpečnost, MFA, QA, použitelnost, testování, testování webu

TITLE

Website usability and security testing

ABSTRACT

This Bachelor´s thesis deals with the testing and evaluation of the usability of part of the website of the University of Pardubice and security. There are main usability and security testing methods, the connection between usability and security described. Using defined methods, usability testing of multifactor authentication is carried out. At the end of the thesis, there is a list of recommendations that were discovered during testing.

KEY WORDS

Authentication, security, MFA, QA, useability, testing, web testing

Obsah

Seznam obrázků 7

Seznam tabulek 8

Seznam použitých zkratek 9

Úvod 10

1 Autentizace 11

1.1 Autentizace a její proces 11

1.2 Způsoby autentizace 12

1.2.1 PIN 12

1.2.2 Hesla 12

1.2.3 Tokeny 14

1.2.4 SMS 16

1.2.5 Biometrika 17

1.3 Multifaktorová autentizace 18

1.3.1 Rozdíl mezi jednofaktorovou, dvoufaktorovou a multifaktorovou autentizací 18

1.3.2 Multifaktorová autentizace 18

2 Testování informačního systému 19

2.1 Vymezení pojmů 19

2.2 Techniky testování informačního systému 20

3 Testování použitelnosti informačního systému 21

3.1 Použitelnost 21

3.2 Metody testování použitelnosti 21

3.3 Vhodný počet hodnotitelů pro testy použitelnosti 22

4 Vztah mezi použitelností a bezpečností 23

5 Testování multifaktorové autentizace na UPa 25

5.1 Základní informace o webu a intranetu UPa a situace před zavedením MFA 25

5.2 Výběr metody testování použitelnosti 26

5.3 Stanovení postupu testování použitelnosti a bezpečnosti MFA na UPa 27
5.4 Testování použitelnosti vyhledávání a článků o MFA na webech UPa 28
5.4.1 Analýza použitelnosti hlavního webu Univerzity Pardubice 28
5.4.2 Analýza použitelnosti studentského intranetu Univerzity Pardubice 29
5.5 Multifaktorová autentizace pro studenty Univerzity Pardubice 33
5.5.1 Vytvoření dotazníku 33
5.5.2 Vyhodnocení dotazníku 35
5.6 Testování a hodnocení použitelnosti manuálu pro nastavení MFA 45
5.6.1 Testování manuálu 45
5.6.2 Hodnocení manuálu 46
5.7 Testování nastavení multifaktorové autentizace 47
5.7.1 Výběr testovacího vzorku koncových uživatelů 47
5.7.2 Testovací úkoly 48
5.7.3 Průběh a hodnocení testovacích úkolů 49
5.7.4 Nalezené nedostatky 53
5.8 Seznam doporučení na základě testování 54
Závěr 58
Seznam použité literatury 59
Seznam příloh 62

Seznam obrázků

Obrázek 1 Příklad výstupu Yubikey, kdy bylo tlačítko autentizace zmáčknuto 3x 15
Obrázek 2 Princip spárování softwarových tokenů s autentizačním serverem přes QR kód ...16
Obrázek 3 Multifaktorová autentizace.....19
Obrázek 4 Vztah mezi počtem hodnotitelů a procentem odhalených problémů 22
Obrázek 5 Vztah mezi použitelností, bezpečností a cenou.....23
Obrázek 6 Výsledek vyhledávání pro slovo autentizace na www.upce.cz.....28
Obrázek 7 Úvodní stránka studentského intranetu 29
Obrázek 8 Zobrazení sekce "Důležité na domovské stránce intranetu 30
Obrázek 9 Postup k zobrazení článku Multifaktorová autentizace.....31
Obrázek 10 Příklad výsledků vyhledávání pro slovo autentizace 32
Obrázek 11 Diagram návaznosti otázek 34
Obrázek 12 Hodnocení otázky 12.....35
Obrázek 13 Hodnocení otázky 13.....36
Obrázek 14 Hodnocení otázky 14.....36
Obrázek 15 Hodnocení otázky 15.....37
Obrázek 16 Hodnocení otázky 7.....40
Obrázek 17 Hodnocení otázky 3.....41
Obrázek 18 Hodnocení otázky 4.....41
Obrázek 19 Hodnocení otázky 10.....42
Obrázek 20 Hodnocení otázky 5.....43
Obrázek 21 Hodnocení otázky 6.....43
Obrázek 22 Hodnocení otázky 11.....45
Obrázek 23 Výstřižek z návodu – autentizační metody 46
Obrázek 24 Autentizační metody na adrese https://mojeheslo.upce.cz/.....47

Seznam tabulek

Tabulka 1 Odpovědi studentů na otázku 1.....38
Tabulka 2 Odpovědi na otázku 2.....39
Tabulka 3 Odpovědi studentů na otázku 8.....44
Tabulka 4 Odpovědi studentů na otázku 9.....44
Tabulka 5 Testovací vzorek účastníků.....48
Tabulka 6 Splnění testovacích úkolů účastníky.....49
Tabulka 7 Seznam nalezených nedostatků a jejich návrh na úpravu.....54

Seznam použitých zkratek

1FA	jednofázová autentizace
2FA	dvoufázová autentizace
AJ	anglický jazyk
CITS	Centrum informačních a technických služeb
ČJ	český jazyk
HW	hardware, hardwarový
IT	informační technologie
MFA	multifaktorová autentizace
OTP	one-time password (jednorázové heslo závislé na času)
QA	Quality Assurance
QR	Quick Response, rychlá odpověď
RSA	Rives-Shamir-Adleman; veřejný klíč kryptosystému
SW	software, softwarový
TOTP	time-based one-time password (jednorázové heslo závislé na času)
UI	uživatelské rozhraní
UPa	Univerzita Pardubice
URL	Uniform Resource Locator
VPN	Virtual Private Network

Úvod

Dnešní dobu je možné definovat jako dobu digitální, počítačovou. To znamená, že v našem životě hrají velkou roli právě počítače, chytré mobilní telefony, tablety a jiné zařízení. A právě při vývoji aplikací ať už desktopových nebo webových je nutné, aby byl kladen důraz nejen na jejich fungování, ale především na použitelnost softwaru a přidružených aplikací, protože téměř všechny generace používají právě počítače a již chytré telefony aj., avšak ne všichni umějí se složitými a neintuitivními softwary a aplikacemi pracovat. Proto je důležité, aby všechny aplikace byly co nejvíce srozumitelné a dobře se s nimi pracovalo. V současnosti musí mít každý alespoň základní uživatelskou znalost, protože to doba vyžaduje. Např. v době lockdownů si většina obyvatelstva objednávala nákup právě přes internet, téměř všechna komunikace ať už se zaměstnavateli nebo veřejnou správou se přesouvá do virtuálního světa. Také bezpečnost na internetu je v současné době velkým tématem, kterým je dobré se zabývat, protože zkušení hackeři dokážou ne jednoho uživatele obelstít a ukrást mu identitu např. na sociálních sítích.

Tato bakalářská práce se zabývá testováním použitelnosti a bezpečnosti webu. Především se zabývá informačními systémy www.upce.cz a https://student.upce.cz a také multifaktorovou autentizací z pohledu studentů a to, jak snadné je v systémech snadné najít návod k nastavení multifaktorovému ověřování nebo to, jak použitelný návod k nastavení MFA je a zda to studenti zvládnou podle něj. Také se provede analýza návodu, uživatelské testování nastavení MFA na pěti studentech Univerzity Pardubice, studenti vyjádří svůj názor na multifaktorovou autentizaci. V neposlední řadě se na základě zjištěných informací vytvoří seznam doporučení, jak se vyvarovat nalezeným nedostatkům.

Cílem práce je navrhnout řešení zjištěných nedostatků použitelnosti a bezpečnosti vybraného webu na základě výsledků jeho testování.

1 Autentizace

1.1 Autentizace a její proces

Autentizací podle [3] se myslí proces ověření identity subjektu splňující požadovanou míru záruky (§ 2 písm. g). Identita subjektu je definována jako zjištění jeho identity v informačním systému [3].

Autentizace je proces prokázání, že jste tím, za koho říkáte, že jste. Toho se dosahuje ověřením identity osoby nebo zařízení. Někdy se zkracuje na AuthN. [9]

Autorizace je udělení oprávnění k nějaké akci ověřené straně. Určuje, k jakým datům máte povolený přístup a co s daty můžete dělat. Autorizace se někdy zkracuje na AuthZ. [9]

Na základě **typu použitých identifikačních znaků** rozlišujeme [4]

1. *znalostní autentizaci*:
    - využívá konkrétní znalost, kterou má daný subjekt, ale kterou by neměl disponovat žádný jiný,
    - nejčastěji to jsou hesla pro přístup např. do e-mailové schránky, k mobilnímu telefonu apod., dále pak PINy, jednorázová hesla, kontrolní otázky, grafická hesla,
2. *autentizaci prostřednictvím autentizačního předmětu:*
    - subjekt, který chce ověřit svou identitu vlastní jedinečný předmět, který by neměl vlastní žádný jiný subjekt, než jedině a pouze ten, který je oprávněn tento předmět mít,
    - předměty vhodné pro autentizaci mohou být typu
        - předměty pouze s pamětí – paměť obsahuje konkrétní identifikační řetězec,
        - předměty udržující hesla – po zadání uživatelského hesla vydají určený kvalitní klíč,
        - předměty s logikou – zpracovávají jednoduché podněty jako např. vydej následující klíč,
        - tzv. chytré předměty – mohou generovat náhodná čísla, šifrovat apod.,
3. *biometrickou autentizaci*:
    - využívá charakteristik lidského těla, které má každý člověk vždy s sebou, tudíž je není možné zapomenout, ztratit nebo půjčit,
4. *multifaktorovou autentizaci*

Proces autentizace se podle [8] rozděluje na dvě fáze, a to:

5. *registrace:* uložení etalonu do databáze,
6. *identifikace:* předložení identity uživatele neboli zadání svého ID čísla nejčastěji,
7. *verifikace:* ověření, že uživatel je má přidělené ID, které zadal v předchozím kroku.

Kroku č. 1 předchází krok č. 0 *registrace*, což je uložení identifikačních znaků (tzv. etalonu) subjektu/uživatele do databáze systému, který vyžaduje autentizaci [12]. Pak proces autentizace probíhá takto: jakmile subjekt přistoupí k systému, aby se do něj přihlásil, musí nejprve do formuláře pro přihlášení vyplnit své ID, které se porovná s databází, kam se uložily uživatelovy identifikační znaky, které zadal při registraci. Následně se tedy ověří, zda má uživatel přidělené právě to ID, které zadal, například heslem uložené v databázi [8].

1.2 Způsoby autentizace

1.2.1 PIN

PINy jsou krátká hesla složená z čísel. Obvykle je zadáváme při vstupu do budov, v bankovnictví, při používání mobilního telefonu aj. Běžný PIN má čtyři až šest čísel. Protože jsou PINy tak krátké, tak politika uzamčení je zde velice přísná, proto se stává, že po zadání třech špatných pokusech se buď znehodnotí samotný PIN, nebo se zařízení uzamkne a musí se počkat několik sekund až minut, než zařízení povolí další pokus. Výhodou PINů je, že jsou krátké a lehce zapamatovatelné, avšak na druhou stranu jsou jednoduše prolomitelné a uhodnutelné. Další nevýhodou je i to že, většinou neexpirují, a tudíž se používají dlouho [1].

1.2.2 Hesla

Heslo je nějaký kód, používaný pro ověření uživatele, který chce vstoupit do nějakého systému. Pod tento termín spadají všechny typy hesel, od jednorázových hesel přes kontrolní otázky ke grafickým heslům.

Základním kritériem hesla je jeho bezpečnost. Každý systém má však vlastní požadavky na hesla. [11] Avšak existují obecné zásady pro bezpečnost hesel. Taková, že hesla musí být:

1. tajná,
2. unikátní,
3. těžko uhodnutelná,
4. dostatečně dlouhá,
5. složená z různých znaků.

Podle [12] při vytváření hesel používáme jednoduchá pravidla. To ale nezvyšuje bezpečnost, protože je útočníci znají. K takovým pravidlům patří např.:

- necháme si nějaké defaultní heslo (admin, test, guest),
- použijeme některé běžné slovo ze slovníků a něco k němu přidáme,
- spojíme dvě či tři krátká slova (a většinou je zapíšeme malými písmeny, nebo první písmeno každého slova napíšeme velkým písmenem),
- pokud už použijeme velké písmeno, je nejspíš na začátku hesla,
- pokud v hesle použijeme číslo, bude nejspíš přidané na konci, bude dlouhé 1–4 číslice (a dost často to bude nějaký rok),
- stejně tak speciálním znakem je často vykřičník či otazník přilepený na konci,
- případně používáme tzv. *leetspeak*, nahrazování podobně vypadajícími znaky (o → 0, i → 1, z → 2, e → 3, a → 4, a → @),
- tzv. procházka po klávesnici (například qwert, asdfg),
- heslo zapíšeme pozadu (aksuraM),
- slovo zdvojíme (kacerkacer),
- často také v hesle používáme název dané služby (seznam).

Vysokou důležitost by měl uživatel věnovat tomu, jak svá hesla uchovává. Není vhodné hesla ukládat na jednoduše přístupných místech jako například PIN s platební kartou. V případě zapomenutí hesla je nejvhodnější v internetovém světě heslo obnovit, a to okamžitě. Stačí k tomu uživatelské jméno tzv. login. Někdy je vyžadována i tzv. kontrolní otázka [11].

Výhody:

- není třeba žádné speciální zařízení pro ověření hesla,
- při dodržování zásad hesel, jsou hesla velmi bezpečná.

Nevýhody:

- daný subjekt tuto znalost může vyzradit jinému, zapomenout,
- uživatelé používají jednoduše prolomitelná, obecná hesla,
- uživatelé hesla píšou a následně je schovají na běžně dostupné místo.

1.2.3 Tokeny

V [10] je slovo token také identifikátor definováno jako obecné označení pro objekt, který autentizuje svého nositele. Nejznámější jsou identifikační karty, které musí být nepadělatelné a jedinečné [10]. Postupem času se vyvinuly dva typy tokenů, a to:

1. hardwarové,
2. softwarové.

Hardwarové tokeny

Hardwarové (HW) tokeny jsou malé elektronické zařízení, které je možné si připnout na klíče, sloužící pro autentizování do informačních systémů [6]. Dle [5] je nejčastěji používaným typem RSA token. Ten pro generování kódu využívá čas, tzn. že na tokenu se zobrazuje číselný kód, který se např. po každé minutě mění. Přejděme tedy k principu jeho fungování.

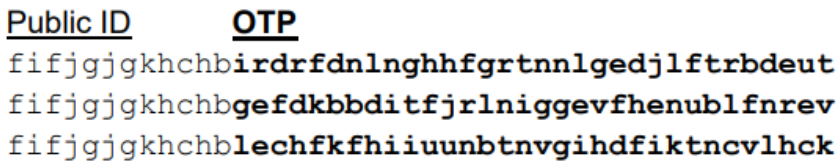
Algoritmus HW tokenu [5]:

1. každý token je unikátně identifikován,
2. autentizační server má tento token přiřazen k uživateli,
3. token generuje přístupový kód dle definovaného algoritmu (na základě času či sekvenční metodou),
4. server zaslaný kód porovná na své straně s kódem, který si vygeneruje stejným algoritmem,
5. pokud se kódy shodují, je uživatel tímto faktorem ověřen.

Přístupový kód se generuje podle daného algoritmu, a to buď na základě času, nebo sekvenční metody. Příkladem sekvenční metody je Yubikey.

Algoritmus na základě času: Kód pro multifaktorovou autentizaci například v aplikaci Microsoft Authenticator je závislý na času, protože se mění každých 30 sekund. Tedy každou půl minutu je zobrazován jiný autentizační kód [17].

Algoritmus na základě sekvenční metody: Token vydává 44 znakové jednorázové heslo (OTP), z nichž prvních 12 znaků je jedinečný veřejný identifikátor samotného tokenu a zbylé znaky jsou dynamická část OTP (viz obr. 1) [14].



Obrázek 1 Příklad výstupu Yubikey, kdy bylo tlačítko autentizace zmáčknuto 3x

Zdroj: [14]

Výhody HW tokenů [5]:

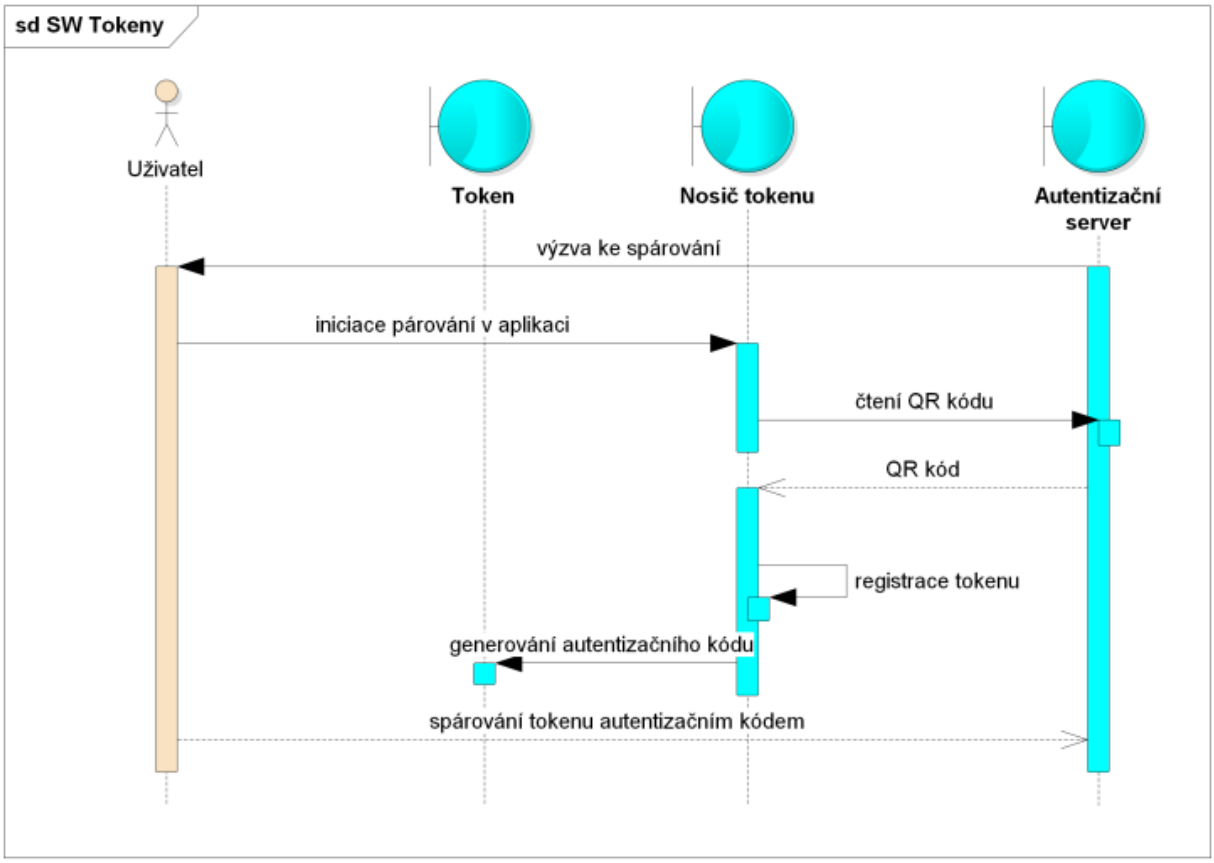
- aby někdo zfalšoval přístup někoho jiného, musí kromě uživatelského jména a hesla získat i fyzický přístup k tokenu.

Nevýhody HW tokenů [5, 12]:

- uživatel musí mít daný fyzický předmět stále u sebe,
- připojuje-li se zařízení k počítači, musí se umět připojit i k chytrým telefonům, tabletům apod.,
- sebere jeden USB slot, kterých se třeba na malých noteboocích obecně nedostává,
- vyšší pořizovací cena zařízení,
- odcizení, nebo ztracení.

Softwarové tokeny

V současné době se více jak HW tokeny využívají spíše softwarové (SW). Ty řeší některé mínusy hardwarových protějšků. Typicky se jedná o aplikaci na smartphonu, která běží na operačních systémech jako je Android, iOS apod. Princip použití je stejný jako u HW tokenů. Rozdíl je pouze v tom, že se software telefonu páruje s autentizačním serverem přes QR kód (viz obr. 1 níže) nebo přihlášením do účtu emailu, který bude propojen s tokenem případně tak, jak umožňuje token. Klasickými příklady SW tokenů jsou Google Authenticator nebo Microsoft Authenticator [5].



Obrázek 2 Princip spárování softwarových tokenů s autentizačním serverem přes QR kód

Zdroj: [5]

Výhody SW tokenů [17]:

- každých např. 30 sekund nový kód ověření,
- nulová pořizovací cena (nebereme-li v úvahu pořizovací cenu chytrého telefonu).

Nevýhody SW tokenů:

- odcizení, nebo ztracení,
- uživatel musí mít daný fyzický předmět stále u sebe.

1.2.4 SMS

Autentizace pomocí SMS je jednou z nejčastějších způsobů, jak potvrdit svou identitu. Tento typ byl vytvořen především kvůli tomu, aby se hesla nekompromitovala.

Ověřování pomocí SMS funguje při dodržení třech kroků [13]:

1. poskytnutí telefonního čísla během registrace např. pro e-mail apod.
2. vložte uživatelské jméno a heslo na webu nebo do aplikace, abyste obdrželi jednorázové ověřovací heslo.
3. opište kód do aplikace nebo na web, abyste dokončili přihlašovací proces.

Výhody: [13]

- v případě, že nepoužíváme moderní alternativy autentizace, jako TOTP, tak SMS je bezpečnější než pouze heslo samotné,
- použití je snadné a rychlé,
- téměř žádné náklady.

Nevýhody: [13]

- je zde nebezpečí zneužití údajů na SIM kartě,
- zařízení lze ztratit nebo ho lze ukradnout.

1.2.5 Biometrika

V současné době jsou zařízení pro rozpoznávání lidských rysů zdokonalována. Jde o zařízení využívajících především takové vlastnosti, které jsou nejvíce používané jsou např. otisky prstů a dlaní, znaky v obličeji nebo ověření hlasu, aj. Takové rysy si každý člověk nosí s sebou, nelze je ztratit nebo být odcizeny. Biometrická zařízení provádí autentizaci na vysoké úrovni a jsou velice spolehlivé mluvíme-li např. o armádě. Snímače těchto typů v mobilních telefonech či počítačích nejsou již tak spolehlivé [10].

Výhody:

- rychlá autentizace,
- není nutná znalost hesel aj nebo přítomnost tokenu,
- v případě hendikepu netřeba textové akce.

Nevýhody:

- charakteristiky člověka jsou stochastické, tedy se mohou v průběhu života měnit,
- kvalitní snímače biometrik jsou drahé, zatímco ty v běžném životě jsou levnější, ale jednoduše prolomitelné.

1.3 Multifaktorová autentizace

1.3.1 Rozdíl mezi jednofaktorovou, dvoufaktorovou a multifaktorovou autentizací

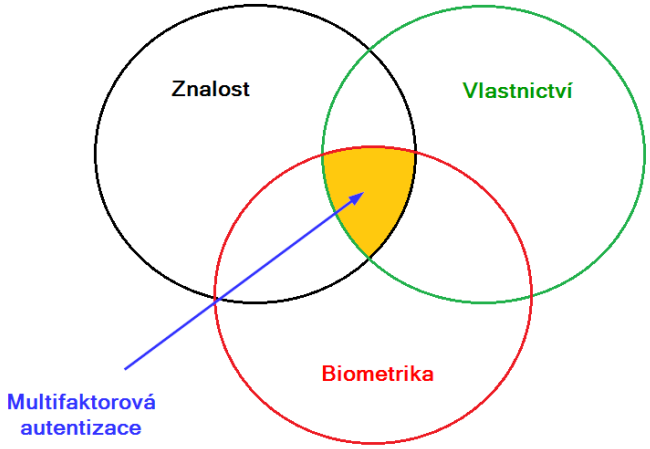
V [8] tvrdí, že jednofaktorová autentizace požaduje pouze jeden faktor ke zjištění, zda bude nebo nebude subjekt autentizován. To je například situace, kdy se přihlašujeme např. do e-shopu zadáním uživatelského jména a hesla. Dvoufaktorové ověřování již vyžaduje dva různé nezávislé faktory potvrzení identity, a to něčím, co ví a něčím, co vlastní. 2FA je podmnožinou MFA. Příkladem může být výběr peněz z bankomatu, kdy důkaz identity je platební karta a znalost PIN kódu karty. Nicméně k použití multifaktorové autentizace je nutné zadat již dva a více nezávislých faktorů, a to tedy co ví, něco, co vlastní a něco co je. Je nutné podotknout, že pouze uživatel, který splňuje tyto požadavky by se měl správně autentizovat, a ne nikdo jiný [1]. Tedy rozdíl mezi 1FA, 2FA a MFA je v počtu a druhu použitých faktorů autentizace.

1.3.2 Multifaktorová autentizace

Do oblasti multifaktorové autentizace patří i dvoufaktorová autentizace. Cílem multifaktorové autentizace je bezpečnější proces ověřování identity uživatele a snížit tak pravděpodobnost kybernetického útoku, a to díky tomu, že kombinuje zabezpečení ve třech autentizačních faktorech:

1. něco známe,
2. něco vlastníme,
3. někým jsme.

Tyto faktory charakterizuje obrázek č. 3. Průnik těchto tří faktorů je multifaktorová autentizace. Výhodou MFA je její bezpečnost, protože aby se útočník dostal k citlivým datům apod., musí disponovat přístupy ke všem zmiňovaným faktorům, které uživatel používá k ověření jeho identity [18].



Obrázek 3 Multifaktorová autentizace

Zdroj: [18]

2 Testování informačního systému

2.1 Vymezení pojmů

Z hlediska testování jsou Quality Assurance (neboli QA) a testování jsou dvě různá slova, která se používají již začátku vývoje jakéhokoliv systému, ale mnohdy jsou používaná v jiných významech, než v jakých dávají opravdu smysl, ale souvisejí spolu.

Testování je to proces, který zahrnuje několik různých aktivit jako plánování, analýzu, design a implementaci testů, reportování výsledků testů apod. Jeho cílem je najít chyby [2].

QA (Quality Assurance) je plánovaná a koordinovaná aktivita, která zasahuje celou organizaci a zahrnuje koncepty jako je politika cíle kvality, plánování kvality, kontrola kvalit, zajištění a zlepšování kvality. [19]

Další dvojicí slov, které je dobré definovat z testovacího pohledu, jsou verifikace a validace.

Verifikace je ověření, že byly splněny stanovené cíle. Týká se kontroly dokumentace, designu, kódu, testovacích případů. Verifikace se ptá otázkou „Vytváříme produkt správně?“. [2, 19]

Validace je ověření na základě reálných, skutečných výsledků, tedy že byly splněny požadavky pro konkrétní použití nebo aplikaci. Týká se produktu. Validace se ptá otázkou „Vytváříme správný produkt?“. [2, 19]

2.2 Techniky testování informačního systému

Podle [2]: jsou dvě techniky testování, které se dále rozdělují:

1. **Statické** testování je takové testování, kdy výsledný software nebyl spuštěn, nebo kdy ještě neexistuje.
    A. **Testování dokumentace** se zaměřuje především na správnost, úplnost a konzistenci obsahu. Hlavními kritériemi, které by měl obsahu dokumentu splnit – úplnost, správnost, relevantnost, jednoznačnost, konzistence. Pokud je dokument správně po formální stránce, pak se přechází ke správnosti struktury jeho obsahu, gramatické správnosti a vzhledu [19].
    B. Při **testování kódu** se postupuje podle více pravidel a metrik než u dokumentace, ty se můžou automaticky měřit a vyhodnocovat. Cílem je kvalitní zdrojový kód [19].
2. **Dynamické** testování je takové testování, kdy již se spouští výsledný software [2].
    A. **Black box** (černá skříňka) je založeno na analýze testovací báze (například specifikace systému, uživatelské případy). Zaměřuje se na vstupy a výstupy testovacího objektu, aniž by tester měl povědomí o vnitřní struktuře systému.
    B. **White box** (bílá skříňka) je založena na analýze architektury, detailního návrhu, vnitřní struktury nebo kódu testovacího objektu, tedy se tato technika zaměřuje na strukturu a proces systému, o kterém již tester povědomí má.
    C. **Grey box** (šedá skříňka) je kombinace černé a bílé skříňky.

Tyto techniky se prolínají všemi typy testů i v bezpečnostním testování, avšak bezpečnostní testování se rozděluje na další druhy testování jako [25]:

- test zranitelnosti,
- test síťové bezpečnosti,
- penetrační test,
- odhad rizika,
- bezpečnostní audit,
- etické hackování,
- API bezpečnostní test,
- a další.

3 Testování použitelnosti informačního systému

3.1 Použitelnost

V [8] je uvedeno, že na základě maximalizovat použitelnost a bezpečnost systému Salthzer a Schroeder vymysleli princip psychologické přijatelnosti. Ten říká, že bezpečnostní mechanismy by neměli ztěžovat nebo vyžadovat další úkony k přístupu do systému, než kdyby tam nebylo žádné zabezpečení. Tedy ovládání systémů by mělo být intuitivní. Aplikováním tohoto principu je třeba vzít v úvahu, že uživatelé internetu se mezi sebou odlišují hned několika faktory a to schopnostmi, znalostmi a jejich myšlením. To znamená, že například pro programátora je daný systém mnohem jednodušší než pro sekretářku, která mu nerozumí a neumí ho použít. Tudíž si musíme při vývoji systému uvědomit, pro koho je určen a zda je pro ně pochopitelný. Bohužel v praxi je to často naopak. Programátoři totiž vytvářejí systém podle svých představ o jeho fungování bez ohledu na očekávání uživatele. To je často důvod, proč se uživatelé nedokážou chovat očekávaným nebo vyžadovaným způsobem v systému.

3.2 Metody testování použitelnosti

Metody testování použitelnosti je možné rozdělit na kvantitativní a kvalitativní. V kvantitativních metodách jde o to, že testování se účastní velký počet uživatelů K tomuto typu testování většinou používají analytické nástroje. Takto se například dělají A/B testy, při kterých se zkoumá, která z variant je příznivější. Tedy tyto testy nám dají možnost analyzovat chování zákazníka, například kolikrát a kam klikají. [24]

Kvalitativní testování je časově náročnější, ale je kvalitní analýzou. Odpoví na otázky typu, proč uživatelé neklikají na přihlášení k newsletteru. Kvalitativních metod testování je také celá řada, nejznámější jsou [24]:

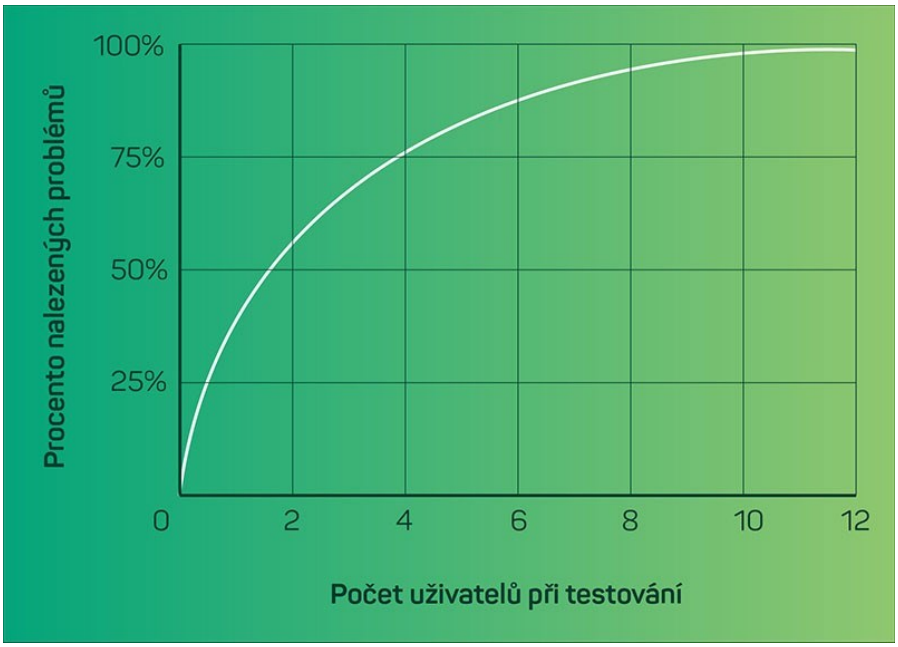
- Focus group – skupinové dotazování, které může být skvělé i v rámci vaší firmy jako brainstorming při vývoji nových stránek.
- Hloubkový rozhovor – při kterém sledujeme pohyb uživatele po webu k předem danému cíli (například vyplnění dotazníku).
- Card sorting – metoda, kdy uživatelé přiřazují kartičky s přídavnými jmény (například osobitý, matoucí, nevýrazný atd.). Metodu představil Microsoft v roce 2002, jako metodu, která umožňuje lépe popsat subjektivní pocity uživatelů.
- Heuristické testování – metoda spočívá v odhalování chyb pomocí porovnávání současného stavu s předem danými pravidly (heuristikami).

- Uživatelské testování – metoda na základě interakcí reálných uživatelů s webem, nebo jinou aplikací. Metoda pracuje tedy se skutečnými zákazníky a pomáhá přeměnit původní dohady a předpoklady v podložená data.

Metod testování je samozřejmě mnohem víc, toto jsou jen ty, které dokážete využít i při amatérském testování. Kvalitativní testování nám poskytuje softdata – neboli říká, co si uživatel myslel nebo jak se cítil. Při nákupu se stále rozhodujeme na základě pocitů a emocí, takže tento aspekt nelze podceňovat. [24]

3.3 Vhodný počet hodnotitelů pro testy použitelnosti

Na jeden test použitelnosti je optimální počet hodnotitelů je pět až šest v závislosti na rozsahu a důležitosti testovaného objektu. Je to takový počet lidí, který nalezne asi 70–80 % chyb použitelnosti, v případě, že ten samý problém má každý třetí uživatel. [16] Při větším počtu účastníků se nalezené problémy opakují, většinou [15], tzn. počet odhalených problémů se vzrůstajícím počtem hodnotitelů stále klesá. Samozřejmě, je možné využít více respondentů a zkusit tak, zda odhalí větší počet problémů, je však nutné si uvědomit, že s každým dalším hodnotitelem rostou náklady na testování. Proto pro zvolení optimálního počtu hodnotitelů je třeba brát v úvahu optimální poměr nákladů na testování a přínosů, které odhalení problémů přinese. Vztah mezi počtem hodnotitelů a procentem odhalených problémů zachycuje obrázek č. 4 [15].



Obrázek 4 Vztah mezi počtem hodnotitelů a procentem odhalených problémů

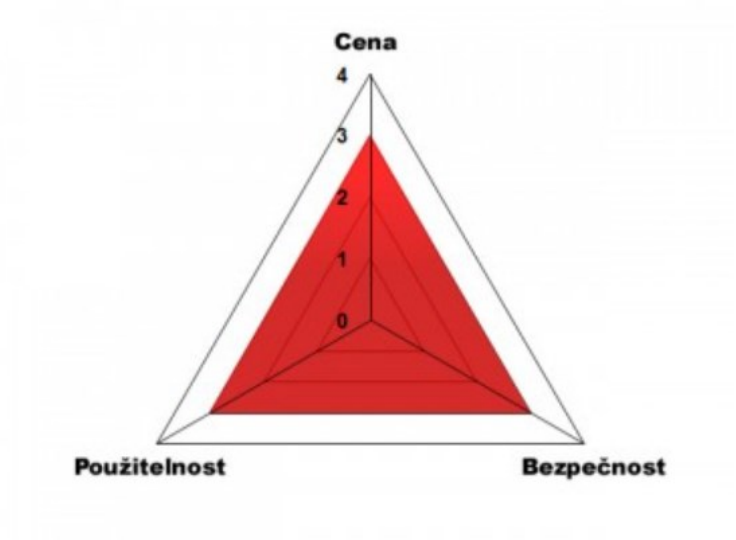
Zdroj: [15]

4 Vztah mezi použitelností a bezpečností

V současné době stále je problém najít mezi použitelností a bezpečností systémů rovnováhu. Je zřejmé, že např. počítač je bez zabezpečení pomocí hesel použitelný, ale ve výsledku není dostatečně zabezpečený. Na druhou stranu, počítač, který vyžaduje autentizaci každých deset minut, je dobře chráněn před útoky, ale nepracuje se s ním už tak dobře, protože pořád musíme ověřovat svou identitu. Proto je nutné najít kompromis, aby byl systém jak použitelný, tak bezpečný.

Pro malé a střední firmy je cenové hledisko také důležité, samozřejmě i pro velké podniky je toto hledisko významné, ale už ne tolik jako u těch menších.

Nejlépe se tento vztah dá vyjádřit pomocí trojúhelníku, kde právě jedna strana představuje jednu veličinu. Platí zde pravidlo, že pokud se změní jedna veličina, pak se změní alespoň jedna další veličina. Dále pak čím vyšší konkrétní veličině přisoudíme, tím je možné považovat dané řešení za použitelnější, bezpečnější nebo lacinější [7].



Obrázek 5 Vztah mezi použitelností, bezpečností a cenou

Zdroj: [7]

Použitelnější řešení: chceme-li systém, který je lehký na ovládání, tj. použitelný, pak se ale sníží jeho bezpečnost, a tudíž cena klesá.
Bezpečnější řešení: požadujeme-li vysokou bezpečnost, pak použitelnost klesá, a naopak cena klesá.
Lacinější řešení: je-li pro firmu důležitá cena než zbylé dva faktory, pak systém není dostatečně bezpečný, ani použitelný.

Další hledisko vztahu mezi použitelností a bezpečností z toho hlediska, že čím míň chyb bude uživatel dělat, tím je systém bezpečnější. Když uživatelé nedodržují požadované chování zabezpečeným systémem, kvůli tomu zabezpečení nebude fungovat tak, jak se zamýšlelo. Existují dva důvody, proč jsou uživatelé neúspěšní při používání systému. A to buď že nejsou schopni se chovat, jak je požadováno, nebo že se nechtějí chovat požadovaným způsobem.

Příkladem první situace jsou silná – špatně zapamatovatelná dlouhá hesla, tudíž lidé používají hesla jednoduchá, krátká a snadno uhodnutelná. Zde je na vině paměť člověka. Tudíž si je uživatelé zapisují, nebo je řeknou někomu jinému, aby si ho za něj pamatoval, nebo si zvolí takové heslo, které je jednoduché si zapamatovat, ale ne bezpečné. Tedy lidé vědomě porušují např. firemní nařízení ohledně hesel. A proto firmy pro své nové zaměstnance školí, jak si zvolit „dobré heslo“ – je přiměřeně dlouhé a používá dostatečně velkou sadu znaků – ale stále je jednoduché k zapamatování. Pokud bychom zkusili na internetu vyhledat slova „zvolit“, „vybrat“, „dobrý/é/á“, a „heslo/a“, tak zjistíme, že spousta webů zapomíná na důležitost zapamatovatelnosti [8]. Z toho tedy vyplývá, že čím víc se uživatelé budou držet např. doporučeným nařízením, tím míň chyb budou dělat, a tudíž přispějí k bezpečnosti systému proti ztrátě dat apod.

5 Testování multifaktorové autentizace na UPa

5.1 Základní informace o webu a intranetu UPa a situace před zavedením MFA

V roce 2018 byl spuštěn nový design webu Univerzity Pardubice od Drupal Arts. Zaměstnanci Drupal Arts měli za cíl vytvořit jednotný webový prostor, to znamená místo, kde se na jedné platformě nachází: ústřední webový portál www.upce.cz, všech 7 fakult i s katedrami a ústavy, weby knihovny, katedry sportu a jazykového centra, studentský a zaměstnanecký intranet a uživatelská data z interních systémů univerzity od zobrazování dovolených, cestovních cest až po počet zbylých kreditů v menze [6].

Technické parametry:

- navrhovatel a implementátor: Drupal Arts,
- nový design: od roku 2018,
- responzivita: ano,
- přístupnost: ano.

Dle Ing. Slaniny, člena výboru pro řízení kyberbezpečnosti, byla bezpečnost na Univerzitě Pardubice do roku 2020 dána bezpečnostní směrnicí viz příloha č. 2, podle níž byla povinnost použití uživatelského jména a hesla jak pro zaměstnance univerzity, tak pro studenty.

Situace související s implementací multifaktorové autentizace na Univerzitě Pardubice

Koncem roku 2017 se na univerzitě od IT UPCE začaly objevovat zmínky o rozšířeném zabezpečení informačních systémů, kdy se uvažovalo o použití dostupného řešení v rámci Microsoft Azure. Díky pandemii Covid-19 byla univerzita se adaptovat na online prostředí – zaměstnanci pracovali na tzv. homeoffice (práce z domu), studenti byli vyučováni učiteli přes aplikaci Microsoft Teams. V roce 2021 byla kybernetická bezpečnost zanesena do interní legislativy univerzity a oficiálně je zastřešována manažerem kybernetické bezpečnosti a výborem pro kybernetickou bezpečnost. Poté začala další fáze, a to plošné nasazení multifaktorové autentizace na univerzitě se zaměřením na zaměstnance. To se ale setkalo s odporem zaměstnanců (2021). To zapříčinilo to, že bylo potřeba zpracovat tzv. opatření rektora pro zabezpečení uživatelských účtů zaměstnanců – informační kampaň (2022). Dokument vešel v účinnost 8. dubna 2022. oddělení kybernetické bezpečnosti dále informovala zaměstnance o bezpečnosti a aby zaměstnanci změnili názor na multifaktorovou autentizaci. Také postupně vynucovalo MFA na informačních systémech univerzity, a tudíž byli

zaměstnanci nuceni si MFA nastavit na systémech jako Office365, VPN apod. Studenti o multifaktorové autentizaci byly poprvé informováni pomocí školní e-mailové schránky 5. prosince 2022 První připomínkový e-mail dostali studenti 3. února 2023 a druhý 29. března 2023. Implementace multifaktorové autentizace byla kvůli rozsáhlému kybernetickému útoku urychlena, a proto od poloviny dubna 2023 probíhá postupné zapínání registrační politiky na systémech univerzity [informace od CITS].

5.2 Výběr metody testování použitelnosti

Dotazník byl vytvořen za účelem průzkumu mezi studenty Univerzity Pardubice a zjistit jaký je názor na multifaktorové ověřování na univerzitě. Byl vytvořen pomocí nástroje pro tvorbu online formulářů od společnosti Google – Formuláře Google. Tento nástroj byl vybrán z těchto důvodů:

- je zdarma,
- je intuitivní,
- jednoduchý,
- mezi otázkami je možné vytvořit logiku,
- uchovává jednotlivé odpovědi dle otázky, respondenta,
- grafy jsou automaticky vytvářeny ze získaných odpovědí,
- získaná data se dají exportovat do nástroje Tabulek Google,
- je možné určit rozložení v uživatelském rozhraní (UI) – všechny otázky pod sebou na jedné straně, nebo po zodpovězení jedné otázky přejít na další.

Například rozhovory z očí do očí nejsou příliš vhodné, protože se účastníci většinou stydí a bojí se, co si o nich tazatel myslí apod., tudíž je lepší zvolit anonymní dotazník, který mohou vyplnit kdekoliv a kdykoliv v určitém čase stanovený pro sběr dat a nikdo je za jejich odpovědi nesoudí.

Uživatelské testování je jedna z metod, jak použitelnost testovat. Použijeme-li vhodný testovací vzorek je možné se pomocí uživatelských testů dozvědět o chování uživatele více, než pouze z dotazníků nebo otázek.

Doplňující otázky jsou dobré k tomu, aby se tazatel dozvěděl detailnější informace o tom, co ho zajímá. Problém tak pomocí dalšími otázkami je možné upřesnit, či dovysvětlit.

5.3 Stanovení postupu testování použitelnosti a bezpečnosti MFA na UPa

Cílem testování bylo nalézt nedostatky použitelnosti a bezpečnosti a navrhnout jejich řešení. Celé testování probíhalo v následujícím pořadí.

1. Testování použitelnosti probíhalo na www.upce.cz a na studentském intranetu https://studenti.upce.cz. Zaměstnanecký intranet, weby fakult, knihovny apod. nejsou do tohoto testování zahrnuty. Intranet a hlavní web Univerzity Pardubice byly vybrány do této bakalářské práce, protože se autorce zdály z hlediska testování použitelnosti webu uživatelsky nepřívětivé, tzn. že například ne lehce se na nich vyhledávají např. informace o MFA v případě nepoužití funkce vyhledávání. Z hlediska testování bezpečnosti se práce zabývá nejkritičtějším článkem, a to studenty a potencionálními studenty Univerzity Pardubice.
2. Byl vytvořen dotazník pro studenty Univerzity Pardubice, za účelem průzkumu mezi studenty Univerzity Pardubice a zjistit jaký je názor na multifaktorové ověřování na univerzitě. Následně se studentům elektronicky rozeslal dotazník s průzkumem, jak si poradili s instalací MFA, zda používají MFA i mimo univerzitu apod. Po dvou týdnech, kdy studenti měli možnost zúčastnit se dotazníkového šetření, se udělalo vyhodnocení.
3. Následně bylo kontaktováno IT oddělení univerzity a položila ji několik otázek o MFA.
4. Byla otestována uživatelská příručka neboli manuál, které poskytlo IT oddělení univerzity zaslané e-mailem studentům k instalaci a nastavení MFA z hlediska použitelnosti pomocí statického testování, aby se předešlo např. gramatickým chybám aj.
5. Byly vytvořeny testovací úkoly, které účastníci testování zkoušeli splnit. Také se vybralo 5 studentů z UPa, kteří na základě připravených úkolů otestovali MFA. Zda jsou studenti schopni na intranetu univerzity najít návod, jak nastavit autentizační metody a zda je schopný si podle něj nastavit alespoň jednu metodu sám, bez jakékoli podpory.
6. Na základě všech provedených testování se sestavil seznam nalezených nedostatků a k jednotlivým slabinám bylo navrženo řešení, jak takovým nedostatkům předcházet.

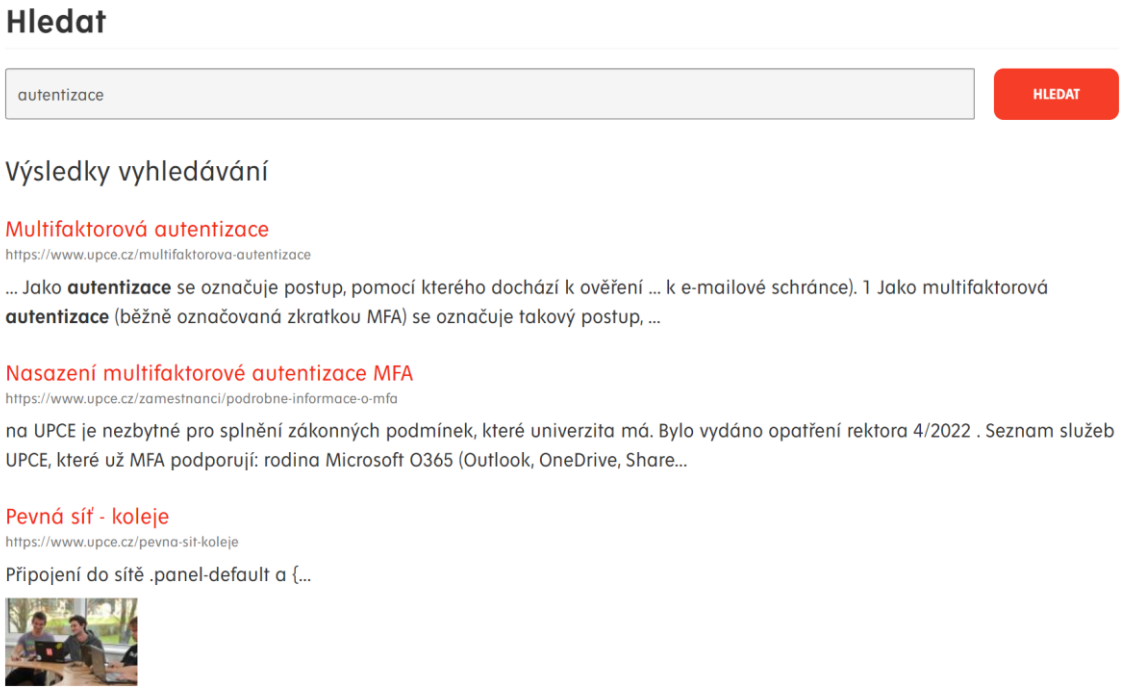
5.4 Testování použitelnosti vyhledávání a článků o MFA na webech UPa

5.4.1 Analýza použitelnosti hlavního webu Univerzity Pardubice

Testování bylo prováděno 14. února 2023

Najít informace o MFA na webu UPa není nijak složité za pomocí vyhledávače. Avšak musíme použít ta správná klíčová slova, pod kterými se multifaktorové ověřování nachází, jako autentizace, multifaktorový apod.

Vepíšeme-li do vyhledávače slovo autentizace, dostaneme jako výsledek 3 odkazy (viz obr 6). Ale pouze odkazy „Multifaktorová autentizace“ a „Nasazení multifaktorové autentizace MFA“ se vztahují k tématu této bakalářské práce.



Obrázek 6 Výsledek vyhledávání pro slovo autentizace na www.upce.cz

Zdroj: vlastní

Článek „Multifaktorová autentizace“ informuje čtenáře o spoustě informací a je s největší pravděpodobností určen studentům a veřejnosti:

- Co je to MFA?
- Princip MFA.
- Způsoby ověřování.
- Vynucování MFA.

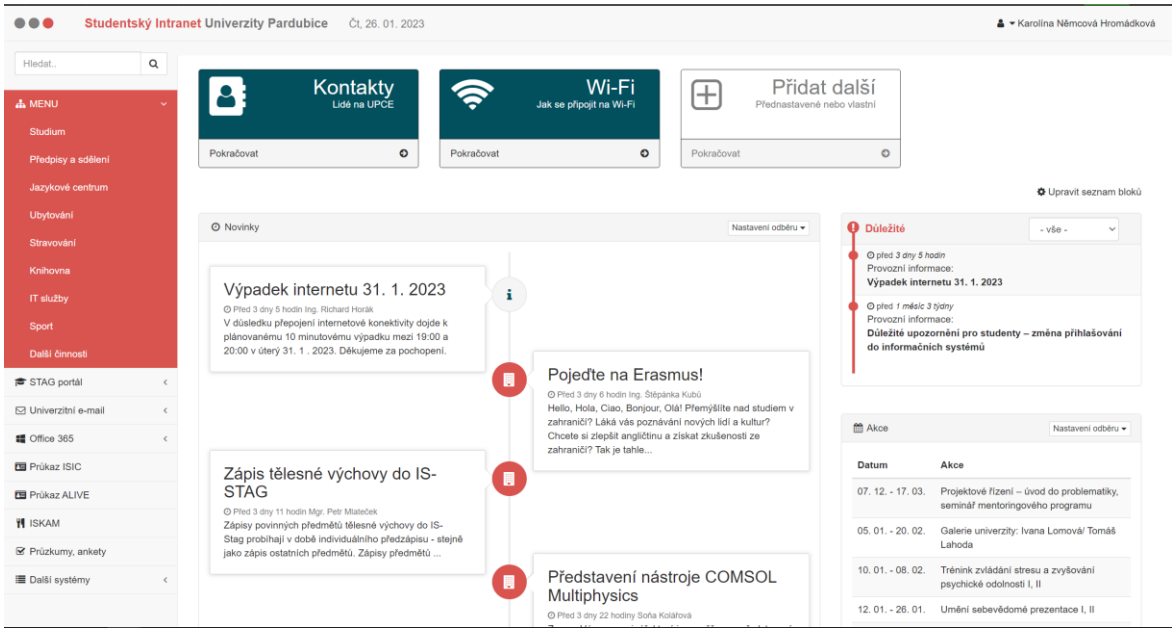
Text článku není nijak špatně strukturován, ale návod v něm nelze jednoduše rozeznat od ostatního textu. Je to proto, že článek je zdlouhavý a jeho čtení přestává bavit, tudíž čtenář se ani k odstavci s návodem na nastavení MFA pravděpodobně nedostane. Z tohoto pohledu je lepší dát odkaz na návod na začátek článku, protože to je to, co uživatele PC nejspíše nejvíce zajímá.

Druhá sekce „Nasazení multifaktorové autentizace MFA“ není již tak rozsáhlá, ale je psaná spíše pro zaměstnance univerzity než pro studenty už kvůli tomu, že jedno z nejčastějších slov v ní je slovo „zaměstnanec“ a jeho varianty. Návod je v tomto článku k dohledání, ale je zde riziko, že čtenář, pokud je to student, může usoudit, že v něm nenajde to, co hledá, už kvůli slovu zaměstnanec. Také už název článku může být zavádějící, protože informuje o nasazení MFA do praxe a mohl by pojednávat o statistice bezpečnosti za použití této metody.

V případě, že bychom nepoužili funkci vyhledávání, pak bychom pravděpodobně informace o MFA nenašli. Pokud by se nám to však podařilo, trvalo by to hodiny až dny, možná i déle. Web je relativně komplexní a jeho zjednodušení by mělo být v zájmu univerzity. Případně všechny důležité informace by se mohly uchovávat v horní části webu v sekci Novinky.

5.4.2 Analýza použitelnosti studentského intranetu Univerzity Pardubice

Intranet je velice komplexní a není lehké se v něm vyznat, i když jste na webu byli již několikrát.

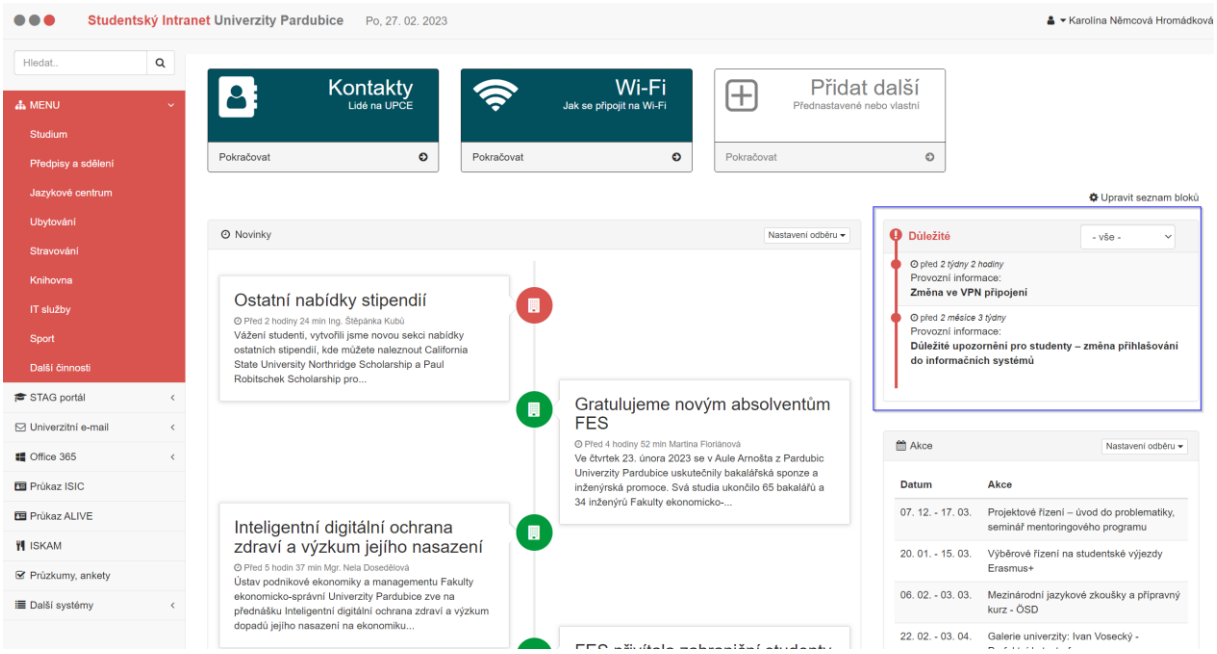


Obrázek 7 Úvodní stránka studentského intranetu

Zdroj: vlastní

Po přihlášení do intranetu (dne 22. února 2023), na první pohled nelze říci, zda jsou na úvodní stránce nějaké důležité informace, které by se student měl dozvědět. Ale pokud se podíváme více do pravé části obrazovky, najdeme malou sekci „Důležité“, kde se právě nacházejí informace o změně přihlašování do informačních systémů a VPN.

Zde důležité si uvědomit, že intranet je designován v červeno-bílém návrhu, stejně tak i část s důležitými informacemi, které by neměly být přehlédnutelné. Tedy je tu riziko, že student si tyto informace nikdy nepřečte, protože je jednoduše neuvidí. Je to především kvůli tomu, že v levé části se nachází menu, kam se nejvíce uživatelé dívají, protože si myslí, že právě tam najdou navigaci na to, co je zajímá. Další důvod je design stránky, který by měl být v jiných barvách kvůli tomu, aby v případě zanechání sekce „Důležité“ v současném návrhu nebylo možné informace v této části přehlédnout. Pak také by bylo vhodné umístit tuto sekci blíže k menu, např. nahradit dlaždice „Kontakty“, „Wi-Fi“, „Přidat další“, právě sekcí „Důležité“.



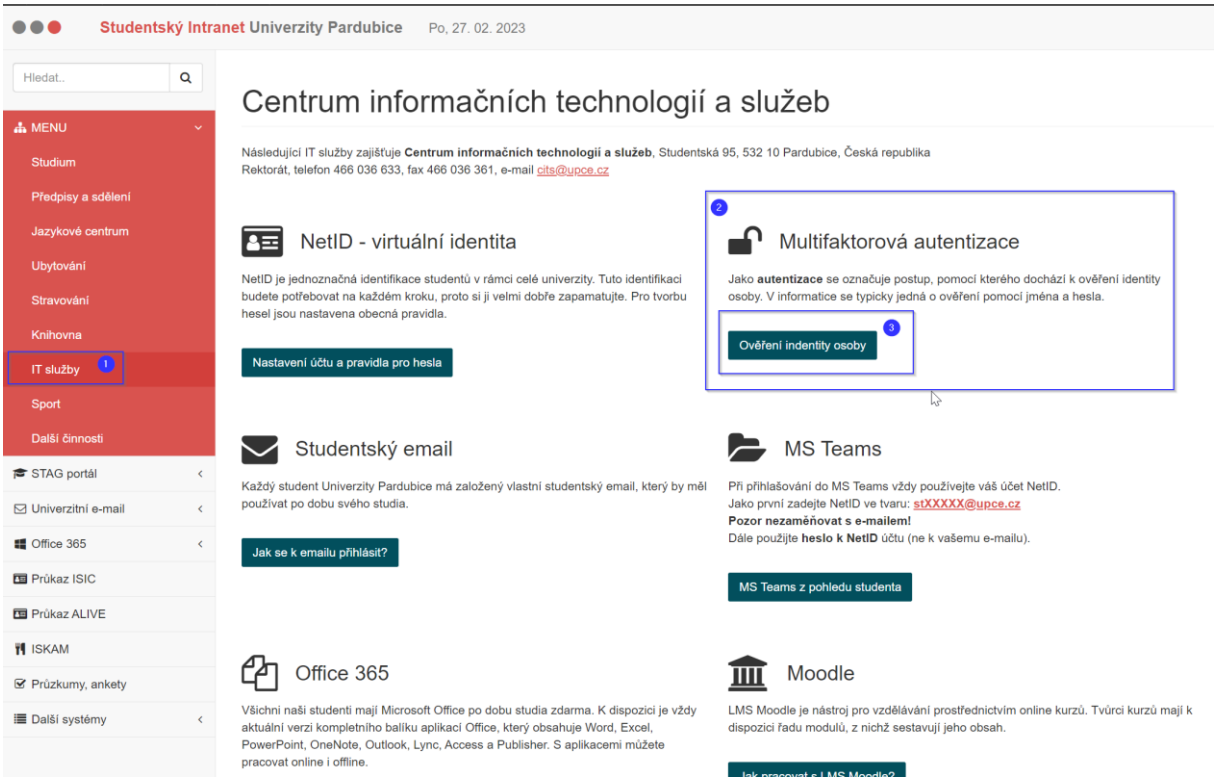
Obrázek 8 Zobrazení sekce "Důležité na domovské stránce intranetu

Zdroj: vlastní

Také informace o změnách v přihlašování lze najít v části „Novinky“ ale ne už tak snadno. Je to z toho důvodu, že v novinkách lze najít všechno, co se na Univerzitě Pardubice děje. Tedy záleží na frekvenci přidávání nových příspěvků. Protože pokud by se přidával jeden článek za měsíc, byly by informace o přihlašování jednoduše dohledatelné, jen by uživatel musel proklikat stránkování této sekce, až by našel právě ten článek, který chce vidět. Pokud by ale

byla frekvence deset příspěvků za týden, tak právě ten jeden konkrétní článek by nenašel a trvalo by mu to několik hodin možná i dní.

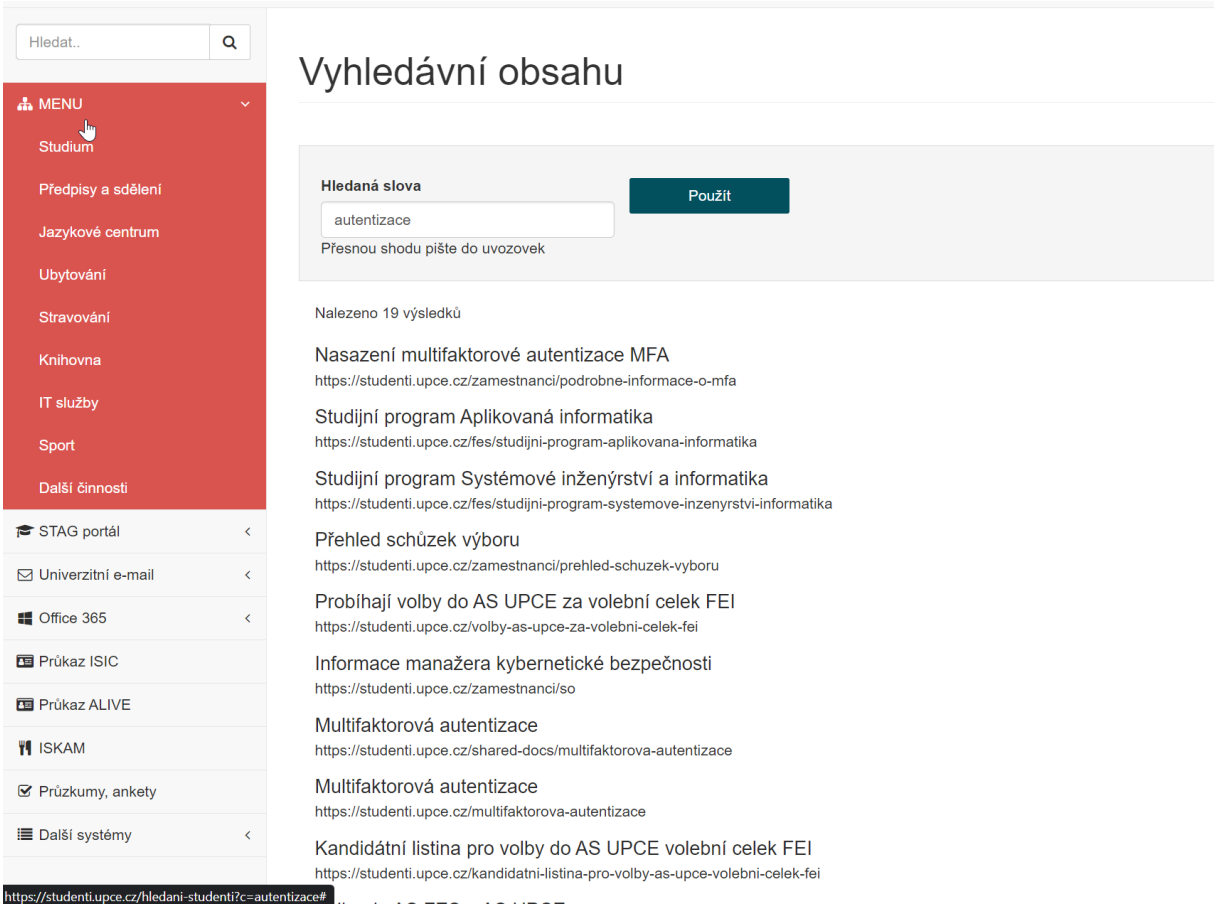
Dále se pak můžeme podívat do menu intranetu, kde nalezneme záložku IT služby. Klikneme-li na ni zobrazí se nám stránka Centrum informačních technologií a služeb (číslo 1 v obr. 7), kde najdeme Multifaktorová autentizace (číslo 2 v obr. 7). To ale uživatele informuje pouze o tom, co autentizace znamená. V případě, že student klikne na tlačítko „Ověření identity osoby“ (číslo 3 v obr. 7), intranet ho přesměruje na článek Multifaktorová autentizace nacházející se na webu www.upce.cz.



Obrázek 9 Postup k zobrazení článku Multifaktorová autentizace

Zdroj: vlastní

Použijeme-li funkci vyhledávání nad navigací stejně jako tomu bylo v předchozí kapitole, tak ve výsledcích vyhledávání nalezneme 19 článků pro slovo autentizace viz obr 10. Ne ale všechny se týkají právě multifaktorové autentizace a také ne každý odkaz by se měl zobrazit na studentském intranetu.



Obrázek 10 Příklad výsledků vyhledávání pro slovo autentizace

Zdroj: vlastní

Odkazy, které by se neměly zobrazovat na studentském intranetu jsou například „Přehled schůzek výboru“, nebo „Informace manažera kybernetického bezpečnosti“, protože subdoména URL těchto odkazů vyvolává dojem, že https://studenti.upce.cz obsahuje pouze informace pro studenty udělené správcem intranetu. Zde by bylo dobré, kdyby zaměstnanecký intranet měl svou subdoménu např. https://zamestnanci.upce.cz. Druhý důvod je i to, že za subdoménou se nachází slovo zaměstnanci např. https://studenti.upce.cz/zamestnanci/..., což také indikuje, že takové odkazy nejsou určeny studentům. Tedy by bylo vhodné takové odkazy, články aj. přesunout na zaměstnanecký intranet. Následně se bude uživatel moci najít relevantní informace rychleji aniž by mu po otevření odkazů byl přístup odmítnut. Například článek „Nasazení multifaktorové autentizace MFA“ by mohl obsahovat informace, kde najít návod na instalaci MFA pro studenta, avšak po otevření odkazu je studentovi přístup zamítnut, protože nemá práva pro zaměstnance. Dále by také bylo vhodné filtrovat odkazy, ke kterým nemají přístup, a tedy jim takové vůbec nezobrazovat. Například URL článku Studijní program Systémové inženýrství a informatika neindikuje, že by studentovi po jeho rozkliknutí měl být

přístup odepřen, protože URL je https://studenti.upce.cz/fes/studijni-program-systemove-inzenyrstvi-informatika, kde subdoména je „studenti“ a ani neobsahuje podsložku zaměstnanci.

Jak z výše uvedeného vyplývá, studentský intranet je velice komplexní a není v něm lehké se zorientovat, natož najít návod k instalaci MFA a je pouze na univerzitě, zda dá podnět tvůrcům intranetu ke zlepšení.

5.5 Multifaktorová autentizace pro studenty Univerzity Pardubice

5.5.1 Vytvoření dotazníku

Otázky v dotazníku byly rozřazeny do třech bloků. První část obsahovala spíše názorové otázky (1-4), v druhé části se zařadily otázky (5-11), které již měly zjišťovací charakter, ohledně situace na univerzitě s MFA a názorů studentů na multifaktorové ověřování. Třetí a zároveň poslední blok obsahoval zjišťující otázky (12-15) spojené se studiem na Univerzitě Pardubice. Poté byly otázky uspořádány dle diagramu viz obr. 11, aby na sebe navazovaly, ale zároveň aby otázky měly i logickou návaznost dle odpovědí respondentů.

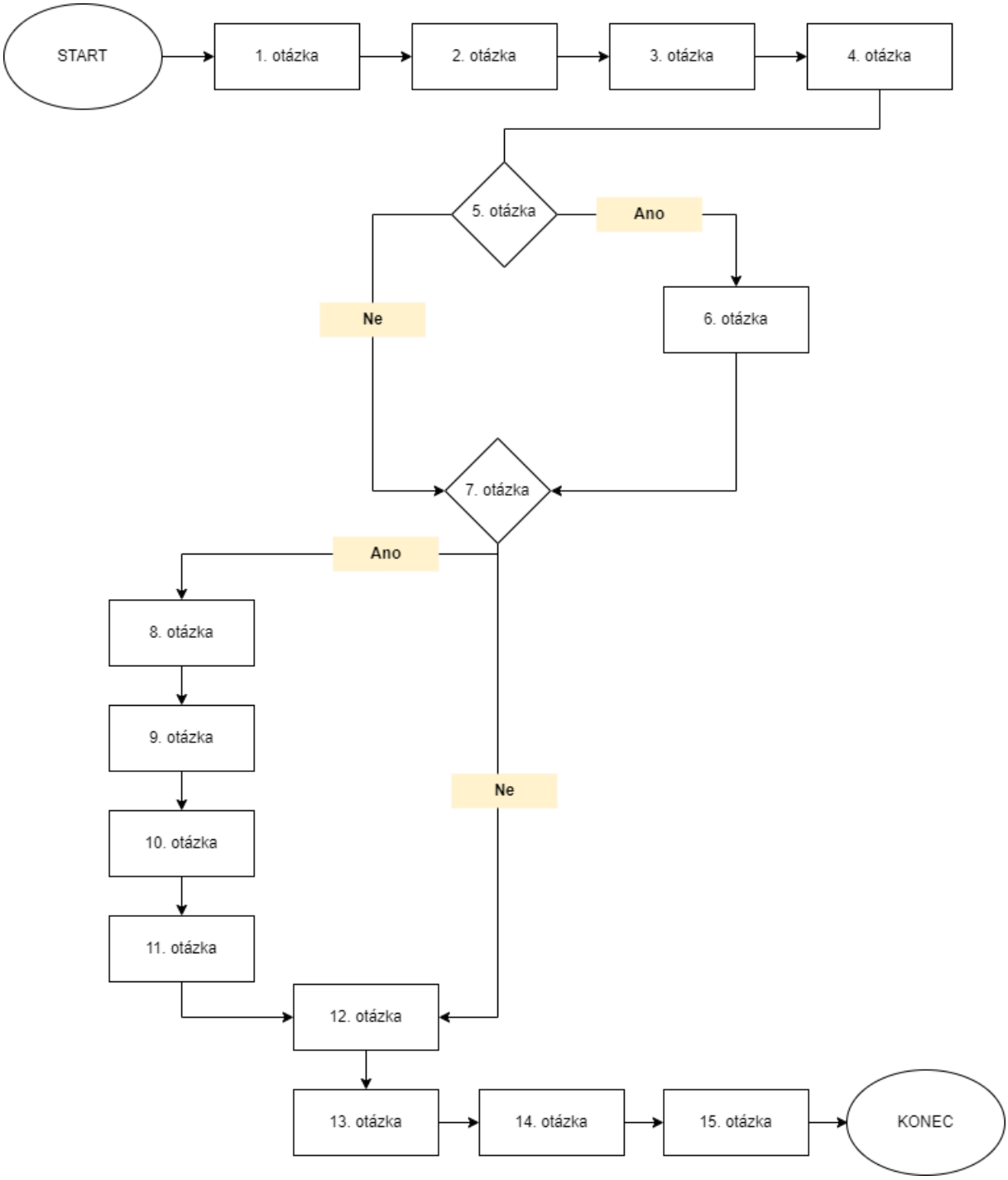
Do průzkumu byly zařazeny otázky jak otevřené (1-2, 8-9), tak uzavřené (3-7, 10-15). Na otázky otevřené, musí studenti odpověď slovy.

Otázky v dotazníku:

1. Co si myslíš o multifaktorovém ověřování?
2. Je multifaktorové ověřování bezpečnější, nebo bylo použití ID a hesla dostatečné?
3. Používáš/Jsi ochoten používat svůj osobní telefon k ověřování?
4. Jsi případně ochoten si zakoupit autentizační klíčenku, pokud by se její cena pohybovala do 500 Kč?
5. Byl jsi informován o změně přihlašování do systémů Univerzity Pardubice?
6. Jakým způsobem jsi byl informován?
7. Už sis nainstaloval MFA?
8. Jak a kde jsi našel návod na instalaci MFA?
9. Napiš svůj názor, jak lehce/těžko se MFA instalovalo podle návodu. Napiš také, jaké jsi měl s instalací problémy, pokud jsi nějaké měl, své dojmy z manuálu.
10. Jakou formu autentizace sis vybral?
11. Používáš multifaktorové ověřování i jinde? Kde?
12. Jakou formou studuješ?
13. Na jaké fakultě studuješ?

14. Ve kterém ročníku jsi?

15. Kolik ti je let?



Obrázek 11 Diagram návaznosti otázek

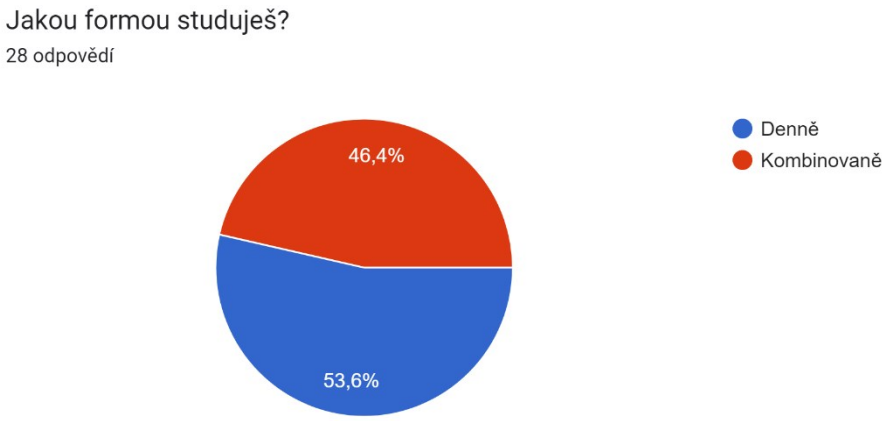
Zdroj: vlastní

Předtím než se otázky zaslaly studentům univerzity, byl zaslán na ověření, že se otázky zobrazují, tak jak byla stanovena logika dotazníku viz obr. 11, zda některé otázky by nebylo lepší rozdělit na více otázek, bývalému kolegovi z NTT Data Business solutions, který se dlouhodobě věnoval testováním webových aplikací. Takovéto ověření proběhlo třikrát v intervalech dvou dnů, tzn. dva dny na opravu připomínek a dva dny na ověření, abychom já, autorka ani bývalý kolega nebyli příliš ve stresu. Následně po opravení všech připomínek byl dotazník rozeslán studentům Univerzity Pardubice bez ohledu na věk, formu a obor studia apod. panem doc. Ing. Miloslavem Hubem, Ph.D., vedoucím této bakalářské práce, který byl požádán o spolupráci.

Průzkum se prováděl v období 6. až 19. března 2023. Tedy v době, kdy studenti již měli možnost dobrovolně si MFA nainstalovat, avšak pro studenty, kteří používali VPN UPa, bylo nastavení multifaktorové autentizace povinné.

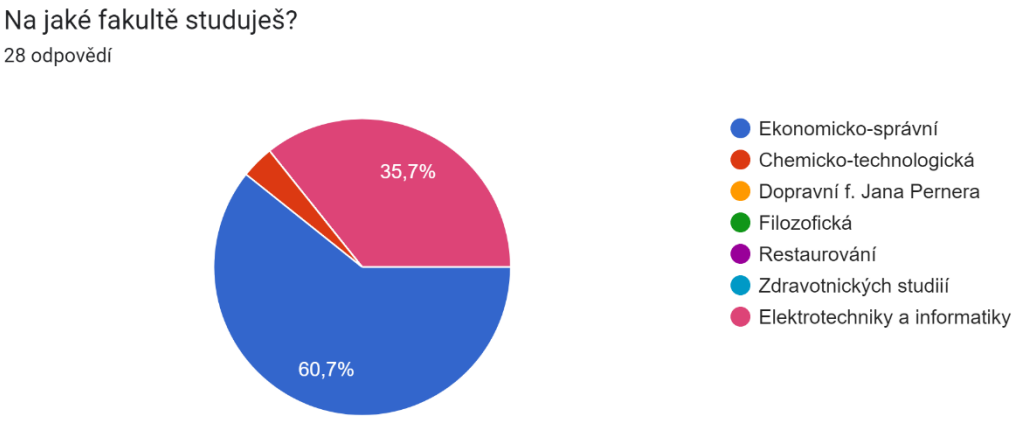
5.5.2 Vyhodnocení dotazníku

Šetření se zúčastnilo 28 studentů ze všech ročníků bakalářského a navazujícího studia (viz obr. 13). Studenti byly ze 3 fakult (ekonomicko-správní, chemickotechnologická, elektrotechniky a informatiky) ve věku od 19 do 50 let v závislosti na formě studia viz obr 13 a 14. Z denního studia se odpovědělo 15 a z kombinovaného 13 studentů, což je velice vyrovnané (viz obr 12).



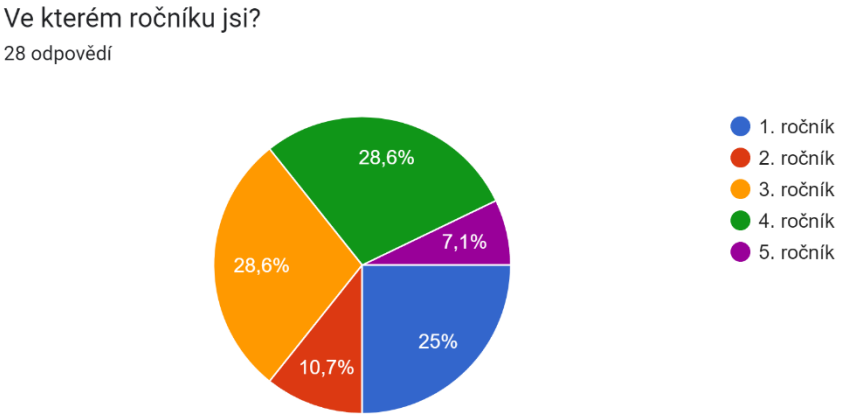
Obrázek 12 Hodnocení otázky 12

Zdroj: vlastní



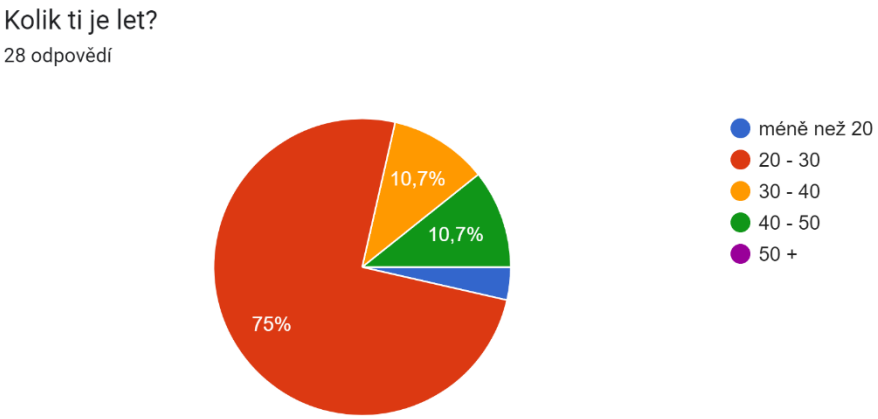
Obrázek 13 Hodnocení otázky 13

Zdroj: vlastní



Obrázek 14 Hodnocení otázky 14

Zdroj: vlastní



Obrázek 15 Hodnocení otázky 15

Zdroj: vlastní

Otázky 1, 2, 7

Na základě získaných odpovědí od studentů Univerzity Pardubice se zjistilo, že téměř všichni považují multifaktorové ověřování za bezpečnější než zadávání uživatelského jména a hesla viz. tabulka č. 1 a 2. Několik z nich však udává, že multifaktorová autentizace je otravná, protože při každém přihlašování musí ověřit svou identitu, což bývá někdy zdlouhavé. Je však zajímavé, že i když studenti uvedli, že MFA je bezpečnější, tak 17 z 28 respondentů napsalo, že zatím si multifaktorové ověřování nenainstalovalo viz obr. 16. Je velice pravděpodobné, že dokud to univerzita neuvede v povinnost, tak studenti si MFA nenainstalují.

Tabulka 1 Odpovědi studentů na otázku 1

Co si myslíš o multifaktorovém ověřování?

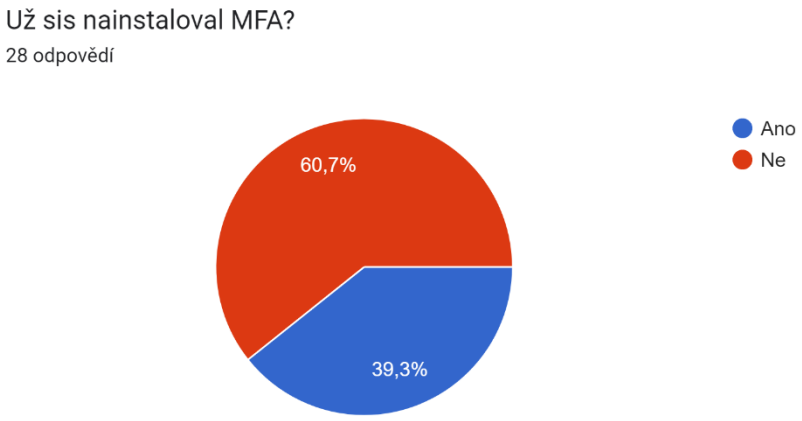
Je to bezpečnější než pouze heslo.
Nevadí mi, beru to jako dobrý způsob ověřování a zabezpečení
Jde o navýšení bezpečnosti účtů.
Považuji za účinnější kontrolu neoprávněného přístupu.
Dobrý způsob zabezpečení
Velmi dobrá věc.
Je třeba k zajištění bezpečnosti.
Větší bezpečnost
Na jednu stranu je to super, ale tu druhou je to děsně otravný. Dokonce se mi stalo, že jsem nechala mobil v Chrudimi, ale byla jsem v Praze, když jsem zrovna potřebovala zadat kód, což nebylo dobré. Jediné, co jsem mohla udělat, zavolat na helpdesk v práci, aby mi povolili přístup.
Otravné, ale bezpečnější řešení
Dobrá věc, občas otravná
Je to dobré zabezpečení, ale občas je to otravný, když člověk spěchá.
Je to rozhodně bezpečnější než jen mít uložené heslo v prohlížeči, který ho sám předvyplní z dříve uloženého přihlášení, nicméně potřeba vždy hledat telefon, odemykat ho a povolovat přihlášení je zdlouhavá a otravná procedura.
Zodpovědné a vetší protekce účtu, avšak k ničemu, když se hacker dostane do počítače samotného a má přístup ke cookies z PC
Velice užitečná věc proti hackerům
Dobrá věc
Pro další ochranu účtů apod dobré.
Supr věc
Na důležité portály, kam se uživatel přihlašuje méně často je užitečný
Dobrý nástroj pro zabezpečení vstupu na webu upce.cz. Osobně zatím nemám aktivované.
Vnímám ho jako užitečné a potřebné.
Nemám vyhraněný názor
Je hodně užitečné.
Je to dobré zabezpečení proti možnému získání účtu.
Aspoň něco
Je to zbytečný
K ničemu

Zdroj: vlastní

Tabulka 2 Odpovědi na otázku 2

Je vícefaktorové ověřování bezpečnější, nebo bylo použití ID a hesla dostatečné?
Bezpečnější
Rozhodně bezpečnější
Vícefaktorové ověření je bezpečnější
Myslím si, že ID a heslo bylo dostačující.
Je to bezpečnější.
Vícefaktrorové ověřování považuji za bezpečnější.
Ano
Rozhodně bezpečnější.
Více faktorové je bezpečnější
Nejlepší by bylo kombinace obojího.
Více faktorů, více bezpečnosti
Je bezpečnější, ale zase ID a heslo lepší, než nic
Dostatečné
Je to bezpečnější, nicméně ne do všech systémů je třeba mít MFA, ID a heslo by postačilo třeba do emailu.
Vícefaktorové ověřování je bezpečnější
Rozhodně je bezpečnější v dnešní době se heslo dá prolomit v řádu minut nebo hodin
Na nějakých stránkách se přes to dostanou ale určitě je bezpečnější
Vícefaktorové ověřování je bezpečnější
Je lepší mít vícefaktorové, více vrstev ochrany je lepší
Je bezpečnější
Je bezpečnější, ale kvalitní hacker se nezalekne ničeho
Netuším
Ano
Vícefaktorové ověřovaní je bezpečnější, ale přijde použití ID a hesla mi přijde pro web univerzity dostačující.
Bezpečnější
Určitě nebylo dostatečné, ze zkušenosti vím, že pomocí softwaru se dá zjistit prakticky jakékoliv heslo
Je bezpečnější.
Vícefaktorové ověření je bezpečnější.

Zdroj: vlastní



Obrázek 16 Hodnocení otázky 7

Zdroj: vlastní

Otázky 3, 4 a 10

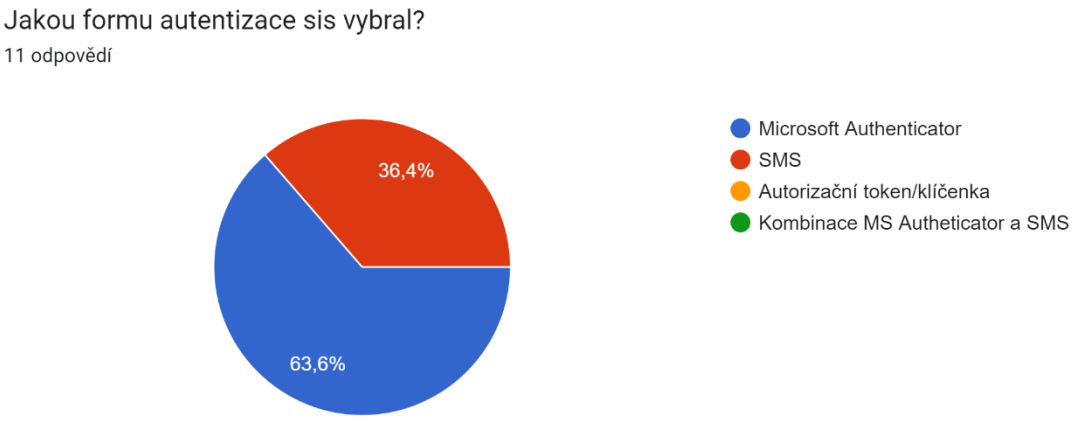
V případě, kdyby univerzita uvedla v povinnost používat autentizační tokeny, které by byly v ceně do 500 Kč a zároveň by si je studenti museli kupovat sami, tak pouze 8 z 28 dotazovaných by bylo ochotno si je zakoupit viz obr.18. Pro všechny je z tázaných je vhodnější jejich osobní mobilní telefon viz obr., protože nejčastější využívanou formu byla zvolena aplikace Microsoft Authenticator viz obr.17. Jako druhá nejčastější byla autentizace pomocí SMS viz obr. 19. Také je to pravděpodobně kvůli tomu, že mobilní telefon mají stále u sebe, zatímco klíče snadno zapomenou. Metoda kombinací např. dvou autentizačních metod (nejprve se studenti identifikují pomocí jedné metody a následně hned druhou) není možná podle informací od Ing. Slaniny a jeho kolegů z CIST (29. 3. 2023). Je možné pouze nastavit si více metod. To je možné využít např. v situaci, kdy u sebe studenti nemají chytrý mobilní telefon, a tudíž mohou zvolit ověření identity jinou než výchozí metodou např. autentizační klíčenkou, pokud ji vlastní. Při implementaci MFA však nebylo myšleno na to, že studenti mohou ztratit, či zapomenout telefon, a tudíž nejsou schopni se do systémů autentizovat, protože pro všechny autentizační metody je nutné u sebe mít telefon krom autentizačního tokenu. Z toho vyplývá, že pokud student nebude mít u sebe telefon nebo token, není možné, aby se do systémů přihlásil.

Obrázek 17 Hodnocení otázky 3

Zdroj: vlastní

Obrázek 18 Hodnocení otázky 4

Zdroj: vlastní

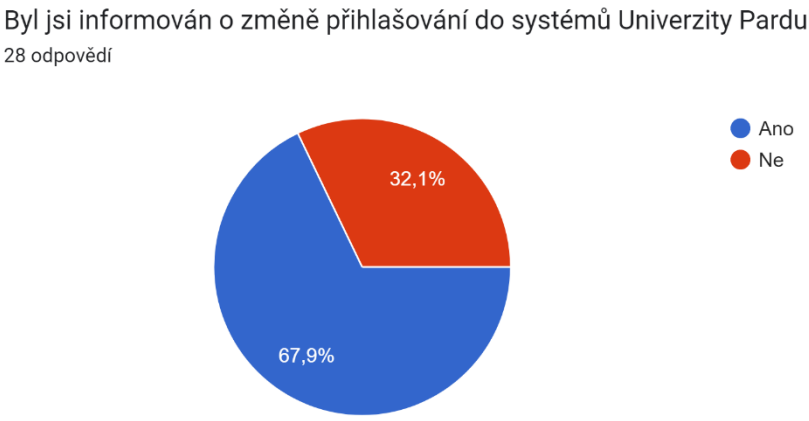


Obrázek 19 Hodnocení otázky 10

Zdroj: vlastní

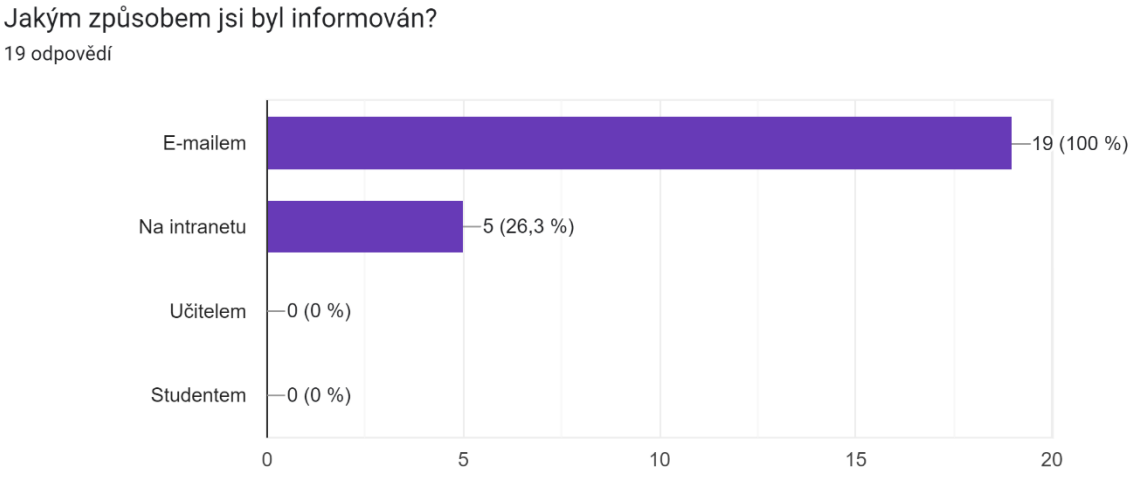
Otázky 5 a 6

Je velice zajímavé, že 9 z 28 respondentů odpovědělo, že nebyly nikým informováni o změně přihlašování do systémů Univerzity Pardubice, i když kybernetické oddělení poslalo informativní email všem studentům viz obr.20. Ostatní, kteří informováni byli, odpověděli, že nejčastěji dostali do své školní emailové schránky informace o chystané změně. Avšak pouze 5 z 19, kteří v otázce č. 5 odpověděli, že informováni byli, udalo, že informaci o změně zaznamenali i na studentském intranetu viz obr.19. Dne 17. dubna 2023 bylo zjištěno z rozhovoru s CITS, že dokument viz příloha č. 1 nelze dle nich brána jako návod, ale jako informativní článek o tom, jaké změny a jak budou probíhat na Univerzitě Pardubice. Avšak z dotazníku pro studenty, vyplynulo, že právě tento dokument se studentům jeví jako návod k nastavení autentizačních metod.



Obrázek 20 Hodnocení otázky 5

Zdroj: vlastní



Obrázek 21 Hodnocení otázky 6

Zdroj: vlastní

Otázky 7, 8 ,9, 11

Většina studentů z těch, kteří vyplnili dotazník, uvedla, že zároveň s informací o změně v přihlašování nalezli i návod k instalaci v informativním emailu. Dle studentů nebylo ani nutno návod použít, protože instalace je logická, nebo daný proces již znají z elektronického bankovnictví, práce, emailu nebo z jiného systému, který MFA vyžaduje viz. tabulka 3 a 4, obr. 22.

Tabulka 3 Odpovědi studentů na otázku 8

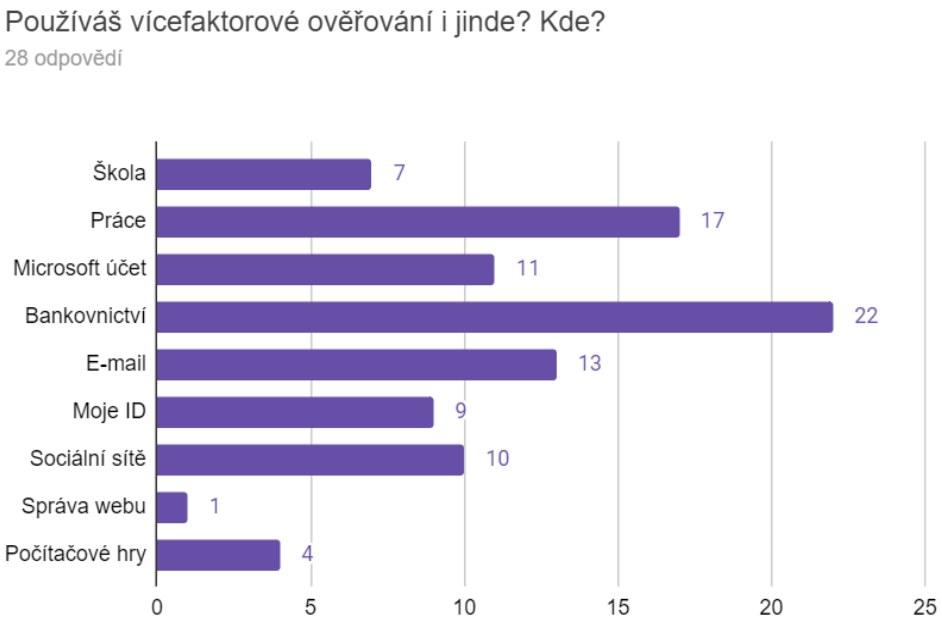
Jak a kde jsi našel návod na instalaci MFA? (napiš kroky nalezení)
Nehledal jsem
Návod byl v e-mailu.
V příloze mailu
E-mail od administrátora univerzitní sítě – stačilo jen postupovat krok za krokem
V e-mailu v příloze
Odkaz v mailu, na webu a umím to z práce
V informačním emailu byl návod dost strohý, tak jsem šel na Intranet do sekce IT služby - Multifaktorová autentizace, kde je v článku odkaz na "Bázi znalostí na univerzitním ServiceDesku" a níže ve článku byla příloha "MFA popis a navod.pdf" s daným návodem.
Zaslané v emailu.
Již jsem o něm věděla
Google
Intranet

Zdroj: vlastní

Tabulka 4 Odpovědi studentů na otázku 9

Napiš svůj názor, jak lehce/těžko se MFA instalovalo podle návodu. Napiš také, jaké jsi měl s instalací problémy, pokud jsi nějaké měl, své pocity z manuálu.
Nepoužil jsem návod
Šlo o klasické nastavení, jak u ostatních aplikací.
Vše bylo v pořádku a během chvíle nastaveno
Už nějakou dobu využívám aplikaci Microsoft Authenticator, takže nastavení MFA bylo jednoduché.
Podle návodu jsem vše zvládla snadno a rychle. Žádný problém nenastal.
Problém byl s nalogováním
Jelikož již mám ověřování pro Microsoft účet, tak postup byl defacto identický.
Musel jsem si bohužel proklikat stránku s nastavením, pro mě dodaný návod nebyl dobře sepsán.
Lehce, bez problému
Celkem v pohodě, věž patřičných problémů
Lehká instalace. Bez problému. Manuál je sepsán dobře.

Zdroj: vlastní



Obrázek 22 Hodnocení otázky 11

Zdroj: vlastní

5.6 Testování a hodnocení použitelnosti manuálu pro nastavení MFA

5.6.1 Testování manuálu

Testování manuálu (viz příloha č. 1) proběhlo pomocí statického testování, tedy se provedly takové úkony, při kterých není třeba spustit aplikaci MFA nebo jinou webovou aplikaci. Stačí otevřít pouze dokument Word, ve kterém je napsaná uživatelská příručka.

Úkony, které se provedly dne 8. února 2023:

- zda dokument obsahuje gramatické chyby,
- zda odkazy na další informace fungují,
- kontrola struktury manuálu,
- zda se dají texty napsat přesněji,
- porovnání návodu s aplikacemi.

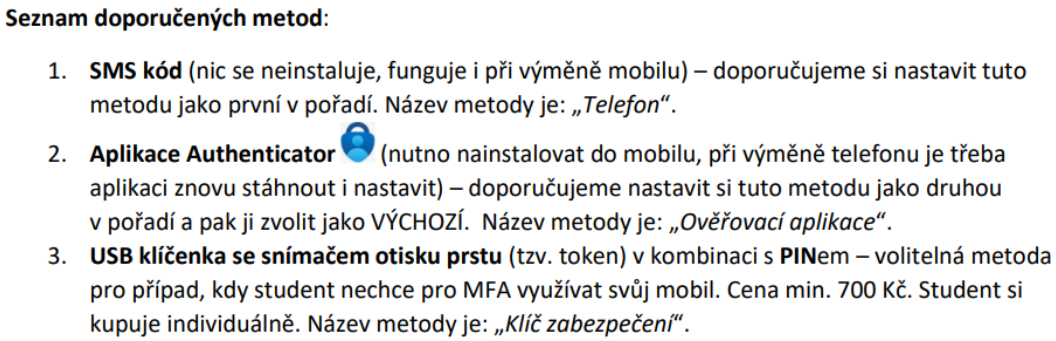
Kontrola anglického textu nebyla součástí testu, protože autorka nemá schopnosti certifikovaného překladatele.

Dne 17. dubna 2023 bylo zjištěno z rozhovoru s CITS, že dokument viz příloha č. 1 nelze dle nich brána jako návod, ale jako informativní článek o tom, jaké změny a jak budou probíhat na Univerzitě Pardubice. Avšak z dotazníku pro studenty, vyplynulo, že právě tento dokument se studentům jeví jako návod k nastavení autentizačních metod.

5.6.2 Hodnocení manuálu

Při testování byly zjištěny tyto nedostatky:

1. Lidé mluvící jiným jazykem než češtinou a slovenštinou, nepoznají, co se pod názvem manuálu skrývá, bylo by lepší, kdyby manuál nejprve obsahoval českou verzi, a ihned pod českým odstavcem byl anglický překlad.
2. Manuál neobsahuje informace, jak si nainstalovat MFA, tedy není dostatečně použitelný. Je třeba vytvořit detailní popis nastavení multifaktorové autentizace.
3. Pokud v manuálu odkazujeme například na video instalace MFA, je dobré ho nazvat např. „Návod instalace MFA – video“ místo „Nastavení multifaktorového ověřování (MFA) - ALVAO (upce.cz)“.
4. Seznam doporučených metod by bylo lepší nazvat dle toho, jak se nazývají při instalaci, tj. např. SMS kód (původní návod) ale „Telefon“, tudíž by to uživatele při instalaci nemátlo. Pokud bychom to nechali tak, jak je v původním návodu, uživatel by nemusel tuto informaci zachytit a musel by se vracet stále na vysvětlovací stránku metod.
5. Autentizační metody vyjmenované v návodu jsou pouze tři, ale v aplikaci s URL https://mysignins.microsoft.com/security-info je metod pět viz obr. 23. Toto by mělo být sjednocené, protože uživatele v tomto případě může návod nebo aplikace zmást. Avšak ne všichni studenti mohou být zmateni, protože studenti studující doktorský program se mohou přihlašovat pomocí metody např. kancelářský telefon, protože na půdě univerzity jsou jak studenti, tak zaměstnanci univerzity. Bohužel omezit metody pouze na segmenty není možné, protože univerzita používá řešení Microsoft Azure, kde prostředí nemůže být změněno.

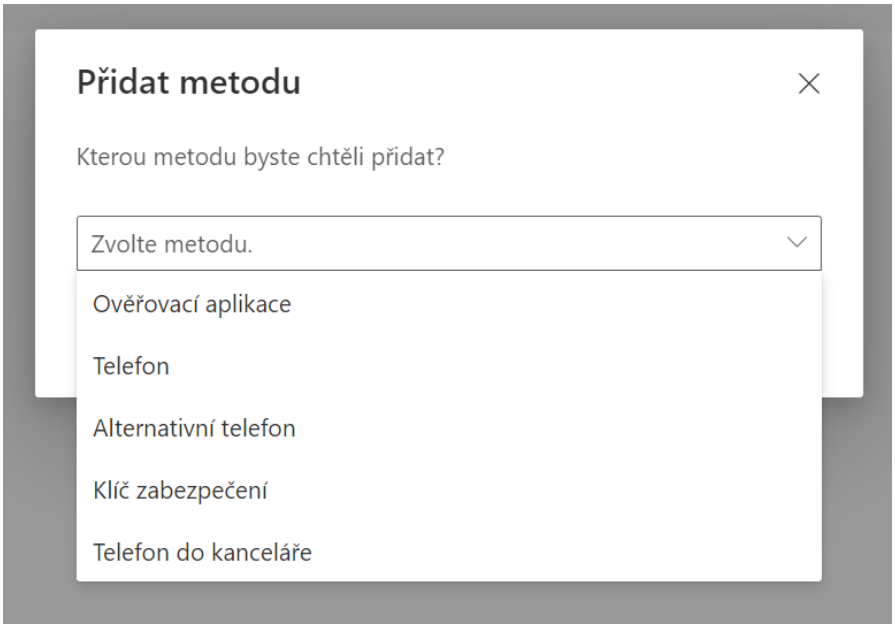


Seznam doporučených metod:

1. **SMS kód** (nic se neinstaluje, funguje i při výměně mobilu) – doporučujeme si nastavit tuto metodu jako první v pořadí. Název metody je: *„Telefon“*.
2. **Aplikace Authenticator** (nutno nainstalovat do mobilu, při výměně telefonu je třeba aplikaci znovu stáhnout i nastavit) – doporučujeme nastavit si tuto metodu jako druhou v pořadí a pak ji zvolit jako VÝCHOZÍ. Název metody je: *„Ověřovací aplikace“*.
3. **USB klíčenka se snímačem otisku prstu** (tzv. token) v kombinaci s **PIN**em – volitelná metoda pro případ, kdy student nechce pro MFA využívat svůj mobil. Cena min. 700 Kč. Student si kupuje individuálně. Název metody je: *„Klíč zabezpečení“*.

Obrázek 23 Výstřižek z návodu – autentizační metody

Zdroj: [20]



Obrázek 24 Autentizační metody na adrese https://mojeheslo.upce.cz/

Zdroj: [21]

5.7 Testování nastavení multifaktorové autentizace

5.7.1 Výběr testovacího vzorku koncových uživatelů

Na univerzitě jsou 3 skupiny lidí a to akademici, studenti a ostatní zaměstnanci.

Akademici jsou zaměstnanci univerzity mající za úkol vzdělávání studentů na UPa (pedagogická činnost). Mají vysokoškolské vzdělání. Také se věnující vědecké činnosti v rámci jejich zaměření, ve kterém se neustále vzdělávají. Mají přístup k citlivým údajům.

Studenti jsou ve věku 19-50 let v závislosti na tom, zda studují prezenčně či kombinovaně. Mají ukončené střední vzdělání ukončené maturitní zkouškou. Chtějí získat titul Bc., nebo Ing. podle toho, zda studují bakalářský, nebo navazující (magisterský) program. Stejně jako akademici, mají také přístup k citlivým údajům, především ke svým údajům jako je rodné číslo aj.

V poslední skupině jsou zaměstnanci, kteří zajišťující chod univerzity, jako administrativní pracovníci, asistentky, IT pracovníci, pracovnice úklidu, psycholog, správci budov aj. Přístup k citlivým informacím mají asistentky akademiků a studijní oddělení.

Jelikož se práce zabývá studenty, tak i v testování se vybral takový vzorek, a tím jsou přímo studenti UPa viz tabulka 1. Protože studenti mají své přihlašovací údaje, tudíž ke svému účtu budou přistupovat pouze oni s autorkou za jejich zády. Autorka samozřejmě dodržovala všechny bezpečnostní principy, tedy nepožadovala, aby ji testovací vzorek studentů sdílel jejich

přístupové údaje. Hesla nebyla viditelná pro autorku, tedy znaky byly nahrazeny znakem „*“. Výběr vzorku probíhal přímým oslovováním studentů na chodbách univerzity a také v internetových studentských skupinách na Facebooku, kde byly studenti osloveni hromadně, a to příspěvkem ve skupinách. K testování MFA byly vybráni ti studenti, kteří si ještě nenastavili žádnou autentizační metodu. Je to z toho důvodu, že zatím nezkoušeli projít proces nastavení a nastavit si jakoukoli autentizační metodu.

Tabulka 5 Testovací vzorek účastníků

Účastníci	Vzdělání	Věk	Pohlaví	Obor	Forma studia
1	SŠ	25	žena	IBS	kombinovaná
3	SŠ	27	muž	IBS	prezenční
2	SŠ	22	muž	APEL	prezenční
4	SŠ	30	žena	MP	kombinovaná
5	SŠ	30	muž	IBS	kombinovaná

Zdroj: vlastní

5.7.2 Testovací úkoly

Testovací úkoly byly vybrány a sestaveny tak, aby průchod úkolů na sebe logicky co nejvíce navazoval a aby bylo možné při vyhodnocení zjistit, zda lze najít manuál k nastavení MFA jednoduše a zda opravdu je manuál sepsán dostatečně detailně, že uživatel sám podle návodu bude schopný si autentizační metodu nastavit. V případě že se uživateli nepodařil úkol splnit, dostal doplňující otázky, aby autor mohl identifikovat problém a následně navrhnout řešení, a autor uživateli poskytl informace k tomu, aby úkol byl student schopný zvládnout. Úkoly nebyly záměrně popsány kroky, které byly ke splnění úkolu nutné.

Z hlediska multifaktorové autentizace se testovaly metody:

- aplikace Microsoft Authenticator,
- SMS.

Seznam testovacích úkolů:

1. Na intranetu Univerzity Pardubice najdi manuál pro instalaci a nastavení multifaktorového ověřování.
2. Nastav si metodu – SMS podle návodu, který jsi našel.
3. Přihlas se pomocí MFA na https://testmfa.upce.cz.
4. Přihlas se na Stag UPa pomocí MFA – SMS (pokud jsi přihlášen, nejprve se odhlas).
5. Odhlas se ze Stagu Upa.

6. Odeber metodu MFA – SMS a přidej si aplikaci Microsoft Authenticator (jakkoli).
7. Přihlas se na Stag pomocí MFA – Microsoft Authenticator (pokud jsi přihlášen, odhlas se).
8. Odhlas se ze Stagu UPa.

Studenti se zkoušeli přihlašovat pomocí multifaktorového ověřování na Stag Unverzity Pardubice, protože autorka této práce považuje tento informační systém, jako nejcitlivější, kde studenti mají uložené své např. rodné číslo, datum narození apod.

Od studentů se očekávalo, že používají informační systémy Univerzity Pardubice a jsou s nimi alespoň trochu sžiti. Předpokládalo se, že studenti neignorují informace od univerzity, které obdrží do své školní e-mailové schránky, tzn. že čtou zprávy v e-mailové schránce.

5.7.3 Průběh a hodnocení testovacích úkolů

Uživatelské testování na 5 studentech Univerzity Pardubice probíhalo od 20. března do 9. dubna, kdy nebylo nastavení alespoň jedné autentizační metody povinné. Samotné testování probíhalo na počítačích jednotlivých studentů v klidném prostředí např. u nich doma. Jako testovací prostředí se stanovilo anonymní okno ve webovém prohlížeči Google Chrome. Anonymní okno prohlížeče by nemělo být afektováno žádným nastavením, které již uživatel ve svém standardním prohlížeči má nastaveno. Splnění úkolů dle jednotlivých účastníků je v tabulce č. 6.

Tabulka 6 Splnění testovacích úkolů účastníky

Číslo	Úkol	Participanti				
		1	2	3	4	5
1	**Na intranetu Univerzity Pardubice najdi manuál pro instalaci a nastavení multifaktorového ověřování**	Ano	Ano	Ne	Ne	Ano
2	**Nastav si metodu – SMS podle návodu, který jsi našel**	Ne	Ano	Ano	Ne	Ano
3	**Přihlas se pomocí MFA na testmfa.upce.cz**	Ano	Ano	Ano	Ano	Ano
4	**Přihlas se na Stag UPa pomocí MFA – SMS (pokud jsi přihlášen, nejprve se odhlas)**	Ne	Ne	Ne	Ne	Ne
5	**Odhlas se ze Stagu UPa**	Ano	Ano	Ano	Ano	Ano

6	**Odeber metodu MFA – SMS a přidej si aplikaci Microsoft Authenticator (jakkoli)**	Ano	Ano	Ano	Ano	Ano
7	**Přihlas se na Stag pomocí MFA – Microsoft Authenticator (pokud jsi přihlášen, odhlas se)**	Ne	Ne	Ne	Ne	Ne
8	**Odhlas se ze Stagu UPa**	Ano	Ano	Ano	Ano	Ano

Zdroj: vlastní

Student č. 1

Testování úkolů proběhlo 20. března 2023.

Student se zvládl přihlásit do informačního systému intranet UPa. Student nepoužil funkci vyhledat, ale v menu zvolil „IT služby“. Po kliknutí na „IT služby“ se mu zobrazila stránka, kde vpravo nahoře je dlaždice „Multifaktorová autentizace“ a klikl na tlačítko „Ověření identity“. Tam se ale nachází článek „Multifaktorová autentizace“. Hned jak to student viděl, vrátil se na hlavní stránku, kde v sekce Důležité našel článek „Změna ve VPN připojení“, ve kterém našel odkaz „Jak jsme Vás již informovali“, který ho přesměroval na článek „Důležité upozornění pro studenty – změna přihlašování do informačních systémů“, kde byl další odkaz „Změny v přihlašování studentů – PDF. Po kliknutí se mu zobrazil soubor PDF, který obsahuje návod k nastavení multifaktorové autentizace. Nejednalo se však o návod krok za krokem, ale pouze hrubé informace o nastavení metod autentizace. Student dle návodu nebyl schopný nastavit metodu Telefon, protože v návodu nebylo uvedeno, na jakou dlaždici měl kliknout. Po nápovědě kliknul na „Bezpečnostní údaje“, avšak opět v návodu nebyl dostatek informací, jak si metodu přidat. Obdržel další nápovědu a to, že si měl metodu nainstalovat dle své intuice. Nakonec bez problému si metodu Telefon nastavil. Verifikační aplikace ho autentizovala. Po přihlášení do Stagu po něm multifaktorová autentizace nebyla vyžadována, pouze stačilo zadat ID a heslo. Následně se odhlásil. Poté již ne s návodem ale opět dle své intuice odebral metodu SMS a nastavil si metodu pomocí aplikace Microsoft Authenticator. Pak se zkusil autentizovat do informačního systému Stag pomocí aplikace, kde po něm opět autentizace nebyla vyžádána. Na konec se ze Stagu odhlásil.

Student č. 2

Testování úkolů proběhlo 24. března 2023.

Student č. 2 se jako studen č. 1 zvládl přihlásit do informačního systému intranet UPa, kde použil funkci vyhledávání k nalezení návodu k nastavení multifaktorové autentizace. Hledal spojení „Multifaktorová autentizace“, kde mu systém zobrazil tři články. Student klikl na poslední článek „Multifaktorová autentizace“. V článku byly základní informace o MFA a asi uprostřed klikl na odkaz „Báze znalostí na univerzitním ServiceDesku“, který ho přesměroval na portál Alvao, kde našel soubor „mfa popis a návod.pdf“, který obsahuje krok za krokem, jak si MFA nastavit. Metodu Telefon se mu podařilo nastavit podle návodu, který našel na intranetu. Následně se přihlásil do testovací aplikace testmfa.upce.cz, kde si vyzkoušel ověření identity. Poté si zvládl odebrat metodu a nastavit si místo ní metodu Ověřovací aplikace. To podle návodu zvládl také, avšak přihlásit se do systému Stag pomocí MFA se mu nepodařilo. Systém nevyžadoval potvrzení identity studenta.

Student č. 3

Testování úkolů proběhlo 25. března 2023.

Student u prvního úkolu nevěděl, jak se dostat na intranet Univerzity Pardubice. To bylo velice překvapující, protože se předpokládalo, že student zná všechny informační systémy univerzity, kde se ukládají informace např. o harmonogramu akademického roku. Tedy mu byla poskytnuta nápověda, jak se na tento informační systém dostane. Po přihlášení do systému využil funkci vyhledat, aby zkusil najít návod, jak si nastavit multifaktorovou autentizaci. Vyhledal spojení „multifaktorová autentizace“, což mu našlo 3 výsledky, kde zvolil odkaz na článek „Nasazení multifaktorové autentizace“, ve kterém kliknul na odkaz Servicedesku a to ho přesměrovalo na portál Alvao, kde na konci stránky nalezl návod na nastavení MFA. Jelikož se jednalo o návod tzn. krok za krokem, Nastavení metody SMS zvládl. Následně byl vyzván, aby se přihlásil pomocí nově nastavené multifaktorové autentizace na verifikační portál testmfa.upce.cz, aby si ověřil, že mu funguje MFA. Přihlášení na tento portál proběhlo úspěšně, byla požadována autentizace přes SMS. Dále byl požádán, aby zkusil splnit úkol č. 4 a to, přihlásit se do informačního systému Stag. Zde systém vyžadoval zadání studentova ID a jeho hesla, ale multifaktorová autentizace přes SMS již potřeba nebyla. Po tomto zjištění se uživatel ze systému odhlásil. Dalším úkolem bylo odebrání autentizační metody Telefon a nastavení nové metody Ověřovací aplikace. To student zvládl také. Následně se přihlásil opět na Stag

Univerzity Pardubice, kde ani přes aplikaci Microsoft Authenticator nebyla autentizace vynucena. Pak se ze systému odhlásil.

Student č. 4

Testování úkolů proběhlo 30. března 2023.

Student se zvládl přihlásit na intranet univerzity. Návod našel v krátkém čase. Na hlavní stránce intranetu se podíval do sekce Důležité, kde jsou informace, které by student neměl minout, tam našel článek „Změna ve VPN připojení“, ve kterém našel odkaz „Jak jsme Vás již informovali“, který ho přesměroval na článek „Důležité upozornění pro studenty – změna přihlašování do informačních systémů“, kde byl další odkaz „Změny v přihlašování studentů – PDF. Po kliknutí se mu zobrazil soubor PDF, který obsahuje návod k nastavení multifaktorové autentizace. Avšak tento návod neobsahoval postup krok za krokem, ale pouze informace o MFA. Návod byl velice stručně popsán. Student podle návodu, který našel na intranetu, se pokusil nastavit autentizační metodu SMS, avšak nebyl schopen nastavení dokončit, protože hned po kliknutí na odkaz mojeheslo.upce.cz nevěděl na kterou dlaždici kliknout, protože se mu zdálo, že by mohl kliknout na tři dlaždice, které mu dávaly signály, že právě v nich by mohlo být nastavení multifaktorové autentizace. Byly to dlaždice „Bezpečnostní údaje“, „Nastavení a ochrana osobních údajů“, a „Moje přihlášení“. Zde mu byla dána nápověda, a to informování ho, že nastavení nalezne v dlaždici „Bezpečnostní údaje“. Poté zkoušel nastavit autentizační metodu Telefon – SMS, to se mu také nepodařilo, protože v návodu nejsou dostatečné informace, jak tuto metodu nastavit. Byl tedy vyzván, aby si metodu zkusil nainstalovat intuitivně. Poté tento úkol zvládl. Ověřovací aplikace testmfa.upce.cz ho bez problémů autentizovala. Ale poté se snažil přihlásit na Stag, tam ale autentizace vynucena nebyla stejně jako u předchozích studentů. Následně si odstranil metodu SMS a nastavil si metodu Ověřovací aplikace. V návodu opět nebyly dostatečné informace, a tak zkusil nastavit sám. To zvládl téměř bez problémů, pouze jediný zádrhel, a to že na prvním kroku, který systém spustil, byl odkaz „Stáhnout hned“, na který klikl. Student očekával, že se mu stáhne aplikace, to se ale nestalo a místo toho se mu zobrazila stránka, kde si mohl načíst QR kód, aby se mu aplikace nainstalovala. Tedy uživatel z nápovědy, kterou spustil systém, nepoznal, že si aplikaci má stáhnout do svého telefonu. Následně prošel všechny kroky, které systém ukazoval a aplikaci nainstaloval. Poté se zkusil přihlásit znovu do Stagu, kde po něm opět nebyla autentizace vyžadována. Pak se ze systému odhlásil.

Student č. 5

Testování úkolů proběhlo 1. dubna 2023.

Student se zvládl přihlásit do informačního systému intranet UPa. Student na hlavní stránce, kde v sekce Důležité našel článek „2. připomínka změn v přihlašování studentů k informačním systémům“, ve kterém je odkaz „jak jsme vás již informovali“, a ten studenta přesměroval na článek „Důležité upozornění pro studenty – změna přihlašování do informačních systémů“. Tam je odkaz na soubor PDF „Změny v přihlašování studentů – PDF. Po kliknutí se mu zobrazil soubor PDF, který obsahuje návod k nastavení multifaktorové autentizace. Nejednalo se však o návod krok za krokem, ale pouze hrubé informace o nastavení metod autentizace. Student dle návodu nebyl schopný nastavit metodu Telefon, protože v návodu nebylo uvedeno, na jakou dlaždici měl kliknout. Po nápovědě kliknul na „Bezpečnostní údaje“, avšak opět v návodu nebyl dostatek informací, jak si metodu přidat. Obdržel další nápovědu a to, že si měl metodu nainstalovat dle své intuice. Nakonec bez problému si metodu Telefon nastavil. Verifikační aplikace ho autentizovala. Po přihlášení do Stagu po něm multifaktorová autentizace nebyla vyžadována, pouze stačilo zadat ID a heslo. Následně se odhlásil. Poté již ne s návodem ale opět dle své intuice odebral metodu SMS a nastavil si metodu pomocí aplikace Microsoft Authenticator. Pak se zkusil autentizovat do informačního systému Stag pomocí aplikace, kde po něm opět autentizace nebyla vyžádána. Na konec se ze Stagu odhlásil.

5.7.4 Nalezené nedostatky

1. Informační systémy ihned po nastavení autentizační metody nevyžadují multifaktorovou autentizaci. Autentizace by měla být vyžadována ihned, jak se student přihlásí do jakéhokoli systému Univerzity Pardubice, a má ji již nastavenou. To znamená, že pokud si student nastaví autentizační metodu např. 25.3.2023 v 10:00, a hned poté např. 25.3.2023 v 10:05 se pokusí přihlásit do jakéhokoli systému UPa nezávisle na tom, zda jde o desktopovou aplikaci či pouze internetovou, aby ověřil nastavení autentizační metody, tak autentizace by měla být vyžádána a nepřihlásit studenta bez ověření jeho identity. Pravděpodobně existuje prodleva mezi nastavením autentizační metody a propsáním do databáze, která uchovává informace o studentovi, na základě, které autentizační server ověřuje identity studentů. Dne 17. dubna 2023 bylo na základě rozhovoru s CITS zjištěno, že opravdu existuje prodleva mezi tím, kdy si student nastaví autentizační metodu a tím, kdy se po studentovi již bude MFA vyžadovat. Další zjištění od CITS bylo, že pokud student před nastavením metody

povolí systému, aby zůstal přihlášen, tak systém po nastavení metody a zaktivování MFA nemusí po studentovi být multifaktorová autentizace nemusí být vyžadována. Tedy logika, proč a za jakých okolností systém po studentovi může a nemusí multifaktorovou autentizaci vyžadovat.

2. Články o multifaktorové autentizaci by měly obsahovat návod, podle kterého je student schopný si bez pomoci nastavit autentizační metody. Nyní takové články obsahují návod je pro zkušené studenty v nastavování MFA.
3. Někteří studenti nepoužívají všechny informační systémy Univerzity Pardubice.
4. Některé články na intranetu nejsou studentům zpřístupněné – nemají práva k zobrazí příspěvků.

5.8 Seznam doporučení na základě testování

Seznam nalezených chyb a navrhovaných řešení byl vytvořen v programu Microsoft Word s rozšířenými prvky z Microsoft Excel, aby byla zajištěna přehlednost.

Tabulka 7 Seznam nalezených nedostatků a jejich návrh na úpravu

Číslo	Chyba	Návrh řešení
1	**Hlavní web UPa: článek „Multifaktorová autentizace“** Informace a návod k nastavení MFA se nachází uprostřed dlouhého článku, který uživatel pravděpodobně nepřečte dokonce.	Informace a návod s nastavením MFA přesunout do horní části, nebo na něj z první části odkazovat.
2	**Hlavní web Upa: článek „Nasazení multifaktorové autentizace MFA“** Článek je psaný spíše pro zaměstnance univerzity než pro studenty už kvůli tomu, že jedno z nejčastějších slov v ní je slovo „zaměstnanec“ a jeho varianty. Návod je v tomto článku k dohledání, ale je zde riziko, že čtenář, je-li to student, může usoudit, že v něm nenajde to, co hledá, už kvůli slovu zaměstnanec. Také už název článku může být zavádějící, protože informuje o nasazení MFA do praxe a mohl by pojednávat o statistice bezpečnosti za použití této metody.	Viz návrh řešení č. 1. Změnit název na výstižnější. V případě, že je článek určen spíše zaměsntnacům než veřejnosti a studetům, bylo by dobré je o tom informovat již na začátku článku, nebo takový článek zobrazovat spíše např. na zaměstnaneckém intranetu.
3	**Hlavní web Upa: bez použití fukce vyhledávání nelze najít články o multifaktorovém ověřování** Hlavní web UPa je velice komplexní a hledání konkrétních informací je velice těžko použitelné.	Doporučuji zjednodušit nabídku webu, např. stromovou strukturou. Všechny důležité informace by se měly uchovávat v horní části webu např. v sekci Novinky.

4	**Studentský intranet: komplexní portál, k nalezení určitých informací je nutné již web znát.** Intranet je příliš komplexní a uživatel v něm špatně a dlouho hledá informace, které hledá.	Možné řešení by mohlo být zjednodušení intranetu např. tak, že pokud se klikne na záložku IT služby, tak uživatel dostane všechny informace či návody, odkazy apod. na jednom místě o které předpokládá, že tam takové informace o např MFA nalezne.
5	**Studentský intranet: úvodní stránka není přehledná** Na první pohled nelze říci, zda jsou na úvodní stránce nějaké důležité informace, které by se student měl dozvědět.	Sekci Důležité bylo lepší dát blíže k navigačnímu menu. Dlaždice Wi-Fi apod. by bylo lepší odstranit. Sekci Novinky zmenšit.
6	**Studentský intranet: špatný design – informace v sekci Důležité na úvodní stránce jsou přehlédnutelné** Intranet je designován v červeno-bílém návrhu, stejně tak i část s důležitými informacemi, které by neměly být přehlédnutelné. Tedy je tu riziko, že student si tyto informace nikdy nepřečte, protože je jednoduše neuvidí.	Bylo by dobré, kdyby se změnily použité barvy v intranetu. Červená, která se téměř všude, evokuje, že je něco důležité, avšak opravdu důležité informace se na intranetu ztratí a uživatel je nevnímá jako důležité. Bylo by lepší, kdyby pouze sekce Důležité nebo důležité informace byly zvýrazněné např. červeně, a ostatní části, které jsou v současné době červené, byly např. oranžové.
7	**Studentský intranet: nepřehlednost v sekci Novinky** V sekci je spoustu článků a informací, avšak najít např. článek o vícefaktorové autentizaci je nemožné. Sekce obsahuje úplně všechny informace o dění na univerzitě. Jejich četnost taková, že studenti tuto sekci pravděpodobně nečtou.	Odstranit staré a již nerelevantní informace a články.
8	**Studentský intranet: tlačítko "Ověření identity" nemá očekávanou funkci** Klikneme-li na záložku "IT služby" zobrazí se nám stránka Centrum informačních technologií a služeb (číslo 1 v obr. 7), kde najdeme Multifaktorová autentizace (číslo 2 v obr. 7). To ale uživatele informuje pouze o tom, co autentizace znamená. V případě, že student klikne na tlačítko „Ověření identity osoby“ (číslo 3 v obr. 7), intranet ho přesměruje na článek Multifaktorová autentizace nacházející se na webu www.upce.cz	Tlačítko "Ověření identity" by mělo směřovat na ověření identity, tedy na aplikaci ověření, že studentovi funguje multifaktorové ověřování.

9	**Studentský intranet: ve výsledcích vyhledávání se zobrazí i nerelavatní články apod.** Použijeme-li funkci vyhledávání nad navigací stejně jako tomu bylo v předchozí kapitole, tak ve výsledcích vyhledávání nalezneme 19 článků pro slovo autentizace viz obr 10. Ne ale všechny se týkají právě vícefaktorové autentizace a také ne každý odkaz by se měl zobrazit na studentském intranetu.	Výsledky vyhledávání by měly odpovídat hledanému výrazu a nezobrazovat výsledky, které jsou mimo téma. Zde závisí na tom, jak je vyhledávač vytvořen a zda se hledaný výraz hledá v názvu článku nebo v celém textu.
10	**Studentský intranet: k některým odkazům studenti nemají právo k zobrazení** Studentům se po kliknutí na odkaz článku či článek zobrazí hlaška "Přístup zamítnut.". Například URL článku Studijní program Systémové inženýrství a informatika neindikuje, že by studentovi po jeho rozkliknutí měl být přístup odepřen, protože URL je https://studenti.upce.cz/fes/studijni-program-systemove-inzenyrstvi-informatika, kde subdoména je „studenti“ a ani neobsahuje podsložku zaměstnanci.	Nezobrazovat odkazy na články apod, ke kterým studenti nemají přidělené právo k zobrazení a zároveň studentům přidělit právo k zobrazení k článkům, které jsou pro ně určeny. Nezobrazovat články apod., které nejsou určeny pro studenty.
11	**Studentský intranet: chybně sestavená struktura URL a zobrazující se články určené zaměstnancům na studentském intranetu** Odkazy, které by se neměly zobrazovat na studentském intranetu jsou například „Přehled schůzek výboru“, nebo „Informace manažera kybernetického bezpečnosti“, protože subdoména URL těchto odkazů vyvolává dojem, že https://studenti.upce.cz obsahuje pouze informace pro studenty udělené správcem intranetu. Zde by bylo dobré, kdyby zaměstnanecký intranet měl svou subdoménu např. https://zamestnanci.upce.cz. Druhý důvod je i to, že za subdoménou se nachází slovo zaměstnanci např. https://studenti.upce.cz/zamestnanci/..., což také indikuje, že takové odkazy nejsou určeny studentům. Tedy by bylo vhodné takové odkazy, články aj. přesunout na zaměstnanecký intranet.	Viz návrh řešení č. 9, 10 a upravit strukturu tvorby URL.
12	**Manuál od IT z emailu: dvojjazyčný manuál není vhodně uspořádán** Lidé mluvící jiným jazykem než češtinou a slovenštinou, nepoznají, co se pod názvem manuálu skrývá.	Bylo by lepší, kdyby manuál nejprve obsahoval českou verzi, a ihned pod českým odstavcem byl anglický překlad.
13	**Manuál od IT z emailu: nedostatečné pokyny k instalaci multifaktorové autentizace** Manuál neobsahuje detailní informace, jak si nainstalovat MFA, tedy není dostatečně použitelný.	Je třeba vytvořit detailní popis nastavení multifaktorové autentizace.

14	**Manuál od IT z emailu: nepřesně pojmenované odkazy** V manuálu jsou nepřesně pojmenované odkazy, tzn. že z názvů uživatel okamžitě nepozná, co se pod nimi skrývá.	Pokud v manuálu odkazujeme například na video instalace MFA, je dobré ho nazvat např. „Návod instalace MFA – video“ místo „Nastavení multifaktorového ověřování (MFA) - ALVAO (upce.cz)“.
15	**Manuál od IT z emailu: zmatečný popis metod MFA** V manuálu jsou nepřesně pojmenované metody MFA, tzn. že uživatel z názvů okamžitě nepozná, co za metodu si vybrat.	Seznam doporučených metod by bylo lepší nazvat dle toho, jak se nazývají při instalaci, tj. např. SMS kód (původní návod) ale „Telefon“, tudíž by to uživatele při instalaci nemátlo. Pokud bychom to nechali tak, jak je v původním návodu, uživatel by nemusel tuto informaci zachytit a musel by se vracet stále na vysvětlovací stránku metod.
16	**Uživatelské testování: informační systémy nevyžadují MFA** Informační systémy ihned po nastavení autentizační metody nevyžadují multifaktorovou autentizaci.	Autentizace by měla být vyžadována ihned, jak se student přihlásí do jakéhokoli systému Univerzity Pardubice, a má ji již nastavenou.
17	**Uživatelské testování: články obsahují návod, který není dostatečně detailní.**	Mít pouze jeden návod, který bude obsahovat krok za krokem, jak si MFA nastavit a odkazovat na něj ze všech článků v informačních systémech Univerzity Pardubice
18	**Uživatelské testování: studenti nepoužívají všechny informační systémy Univerzity Pardubice**	Buď univerzita zajistí, že studenti budou používat všechny informační systémy od 1. ročníku, nebo může všechny informace z intranetu spojit se systémem Stag do jedné aplikace, a tudíž intranet by bylo možné zrušit
19	**Uživatelské testování: Některé články na intranetu nejsou studentům zpřístupněné**	viz řešení 10
20	**Rozhovor s CITS: v případě zapomenutí mobilního telefonu (předpoklad student nemá token) se nelze jinak autentizovat** Pokud si student zapomene nebo ztratí mobilní zařízení, není možné, aby student ověřil svou identitu jinou metodou	Bylo by dobré, kdyby se vytvořilo řešení pro případ, že studenti ztratí nebo zapomenou mobilní zařízení. Např. by se studenti mohli autentizovat pomocí otázky např. „Kdo je rektorem Univerzity Pardubice?“.

Zdroj: vlastní

Závěr

Cílem této práce bylo navrhnout řešení zjištěných nedostatků použitelnosti a bezpečnosti vybraného webu na základě výsledků jeho testování. Nejprve se stanovilo, jaký web – informační systém bude testován, dle autorčina výběru se práce zaměřila na hlavní web Univerzity Pardubice (www.upce.cz), ne na fakultní weby; a na intranetový portál Univerzity Pardubice se zaměřením na multifaktorovou autentizaci. Pro testování procesu autentizace na Univerzitě Pardubice byla využita metodika, kterou si autorka zvolila a kterou při testování využila se zaměřením na studenty a autentizaci. V uživatelském testování se autorka zaměřila na proces nastavování multifaktorové autentizace na mobilní telefon, a to od hledání návodu na intranetu univerzity až po samotné ověření, zda bude multifaktorová autentizace vyžádána po jejím nastavení. Uživatelské testování probíhalo na pěti participantech, studentech, kteří byli ochotni toto testování provést. Na základě zjištěných nedostatků, jako je například vynucení multifaktorové autentizace při přihlášení po prvním nastavení nebo nedostatečně laický návod pro nastavení správné metody, který je mnohdy nedostupný pro studenty, byl na závěr práce vytvořen seznam s návrhem řešení každého problému. V práci také bylo také podrobně popsáno téma autentizace, kde Univerzita Pardubice využívá multifaktorové ověřování za pomoci softwarového tokenu, mobilní aplikace Microsoft Authenticator.

Testování použitelnosti hlavního webu a intranetu Univerzity Pardubice bylo ztíženo tím, že probíhalo na produkčním prostředí, které je dynamické v závislosti na tom, zda správci přidávali nebo odstraňovali nový obsah na těchto portálech. Proto jsou důležité datumy, které byly stanoveny u každého testování, které proběhlo, protože fungování webů se již mohlo lišit a to např. z důvodu, že byl odebrán starý obsah a navržen jiným obsahem nebo administrátoři změnili proces, který mohl ovlivnit web či proces nastavení autentizační metody. Navzdory těmto faktům proběhlo testování použitelnosti a bezpečnosti bez větších problémů, protože jádro platformy navrhlo studio Drupal Arts a kybernetická bezpečnost je realizována pomocí Microsoft Azure.

V případě testování informačních systémů, či jiných webových aplikací, je dobré začít testování již při jejich vývoji a brát v úvahu všechny aspekty, ve kterých mohou nastat problémy včetně kvalitního návrhu struktury, designu, použití, osoby, na které je systém cílen apod.

Tato práce se dále může zabývat tím, jak Univerzita Pardubice postupuje při nasazování multifaktorové autentizace, zmapovat a navrhnout zlepšení v procesech univerzity, aby v budoucnu chybám nalezených v této práci již nedocházelo.

Seznam použité literatury

[1] GRIMES, R.A., 2020. *Hacking Multifactor Authentication*. John Wiley & Sons.

[2] *Certified Tester Foundation Level* [online]. 2018 V3.1. International Software Testing Qualifications Board, 2019 [cit. 2023-06-10]. Dostupné z: https://castb.org/uploads/downloadables/_files_0/6__files_0.pdf

[3] *Vyhláška č. 523/2011 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb*. Národní bezpečnostní úřad. [cit. 28.1.2023] Dostupné na: https://www.nbu.cz/download/pravni-predpisy/vyhlaska-c-5232005-ve-zneni-4532011/container-nodeid-1968/52320054532011.docx&sa=U&ved=2ahUKEwiA4tq39IP9AhULif0HHcJmC1wQFnoECAEQAQ&usg=AOvVaw3FA_u2JFFuJhJ8jpSR-QS7

[4] HUB, Miloslav. Univerzita Pardubice. Ekonomicko-správní fakulta. *Bezpečnost a ochrana informací v prostředí internetu*. Pardubice: Univerzita Pardubice, 2013, 89 s. : il. ; 30 cm. ISBN 978-80-7395-701-8.

[5] GAŠPARÍK, Petr. Vícefaktorová autentizace. *Security World*. Internet Info DG, 2014, 2014(4).

[6] Univerzita Pardubice. *Drupal Arts* [online]. 8. 9. 2018 [cit. 2023-04-13]. Dostupné z: https://drupalarts.cz/portal-univerzity-pardubice

[7] ČERMÁK, Miroslav. Bezpečnost-náklady-použitelnost. *Clever and Smart* [online]. 2012, 11.12.2012 [cit. 2023-02-07]. Dostupné z: https://www.cleverandsmart.cz/bezpecnost-naklady-pouzitelnost/

[8] CRANOR, Lorrie Faith a Simson GARFINKEL, ed. *Security and usability: designing secure systems that people can use*. Sebastopol: O'Reilly, c2005. ISBN 0-596-00827-9.

[9] Ověřování vs. autorizace. *Microsoft* [online]. 2022, 05. 12. 2022 [cit. 2023-02-07]. Dostupné z: https://learn.microsoft.com/cs-cz/azure/active-directory/develop/authentication-vs-authorization

[10] PŘIBYL, Jiří a Jindřich KODL. *Ochrana dat v informatice*. Praha: Vydavatelství ČVUT, 1996. ISBN 80-01-01664-1.

[11] *Co je to heslo?* [online]. [cit. 2023-02-07]. Dostupné z: https://it-slovnik.cz/pojem/heslo/?utm_source=cp&utm_medium=link&utm_campaign=cp

[12] ŠTRÁFELDA, Jan. Heslo. *Štráfelda* [online]. Dostupné z: https://www.strafelda.cz/heslo#jak-hesla-obvykle-vytvarime

[13] SUMRAK, Jesse. SMS Verification: What It Is & How It Works. *Twilio* [online]. 12.12.2022 [cit. 2022-04-13]. Dostupné z: https://www.twilio.com/blog/what-is-sms-verification

[14] *YubiKey Authentication Module Design Guideline* [online]. 7.5.2012, 20 [cit. 2023-04-13]. Dostupné z: https://resources.yubico.com/53ZDUYE6/as/pvknxfcmgb2kv6bjw8pvp2k/YubiKey-Authentication-Module-Design-Guideline-v10.pdf

[15] PILKA, Lukáš. Velký průvodce uživatelským testováním webů a aplikací. *BlueGhost* [online]. 05. 12. 2019 [cit. 2023-04-13]. Dostupné z: https://www.blueghost.cz/clanek/velky-pruvodce-uzivatelskym-testovanim-webu-a-aplikaci/

[16] VOJÁK, Michal. Jak dělat uživatelské testování. *Design Dev* [online]. 15. 9. 2020 [cit. 2023-04-13]. Dostupné z: https://designdev.cz/jak-delat-uzivatelske-testovani

[17] Co je: Vícefaktorové ověřování. *Microsoft* [online]. [cit. 2023-04-13]. Dostupné z: https://support.microsoft.com/cs-cz/topic/co-je-v%C3%ADcefaktorov%C3%A9-ov%C4%9B%C5%99ov%C3%A1n%C3%AD-e5e39437-121c-be60-d123-eda06bddf661

[18] Bezpečnostní politika hesel a vícefaktorová autentizace. System Online [online]. 15. 12. 2016 [cit. 2023-04-13]. Dostupné z: https://m.systemonline.cz/it-security/bezpecnostni-politika-hesel-a-vicefaktorova-autentizace.htm

[19] BUREŠ, Miroslav, Miroslav RENDA, and Michal DOLEŽEL. *Efektivní testování softwaru: klíčové otázky pro efektivitu testovacího procesu*. Grada Publishing as, 2016.

[20] *Změna v přihlašování studentů k informačním systémům* [online]. Pardubice: Univerzita Pardubice, 4 [cit. 2023-04-13].
Dostupné z: https://studenti.upce.cz/sites/default/files/zmeny_v_prihlasovani_studentu_195866.pdf

[21] Bezpečnostní údaje. Security info Microsoft [online]. [cit. 2023-04-13]. Dostupné z: https://mysignins.microsoft.com/security-info

[23] Studentský intranet Univerzity Pardubice [online]. Pardubice: Univerzita Pardubice [cit. 2023-04-13]. Dostupné z: https://studenti.upce.cz/

[24] MALKUSOVÁ, Tereza. *Testování použitelnosti díl 2: Testuji, tedy jsem* [online]. 21.09.2015 [cit. 2023-05-21]. Dostupné z: https://www.aitom.cz/co-je-noveho/testovani-pouzitelnosti-dil-2

[25] *What is Security Testing?* [online]. [cit. 2023-05-21]. Dostupné z: https://www.sisainfosec.com/blogs/10-types-of-security-testing-techniques/

Seznam příloh

Příloha č. 1 Manuál k instalaci multifaktorové autentizace obdržený e-mailem od IT oddělení

Příloha č. 2 Opatření rektora č 4/2022

Příloha 1

Změna v přihlašování studentů k informačním systémům

English version follows.

Aktuální stav

Přístup k informačním systémům univerzity, jako je např. e-mail, intranet, STAG, je studentům umožněn po zadání univerzitních přihlašovacích údajů, kterými jsou uživatelské jméno (dále NetID – ve tvaru st12345) a heslo.

Podrobnější informace: NetID | Univerzita Pardubice (upce.cz)

Chystaná změna

Po zadání NetID a hesla budou studenti muset přihlášení potvrdit dalším způsobem. Tento princip, známý např. z internetového bankovnictví, se označuje jako tzv. **MULTIFAKTOROVÁ AUTENTIZACE** (dále **MFA**). Zavedení **MFA** na UPCE proběhne v několika krocích a jeho důvodem je zvýšení zabezpečení přihlašování.

Podrobnější informace: Multifaktorová autentizace (MFA) | Univerzita Pardubice (upce.cz)

Krok 1 – Výběr metody

Od 5. 12. 2022 si studenti mohou **vybrat a zaregistrovat metodu**, kterou chtějí použít pro MFA, a to na adrese https://mojeheslo.upce.cz.

Seznam doporučených metod:

1. **SMS kód** (nic se neinstaluje, funguje i při výměně mobilu) – doporučujeme si nastavit tuto metodu jako první v pořadí. Název metody je: *„Telefon“*.
2. **Aplikace Authenticator** (nutno nainstalovat do mobilu, při výměně telefonu je třeba aplikaci znovu stáhnout i nastavit) – doporučujeme nastavit si tuto metodu jako druhou v pořadí a pak ji zvolit jako VÝCHOZÍ. Název metody je: *„Ověřovací aplikace“*.
3. **USB klíčenka se snímačem otisku prstu** (tzv. token) v kombinaci s **PIN**em – volitelná metoda pro případ, kdy student nechce pro MFA využívat svůj mobil. Cena min. 700 Kč. Student si kupuje individuálně. Název metody je: *„Klíč zabezpečení“*.

Od okamžiku, kdy si studenti metodu zaregistrují, mohou být při přihlašování, např. do e-mailu, vyzváni k potvrzení přihlášení danou metodou.

Funkčnost MFA lze otestovat přihlášením na https://testmfa.upce.cz.

Podrobnější informace: Nastavení multifaktorového ověřování (MFA) - ALVAO (upce.cz)

Krok 2 – Změna přihlašování do VPN

Od 13. 2. 2023 se studenti nebudou moci přihlásit do VPN bez využití MFA. Tato fáze se dotkne studentů, kteří využívají VPN pro vzdálený přístup např. k terminálovým serverům.

Pokud student VPN nevyužívá, nebude jeho přihlašování ještě nijak omezeno. Pokud VPN bude chtít použít, může si MFA nastavit i po 13. 2. 2023.

Podrobnější informace: VPN na UPCE | Univerzita Pardubice

Krok 3 – Povinná MFA od 1. 10. 2023

Od 1. 10. 2023 bude **nastavení MFA povinné** pro všechny studenty a ovlivní **všechny informační systémy** univerzity. Pokud si studenti do tohoto data MFA nenastaví, budou při prvním přihlášení vyzváni, aby tak ve lhůtě 7 dnů učinili.

Výhody MFA

Bezpečnost

Přihlašovací údaje zabezpečené pomocí MFA je mnohem těžší kompromitovat. (*Kvůli kompromitovaným přihlašovacím údajům musí IT odd. blokovat přihlašovací údaje každý týden u několika studentů. Vyřešení situace může zabrat i několik hodin či dní.*) Studenti, kteří si nastaví MFA, dosáhnou již v první fázi nejen většího zabezpečení připojení do VPN, ale i do e-mailových schránek.

Věnujte prosím pozornost zasílaným notifikacím. Při jakýchkoli pochybnostech ověření odmítněte.

Reset hesla svépomocí

Studenti, kteří budou mít nastavenou MFA, si budou moci zapomenuté heslo sami obnovit na adrese https://nastavheslo.upce.cz.

Podrobnější informace: Reset hesla / Password reset - ALVAO (upce.cz)

Podpora

ServiceDesk

Studenti mohou požádat o vyřešení problému s MFA zadáním požadavku do služby ServiceDesk.

Pomoc přes e-mail

Studenti mohou žádost o pomoc také zaslat na e-mailovou adresu servicedesk@upce.cz, nejedná se však o preferovaný způsob a doba vyřízení může být delší než v případě přímého zadání požadavku do ServiceDesku.

Change in student login to information systems

Current state

Students can access the UPCE information systems, such as e-mail, intranet, STAG, by entering their university login details, which are a username (NetID – in the form st12345) and password.

For details see: NetID | University of Pardubice (upce.cz)

Upcoming change

After entering the NetID and password, students will have to confirm their login in another way. This principle, known e. g. from internet banking, is called **MULTIFACTOR AUTHENTICATION** (**MFA**). The implementation of **MFA** at UPCE will take place in several steps and its reason is to increase login security.

For details see: Multifactor authentication | University of Pardubice (upce.cz)

Step 1 – Choose a method

From 5 December 2022, students can select and register the method they wish to use for the MFA at http://mypassword.upce.cz/.

List of recommended methods:

1. **SMS code** (nothing to install, works even if you replace your mobile phone) – we recommend setting this method first in order.
2. **Authenticator app** (must be installed on the phone, must be downloaded and set up again when replacing the phone) – we recommend setting this method second in order and then selecting it as the PRIMARY method.
3. **USB security key** (token) + **PIN –** optional method in case the student does not want to use his/her mobile phone for MFA. Price: 25 EUR at least. The student buys it individually.

From the moment students register the method, they may be asked to confirm their login via MFA (for example to an e-mail).

The functionality of MFA can be tested by logging on to https://testmfa.upce.cz

For details see: Setting up multifactor authentication (MFA) - ALVAO (upce.cz)

Step 2 – Change VPN login

From 13 February 2023, students will not be able to log into the VPN without using MFA. This phase will affect students who use the VPN for remote access e. g. to terminal servers.

If a student does not use a VPN, his login will still not be restricted in any way. If he/she wants to use the VPN, he/she can set up MFA after 13 February 2023.

For details see: VPN at UPCE | University of Pardubice

Step 3 – Obligatory MFA from 1 October 2023

From 1 October 2023, MFA will be obligatory for all students and will affect all information systems of the university. If students do not set up MFA by this date, they will be asked to do so within 7 days when they first log in.

Benefits of MFA

Security

Login credentials secured with MFA are much harder to compromise. (B*ecause of compromised logins, the IT department must block accounts for some students each week. It can take several hours or days to resolve the situation.*) Students who set up MFA will not only achieve greater security in the first phase of connecting to the VPN, but also to their e-mail inboxes.

Please pay attention to the notifications you receive. If you are in any doubt, decline verification.

Reset password by yourself

Students who set up MFA will be able to reset forgotten passwords by themselves at https://setpassword.upce.cz/.

For details see: Reset hesla / Password reset - ALVAO (upce.cz)

Support

ServiceDesk

Students can submit a request to the ServiceDesk to resolve an MFA issue.

Help via e-mail

Students can also send an e-mail request for assistance to servicedesk@upce.cz, however this is not the preferred method, and the response time may be longer.

Příloha 2

UNIVERZITA PARDUBICE	
Opatření rektora č. 4/2022	
Věc:	Zabezpečení uživatelských účtů zaměstnanců multifaktorovou autentizací
Působnost:	všechny útvary Univerzity Pardubice
Účinnost:	8. 4. 2022
Číslo jednací:	RPO/0010/22
Vypracoval a předkládá:	Ing. Jiří Slanina, manažer kybernetické bezpečnosti
Schválila:	doc. Ing. Liběna Černohorská, Ph.D., prorektorka pro vnitřní záležitosti

Článek 1

Úvodní ustanovení

1) Rektor Univerzity Pardubice (dále jen „univerzita“) vydává toto opatření za účelem zvýšení zabezpečení informačních systémů univerzity vzhledem k následujícím důvodům:

a) Univerzita je ve svěřené působnosti v oblasti veřejné správy orgánem veřejné moci, na který se vztahují ustanovení zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, a jeho prováděcích předpisů.
b) Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) v rámci preventivních kroků vydal v souvislosti s kritickou hrozbou kyberšpionáže a dalších kybernetických útoků varování, v němž nabádá organizace řídící se zákonem o kybernetické bezpečnosti, k ostražitosti proti nejčastěji používaným technikám útoků a k provedení aktualizace informačních systémů a jejich komponent tak, aby nedocházelo ke zneužití známých zranitelností.
c) V hodnocení kybernetických incidentů, které NÚKIB zveřejňuje na svých webových stránkách, je zmíněn rostoucí trend v kybernetické bezpečnosti v oblasti tzv. *phishingu*, *spear-phishingu* a sociálního inženýrství s následnou kompromitací uživatelských účtů.
d) V rámci porady vedení univerzity dne 13. 12. 2021 v návaznosti na doporučení Výboru pro kybernetickou bezpečnost byl ze strany vedení univerzity pověřen manažer kybernetické bezpečnosti koordinací zvýšení zabezpečení informačních systémů univerzity postupným nasazením multifaktorové autentizace (dále jen „MFA“) pro bezpečné přihlašování.

Článek 2

Harmonogram nasazení MFA

1) Rektor tímto opatřením ukládá vedoucím útvarů přímo podřízených rektorovi, prorektorům, kvestorovi nebo děkanům, aby:
   a) do 14 dnů od nabytí účinnosti tohoto opatření u zaměstnanců příslušného útvaru stanovili, jaký způsob zabezpečení (alespoň jedna metoda MFA) ve smyslu čl. 3 odst. 1 tohoto opatření bude u jednotlivých zaměstnanců použit, resp. v případě, kdy není metoda MFA u konkrétního zaměstnance vyžadována (nepřiděleno NetID/nepřistupuje k informačním systémům), zvolili variantu „nebude používat MFA“, a tuto informaci prostřednictvím formuláře dostupného na https://zamestnanci.upce.cz/uredni-sdeleni v sekci Výboru pro řízení kybernetické bezpečnosti předali manažerovi kybernetické bezpečnosti;
   b) nejpozději do 30. 4. 2022 zajistili, že zaměstnanci příslušného útvaru, kteří jsou vůči univerzitě v pracovním poměru, budou mít způsob zabezpečení stanovený dle písm. a) tohoto odstavce zaregistrovaný v portálu https://mojeheslo.upce.cz; podrobnosti způsobu registrace zvolené metody pro realizaci MFA jsou k dispozici v návodu pro MFA na https://servicedesk.upce.cz;
   c) nejpozději do 30. 9. 2022 zajistili, že jim podřízení zaměstnanci, jejichž vztah vůči univerzitě vyplývá z uzavřené dohody o provedení práce nebo dohody o pracovní činnosti, budou mít způsob zabezpečení stanovený dle písm. a) tohoto odstavce zaregistrovaný v portálu https://mojeheslo.upce.cz; podrobnosti způsobu registrace zvolené metody pro realizaci MFA jsou k dispozici v návodu pro MFA na https://servicedesk.upce.cz.
2) Rektor dále ukládá vedoucí OPM nejpozději do 30. 4. 2022 ve spolupráci s manažerem kybernetické bezpečnosti navrhnout a zrealizovat změny v dokumentech a postupech souvisejících se vznikem a skončením pracovněprávních vztahů, které zahrnou nastavení metody MFA a správu poskytnutých bezpečnostních tokenů do standardních procesů univerzity.
3) Rektor dále ukládá manažerovi kybernetické bezpečnosti ve spolupráci s Centrem informačních technologií a služeb (dále jen „CITS“) na základě dat získaných dle odst. 1 tohoto článku stanovit potřeby hardwarového vybavení a harmonogram nasazování MFA na jednotlivých fakultách, celouniverzitních útvarech a rektorátních útvarech (dále jen „harmonogram“) a informovat o něm vedení univerzity. Na základě harmonogramu ukládá CITS podniknout nezbytné kroky k jeho realizaci.
4) Aktuální seznam informačních systémů chráněných MFA vč. harmonogramu a seznam použitelných hardwarových prostředků včetně dalších podrobností je dostupný na https://zamestnanci.upce.cz/uredni-sdeleni v sekci Výboru pro řízení kybernetické bezpečnosti.

Článek 3

Způsob realizace MFA

1) MFA bude na univerzitě realizována některou z těchto metod:
   a) zasíláním potvrzovacích SMS kódů,
   b) využitím ověřovací aplikace nainstalované na chytrém mobilním telefonu nebo
   c) využitím fyzického zařízení pro elektronické ověření identity uživatele (tzv. bezpečnostní token).
2) Zaměstnanci, kterým je ze strany univerzity poskytován služební mobilní tarif, si zaregistrují metodu MFA podle odst. 1 písm. a) nebo b) tohoto článku prostřednictvím https://mojeheslo.upce.cz (návod pro MFA je k dispozici na https://servicedesk.upce.cz).
3) Zaměstnancům, kterým nebyl ze strany univerzity poskytnut služební mobilní tarif, univerzita v případě jejich zájmu umožní realizovat MFA prostřednictvím soukromého telefonu podle odst. 1 písm. a) nebo b) tohoto článku nebo soukromého bezpečnostního tokenu podle odst. 1 písm. c) tohoto článku.
4) Zaměstnancům, kterým nebyl ze strany univerzity poskytnut služební telefon a kteří neprojeví zájem o využití soukromého telefonu nebo soukromého bezpečnostního tokenu, bude zaregistrována MFA služebním bezpečnostním tokenem podle odst. 1 písm. c) tohoto článku v souladu s harmonogramem.
5) Technické požadavky a technickou podporu metody MFA poskytuje Oddělení správy výpočetní techniky.
6) Standardní proces pořizování a správu bezpečnostních tokenů podle odst. 1 písm. c) tohoto článku zajišťuje CITS. Žádost o poskytnutí bezpečnostního tokenu podá příslušný vedoucí zaměstnanec prostřednictvím univerzitního systému https://servicedesk.upce.cz.
7) Náklady spojené s pořízením bezpečnostního tokenu, případně služebního telefonu se hradí z prostředků útvaru, na kterém je příslušný zaměstnanec zaměstnán.

Článek 4

Závěrečná ustanovení

1) Toto opatření nabývá platnosti a účinnosti dnem podpisu rektora.

V Pardubicích dne 8. 4. 2022

prof. Ing. Libor Čapek, Ph.D.

rektor