

Strategie získávání nových klientů pro firemní řešení na evropském trhu

Adam Škodík

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Adam Škodík
Osobní číslo: A22127
Studijní program: B0688A140008 Informační technologie v administrativě
Forma studia: Prezenční
Téma práce: Strategie získávání nových klientů pro firemní řešení na evropském trh
Téma práce anglicky: Strategy for Acquiring New Clients for Corporate Solutions in the European Market

Zásady pro vypracování

- Vyhledejte potenciální partnery pro integraci řešení ProID na cílových trzích.
- Připravte prezentaci a oslovte vybrané partnery s návrhem spolupráce.
- Navrhněte strukturu landing page optimalizovanou pro konverzi návštěvníků.
- Implementujte A/B testování a PPC kampaně zaměřené na získávání nových klientů.
- Vyhodnoťte účinnost kampaní a návrhu stránky, analyzujte výsledky a doporučte optimální přístup.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. TOUHILL, Georgy J a C. Joseph TOUHILL. Cybersecurity for Executives: A Practical Guide. Wiley-AIChE, 2014. ISBN 9781118888148.
2. CLARKE, Adam. SEO 2023: Learn search engine optimization with smart internet marketing strategies. Simple Effectiveness, 2023. ISBN 979-8365383173.
3. CIALDINI, Robert B. Influence The Psychology of Persuasion. Harper Business, 2021. ISBN 9780063136892.
4. NIZICH, Michael. *The cybersecurity workforce of tomorrow*. Bingley, U.K. : Emerald Publishing Limited, 2023. ISBN 9781803829173.
5. MASON, Stephen a Daniel. Electronic Evidence and Electronic Signatures. University of London Press, 2021. ISBN 978-1911507222.
6. FANTI, Marco. Implementing Multifactor Authentication. Packt Publishing, 2023. ISBN 978-1803246963.
7. WIESSMAN, Jerry. *Presenting to win : the art of telling your story*. 3rd. Upper Saddle River : FT Press, 2009. ISBN 9780137144174.

Vedoucí bakalářské práce: **doc. Ing. Petr Šilhavý, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **4. prosince 2024**
Termín odevzdání bakalářské práce: **9. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Miroslav Matýšek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 4. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato bakalářská práce se zaměřuje na návrh a realizaci strategie získávání nových klientů pro řešení digitální identity ProID na evropském trhu v prostředí B2B. Cílem bylo identifikovat vhodné partnery pro integraci, připravit prezentaci řešení, navrhnout a optimalizovat konverzní landing page, implementovat A/B testování a PPC kampaně a následně vyhodnotit jejich účinnost. Teoretická část popisuje principy kybernetické bezpečnosti, moderní autentizační metody a přístupy k digitálnímu marketingu v segmentu B2B. Praktická část demonstruje výběr vhodného integračního partnera pomocí benchmarkingu, realizaci technické integrace, návrh a testování variant landing page a optimalizaci PPC kampaní. Výsledkem je doporučený akviziční postup založený na analytickém vyhodnocení jednotlivých komunikačních kanálů a konverzních prvků.

Klíčová slova: digitální identita, kybernetická bezpečnost, autentizace, B2B marketing, landing page, A/B testování, PPC kampaně, ProID, lead generation, integrace

ABSTRACT

This bachelor's thesis focuses on designing and implementing a client acquisition strategy for the digital identity solution ProID in the European B2B market. The objective was to identify suitable integration partners, prepare a product presentation, design and optimize a conversion-focused landing page, implement A/B testing and PPC campaigns, and evaluate their effectiveness. The theoretical section outlines the principles of cybersecurity, modern authentication methods, and digital marketing approaches in the B2B segment. The practical part demonstrates the selection of a suitable integration partner through benchmarking, execution of a technical integration, development and testing of landing page variants, and PPC campaign optimization. The result is a recommended acquisition strategy based on analytical evaluation of communication channels and conversion elements.

Keywords: digital identity, cybersecurity, authentication, B2B marketing, landing page, A/B testing, PPC campaigns, ProID, lead generation, integration

Touto cestou bych rád poděkoval všem, kteří mě během studia a psaní této bakalářské práce podporovali.

Především děkuji své rodině a přátelům za maximální podporu po celou dobu studia – jejich důvěra, trpělivost a povzbuzení pro mě znamenaly velkou oporu, zejména v náročnějších obdobích.

Velké poděkování patří také celému týmu ProID za možnost podílet se na reálném projektu. Díky jejich důvěře jsem měl příležitost vést samostatnou iniciativu a rozvíjet své odborné i osobní schopnosti. Spolupráce s tak inspirativními a schopnými lidmi pro mě byla nesmírně cenná zkušenost.

V neposlední řadě bych rád vyjádřil upřímné poděkování všem vyučujícím z Fakulty aplikované informatiky za předané znalosti a praktické zkušenosti. Zvláštní poděkování si zaslouží doc. Ing. Petr Šilhavý, Ph.D., vedoucí této bakalářské práce, za odborné vedení, cenné rady a trpělivost během celého procesu zpracování.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST.....	12
1 DIGITÁLNÍ IDENTITA A BEZPEČNOSTNÍ ŘEŠENÍ.....	13
1.1 VÝZNAM DIGITÁLNÍ IDENTITY.....	13
1.2 DŮLEŽITOST KYBERNETICKÉ BEZPEČNOSTI.....	14
1.3 IDENTITY AND ACCESS MANAGEMENT.....	15
1.4 MODERNÍ AUTENTIZAČNÍ METODY.....	16
1.4.1 Dvoufaktorová a více faktorová autentizace (2FA/MFA).....	16
1.4.2 FIDO 2 a přihlašování bez hesla.....	17
1.5 LEGISLATIVA V OBLASTI DIGITÁLNÍ IDENTITY.....	18
1.5.1 GDPR – Ochrana osobních údajů.....	18
1.5.2 eIDAS – Elektronická identifikace a podpis.....	19
1.5.3 Zajištění bezpečnosti a ISO.....	20
1.6 ÚVOD DO INTEGRACE BEZPEČNOSTNÍHO ŘEŠENÍ.....	21
1.7 SINGLE SIGN-ON (SSO).....	22
1.8 FEDERAČNÍ PROTOKOLY.....	22
1.8.1 SAML.....	22
1.8.2 OIDC.....	24
1.9 ŘEŠENÍ SPRÁVY IDENTITY.....	25
2 STRATEGIE AKVIZICE PARTNERŮ A ONLINE PREZENTACE ŘEŠENÍ.....	27
2.1 PARTNERSTVÍ JAKO FORMA AKVIZICE B2B PROSTŘEDÍ.....	27
2.2 MOŽNOSTI OSLOVOVÁNÍ FIREM.....	28
2.2.1 E-mailová komunikace.....	28
2.2.2 LinkedIn.....	28
2.2.3 Kontaktní formuláře a demo požadavky.....	28
2.2.4 B2B platformy jako G2 a Capterra.....	29
2.2.5 Online schůzka a prezentace řešení.....	29
2.3 LANDING PAGE JAKO NÁSTROJ KONVERZE.....	29
2.4 PPC A SEO JAKO NÁSTROJE PROPAGACE.....	30
2.5 A/B TESTOVÁNÍ.....	31
2.6 SHRNUTÍ.....	31
II PRAKTICKÁ ČÁST.....	33
3 VÝBĚR PARTNERA PRO INTEGRACI.....	34
3.1 KRITÉRIA VÝBĚRU SOFTWARE.....	34
3.2 PARAMETRY HODNOCENÍ SOFTWARE.....	35
4 ZÍSKÁVÁNÍ KONTAKTŮ A NAVÁZÁNÍ SPOLUPRÁCE.....	36

4.1.1	Komunikace s partnery.....	36
4.1.2	Přes „Demo“ žádost.....	39
4.1.3	Vyhledávání přes LinkedIn	39
4.2	PŘEDSTAVENÍ ŘEŠENÍ ONLINE.....	40
4.3	VYHODNOCENÍ KOMUNIKAČNÍCH KANÁLŮ.....	42
5	PROCES INTEGRACE.....	44
5.1	REALIZACE INTEGRACE S PROID	44
5.2	UKÁZKA PŘIHLÁŠENÍ.....	45
6	MARKETINGOVÁ AKTIVITA	47
6.1	BENCHMARKING LANDING PAGE KONKURENCE.....	47
6.2	NÁVRH VLASTNÍ LANDING PAGE.....	47
6.3	A/B TESTOVÁNÍ.....	50
6.3.1	Varianta A – původní verze landing page	50
6.3.2	Varianta B – optimalizovaná verze landing page.....	53
6.4	TVORBA WEBOVÉ STRÁNKY VE WORDPRESS	57
6.4.1	Tvorba grafických prvků	58
6.5	SHRNUTÍ OPTIMALIZACE DIGITÁLNÍ PREZENTACE.....	59
6.6	PLÁNOVÁNÍ A REALIZACE PPC KAMPANÍ	60
6.6.1	Nastavení PPC.....	61
6.6.2	A/B testování klíčových slov	63
6.6.3	Chování uživatele	65
7	VÝSLEDKY A VYHODNOCENÍ	67
7.1	DOPAD PROJEKTU	67
7.2	MOŽNOSTI DALŠÍHO ROZVOJE	67
7.3	PŘEKÁŽKY.....	67
7.4	NÁVRHY NA ZLEPŠENÍ DO BUDOUCNA	67
7.5	VLASTNÍ PŘÍNOS	68
	ZÁVĚR.....	69
	SEZNAM POUŽITÉ LITERATURY	70
	SEZNAM OBRÁZKŮ	73
	SEZNAM TABULEK.....	74
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	75

ÚVOD

Digitalizace stále více prostupuje podnikovým prostředím a s tím roste i důraz na bezpečnost a efektivní správu digitální identity. Organizace čelí rostoucím nárokům na ochranu citlivých dat, bezpečný přístup k informačním systémům a zároveň potřebují adekvátně komunikovat svá řešení směrem k cílovým trhům. Tyto požadavky jsou obzvláště výrazné v B2B segmentu, kde hraje klíčovou roli důvěra, technická kompetence a transparentnost komunikace.

Tato bakalářská práce se zaměřuje na konkrétní případ aplikace akviziční a komunikační strategie pro firemní řešení digitální identity ProID se zaměřením na expanzi na zahraniční trhy. Cílem bylo navrhnout a realizovat soubor aktivit vedoucích ke zvýšení povědomí o produktu, získání nových obchodních příležitostí a navázání spolupráce s potenciálními partnery. Využity byly nástroje jako webová prezentace, PPC kampaně, platforma G2 a další formy online marketingu.

Práce propojuje teoretický rámec kybernetické bezpečnosti a marketingu s praktickou realizací konkrétního projektu. Demonstruje, jak lze i s omezenými zdroji vytvořit účinnou marketingovou strategii v segmentu, kde je technická důvěryhodnost stejně podstatná jako samotný obchodní výsledek.

I TEORETICKÁ ČÁST

1 DIGITÁLNÍ IDENTITA A BEZPEČNOSTNÍ ŘEŠENÍ

Digitální identita představuje v současném firemním prostředí zásadní prvek pro správu uživatelských přístupů a ochranu citlivých informací. Už dávno nejde pouze o technický pojem, ale o strategickou oblast, která ovlivňuje každodenní provoz organizací a jejich schopnost čelit kybernetickým hrozbám. Správně nastavená digitální identita umožňuje efektivní řízení přístupových práv, minimalizuje riziko neoprávněného přístupu a zajišťuje splnění legislativních požadavků na ochranu dat [1].

V této kapitole je vysvětlen význam digitální identity ve firemním prostředí, její role při ochraně systémů a dat a souvislost s kybernetickou bezpečností. Důraz je kladen na to, proč je nezbytné digitální identitu spravovat a chránit, jaké hrozby vyplývají z její kompromitace a jaké mohou být dopady na chod firmy. Součástí kapitoly je i přehled typických rizik a útoků spojených se zneužitím identity, včetně konkrétních příkladů dopadů na organizace.

V závěrečné části je analyzována problematika integrace digitální identity do firemních procesů prostřednictvím moderních bezpečnostních technologií a autentizačních protokolů. Jsou popsány klíčové principy a nástroje využívané v praxi k ochraně přístupů, správě identit a prevenci kybernetických incidentů. Kapitola poskytuje základní rámec pro pochopení významu digitální identity jako jednoho z hlavních pilířů moderní kybernetické bezpečnosti a ukazuje, jak její správná správa přispívá k odolnosti organizací vůči aktuálním hrozbám.

1.1 Význam digitální identity

Digitální identita dnes představuje základní stavební kámen bezpečnosti v každé moderní organizaci. Nejde pouze o přihlašovací jméno a heslo, ale o komplexní soubor informací, které jednoznačně identifikují uživatele vůči systémům a službám – může jít o e-mail, certifikát, biometrické údaje, mobilní zařízení nebo jejich kombinaci. Správně nastavená digitální identita umožňuje efektivní řízení přístupů, zajišťuje ochranu citlivých dat a minimalizuje riziko zneužití práv v rámci firemního prostředí [1].

Ve firemní praxi digitální identita definuje, jaké má zaměstnanec role a oprávnění, ke kterým systémům a datům má přístup a jakým způsobem je jeho přístup ověřován. Díky tomu lze přesně nastavit, kdo může pracovat s citlivými informacemi, kdo má administrátorská práva a kdo například pouze omezený přístup k vybraným aplikacím.

Pokud není možné identitu uživatele spolehlivě ověřit, hrozí zneužití práv, únik dat nebo narušení provozu firmy [2].

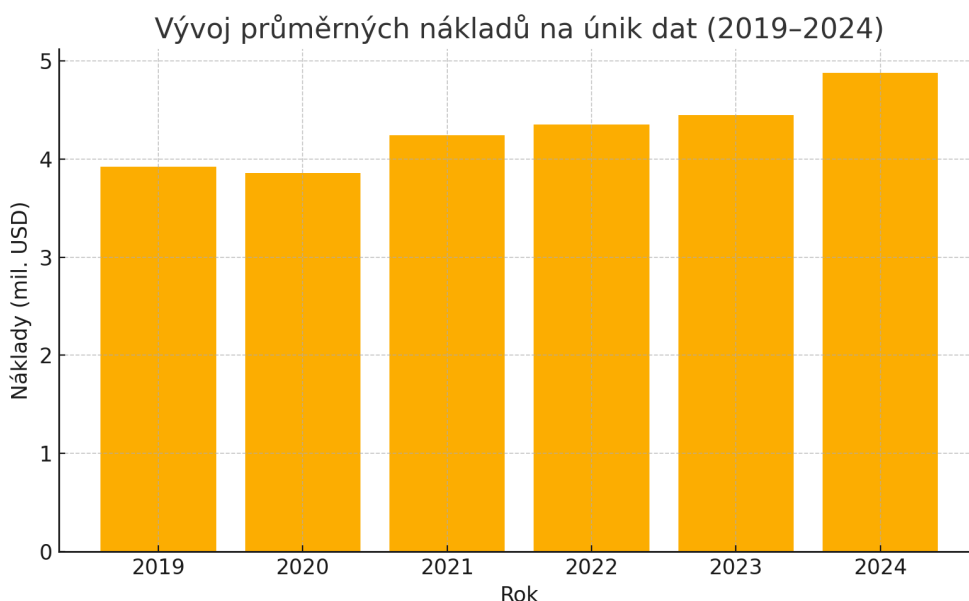
Výhodou moderní digitální identity je nejen zvýšení bezpečnosti, ale i zjednodušení každodenní práce zaměstnanců. Díky technologiím jako je vícefaktorová autentizace (MFA) nebo biometrické ověření často odpadá nutnost zadávat složitá hesla – uživatelé se mohou přihlašovat například pomocí mobilní aplikace nebo otisku prstu. To přispívá k vyššímu komfortu i bezpečnosti [3].

V souvislosti s rostoucím počtem online služeb a přesunem dat do cloudových prostředí se problematika správy digitální identity stává zásadní. Pro zajištění bezpečnosti již nestačí používat hesla – je nezbytné zavádět silné autentizační metody a nástroje umožňující bezpečné a uživatelsky přívětivé ověřování identity. Řádně chráněná digitální identita představuje základní předpoklad pro ochranu firemních systémů a zajištění plynulého provozu organizace [3].

1.2 Důležitost kybernetické bezpečnosti

Kybernetická bezpečnost je dnes klíčová pro ochranu firemní pověsti, ekonomickou stabilitu i dlouhodobou konkurenceschopnost. Úspěšný kybernetický útok může vést nejen ke ztrátě dat a finančním škodám, ale také k poškození důvěry zákazníků, poklesu tržeb a v krajním případě až k úpadku firmy. Reputace organizace může být po incidentu poškozena na roky dopředu a návrat ke stejné úrovni důvěry je často velmi obtížný. Prevence, včasná detekce a efektivní reakce na incidenty jsou proto zásadními prvky řízení kybernetických rizik.

Podle zprávy IBM Cost of a Data Breach Report 2024 dosáhly celosvětové průměrné náklady na únik dat rekordní hodnoty 4,88 milionu dolarů [4]. Tento trend je dlouhodobě rostoucí, jak ukazuje Obrázek 1, který byl zpracován na základě údajů ze zmíněné zprávy. Náklady zahrnují nejen technické a právní výdaje, ale také ztráty způsobené přerušením provozu, odchodem zákazníků a poškozením pověsti. Právě tyto skryté dopady často znamenají pro firmy největší ztráty a mohou výrazně ovlivnit jejich postavení na trhu.



Obrázek 1 Průměrné náklady na únik dat

(Vlastní zpracování na základě dat z [4])

1.3 Identity and Access Management

Identity and Access Management (IAM) označuje soubor pravidel, procesů a technologií sloužících k bezpečné správě digitálních identit uživatelů a řízení jejich přístupu k informačním systémům a datovým zdrojům. Hlavním cílem je zajistit, aby každý uživatel disponoval přístupem pouze k těm prostředkům, které jsou nezbytné pro výkon jeho pracovní role, a aby byl tento přístup bezpečně ověřován.

Základními stavebními kameny IAM jsou autentizace a autorizace. Autentizace ověřuje, že uživatel je skutečně tím, za koho se vydává – například pomocí hesla, biometrických údajů nebo vícefaktorového ověření. Autorizace pak určuje, k jakým systémům, aplikacím nebo datům má uživatel přístup na základě jeho pracovní pozice nebo potřeb. IAM systémy také umožňují efektivní správu uživatelských účtů po celou dobu jejich životního cyklu – od vytvoření účtu při nástupu zaměstnance, přes změny oprávnění až po odebrání přístupů při jeho odchodu z organizace [5].

Moderní IAM řešení přinášejí centralizovanou správu identit, automatizaci nastavování oprávnění a pravidelný audit přístupů. To významně zvyšuje úroveň bezpečnosti, snižuje riziko neoprávněného přístupu a zároveň usnadňuje splnění legislativních požadavků na

ochranu dat. IAM je tak klíčovým prvkem každé strategie kybernetické bezpečnosti a nezbytným nástrojem pro ochranu firemních i osobních informací v digitálním prostředí [5].

1.4 Moderní Autentizační Metody

Moderní autentizační metody tvoří základní prvek ochrany digitální identity a firemních systémů. Vzhledem k rostoucímu počtu útoků zaměřených na prolomení nebo odcizení hesel je tradiční spoléhání na hesla považováno za nedostatečné. V důsledku toho dochází k zavádění pokročilejších autentizačních mechanismů [1].

Mezi nejčastěji využívané moderní metody patří vícefaktorová autentizace (MFA), biometrické ověření (například otisk prstu nebo rozpoznání obličeje), přihlašování pomocí bezpečnostních klíčů (například FIDO2) a využití elektronických certifikátů. Tyto přístupy kombinují různé typy ověřovacích údajů – například něco, co uživatel ví (heslo nebo PIN), něco, co má (mobilní zařízení, token), a něco, čím je (biometrie). Díky tomu výrazně zvyšují úroveň zabezpečení přístupu a zároveň zjednodušují uživatelskou zkušenost [6].

Zavádění moderních autentizačních metod je dnes považováno za standardní součást firemní bezpečnostní politiky a významně přispívá k ochraně před nejčastějšími typy kybernetických útoků [5].

1.4.1 Dvoufaktorová a více faktorová autentizace (2FA/MFA)

Vícefaktorová autentizace (Multi-Factor Authentication, MFA) je v současnosti jedním z nejúčinnějších způsobů zabezpečení přihlašování do informačních systémů. Hlavní princip spočívá v tom, že uživatel při přihlašování musí prokázat svou identitu pomocí alespoň dvou různých typů ověřovacích údajů, které se obecně dělí do tří základních kategorií [7]:

- Něco, co uživatel ví (something you know): například heslo, PIN nebo odpověď na bezpečnostní otázku.
- Něco, co uživatel má (something you have): například mobilní telefon s autentizační aplikací, hardwarový token, čipová karta nebo bezpečnostní klíč.
- Něco, čím uživatel je (something you are): biometrické údaje, jako je otisk prstu, rozpoznání obličeje nebo sken oční duhovky.

V praxi to znamená, že například po zadání hesla je uživatel vyzván k zadání jednorázového kódu z mobilní aplikace nebo k biometrickému ověření. Pokud by útočník získal jeden z těchto faktorů (například heslo), stále potřebuje i další faktor, aby získal

přístup do systému. Díky tomu MFA výrazně snižuje riziko úspěšného útoku, jako je phishing nebo zneužití odcizených údajů [7].

Moderní autentizační systémy umožňují přizpůsobit požadavky na MFA podle citlivosti dat, typu aplikace nebo míry rizika konkrétního přihlášení. Vícefaktorová autentizace je dnes doporučována nejen odborníky, ale bývá i požadavkem legislativy a bezpečnostních standardů. Její zavedení významně zvyšuje ochranu firemních systémů a citlivých dat, aniž by výrazně komplikovalo uživatelskou zkušenost [8, 9].

Další kapitola je zaměřena na jednotlivé autentizační faktory, které tvoří základ.

1.4.1.1 Biometrie a elektronické certifikáty

Biometrické metody autentizace využívají jedinečné fyzické nebo behaviorální charakteristiky uživatele, jako jsou otisky prstů, rozpoznání obličeje, sken oční duhovky nebo hlasová biometrie. Hlavní výhodou biometrie je, že tyto údaje jsou pro každého člověka unikátní a nelze je snadno zkopírovat nebo zapomenout. Díky tomu poskytuje biometrická autentizace vysokou úroveň jistoty, že přístup získává skutečně oprávněná osoba. Moderní systémy často využívají biometrické ověření lokálně na zařízení uživatele, což minimalizuje riziko zneužití biometrických dat. Zároveň je biometrie velmi uživatelsky přívětivá, protože nevyžaduje zadávání hesel ani nošení dalších zařízení [10].

Elektronické certifikáty představují další silný autentizační faktor, který je založen na asymetrické kryptografii. Každý uživatel má přiřazený unikátní certifikát vydaný důvěryhodnou certifikační autoritou, který slouží nejen pro bezpečné přihlašování, ale i pro elektronické podepisování dokumentů nebo šifrování komunikace. Výhodou elektronických certifikátů je jejich vysoká úroveň bezpečnosti a možnost integrace do firemního prostředí, například při přístupu do VPN, firemních aplikací nebo při komunikaci s veřejnou správou. Elektronické certifikáty jsou také klíčovým prvkem pro splnění legislativních požadavků, například v rámci nařízení eIDAS [9, 11].

Obě tyto metody – biometrie i elektronické certifikáty – patří mezi nejspolehlivější způsoby ověřování identity a často se používají v kombinaci s dalšími autentizačními faktory v rámci vícefaktorové autentizace [11].

1.4.2 FIDO 2 a přihlašování bez hesla

FIDO2 je moderní autentizační standard, který umožňuje bezpečné přihlašování do systémů bez nutnosti zadávat tradiční hesla. Tento přístup je postaven na využití silné kryptografie a

ověřování identity pomocí zařízení, které uživatel vlastní, například bezpečnostního klíče, biometrie (otisk prstu, rozpoznání obličeje) nebo chytrého telefonu. FIDO2 kombinuje protokoly WebAuthn a CTAP, což umožňuje ověřit uživatele na základě asymetrického šifrování – soukromý klíč zůstává bezpečně uložený na zařízení uživatele a nikdy neopouští jeho úložiště, zatímco veřejný klíč je sdílen s ověřovanou službou [12].

Přihlašování bez hesla výrazně zvyšuje úroveň bezpečnosti, protože eliminuje rizika spojená se slabými, opakovaně používanými nebo odcizenými hesly. FIDO2 je odolné vůči phishingu, útokům typu man-in-the-middle i dalším běžným metodám zneužití přístupových údajů. Díky podpoře v moderních prohlížečích a operačních systémech lze FIDO2 nasadit jak v podnikových, tak v cloudových a spotřebitelských aplikacích. Firmy tak mohou nabídnout uživatelům jednoduché a bezpečné přihlašování, které snižuje nároky na správu hesel a zároveň splňuje nejprísnější bezpečnostní standardy [6, 12].

1.5 Legislativa v oblasti Digitální Identity

Směrnice NIS2 představuje aktuální evropský rámec pro zvýšení ochrany sítí, informačních systémů a digitálních služeb napříč EU. Oproti předchozí verzi výrazně rozšiřuje okruh organizací, kterých se požadavky týkají - nově zahrnuje například digitální infrastrukturu, veřejnou správu či výrobní sektor. V praxi to znamená, že více firem bude muset zavádět opatření v oblasti řízení kybernetických rizik, správy přístupových práv a ochrany identity.

V rámci směrnice NIS2 je stanovena povinnost zavedení vícefaktorové autentizace, pravidelného školení zaměstnanců a důsledného řízení bezpečnostních rizik, a to nejen uvnitř organizací, ale i u jejich dodavatelů. Větší odpovědnost je přenesena na vedení organizací. Tyto požadavky představují jak výzvu, tak příležitost pro poskytovatele řešení správy identity, jako je ProID [13].

1.5.1 GDPR – Ochrana osobních údajů

Obecné nařízení o ochraně osobních údajů, známé jako GDPR (General Data Protection Regulation), představuje základní právní rámec pro ochranu osobních údajů v rámci celé Evropské unie. Nařízení vstoupilo v platnost v roce 2018 a jeho hlavním cílem je zajistit, aby organizace nakládaly s osobními údaji fyzických osob transparentně, bezpečně a v souladu se zákonem. Z pohledu digitální identity GDPR klade důraz zejména na ochranu údajů, které se týkají identity zaměstnanců, jejich přístupových údajů a aktivit v rámci firemních systémů.

V rámci nařízení GDPR jsou definovány klíčové principy, které je nutné dodržovat při zpracování osobních údajů - mezi nejvýznamnější patří minimalizace údajů, zákonnost, integrita, důvěrnost a odpovídající zabezpečení přístupů. Zvláštní důraz je kladen na správné nastavení autentizace, řízení přístupových práv a ochranu dat při přihlašování do systémů. Podle článku 32 GDPR je požadováno přijetí vhodných technických a organizačních opatření odpovídajících míře rizika - včetně vícefaktorové autentizace, šifrování, auditů přístupů či školení zaměstnanců [13].

Zaměstnanci často používají přístupové údaje, jako jsou uživatelská jména, logy nebo IP adresy, které jsou podle GDPR považovány za osobní údaje. Organizace proto musí zajistit, že tyto informace jsou chráněné nejen technicky, ale i procesně – například omezením přístupových práv, nastavením interních pravidel nebo pravidelným školením zaměstnanců. GDPR rovněž zdůrazňuje princip tzv. odpovědnosti (accountability), což znamená, že firma musí být schopna prokázat, že s osobními údaji nakládá správně a bezpečně. V praxi to znamená například vedení záznamů o přístupech, dokumentaci bezpečnostních opatření a schopnost doložit, kdo má ke konkrétním údajům přístup a proč [14].

Nástroje pro správu digitální identity, jako jsou systémy Identity and Access Management (IAM) nebo elektronické certifikáty, významně usnadňují naplnění požadavků GDPR - umožňují efektivní řízení přístupů, auditovatelnost a transparentnost v nakládání s osobními údaji. Správně nastavené procesy a technologie tak nejen snižují riziko úniku dat, ale také pomáhají firmám splnit legislativní povinnosti a posilují důvěru zaměstnanců i zákazníků [5].

1.5.2 eIDAS – Elektronická identifikace a podpis

Nařízení eIDAS představuje klíčový evropský právní rámec, který upravuje oblast elektronické identifikace, autentizace a důvěryhodných služeb v digitálním prostředí napříč členskými státy Evropské unie. Cílem nařízení eIDAS je zajistit, aby bylo možné bezpečně a právně závazně ověřovat identitu osob a organizací, podepisovat dokumenty a poskytovat elektronické služby bez ohledu na hranice jednotlivých států EU [11].

Jedním z hlavních přínosů eIDAS je zavedení tří úrovní elektronických podpisů – jednoduchého, zaručeného (advanced) a kvalifikovaného (qualified). Právě kvalifikovaný elektronický podpis má podle nařízení stejnou právní váhu jako vlastnoruční podpis a je uznáván ve všech členských státech. Pro jeho vytvoření je nutné využít kvalifikovaný

certifikát vydaný důvěryhodnou certifikační autoritou a bezpečné prostředky pro vytváření podpisu, například čipové karty nebo speciální aplikace [11].

Nařízení eIDAS dále podporuje vzájemné uznávání elektronických identit mezi členskými státy, což umožňuje občanům i firmám bezpečně přistupovat ke službám veřejné správy nebo komerčních subjektů v celé EU. Pro firmy to znamená možnost využívat jednotné mechanismy pro ověřování uživatelů, elektronické podepisování smluv či faktur a zajištění právní jistoty v digitálních procesech. eIDAS tak významně přispívá k rozvoji digitální ekonomiky, zvyšuje důvěru v elektronické služby a usnadňuje přeshraniční obchod i komunikaci [13].

1.5.3 Zajištění bezpečnosti a ISO

Zajištění bezpečnosti ve firemním prostředí nespočívá pouze v dodržování BOZP, ale zahrnuje také důsledné zabezpečení identity zaměstnanců, které je s ohledem na rostoucí četnost kybernetických útoků považováno za kritickou oblast, zejména ve velkých podnicích.

Aby organizace splňovaly určitou úroveň bezpečnosti a měly správně nastavené procesy, vznikla ISO rodina standardů, která se zabývá kybernetickou bezpečností.

Rodina standardů ISO/IEC 27000 představuje mezinárodní rámec pro řízení bezpečnosti informací v organizacích všech velikostí a typů. Tyto standardy, vyvíjené Mezinárodní organizací pro normalizaci (ISO) a Mezinárodní elektrotechnickou komisí (IEC), pomáhají organizacím zavádět, udržovat a neustále zlepšovat systémy řízení bezpečnosti informací (ISMS, Information Security Management System). Hlavním cílem je chránit důvěrnost, integritu a dostupnost informací a minimalizovat rizika spojená s kybernetickými hrozbami, lidskými chybami i technologickými zranitelnostmi [15].

Centrálním prvkem této rodiny je norma ISO/IEC 27001, která stanovuje požadavky na vytvoření, implementaci, provoz, monitorování a neustálé zlepšování ISMS. Organizace, které tuto normu implementují, získávají systematický přístup k identifikaci a řízení rizik, nastavují bezpečnostní politiky a procesy, a pravidelně hodnotí účinnost svých opatření. ISO 27001 je zároveň jedinou normou z této řady, na kterou lze získat oficiální certifikaci, což organizaci umožňuje prokázat svým zákazníkům, partnerům i regulatorním orgánům, že přistupuje k ochraně informací zodpovědně a v souladu s mezinárodními standardy [16].

Nová verze ISO/IEC 27001:2022 přináší důraz na řízení rizik, zapojení zaměstnanců do kultury bezpečnosti a rozšiřuje sadu kontrolních mechanismů například o oblasti cloudových služeb, ochranu osobních údajů nebo monitoring aktivit. Součástí normy je také příloha s konkrétními bezpečnostními opatřeními (Annex A), která zahrnuje například řízení přístupových práv, šifrování, správu incidentů či školení zaměstnanců [16].

Zavedením systému řízení bezpečnosti informací (ISMS) dle normy ISO 27001 jsou organizacím poskytovány výhody v podobě efektivnějšího řízení bezpečnostních rizik, posílení důvěry zákazníků a partnerů a splnění legislativních požadavků v oblasti ochrany dat. Důraz je kladen na pravidelné audity, neustálé zlepšování a přizpůsobení politik aktuálním hrozbám a potřebám organizace [17].

Vedle základní normy ISO 27001 existují i další specializované standardy této rodiny, například ISO 27002 (doporučení a osvědčené postupy pro implementaci bezpečnostních opatření), ISO 27005 (řízení rizik v oblasti informační bezpečnosti) nebo ISO 27017 a ISO 27018 (bezpečnost a ochrana osobních údajů v cloudových službách) [17].

Celkově je rodina ISO 27000 v současnosti považována za základní nástroj pro systematické a efektivní řízení kybernetické bezpečnosti v moderních organizacích a představuje jasný rámec pro ochranu informací v digitálním věku.

1.6 Úvod do integrace bezpečnostního řešení

Integrace bezpečnostních řešení představuje zásadní krok pro efektivní ochranu firemních dat a správu digitální identity v moderním podnikovém prostředí. Nestačí pouze nasadit jednotlivé bezpečnostní technologie – klíčové je jejich propojení s existujícími systémy a procesy tak, aby bylo možné centrálně řídit přístupy, zajišťovat auditovatelnost a splnit legislativní požadavky na ochranu informací. Jak uvádí Jašek, úspěšná integrace vyžaduje nejen technické znalosti, ale i pochopení organizačních potřeb a bezpečnostních standardů.

V této souvislosti hrají zásadní roli tzv. federační protokoly, jako jsou SAML nebo OpenID Connect, které umožňují bezpečné ověřování identity napříč různými aplikacemi a službami. Právě tyto protokoly zajišťují jednotné přihlašování (Single Sign-On) a efektivní správu uživatelských identit napříč firemním ekosystémem. Podrobný popis principů a výhod federačních protokolů bude rozpracován v následujících kapitolách [18].

1.7 Single Sign-On (SSO)

Mezi hlavní výhody přihlašovacího mechanismu SSO patří výrazné zjednodušení přístupového procesu, kdy je vyžadováno zapamatování pouze jedné sady přihlašovacích údajů. Po ověření identity je automaticky umožněn přístup k navazujícím systémům bez nutnosti opakovaného zadávání údajů. Tím dochází ke zvýšení uživatelského komfortu a současně ke snížení rizik spojených s používáním slabých nebo opakovaných hesel.

Z bezpečnostního hlediska SSO umožňuje centrálně řídit a auditovat přístupy, což usnadňuje správu uživatelských účtů a rychlou reakci při změně oprávnění nebo odchodu zaměstnance. Implementace SSO je v praxi často realizována pomocí federačních protokolů, jako jsou SAML nebo OpenID Connect, které zajišťují bezpečné předávání informací o identitě mezi jednotlivými systémy a poskytovateli služeb. Díky tomu je SSO dnes považováno za standardní součást moderního firemního prostředí a klíčový prvek efektivní správy digitální identity [18].

1.8 Federační protokoly

Single Sign-On (SSO) umožňuje uživatelům přihlásit se pouze jednou a následně získat přístup k více aplikacím nebo službám bez nutnosti opakovaného zadávání přihlašovacích údajů. Tento princip je postaven na spolupráci mezi poskytovatelem identity a poskytovatelem služby. Uživatel se ověří u IdP a následně může bezpečně přistupovat k dalším systémům, které důvěřují tomuto poskytovateli identity.

V praxi je SSO realizováno především prostřednictvím federačních protokolů, jako jsou SAML (Security Assertion Markup Language) a OpenID Connect (OIDC). Tyto protokoly umožňují bezpečné předávání informací o identitě mezi IdP a SP, čímž zajišťují, že uživatel nemusí spravovat více účtů nebo hesel napříč různými systémy. Federativní identita tak uživatelům umožňuje rychlý, spolehlivý a bezpečný pohyb napříč různými aplikacemi a službami. Klíčovým prvkem je shoda a důvěra mezi identitou uživatele u IdP a požadavky SP, což zajišťuje bezpečnost i pohodlí při každodenním používání firemních systémů [19].

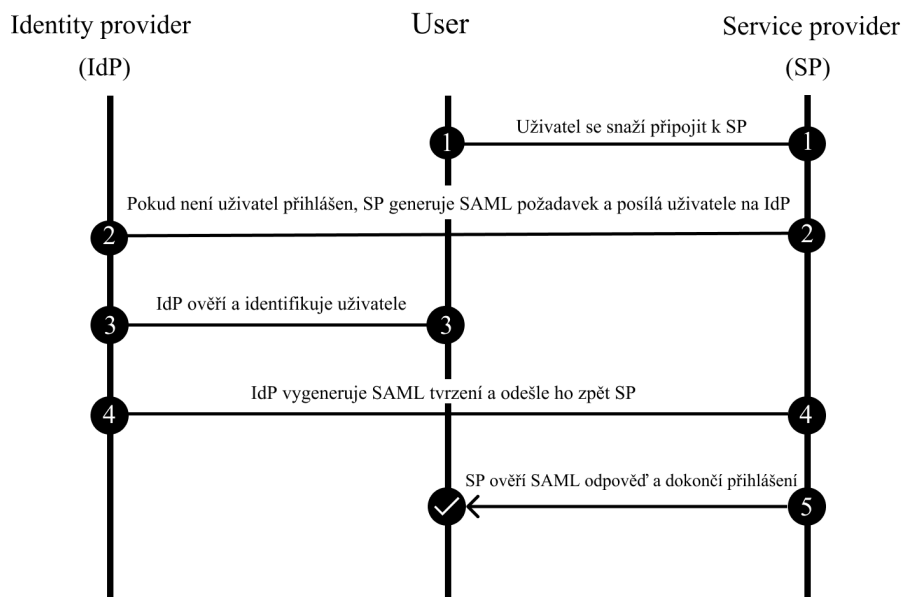
1.8.1 SAML

SAML (Security Assertion Markup Language) je otevřený XML - založený protokol, který slouží k bezpečné výměně informací o identitě a autentizaci mezi poskytovatelem identity (Identity Provider, IdP) a poskytovatelem služeb (Service Provider, SP). Hlavní výhodou SAML je možnost jednotného přihlášení (Single Sign-On, SSO), kdy uživatel ověří svou

identitu pouze jednou a následně získá přístup k více aplikacím napříč různými systémy. Tento princip se hojně využívá zejména v podnikových (B2B) i zákaznických (B2C) scénářích, kde je potřeba bezpečně sdílet identitu mezi více subjekty [19].

SAML 2.0, standardizovaný v roce 2005, umožňuje tzv. federovanou identitu, což znamená, že různé organizace mohou vzájemně důvěřovat ověření identity provedenému jiným subjektem. V rámci SAML vystupují tři hlavní entity: poskytovatel identity (IdP), poskytovatel služeb (SP) a uživatelský agent (typicky webový prohlížeč), který zprostředkovává komunikaci mezi IdP a SP [19].

Typický scénář přihlášení pomocí SAML je znázorněn na obrázku níže. Uživatel se nejprve pokusí přistoupit ke službě (SP). Pokud není ověřen, SP vygeneruje SAML požadavek a posílá uživatele na IdP. IdP provede autentizaci uživatele (například pomocí hesla nebo vícefaktorové autentizace) a následně vytvoří SAML tvrzení, které odešle zpět SP prostřednictvím prohlížeče. SP ověří platnost a integritu SAML odpovědi a dokončí přihlášení uživatele. Tento proces je detailně znázorněn v sekvenčním diagramu:



Obrázek 2 Schéma SAML protokolu

Zdroj: Vlastní zpracování na základě ONELOGIN: SAML vs OIDC [28]

SAML definuje několik klíčových komponent, zejména tvrzení (assertions), která obsahují informace o uživateli, jeho ověření a oprávněních. Dále jsou specifikovány protokoly (např. AuthNRequest), vazby (například HTTP Redirect) a profily, které určují konkrétní scénáře použití, například webové jednotné přihlášení [20].

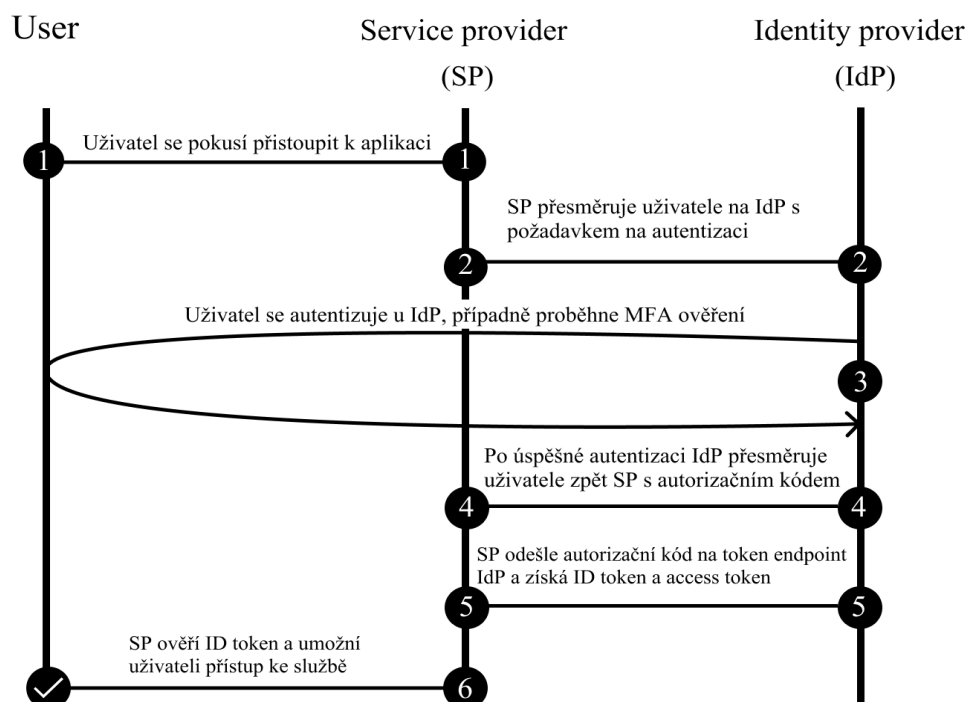
Mezi hlavní výhody SAML patří platformní nezávislost, robustní bezpečnostní mechanismy (digitální podpisy, šifrování) a široká podpora u poskytovatelů IdP i SP. SAML je hojně využíván v podnikových prostředích například pro integraci s Azure AD, PingFederate, Salesforce nebo Slack. Nevýhodou je vyšší složitost implementace, omezená vhodnost pro mobilní scénáře a skutečnost, že jde o technologii, která byla standardizována již v roce 2005. Přesto SAML zůstává klíčovým nástrojem pro bezpečné a auditovatelné jednotné přihlášení napříč různými systémy [20].

1.8.2 OIDC

OpenID Connect (OIDC) je moderní autentizační protokol, který rozšiřuje autorizační framework OAuth 2.0 o identitní vrstvu. OIDC umožňuje klientským aplikacím (SP) ověřit identitu uživatele na základě autentizace provedené poskytovatelem identity (IdP). Tento protokol je široce využíván v moderních webových, mobilních i desktopových aplikacích, protože nabízí jednoduchý a bezpečný způsob jednotného přihlášení (Single Sign-On, SSO) [19].

Hlavním přínosem OIDC je možnost bezpečně získat informace o uživateli prostřednictvím tzv. ID tokenu (ve formátu JWT), který obsahuje základní údaje o uživateli a autentizační události. OIDC tak umožňuje nejen ověřit identitu uživatele, ale také získat další profilové informace prostřednictvím UserInfo endpointu [21].

Typický průběh autentizace pomocí OIDC Authorization Code Flow je znázorněn na obrázku níže. Celý proces začíná tím, že uživatel se pokusí přistoupit k aplikaci (SP). SP následně přesměruje uživatele na IdP s požadavkem na autentizaci. Uživatel se autentizuje u IdP, případně proběhne vícefaktorové ověření (MFA). Po úspěšné autentizaci IdP přesměruje uživatele zpět na SP s autorizačním kódem. SP následně odešle tento autorizační kód na token endpoint IdP a získá ID token a access token. Po ověření ID tokenu umožní SP uživateli přístup ke službě [21].



Obrázek 3 Schéma OIDC protokolu

Zdroj: Vlastní zpracování na základě ONELOGIN: SAML vs OIDC [28]

Díky této architektuře je možné bezpečně a efektivně ověřovat uživatele napříč různými aplikacemi a platformami. OIDC je dnes považován za standard pro moderní autentizaci a je podporován širokou škálou poskytovatelů identity i služeb.

1.9 Řešení správy identity

Jak bylo uvedeno v předchozích kapitolách, efektivní řízení digitální identity ve firemním prostředí vyžaduje implementaci vícefaktorové autentizace (MFA), podporu moderních autentizačních protokolů (např. SAML, OIDC), práci s elektronickými certifikáty a dodržování bezpečnostních a legislativních standardů (např. ISO/IEC 27001, GDPR, eIDAS). Pro účely praktické části této práce bylo proto zvoleno řešení ProID, které tyto požadavky komplexně naplňuje.

ProID představuje platformu určenou pro správu identity a zabezpečený přístup k informačním systémům. Podporuje jak mobilní autentizaci (např. aplikace ProID Mobile), tak hardwarová řešení (např. čipové karty či USB tokeny), a umožňuje přihlašování ke

cloudovým i on-premise systémům s využitím silných autentizačních metod. Jeho architektura zohledňuje požadavky na vysokou míru zabezpečení i uživatelský komfort [22].

Z pohledu této práce bylo řešení ProID využito jako konkrétní příklad nástroje, pro který lze navrhnout a testovat digitální marketingovou strategii v B2B segmentu. V praktické části jsou popsány akviziční aktivity realizované na tomto produktu – včetně návrhu a optimalizace landing page, nastavení PPC kampaní, organizace odborného webináře a vyhodnocení výsledků z hlediska lead generation. Díky tomu bylo možné ověřit účinnost zvoleného postupu a identifikovat doporučení pro další rozvoj [22].

2 STRATEGIE AKVIZICE PARTNERŮ A ONLINE PREZENTACE ŘEŠENÍ

Tato kapitola se zaměřuje na metody, které slouží k navázání kontaktu s novými partnery a k prezentaci řešení ProID na cílových trzích. Cílem je přiblížit digitální nástroje a přístupy využívané v rámci B2B marketingu, které umožňují identifikaci vhodných integračních partnerů, oslovení firem, tvorbu konverzní landing page a optimalizaci marketingových kampaní. Popsané metody tvoří teoretický základ pro praktickou část, ve které byly testovány konkrétní strategie směřující k získání nových obchodních kontaktů.

2.1 Partnerství jako forma akvizice B2B prostředí

V prostředí B2B marketingu je navazování partnerství jedním z klíčových nástrojů pro expanzi na nové trhy. Namísto přímého oslovování koncových zákazníků se firma může zaměřit na vyhledávání integračních partnerů – tedy firem, které disponují znalostmi cílového trhu a zároveň jsou schopny začlenit dané řešení do svých vlastních produktů nebo služeb. Tento přístup je obzvlášť efektivní v případě technicky komplexních řešení, jako je ProID, která vyžadují určitou úroveň odbornosti a důvěry mezi stranami.

Integrační partneři mohou plnit více rolí – od technické implementace a zákaznické podpory až po aktivní obchodní zastoupení a propagaci řešení. Výběr vhodného partnera je proto strategickým rozhodnutím, které ovlivňuje úspěch celkové akviziční strategie. Klíčovými kritérii jsou technická způsobilost, reputace na trhu, reference, velikost klientské báze a zaměření na kompatibilní sektor (např. veřejná správa, enterprise segment, poskytovatelé cloudových služeb apod.).

Pro zmapování relevantních společností na cílových trzích byl využit portál G2, který slouží jako benchmarkingová platforma zaměřená na B2B software. Nabízí přehledné srovnání produktů a dodavatelů na základě uživatelských recenzí, tržního podílu, hodnocení funkcionality a typického zákaznického segmentu. Nástroj G2 Grid umožňuje vizuálně porovnávat poskytovatele řešení podle kategorií jako „Leaders“, „Contenders“ nebo „Niche“, což usnadňuje předvýběr relevantních partnerů pro další kontaktování a analýzu. Díky těmto datům mohla být identifikována skupina firem s potenciálem pro navázání obchodní spolupráce, u kterých byl následně zkoumán obchodní model, technická připravenost a ochota k integraci externího řešení [23].

2.2 Možnosti oslovování firem

Úspěšné navázání obchodního kontaktu v B2B prostředí závisí na volbě vhodného komunikačního kanálu a formy oslovení. Jednotlivé metody oslovování se liší podle míry personalizace, technického zaměření cílové skupiny i formátu předávané informace. V následujících podkapitolách jsou shrnuty hlavní způsoby využívané v rámci B2B akvizice partnerů pro řešení typu ProID.

2.2.1 E-mailová komunikace

E-mailová komunikace patří mezi nejběžněji využívané nástroje přímého oslovení v B2B prostředí. Její výhodou je možnost snadné personalizace, strukturovaného předání informací a relativně nízká bariéra pro navázání kontaktu. Účinný e-mail by měl být stručný, věcný a obsahovat jasnou výzvu k akci – například nabídku osobní konzultace, odkaz na produktové materiály nebo návrh na partnerskou spolupráci. V rámci této práce byla e-mailová komunikace využita zejména při prvotním oslovení vybraných firem. Přestože jde o široce rozšířenou metodu, její slabinou bývá nižší míra odezvy ze strany oslovených kontaktů, což je nutné zohlednit při návrhu celkové akviziční strategie [24].

2.2.2 LinkedIn

LinkedIn představuje efektivní nástroj pro vyhledávání a kontaktování relevantních osob ve firmách – zejména v oblastech IT, bezpečnosti, obchodu a managementu. Ve srovnání s e-mailovou komunikací umožňuje osobnější formu oslovení a zároveň poskytuje širší kontext o cílové osobě, jako je její pracovní zařazení, aktuální projekty či profesní zaměření. Pro řešení typu ProID byl LinkedIn využit k navázání přímého kontaktu s osobami odpovědnými za oblast IT bezpečnosti nebo za rozvoj partnerské sítě. Po přijetí žádosti o spojení je navazující komunikace často vnímána neformálněji a umožňuje snazší navázání vztahu. V rámci této práce však byla míra odezvy na oslovení přes LinkedIn srovnatelná nebo mírně nižší než u e-mailové komunikace, což potvrzuje, že samotný výběr kanálu nezaručuje vyšší efektivitu bez další personalizace a relevance sdělení [24].

2.2.3 Kontaktní formuláře a demo požadavky

Některé firmy preferují formální způsob oslovení prostřednictvím vlastních webových formulářů – typicky určených pro poptávky, partnerskou spolupráci nebo technické dotazy. Tento přístup bývá méně flexibilní než přímý e-mail nebo komunikace přes sociální sítě, ale je vhodný zejména pro firmy, které neuvádějí přímé kontaktní údaje, nebo vyžadují

strukturovaný proces schvalování komunikace. V rámci práce se ukázalo, že odpovědnost u tohoto způsobu oslovení byla vyšší než u komunikace přes LinkedIn, a mírně převyšovala i klasickou e-mailovou komunikaci.

Zvláštní skupinu tvoří formuláře určené k žádosti o předvedení produktu (demo request), které jsou běžnou součástí nabídky SaaS řešení. Tento kanál bývá jednoznačně vnímán jako žádost o obchodní kontakt, což zvyšuje ochotu firmy na poptávku reagovat. V rámci praktické části práce se právě tento způsob komunikace ukázal jako nejefektivnější, a to zejména po navázání kontaktu s odpovědnou osobou, kdy následná komunikace probíhala výrazně hladčeji.

2.2.4 B2B platformy jako G2 a Capterra

Specializované platformy typu G2 nebo Capterra slouží primárně pro vyhledávání a porovnávání softwarových řešení, ale zároveň umožňují firemní kontakt mezi dodavateli a zájemci. Některé profily obsahují kontaktní formuláře nebo propojení na zástupce daného řešení. V rámci této práce byly tyto platformy využity jednak pro benchmarking, jednak pro identifikaci kontaktů u vytipovaných partnerů.

2.2.5 Online schůzka a prezentace řešení

Osobní prezentace je jedním z nejúčinnějších nástrojů v rámci budování důvěry a získání zájmu o spolupráci. V prostředí B2B se často využívají online schůzky, které umožňují interaktivní představení řešení, zodpovězení technických dotazů a přímou diskusi s rozhodovacími osobami na straně potenciálního partnera. Před samotnou schůzkou bývá vhodné zaslat stručnou produktovou prezentaci, která shrnuje přínosy řešení a slouží jako výchozí bod pro další komunikaci.

Podle Wiessmana [25] je klíčovým prvkem úspěšné prezentace jasné vymezení hlavního sdělení, strukturovaný tok informací a schopnost přizpůsobit obsah očekáváním publika. Tyto principy byly aplikovány i při tvorbě prezentačních materiálů v rámci této práce, jejichž cílem bylo stručně a srozumitelně představit výhody řešení ProID s důrazem na jeho přidanou hodnotu pro potenciálního partnera.

2.3 Landing page jako nástroj konverze

Landing page, neboli cílová vstupní stránka, je navržena s cílem převést návštěvníka na konkrétní akci – typicky vyplnění formuláře, odeslání poptávky, stažení materiálů nebo

žádost o kontakt. V digitální akviziční strategii představuje klíčový nástroj pro sběr kontaktů a generování obchodních příležitostí, zejména v prostředí B2B, kde je rozhodovací proces delší a více strukturovaný. Hlavním cílem landing page je přimět návštěvníka, aby na stránce zanechal svůj kontakt a tím umožnil navazující obchodní komunikaci.

Účinná landing page by měla obsahovat výstižný nadpis, stručné a srozumitelné shrnutí hlavních přínosů řešení, vizuální prvky zvyšující důvěryhodnost (například loga klientů, certifikace) a jasnou výzvu k akci (CTA). Zcela zásadní je rovněž optimalizovaný kontaktní formulář, který by měl být co nejjednodušší a zároveň sbírat relevantní informace. Podle Clarkea [26] hraje v konverzním poměru zásadní roli přehlednost a vizuální jednoduchost stránky, která napomáhá rychlé orientaci a podporuje požadované chování návštěvníka.

Psychologické principy přesvědčování, jak je popisuje Cialdini [24], mohou přispět ke zvýšení účinnosti landing page. Využití principu reciprocity (například nabídka bezplatného materiálu výměnou za kontakt), sociálního důkazu (recenze, počet uživatelů) nebo autority (certifikace, odborné garance) zvyšuje důvěryhodnost a motivuje návštěvníka k interakci. Důraz by měl být kladen na jasné sdělení hodnoty a odstranění bariér, které by mohly návštěvníka odradit od odeslání formuláře.

2.4 PPC a SEO jako nástroje propagace

Placené kampaně typu PPC (pay-per-click) a optimalizace pro vyhledávače (SEO) patří mezi základní digitální nástroje pro získávání návštěvnosti a podporu konverzních stránek. Jejich společným cílem je přivést na web relevantní publikum a maximalizovat pravděpodobnost, že návštěvník provede požadovanou akci – například zanechá kontakt nebo požádá o produktovou ukázkou.

PPC kampaně umožňují přesné cílení podle klíčových slov, demografických údajů, zájmů nebo profesních rolí, což je v B2B prostředí obzvlášť cenné. V kombinaci s kvalitní landing page dokážou generovat měřitelnou návštěvnost a přímé obchodní příležitosti. Nejčastěji využívanými platformami jsou Google Ads a LinkedIn Ads, které umožňují oslovení rozhodovacích pozic ve firmách. Podle Clarkea [26] je zásadním faktorem úspěšné PPC kampaně kvalita cílové stránky, relevance klíčových slov a konzistentnost mezi textem reklamy a obsahem stránky.

SEO (Search Engine Optimization) představuje dlouhodobý přístup k získávání organické návštěvnosti z vyhledávačů. Na rozdíl od PPC, kde platí inzerent za každé

kliknutí, je cílem SEO budování kvalitního obsahu, technické optimalizace webu a zpětných odkazů. Výhodou SEO je nižší dlouhodobá nákladovost a větší důvěryhodnost ve srovnání s placenou reklamou. Clarke [26] zdůrazňuje, že úspěšná SEO strategie spočívá ve správné volbě klíčových slov, tvorbě hodnotného obsahu a optimalizaci technických faktorů, jako je rychlost načítání nebo struktura HTML a CSS kódu.

2.5 A/B testování

A/B testování je experimentální metoda, která umožňuje porovnávat dvě nebo více variant jednoho prvku s cílem zjistit, která verze vede k lepšímu výsledku. V oblasti digitálního marketingu se tento přístup využívá zejména při optimalizaci konverzních prvků – jako jsou nadpisy, texty výzev k akci (CTA), vizuální uspořádání nebo struktura formuláře. Klíčovým principem je izolování jedné proměnné a její testování v reálném prostředí s cílovými uživateli.

V B2B segmentu, kde jsou rozhodovací cykly delší a návštěvnost nižší než v B2C, je obzvláště důležité navrhovat testy s jasně definovanou hypotézou a dostatečným časovým rozptylem. Testovat lze například odlišnou formulaci benefitu, délku textu, umístění formuláře nebo barvu tlačítka. Sledovanými metrikami bývají míra prokliku (CTR), míra odeslání formuláře nebo konverzní poměr.

Jak uvádí Nassery [27], A/B testování je jedním z nejefektivnějších způsobů, jak činit rozhodnutí na základě dat, a nikoliv subjektivních dojmů. Při správném nastavení a interpretaci výsledků vede k průběžné optimalizaci uživatelského zážitku a zvyšování výkonnosti digitálních kampaní. V rámci této práce byly otestovány různé varianty landing page a reklamních sdělení, jejichž výsledky jsou podrobně rozebrány v praktické části.

2.6 Shrnutí

Tato kapitola představila klíčové digitální nástroje a přístupy využívané při akvizici partnerů a propagaci řešení v B2B prostředí. Byly popsány metody výběru integračních partnerů, způsoby jejich oslovení prostřednictvím různých komunikačních kanálů, návrh a význam landing page, využití PPC kampaní a role SEO v podpoře návštěvnosti. Dále byla vysvětlena metoda A/B testování jako efektivní nástroj pro optimalizaci výkonnosti marketingových aktivit.

Představené teoretické poznatky tvoří základ pro návrh a realizaci konkrétní akviziční strategie, která je rozpracována v praktické části této práce. Na základě zmíněných principů

byla provedena analýza cílového trhu, identifikace vhodných partnerů, návrh komunikačních a prezentačních materiálů, vytvoření landing page a spuštění PPC kampaní. Výsledky jednotlivých kroků, včetně A/B testování a vyhodnocení účinnosti použitých nástrojů, jsou uvedeny v následujících kapitolách.

II PRAKTICKÁ ČÁST

3 VÝBĚR PARTNERA PRO INTEGRACI

Tato kapitola se věnuje výběru vhodného softwarového řešení, jehož poskytovatel zároveň představuje potenciálního partnera pro technickou integraci a společné marketingové aktivity. Pro systematické porovnání dostupných možností byla využita platforma G2, která poskytuje přehled o SaaS nástrojích na základě uživatelských recenzí, tržního postavení a funkčních kategorií.

S ohledem na více než 30 000 aktivních SaaS společností na globálním trhu byl nutný výběrový filtr, který by umožnil efektivně identifikovat kandidáty splňující požadovaná technická a obchodní kritéria. Následující podkapitola popisuje konkrétní parametry, které vedly k výběru softwaru vhodného pro navázání partnerské spolupráce v rámci expanze na evropské trhy.

3.1 Kritéria výběru softwaru

Výběrový proces byl navržen tak, aby umožnil identifikaci softwarového řešení s potenciálem pro technickou integraci a zároveň pro navázání obchodní spolupráce. Kritéria zohledňovala jak technickou připravenost, tak marketingovou aktivitu a regionální působnost.

Prvním filtrem byla aktivita na platformě G2. Do výběru se dostala pouze řešení, která dosahovala minimálně 4 z 5 hvězd a měla alespoň 20 ověřených recenzí. G2 byla zvolena jako spolehlivý nástroj pro orientaci v rozsáhlé nabídce softwarových produktů. Firmy aktivně prezentující svá řešení na této platformě obvykle usilují o vyšší viditelnost a projevují zájem o marketingové partnerství.

Důležitou roli hrála také marketingová angažovanost poskytovatele. Byly preferovány společnosti, které pořádají webináře, publikují odborný obsah, komunikují na sociálních sítích nebo se účastní oborových konferencí. Taková aktivita naznačuje otevřenost ke spolupráci na společných kampaních, což je pro účely této práce zásadní.

Z technického hlediska byla hodnocena podpora moderních integračních protokolů (např. SAML, OIDC), stabilita produktu, zkušenosti s podobnými integracemi a celková připravenost přizpůsobit řešení specifickým požadavkům bezpečnostní platformy.

Zohledněna byla i velikost cílového segmentu. Upřednostněny byly produkty určené pro střední a velké podniky, u nichž se předpokládá vyšší zájem o pokročilá bezpečnostní řešení a zároveň větší kapacita na straně partnera pro spolupráci.

Konečně byl brán ohled na geografické zaměření – výběr se soustředil na firmy s působností v DACH regionu a v Polsku, které představují klíčové trhy pro expanzi řešení ProID.

Takto definovaný rámec umožnil zúžit výběr na relevantní společnosti, u nichž existuje vysoký potenciál pro technické propojení i obchodní synergie.

3.2 Parametry hodnocení softwaru

Na základě výběrových kritérií bylo vytipováno deset relevantních softwarových řešení, kterým byly následně přiřazeny body podle několika klíčových parametrů. Největší váhu měly faktory jako marketingová aktivita v cílových regionech, velikost společnosti, existence podobné integrace u konkurenčních produktů a uživatelské hodnocení na platformě G2.

Vedle těchto hlavních kritérií byly udělovány i bonusové body – například za ocenění „Easy to Use“, které odráží pozitivní uživatelskou zkušenost a přívětivost rozhraní.

Souhrnné bodové hodnocení všech kandidátů je uvedeno v následující tabulce. Sloužilo jako podklad pro výběr konkrétního partnera, s nímž byla navázána komunikace v další fázi projektu.

Software	G2 Grid	Zaměstnanci	Typ zákazníků	G2 recenze	Aktivita	Region (DACH/PL)	Konkurence	Hodnocení	Priorita
HubSpot	Leaders	7 400	Small, Mid-size, Ent.	4.7/5	Velmi vysoká	Globální	Ano	10	1
Pipedrive	Leaders	800	Mid-size	4.5/5	Vysoká	DACH, Polsko	Ano	10	1
Instantly	High Performers	210	Small, Mid-size	4.6/5	Nízká	N/A	NE	9	1
Localiq	High Performers	1500	Mid-size	4.3/5	Nízká	Mají partnery - DACH, Polsko	Ano	9	1
Salesforce	Leaders	75 000	Enterprise	4.1/5	Velmi vysoká	Globální, DACH, PL	Ano	9	1
CRM One	High Performers	220	Neznámý	4.3/5	Nízká	N/A	NE	8	2
Copper	High Performers	273	Small, Mid-size	4.7/5	Střední	Globální, USA, EU	Ne	8	2
Close	Leaders	170	Mid-size	4.2/5	Vysoká	Globální - mají partnery	ANO	8	2
Livespace	Niche	77	Small, Mid-size	4.5/5	Střední	Polsko	Ne	7	3
Zoho CRM	High Performers	1 000	Small, Mid-size, Ent.	4.3/5	Vysoká	Globální - žádní partneři	Ano	8	2

Tabulka 1 Seznam softwaru

(Zdroj: Vlastní tvorba)

4 ZÍSKÁVÁNÍ KONTAKTŮ A NAVÁZÁNÍ SPOLUPRÁCE

Jak bylo uvedeno v teoretické části, kontaktování potenciálních partnerů probíhalo prostřednictvím tří hlavních kanálů – e-mailu, sítě LinkedIn a žádostí o demo nebo kontaktních formulářů dostupných na webech jednotlivých společností. Nejvíce oslovení proběhlo e-mailem, zejména díky využití nástroje Leadspicker, jehož postup a výsledky jsou podrobně popsány v následující podkapitole.

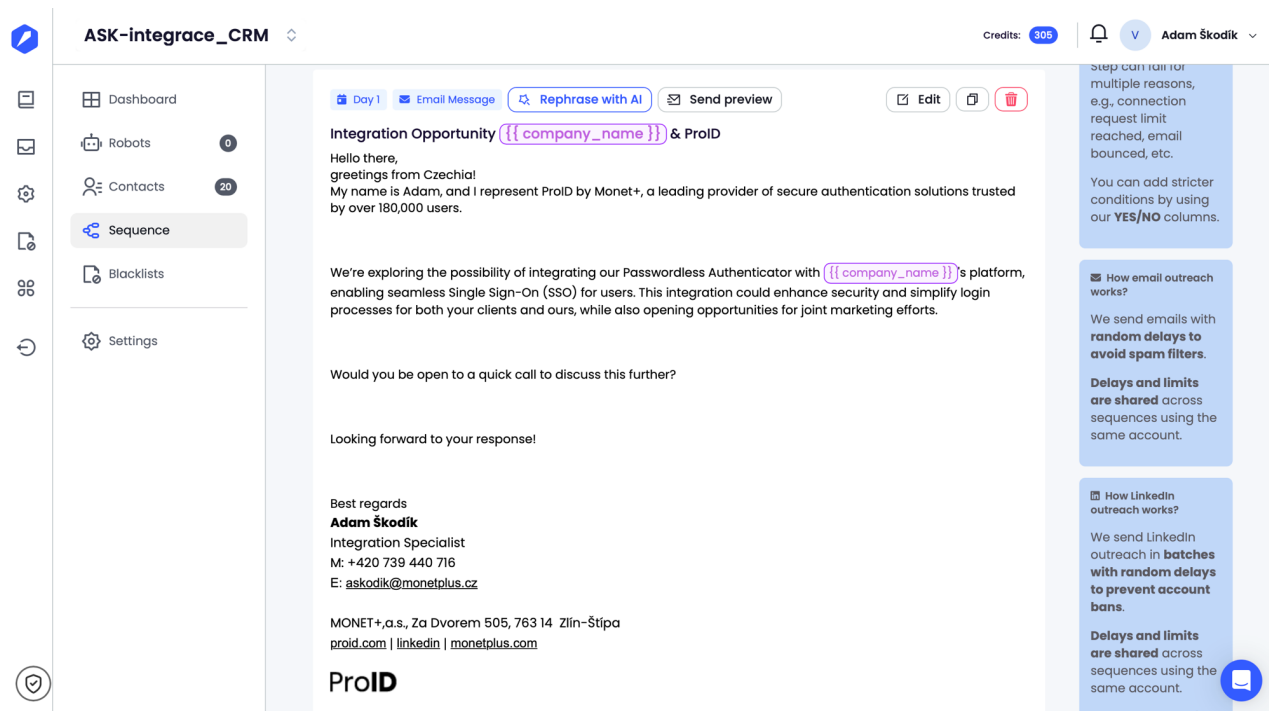
4.1.1 Komunikace s partnery

E-mail byl zvolen jako hlavní kanál pro navázání prvního kontaktu s vybranými softwarovými společnostmi. Oslovovány byly především adresy typu „partnership@domena.cz“ nebo „partners@domena.com“, které jsou veřejně dostupné a typicky směřují na osoby odpovědné za spolupráci a integrace.

S ohledem na rozsah cílového seznamu byl celý proces automatizován pomocí nástroje Leadspicker. Ten umožnil hromadné odesílání personalizovaných zpráv, sledování úspěšnosti jednotlivých kampaní (např. míra otevření či odpovědi) a následnou optimalizaci obsahu na základě reálných dat.

V rámci komunikace byla využívána jednoduchá, ale účinná šablona e-mailu s dynamickými proměnnými (např. {{ company_name }}) a stručným představením přínosů řešení ProID – zejména možnosti integrace prostřednictvím SSO a nabídky společných marketingových aktivit.

Důraz byl kladen na věcnost, jasnou výzvu k akci a přidanou hodnotu v podobě pozvánky na schůzku či přístupu k demo verzi. Tento přístup se ukázal jako nejefektivnější – nejvyšší míru odezvy vykazaly právě personalizované e-maily odeslané prostřednictvím nástroje Leadspicker. Vzorová šablona použitá v rámci kampaně je uvedena na následujícím obrázku (viz. Obrázek 4).

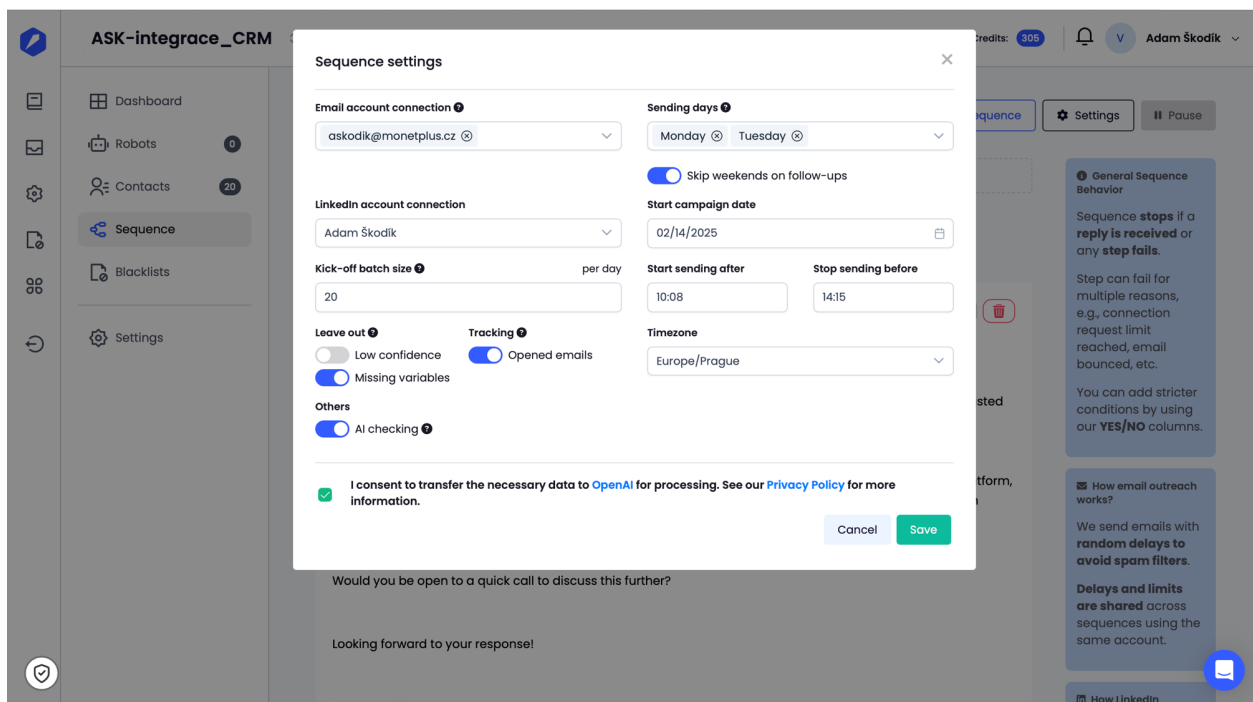


Obrázek 4 Rozhraní Leadspickeru

(Zdroj: Leadspicker účet)

Na obrázku je zachyceno detailní nastavení sekvence pro automatizované rozesílání e-mailů pomocí nástroje Leadspicker. Konfigurovány jsou zde parametry jako výběr konkrétního odesílacího účtu, rozvržení časového plánu (dny a hodiny rozesílky), velikost jednotlivých dávek či sledování metrik (např. otevření e-mailů a odpovědi).

Součástí nastavení jsou také pravidla pro optimalizaci doručitelnosti – například rozestupy mezi zprávami, které pomáhají minimalizovat riziko zařazení do spamových filtrů. Díky těmto možnostem bylo možné řídit distribuci obchodních sdělení tak, aby byly zasílány efektivně, bezpečně a s ohledem na nejlepší doručitelnost (viz. Obrázek 5).



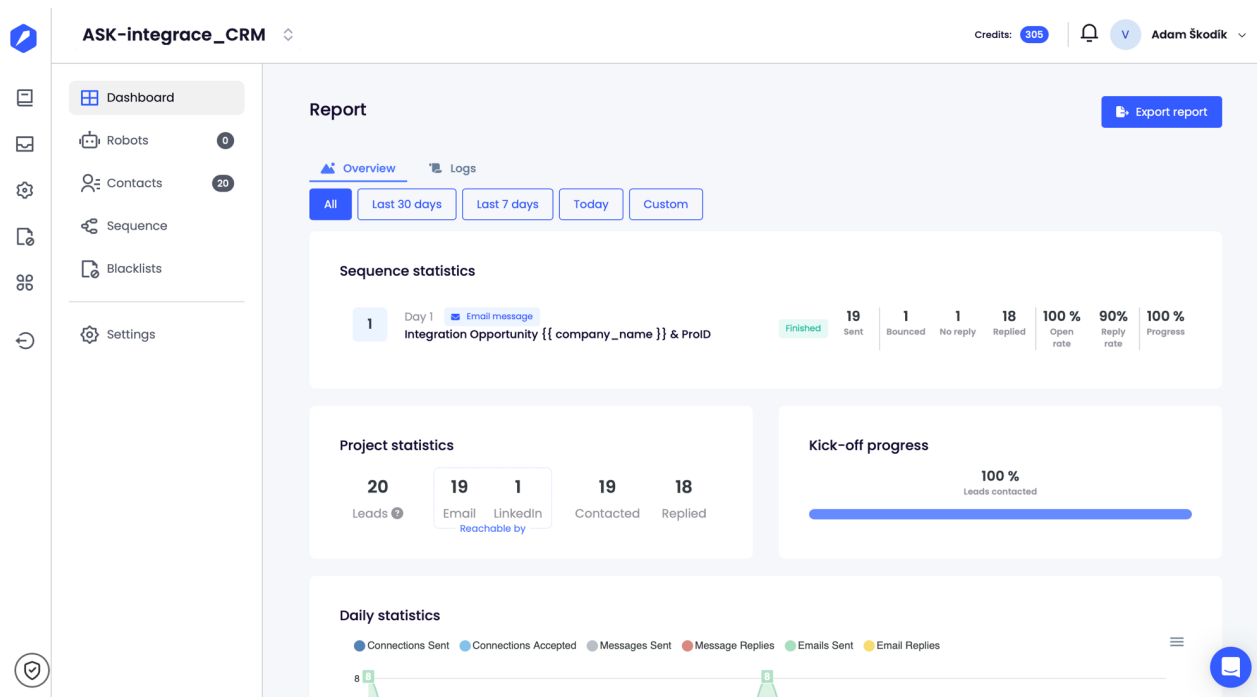
Obrázek 5 Rozhraní Leadspickeru pro odesílání

(Zdroj: Leadspicker účet)

Na obrázku je znázorněn přehled výsledků e-mailové kampaně zaměřené na oslovení firem s nabídkou integrace řešení ProID. V sekci „Sequence statistics“ je uvedeno, že z 20 připravených kontaktů bylo úspěšně odesláno 19 e-mailů – jeden záznam byl nedoručitelný kvůli neplatné adrese.

Z těchto 19 oslovených kontaktů odpovědělo 18 příjemců, což představuje mimořádně vysokou míru odpovědí 90 %. Míra otevření e-mailů dosáhla 100 %, což výrazně překračuje běžný průměr v B2B komunikaci, kde se otevřenost pohybuje mezi 15–28 % a odpovědní míra obvykle nepřesahuje 10 %.

Výsledky potvrzují správnou volbu cílové skupiny, vhodně zvolený obsah zpráv i efektivní časování a personalizaci (viz. Obrázek 6).



Obrázek 6 Report Leadpickeru odeslaných emailů

(Zdroj: Leadpicker účet)

4.1.2 Přes „Demo“ žádost

Žádost o demo verzi softwaru byla využita zejména v případech, kdy nedošlo k žádné reakci na předchozí e-mailovou komunikaci. Tento přístup sice vytváří zdání zájmu o produkt, ale ve skutečnosti sloužil k navázání kontaktu s relevantní osobou ve firmě.

Při testování na vzorku 20 společností byla míra odpovědi 100 %, přičemž v každém případě došlo k předání adekvátního a kvalifikovaného kontaktu. Tento kanál tak představoval spolehlivou, i když méně standardní cestu pro získání přímého spojení s odpovědnými osobami.

4.1.3 Vyhledávání přes LinkedIn

V případech, kdy nebylo možné navázat kontakt prostřednictvím e-mailu a zároveň chyběla možnost požádat o demo, byla využita profesní síť LinkedIn. Cílem bylo oslovit především osoby s rozhodovací pravomocí – nejčastěji s označením „Partnership Manager“ nebo „Decision Maker“.

Proces spočíval v navázání spojení a následném zaslání stručné zprávy s vysvětlením záměru spolupráce. Přestože se očekával vyšší efekt, míra odpovědí byla v praxi poměrně nízká. Při testování na vzorku 20 kontaktovaných osob odpověděly přibližně 2, což představuje míru konverze kolem 10 %. Ta odpovídá obecným trendům B2B komunikace na této platformě.

LinkedIn se tak ukázal jako méně efektivní kanál pro přímé oslovení, ale nadále představuje užitečný nástroj pro rozšiřování profesní sítě a doplňkový zdroj informací o cílových osobách a jejich rolích ve firmách.

4.2 Představení řešení online

Po úspěšném navázání kontaktu bylo naplánováno krátké online setkání, v jehož rámci byl prezentován návrh spolupráce a hlavní přínosy integrace řešení ProID (viz. Obrázek 7). Prezentace byla koncipována tak, aby zdůraznila výhody pro potenciálního partnera - konkrétně technické benefity, příležitosti pro společný marketing a obchodní přínos vzájemné spolupráce (viz. Obrázek 8). Součástí prezentace bylo také ocenění partnera jako významného hráče na trhu s potenciálem oslovit nové zákazníky (viz. Obrázek 9).

Obsah prezentace byl přizpůsobován profilu oslovené společnosti. Důraz byl kladen na oblasti relevantní pro daný subjekt — například podporu SSO integrace, bezpečnostní standardy nebo možnost účasti na společných marketingových aktivitách. Cílem bylo zaujmout druhou stranu jak z technického, tak z obchodního hlediska.

Níže jsou uvedeny vybrané snímky z prezentace, které byly zásadní pro rozhodovací proces oslovených firem. Celý materiál byl buď sdílen přímo v rámci online schůzky, nebo následně zaslán e-mailem.



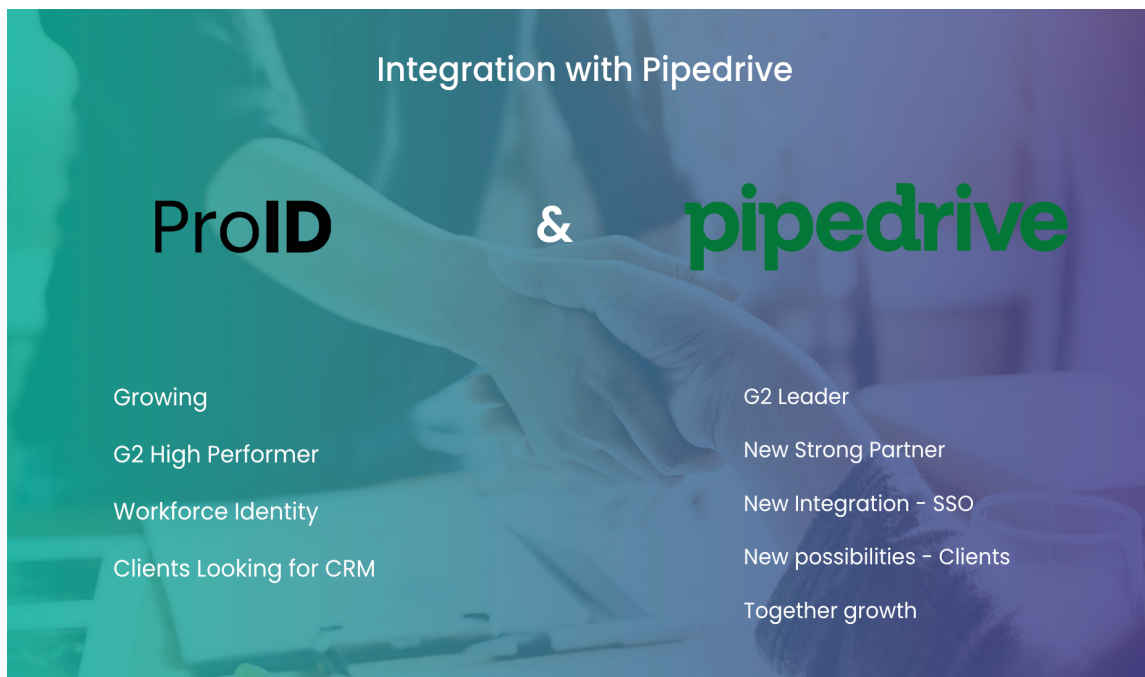
Obrázek 7 Ukázka prezentace

(Zdroj: Vlastní tvorba v Google prezentace)



Obrázek 8 Ukázka prezentace

(Zdroj: Vlastní tvorba v Google prezentace)



Obrázek 9 Ukázka prezentace

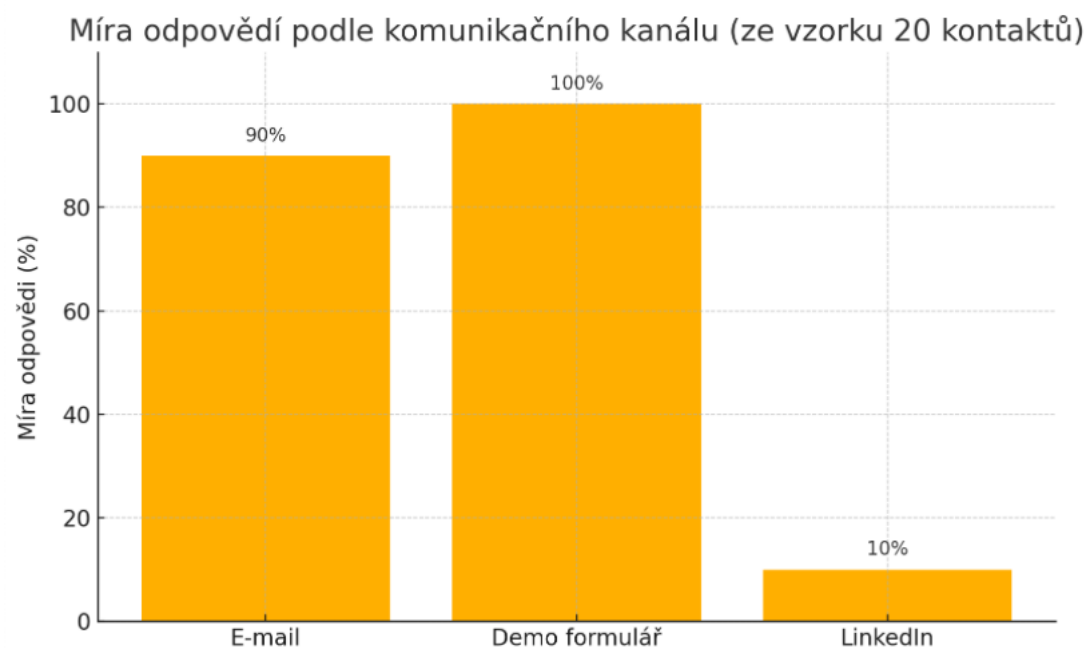
(Zdroj: Vlastní tvorba v Google prezentace)

4.3 Vyhodnocení komunikačních kanálů

Na základě praktického testování jednotlivých komunikačních kanálů lze vyhodnotit jejich efektivitu z hlediska míry odpovědí. Nejvyšší úspěšnosti bylo dosaženo při využití demo formulářů na webových stránkách softwarových společností, kde míra konverze dosáhla 100 %. Tento způsob však nelze považovat za zcela standardní, jelikož vytváří dojem zájmu o samotný produkt.

Druhou nejefektivnější cestou byl personalizovaný e-mail, který díky použití nástroje Leadspicker a dobře zvolenému obsahu dosáhl míry odpovědí 90 %. Překvapivě nejnižší úspěšnost byla zaznamenána u platformy LinkedIn, kde odpovědělo přibližně 10 % oslovených kontaktů, přestože se očekávaly výrazně lepší výsledky.

Přehledné porovnání jednotlivých kanálů je uvedeno v následujícím grafu.



Obrázek 10 Graf úspěšnosti oslovení

(Zdroj: Vlastní tvorba v MS Excel)

Ačkoli nejvyšší úspěšnost byla zaznamenána při využití demo formulářů, jako preferovaný způsob prvního kontaktování je doporučeno využít personalizovaný e-mail. Žádost o demo by měla být použita až jako doplňkový nástroj v případě, že na e-mailové oslovení nebyla obdržena odpověď, jelikož může být vnímána jako méně vhodná forma pro iniciaci obchodní spolupráce.

5 PROCES INTEGRACE

Před zahájením integrace bylo ověřeno, zda zvolené softwarové řešení podporuje moderní autentizační protokoly – konkrétně SAML a OIDC, které jsou dnes standardem pro bezpečné ověřování v rámci Single Sign-On (SSO). Umožňují propojení systémů bez nutnosti zadávání přihlašovacích údajů v každé aplikaci zvlášť. V některých případech může být celý proces dále zabezpečen prostřednictvím infrastruktury veřejných klíčů (PKI – Public Key Infrastructure), která umožňuje ověřování uživatelů a zařízení pomocí digitálních certifikátů.

Popis principů těchto protokolů je uveden v teoretické části této práce. Většina softwarových produktů poskytuje k integraci veřejnou dokumentaci s popsányými kroky a doporučeními, která celý proces výrazně usnadňuje. Pro testování byl zajištěn přístup k rozšířené verzi softwaru, neboť základní licence obvykle nepodporují pokročilé integrační možnosti. Následovala analýza možností propojení, konfigurace připojení a testování reálných scénářů.

5.1 Realizace integrace s ProID

Cílem této fáze bylo prakticky ověřit možnost integrace řešení ProID do vybraného softwaru prostřednictvím moderních autentizačních protokolů (SAML nebo OIDC). Proces zahrnoval přípravu technického prostředí, konfiguraci parametrů a následné ověření funkčnosti přihlášení v reálném scénáři.

V první fázi bylo zajištěno zřízení testovacího účtu ve vybraném softwaru, přičemž v některých případech bylo nutné požádat o vyšší licenční variantu, která umožňovala nastavení externí identity provider služby. Následně byly prostudovány integrační materiály a dokumentace poskytovaná výrobcem softwaru s cílem připravit přehledný postup propojení.

Konfigurace zahrnovala zadání klíčových parametrů – např. URL pro přesměrování uživatele (Redirect URI), identifikátor poskytovatele (Entity ID), veřejné certifikáty a volbu metody ověření. Na straně řešení ProID bylo rovněž nutné připravit metadata služby a zajistit odpovídající úroveň zabezpečení přenosu.

Po úspěšném nastavení následovalo testování přihlášení – uživatel se nejprve přihlásil pomocí své e-mailové adresy do cílové aplikace, byl přesměrován na ověřovací portál ProID, kde zvolil jednu z dostupných metod ověření (např. mobilní aplikaci ProID Mobile s biometrií), a po úspěšném ověření byl automaticky přihlášen zpět do aplikace.

Tento postup byl následně ověřen i běžnými uživateli a byla potvrzena jak funkčnost, tak uživatelská přívětivost celého řešení. Výsledkem bylo plně funkční propojení mezi řešením ProID a cílovou aplikací, které odpovídá požadavkům na bezpečnost, komfort i technickou kompatibilitu (viz. Obrázek 11, 12, 13).

5.2 Ukázka přihlášení

V rámci testování byla ověřena funkčnost integrace řešení ProID v prostředí softwaru Pipedrive. Na následujících snímcích je zachycen celý proces přihlášení prostřednictvím federovaného ověřování.

Po zadání e-mailové adresy v prostředí Pipedrive byl uživatel přesměrován na portál ProID, kde si mohl zvolit jednu ze tří dostupných metod ověření. V rámci testování byla zvolena autentizace pomocí mobilní aplikace ProID Mobile. Následovalo potvrzení identity prostřednictvím biometrie (otisk prstu / rozpoznání obličeje). Po úspěšném ověření byl uživatel automaticky přihlášen zpět do prostředí Pipedrive bez nutnosti zadávání hesla.

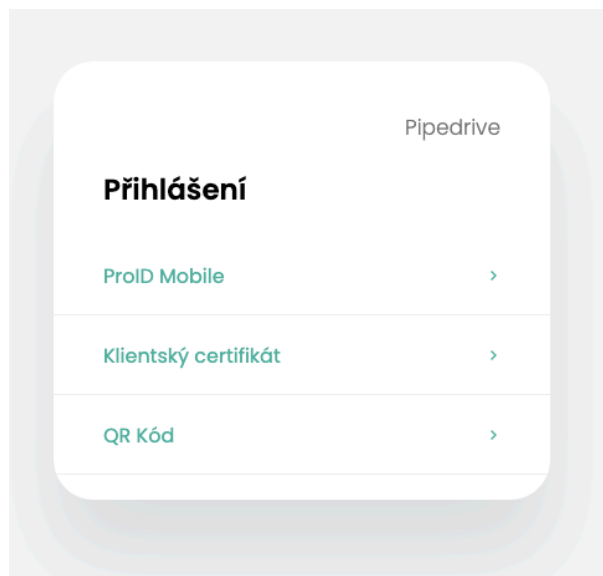
Níže uvedené snímky dokumentují jednotlivé kroky tohoto procesu:

- Obrázek 11: Přihlašovací formulář v Pipedrive
- Obrázek 12: Výběr metody ověření v ProID portálu
- Obrázek 13: Potvrzení identity pomocí ProID Mobile

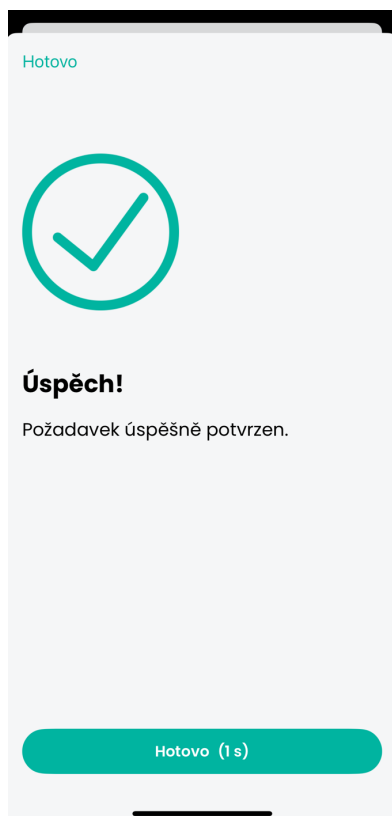


Obrázek 11 Ukázka přihlášení

(Zdroj: Přihlašovací stránka Pipedrive)



Obrázek 12 Ukázka ProID Mobile

(Zdroj: ProID Portal)

Obrázek 13 Ukázka ProID Mobile

(Zdroj: ProID Mobile)

6 MARKETINGOVÁ AKTIVITA

Marketingová aktivita sehrála v rámci projektu klíčovou roli – cílem nebyla pouze prezentace řešení ProID, ale zejména aktivní sběr kontaktů na potenciální klienty a validace zájmu o integrovaný produkt. K dosažení tohoto cíle byla zvolena kombinace několika taktických prvků: návrh vlastní landing page, její optimalizace a následné A/B testování, které mělo za cíl ověřit účinnost různých variant stránky. V další fázi pak proběhla podpora pomocí PPC kampaní, která pomohla přivádět relevantní návštěvníky a maximalizovat konverze.

6.1 Benchmarking landing page konkurence

Před návrhem vlastní landing page byla provedena analýza konkurenčních řešení s cílem identifikovat osvědčené prvky, které přispívají k vyšší konverzní efektivitě a lepší uživatelské zkušenosti. Pozornost byla věnována zejména způsobu prezentace hlavních přínosů řešení, struktuře uživatelské cesty a použitým technikám pro získání kontaktu.

Z benchmarkingové analýzy vyplynulo několik klíčových poznatků:

- Nedostatečný počet výzev k akci (CTA) významně snižuje pravděpodobnost, že návštěvník provede požadovanou interakci – zejména pokud se na stránce zdrží pouze krátkou dobu.
- Rozvržení stránky a srozumitelnost obsahu mají zásadní vliv na ochotu uživatele zůstat déle a získat potřebné informace.
- Viditelná CTA, přehledné členění obsahu a konkrétně vyjádřené přínosy patří mezi nejčastěji opakující se prvky u stránek s vysokou konverzní úspěšností.

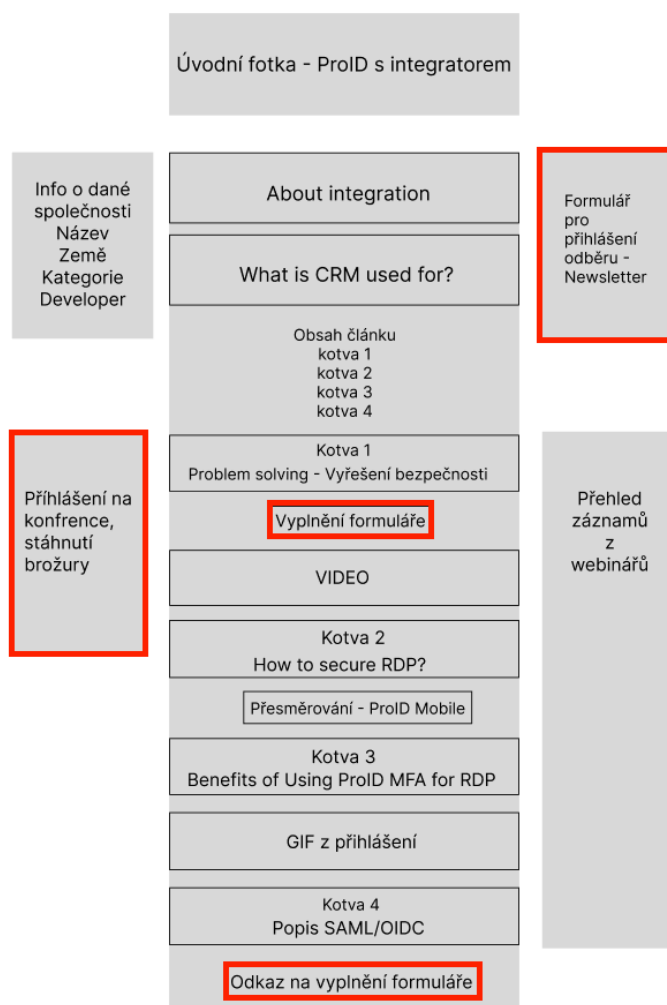
Na základě těchto zjištění bylo rozhodnuto navrhnout vlastní landing page jako vizuálně přehlednou, obsahově údernou a s vícečetnými výzvami k akci. Cílem bylo optimalizovat stránku tak, aby maximálně podporovala konverzi návštěvníků, jak bylo stanoveno v zadání této bakalářské práce.

6.2 Návrh vlastní landing page

Na základě provedeného benchmarkingu konkurenčních řešení byl vytvořen wireframe návrh vlastní landing page. Cílem bylo navrhnout stránku, která bude přehledná, snadno pochopitelná, a především navržena s ohledem na zvýšení konverzního poměru.

Wireframe sloužil jako vizuální koncept, který pomohl lépe strukturovat informace, definovat rozmístění klíčových prvků a připravit podklady pro následné testování. Díky přehlednému návrhu bylo možné předem posoudit uživatelskou cestu a zohlednit umístění jednotlivých výzev k akci (CTA), informačních bloků a kontaktních formulářů.

Zvolený přístup zároveň umožnil připravit podmínky pro budoucí A/B testování, jelikož návrh vycházel z nejlépe fungujících principů ověřených u konkurence. To umožnilo dále zkoumat, které konkrétní prvky či textace mají největší dopad na míru konverze návštěvníků.

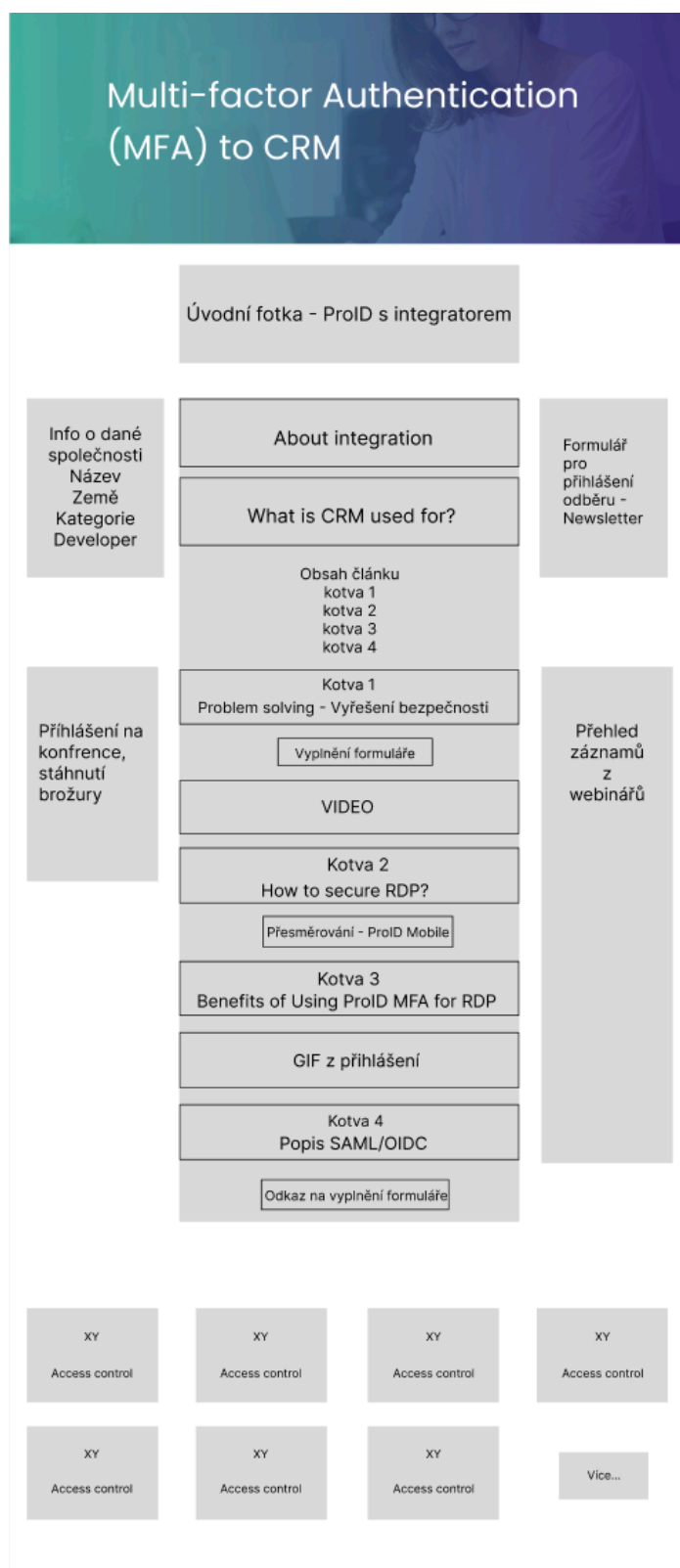


Obrázek 14 Wireframe - sběr kontaktů

(Zdroj: Vlastní výroba)

Jak bylo zmíněno v předchozích kapitolách, jedním z klíčových cílů bylo udržet návštěvníka na landing page co nejdéle a motivovat jej k provedení požadované akce. Z

tohoto důvodu byl zvolen vyšší počet výzev k akci (CTA) než u většiny konkurenčních řešení, a to s ohledem na rozsah a strukturu prezentovaného obsahu (viz. Obrázek 14).



Obrázek 15 Celý wireframe

(Zdroj: Vlastní tvorba)

6.3 A/B testování

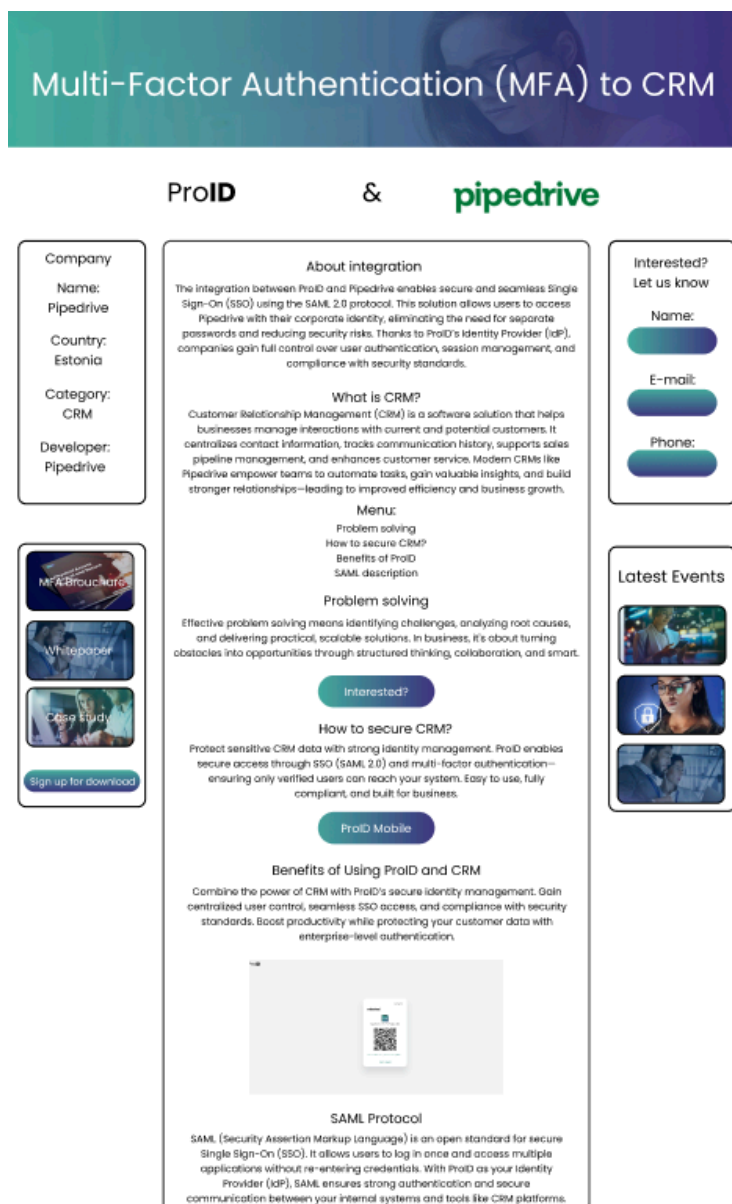
Po spuštění první verze landing page vytvořené dle navrženého wireframu (viz. Obrázek 15) bylo možné na základě nasbíraných dat vyhodnotit její efektivitu a identifikovat prostor pro optimalizaci. K analýze byly využity nástroje pro sledování uživatelského chování, jako je například Hotjar, které poskytly cenné informace o pohybu návštěvníků na stránce, délce setrvání či míře interakce s jednotlivými prvky.

Na základě těchto poznatků byly navrženy konkrétní úpravy a následně realizováno A/B testování, jehož cílem bylo porovnat výkonnost původní a upravené verze stránky z hlediska konverzního poměru a chování uživatelů. Přehled testovaných variant, klíčových změn a vyhodnocení výsledků je uveden v následujících částech kapitoly.

6.3.1 Varianta A – původní verze landing page

Po dokončení wireframu byla zahájena samotná tvorba webové stránky. Již v průběhu realizace se ukázalo, že některé návrhové prvky z wireframu nejsou v praxi optimální. Toto zjištění vedlo k jejich úpravě či úplnému nahrazení. Uvedené změny byly součástí plánovaného procesu, jelikož bylo od počátku počítáno s A/B testováním a wireframe byl chápán jako pracovní, nikoliv finální verze stránky.

Úpravy neprobíhaly pouze během vývoje, ale i v následujících týdnech a měsících, kdy byla stránka průběžně analyzována. Pomocí nástrojů pro sledování chování uživatelů byla vyhodnocována místa, kde návštěvníci z webu nejčastěji odcházeli, a do jaké části stránky scrollovali. Na základě těchto dat byla stránka několikrát upravena s cílem zvýšit její efektivitu a konverzní poměr. Aktuální verze představuje nejvýkonnější variantu z dosavadních testovaných, avšak s ohledem na dynamicky se měnící trh nelze vyloučit další úpravy v budoucnu.



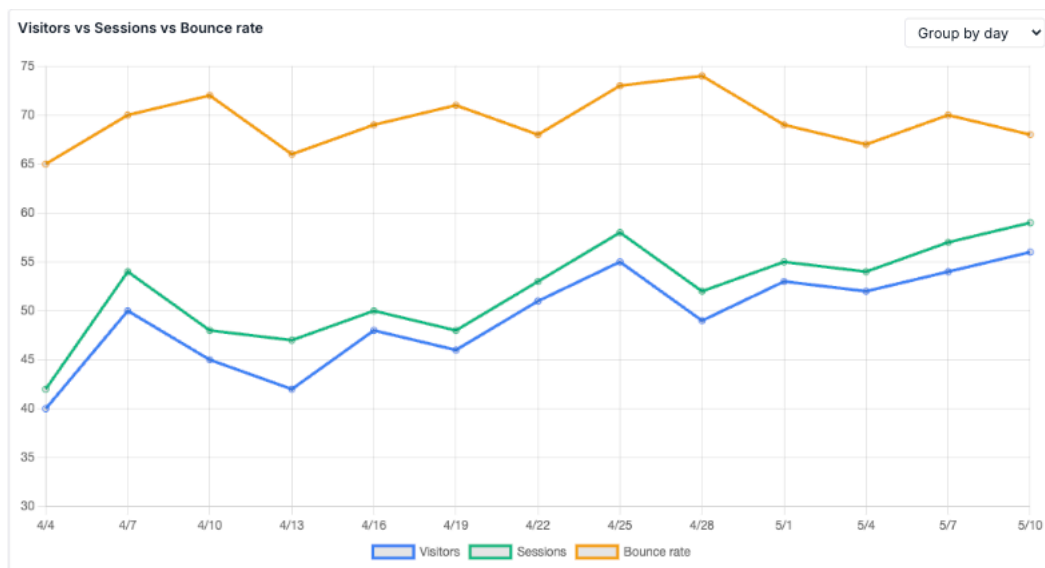
Obrázek 16 První landing page

(Zdroj: ProID web – Vlastní tvorba)

Na základě vytvořeného wireframu byla landing page převedena do finální podoby (viz. Obrázek 16). Po jejím spuštění byla kontinuálně sledována pomocí analytického nástroje Piwik, který poskytl detailní přehled o chování návštěvníků a celkové výkonnosti stránky.

Zaznamenaná míra okamžitého opuštění (tzv. bounce rate) se za období jednoho měsíce ustálila na průměrné hodnotě 67,4 %, což značí, že přibližně dvě třetiny návštěvníků stránku opustily bez jakékoliv interakce (viz. Obrázek 17). Celkový počet návštěvníků za sledované období dosáhl 402 (viz. Obrázek 18). Z nich 2,3 % provedla konverzní akci – tedy zanechala kontakt nebo využila formulář k dalšímu kroku v nákupním rozhodování (viz. Obrázek 18).

Tyto hodnoty sloužily jako výchozí metrika pro návrh a implementaci A/B testování s cílem optimalizovat stránku směrem k vyšší míře interakce a snížení bounce rate.



Obrázek 17 Graf návštěvnosti z Piwik

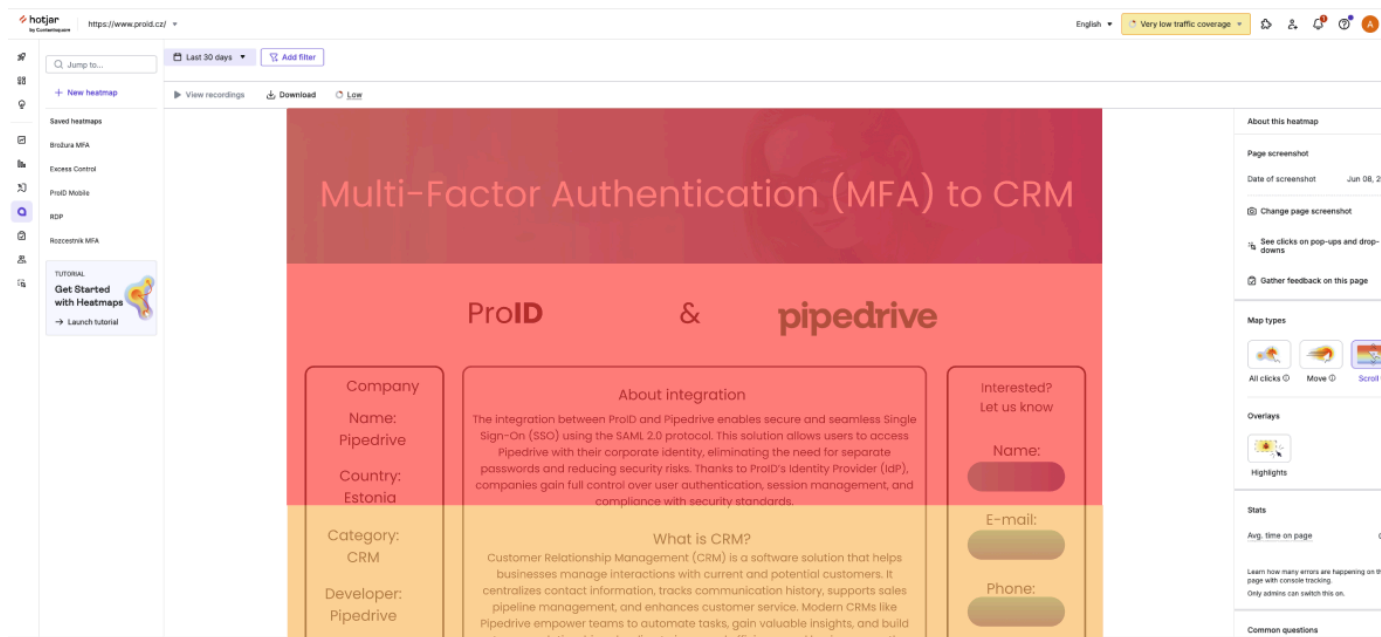
(Zdroj: Piwik)

A/B Test – Landing Page Comparison

Variant	Visitors	Sessions	Bounce rate	Pages/Session	Avg. Duration	Goal conversions	Goal conversion rate
Integration – Pipedrive	402	423	67.4%	1.22	00:01:12	9	2.3%
Integration – Smartcard Login	387	399	72.1%	1.05	00:00:56	6	1.55%

Obrázek 18 Data z Piwik

(Zdroj: Piwik)



Obrázek 19 Data z Hotjar

(Zdroj: Hotjar)

Doplňkovou analytickou vrstvou bylo využití nástroje Hotjar, který pomocí heatmap a scroll tracking vizualizuje chování návštěvníků na stránce. Ze získaných dat (viz. Obrázek 19) vyplývá, že většina návštěvníků opustila stránku již v její úvodní části – konkrétně v první čtvrtině obsahu. Tato zjištění naznačují, že návštěvníky buď nezaujaly klíčové informace v horní části stránky, nebo byl obsah nedostatečně motivující k dalšímu prohlížení.

Tento poznatek se stal podkladem pro návrh variantního řešení v rámci A/B testování, jehož cílem bylo zvýšit retenční schopnost stránky a prodloužit dobu interakce uživatele.

6.3.2 Varianta B – optimalizovaná verze landing page

Na základě analýzy první verze landing page (viz. kapitola 6.3.1), která vykazovala vysokou míru okamžitého opuštění (bounce rate), nízký průměrný čas strávený na stránce a slabý konverzní poměr, byla navržena nová – optimalizovaná varianta stránky.

Cílem úprav bylo zvýšit celkovou přehlednost, zatraktivnit obsah a prodloužit dobu, kterou návštěvník na stránce stráví (viz. Obrázek 20a, b, c). Byla přepracována struktura obsahu, jednotlivé bloky dostaly více prostoru a stránka získala světlejší vizuální styl, který zlepšuje čitelnost a působí profesionálněji. Textace byla upravena tak, aby návštěvníka více zaujala a motivovala k interakci.

Dále došlo ke zvýšení počtu výzev k akci (CTA), především ve střední části stránky, která byla identifikována jako klíčová oblast pro interakci. Doplněním ilustrací a vizuálních prvků došlo rovněž ke zvýšení atraktivity pro uživatele. Nová podoba stránky vykazala při testování výrazně lepší výsledky – zejména v oblasti míry konverze, bounce rate a průměrného času stráveného na webu.

Integration

Multi-factor authentication (MFA) to Pipedrive

Secure login (MFA/2FA) for CRM access & user authentication

Try ProlD

pipedrive™

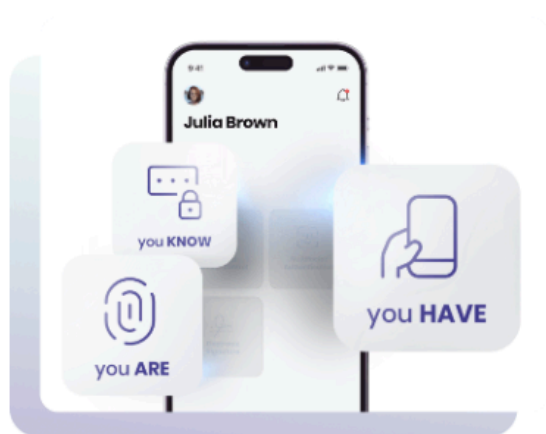
Introduction ↓

What is Pipedrive ↓

Security Risks ↓

How it works ↓

Free Trial ↓



Introduction

Sales teams and businesses rely on Pipedrive, a powerful CRM platform, to manage their customer relationships and sales pipelines. However, protecting sensitive client data and sales strategies is essential.

With ProlD, you can secure Pipedrive access using Multi-Factor Authentication (MFA), ensuring that only authorized users can log in. ProlD integrates seamlessly with Pipedrive's authentication system, providing strong protection against unauthorized access and account takeovers.

About Pipedrive?

Pipedrive is a customer relationship management (CRM) platform designed to help sales teams track deals, automate workflows, and manage customer interactions efficiently.

Key features include:

- Sales pipeline management – Organize and track leads through every stage
- Automation & integrations – Streamline tasks and connect with other tools
- Data security & analytics – Protect customer data while gaining valuable insights

Since Pipedrive stores business-critical data, ensuring secure access with MFA authentication is crucial for protecting sales teams and preventing unauthorized access.

What?

Obrázek 20a Optimalizovaná landing page

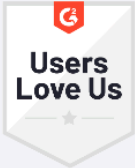
Common Security Risks

- 81% of hacking-related breaches are caused by stolen or weak passwords
- A single compromised CRM account can lead to massive sales disruptions and data loss – including sensitive client data and internal strategies.
- Reusing passwords across tools like Pipedrive, email, and cloud storage increases the attack surface dramatically.
- Phishing and social engineering attacks target CRM logins – especially in sales and customer support roles.

How ProID Solves Them

- Eliminates password-based risks – ProID supports passwordless login using smart cards or mobile MFA, protecting against stolen credentials.
- Secure MFA/2FA for every login – Even if login data is compromised, attackers can't access accounts without the second authentication factor.
- Native SAML integration with Pipedrive – ProID enables seamless and user-friendly login to Pipedrive with no extra steps or delays. Users authenticate once and gain access securely.

[Try ProID for Free](#)



Employee Digital Identity you've never seen before!

Are You Intrested? Register for Free Trial.

[Free Trial](#)



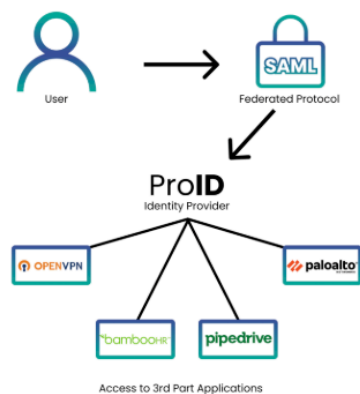
High Performer

Europe
FALL 2024



High Performer

EMEA
WINTER 2025



Why use ProID with Pipedrive?

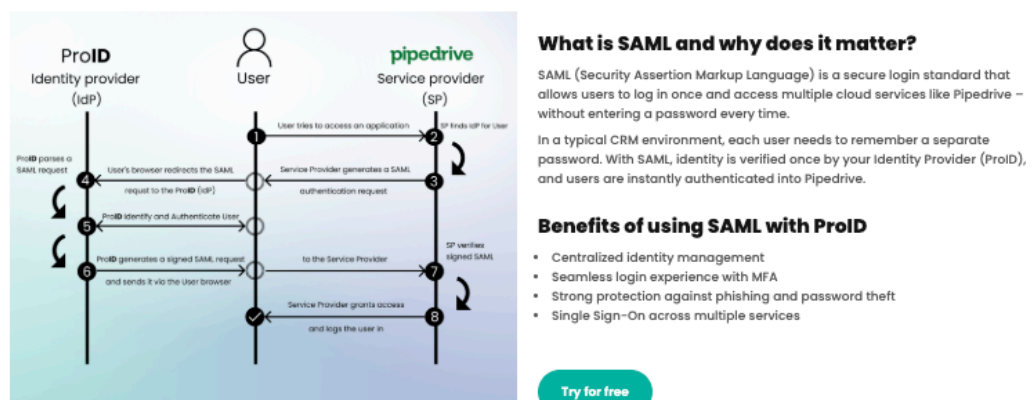
With ProID, businesses can ensure that only verified employees have access to their CRM system, protecting customer data, sales records, and confidential business information from unauthorized users.

Key Benefits:

- Stronger security for CRM data & sales teams
- Compliance with data protection regulations (GDPR, SOC2, ISO 27001)
- Flexible authentication methods (smart cards, mobile MFA, passwordless login)
- Easy deployment – No complex setup required

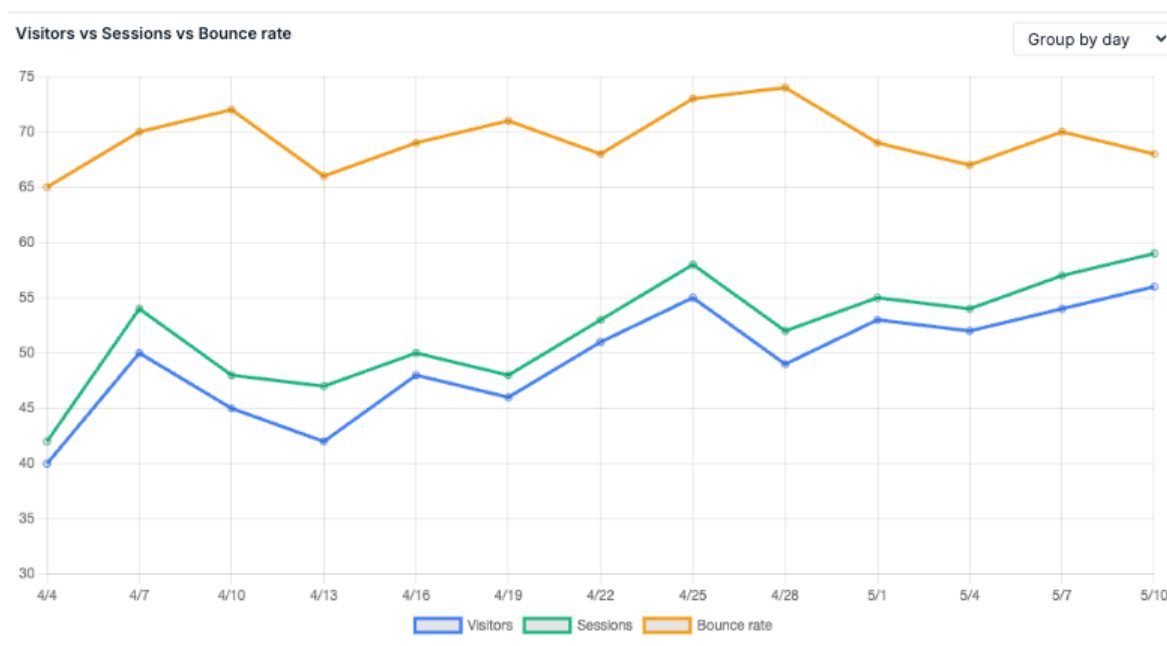
[ProID Mobile](#)

Obrázek 20b Optimalizovaná landing page



Obrázek 20c Optimalizovaná landing page

Na optimalizované stránce také stoupla návštěvnost, snížil se bounce rate a navýšil se konverzní poměr, návštěvníci na 612 (viz. Obrázek 21), bounce rate 48.2 % a konverzní poměr celkové stránky na 3.78 % (viz. Obrázek 22), což značně porazilo předchozí landing page, a bylo dosaženo požadovaných čísel.



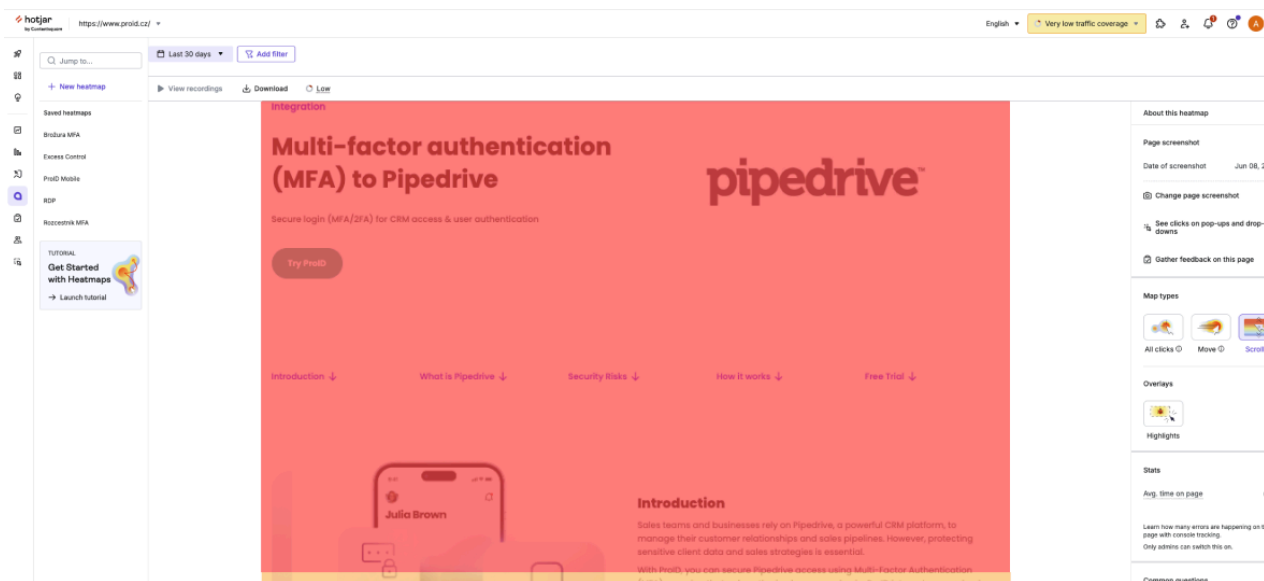
Obrázek 21 Graf návštěvnosti z Piwik

(Zdroj: Piwik)

A/B Test – Landing Page Comparison								Search
Variant	Visitors	Sessions	Bounce rate	Pages/Session	Avg. Duration	Goal conversions	Goal conversion rate	
Integration – Pipedrive	612	634	48.2%	2.15	00:02:34	24	3.78%	
Integration – Smartcard Login	387	399	72.1%	1.05	00:00:56	6	1.55%	

Obrázek 22 Data z Piwik

(Zdroj: Piwik)



Obrázek 23 Data z Hotjar

(Zdroj: Hotjar)

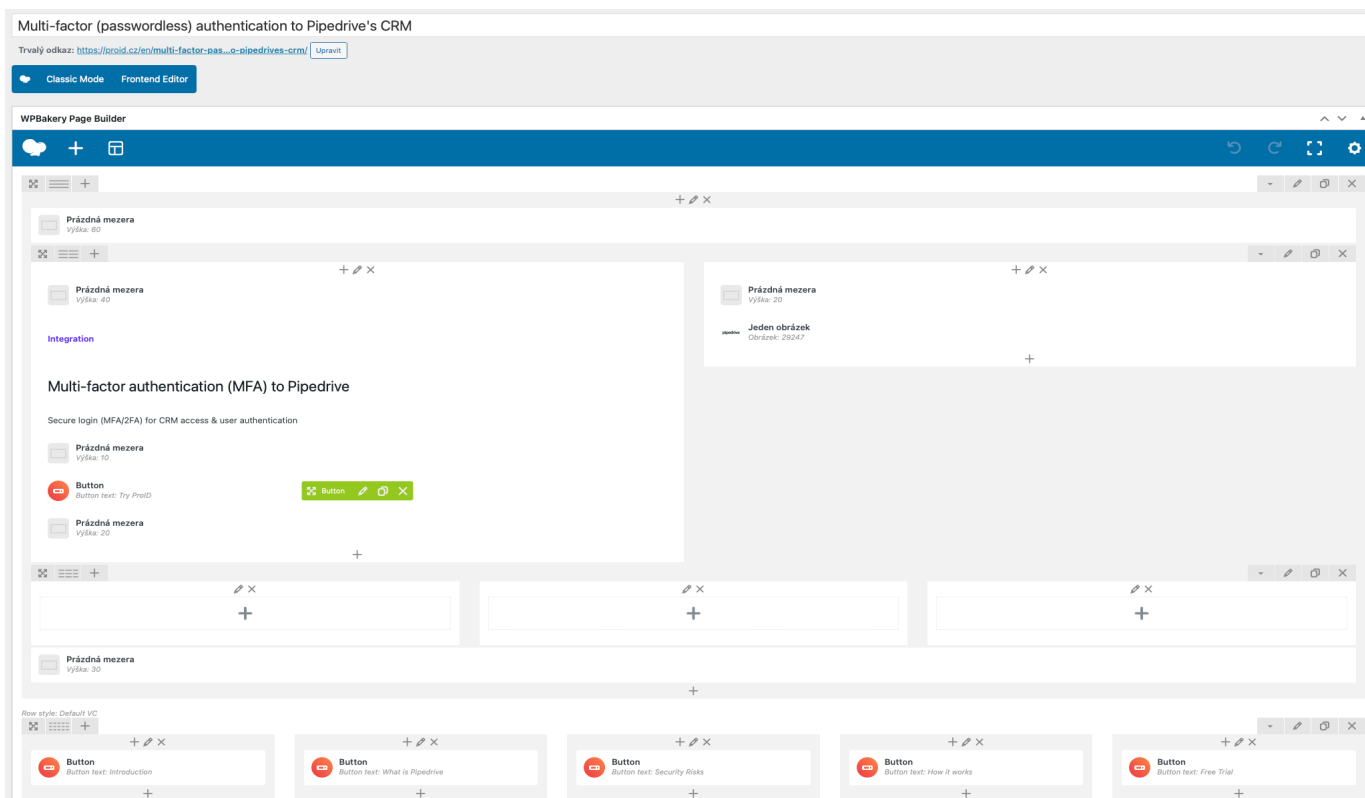
Jak vyplývá z analytických dat nástroje Hotjar (viz Obrázek 23), došlo také k prodloužení průměrného času stráveného návštěvníky na stránce. Tento nárůst lze přičíst celkově přehlednějšímu rozvržení, vizuální atraktivitě a vyšší informační hodnotě nové verze stránky, která působí pro uživatele přívětivěji než původní varianta.

6.4 Tvorba webové stránky ve WordPress

Landing page byla vytvořena pomocí redakčního systému WordPress, který poskytuje flexibilní prostředí pro tvorbu webových stránek bez nutnosti hlubšího programování. Pro návrh a implementaci byl využit vizuální editor WPBakery Page Builder, který umožňuje snadnou úpravu vzhledu a struktury stránky prostřednictvím předpřipravených bloků.

Základem bylo nasazení vhodné šablony (theme), která odpovídala požadavkům na rychlost načítání, responzivitu a čistý design. Na jejím základě byla následně vytvořena struktura jednotlivých sekcí stránky, doplněná o formuláře, CTA prvky a grafické prvky podporující vizuální přehlednost. Stránka byla napojena na analytické nástroje a připravena pro měření konverzí z reklamních kampaní.

Veškeré úpravy byly prováděny s ohledem na dříve připravený wireframe návrh a výsledky z A/B testování, čímž bylo dosaženo optimalizace obsahu a layoutu pro maximální konverzní výkon.



Obrázek 24 Landing page ze strany WordPressu

(Zdroj: Rozhraní WordPress)

Stránka byla vytvořena pomocí blokových prvků dostupných ve vizuálním editoru WPBakery. Použity byly základní elementy jako textová pole, obrázky a nadpisy, které sloužily k přehlednému a vizuálně atraktivnímu předání informací.

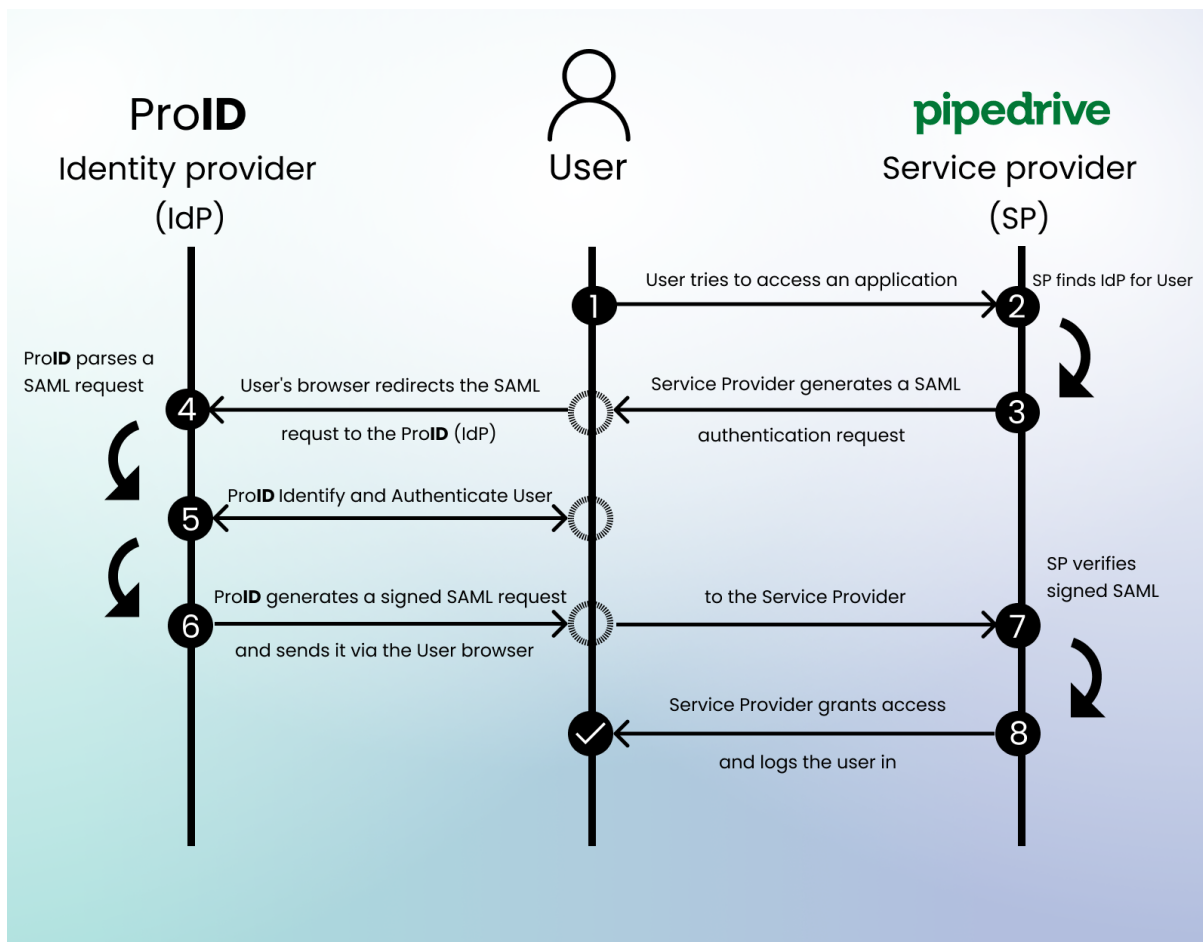
Zvláštní důraz byl kladen na umístění tlačítek s výzvou k akci (CTA), která byla rozmístěna strategicky podle návrhu wireframu. Cílem bylo podpořit interakci návštěvníka a zvýšit šanci na získání konverze. CTA prvky byly integrovány například do úvodu stránky, středu i zápatí, aby byly vždy snadno dostupné.

Rozvržení jednotlivých bloků odpovídalo výsledkům A/B testování a bylo upraveno tak, aby usnadnilo orientaci, zvýšilo srozumitelnost sdělení a motivovalo návštěvníka k akci – např. vyplnění formuláře nebo žádost o demo.

6.4.1 Tvorba grafických prvků

Grafické prvky pro potřeby landing page a doprovodných materiálů byly navrženy ve vizuálním nástroji Figma. Jejich cílem bylo přehledně vizualizovat klíčové technické koncepty – zejména principy fungování autentizačních protokolů SAML a OIDC – a zároveň podpořit celkovou orientaci návštěvníka na stránce (viz. Obrázek 25).

Na základě výsledků A/B testování a návrhu wireframu byly vytvořeny schémata, která sloužila k rychlému pochopení přínosů integrace řešení ProID. Důraz byl kladen na jednoduchost, čistý design a logické provázání jednotlivých prvků. Grafika byla následně exportována a optimalizována pro webové použití tak, aby nenarušovala rychlost načítání stránky.



Obrázek 25 SAML schéma

(Zdroj: Vlastní zpracování na základě ONELOGIN: SAML vs OIDC [28])

6.5 Shrnutí optimalizace digitální prezentace

Cílem digitální prezentace bylo podpořit získávání nových klientů prostřednictvím efektivně navržené landing page, která bude optimalizována jak z pohledu obsahu, tak uživatelského rozhraní. Na základě benchmarkingu konkurenčních řešení byl vytvořen původní návrh, který byl následně testován pomocí analytických nástrojů Piwik a Hotjar.

Zjištěné nedostatky – zejména vysoký bounce rate a nízká konverze – vedly k vytvoření nové, optimalizované varianty stránky. Klíčové změny zahrnovaly:

- lepší vizuální strukturu a rozvržení obsahu,
- navýšení počtu CTA prvků,
- lepší hierarchii informací a přehlednost,
- doplnění vizuálních prvků (obrázky, ikony),
- úpravu textů a stylu komunikace.

Výsledkem bylo výrazné zlepšení metrik:

- bounce rate klesl z 67,4 % na 48,2 %,
- konverzní poměr vzrostl z 2,3 % na 3,78 %,
- celkový počet návštěvníků se zvýšil z 402 na 612,
- prodloužil se průměrný čas strávený na stránce.

Tyto výsledky potvrzují, že A/B testování, správně strukturovaný obsah a responzivní design hrají klíčovou roli v optimalizaci digitální komunikace směrem ke konverzi návštěvníků.

6.6 Plánování a realizace PPC kampaní

Po vytvoření a optimalizaci finální verze landing page následovalo spuštění PPC kampaní, jejichž hlavním cílem bylo přivést nové relevantní návštěvníky a získat z nich kvalitní leady. Reklamy byly cíleny na prioritní regiony – Německo, Rakousko, Švýcarsko a Polsko – kde je poptávka po řešeních v oblasti identit a bezpečnosti tradičně vysoká.

Kampaně byly nastaveny přes nástroj Google Ads a zaměřovaly se na kombinaci vyhledávacích dotazů souvisejících s tématy jako MFA, SSO nebo Identity Provider. PPC sloužilo jako hlavní akviziční kanál, který měl za úkol přivést návštěvníky přímo na vytvořenou landing page a následně je motivovat k odeslání formuláře, stažení brožury nebo žádosti o demo.

Nastavení kampaní a následné ladění probíhalo postupně – od testování vhodných klíčových slov až po úpravy reklamních sestav, textů a cílení. Postup a výsledky jsou popsány v následujících podkapitolách.

6.6.1 Nastavení PPC

Jak bylo uvedeno výše, reklamní kampaně byly primárně zaměřeny na náš cílový region – DACH (Německo, Rakousko, Švýcarsko), který je z hlediska zájmu o kybernetickou bezpečnost a firemní řešení nejperspektivnější. Pro jejich realizaci byl zvolen nástroj Google Ads.

Nejprve bylo vytvořeno geografické cílení na zmíněné země a jazyk kampaně byl nastaven na angličtinu, která je v B2B segmentu běžná. Následně byla nastavena Search kampaň s vybranými klíčovými slovy, která byla relevantní pro dané řešení (viz. Obrázek 26). Kampaň byla doplněna o reklamy ve vyhledávači, v nichž byly použity běžně vyhledávané výrazy typu vpn security, mfa vpn nebo mfa for openvpn, které slibovaly vyšší míru zobrazení (viz. Obrázek 27).

Každá z reklam v této kampani směřovala výhradně na optimalizovanou landing page vytvořenou pro řešení OpenVPN (viz. Obrázek 20a, b, c), jejímž cílem byl sběr nových kontaktů prostřednictvím jasně definovaných výzev k akci. Právě na tuto stránku byla předtím provedena A/B testovací optimalizace (kapitola 6.3), aby se maximalizoval konverzní poměr.

Kampaň byla aktivní po dobu jednoho měsíce, v jehož průběhu byla průběžně monitorována výkonnost jednotlivých klíčových slov a úpravami optimalizována pro dosažení lepších výsledků.

Název kampaně	RDP (DACH)	▼
Cíle konverzí	Cíl kampaně: Odeslání formuláře pro zájemce	▼
Získání zákazníka	Nabízet stejnou cenu za nové i za stávající zákazníky	▼
Marketingový cíl	Potenciální zákazníci	▼
Stav kampaně	● Aktivní	▼
Sítě	Vyhledávací síť Google	▼

Lokality

Vyberte lokality pro tuto kampaň ?

☐ Všechny země a území
☐ Česko
☒ Zadat jinou lokalitu

Lokalita (4)	Zásah ?	×
Německo země	78 400 000	×
Rakousko země	10 800 000	×
Švýcarsko země	9 510 000	×

Obrázek 26 Nastavené regiony

(Zdroj: Google Ads)

☐ ● [vpn security]	Přesná shoda	Aktivní	22,00	692,39 Kč	—	277	5 720	4,84 %
☐ ● "mfa vpn"	Frázová shoda	Aktivní	0,00	0,00 Kč	—	1	30	3,33 %
☐ ● "mfa for vpn"	Frázová shoda	Aktivní	0,00	0,00 Kč	—	1	21	4,27 %
☐ ● [mfa vpn]	Přesná shoda	Aktivní	0,00	0,00 Kč	—	0	4	0,00 %
☐ ● [mfa for openvpn]	Přesná shoda	Aktivní	0,00	0,00 Kč	—	0	4	0,00 %

Obrázek 27 Nastavení klíčových slov

(Zdroj: Google Ads)

Zkuste přidat několik dalších odlišných nadpisů nebo odepněte některé podklady

Síla reklamy ?
Dobrá

- ✓ Přidejte další nadpisy [Zobrazit návrhy](#)
- ✓ Přidejte do nadpisů oblíbená klíčová slova [Zobrazit návrhy](#)
- ✓ Nechte své nadpisy více vyniknout [Zobrazit návrhy](#)
- ✓ Nechte své popisy více vyniknout [Zobrazit návrhy](#)

U responzivních reklam ve vyhledávání zadáte několik nadpisů a popisů a Google z nich potom složí reklamy. ?

Cílová URL ?

Cílová URL
`https://proid.cz/aplikace-proid-mobile-nove-podporuje-oj`
Bude se používat při navrhování podkladů pro vaši reklamu

Zobrazovaná cesta ?

proid.cz / `mfa-for-openvpn` /
15 / 15 0 / 15

Nadpisy 15/15 ?

Náhled

Sponsored

Proid
www.proid.cz/mfa-for-openvpn

2FA for VPN - Secure and Seamless Connection

Secure Your Remote Desktops with Multi-Factor Authenticator. Simple for Users & Admins. Secure OpenVPN with MFA, Smart Cards or Tokens. Protect Your Most Valuable Assets. Free Demo. Easy & Quick Setup. Simple & Secure.

[Modern MFA for Companies](#) [How to set up MFA](#)

Obrázek 28 Nastavená reklama

(Zdroj: Google Ads)

6.6.2 A/B testování klíčových slov – Varianta A

Tato část se věnuje první testované variantě klíčových slov v rámci A/B kampaně – konkrétně sadě obsahující zkratku MFA (Multi-Factor Authentication). Cílem bylo ověřit, jaký výkon tato klíčová slova dosahují z hlediska míry prokliku (CTR), počtu konverzí a celkového konverzního poměru. Varianta A byla nasazena jako první, za stejných podmínek jako druhá testovaná skupina – tedy se stejným rozpočtem, cílením i strukturou reklamních sestav.

Výsledky testování varianty A jsou shrnuty v následující tabulce (viz. Tabulka 2) a budou dále porovnány s výsledky varianty B.

Klíčové slovo	Typ shody	Stav	Konverze	Kliknutí	Zobrazení	CTR	Konverzní poměr
[MFA to PVN]	Přesná shoda	Aktivní	25	300	6000	5,00 %	8,33 %
"mfa vpn"	Frázová shoda	Aktivní	18	175	3400	5,15 %	7,14 %
"mfa secure vpn"	Frázová shoda	Aktivní	10	90	1600	5,63 %	6,25 %
[MFA with VPN]	Přesná shoda	Aktivní	4	38	700	5,43 %	5,26 %
[mfa for openvpn]	Přesná shoda	Aktivní	7	25	550	4,55 %	4,00 %

Tabulka 2 Porovnání klíčových slov

(Zdroj: Google Ads)

6.6.3 A/B testování klíčových slov – Varianta B

Ve druhé fázi A/B testování byla nasazena sada klíčových slov obsahujících zkratku 2FA (Two-Factor Authentication), která je rovněž běžně využívána v oblasti IT bezpečnosti. Cílem této varianty bylo vyhodnotit, zda klíčová slova se zkratkou 2FA dosahují srovnatelných nebo lepších výsledků oproti předchozí variantě založené na výrazu MFA.

Podmínky testování zůstaly nezměněny – stejný rozpočet, identické geografické cílení i struktura kampaně. Výsledky varianty B jsou shrnuty v následující tabulce (viz. Tabulka 3) a slouží jako podklad pro závěrečné porovnání obou testovaných skupin.

Klíčové slovo	Typ shody	Stav	Konverze	Kliknutí	Zobrazení	CTR	Konverzní poměr
[2FA to PVN]	Přesná shoda	Aktivní	8	120	2600	4,62 %	6,67 %
"2fa vpn"	Frázová shoda	Aktivní	5	68	1200	5,67 %	5,88 %
"2fa secure vpn"	Frázová shoda	Aktivní	2	16	400	4,00 %	3,12 %
[2FA with VPN]	Přesná shoda	Aktivní	1	12	260	4,62 %	2,50 %
[2fa for openvpn]	Přesná shoda	Aktivní	2	7	200	3,50 %	2,86 %

Tabulka 3 Porovnání klíčových slov

(Zdroj: Google Ads)

6.6.3.1 Vyhodnocení A/B testování

V rámci optimalizace výkonnostní kampaně v systému Google Ads bylo provedeno A/B testování, jehož cílem bylo zjistit, zda klíčová slova obsahující zkratku MFA (Multi-Factor Authentication) dosahují lepších výsledků než jejich ekvivalentní varianty se zkratkou 2FA (Two-Factor Authentication). Obě testované skupiny obsahovaly pět tematicky souvisejících klíčových slov ve frázové a přesné shodě. Klíčová slova byla nasazena do samostatných reklamních sestav se stejným rozpočtem, totožným geografickým cílením a shodnou strukturou.

Výkonnost byla hodnocena na základě hlavních metrik: počet kliknutí, počet zobrazení, míra prokliku (CTR), počet konverzí a konverzní poměr.

Na základě získaných dat bylo zjištěno, že klíčová slova se zkratkou MFA vykazovala vyšší míru prokliku i konverzní poměr a generovala více než trojnásobný počet konverzí ve srovnání s variantou 2FA. Tato výkonnostní převaha byla patrná napříč všemi sledovanými metrikami.

Výsledky testování naznačují, že zkratka „MFA“ působí v kontextu B2B segmentu a tématu digitální identity důvěryhodněji a přitažlivěji než tradičnější označení „2FA“.

Na základě těchto poznatků lze doporučit, aby byly při optimalizaci PPC kampaní v oblasti vícefaktorového ověřování a přístupového zabezpečení preferovány varianty s označením MFA, které vykazují vyšší efektivitu z hlediska získávání relevantních návštěvníků i dosažených konverzí.

6.6.3.2 Hodnocení kampaní

Přestože se původně očekával výrazně lepší výkon varianty A (viz. kapitola 6.6.2), výsledky varianty B (viz. kapitola 6.6.3) příjemně překvapily a ukázaly, že rozdíly nejsou tak výrazné, jak předpokládala původní hypotéza. Obě varianty přinesly cenné poznatky o chování cílové skupiny. Klíčovým zjištěním bylo, že efektivita klíčových slov není dána pouze použitou zkratkou (MFA vs. 2FA), ale především jejich kombinací s kontextově silnými výrazy, jako je například „VPN“. V době testování byla tato tematika v DACH regionu výrazně vyhledávaná, což se odrazilo na vyšší míře prokliků i konverzním poměru.

Pro potvrzení těchto výsledků bylo provedeno obdobné testování také ve spojení s klíčovým slovem „RDP“, kde se ukázal prakticky totožný trend – varianta MFA opět dosahovala lepších výsledků, nicméně výkonnost 2FA frází nebyla výrazně pozadu. Testování s VPN navíc přineslo statisticky validnější data díky vyššímu objemu vyhledávání a širší cílové skupině.

Z toho vyplývá, že pro budoucí kampaně má smysl využívat oba pojmy, s důrazem na kombinace s aktuálně vyhledávanými technologiemi v daném trhu a čase.

6.6.4 Chování uživatele

Pro detailnější porozumění chování návštěvníků kampaní byla provedena analýza dostupných dat z nástroje Google Ads. Z ní vyplynulo několik důležitých poznatků, které byly využity pro optimalizaci cílení a lepší pochopení cílové skupiny.

Největší počet návštěv i konverzí byl zaznamenán z mobilních zařízení, zatímco počítače zůstaly na druhém místě. Tento výsledek mírně překvapil vzhledem k očekávání dominantního využití desktopových zařízení v rámci B2B segmentu, avšak může být ovlivněn hybridní pracovní dobou nebo uživatelskými zvyklostmi při vyhledávání informací mimo pracovní prostředí.

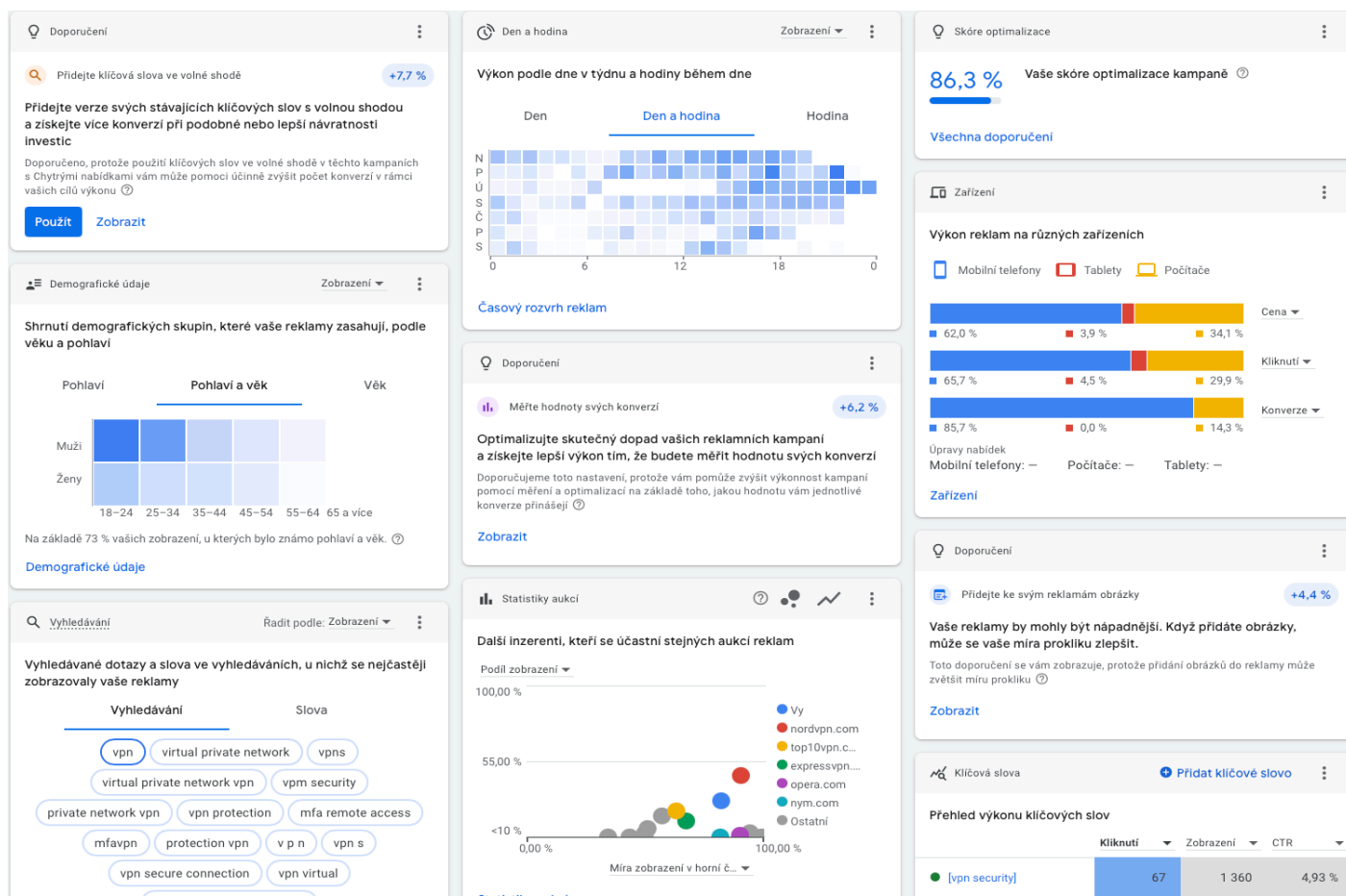
Nejčastěji používané vyhledávací výrazy zahrnovaly například:

- vpn security
- mfa remote access
- vpn protection

což potvrzuje relevance nastavených klíčových slov v kampaních.

Nejvyšší míra zobrazení i prokliků byla zaznamenána ve všední dny, zejména od pondělí do středy v odpoledních a večerních hodinách (cca mezi 17:00–22:00) (viz. Obrázek 27), což odpovídá období, kdy se cílová skupina intenzivně věnuje odborným tématům a vyhledává informace pro pracovní účely.

Z demografického pohledu byli nejčastějšími návštěvníky muži ve věku 18–24 a 25–34 let (viz. Obrázek 29), což je v souladu s očekáváním vzhledem k technickému zaměření kampaní a typickému věkovému rozložení pracovníků v IT a technologiích.



Obrázek 29 Přehled z Google Ads

(Zdroj: Google Ads)

7 VÝSLEDKY A VYHODNOCENÍ

7.1 Dopad projektu

Cílem projektu bylo zvýšit digitální přítomnost řešení ProID na zahraničních trzích a navrhnout funkční strategii pro akvizici nových kontaktů, včetně oslovení potenciálních partnerů – jak stanovuje zadání bakalářské práce. Tohoto cíle se podařilo dosáhnout prostřednictvím kombinace technické integrace, vytvoření optimalizované landing page, řízených PPC kampaní a e-mailových oslovení. Výsledkem byl nárůst kvalifikovaných leadů a zájem partnerů o další komunikaci. Generované kontakty byly následně předány obchodnímu oddělení k dalšímu zpracování. Kromě toho projekt přispěl ke zvýšení povědomí o značce ProID, zejména v regionu DACH, a potvrdil, že i s omezenými prostředky lze v B2B prostředí realizovat efektivní akviziční strategii.

7.2 Možnosti dalšího rozvoje

Na základě získaných dat a praktických zkušeností se jako vhodný krok dalšího rozvoje jeví navázání hlubší spolupráce s distributory a systémovými integrátory, a to především v regionech, kde již vznikl základní zájem. Udržitelnost a škálovatelnost projektu lze dále podpořit využitím referencí z úspěšných integrací, rozšířením přítomnosti na platformě G2, nebo tvorbou specializovaných obsahových kampaní. Cenné výstupy z této fáze lze využít i pro tvorbu šablon a procesních rámců pro budoucí trhy či další produktové řady.

7.3 Překážky

Za největší výzvu se ukázala fáze oslovování potenciálních partnerů, zejména u zahraničních společností, kde bylo často obtížné navázat konzistentní dialog. V některých případech sice dorazila úvodní odpověď, nicméně následná komunikace již nepokračovala a follow-up nevedl k domluvení schůzky či navázání další spolupráce. Ukázalo se, že zásadní roli hraje nejen kvalita prvotního oslovení, ale také načasování a motivace protistrany. I přes tato omezení se podařilo identifikovat segmenty a typy společností, které jsou pro budoucí akviziční aktivity nejvhodnější.

7.4 Návrhy na zlepšení do budoucna

Jelikož se svět digitální akvizice neustále vyvíjí a tempo změn je stále rychlejší, je důležité pokračovat v A/B testování nejen na úrovni kampaní a klíčových slov, ale i struktury a

vizuální stránky landing page. Vhodné je také experimentovat s formátem obsahu a způsobem prezentace přínosů pro zákazníka. Z dlouhodobého hlediska může být přínosné rozšířit práci s remarketingem a začít využívat automatizované e-mailové sekvence pro lepší konverzi nově získaných leadů. Veškeré změny by měly být řízeny daty a průběžně vyhodnocovány za účelem kontinuální optimalizace.

7.5 Vlastní přínos

V průběhu realizace byly provedeny praktické úkony napříč celým marketingovým a technickým spektrem – od návrhu a implementace landing page, přes přípravu PPC kampaní, vedení A/B testů a správu analytických nástrojů, až po komunikaci s partnery a validaci integrací. Zvláštní důraz byl kladen na měření a vyhodnocení výsledků, což vedlo ke zvyšování efektivity jednotlivých kroků. Realizací projektu se výrazně prohloubily znalosti v oblasti B2B marketingu, akvizičních strategií a digitální analytiky, které budou nadále využitelné v profesní praxi.

ZÁVĚR

Cílem této bakalářské práce bylo představit strategii získávání nových klientů pro firemní řešení ProID na evropském trhu, a to s využitím kombinace technické integrace, digitálního marketingu a přímé akviziční aktivity. Práce ukázala, že i v prostředí B2B, kde je kladen důraz na odbornost, důvěryhodnost a efektivní komunikaci, lze při správném nastavení jednotlivých aktivit dosáhnout reálných a měřitelných výsledků.

V teoretické části byly popsány klíčové aspekty kybernetické bezpečnosti a digitální identity, stejně jako principy moderní autentizace a marketingové nástroje využitelné pro akvizici nových partnerů. Praktická část následně demonstrovala, jak lze tyto poznatky aplikovat v reálném projektu – od benchmarkingu, přes návrh a optimalizaci landing page, realizaci PPC kampaní, A/B testování klíčových slov až po navazování spolupráce s vybranými softwarovými společnostmi.

Projekt prokázal, že cílenou a vytrvalou prací, založenou na testování a analytickém vyhodnocování, lze i s omezenými prostředky výrazně zvýšit digitální viditelnost řešení, generovat kvalitní leady a posílit pozici značky na zahraničních trzích. Zároveň byly identifikovány oblasti s potenciálem dalšího rozvoje – například využití osobních doporučení nebo hlubší práce s komunitou partnerů.

Tato práce tak může sloužit nejen jako případová studie úspěšné marketingové a obchodní iniciativy, ale i jako praktický návod pro firmy, které chtějí v evropském prostoru rozvíjet své řešení v oblasti digitální identity a bezpečného přístupu.

SEZNAM POUŽITÉ LITERATURY

- [1] TOUHILL, Gregory J. a C. Joseph TOUHILL. Cybersecurity for executives: a practical guide. Hoboken, New Jersey: Touhill, 2014. ISBN 978-1-118-90881-5. Dostupné také z: <https://ebookcentral.proquest.com/lib/natl-ebooks/detail.action?docID=1707094>
- [2] Doporučení pro správu identit a přístupu. rwfsoft Learn [online]. 2024 [cit. 2025-06-04]. Dostupné z: <https://learn.microsoft.com/cs-cz/azure/well-architected/security/identity-access>
- [3] NIZICH, Michael. The cybersecurity workforce of tomorrow. Bingley, U.K.: Emerald Publishing Limited, 2023. The future of work. ISBN 978-1-80382-917-3. Dostupné také z: <https://doi.org/10.1108/9781803829159>
- [4] Cost of a Data Breach Report 2024 [online]. IBM Corporation, 2024 [cit. 2025-06-04]. Dostupné z: <https://www.ibm.com/reports/data-breach>
- [5] RAWAL, Bharat S. Cybersecurity and Identity Access Management [online]. Springer, 2022 [cit. 2025-06-04]. ISBN 9811926581. Dostupné z: https://www.google.cz/books/edition/Cybersecurity_and_Identity_Access_Manage/N-p3EAAAQBAJ?hl=cs&gbpv=0
- [6] Co to je Fido2? Microsoft [online]. 2024 [cit. 2025-06-04]. Dostupné z: <https://www.microsoft.com/cs-cz/security/business/security-101/what-is-fido2>
- [7] FANTI, Marco. Implementing Multifactor Authentication: Protect your applications from cyberattacks with the help of MFA. Fanti, 2023. ISBN 978-1803246963.
- [8] Zero Trust Networks: Building Secure Systems in Untrusted Networks. Gilman, 2017. ISBN 978-1491962190.
- [9] EIDAS Regulation. European Commission [online]. 2024 [cit. 2025-06-04]. Dostupné z: <https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation>
- [10] NGO, David Chek Ling. Biometric Security. Cambridge, 2015. ISBN 9781443874991.
- [11] MASON, Stephen. Electronic Evidence and Electronic Signatures. Mason, 2021. ISBN 9781911507260.
- [12] FIDO Alliance. FIDO2 Specifications. FIDO Alliance [online]. 2024 [cit. 2025-06-04]. Dostupné z: <https://fidoalliance.org/specifications/>
- [13] Cybersecurity and EU Law. Karathanasis, 2024. ISBN 9781040229682.

- [14] Bezpečnost informačních systémů. Jašek, Roman, 2022. ISBN 978-80-7454-312-8.
- [15] WANECKI, Pavel, Roman JAŠEK a Irena DROFOVÁ. The contribution of the European NIS2 directive to the design of the cyber security model. In: International Conference on Information and Digital Technologies 2023 (IDT 2023). 2023, s. 149–154. ISBN 979-835030586-9. Dostupné z: <https://doi.org/10.1109/IDT59031.2023.10194454>
- [16] ISO/IEC 27001:2022 – Information Security Management. IT Governance [online]. 2023 [cit. 2025-06-04]. Dostupné z: <https://www.itgovernance.co.uk/iso27001>
- [17] ISO 27001/ISO 27002 A guide to information security management systems [online]. It Governance Publishing, 2023 [cit. 2025-06-04]. ISBN 9781787784956. Dostupné z: https://www.google.cz/books/edition/ISO_27001_ISO_27002_A_guide_to_informati/qyHkEAAAQBAJ?hl=cs&gbpv=0
- [18] Mastering SSO. Cybellium, 2023. ISBN 9798859143269.
- [19] METHENY, Matthew. Federal Cloud Computing. Metheny, 2017. ISBN 9780128096871.
- [20] AUTH0. What is SAML? Auth0 [online]. 2024 [cit. 2025-06-04]. Dostupné z: <https://auth0.com/intro-to-iam/what-is-saml>
- [21] OpenID Foundation. How OpenID Connect Works. OpenID.net [online]. 2024 [cit. 2025-06-04]. Dostupné z: <https://openid.net/developers/how-connect-works/>
- [22] Interní materiály firmy, 2025
- [23] G2. Get started with G2 [online]. G2, 2022 [cit. 2025-06-04]. Dostupné z: <https://documentation.g2.com/docs>
- [24] CIALDINI. Influence, New and Expanded: The Psychology of Persuasion. Harper, 2021. ISBN 9780063136892.
- [25] WEISSMAN, Jerry. Presenting to win: the art of telling your story. Updated and expanded ed. New Jersey: Upper Saddle River, 2009. ISBN 978-0-13-714417- 4
- [26] CLARKE, Adam. SEO 2023: Learn search engine optimization with smart internet marketing strategies. Clarke, 2022. ISBN 979-8365383173.
- [27] NASSERY, Leemay. Practical A/B Testing: Creating Experimentation-Driven Products. 1. vydání. [s.l.]: Pragmatic Programmers, 2023. 166 s. ISBN 9798888650080.

[28] ONELOGIN. SAML vs OIDC: All You Need to Know [online]. [cit. 2025-06-08].

Dostupné z: <https://www.onelogin.com/learn/oidc-vs-saml>

SEZNAM OBRÁZKŮ

Obrázek 1 Průměrné náklady na únik dat.....	15
Obrázek 2 Schéma SAML protokolu.....	23
Obrázek 3 Schéma OIDC protokolu.....	25
Obrázek 4 Rozhraní Leadspickeru.....	37
Obrázek 5 Rozhraní Leadspickeru pro odesílání.....	38
Obrázek 6 Report Leadspickeru odeslaných emailů.....	39
Obrázek 7 Ukázka prezentace.....	41
Obrázek 8 Ukázka prezentace.....	41
Obrázek 9 Ukázka prezentace.....	42
Obrázek 10 Graf úspěšnosti oslovení	43
Obrázek 11 Ukázka přihlášení.....	45
Obrázek 12 Ukázka ProID Mobile	46
Obrázek 13 Ukázka ProID Mobile	46
Obrázek 14 Wireframe - sběr kontaktů.....	48
Obrázek 15 Celý wireframe.....	49
Obrázek 16 První landing page.....	51
Obrázek 17 Graf návštěvnosti z Piwik	52
Obrázek 18 Data z Piwik	52
Obrázek 19 Data z Hotjar	52
Obrázek 20a Optimalizovaná landing page.....	54
Obrázek 21 Graf návštěvnosti z Piwik	56
Obrázek 22 Data z Piwik	56
Obrázek 23 Data z Hotjar	57
Obrázek 24 Landing page ze strany WordPressu.....	58
Obrázek 25 SAML schéma.....	59
Obrázek 26 Nastavené regiony	62
Obrázek 27 Nastavení klíčových slov	62
Obrázek 28 Nastavená reklama	63

SEZNAM TABULEK

Tabulka 1 Seznam softwaru.....	35
Tabulka 2 Porovnání klíčových slov.....	63
Tabulka 3 Porovnání klíčových slov.....	64

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2FA	Two-Factor Authentication – dvoufaktorová autentizace
B2B	Business-to-Business – obchod mezi firmami
B2C	Business-to-Consumer – obchod se spotřebiteli
BOZP	Bezpečnost a ochrana zdraví při práci
CSS	Cascading Style Sheets – stylování webových stránek
CTR	Click-Through Rate – míra prokliků
DACH	Deutschland, Austria, Confoederatio Helvetica – německy mluvící trh
eIDAS	electronic IDentification, Authentication and trust Services – evropské nařízení pro elektronickou identitu a důvěryhodné služby
FIDO2	Fast IDentity Online 2 – standard pro silnou autentizaci
GDPR	General Data Protection Regulation – nařízení EU o ochraně osobních údajů
G2	Platforma pro recenze B2B softwaru
HTML	HyperText Markup Language – značkovací jazyk
HTTP	HyperText Transfer Protocol – protokol pro přenos dat
IAM	Identity and Access Management – správa identit a přístupů
IdP	Identity Provider – poskytovatel identity
IBM	International Business Machines – technologická společnost
IS	Informační systém
ISMS	Information Security Management System – systém řízení bezpečnosti informací
ISO	International Organization for Standardization – mezinárodní standardizace
JWT	JSON Web Token – bezpečný formát pro přenos informací
MFA	Multi-Factor Authentication – vícefaktorová autentizace
NIS2	Network and Information Security Directive 2 – evropská směrnice o kybernetické bezpečnosti
OIDC	OpenID Connect – autentizační protokol pro jednotné přihlášení

OAuth 2.0	Otevřený protokol pro autorizaci
PIN	Personal Identification Number – osobní identifikační číslo
PPC	Pay-Per-Click – reklamní model založený na prokliku
QES	Qualified Electronic Signature – kvalifikovaný elektronický podpis
RDP	Remote Desktop Protocol – vzdálený přístup k počítači
SaaS	Software as a Service – software jako služba
SAML	Security Assertion Markup Language – protokol pro autentizaci
SEO	Search Engine Optimization – optimalizace pro vyhledávače
SP	Service Provider – poskytovatel služby
SSO	Single Sign-On – jednotné přihlášení
UTB	Univerzita Tomáše Bati ve Zlíně
VPN	Virtual Private Network – virtuální privátní síť
XML	Extensible Markup Language – značkovací jazyk