

Zabezpečení dat v Salesforce: analýza rizik, implementace bezpečnostních opatření a doporučení pro správu

Ing. Štěpán Bill



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav informatiky a umělé inteligence

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Ing. Štěpán Bill
Osobní číslo:	A23398
Studijní program:	N0613A140022 Informační technologie
Specializace:	Kybernetická bezpečnost
Forma studia:	Kombinovaná
Téma práce:	Zabezpečení dat v Salesforce: analýza rizik, implementace bezpečnostních opatření a doporučení pro správu
Téma práce anglicky:	Data Security in Salesforce: Risk Analysis, Implementation of Security Measures and Management Recommendations

Zásady pro vypracování

- Proveďte literární rešerši problematiky zabezpečení dat na cloudové CRM platformě Salesforce.
- Identifikujte hlavní hrozby a zranitelnosti, které mohou ohrozit data a přístup v Salesforce.
- Sstanovte vhodná bezpečnostní doporučení pro efektivní správu Salesforce prostředí.
- Proveďte technická opatření a ověřte pomocí vybraných simulovaných útoků jejich účinnost.
- Proveďte kritickou diskusi nad výstupy práce.

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

Seznam doporučené literatury:

1. BLOKDYK, Gerardus. Salesforce Security Testing. 5STARCook, 2022. ISBN 978-0655447849.
2. DOLEJŠ, Milan. Cloud computing a jeho bezpečnost. Praha: Grada, 2015. ISBN 978-80-247-5360-3
3. CHEN, T., et al. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. 2. vyd. Sebastopol: O'Reilly Media, 2021. ISBN 978-1-492-02793-7
4. Oracle Corporation. Securing the Cloud: A Comprehensive Guide. San Francisco: McGraw-Hill, 2020. ISBN 978-1-260-45345-6.
5. Salesforce. Salesforce Security Guide. [online]. [cit. 2024-10-19]. Dostupné z: https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide/meta/securityImplGuide/salesforce_security_guide.htm

Vedoucí diplomové práce: **prof. Mgr. Roman Jašek, Ph.D., DBA**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **27. října 2024**
Termín odevzdání diplomové práce: **2. června 2025**



L.S.

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

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 17. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou 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 – diplomovou 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 diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové 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 diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato diplomová práce se zabývá problematikou zabezpečení dat v prostředí cloudové platformy Salesforce. Cílem práce je analyzovat bezpečnostní architekturu systému, identifikovat klíčové hrozby a zranitelnosti a navrhnout účinná bezpečnostní opatření pro ochranu dat a řízení přístupu. Součástí práce je také praktické ověření vybraných bezpečnostních funkcí a testování možných scénářů zneužití. Pozornost je věnována především přístupovým tokenům, možnostem omezení přístupu podle IP adres a času, správě oprávnění a chování systému při různých konfiguracích. Práce rovněž upozorňuje na riziko zneužití access tokenu, pokud není správně zabezpečeno prostředí. Výsledkem je soubor doporučených bezpečnostních opatření a konfigurací, které mohou pomoci organizacím zvýšit úroveň ochrany dat v Salesforce. Pro pokročilé bezpečnostní nastavení je dále doporučeno využití rozšíření Salesforce Shield.

Klíčová slova: Salesforce, CRM, cloud, cloudové CRM, zabezpečení dat, přístupová oprávnění, autentizace, API, audit, GDPR, Salesforce Shield

ABSTRACT

This thesis focuses on the issue of data security within the Salesforce cloud platform. The aim of the work is to analyze the system's security architecture, identify key threats and vulnerabilities, and propose effective measures for data protection and access control. The thesis also includes practical verification of selected security functions and testing of potential misuse scenarios. Special attention is given to access tokens, access restrictions based on IP ranges and login hours, permission set management, and system behavior under various configurations. The thesis highlights the risk of abusing the access token as a substitute for a standard API bearer token when the environment is not properly secured. The result is a set of recommended security configurations and practices that can help organizations enhance their data protection in Salesforce. For advanced auditing and encryption, the use of Salesforce Shield is recommended.

Keywords: Salesforce, CRM, cloud, cloud CRM, data security, access permissions, authentication, API, audit, GDPR, Salesforce Shield

Rád bych poděkoval vedoucímu diplomové práce, panu prof. Mgr. Romanu Jaškovi, Ph.D., DBA, za odborné vedení, cenné rady, vstřícnost a podporu během celého zpracování této práce. Velké poděkování patří také mé rodině za trpělivost, pochopení a podporu, kterou mi po celou dobu studia poskytovala.

OBSAH

ÚVOD	11
I TEORETICKÁ ČÁST	12
1 CRM A CLOUD COMPUTING.....	13
1.1 CRM	13
1.2 IMPLEMENTACE CRM	13
1.3 BEZPEČNOSTNÍ ASPEKTY CRM.....	15
1.4 CLOUD COMPUTING	15
1.4.1 Bezpečnost Cloud computingu.....	16
2 SALESFORCE	18
2.1 HISTORIE SALESFORCE	20
2.2 DALŠÍ CLOUDOVÉ CRM	20
2.2.1 Microsoft Dynamics 365.....	21
2.2.2 Oracle CRM Cloud.....	21
2.2.3 SAP CRM	22
2.2.4 Adobe Experience Cloud	22
3 GDPR A PRÁVNÍ POŽADAVKY	23
3.1 ZÁKLADNÍ PRINCIPY GDPR.....	23
3.2 PRÁCE S DATY V SALESFORCE	24
4 BEZPEČNOSTNÍ ARCHITEKTURA SALESFORCE	26
4.1 ŠIFROVÁNÍ DAT	26
4.2 ARCHITEKTURA A SEGREGACE DAT	27
4.3 BEZPEČNOSTNÍ STANDARDY SALESFORCE.....	27
4.4 SALESFORCE SHIELD	29
4.4.1 Platform Encryption	29
4.4.2 Real Time Event Monitoring	30
4.4.3 Field Audit Trail.....	31
4.4.4 Data Detect.....	31
4.5 BEZPEČNOST JAZYKA APEX	32
4.6 SECURITY HEALTH CHECK	33
5 SPRÁVA OPRÁVNĚNÍ A PŘÍSTUPU.....	35
5.1 OVĚŘOVÁNÍ UŽIVATELŮ	35
5.2 SPRÁVA OPRÁVNĚNÍ.....	36
5.2.1 Profile.....	36
5.2.2 Permission Set	37
5.2.3 Role.....	37
II PRAKTICKÁ ČÁST.....	39

6	PŘÍPRAVA SALESFORCE PROSTŘEDÍ	40
7	ANALÝZA PŘÍSTUPOVÝCH OPRÁVNĚNÍ	42
7.1	DATA MINING SALESFORCE PROFILŮ.....	42
7.1.1	Vstupní data	42
7.1.2	Frekvenční analýza.....	42
7.1.3	Clustering profilů pomocí K-Means	44
7.1.4	Detekce anomálií pomocí DBSCAN.....	45
8	ZABEZPEČENÍ API A TOKENŮ.....	46
8.1	AUTORIZACE PŘES CONNECTED APP.....	46
8.1.1	OAuth Autorizace	50
8.1.2	Přístup k objektům přes API.....	52
8.2	AUTORIZACE PŘES WEB.....	55
8.3	MOŽNOSTI ZNEUŽITÍ ACCESS TOKENU	57
8.4	TESTOVÁNÍ LOGIN HOURS A LOGIN IP RANGES	58
9	ANALÝZA ZRANITELNOSTI SALESFORCE.....	60
9.1	RIZIKA 3RD PARTY APLIKACÍ.....	61
9.2	ZNÁMÉ ZRANITELNOSTI SALESFORCE	61
10	BEZPEČNOSTNÍ INCIDENTY A MONITORING	63
11	DOPORUČENÉ POSTUPY.....	65
	ZÁVĚR.....	67
	SEZNAM POUŽITÉ LITERATURY	69
	SEZNAM OBRÁZKŮ.....	72
	SEZNAM TABULEK	73
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	74
	SEZNAM PŘÍLOH.....	75

ÚVOD

V dnešní době se cloudová řešení stávají nedílnou součástí firemní infrastruktury. Podniky všech velikostí se stále častěji spoléhají na externí platformy, které jim umožňují flexibilní správu zákaznických dat, komunikaci, plánování i automatizaci obchodních procesů. Jedním z nejvýznamnějších poskytovatelů cloudových CRM systémů je společnost Salesforce, jejíž platforma je využívána miliony uživatelů po celém světě. V posledních letech je Salesforce velice populárním řešením a jeho podíl na trhu neustále roste. Ačkoliv přináší výhody z hlediska dostupnosti, škálovatelnosti a integrace, současně s sebou nese i zvýšené nároky na zabezpečení dat, která jsou v prostředí cloudu uložena.

Tato diplomová práce se zaměřuje na zabezpečení dat v prostředí Salesforce, a to jak z hlediska teoretického rámce, tak z pohledu konkrétních technických opatření a jejich účinnosti. Cílem práce je poskytnout ucelený přehled o bezpečnostním modelu platformy, identifikovat možné hrozby a zranitelnosti, navrhnout vhodná opatření a ověřit jejich funkčnost v kontrolovaném prostředí.

V první části je provedena literární rešerše zaměřená na problematiku cloudových CRM systémů, ochrany osobních údajů dle nařízení GDPR a architekturu platformy Salesforce. Dále je zde popsán její bezpečnostní model, zejména v oblasti autentizace, řízení přístupu, správy oprávnění a ochrany dat. Tato teoretická část tvoří rámec pro následné praktické ověření konkrétních opatření.

Na teoretický základ navazuje praktická část, ve které je provedena analýza přístupových oprávnění pomocí datové analýzy, jsou testovány různé přístupy k autentizaci, nastavování oprávnění a zabezpečení přístupu přes API. Dále jsou popsány konkrétní bezpečnostní hrozby včetně zneužití tokenů a phishingových útoků. Součástí práce je také návrh doporučených bezpečnostních postupů, které vycházejí z osvědčených praktik a výsledků vlastního testování.

I TEORETICKÁ ČÁST

1 CRM A CLOUD COMPUTING

CRM (Customer Relationship Management) a cloud computing jsou dnes klíčovými technologiemi pro moderní podnikání. CRM systémy slouží k efektivnímu řízení vztahů se zákazníky, umožňují firmám analyzovat data a automatizovat interní i externí procesy. Díky cloud computingu jsou tyto systémy dostupné odkudkoliv a odstraňují potřebu nákladné infrastruktury. Další výhodou je vysoká úroveň zabezpečení, pravidelné aktualizace a snadná integrace s dalšími nástroji a platformami. [1]

1.1 CRM

Jedna z definic CRM je, že se jedná o podnikatelskou filozofii a strategii pro získávání a udržení nejhodnotnějších vztahů se zákazníky. CRM vyžaduje zákaznický orientovanou podnikatelskou kulturu pro podporu efektivních marketingových, obchodních a servisních procesů. Cílem je lepší porozumění potřebám zákazníků a kvalitnější reakce na tyto potřeby. [2]

Toto je definice z pohledu podnikatelského neboli firemního a je z ní patrné, že CRM není jen o používání aplikace, ale o celkovém přístupu a orientaci celého business modelu. Z druhého, technického pohledu je CRM software, který přistupuje do databáze k datům a na druhé straně je zobrazuje uživateli. Nad rámec toho jsou přidány analytické nástroje poskytující přehledné reporty, automatizace a obchodní procesy. CRM systém se skládá z několika vrstev: databáze, aplikační logika, uživatelské rozhraní (UI), integrace (API), bezpečnostní a analytická vrstva. Každá databáze má uložená data a již na této úrovni je potřeba řešit rychlost a bezpečnost. [3] [4]

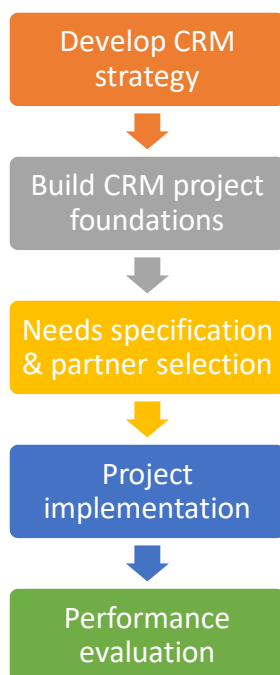
1.2 Implementace CRM

Úspěšná implementace CRM systému není pouze technickou záležitostí, ale představuje komplexní proces, který zahrnuje analýzu potřeb organizace, nastavení procesů, migraci dat, školení uživatelů a postupné přijetí systému v každodenní praxi. Jedním z nejčastějších důvodů selhání CRM projektů je právě podcenění organizačních a lidských faktorů, nikoliv samotné technologie.

V knize Customer Relationship Management Concepts and Technologies je znázorněn tento pěti krokový implementační proces:

- Stanovení CRM strategie

- Rámcové představení vize, nastavení priorit
- Vybudování základů projektu CRM
 - Seznam kritických faktorů, klíčových cílů, identifikace zúčastněných stran, nastavení řídicích struktur projektu
- Specifikace požadavků a výběr dodavatele
 - Analýza požadavků, zhodnocení nabídek, porovnání technologií
- Implementace projektu
 - Implementační plán, záložní plán, návrh architektury, vývoj specifických požadavků, migrace dat, školení uživatelů
- Hodnocení
 - Hodnocení výstupů z projektu a z businessu



Obrázek 1: The five-step implementation process [5]

1.3 Bezpečnostní aspekty CRM

CRM systémy pracují s rozsáhlým množstvím osobních, obchodních a citlivých údajů, proto je jejich zabezpečení klíčovým aspektem celkové důvěryhodnosti a souladu s legislativou. Mezi hlavní bezpečnostní výzvy v CRM prostředí patří autentizace a řízení přístupů, šifrování a ukládání dat, logy a monitoring. Dále je také důležité zabezpečení integrací se systémy třetích stran a pravidelná záloha dat. [5]

Součástí bezpečnostní správy CRM by mělo být také pravidelné školení uživatelů, analýza bezpečnostních událostí a využití nástrojů pro detekci anomálií, na což se dá v dnešní době efektivně využít s umělá inteligence. [5]

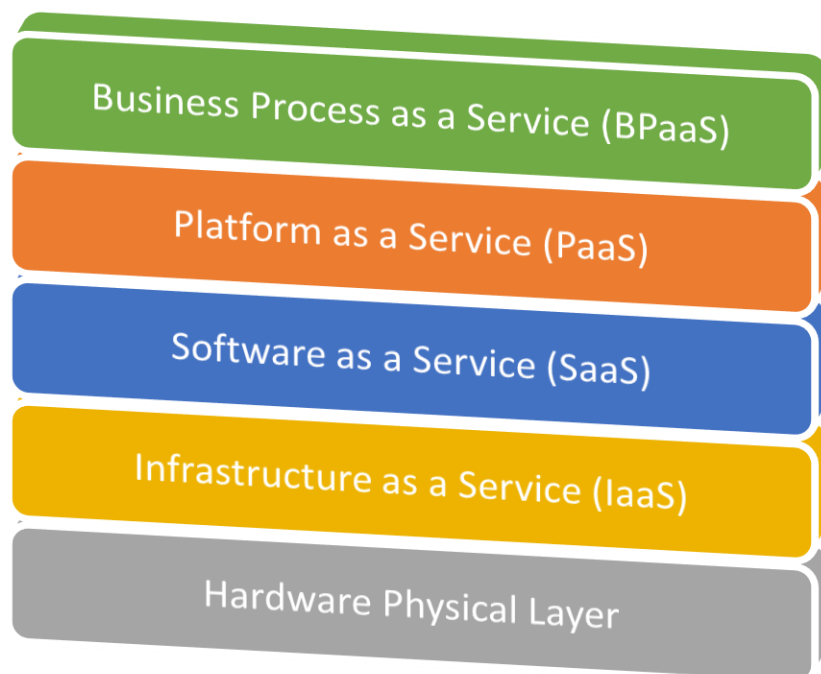
1.4 Cloud Computing

Cloud computing lze definovat jako výpočetní prostředky, uložení, infrastrukturu, procesy a aplikace, které lze kdykoliv používat jako službu, nebo kolekci více služeb přístupem přes síť. Mezi hlavní výhody patří dostupnost, minimální správa a škálovatelnost, podle aktuálních potřeb. Pro firmy tak odpadá nákladná počáteční investice do hardware, který se musí pravidelně aktualizovat. [6]

V současnosti jsou populární tyto modely cloudových služeb:

- **IaaS (Infrastructure as a Service)**
 - Poskytuje základní výpočetní infrastrukturu, virtuální servery, uložení, síť
- **PaaS (Platform as a Service)**
 - Nabízí platformu pro vývoj aplikací
- **SaaS (Software as a Service)**
 - Poskytuje hotovou aplikaci dostupnou přes internet
- **BPaaS (Business Process as a Service)**
 - Služba, obsahující celé obchodní procesy

Jako základní vrstva pro všechny tyto modely je hardwarová, fyzická vrstva, která obsahuje servery, disková pole, sítě, případně celá datacentra. Tato vrstva není pro uživatele dostupná. Přehled jednotlivých vrstev a modelů je zobrazen v následujícím diagramu.



Obrázek 2: Struktura modelů v kontextu cloud computingu [6]

1.4.1 Bezpečnost Cloud computingu

Přestože cloud computing přináší mnoho výhod, přináší i určitá omezení a rizika. Mezi poskytovatelem cloudových služeb a zákazníkem musí vzniknout určitá úroveň důvěry. V rámci toho je přenesena zodpovědnost za bezpečnost dat z firmy na poskytovatele cloudu. [6]

Bezpečnost dat je zcela zásadní pro každou organizaci a jejich ztráta nebo nedostupnost může výrazně poškodit chod firmy. Poskytovatel cloudu je sice plně zodpovědný za správu databáze, avšak zodpovědnost za správu dat zůstává na straně zákazníka. Ten musí zajistit ochranu proti krádeži, neautorizovaným změnám a dodržovat právní normy. Pokud jsou data uložena fyzicky na serveru v jiné zemi mohou podléhat jiným zákonům o ochraně dat. Pokud chce organizace minimalizovat riziko zneužití dat, měla by uvažovat o jejich šifrování.

Další klíčovou rolí v bezpečnosti cloud computingu je síťová bezpečnost. Přesun firemní infrastruktury do cloudu přináší nové výzvy, zejména pokud jde o přenos síťového

provozu. Aplikace různých zákazníků sdílejí stejnou fyzickou síťovou infrastrukturu, což znamená, že citlivá data z jedné aplikace mohou být přenášena po stejné síti jako méně důležitá data jiných uživatelů. Tato skutečnost přináší nové bezpečnostní hrozby, zejména pokud má některý administrátor přístup k celé infrastruktuře a potenciálně může nahlížet na síťový provoz, přestože k tomu nemá žádný oprávněný důvod. V prostředí cloudu, kde poskytovatel spravuje infrastrukturu mimo přímou kontrolu zákazníka, je proto důležité zavádět silnější opatření na kontrolu přístupových práv.[7]

Jako efektivní řešení se nabízí šifrování datového provozu mezi aplikacemi pomocí end-to-end šifrování. Zvláště důležité je to v případě, kdy ke cloudovým službám přistupujeme přes veřejný internet, kde je riziko sdílení infrastruktury s jinými subjekty, včetně konkurence. Jednou z možností, jak zvýšit bezpečnost, je zavedení virtuální privátní sítě (VPN), která vytváří šifrovaný kanál mezi podnikem a poskytovatelem. Ideálně by VPN spojení mělo končit až na úrovni samotné aplikace, aby byla zajištěna maximální ochrana.[7]

2 SALESFORCE

Salesforce je aktuálně jednou z nejvýznamnějších cloudových platforem na světě, zaměřená na správu vztahů se zákazníky. Nabízí širokou škálu nástrojů pro správu obchodních procesů, marketingu, zákaznické podpory a analýzy dat. Díky své cloudové infrastruktuře umožňuje firmám přístup k odkudkoliv a nabízí také bezpečnostní mechanismy. Kromě standardních funkcí lze Salesforce rozšířit pomocí vlastních aplikací, které se vyvíjejí v programovacím jazyce Apex a LWC komponentách. Dále lze Salesforce propojit integrací s dalšími službami a automatizovat procesy pomocí nástrojů Flow.[8]



Obrázek 3: Logo Salesforce

zdroj: Salesforce Media Library

Díky své flexibilitě je oblíbený mezi firmami různých velikostí i odvětví a dnes pomáhá milionům uživatelů efektivněji řídit své podnikání a komunikaci se zákazníky. Salesforce nabízí širokou škálu nástrojů a produktů, které přesahují tradiční CRM systémy. Dnes více než 150 000 firem využívá tento nástroj a má přes 4 miliony aktivních uživatelů ve více než 120 zemích. V roce 2024 dosáhla společnost obrat přes 35 miliard dolarů a aktuálně zaměstnává přes 80 000 lidí po celém světě.[8]

Mezi známé společnosti, používající Salesforce patří například: [9]

- Spotify

- Amazon Web Services
- U.S. Bank
- Toyota
- T-Mobile
- The New York Post
- Canon
- BMW
- Ford
- PayPal
- Mercedes Benz
- ČSOB
- Česká spořitelna



Obrázek 4: Salesforce CRM

zdroj: Salesforce Media Library

2.1 Historie Salesforce

Salesforce byl založen v roce 1999 v San Franciscu. U zrodu stáli Marc Benioff, Parker Harris, Frank Dominguez a Dave Moellenhoff, kteří založili firmu pro automatizaci prodeje. Během prvního roku se společnost rozšířila na 40 zaměstnanců a přesunula se do větších kanceláří. [10]

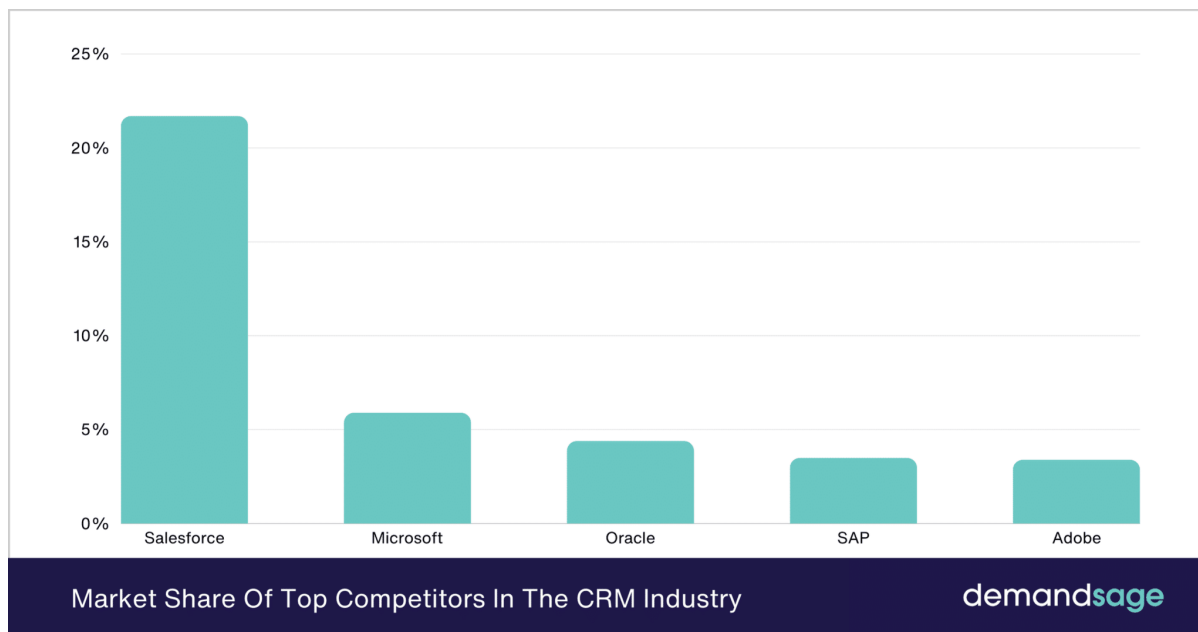
V roce 2000 odstartovali prodej na velké akci v San Franciscu pod sloganem „The end of Software“. Salesforce rychle rostl a v roce 2003 uspořádal první Dreamforce, svou každoroční konferenci, kde představil sForce 2.0, první cloudovou platformu pro vývoj aplikací. O rok později firma vstoupila na burzu a získala 110 milionů dolarů. V roce 2005 uvedla AppExchange, obchod s aplikacemi pro Salesforce. Ve stejném roce měla firma již 1300 zaměstnanců a přes 20 000 zákazníků po celém světě. [10]

V následujících letech Salesforce pokračoval v inovacích, v roce 2009 uvedl Service Cloud pro zákaznickou podporu a v roce 2010 koupil Heroku. Během roku 2012 měl Salesforce obrat přes 3 miliardy amerických dolarů. V roce 2015 představila přelomovou Lightning Experience, zcela nové rozhraní svého CRM, a v roce 2016 přesáhli hranici 25 000 zaměstnanců v 25 zemích světa. [10]

V posledních letech se Salesforce také zaměřil na umělou inteligenci Einstein GPT, kterou představil v roce 2023 a pomáhá zákazníkům využívat AI v CRM. V roce 2024 byl představen Agentforce, nový AI systém zabudovaný přímo v Salesforce platformě. [10]

2.2 Další cloudové CRM

Salesforce si dlouhodobě drží dominantní pozici na trhu CRM řešení s více než 20% podílem, jak ukazuje i aktuální graf podílu jednotlivých hráčů v oboru. [8] Kromě něj však existuje několik dalších významných cloudových CRM platforem, které tvoří konkurenci a nabízejí srovnatelnou nebo specializovanou funkcionalitu. Mezi hlavní konkurenty patří Microsoft Dynamics, Oracle CRM, SAP CRM a Adobe Experience Cloud. Tyto platformy podporují automatizaci obchodních procesů, správu zákaznických vztahů a integraci s dalšími podnikovými nástroji.[8]



Obrázek 5: Podíl jednotlivých CRM platforem na trhu. [8]

2.2.1 Microsoft Dynamics 365

Microsoft Dynamics 365 je podnikové řešení, které kombinuje funkce CRM a ERP. Podporuje řízení prodeje, marketingových aktivit a zákaznické podpory. Díky napojení na další nástroje Microsoftu, jako jsou Azure, Power Platform nebo Microsoft Teams, tvoří integrovaný ekosystém pro střední a velké firmy. Zabezpečení je řešeno přes Azure Active Directory, šifrování a pokročilou správu přístupů. Podle aktuálních statistik drží Dynamics přibližně 5–6% podíl na trhu CRM.[11]

2.2.2 Oracle CRM Cloud

Oracle CX Cloud je řešení cílené především na velké organizace. Nabízí pokročilé nástroje pro řízení prodeje, marketingovou automatizaci, zákaznickou podporu a analýzy chování zákazníků. Oracle se zaměřuje na škálovatelnost a bezpečnost – systém využívá řízení přístupů, šifrování, auditní logy a splňuje požadavky GDPR nebo HIPAA. Jeho podíl na CRM trhu je okolo 4 %.[12]

2.2.3 SAP CRM

SAP je jeden z nejznámějších CRM systémů, který je stále hodně rozšířený, avšak ne v cloudovém řešení. SAP tuto možnost nabízí v rámci svého řešení SAP Customer Experience. Zaměřuje se na komplexní řízení vztahů se zákazníky s návazností na ERP, e-commerce a marketingové nástroje. SAP je oblíbený ve výrobních a logistických firmách. Podporuje robustní datový model, workflow automatizaci a přísné bezpečnostní standardy, včetně ochrany osobních údajů dle evropské legislativy. Podíl SAP na CRM trhu se pohybuje kolem 3–4 %. [13]

2.2.4 Adobe Experience Cloud

Adobe Experience Cloud kombinuje CRM funkce s nástroji pro digitální marketing, zákaznickou analytiku a personalizaci. Je vhodný především pro firmy zaměřené na online kampaně, digitální média a tvorbu personalizovaného obsahu. Zahrnuje komponenty jako Adobe Campaign, Adobe Analytics a Adobe Target. V oblasti bezpečnosti využívá šifrování dat, řízení přístupů a integraci s Adobe Identity Management. Adobe se na CRM trhu drží s podílem přibližně 3 %. [14]

3 GDPR A PRÁVNÍ POŽADAVKY

Tato kapitola se věnuje problematice GDPR v systému Salesforce. Popisuje základní principy GDPR, jednotlivé role, výzvy a výhody. Další kapitola pojednává o práci s daty v rámci Salesforce.

3.1 Základní principy GDPR

Nařízení Evropského parlamentu a Rady (EU) 2016/679, známé jako GDPR (General Data Protection Regulation), vstoupilo v platnost 25. května 2018 a představuje komplexní právní rámec pro ochranu osobních údajů v celé Evropské unii. Cílem tohoto nařízení je chránit základní práva jednotlivců, zejména právo na soukromí, a zároveň vytvořit jednotné podmínky pro zpracování osobních údajů napříč členskými státy EU. [16]

GDPR se vztahuje na všechny organizace, které zpracovávají osobní údaje občanů EU, bez ohledu na to, kde se tyto organizace nacházejí. To znamená, že se týká i mezinárodních firem využívajících cloudová řešení, jako je Salesforce, pokud jimi spravovaná data obsahují informace o obyvatelích EU.

Mezi klíčové principy GDPR patří:[16]

Zákonnost, korektnost a transparentnost – osobní údaje musí být zpracovávány zákonným způsobem a subjekt údajů musí být informován o účelu zpracování.

Účelové omezení – údaje musí být shromažďovány pouze pro jasně stanovené a legitimní účely.

Minimalizace údajů – sběr údajů by měl být omezen pouze na ty, které jsou nezbytné.

Přesnost – zajištění aktuálnosti a správnosti údajů.

Omezení uložení – osobní údaje by měly být uchovávány pouze po dobu nezbytně nutnou.

Integrita a důvěrnost – zajištění zabezpečení údajů proti neoprávněnému nebo nezákonnému zpracování.

Dalším klíčovým prvkem GDPR je vymezení rolí:[16]

Správce – subjekt, který určuje účely a prostředky zpracování osobních údajů.

Zpracovatel – subjekt, který zpracovává údaje jménem správce.

GDPR rovněž zavádí nové povinnosti, jako je vedení záznamů o zpracovatelských činnostech, povinnost oznamovat porušení zabezpečení do 72 hodin nebo nutnost získat informovaný souhlas od subjektu údajů. V praxi to znamená, že každý systém, včetně Salesforce, musí být schopen poskytnout funkce pro správu souhlasů, audit záznamů a vyhovění právům subjektů údajů (např. právo na přístup, opravu nebo výmaz).[16]

Organizace využívající Salesforce musí brát v úvahu, že pokud jsou data uložena na serverech mimo EU, může být narušen jejich soulad s GDPR. Proto Salesforce nabízí možnost geografické lokalizace dat, šifrování a nástroje pro správu datových požadavků dle GDPR.[16]

3.2 Práce s daty v Salesforce

Salesforce zpracovává data prostřednictvím sofistikované struktury a funkcionalit, které zajišťují efektivitu, bezpečnost a splnění regulačních požadavků. Data jsou organizována do objektů, které představují datové tabulky podobné těm v relačních databázích. Data jsou uložena ve formě záznamů (řádky) a polí (sloupce) v těchto objektech. Platforma také umožňuje vytvářet vztahy mezi objekty, například hierarchii rodič-dítě nebo vztahy typu mnoho k mnoha.

Data do Salesforce přicházejí několika způsoby. Uživatelé mohou informace zadávat manuálně přímo do platformy, data mohou být přenesena prostřednictvím API nebo integrací s externími systémy a také mohou být získána z webových formulářů, například při shromažďování údajů o potenciálních zákaznících.

Ukládání dat probíhá na serverech Salesforce, které jsou umístěny v datových centrech. Salesforce umožňuje výběr regionu pro ukládání dat, například v EU, což je klíčové pro splnění požadavků GDPR na lokalizaci dat. Navíc jsou data ukládána redundantně, což zajišťuje jejich vysokou dostupnost a ochranu před ztrátou.

Zpracování dat v Salesforce probíhá jak manuálně, tak automaticky. Automatizace je podporována pomocí flow a vlastního programovacího jazyka Apex. Kromě toho využívá Salesforce umělou inteligenci Einstein AI, která analyzuje data a poskytuje užitečné předpovědi nebo doporučení. Platforma také umožňuje zpracování a synchronizaci dat v reálném čase, což je nezbytné pro plynulé obchodní procesy.

Přístup k datům je řízen prostřednictvím granulárních bezpečnostních opatření. Přístupové role a hierarchie umožňují kontrolu na základě organizační struktury, přičemž sdílení dat může být nastaveno na úrovni celé organizace, objektů, jednotlivých záznamů nebo polí. Pro zvýšení bezpečnosti jsou data šifrována jak při přenosu pomocí TLS, tak při uložení pomocí AES-256.

Salesforce také podporuje mazání dat v souladu s požadavky GDPR, například umožňuje využití práva být zapomenut. Neaktivní data mohou být archivována, pokud jejich smazání není požadováno. Integrace dat s jinými systémy je zajištěna prostřednictvím REST a SOAP API nebo middleware nástrojů, jako je například Mulesoft, který Salesforce vlastní.

Bezpečnost dat je jednou z hlavních priorit Salesforce. Data jsou šifrována jak při přenosu, tak v klidu, a přístup k nim je chráněn dvou faktorovou autentizací (MFA). Salesforce poskytuje také možnosti auditů a zaznamenávání přístupu k datům, což zajišťuje transparentnost a umožňuje rychlé reakce na potenciální bezpečnostní incidenty. Tímto komplexním přístupem Salesforce nejen zpracovává data, ale také poskytuje prostředí, které podporuje bezpečnost a soulad s legislativními normami. [18]

4 BEZPEČNOSTNÍ ARCHITEKTURA SALESFORCE

Bezpečnostní architektura Salesforce je navržena tak, aby zajistila vysokou úroveň ochrany dat a zároveň umožnila flexibilní přístup k informacím na základě rolí, oprávnění a kontextu. Salesforce jako cloudová platforma poskytuje kombinaci technických, organizačních a provozních opatření pro zabezpečení dat před neoprávněným přístupem, únikem nebo zneužitím. Architektura zahrnuje jak šifrovací technologie, tak autentizační mechanismy, monitoring a standardy souladu s legislativou.[19]

Salesforce přistupuje k bezpečnosti komplexně a staví na principech obrany ve více vrstvách. Využívá zabezpečení na úrovni sítě, aplikace, uživatelského rozhraní i samotné databáze. Součástí bezpečnostní architektury jsou i pokročilé nástroje jako Salesforce Shield, který přidává šifrování polí, auditní logy a detekci událostí v reálném čase.[21]

4.1 Šifrování dat

Šifrování dat je jedním z klíčových nástrojů, které Salesforce používá k ochraně důvěrnosti informací. Platforma šifruje data přímo v databázi i během přenosu. Pro šifrování v databázi se používá algoritmus AES-256, který je v současnosti považován za průmyslový standard. Šifrování při přenosu dat je zajištěno pomocí protokolu TLS (Transport Layer Security).[22]

Salesforce implementuje šifrování na více úrovních:

- šifrování celé databáze (platform encryption),
- šifrování specifických polí (field-level encryption),
- šifrování záloh a exportů,
- šifrování souborů a příloh.

Zákazníci mohou využít také Customer Managed Keys (CMK), které zvyšují úroveň kontroly nad daty tím, že si sami mohou kontrolovat klíče, kterými jsou data šifrována. Pro náročné organizace je k dispozici rozšíření v podobě Salesforce Shield, který umožňuje detailní nastavení šifrování, auditování a správu bezpečnostních pravidel.[19]

4.2 Architektura a segregace dat

Z dokumentu Salesforce PSA Security, Privacy and Architecture [17] vyplývá, že Salesforce implementuje vícevrstvý model bezpečnosti, jehož základními pilíři jsou logická separace dat, řízení přístupu na základě rolí (RBAC) a šifrování na úrovni úložiště.

Logická separace dat zajišťuje, že data jednoho zákazníka nemohou být přístupná jinému zákazníkovi. I když mohou být data více klientů technicky uchovávána v rámci jedné databázové infrastruktury, jejich přístup je důsledně oddělen na aplikační úrovni. Salesforce tímto způsobem poskytuje „víceclientské“ prostředí, aniž by došlo ke kompromitaci důvěrnosti dat.

Další vrstvou zabezpečení je řízení přístupu na základě rolí (Role-Based Access Control – RBAC). Každý zaměstnanec Salesforce, který má přístup k zákaznickým datům v rámci poskytování profesionálních služeb, má přiřazenu přesně definovanou roli a odpovídající oprávnění. Přístup je povolován pouze na základě principu minimálních oprávnění (Least Privilege), a to pouze po dobu nezbytně nutnou k provedení konkrétní činnosti.

Tato architektura dokládá důsledný přístup Salesforce k ochraně dat klientů i v rámci služeb, které neprobíhají přímo na instanci zákazníka. Oddělení datových toků, přístupových práv a šifrování poskytuje silnou záruku, že i při interakci se zaměstnanci Salesforce Professional Services zůstávají data chráněna proti úniku či neoprávněnému přístupu.

4.3 Bezpečnostní standardy Salesforce

V prostředí rostoucích kybernetických hrozeb je implementace robustních standardů datové bezpečnosti nezbytná pro ochranu citlivých informací a zajištění souladu s regulačními požadavky. Salesforce integruje širokou škálu mezinárodně uznávaných bezpečnostních standardů a rámců, které společně tvoří komplexní bezpečnostní architekturu platformy.[19]

Datové bezpečnostní standardy slouží jako strukturovaný rámec pro ochranu důvěrnosti, integrity a dostupnosti dat. Tyto standardy poskytují organizacím jasné směrnice pro implementaci kontrolních mechanismů, které minimalizují riziko neoprávněného přístupu, ztráty nebo zneužití dat. Dodržování těchto standardů nejenže chrání data před externími hrozbami, ale také posiluje důvěru zákazníků a partnerů v schopnost organizace bezpečně spravovat citlivé informace.[20]

Salesforce podporuje a integruje několik klíčových bezpečnostních standardů, které jsou relevantní pro různé průmyslové sektory:[20]

- **ISO/IEC 27001:** Mezinárodní standard pro systémy řízení informační bezpečnosti (ISMS), který stanovuje požadavky na zavedení, implementaci, udržování a neustálé zlepšování ISMS.
- **NIST SP 800-53:** Soubor kontrolních opatření vydaný Národním institutem pro standardy a technologie (NIST) USA, zaměřený na zabezpečení federálních informačních systémů a organizací.
- **PCI DSS (Payment Card Industry Data Security Standard):** Standard pro zabezpečení dat držitelů platebních karet, který je povinný pro všechny organizace zpracovávající, uchovávající nebo přenášející údaje o platebních kartách.
- **HIPAA (Health Insurance Portability and Accountability Act):** Americký zákon stanovující standardy pro ochranu citlivých zdravotních informací, relevantní pro zdravotnické organizace a jejich partnery.
- **GDPR (General Data Protection Regulation):** Nařízení Evropské unie, které stanovuje pravidla pro ochranu osobních údajů jednotlivců v rámci EU a EHP.
- **CCPA (California Consumer Privacy Act):** Kalifornský zákon poskytující obyvatelům Kalifornie práva týkající se sběru, používání a sdílení jejich osobních údajů.
- **GLBA (Gramm-Leach-Bliley Act):** Americký zákon vyžadující, aby finanční instituce chránily důvěrnost a bezpečnost osobních finančních informací svých zákazníků.

Tyto certifikace jsou pravidelně auditovány nezávislými organizacemi. Kromě toho Salesforce publikuje zprávy o dostupnosti a výpadech svých služeb a umožňuje zákazníkům přístup k dokumentaci. Zavedení a udržování těchto standardů zajišťuje, že platforma je vhodná i pro organizace s vysokými nároky na bezpečnost – od finančních institucí přes zdravotnické organizace až po vládní sektor.[19][22]

4.4 Salesforce Shield

Salesforce Shield představuje nadstavbu bezpečnostního rámce platformy Salesforce a je určen pro organizace, které vyžadují pokročilé bezpečnostní funkce, rozšířené audity a detailní kontrolu nad zpracováním dat. Tento bezpečnostní balík se skládá ze čtyř klíčových komponent:[23]

- Platform Encryption
- Real Time Event Monitoring
- Field Audit Trail
- Data Detect

Kritérium	Klasické šifrování Salesforce	Salesforce Shield (Platform Encryption)
Algoritmus šifrování	128-bit AES	256-bit AES
Možnost šifrovat vlastní pole	Ne	Ano
Možnost šifrovat standardní pole	Ne	Ano
Využití vlastního šifrovacího klíče	Ne	Ano
Správa klíčů a rotace	Ne	Ano
Audit přístupu k zašifrovaným datům	Ne	Ano
Cena a dostupnost	Součástí základní licence	Licence Salesforce Shield

Tabulka 1: Porovnání klasického šifrování a Salesforce Shield [23]

4.4.1 Platform Encryption

Platform Encryption umožňuje organizacím šifrovat citlivá data uložená v Salesforce pomocí algoritmu AES-256. Na rozdíl od klasického šifrování přidává tato funkce možnost šifrovat konkrétní pole v objektech bez ztráty funkčnosti aplikace – tedy i nadále fungují reporty, workflow pravidla či vyhledávání. Tato vlastnost je zásadní v prostředí, kde je nutné chránit osobní nebo finanční údaje při zachování provozních funkcí systému.[21]

Platforma podporuje i tzv. Customer Managed Keys (CMK), které umožňují spravovat vlastní šifrovací klíče v rámci služby Key Management System (KMS). Tyto klíče lze uložit do služby Salesforce nebo je propojit s externím klíčovým úložištěm. Podporován je rovněž koncept Bring Your Own Key (BYOK), což umožňuje ještě vyšší úroveň kontroly nad šifrováním a usnadňuje integraci s interní bezpečnostní politikou firmy.[23]

Platform Encryption také splňuje požadavky mnoha mezinárodních bezpečnostních standardů jako GDPR, HIPAA nebo PCI-DSS, a je tak vhodná pro regulovaná odvětví jako zdravotnictví, finance nebo státní správu.

4.4.2 Real Time Event Monitoring

Event Monitoring poskytuje administrátorům a bezpečnostním týmům detailní logování více než 50 typů událostí v Salesforce. Mezi nejdůležitější patří:[21]

- přihlášení a odhlášení uživatelů,
- exporty dat,
- zobrazování záznamů,
- volání REST a SOAP API,
- změny nastavení a konfigurace systému.

Každá událost je zaznamenána jako Event Log File, které je možné stáhnout a analyzovat pomocí nástrojů třetích stran (např. Splunk, Snowflake) nebo prostřednictvím Salesforce Event Monitoring Analytics App. Logy umožňují detekovat anomálie v chování uživatelů, například neobvyklé objemy exportů, přístupy mimo pracovní dobu nebo přihlášení z neznámé IP adresy.[21]

Event Monitoring podporuje rovněž klasifikaci událostí podle úrovně závažnosti (Critical, Warning, Info) a umožňuje nastavení alertů pro konkrétní typy incidentů. Tím se výrazně zvyšuje schopnost organizace reagovat na bezpečnostní hrozby v reálném čase.

4.4.3 Field Audit Trail

Field Audit Trail je rozšířením klasického auditního logování změn polí (field history tracking). Umožňuje sledovat historii změn až u 60 polí na objekt a uchovávat tuto historii po dobu až 10 let. Standardní Salesforce umožňuje uchovávat historii změn pouze u 20 polí a po dobu 18 měsíců, což je pro mnoho organizací nedostačující z pohledu bezpečnostních politik.[21]

Funkce je navržena tak, aby odpovídala požadavkům regulací jako Sarbanes-Oxley (SOX), GDPR, HIPAA nebo zákonů o kybernetické bezpečnosti. V praxi umožňuje sledovat, kdo změnil konkrétní pole, kdy, odkud a jaká byla původní a nová hodnota. Tyto informace jsou klíčové například při vyšetřování incidentů, auditech nebo řešení sporů.[23]

Auditní záznamy lze archivovat, exportovat a analyzovat, přičemž jsou uloženy nezávisle na aktuální databázové vrstvě – čímž se zajišťuje jejich integrita a odolnost proti manipulaci.

4.4.4 Data Detect

Data Detect je nejnovější součástí Salesforce Shield a využívá umělou inteligenci k automatické detekci citlivých údajů v rámci celé platformy. Pomocí předdefinovaných i vlastních detekčních vzorů je možné identifikovat data, jako jsou:[23]

- čísla kreditních karet,
- e-mailové adresy,
- telefonní čísla,
- rodná čísla,
- osobní identifikátory (PII).

Data Detect zjednodušuje klasifikaci dat a pomáhá organizacím při plnění požadavků na ochranu osobních údajů (GDPR, CCPA apod.). Výstupem detekce je přehledná mapa citlivých dat (Data Sensitivity Map), která slouží jako základ pro další kroky – například šifrování, omezení přístupu nebo anonymizaci. AI engine je neustále aktualizován a

rozšiřován o nové vzory a klasifikační metody, čímž se zajišťuje jeho schopnost odhalovat i nové typy citlivých údajů nebo zranitelností.[23]

4.5 Bezpečnost jazyka Apex

Vývoj aplikací v prostředí Salesforce prostřednictvím programovacího jazyka Apex přináší výkonné možnosti rozšíření platformy, ale zároveň s sebou nese odpovědnost za dodržování bezpečnostních principů. Aplikace běžící na Salesforce mají často přístup k citlivým datům, což klade důraz na bezpečnostní audit a správné programovací postupy.

Salesforce vývojáři jsou vedeni k dodržování bezpečnostních doporučení publikovaných ve Security Implementation Guide. [24] Tento dokument se zabývá mimo jiné i typickými zranitelnostmi, které mohou vést ke kompromitaci dat nebo zneužití funkcionality aplikace. Mezi ty nejzásadnější patří Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF) a SOQL Injection.

XSS je zranitelnost, která vzniká tehdy, pokud vývojář nesprávně ošetří vstupy uživatele a následně je vypisuje do stránky bez odpovídajícího filtrování nebo escapingu. Útočník může do takového vstupu vložit škodlivý JavaScript kód, který se při zobrazení stránky spustí. V Salesforce může k této zranitelnosti dojít například v komponentách Visualforce nebo Lightning Web Components, pokud nejsou správně ošetřeny výstupy.

CSRF útok spočívá v tom, že útočník podstrčí uživateli požadavek, který je odeslán v kontextu platné relace, například POST request do interního endpointu aplikace. Salesforce tento typ útoku ošetřuje na úrovni platformy, ale vývojář musí přesto dbát na správné zacházení s uživatelskými akcemi a komponentami.[24]

SOQL Injection je typ útoku, kdy útočník zneužije nedostatečně kontrolovaný vstup ve spojení s konstrukcí SOQL dotazu do databáze. Pokud je například část dotazu sestavena přímo z parametru z formuláře, může být manipulována tak, aby vrátila citlivá data nebo změnila logiku dotazu.[24]

Apex třídy v Salesforce mohou být spouštěny s různými úrovněmi přístupových oprávnění. Pokud není explicitně určeno jinak, Apex třída běží v tzv. system contextu, což znamená, že ignoruje oprávnění a sdílená pravidla (sharing rules) aktuálního uživatele. To může vést ke scénářům, kdy se uživateli zobrazí data, ke kterým by za běžných okolností neměl mít přístup.

Aby vývojář zajistil, že třída bude respektovat nastavení sdílení záznamů, je potřeba použít klauzuli `with sharing` v definici třídy. Naopak použití `without sharing` může být v některých specifických případech žádoucí (např. v integračních scénářích), ale jeho použití by mělo být pečlivě odůvodněno a zdokumentováno.

Dalším důležitým prvkem je metoda `Security.stripInaccessible()`, která umožňuje vývojářům odstranit záznamy nebo pole, ke kterým nemá daný uživatel přístup. Tato metoda je užitečná především při zápisu dat, kdy by mohlo dojít k chybě nebo dokonce neúmyslnému odhalení struktury objektů.

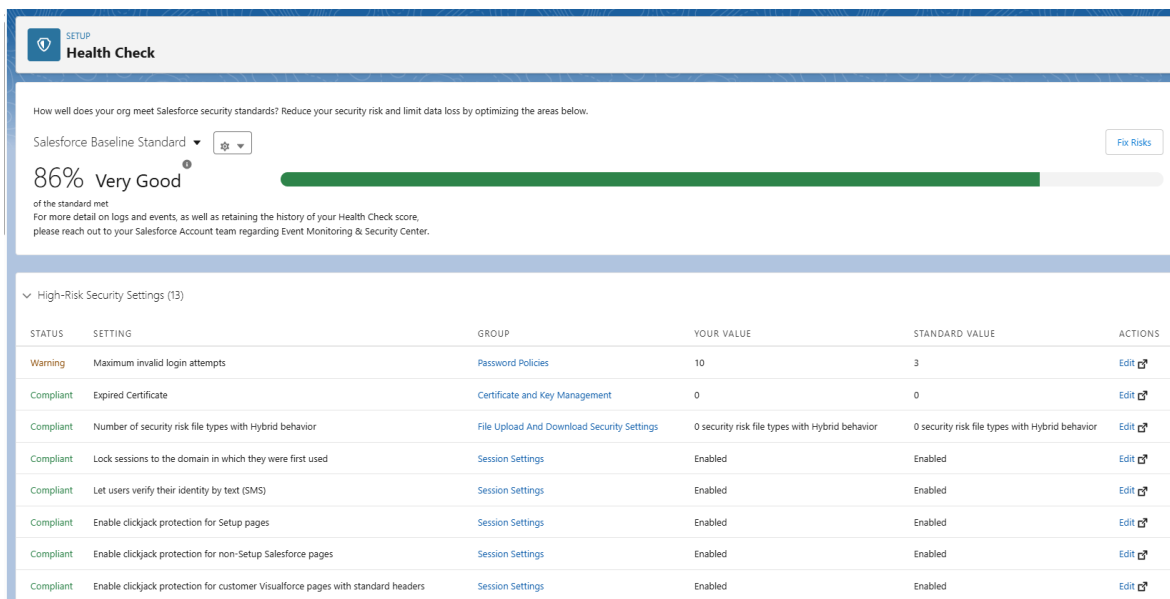
Tímto způsobem lze výrazně omezit riziko spojené s neoprávněným přístupem k polím nebo objektům. Součástí vývoje by mělo být také testování bezpečnostních scénářů a provedení code review zaměřeného na rizikové konstrukce. V případě vývoje aplikace určené k distribuci v AppExchange je navíc požadováno, aby kód prošel bezpečnostní certifikací od Salesforce, kde jsou všechny zmíněné oblasti kontrolovány.

4.6 Security Health Check

Další důležitou součástí bezpečnostního rámce Salesforce je nástroj Security Health Check, který umožňuje administrátorům rychle zhodnotit aktuální bezpečnostní nastavení organizace. Tento nástroj porovnává konfiguraci instanci s doporučenými bezpečnostními hodnotami a přehledně vizualizuje případné odchylky, které mohou představovat riziko.

Kontrola zabezpečení hodnotí například sílu a expiraci hesel, timeouty relací, úroveň ochrany před phishingem nebo možnosti spouštění skriptů. Výsledky jsou prezentovány formou celkového bezpečnostního skóre, přičemž každé nastavení je zařazeno do jedné ze čtyř kategorií: High Risk, Medium Risk, Low Risk a Compliant.

Výhodou Health Checku je i možnost vlastního nastavení bezpečnostní základny, podle specifických požadavků organizace. Uživatelé s přístupem k Salesforce Shield mají navíc k dispozici rozšířené možnosti monitoringu a výkaznictví. Tento nástroj tak představuje rychlý a efektivní způsob, jak pravidelně prověřovat konfiguraci systému a udržovat jeho bezpečnostní úroveň na požadované úrovni.



Obrázek 6: Ukázka Security Health Check v Salesforce

5 SPRÁVA OPRÁVNĚNÍ A PŘÍSTUPU

Jedním ze základních stavebních kamenů bezpečnosti v Salesforce je správa přístupu. Systém nabízí velmi detailní možnosti konfigurace toho, kdo má přístup, ke kterým datům a funkcím, a v jakém rozsahu. Správa oprávnění v Salesforce se řídí principem minimálních oprávnění (principle of least privilege), tedy každý uživatel by měl mít přístup pouze k těm datům a funkcím, které nutně potřebuje ke své práci. **Chyba! Nenalezen zdroj odkazů.**

Salesforce rozděluje správu přístupu do několika úrovní, které se vzájemně doplňují:

- **Ověřování uživatelů (authentication)** – ověření identity uživatele při přihlašování.
- **Autorizace (authorization)** – určení, k jakým funkcím, objektům nebo záznamům má ověřený uživatel přístup.
- **Zabezpečení na úrovni objektů, polí a záznamů** – tzv. OWD (organization-wide defaults), role, sdílení (sharing rules), profily, permission sety.
- **Session management a IP restrikce** – omezení přístupů podle lokace, času nebo zařízení.

Tato víceúrovňová struktura umožňuje velmi granulární řízení přístupu, což je klíčové zejména v prostředí větších firem nebo organizací, které pracují s citlivými údaji.

5.1 Ověřování uživatelů

Ověřování identity uživatele je prvním krokem v přístupovém procesu. Salesforce umožňuje několik metod ověření, které lze mezi sebou kombinovat podle bezpečnostní politiky organizace.[25][26]

- **Jméno a heslo** – základní metoda, kterou lze rozšířit o komplexní požadavky na délku, expiraci a historii hesel.
- **Dvou faktorové ověření (2FA)** – posílení bezpečnosti pomocí druhého faktoru (např. SMS, TOTP aplikace, biometrie). Povinné pro administrátory a silně doporučené pro všechny uživatele.
- **Single Sign-On (SSO)** – umožňuje uživatelům přihlásit se pomocí jejich firemní identity (např. Active Directory nebo Google Workspace). Implementuje se pomocí SAML nebo OpenID Connect protokolů.

- **OAuth 2.0** – používaný pro připojení externích aplikací k Salesforce API. Umožňuje přístup bez nutnosti zadávat heslo.

Bezpečnostní politika může být dále nastavena prostřednictvím IP rozsahů a časových oken pro přihlášení, což výrazně omezuje riziko neoprávněného přístupu z neznámých lokalit.

5.2 Správa oprávnění

Správa oprávnění určuje, co uživatel v systému může nebo nemůže dělat. V Salesforce existují dva hlavní nástroje pro správu oprávnění – profily (Profiles) a permission sety (Permission Sets) (Tabulka 1). Ty mimo jiné nastavují systémový přístup k objektům a polím. Dalším nastavením v Salesforce jsou role (Roles), které se zaměřují na viditelnost záznamů (spolu s dalšími mechanismy sdílení jako sharing rules a manual sharing).[26]

5.2.1 Profile

Profil je základní prvek, který definuje oprávnění uživatele. Každému uživateli je přiřazen právě jeden profil ihned při jeho vytvoření. Profily určují, ke kterým objektům má uživatel přístup, co s nimi může dělat (CRUD), jaké layouty a aplikace vidí, jaké flow nebo Apex třídy může spustit, a také např. IP omezení nebo časová okna pro přihlášení.[26]

Mezi klíčové komponenty profilu patří:

- Object settings – Create, Read, Update, Delete
- Field-level security – viditelnost a možnost editace polí
- Tab settings – viditelnost záložek v UI
- Record types a page layouts
- Login hours a login IP ranges

Profily jsou rigidní a nejsou ideální pro škálovatelnou správu. Proto Salesforce doporučuje omezit jejich množství a využívat je spíše pro základní nastavení. Využívají se primárně pro skupinu uživatelů, kteří mají stejné, nebo velice podobné oprávnění.

5.2.2 Permission Set

Permission sety jsou flexibilním nástrojem pro rozšíření oprávnění bez nutnosti vytvářet nové profily. Uživatel jich může mít přiřazeno více. Typickým použitím je např. přiřazení přístupu ke specifickému objektu, aplikaci nebo poli pro omezený počet uživatelů.[26]

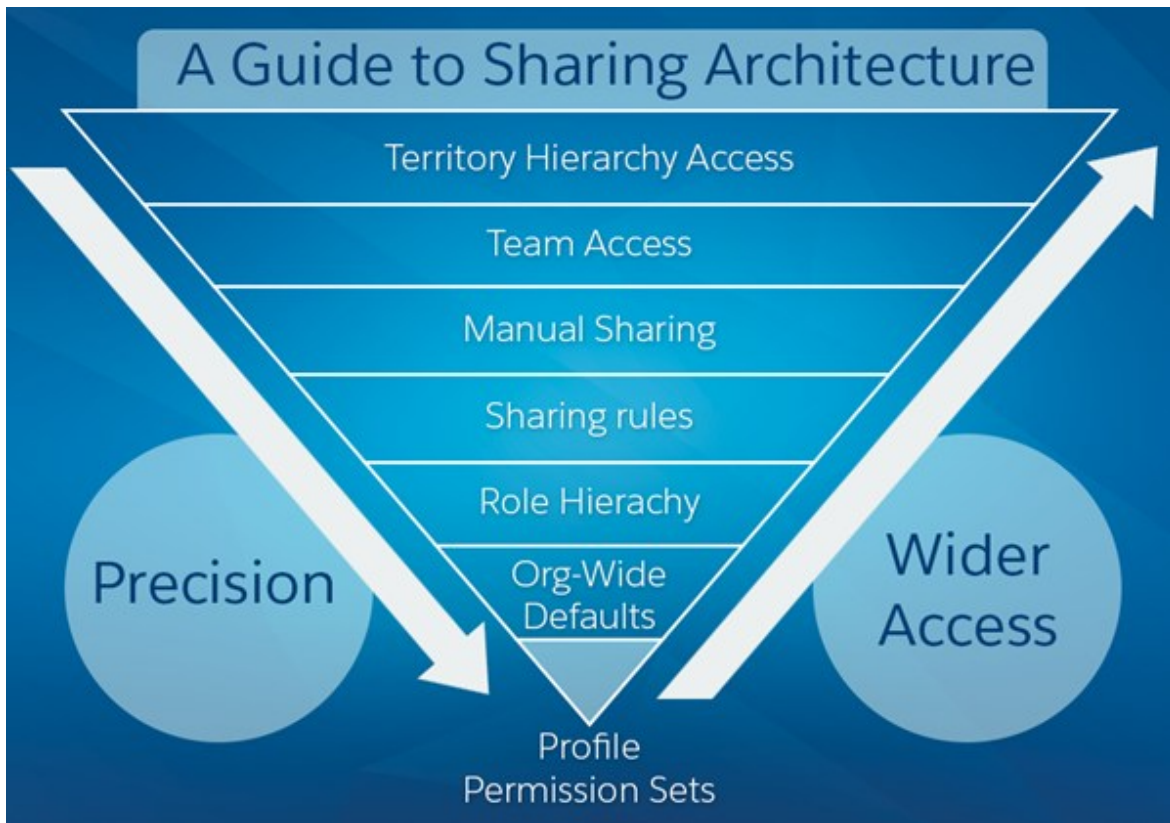
Existují i Permission Set Groups, které umožňují seskupit více permission setů do jednoho balíčku. To zjednodušuje administraci, zejména ve větších organizacích. Každý permission set může obsahovat objektová oprávnění, systémové oprávnění (např. možnost importovat data), nebo specifická oprávnění jako přístup k Apexu třídám.[26]

5.2.3 Role

Role neslouží k udělování funkcionality, ale k určení, k jakým datům má uživatel přístup. Salesforce využívá hierarchii rolí, kdy nadřazený má automaticky přístup k záznamům svých podřízených.[26]

Obchodní manažer vidí všechny záznamy obchodníků ve svém týmu. Role lze kombinovat se sdílením dat na úrovni organizace (OWD) a pomocí pravidel sdílení (sharing rules), čímž se dosahuje velmi granulární správy přístupu k datům.[26]

V praxi se používá kombinace profilů, permission setů, custom permissions v kombinaci se správným nastavením OWD a rolí. Tato kombinace nástrojů umožňuje vytvořit bezpečný, ale zároveň flexibilní systém přístupů, který se přizpůsobí potřebám i velmi komplexních organizací. Salesforce umožňuje i oprávnění na profilu, nebo permission setu, tzv. „view all“ a „modify all“, které zpřístupní uživateli veškeré záznamy daného objektu. Tento přístup se využívá často pro administrátory.[25]



Obrázek 7: Přehled přístupu k záznamům [25]

Permission Set	Profile
User, object, and field permissions	Default record types
Custom permissions	Default assigned apps
Connected app access	Page layout assignments
Apex class access	Login hours
Visualforce page access	Login IP ranges
Tab settings	

Tabulka 2: Porovnání nastavení přístupu v Permission Setu a Profílu [32]

II PRAKTICKÁ ČÁST

6 PŘÍPRAVA SALESFORCE PROSTŘEDÍ

Salesforce nabízí možnost vytvořit si bezplatnou verzi platformy, tzv. Salesforce Developer Edition (dostupné na <https://developer.salesforce.com/signup>). Tato edice je vhodná především pro vývojáře a administrátory pro experimentování v Salesforce. Většina standardních funkcí, je v této edici dostupná, stejně jako u placených edic, avšak má určitá omezení – např. menší počet uživatelů a kapacita pro data.

Sign up for your Developer Edition

A free Salesforce Platform environment with Agentforce and Data Cloud

First name

Stepan ✓

Last name

Bill ✓

Job title

Developer ✓

Work email

s_bill@utb.cz ✓

Company

UTB ✓

Country/Region

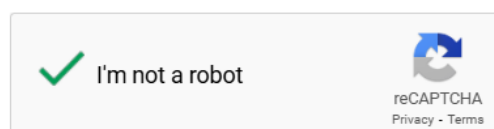
Czech Republic ✓ ▾

Your org may be provisioned on or migrated to Hyperforce, Salesforce's public cloud infrastructure.

☒ I agree to the [Main Services Agreement – Developer Services](#) and [Salesforce Program Agreement](#). I acknowledge, as described in the Developer Documentation: (1) the Developer Edition includes autonomous and other generative AI features; and (2) Salesforce may limit use of those features and the org, and may terminate any org that has been inactive for 45 days.

☐ Yes, I would like to receive marketing communications regarding Salesforce products, services, and events. I can unsubscribe at any time.

We value your privacy. To learn more, visit our [Privacy Statement](#).



Sign Me Up

Obrázek 8: Vytvoření Salesforce Developer Edition

7 ANALÝZA PŘÍSTUPOVÝCH OPRÁVNĚNÍ

7.1 Data mining Salesforce profilů

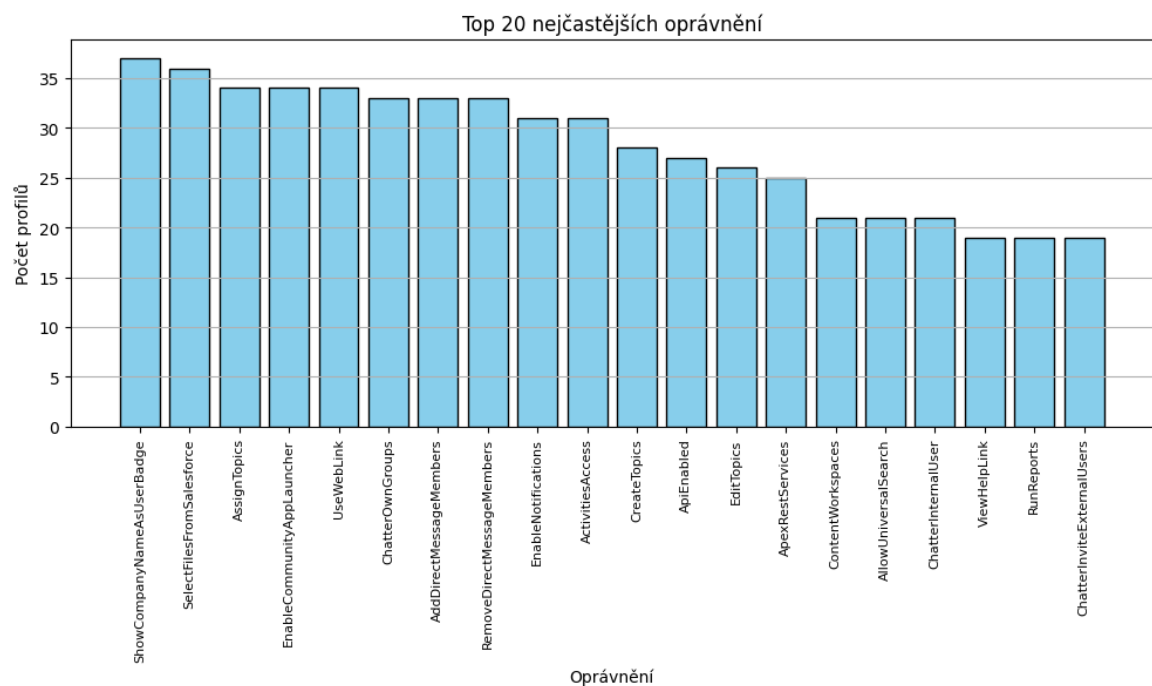
Tato kapitola se zabývá datovou analýzou oprávnění Salesforce profilů pomocí různých metod data miningu. Cílem bylo identifikovat vzorce v jednotlivých profilech a odhalit potenciální anomálie v nastavení přístupu. Vzhledem k tomu, aby řešení bylo univerzální a přenositelné, byly zvoleny metody učení bez učitele. Všechny analýzy byly provedeny v jazyce Python a jsou přílohou této práce.

7.1.1 Vstupní data

Jako vstupní data byly použity xml soubory profilů, staženy pomocí sfdx ze Salesforce prostředí. Tyto soubory obsahují nastavení přístupu pro jednotlivé profily. Data byly normalizovány do csv souboru s binárními hodnotami. Celkem bylo analyzováno 41 profilů s 215 atributy.

7.1.2 Frekvenční analýza

Pomocí frekvenční analýzy bylo zjištěno 20 nejčastějších oprávnění, které jsou nastaveny. Opačný výsledek (oprávnění, které se vyskytuje pouze v 1 profilu) nebyl nijak vypovídající, jelikož takových oprávnění bylo více než 100.



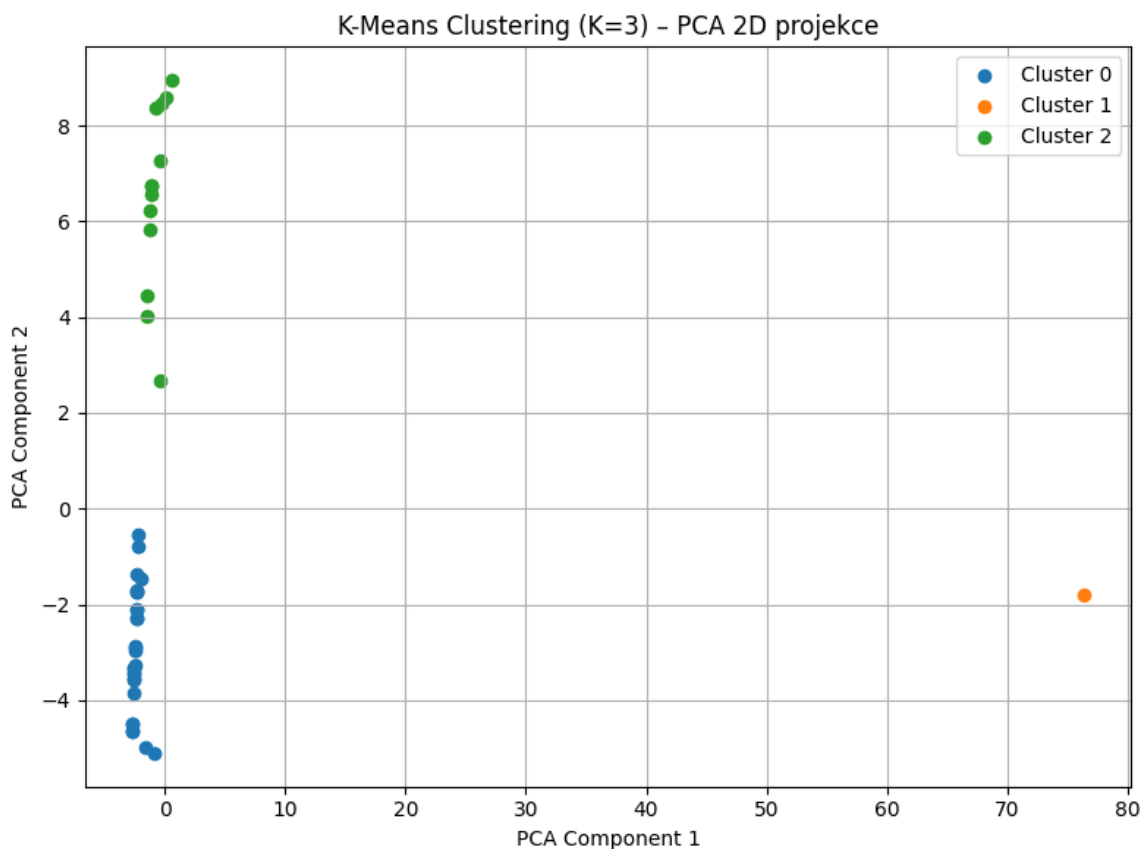
Obrázek 9: Frekvenční analýza oprávnění nastavených na profilech.

Zde je výpis 10 nejčastějších oprávnění vyskytujících se ve všech profilech. Ze názvů je patrné, že se jedná o běžné přístupy:

1. ShowCompanyNameAsUserBadge, 37
2. SelectFilesFromSalesforce, 36
3. AssignTopics, 34
4. EnableCommunityAppLauncher, 34
5. UseWebLink, 34
6. ChatterOwnGroups, 33
7. AddDirectMessageMembers, 33
8. RemoveDirectMessageMembers, 33
9. EnableNotifications, 31
10. ActivitiesAccess, 31

7.1.3 Clustering profilů pomocí K-Means

Clustering pomocí metody K-Means rozdělil profily podle podobnosti v oprávněních. Nejvíce vypovídající hodnotu má rozdělení na 3 clustery, tedy $K=3$, které bylo zvoleno pomocí metody „elbow rule“. Skript také vypisuje rozdělení profilů do clusterů podle názvu a podle očekávání je jediným profilem, který má samostatný cluster administrátorský profil.

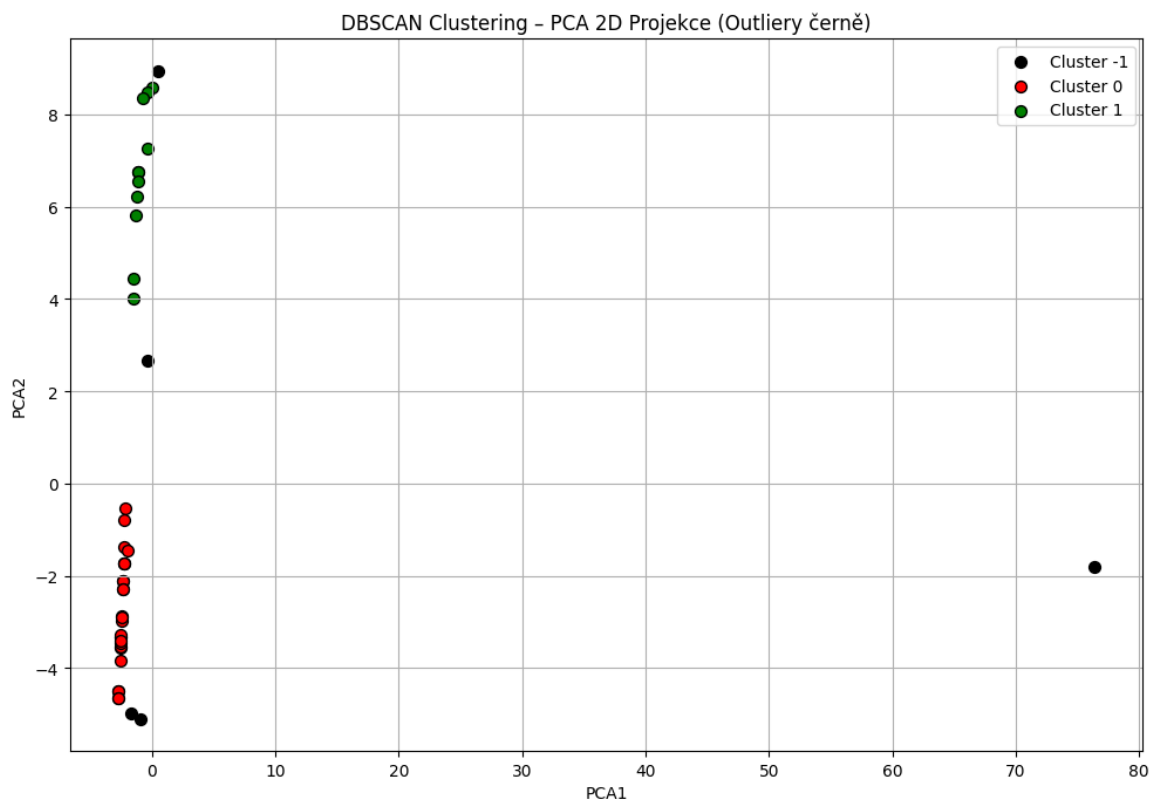


Obrázek 10: Grafické znázornění clusteringu pomocí K-Means

Clustering pomocí metody K-Means rozdělil profily na 3 skupiny. V první se nachází profily pro běžné uživatele s minimálním přístupem, uživatele community portálů, nebo integrační profil. Druhou skupiny tvoří profily s většími oprávněními, např. manažeři, analytici, marketingoví uživatelé. Samostatnou skupinu potom tvoří profil administrátorský, který má nejvíce oprávnění.

7.1.4 Detekce anomálií pomocí DBSCAN

Algoritmus DBSCAN byl použit pro analýzu, která umožňuje hledat přirozené shluky ale zároveň identifikovat hraniční profily, které by mohly znamenat anomálie v nastavení přístupu v jednotlivých profilech. Nejlepší výpovědní hodnotu algoritmus dosahoval s nastavním hodnot $\text{eps} = 10$ a $\text{min_pts} = 3$.



Obrázek 11: Grafické znázornění clusteringu pomocí DBSCAN

Vzhledem k tomu, že byla tato analýza provedena na profilech na čistém prostředí, bez zásahu do jejich nastavení, žádné anomálie se neprojevily. V reálném prostředí, lze takto identifikovat podezřelé, nebo hraniční profily. Tato analýza by šla případně rozšířit i na permission sety, které mají stejnou strukturu.

8 ZABEZPEČENÍ API A TOKENŮ

V prostředí Salesforce jsou API klíče nedílnou součástí autentizačního mechanismu při komunikaci mezi externími systémy a platformou. Nejčastěji jsou generovány prostřednictvím tzv. Connected Apps, které slouží jako prostředník pro OAuth 2.0 autentizaci a autorizaci. Každá Connected App definuje vlastní consumer key a consumer secret, které spolu s grant typem určují způsob získání access tokenu pro přístup k API.

Salesforce podporuje různé OAuth flow – od web server flow přes JWT Bearer token flow až po device-based authorization. Při nesprávné konfiguraci může Connected App představovat riziko, například pokud je access token dlouhodobě platný, není chráněn IP restrikcí nebo scope oprávnění umožňuje přístup k citlivým datům. Proto Salesforce umožňuje konfigurovat bezpečnostní zásady jako je povinné použití PKCE, časová platnost tokenů a schválené IP adresy. Správná správa Connected Apps je zásadní pro zajištění bezpečné integrace mezi Salesforce a externími systémy.

V této kapitole jsem se také zabýval, jak funguje autorizace v přístupu přes web, přes API a přes mobilní aplikaci. Zda jsou tokeny unikátní, nebo je lze použít v různých přístupech.

8.1 Autorizace přes Connected App

Jako první krok je potřeba vytvořit nového uživatele, který bude později využíván pro integrace (Obr. 11 a 12). Profil byl zvolen „Minimum Access – API Only Integrations“ – tento profil nemá přístup k žádným objektům, všechny přístup je řízen pomocí permission setů. Po vytvoření uživatele je nutné vytvořit heslo, přes odkaz v emailu.

SETUP
Users

New User

User Edit Save Save & New Cancel

General Information

First Name
Last Name
Alias
Email
Username
Nickname
Title
Company
Department
Division

Role
User License
Profile
Active ☒
Marketing User ☐
Offline User ☐
Knowledge User ☐
Flow User ☐
Service Cloud User ☐
Site.com Contributor User ☐
Site.com Publisher User ☐
WDC User ☐
Data.com User Type
Data.com Monthly Addition Limit
Accessibility Mode (Classic Only) ☐
High-Contrast Palette on Charts ☐
Lead Lightning Pages While Scrolling ☒
Debug Mode ☐
Quick Access Menu ☒
Salesforce CRM Content User ☒
Receive Salesforce CRM Content Email Alerts ☒
Receive Salesforce CRM Content Alerts as Daily Digest ☒

Obrázek 12: Vytvoření nového integračního uživatele v administraci Salesforce.

salesforce

Change Your Password

Enter a new password for s_bill@utb.cz.integration.
Make sure to include at least:

- 8 characters
- 1 letter
- 1 number

* New Password

* Confirm New Password

* Security Question

* Answer

*=required

Change Password

Obrázek 13: Nastavení hesla pro integračního uživatele.

Dalším krokem je vytvoření samotné Connected App v administraci Salesforce. Při vytváření se definuje množství parametrů, které určují nejen identitu a technické údaje aplikace, ale především její bezpečnostní chování a rozsah oprávnění pro přístup k datům uživatelů. Tato konfigurace je klíčová při nastavování integrací mezi Salesforce a externími systémy.

V první části konfigurace (Obr. 13) se zadávají základní informace o aplikaci, jako je:

- Název aplikace (Connected App Name) – slouží k identifikaci aplikace v rámci instance,
- API Name – technický identifikátor bez mezer, používaný v API volání,
- Contact Email – e-mail odpovědné osoby v případě potřeby bezpečnostní eskalace,
- Callback URL – adresa, na kterou se Salesforce vrací po dokončení autorizace

V další sekci (Obr. 14) se definuje OAuth scope, oprávnění, která aplikace požaduje. Mezi běžné hodnoty patří například:

- api – přístup ke standardnímu REST/SOAP API,
- refresh_token, offline_access – umožňuje obnovu access tokenu bez opakovaného přihlášení,
- openid – přístup k ID uživatele (používá se pro OpenID Connect),
- full, custom_permissions, web, chatter_api – další rozšíření pro konkrétní funkce.

V pokročilém nastavení lze dále definovat podporu jednotlivých OAuth autorizačních flows:

- Web Server Flow,
- User-Agent Flow,
- Device Flow,
- JWT Bearer Token Flow,

- Client Credentials Flow.

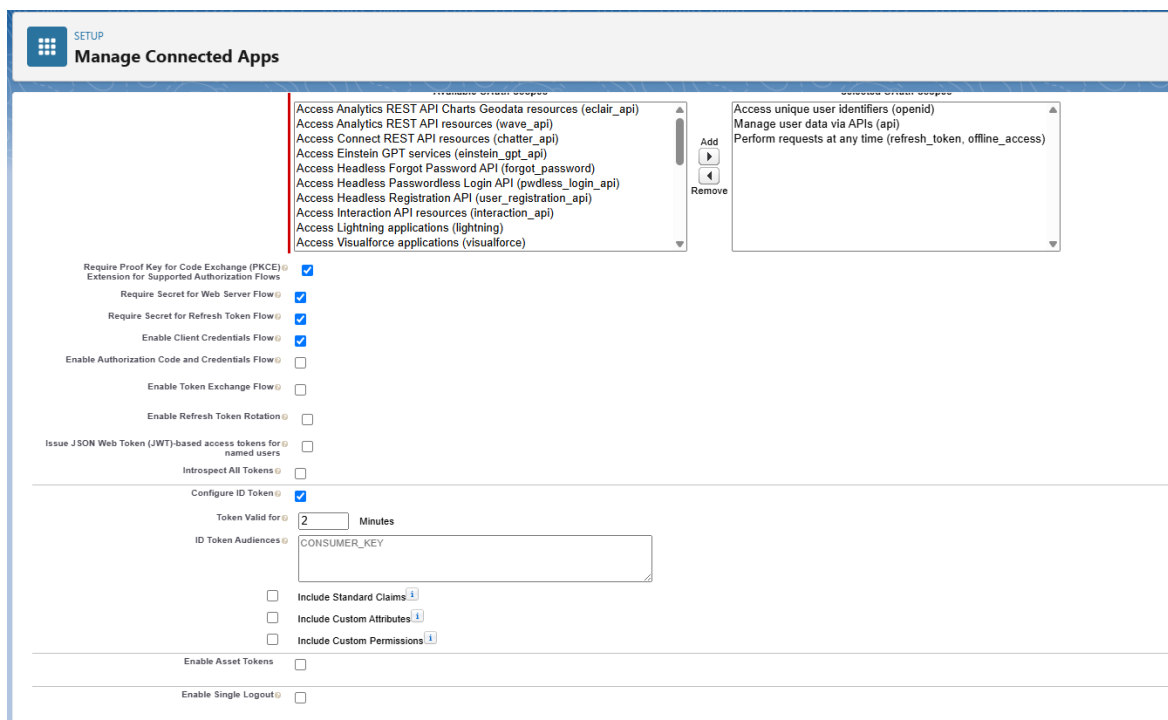
Další možnosti bezpečnostní konfigurace:

- PKCE (Proof Key for Code Exchange) – chrání authorization code flow před zachycením,
- Token Expiration – nastavuje dobu platnosti access nebo ID tokenu,
- Refresh Token Rotation – zvyšuje bezpečnost tím, že při každém použití refresh tokenu se vygeneruje nový,
- ID Token Audience – ověřuje, zda je token určen pro konkrétní klienta,
- Přidání vlastních atributů nebo custom claims do ID tokenu,
- Enable Single Logout – možnost odhlášení uživatele ze všech aplikací současně.

Konfigurace Connected App hraje zásadní roli v architektuře integrace Salesforce s externími systémy a její správné nastavení je nezbytné z pohledu řízení přístupů, ochrany identity a dodržování bezpečnostních politik organizace.

The screenshot displays the 'Manage Connected Apps' configuration interface in Salesforce. It is divided into two main sections: 'Basic Information' and 'API (Enable OAuth Settings)'. The 'Basic Information' section contains fields for 'Connected App Name', 'API Name', 'Contact Email', 'Contact Phone', 'Logo Image URL', 'Icon URL', 'Info URL', and 'Description'. The 'API' section includes checkboxes for 'Enable OAuth Settings' and 'Enable for Device Flow', a 'Callback URL' field, and a 'Use digital signatures' checkbox. Below these are two lists: 'Available OAuth Scopes' and 'Selected OAuth Scopes'. The 'Available OAuth Scopes' list includes various Salesforce APIs such as 'Access Analytics REST API Charts Geodata resources (eclair_api)', 'Access Analytics REST API resources (wave_api)', 'Access Connect REST API resources (chatter_api)', 'Access Einstein GPT services (einstein_gpt_api)', 'Access Headless Forgot Password API (forgot_password)', 'Access Headless Passwordless Login API (pwdless_login_api)', 'Access Headless Registration API (user_registration_api)', 'Access Interaction API resources (interaction_api)', 'Access Lightning applications (lightning)', and 'Access Visualforce applications (visualforce)'. The 'Selected OAuth Scopes' list includes 'Access unique user identifiers (openid)', 'Manage user data via APIs (api)', and 'Perform requests at any time (refresh_token, offline_access)'.

Obrázek 14: Nastavení Connected App v administraci Salesforce.

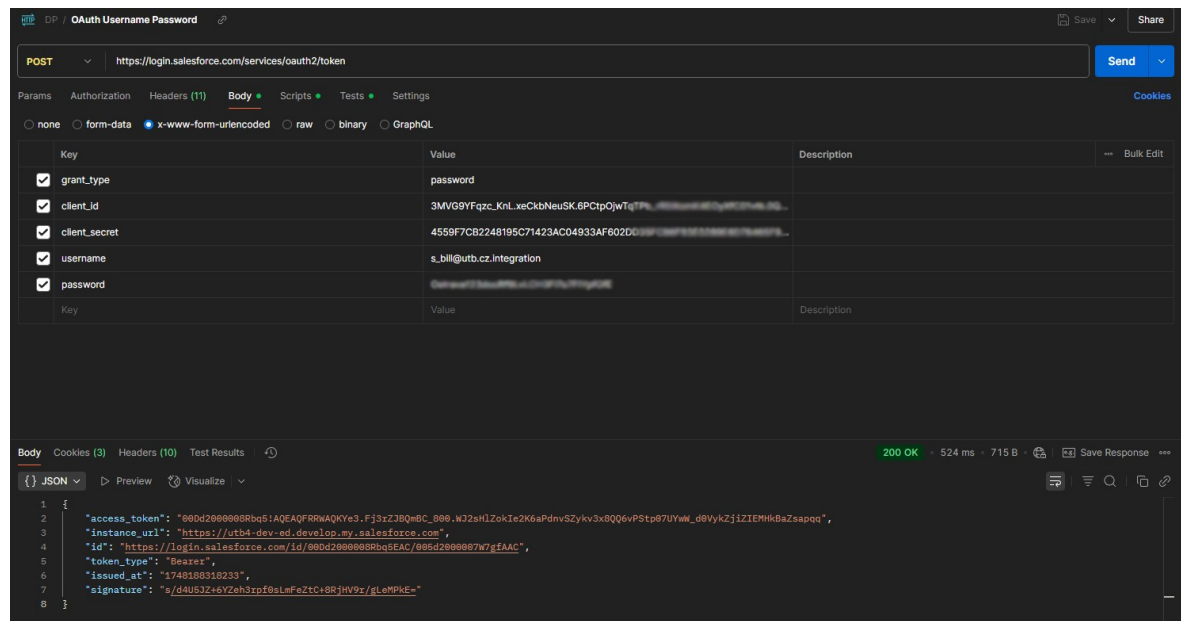


Obrázek 15: Pokročilé nastavení Connected App v administraci Salesforce.

8.1.1 OAuth Autorizace

V rámci testování zabezpečení API v Salesforce byly ověřeny dva různé způsoby autorizace přístupu prostřednictvím OAuth 2.0: Username-Password Flow a Client Credentials Flow. Oba přístupy mají specifické vlastnosti, výhody a omezení, které je nutné zohlednit při návrhu integrace. První zmíněný, s požadavkem typu `grant_type = password` využívá mimo parametry `client_id` a `client_secret` také uživatelské jméno a heslo (za heslem se ještě dává security token). Výhoda této metody je, že se může volat vždy na obecný endpoint <https://login.salesforce.com/services/oauth2/token>.

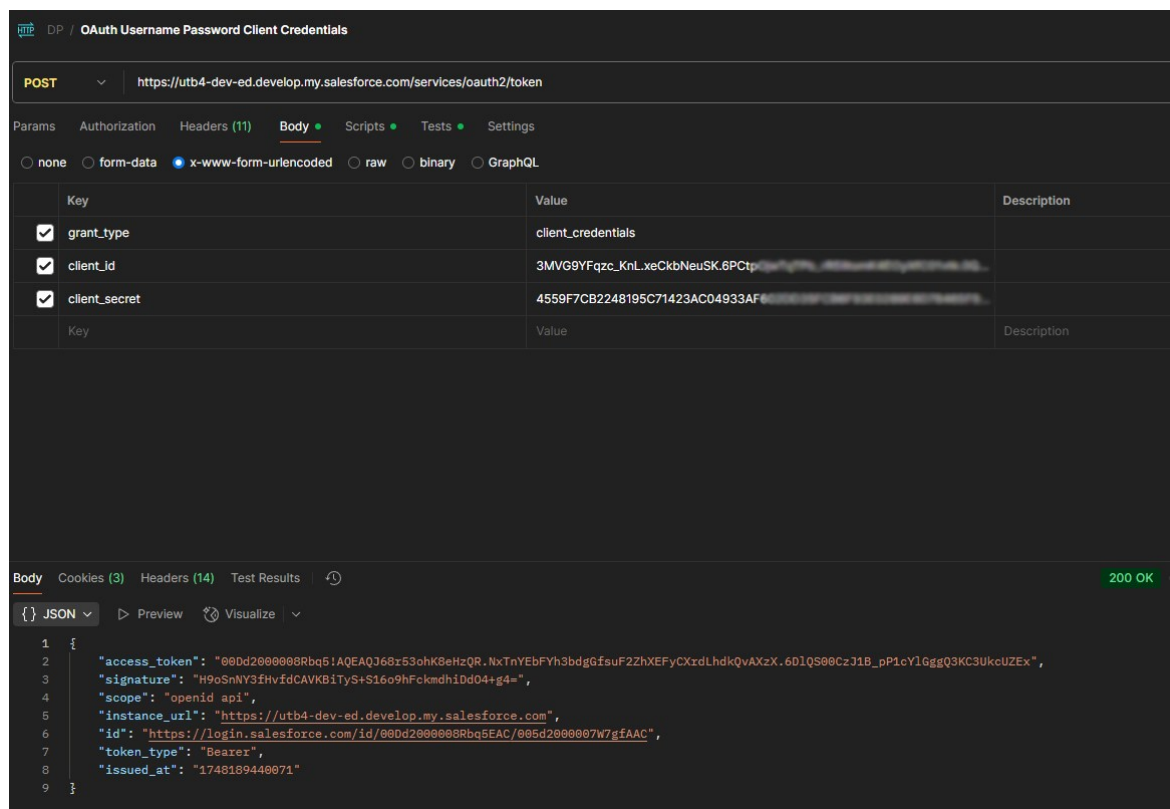
Výhodou je jednoduchost implementace a možnost simulovat běžného uživatele. Nevýhodou je nutnost uchovávat heslo v aplikaci, což zvyšuje bezpečnostní riziko – proto se nedoporučuje pro produkční použití.



Obrázek 16: OAuth autorizace Username-Password Flow

Client Credentials Flow přístup je určen spíše pro systémové integrace, kde není potřeba interaktivní přihlášení uživatele. Token se získává pomocí požadavku `grant_type=client_credentials`, bez nutnosti `username` a `password`. Salesforce však podporuje tento flow pouze na doméně konkrétní instance, nikoliv přes `login.salesforce.com`.

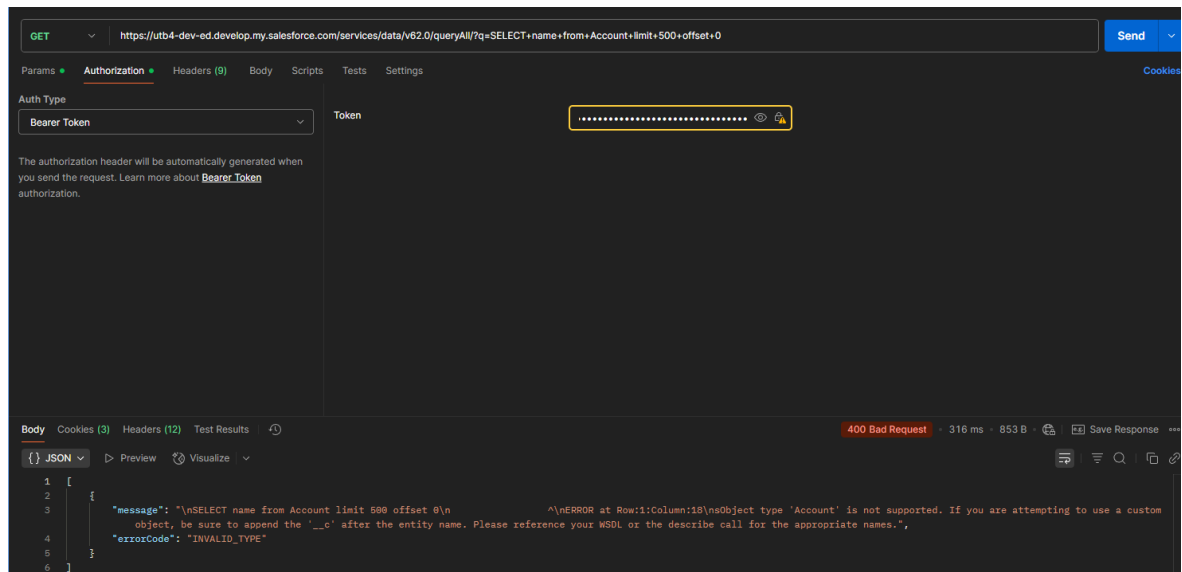
Aby bylo možné Client Credentials Flow použít, je nutné toto nastavení povolit v Connected App a zároveň určit tzv. Client Credentials User – uživatele, jehož oprávnění budou použita při přístupu k API.



Obrázek 17: OAuth autorizace Client Credentials Flow

8.1.2 Přístup k objektům přes API

Podle očekávání neměl integrační uživatel přístup k žádným objektům ani po autorizaci. Pro účely testování API přístupu byl uživateli přiřazen profil „Minimum Access – API Only“. Tento profil zajišťuje, že uživatel po autentizaci nemá přístup k žádným objektům nebo datům, dokud nejsou výslovně povolena pomocí permission setů. Při pokusu o přístup k objektům byla výsledkem chybová hláška (Obr. 17).



Obrázek 18: Testování přístupu k objektu Account bez přiřazeného PS

Po přiřazení konkrétního permission setu (Obr. 19) byly zpřístupněny vybrané objekty (Obr. 20), jako například Account a Contact. Tato architektura odpovídá principu minimálních oprávnění (principle of least privilege), který je klíčový pro zabezpečení přístupových cest.

SETUP
Permission Sets

Permission Set
Create

Save Cancel

Enter permission set information

Label Accounts Access

API Name Accounts_Access

Description

Session Activation Required ☐

Select the type of users who will use this permission set

Who will use this permission set?

- Choose '-None-' if you plan to assign this permission set to multiple users with different user and permission set licenses.
- Choose a specific user license if you want users with only one license type to use this permission set.
- Choose a specific permission set license if you want this permission set license auto-assigned with the permission set.

Not sure what a permission set license is? [Learn more here.](#)

License --None--

Save Cancel

Obrázek 19: Vytvoření Permission Setu pro přístup k objektu Account

SETUP
Permission Sets

Permission Set Assignments
User Integration

Save Cancel

Available Permission Sets

- Authenticated Payer
- Buyer
- Buyer Manager
- C360 High Scale Flow Integration User
- CRM User
- Commerce Admin
- Commerce Session
- Contact Center Admin
- Contact Center Admin (Partner Telephony)
- Contact Center Agent

Add

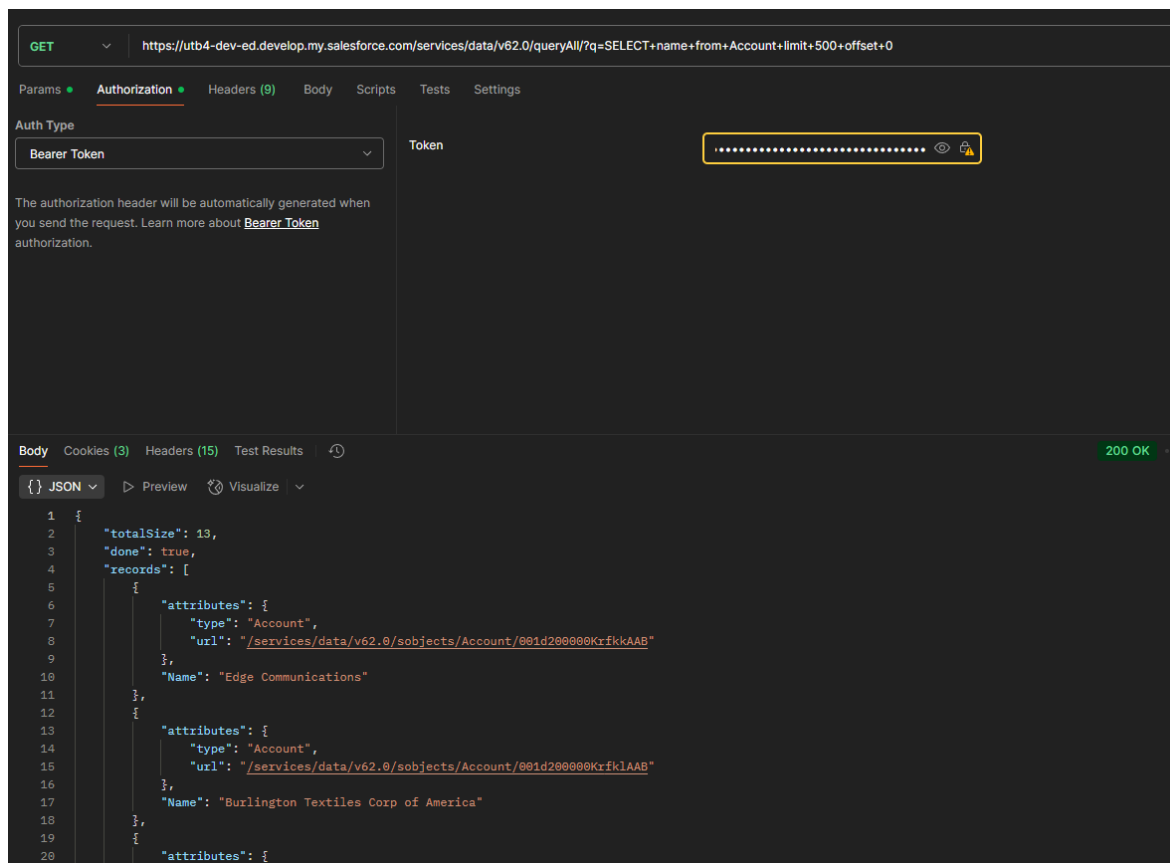
Remove

Enabled Permission Sets

- Accounts Access

Save Cancel

Obrázek 20: Přiřazení PS pro přístup k objektu Account integračnímu uživateli

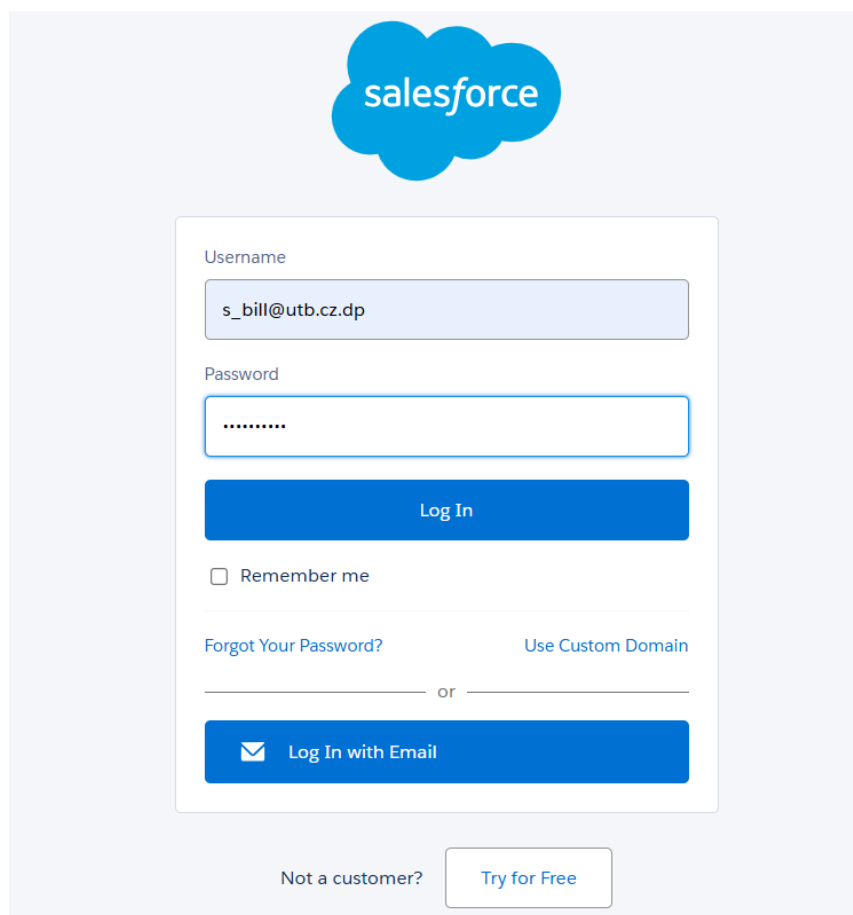


Obrázek 21: Úspěšný API call pro získání objektu Accounts po přiřazení PS

Pro úplné ověření efektivity nastavených oprávnění by bylo možné dále testovat přístupová práva na úrovni jednotlivých operací (Create, Read, Update, Delete – CRUD). To by umožnilo ověřit, zda jsou permission sety správně nakonfigurovány nejen na úrovni objektu, ale i konkrétních akcí, např. možnost číst záznamy, ale nikoliv je upravovat nebo mazat.

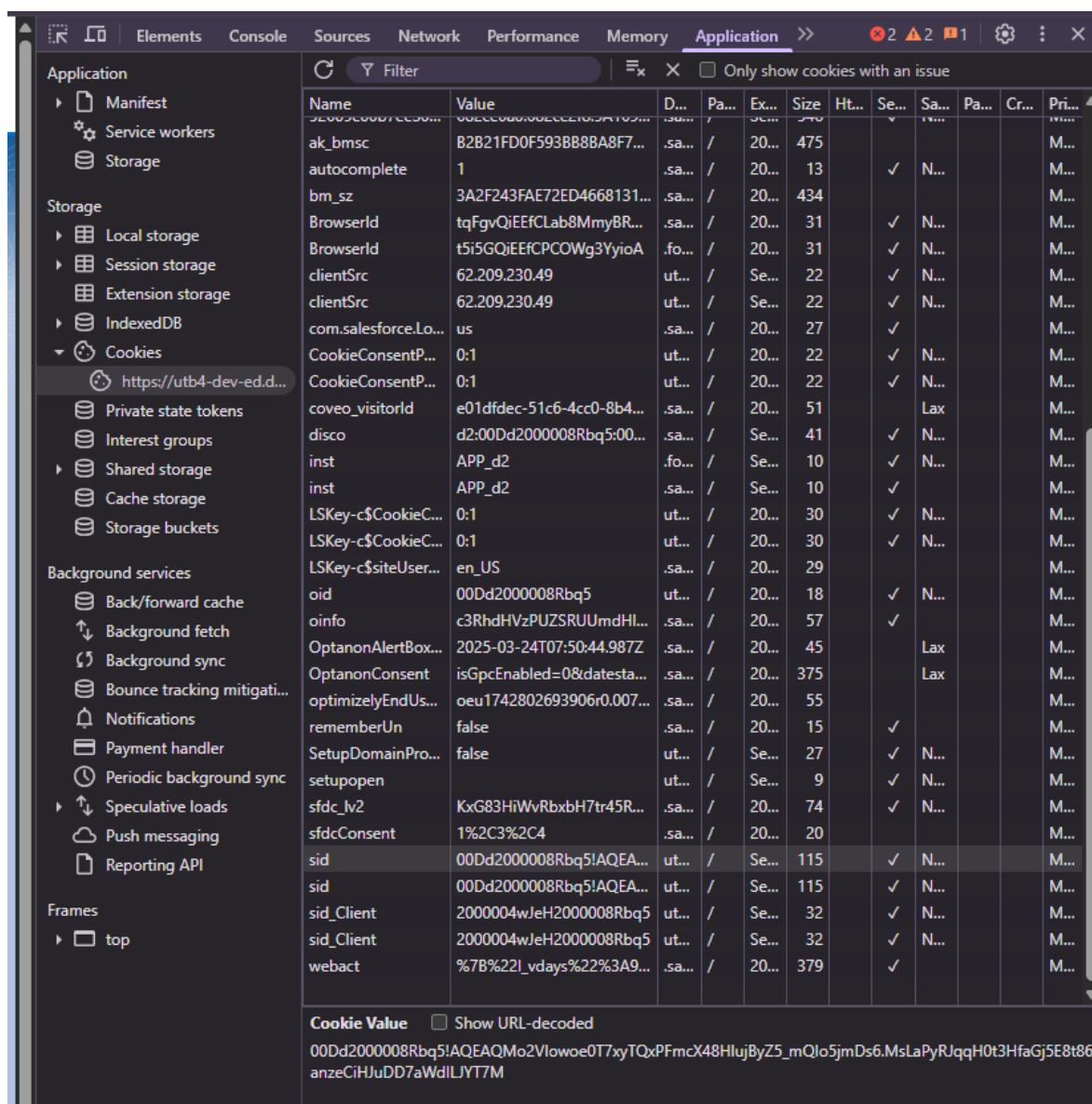
8.2 Autorizace přes web

Při přihlášení uživatele přes klasický login formulář na adrese `login.salesforce.com` (nebo custom doméně) Salesforce vytvoří uživatelskou relaci a uloží session ID (sid) do cookies prohlížeče. Tento sid token není běžně viditelný, ale lze jej snadno zobrazit pomocí nástrojů vývojáře v prohlížeči (např. Chrome > Inspect > Application > Cookies). Token sid slouží pro interní autorizaci uživatele v rámci webového uživatelského rozhraní (Lightning UI).



The image shows the Salesforce login interface. At the top is the Salesforce logo, a blue cloud with the word "salesforce" in white. Below the logo is a white login form with a light blue border. The form contains the following elements: a "Username" label above a text input field containing "s_bill@utb.cz.dp"; a "Password" label above a text input field with masked characters "*****"; a blue "Log In" button; a checkbox labeled "Remember me"; a link "Forgot Your Password?" on the left and a link "Use Custom Domain" on the right; a horizontal separator line with the word "or" in the center; a blue button with a white envelope icon and the text "Log In with Email"; and at the bottom, the text "Not a customer?" followed by a button labeled "Try for Free".

Obrázek 22: Přihlášení do Salesforce přes web na adrese www.login.salesforce.com

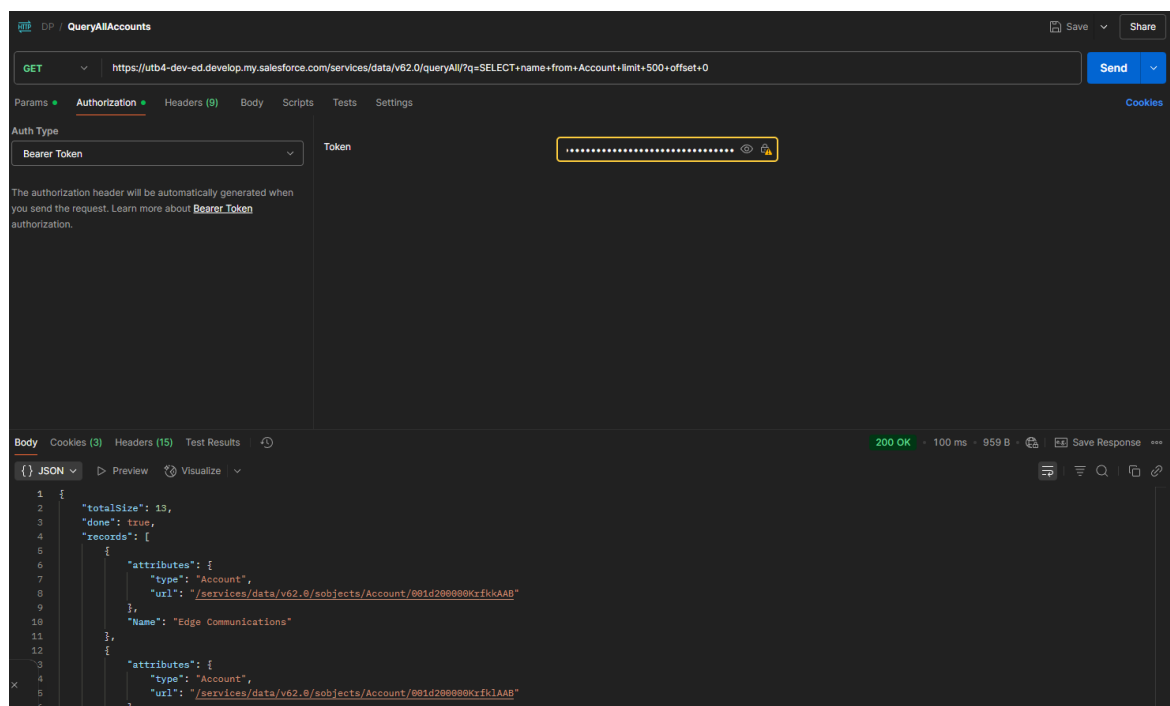


Obrázek 23: Access token uložený v cookies v sid po přihlášení do Salesforce

8.3 Možnosti zneužití access tokenu

Překvapivým zjištěním při testování bylo, že sid token získaný z cookies lze přímo použít jako Bearer token v HTTP Authorization headeru při volání Salesforce REST API. Tento přístup fungoval, a i když access token nebyl získán běžným OAuth flow, zobrazily se výsledky (Obr. 23). Znamená to, že pokud by útočník získal sid token (např. pomocí XSS nebo MITM útoku), mohl by provádět API volání pod identitou daného uživatele. Tato skutečnost podtrhuje důležitost ochrany session tokenů, správného nastavení IP restrikcí a využití dodatečných bezpečnostních opatření, jako je správné nastavení access tokenu nebo zákaz přístupu k API mimo povolené domény.

Další možností přístupu do Salesforce je přes mobilní aplikaci, která je dostupná pro Android i iOS a je oficiálně vydávána a podporována přímo Salesforce. Z pohledu bezpečnosti se jedná o bezpečnou komunikaci, jelikož přístupový token není viditelný, ani se k němu nelze jednoduše dostat.



Obrázek 24: Rest API volání s použitým access tokenem z prohlížeč (sid) s úspěšným výsledkem

8.4 Testování Login Hours a Login IP Ranges

Jedním z nástrojů pro zabezpečení přístupu v Salesforce je omezení přihlášení na základě IP adresy. Tato funkce umožňuje organizaci definovat rozsahy důvěryhodných IP adres, ze kterých se uživatelé mohou přihlásit. IP restrikce lze nakonfigurovat jak na úrovni profilu uživatele, tak na úrovni organizačních bezpečnostních politik.

V rámci testování byla IP adresa nastavena mimo povolený rozsah v profilu. Při pokusu o přihlášení byla autentizace Salesforce serverem odmítnuta a přístup zamítnut s chybovou hláškou (Obr. 25). Naopak po připojení ze správného IP rozsahu byl přístup povolen. To potvrzuje, že Salesforce IP restrikce fungují konzistentně nejen pro webové přihlášení, ale i pro OAuth flow jako Username-Password.

Login Hours definují časové rozpětí, ve kterém se uživatel může přihlásit. Mimo tento interval Salesforce přístup taktéž odmítne se stejnou chybovou hláškou. Pokud se uživatel pokusí přihlásit například v noci, kdy má profil nastavené přístupové okno pouze od 08:00 do 18:00, přihlášení nebude povoleno.

Z hlediska bezpečnosti představují obě funkce velmi jednoduchý, ale účinný způsob, jak omezit riziko neoprávněného přístupu. Typickým scénářem využití je například omezení přístupu pouze ze sítě firmy nebo pouze v rámci pracovní doby.

Login Hours			Edit	Delete
Day	Start Time	End Time		
Sunday	All Day	All Day		
Monday	All Day	All Day		
Tuesday	6:00 CEST	8:00 CEST		
Wednesday	All Day	All Day		
Thursday	All Day	All Day		
Friday	All Day	All Day		
Saturday	All Day	All Day		

Login IP Ranges				New
Action	IP Start Address	IP End Address	Description	
Edit Del	62.209.2...	62.209.2...		

Obrázek 25: Nastavení Login Hours a Login IP Ranges na profilu

POST

https://utb4-dev-ed.develop.my.salesforce.com/services/oauth2/token

Params

Authorization

Headers (11)

Body

Scripts

Tests

Settings

none

form-data

x-www-form-urlencoded

raw

binary

GraphQL

Key	Value	Description
☒ grant_type	client_credentials	
☒ client_id	3MVG9YFqzc_KnL.xeCkbNeuSK.6PCtpOjwTqTPb_rR5lltomK4EOyXfC01vtk.0Q...	
☒ client_secret	4559F7CB2248195C71423AC04933AF602DD35FCB6F93E0289E6D78465F9...	
Key	Value	Description

Body

Cookies (3)

Headers (12)

Test Results

400 Bad Request

JSON

Preview

Visualize

```
1 {
2   "error": "invalid_grant",
3   "error_description": "ip restricted"
4 }
```

Obrázek 26: Chybová hláška při pokusu o přihlášení mimo Login Hours, nebo IP Ranges

9 ANALÝZA ZRANITELNOSTI SALESFORCE

Přestože je Salesforce obecně považován za velmi bezpečnou platformu s robustními nativními ochrannými mechanismy, není imunní vůči zranitelnostem. Cloudové prostředí, vysoký počet integrací a rozsáhlé možnosti přizpůsobení prostřednictvím kódu, rozšíření a externích aplikací otevírají prostor pro potenciální bezpečnostní rizika. V této kapitole se zaměříme na vybrané typy útoků, zranitelnosti a konkrétní hrozby, které mohou ohrozit důvěrnost, integritu a dostupnost dat uložených v Salesforce.

Zranitelnosti mohou vznikat jak na úrovni konfigurace, tak na úrovni kódu nebo integrací. Mezi možné hrozby patří:

- Zneužití session tokenu (SID) – pokud dojde k úniku session ID (např. z cookies při nezabezpečené komunikaci), může útočník získat přístup k datům bez znalosti přihlašovacích údajů. Riziko je obzvláště vysoké při špatné implementaci přístupových práv nebo absenci IP restrikcí. Více se této problematice věnuje kapitola 8.
- Nesprávně nakonfigurované přístupu – chybná konfigurace OWD, přístupu k sídlících pravidel a hierarchie rolí může způsobit, že se důvěrná data stanou přístupná neoprávněným uživatelům v rámci organizace.
- Apex kód s nedostatečnou validací – vlastní kód bez řádné kontroly vstupů může umožnit útoky typu SOQL Injection, nebo neúmyslný přístup k datům.
- Chybná implementace OAuth – nedostatečně zabezpečené Connected Apps mohou umožnit zneužití access tokenů nebo obnovovacích tokenů, např. při absenci časového omezení nebo nesprávném ošetření scope oprávnění.
- Export dat a API zneužití – Salesforce umožňuje export velkého množství dat pomocí reportů nebo API. Pokud nejsou správně nastaveny limity, auditní logy nebo monitoring, může dojít k tichému úniku dat.

Nad rámec toho je samozřejmě důležité bezpečnost řešit i školením uživatelů a pravidelnou aktualizací všech komponent. V Salesforce se nazývá API verze a není nijak vyžadována aktualizace, pouze doporučena. Důležitou roli v detekci těchto hrozeb hraje bezpečnostní audit, monitoring aktivit a pravidelné revize oprávnění.

9.1 Rizika 3rd party aplikací

Salesforce podporuje rozšíření funkcionality několika způsoby. Nejvíce aplikací je dostupných v tzv. AppExchange, zde jsou sice aplikace kontrolovány přímo Salesforce, avšak zodpovědnost je vždy na straně uživatele. Další možností jsou instalace tzv. „unmanaged“, nebo „unlocked package“. V tomto případě se jedná pouze o balíček komponent, které vydavatel vytvořil. V tomto případě je důležité instalovat pouze z ověřených zdrojů a nejlépe si aplikaci nechat zkontrolovat. Další možností je připojení integrace pomocí Connected Apps. Tyto nástroje přinášejí vysokou přidanou hodnotu, ale zároveň zvyšují komplexitu a bezpečnostní rizika prostředí.

Rizika spojená s externími aplikacemi zahrnují např. nadměrná oprávnění – některé aplikace vyžadují přístup ke všem objektům, i když to není nezbytné pro jejich funkci. Access tokeny a refresh tokeny mohou být zneužity, pokud nejsou správně zabezpečeny a kontrolovány jejich expirací. Dalším úskalím může být nešifrovaná komunikace – pokud aplikace komunikuje s externími servery bez TLS, může dojít k odposlechu nebo manipulaci dat.

9.2 Známé zranitelnosti Salesforce

Vedle obecných hrozeb a konfiguračních rizik byla v posledních letech odhalena i řada konkrétních zranitelností v rámci produktů Salesforce, které byly publikovány na webu <https://security.salesforce.com/security-advisories>. Tyto zranitelnosti často vycházejí z chyb v autentizaci, autorizaci nebo v nesprávném ošetření vstupů, což může vést k útokům typu XSS, CSRF nebo neoprávněnému přístupu k datům.

Jedním z nejvýraznějších reálných útoků zaměřených na uživatele Salesforce byl incident označovaný jako PhishForce. Tento útok byl zaznamenán kolem roku 2020 a byl cílen přímo na uživatele platformy Salesforce pomocí podvržených přihlašovacích stránek. Útočníci vytvořili věrné kopie přihlašovací stránky Salesforce (včetně variant jako login.salesforce.com a my.salesforce.com), které byly šířeny pomocí phishingových e-mailů a reklamních kampaní. Jejich cílem bylo získání přihlašovacích údajů, které pak mohly být zneužity pro přístup k interním CRM datům firem.

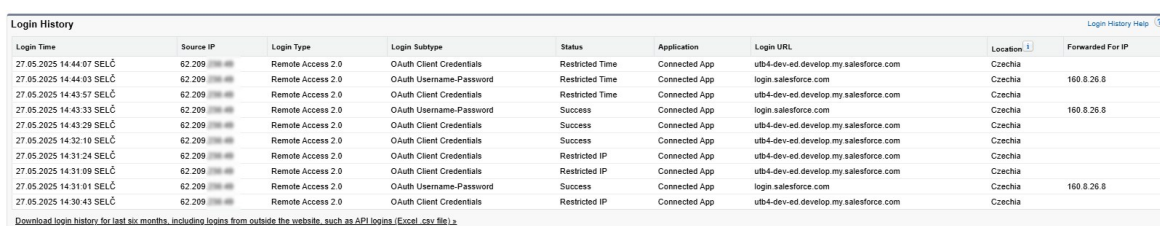
Útok PhishForce byl sofistikovaný nejen v grafickém provedení, ale i v tom, že některé phishingové stránky byly šifrované pomocí HTTPS, čímž mohly působit důvěryhodněji na koncové uživatele. V některých případech byly tyto stránky dokonce hostovány na kompromitovaných webech s důvěryhodnou doménou. Po zadání přihlašovacích údajů byli uživatelé přesměrováni na legitimní přihlašovací obrazovku Salesforce, čímž si útoku často ani nevšimli.

Salesforce na útok zareagoval zvýšením důrazu na dvoufaktorovou autentizaci (MFA) a rozšířením ochrany proti phishingu v rámci doménových politik a SSO konfigurace. Současně doporučil zákazníkům nasadit IP whitelisty, omezení přístupů na základě profilů a aktivní monitoring API přístupů. Tento incident jasně ukázal, že bezpečnostní hrozby se netýkají pouze chyb v systému, ale také sociálního inženýrství a nedostatečné edukace uživatelů.

10 BEZPEČNOSTNÍ INCIDENTY A MONITORING

Zajištění bezpečnosti v prostředí Salesforce není pouze otázkou správného nastavení oprávnění nebo konfigurace přístupových tokenů, ale také schopnosti včas detekovat incidenty a adekvátně na ně reagovat. Salesforce poskytuje k těmto účelům sadu nástrojů pro sledování událostí, analýzu podezřelého chování a vyhodnocování bezpečnostních hrozeb. V rámci této kapitoly byly provedeny dílčí testy zaměřené na auditní logy, detekci podezřelých aktivit a vyhodnocení reakcí systému na incidenty.

Pro sledování aktivit v systému jsou k dispozici Login History a Event Log Files. Login History umožňuje jednoduše zobrazit historii přihlášení konkrétního uživatele, včetně IP adresy, data, času a úspěšnosti přihlášení (obr. 26). Tato data lze získat přímo v uživatelském rozhraní, případně pomocí SOQL dotazů nebo přes REST API. V rámci testu byl opakovaně proveden pokus o přihlášení mimo vymezený časový rámec a mimo schválený rozsah IP adres. Salesforce správně zablokoval přístup a události se následně objevily v historii přihlášení. Tím bylo potvrzeno, že systém umí zaznamenat pokusy o přihlášení, které byly odmítnuty z důvodu porušení bezpečnostních politik.



Login Time	Source IP	Login Type	Login Subtype	Status	Application	Login URL	Location	Forwarded For IP
27.05.2025 14:44:07 SELČ	62.209.144.03	Remote Access 2.0	OAuth Client Credentials	Restricted Time	Connected App	utb4-dev-ed-develop.my.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:44:03 SELČ	62.209.144.03	Remote Access 2.0	OAuth Username-Password	Restricted Time	Connected App	login.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:43:57 SELČ	62.209.144.03	Remote Access 2.0	OAuth Client Credentials	Restricted Time	Connected App	utb4-dev-ed-develop.my.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:43:33 SELČ	62.209.144.03	Remote Access 2.0	OAuth Username-Password	Success	Connected App	login.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:43:29 SELČ	62.209.144.03	Remote Access 2.0	OAuth Client Credentials	Success	Connected App	utb4-dev-ed-develop.my.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:32:10 SELČ	62.209.144.03	Remote Access 2.0	OAuth Client Credentials	Success	Connected App	utb4-dev-ed-develop.my.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:31:24 SELČ	62.209.144.03	Remote Access 2.0	OAuth Client Credentials	Restricted IP	Connected App	utb4-dev-ed-develop.my.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:31:09 SELČ	62.209.144.03	Remote Access 2.0	OAuth Client Credentials	Restricted IP	Connected App	utb4-dev-ed-develop.my.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:31:01 SELČ	62.209.144.03	Remote Access 2.0	OAuth Username-Password	Success	Connected App	login.salesforce.com	Czechia	160.0.26.8
27.05.2025 14:30:43 SELČ	62.209.144.03	Remote Access 2.0	OAuth Client Credentials	Restricted IP	Connected App	utb4-dev-ed-develop.my.salesforce.com	Czechia	160.0.26.8

Download login history for last six months, including logins from outside the website, such as API logins. (Excel, CSV, PDF)

Obrázek 27: Logování přihlašování uživatele do Salesforce

Při pokusu o využití funkce Event Log Monitoring v rámci testování nebyly žádné záznamy dostupné. Je to z důvodu, protože tato funkce je dostupná pouze v edicích s aktivovanou licencí Salesforce Shield. V Developer edici, kde bylo prováděno testování, není tato funkcionálna dostupná přes uživatelské rozhraní a přístup k logům je omezený.

Alternativní možností monitorování aktivit v rámci platformy je Audit Trail (Obr. 27), který zaznamenává změny v nastavení organizace, jako jsou úpravy profilů, permission setů, bezpečnostních politik nebo přístupových toků. V rámci testování byly v tomto záznamu zaznamenány změny konfigurace Connected App a přiřazování oprávnění. Audit Trail tak může sloužit jako základní nástroj sledování administrátorských aktivit, zejména v prostředích, kde není k dispozici plný event monitoring.

View Setup Audit Trail				
Date	User	Source Namespace Prefix	Action	Section
27.05.2025 14:43:52 SELČ	s_bill@utb.cz:dp		Changed profile Standard User: login hours were changed from Tuesday All Day, Wednesday 1:00 AM - 11:00 AM to Tuesday 6:00 AM - 8:00 AM, Wednesday All Day	Manage Users
27.05.2025 14:43:22 SELČ	s_bill@utb.cz:dp		Changed profile Standard User: login hours were changed from Wednesday All Day to Wednesday 1:00 AM - 11:00 AM	Manage Users
27.05.2025 14:32:06 SELČ	s_bill@utb.cz:dp		Added Login Ip Range to Standard User from 62.209.230.49 to 62.209.230.49	Manage Users
27.05.2025 14:30:08 SELČ	s_bill@utb.cz:dp		Added Login Ip Range to Standard User from 10.0.0.0 to 10.0.0.1	Manage Users
27.05.2025 14:27:50 SELČ	s_bill@utb.cz:dp		Created permission set IP Restrictions: with no license	Manage Users
27.05.2025 13:55:02 SELČ	s_bill@utb.cz:dp		Created permission set Accounts Access: with no license	Manage Users
27.05.2025 13:54:53 SELČ	s_bill@utb.cz:dp		Deleted permission set Accounts Access	Manage Users
27.05.2025 13:50:27 SELČ	s_bill@utb.cz:dp		Changed profile for user User Integration from Minimum Access - Salesforce to Standard User	Manage Users
27.05.2025 13:48:57 SELČ	s_bill@utb.cz:dp		Changed profile for user User Integration from Minimum Access - API Only Integrations to Minimum Access - Salesforce	Manage Users
27.05.2025 13:39:35 SELČ	s_bill@utb.cz:dp		Created permission set Accounts Access: with User License Salesforce Integration	Manage Users
27.05.2025 13:39:19 SELČ	s_bill@utb.cz:dp		Deleted permission set Accounts Access	Manage Users
27.05.2025 13:37:38 SELČ	s_bill@utb.cz:dp		Changed profile for user User Integration from Minimum Access - Salesforce to Minimum Access - API Only Integrations	Manage Users
27.05.2025 13:37:13 SELČ	s_bill@utb.cz:dp		Changed profile for user User Integration from Minimum Access - API Only Integrations to Minimum Access - Salesforce	Manage Users
27.05.2025 13:36:12 SELČ	s_bill@utb.cz:dp		Changed permission set Accounts Access: Account object permissions were changed from No Access to Read	Manage Users
27.05.2025 13:34:23 SELČ	s_bill@utb.cz:dp		Created permission set Accounts Access: with no license	Manage Users
25.05.2025 18:10:36 SELČ	s_bill@utb.cz:dp		Assigned OAuth client credentials user s_bill@utb.cz:dp integration (UserID: [005d2000007V7gft]) to app Connected App (AppID: [0H4d2000002z3av])	OAuth Client Credentials User
25.05.2025 17:51:43 SELČ	s_bill@utb.cz:dp		For user s_bill@utb.cz:dp, the User Verified Email status changed to verified	Manage Users
25.05.2025 17:51:07 SELČ	s_bill@utb.cz:dp		Logged out using Login-As access for User Integration	Manage Users
25.05.2025 17:47:31 SELČ	s_bill@utb.cz:dp		Logged in using Login-As access for User Integration	Manage Users
25.05.2025 17:47:23 SELČ	s_bill@utb.cz:dp		Changed Administrators Can Log in as Any User from off to on	Manage Users

Obrázek 28: Setup Audit Trail logování v Salesforce

Co se týče reakce na bezpečnostní incidenty, Salesforce nenabízí vestavěný automatizovaný incident response systém, ale umožňuje jeho implementaci přes Flow, Apex nebo integraci s externími nástroji. Pro simulaci incidentu bylo testováno vytvoření podezřelé aktivity (např. masivní změna oprávnění a současný přístup přes API z neznámé IP adresy). Přestože systém přímo neupozornil na incident, bylo možné tyto události identifikovat pomocí analýzy logů. Pro účely produkčního provozu lze doporučit propojení s nástrojem typu SIEM, který by automaticky detekoval takové kombinace událostí a odeslal upozornění bezpečnostnímu týmu.

Z hlediska best practices je také důležité připravit si základní incident response plán. Tento plán by měl definovat, jak reagovat na zjištěný incident – od okamžité izolace postiženého účtu přes analýzu událostí až po oznámení vedení organizace a případně i subjektům údajů. Součástí by měla být i zpětná kontrola nastavení oprávnění a školení uživatelů.

Z provedeného testování lze potvrdit, že Salesforce disponuje nástroji, které umožňují zachytit a analyzovat bezpečnostní incidenty, nicméně jejich efektivita závisí na míře zapojení administrátora a případné integraci s externími monitorovacími nástroji. Proto je důležité nejen aktivovat auditní funkce, ale také pravidelně kontrolovat záznamy a nastavit automatické výstrahy tam, kde je to možné.

11 DOPORUČENÉ POSTUPY

Na základě provedené analýzy a praktického testování lze formulovat několik klíčových doporučení pro zajištění bezpečnosti dat v prostředí Salesforce. Tato doporučení se týkají nejen technického nastavení samotné platformy, ale i procesních opatření a způsobu, jakým organizace přistupuje k bezpečnostní správě.

Základem každého bezpečně nakonfigurovaného Salesforce prostředí je důsledné nastavení přístupových oprávnění. Uživatelé by měli mít k dispozici pouze ta oprávnění, která skutečně potřebují ke své práci. Toho lze dosáhnout kombinací profilů, které definují základní oprávnění, a permission setů, které slouží k přesnému doladění přístupu. Tato kombinace odpovídá principu minimálních práv, jehož cílem je omezit potenciální dopady případného zneužití přístupu. Stejný přístup je vhodné uplatnit i v rámci přístupů přes API, kde by každý integrační uživatel měl mít přiřazena pouze ta oprávnění, která nezbytně potřebuje.

Kromě správného rozdělení oprávnění je doporučeno konfigurovat také bezpečnostní prvky jako jsou dvoufaktorové ověření (MFA), IP restrikce a omezení přihlášení na základě časového okna (login hours). V rámci testování bylo ověřeno, že IP restrikce v Salesforce fungují spolehlivě jak pro přihlášení přes web, tak i pro autorizaci pomocí OAuth flow, včetně Username-Password flow. Tato opatření představují další vrstvu ochrany proti neoprávněnému přístupu mimo důvěryhodné prostředí.

Další oblastí, která významně přispívá k celkové bezpečnosti, je automatizace kontrol a monitoring podezřelého chování. Salesforce umožňuje pomocí nástrojů jako Flow nebo Scheduled Jobs zavést pravidelné kontroly přiřazených oprávnění, sledování aktivit v systému či upozorňování na přihlášení z neznámých IP adres. V rámci platformy Salesforce je k dispozici Event Monitoring, který umožňuje sledovat a analyzovat události jako jsou exporty dat, přihlášení uživatelů nebo volání API.

Bezpečnostní incidenty, které přesto mohou nastat, by měly být řešeny podle předem připraveného incident response plánu. Ten by měl obsahovat nejen technické kroky jako je deaktivace účtů nebo analýza logů, ale i organizační procesy – oznámení incidentu vedení společnosti, informování dotčených subjektů a revizi interních pravidel. V Salesforce je možné sledovat historii přihlášení a další auditní záznamy pomocí objektů jako LoginHistory nebo pomocí exportu Event Log Files a Audit Trail. Tyto informace slouží jako základ pro forenzní analýzu a návrh nápravných opatření.

Další důležitou bezpečnostní zásadou je využívání testovacích prostředí před nasazením do produkce. Všechny bezpečnostní prvky by měly být nejprve testovány v sandbox prostředí, které Salesforce nabízí v několika variantách.

Na základě těchto zkušeností lze doporučit testování CRUD oprávnění na objektech, simulace vypršení relací, rotace refresh tokenů a nastavení limitů pro API. Tato doporučení by měla být součástí dlouhodobé bezpečnostní strategie každé organizace využívající Salesforce.



Obrázek 29: 5 klíčových bezpečnostních opatření pro Salesforce

ZÁVĚR

Bezpečnost dat v prostředí Salesforce je složitou a stále se vyvíjející oblastí, která vyžaduje nejen správné nastavení systému, ale i důsledné porozumění tomu, jak jednotlivé bezpečnostní mechanismy spolupracují. Tato práce si kladla za cíl nejen teoreticky zmapovat současné možnosti zabezpečení této cloudové platformy, ale především je prakticky otestovat a zhodnotit jejich účinnost.

Testování konkrétních scénářů, jako je omezení přístupu podle IP adres a časového okna, správa oprávnění přes permission sety nebo ověřování chování přístupových tokenů, ukázalo, že Salesforce poskytuje robustní nástroje pro řízení přístupu i auditování. Zároveň se však potvrdilo, že nesprávná konfigurace či nedostatečná kontrola mohou vést k reálným bezpečnostním rizikům.

Významným přínosem práce byla také analýza přístupových oprávnění pomocí datové analýzy, která umožňuje identifikovat anomálie v nastavení práv a upozornit na možné slabiny v řízení přístupu. Za klíčový poznatek lze považovat zjištění, že token získaný z webového prohlížeče lze v určitých případech zneužít jako přístupový token pro API komunikaci. Toto chování sice odpovídá architektuře platformy, ale představuje riziko v případě nedostatečně chráněného klientského prostředí. Práce proto zdůrazňuje důležitost zabezpečení relací, správného nastavení domén a kontrolu možného přístupu k tokenům.

V průběhu práce byly identifikovány hrozby, doporučena konkrétní bezpečnostní opatření a ověřena jejich funkčnost v rámci simulovaných útoků. Na základě těchto poznatků byl sestaven přehled doporučených bezpečnostních postupů, které reflektují jak osvědčené praktiky, tak konkrétní výsledky testování.

Během testování se navíc ukázalo několik dalších směrů, které by bylo možné dále rozvíjet, například hlubší integrace s nástroji pro centralizovaný monitoring, ověřování chování 3rd party aplikací nebo automatizace auditních kontrol změn v oprávněních. Tato témata by mohla být předmětem budoucího výzkumu nebo interního bezpečnostního zhodnocení ve firemní praxi.

SEZNAM POUŽITÉ LITERATURY

- [1] VELTE, Anthony T.; VELTE, Toby J. a ELSERPETER, Robert C. *Cloud Computing: praktický průvodce*. Brno: Computer Press, 2011. ISBN 978-80-251-3333-0.
- [2] HOMMEROVÁ, Dita. *CRM v podnikových procesech*. Praha: Grada, 2012. ISBN 978-80-247-4388-2.
- [3] BARAN, Roger J. a GALKO, Robert J. *CRM: the foundation of contemporary marketing strategy*. New York: Routledge, 2013. ISBN 978-0-415-89656-6.
- [4] SPECCHIA, Antonio. *Customer relationship management (CRM) for medium and small enterprises*. New York : Productivity Press, 2022. ISBN 9781000532692.
- [5] BUTTLE, Francis a MAKLAN, Stan. *Customer relationship management: concepts and technologies*. Fourth edition. London: Routledge, 2019. ISBN 978-1-138-49825-9.
- [6] HILL, Richard. *Guide to cloud computing: principles and practice*. Computer communications and networks. London: Springer, 2013. ISBN 978-1-4471-4602-5.
- [7] SIEPMANN, Frank. *Managing risk and security in outsourcing IT services: onshore, offshore and the cloud*. Boca Raton: CRC Press, c2014. ISBN 978-1-4398-7909-2.
- [8] NAVEEN, Kumar. *58 Salesforce Statistics 2025 (Market Share & Revenue)*. Online. Demand Sage. 2024. Dostupné z: <https://www.demandsage.com/salesforce-statistics/>. [cit. 2025-03-02].
- [9] AGIANG, Vera. *40 Top Companies That Use Salesforce As Their Preferred CRM*. Online. RevopsTeam. 2024. Dostupné z: <https://revopsteam.com/marketing/companies-that-use-salesforce/>. [cit. 2025-03-02].
- [10] *The History of Salesforce*. Online. Salesforce. 2025. Dostupné z: <https://www.salesforce.com/news/stories/the-history-of-salesforce/>. [cit. 2025-03-02].
- [11] *Microsoft Dynamics 365 documentation*. Online. Microsoft Dynamics 365 documentation. Dostupné z: <https://learn.microsoft.com/en-us/dynamics365/>. [cit. 2025-05-15].
- [12] *Oracle Customer Experience (CX)*. Online. Oracle Customer Experience (CX). 2025. Dostupné z: <https://www.oracle.com/cx/>. [cit. 2025-05-15].

- [13] *SAP CRM and CX solutions*. Online. SAP CRM and CX solutions. 2025. Dostupné z: <https://www.sap.com/products/crm.html>. [cit. 2025-05-15].
- [14] *Adobe Enterprise Digital Solution*. Online. Adobe Enterprise Digital Solution. 2025. Dostupné z: <https://business.adobe.com/>. [cit. 2025-05-15].
- [15] VOŘÍŠEK, Jiří. *Strategické řízení informačního systému a systémová integrace*. Praha: Management Press, 2002. ISBN 80-859-4340-9.
- [16] ŽŮREK, Jiří. *Praktický průvodce GDPR: včetně úplného znění GDPR*. 2. aktualizované vydání. Právo. Olomouc: ANAG, 2018. ISBN 978-80-7554-152-9.
- [17] *Professional Services Security Privacy and Architecture*. Online. Salesforce Trust. 2024. Dostupné z: <https://compliance.salesforce.com/en/documents/a006e000013GUaMAAW>. [cit. 2025-05-27].
- [18] *General Data Protection Regulation*. Online. Salesforce Trust Security. 2024. Dostupné z: <https://security.salesforce.com/general-data-protection-regulation>. [cit. 2025-03-02].
- [19] *Salesforce Security Guide*. Online. Salesforce Developers. 2024. Dostupné z: https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/salesforce_security_guide.htm. [cit. 2025-03-01].
- [20] *The Complete List of Data Security Standards*. Online. Salesforce. 2024. Dostupné z: <https://www.salesforce.com/au/blog/data-security-standards/>. [cit. 2025-05-20].
- [21] *Salesforce Shield*. Online. Salesforce Shield. 2025. Dostupné z: <https://www.salesforce.com/platform/shield/>. [cit. 2025-05-15].
- [22] *NIST Computer Security Resource Center*. Online. NIST. 2024. Dostupné z: <https://csrc.nist.gov/>. [cit. 2025-05-18].
- [23] *Salesforce Shield*. Online. Salesforce Shield. Dostupné z: https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/salesforce_shield.htm. [cit. 2025-05-20].
- [24] *Security Guidelines for Apex and Visualforce Development*. Online. Security Guidelines for Apex and Visualforce Development. 2025. Dostupné

- z: https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/review_and_certification.htm. [cit. 2025-05-28].
- [25] *Platform Sharing Architecture*. Online. Salesforce Architects. 2025. Dostupné z: <https://architect.salesforce.com/fundamentals/platform-sharing-architecture>. [cit. 2025-05-18].
- [26] *Manage Users and Data Access*. Online. Salesforce. 2025. Dostupné z: https://help.salesforce.com/s/articleView?id=platform.users_manage_access.htm&type=5. [cit. 2025-05-18].
- [27] SOSINSKY, Barrie A. *Cloud computing bible*. Indianapolis: Wiley Publishing, 2011. ISBN 978-0-470-90356-8.
- [28] *Microsoft Dynamics 365 documentation*. Online. Microsoft Dynamics 365 documentation. Dostupné z: <https://learn.microsoft.com/en-us/dynamics365/>. [cit. 2025-05-15].
- [29] KLODWIG, Jakub. *Příručka právní regulace cloudu*. Brno: Nugis Finem Publishing, [2022]. ISBN 978-80-7614-008-0.
- [30] JOHNSON, Thomas. *Cybersecurity*. USA: CRC Press, 2015. ISBN 978-0367599362.
- [31] RASS, Stefan a SLAMANIG, Daniel. *Cryptography for security and privacy in cloud computing*. Artech House information security and privacy series. Boston: Artech House, [2014]. ISBN 978-1-60807-575-1.
- [32] *User Management Setup and Control Guide*. Online. Salesforce Trailhead. 2025. Dostupné z: https://trailhead.salesforce.com/en/content/learn/modules/lex_implementation_user_setup_mgmt. [cit. 2025-03-22].

SEZNAM OBRÁZKŮ

Obrázek 1: The five-step implementation process [5]	14
Obrázek 2: Struktura modelů v kontextu cloud computingu [8]	16
Obrázek 3: Logo Salesforce	18
Obrázek 4: Salesforce CRM	19
Obrázek 5: Podíl jednotlivých CRM platforem na trhu. [8].....	21
Obrázek 6: Ukázka Security Health Check v Salesforce	34
Obrázek 7: Přehled přístupu k záznamům [25]	38
Obrázek 8: Vytvoření Salesforce Developer Edition.....	41
Obrázek 9: Frekvenční analýza oprávnění nastavených na profilech.....	43
Obrázek 10: Grafické znázornění clusteringu pomocí K-Means	44
Obrázek 11: Grafické znázornění clusteringu pomocí DBSCAN	45
Obrázek 12: Vytvoření nového integračního uživatele v administraci Salesforce.....	47
Obrázek 13: Nastavení hesla pro integračního uživatele.	47
Obrázek 14: Nastavení Connected App v administraci Salesforce.	49
Obrázek 15: Pokročilé nastavení Connected App v administraci Salesforce.....	50
Obrázek 16: OAuth autorizace Username-Password Flow	51
Obrázek 17: OAuth autorizace Client Credentials Flow.....	52
Obrázek 18: Testování přístupu k objektu Account bez přiřazeného PS.....	53
Obrázek 19: Vytvoření Permission Setu pro přístup k objektu Account	54
Obrázek 20: Přiřazení PS pro přístup k objektu Account integračnímu uživateli.....	54
Obrázek 21: Úspěšný API call pro získání objektu Accounts po přiřazení PS	55
Obrázek 22: Přihlášení do Salesforce přes web na adrese www.login.salesforce.com	56
Obrázek 23: Access token uložený v cookies v sid po přihlášení do Salesforce	57
Obrázek 24: Rest API volání s použitým access tokenem z prohlížeč (sid) s úspěšným výsledkem.....	58
Obrázek 25: Nastavení Login Hours a Login IP Ranges na profilu	59
Obrázek 26: Chybová hláška při pokusu o přihlášení mimo Login Hours, nebo IP Ranges	59
Obrázek 27: Logování přihlašování uživatele do Salesforce	63
Obrázek 28: Setup Audit Trail logování v Salesforce	64
Obrázek 29: 5 klíčových bezpečnostních opatření pro Salesforce	66

SEZNAM TABULEK

Tabulka 1: Porovnání klasického šifrování a Salesforce Shield [23].....	29
Tabulka 2: Porovnání nastavení přístupu v Permission Setu a Profilu [32].....	38

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CRM Customer Relationship Management

UI User Interface

API Application Programming Interface

CRUD Create, Read, Update, Delete

2FA Two-factor authentication (Dvojúrovňové ověřování)

SSO Single Sign-On

OWD Organization-Wide default

PKCE Proof Key for Code Exchange

PS Permission Set

AES Advanced Encryption System

XSS Cross-Site Scripting

CSRF Cross-Site Request Forgery

SEZNAM PŘÍLOH

Příloha P I: Data_mining.py

Příloha P II: Frekvencni_analyza.py

Příloha P III: Elbow_rule.py

Příloha P IV: K_means.py

Příloha P V: Dbscan.py