ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ
Факултет „Компютърни системи и технологии“
Катедра „Информационни технологии в индустрията“

Маг. Анастасиос Дионисиос Ливеретос

УПРАВЛЕНИЕ НА ИДЕНТИЧНОСТТА И ДОСТЪПА В МУЛТИКОРПОРАТИВНА СРЕДА

А В Т О Р Е Ф Е Р А Т

на дисертация за придобиване на образователна и научна степен
"ДОКТОР"

Област: 5. Технически науки
Професионално направление: 5.3 Комуникационна и компютърна техника
Научна специалност: „Автоматизирани системи за обработка на информация и управление“

Научни ръководители:
доц. д-р инж. Иво Руменов Драганов
проф. д-р инж. Милена Кирилова Лазарова–Мицева

СОФИЯ, 2025 г.

Дисертационният труд е обсъден и насочен за защита от Катедрения съвет на катедра „Информационни технологии в индустрията“ към Факултет „Компютърни системи и технологии“ на ТУ–София на редовно заседание, проведено на 17.03.2025 г.

Публичната защита на дисертационния труд ще се състои на 19.06.2025 г. от 13:00 часа в Конферентната зала на БИЦ на Технически университет – София на открито заседание на научното жури, определено със заповед № ОЖ-5.3-16/04.04.2025 г. на Ректора на ТУ–София в състав:

1. проф. д-р Румен Иванов Трифонов – председател
2. доц. д-р Галя Веселинова Павлова
3. проф. д-р инж. Вера Ангелова Ангелова–Димитрова
4. проф. д-р Атанас Велков Атанасов
5. доц. д-р инж. Пламен Василев Василев

Рецензенти:

1. проф. д-р Атанас Велков Атанасов
2. доц. д-р Галя Веселинова Павлова

Материалите по защитата са на разположение на интересуващите се в канцеларията на Факултет „Компютърни системи и технологии“ на ТУ–София, блок №1, кабинет №1443а.

Дисертантът е задочен докторант към катедра „Информационни технологии в индустрията“ на Факултет „Компютърни системи и технологии“. Изследванията по дисертационната разработка са направени от автора.

Автор: маг. Анастасиос Дионисиос Ливеретос
Заглавие: Управление на идентичността и достъпа в мултикорпоративна среда
Тираж: 30 броя
Отпечатано в ИПК на Технически университет – София

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема

Цифровата трансформация и хибридната работна среда значително усложниха процесите по управление на идентичността и достъпа (Identity and Access Management, IAM) и по този начин се превърнаха в критични фактори за модернизация на IAM. ***Обект на изследване*** в дисертационният труд е управлението на идентичността и достъпа като част от цифровата трансформация на големите корпорации. ***Предмет*** на дисертационният труд е управлението на идентичността и достъпа в мултикорпоративни среди за сигурен достъп до облачни и локални приложения и данни. ***Работната хипотеза*** на дисертационния труд е както следва: управлението на идентичността и достъпа в мултикорпоративна среда може да бъде осигурено по няколко начина и чрез множество налични решения, предлагани от доставчиците на услуги в тази област. Въпреки че повечето от тях отговарят на една и съща потребност, съществуват разпознаваеми разлики и добри практики, които трябва да се следват за осигуряване на сигурно и надеждно управление и администриране на идентичност и достъпа в мултикорпоративна среда.

Цел на дисертационния труд, основни задачи и методи за изследване

Целта на научните изследвания на дисертационния труд е да се направи цялостен анализ на управлението на идентичността и достъпа в многокорпоративни среди и да се изследват основните предизвикателства, тенденции и решения, подпомагащи цифровата трансформация и гарантиращи сигурността на организационните активи, на базата на което да се предложат стратегии и методологии за постигане на сигурна и ефективна рамка за управление на идентичност, както и за сертифициране на управлението и администрирането на идентичност (Identity Governance and Administration, IGA).

За постигането на поставената цел следва да бъдат изпълнени следните задачи:

- Да се направи обстоен литературен обзор и анализ на настоящите тенденции и състоянието на научните изследвания в областта на управление на идентичността и достъпа;
- Да се проучат съществуващите подходи, използван от големи корпорации, за управление на идентичността и достъпа (IAM) и управление на идентичността и достъпа на клиенти (Customer Identity and Access Management, CIAM);
- Да се направи сравнителен анализ и избор на подходи за непрекъснато развитие и адаптиране на стратегиите за управление на идентичността и достъпа за преодоляване на нововъзникващите заплахи и атаки, включително възможността за използване на изкуствен интелект (Artificial Intelligence, AI), децентрализирана идентичност (Decentralised Identity, DID) и проверими удостоверения (Verifiable Credentials, VC).

Научните методи, които са използвани в дисертационния труд, са свързани с проучване на литературни източници в областта на управление на идентичността и достъпа; проучване на услуги предоставяни от водещи доставчици на технологии за управление на идентичността и достъпа на клиенти; анкетиране на големи световни корпорации за определяне на използваните подходи и слабости при управлението на идентичността и достъпа; сравнителен анализ и избор на подходи и методи за надеждно и сигурно управление на идентичността и достъпа в мултикорпоративна среда.

Научна новост

Предложена е класификация на многофакторната автентификация (Multifactor Authentication, MFA), която определя структурирана таксономия на различните видове атаки и предлага теоретична рамка, подобряваща академичното разбиране за уязвимостите и потенциалните експлойти при многофакторна автентификация и по този начин допринася за по-широкото познаване на предизвикателствата пред

киберсигурността и намаляването на заплахите за сигурността в управлението на идентичността и достъпа. Направен е цялостен анализ на водещите доставчици на технологии за управление на идентичността и достъпа на клиентите, който предлага научно обоснован подход за организациите при избор на решения, съответстващи на техните специфични нужди и организационни цели. Предложена е методология за сертифициране на управлението и администрирането на идентичности, която оптимизира сертифицирането на достъпа като свързва теоретичните рамки с практически стратегии за прилагане и подобрява на видимостта и рационализира процеса на сертифициране, осигурявайки систематичен подход за практическото му приложение. Предложена е нова рамка за сигурно и мащабируемо управление на идентичността, основана на децентрализирани модели на идентичност и парадигми за управление на идентичността, ориентирани към доверие, включително децентрализирана идентичност и проверими удостоверения. Предложени са стратегии за интегриране на изкуствен интелект в рамките на управление на идентичността и достъпа, които позволяват намаляване на риска като отчитат мащабируемостта, автоматизацията и непрекъснатото адаптиране към нововъзникващи заплахи.

Практическа приложимост

В дисертационния труд е направен цялостен анализ на управлението на идентичността и достъпа в многокорпоративни среди като са разгледани основните предизвикателства, тенденции и решения. Изследването показа решаващата роля на управлението на идентичността и достъпа в подкрепа на цифровата трансформация и гарантирането на сигурността на организационните активи. Изводите и препоръките, представени в дисертацията, предлагат ценни идеи за организациите, които се стремят да подобрят своите стратегии за управление на идентичността и достъпа и да постигнат сигурна и ефективна рамка за управление на идентичността. Приносите на тази дисертация надхвърлят академичната сфера, като предлагат практически насоки за вземане на решения при управление на идентичността и достъпа. Предложените методологии и добри практики могат да послужат като пътна карта за организациите, които искат да модернизират използваните решения за управление на идентичността и достъпа и да се справят с променящата се среда за сигурност. Тъй като пътуването към цифровата трансформация продължава, значението на надеждните и адаптивни решения за управление на идентичността и достъпа не може да бъде подценява.

Апробация

Резултатите от дисертационния труд са разглеждани, обсъждани и публикувани в International Journal of Economics and Management Systems, International Journal of Computers, Proceedings of the Technical University of Sofia, International Journal of Advances in Computer Science and Technology, Proceedings of 32nd IEEE National Conference with International Participation TELECOM’2024

Публикации

Основни постижения и резултати от дисертационния труд са публикувани в пет научни статии. Научните статии са представени на национални конференции с международно участие и международни научни издания.

Структура и обем на дисертационния труд

Дисертационният труд е в обем от 133 страници, като включва увод, 6 глави за решаване на формулираните основни задачи, списък на основните приноси, списък на публикациите по дисертацията и използвана литература. Цитирани са общо 109 литературни източници, всичките 109 са на латиница, в това число 5 интернет адреси. Работата включва общо 21 фигури и 12 таблици.

II. СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

ГЛАВА 1. ТЕКУЩО СЪСТОЯНИЕ И ПРЕДИЗВИКАТЕЛСТВА ПРИ УПРАВЛЕНИЕТО НА ИДЕНТИЧНОСТТА И ДОСТЪПА В МНОГОКОРПОРАТИВНА СРЕДА

В тази глава на дисертационния труд е представен литературен преглед на текущото състояние, рисковите фактори и предизвикателствата при управлението на идентичността и достъпа като част от цифровата трансформация на организациите. Представени са и резултати от проучване на автора на базата на анкета за това как големите корпорации подхождат към управлението на идентичността и достъпа.

1.1. Управление на идентичността и достъпа

Цифровата трансформация и хибридната работна среда значително усложняват процесите на управлението на идентичността и достъпа, превръщайки се в ключов стимул за модернизация. Управлението на идентичностите и свързаните с тях разрешения са стратегически аспект на киберсигурността.

Необходим е прагматичен подход към управление на идентичността, който да балансира между подобряването на сигурността на организацията и подпомагането на гъвкавостта на бизнеса. Организациите трябва да осигурят достъп до различни облачни или локални приложения и данни, което налага съвременни инициативи за управление на идентичността и достъпа. Необходими е целенасочен контрол за подобряване на видимостта и рационализиране на предоставянето на достъп без да се ограничава производителността на служителите. Съвременните решения за управление и администриране на идентичности използват внедряване в облачни имплементации за мащабируемост и използват анализи и автоматизация за повишаване на ефективността и сигурността. Автоматизира се предоставянето на фин контрол на достъпа и се идентифицират и коригират прекомерно предоставените и недостатъчно използваните идентичности.

На базата на литературното проучване могат да бъдат направени следните заключения за настоящата ситуация: управлението на достъпа е вторият най-бързо растящ сегмент на софтуера за сигурност с увеличение от 33.5% между 2021 и 2024 г.; организациите преоценяват своите стратегии за управление на идентичността и достъпа поради широко разпространение на хибридна работна среда, което изисква гарантиране на работоспособността на внедрените решения за управление и администриране на идентичност за съвременните хибридни работни среди.

Възможностите на решенията за управление и администриране на идентичност изискват управление на жизнения цикъл на идентичността, политики, управление на ролите и поддръжка на делегирано администриране.

1.2. Рискове за подобряване на управлението и администрирането на идентичностите

Въпреки че модернизирането на управлението и администрирането на идентичност е от решаващо значение за осигуряване на сигурен достъп до облачни и локални приложения, то създава рискове, с които организациите трябва да се справят, в това число:

- Сложност и интеграция: съвременните решения за управление и администриране на идентичност често изискват интеграция с множество системи и приложения, което може да бъде сложен и времеотнемащ процес.

- Мащабируемост: с разрастване на организациите техните решения за управление и администриране на идентичност трябва да се мащабират, което може да бъде предизвикателство особено за големи корпорации с разнообразни и разпределени служители.
- Съответствие с регулаторни изисквания: организациите трябва да гарантират, че процесите им по управление и администриране на идентичност отговарят на различни регулаторни изисквания, които могат да варират в зависимост от региона и индустрията.
- Рискове за сигурността: усъвършенстването на процесите за управление и администриране на идентичност може да доведе до нови рискове за сигурността, като например уязвимости в точките на интеграция между различни системи.
- Приемане и обучение на потребителите: от решаващо значение е да се гарантира, че служителите разбират и приемат новите процеси за управление и администриране на идентичност, което изисква цялостно обучение и постоянна подкрепа на потребителите.

Стратегическият подход към модернизация на управлението и администрирането на идентичност е от съществено значение за балансиране на необходимостта от подобряване на сигурността и съответствието с практически предизвикателства при прилагането на модернизацията.

1.3. Тенденции в процеса на управление и администриране на идентичност

Управлението и администрирането на идентичност е все по-важно в контекста на цифровата трансформация и хибридната работна среда. Ето защо съвременните решения за управление и администриране на идентичност трябва да бъдат мащабируеми и гъвкави и да могат да се интегрират с различни системи и приложения. Организациите все по-често възприемат решения за управление и администриране на идентичност, базирани на облачни технологии за да използват предимствата на мащабируемостта, автоматизацията и усъвършенствания анализ, който облачните решения предоставят.

Една от ключовите тенденции при управление и администриране на идентичност е нарастващият фокус върху автоматизация и анализи на процесите. Съвременните решения за управление и администриране на идентичност използват машинно обучение и изкуствен интелект за автоматизиране на управление на жизнения цикъл на идентичността, управление на политики и роли и сертифициране на достъпа. Тази автоматизация помага на организациите да подобрят ефективността, да намалят грешките и да повишат сигурността.

Друга тенденция е преминаването към по-ориентиран към потребителя подход за управление и администриране на идентичност. Организациите признават важността на осигуряването на безпроблемно и интуитивно потребителско изживяване за администраторите и крайните потребители. Това включва функции като портали за самообслужване, делегирано администриране и поддръжка на различни типове идентичности, включително служители, изпълнители, клиенти и нечовешки идентичности.

Съответствието и регулаторните изисквания са все по-важни при формирането на стратегиите за управление и администриране на идентичност. Организациите трябва да гарантират, че процесите им за управление и администриране на идентичност отговарят на различни разпоредби, като например Общ регламент за защита на данните (General Data Protection Regulation, GDPR), и са в състояние да се адаптират към променяща се регулаторна ситуация.

Необходимостта от мащабируемост, автоматизация, ориентираност към потребителя и съответствие с изискванията определя тенденциите в процеса на управление и администриране на идентичност. Организациите трябва да използват съвременни решения за управление и администриране на идентичност, които са базирани на модерни технологии за да отговорят на тези променящи се изисквания.

1.4. Интегриране на изкуствения интелект и метавселената с управлението на идентичността и достъпа

Една от областите, върху които се фокусира вниманието на изследванията в дисертационния труд, е ролята на изкуствения интелект в управлението на идентичността и достъпа. Изкуственият интелект може да подобри управлението на идентичността и достъпа чрез автоматизиране на управлението на жизнения цикъл на идентичността, подобряване на контрола на достъпа и откриване на аномалии. Решенията за управлението на идентичността и достъпа, управлявани от изкуствен интелект, могат да анализират големи обеми данни за да идентифицират модели и да прогнозират потенциални заплахи за сигурността като по този начин повишават цялостната сигурност на организацията.

Метавселената, разглеждана като виртуално споделено пространство, създадено от конвергенцията на виртуално подобрена физическа реалност и физически устойчива виртуална реалност, представя уникални предизвикателства и възможности за управлението на идентичността и достъпа. Съществува необходимост от надеждни решения за управление на идентичността и достъпа, които да управляват идентичностите и достъпа в метавселената като осигуряват сигурно и безпроблемно взаимодействие между потребителите и виртуалните среди.

Организациите трябва да възприемат иновативни стратегии за управление на идентичността и достъпа, които използват технологиите на изкуствен интелект за повишаване на сигурността, подобряване на потребителското изживяване и подпомагане на гъвкавостта на бизнеса.

1.5. Управление на идентичност и достъп на клиенти

Управлението на идентичността и достъпа на клиентите се фокусира върху управлението и защитата на идентичността на клиентите, което е от решаващо значение за подобряване на клиентското преживяване и гарантиране на сигурността на данните.

Ключовите аспекти при управлението на идентичността и достъпа на клиентите са както следва:

- Доставчици на решения за управление на идентичността и достъпа на клиентите: различни доставчици предоставят решения за управление на идентичността и достъпа на клиентите като избора на доставчик се основа на специфичните организационни нужди.
- Бизнес фактори за управление на идентичността и достъпа на клиентите: основните фактори за приемане на решения за управление на идентичността и достъпа на клиентите включват подобряване на обслужването на клиентите, осигуряване на съответствие с нормативните изисквания и повишаване на сигурността.
- Ползи от внедряването на управление на идентичността и достъпа на клиентите: подобрена удовлетвореност на клиентите, по-добра сигурност на данните и рационализирано управление на достъпа.
- Предизвикателства при внедряването на управление на идентичността и достъпа на клиентите: сложност на интеграцията, проблеми с мащабируемостта и съответствие с нормативните изисквания.

Ролята на управлението на идентичността и достъпа на клиентите е от решаващо значение в съвременните стратегии за управление на идентичност и достъп, особено за подобряване на обслужването на клиентите и осигуряване на надеждни мерки за сигурност.

1.6. Проучване на управлението на идентичността и достъпа и управлението на идентичността и достъпа на клиентите в корпоративна среда

Проведено е авторско проучване за подходите на големите корпорации при управление на идентичността и достъпа и управление на идентичността и достъпа на клиенти. Методологията на проучването описва подробно подхода за събиране на данни от 24 глобални корпорации работещи в 17 различни индустрии като са изяснени критериите за подбор на участниците и методите, използвани за събиране и анализ на данните.

Резултатите и анализът на данните от проучването допринасят за установяване на няколко основни констатации, като например степента на приемане на решенията за управление на идентичността и достъпа и управлението на идентичността и достъпа на клиентите, предизвикателствата, пред които са изправени организациите при внедряването на тези решения, и ползите реализирани от тяхното приемане. Анализът обхваща и различните стратегии, използвани от корпорациите за управление на идентичностите и достъпа, включително използването на облачни и локални решения.

Основните резултати от проучването дават представа за текущото състояние на управление на идентичността и достъпа и управление на идентичността и достъпа на клиенти в големите корпорации, включително тенденции, общи практики и области за подобрение. Резултатите от проучването подчертават важността на внедряването на съвременни решения за управление на идентичността и достъпа и управление на идентичността и достъпа на клиенти за повишаване на сигурността, подобряване на потребителското преживяване и подпомагане на гъвкавостта на бизнеса.

Резултатите в голяма степен съответстват на настоящите тенденции в областта, установени от други скорошни проучвания в световен мащаб. Съществуват обаче интересни примери за изключения в прилагането на решенията за управление на идентичността и достъпа за няколко големи компании и множество специфики относно конкретните очаквания и действителната успеваемост на обработката на всички идентичности при останалите респонденти в проведената анкета. От тези резултати могат да се изведат полезни насоки за по-задълбочено проучване на техническите и организационните аспекти на ефективното прилагане на решения за управление на идентичността и достъпа, последвани от препоръки за по-ефективно използване.

Основните резултати от проведената анкета на големи корпорации при управление на идентичността и достъпа и управление на идентичността и достъпа на клиенти могат да бъдат обобщени както следва:

- Повечето компании са удовлетворени, че разполагат с надеждно решение за управление на вътрешни идентичности, които обхващат различни процеси, както и различни граници между вътрешно и външно управление на решенията. Най-критичната точка за вземане на решения остава нежеланието за поемане на риск, което потвърждава необходимостта от по-нататъшно задълбочаване на оценката в техническите разлики между различните решения за управление и администриране на идентичност.
- Разширяването на обхванатите идентичности с външни такива вече е започнало и повечето компании разглеждат различни решения и идентичности, които да бъдат обхванати.

Пандемията Covid-19 и ускоряването на използването на онлайн маркетингови канали отново потвърждават необходимостта от сигурно ориентирано към клиента осигуряване на достъп. Съответните инструменти не са толкова добре развити, колкото тези за управление и администриране на идентичност. Техническите ограничения, съчетани с бизнес спецификите, превръщат внедряването на решения за управление на идентичността и достъпа на клиенти в предизвикателство за повечето компании. Необходим е допълнителен анализ на стандартните и адаптивните функции на решенията.

1.7. Изводи към първа глава

Задълбоченият анализ на текущото състояние и предизвикателствата пред управлението на идентичността и достъпа в многокорпоративна среда разкрива усложняването на процесите на управлението на идентичността и достъпа в условия на цифрова трансформация и хибридна работна среда, превръщайки ги в критични фактори за модернизация. Управлението на идентичностите и свързаните с тях разрешения е стратегически аспект на киберсигурността, изискващ прагматичен подход, който балансира подобряването на позицията по отношение на сигурността и подкрепата на гъвкавостта на бизнеса. Анализът подчертава необходимостта от съвременни решения за управление и администриране на идентичности, които използват анализи и автоматизация за повишаване на ефективността и сигурността и автоматизират предоставянето на фин контрол на достъпа като идентифицират и отстраняват потенциални несъответствия.

Рисковете, свързани с подобряването на управлението и администрирането на идентичности са свързани с прекомерно предоставен достъп, прекомерни разрешения за привилегировани потребители, нарушения на разделението на задълженията, проблеми с управлението на промените и лошо съответствие с принципите на нулевото доверие. Тенденциите в процеса на управление и администриране на идентичности включват необходимост контролът на достъпа да се адаптира към работа от разстояние, увеличаване на значимостта на многофакторната автентикация и необходимост от подобряване на потребителското преживяване при запазване на сигурността.

От особена важност е интегрирането на изкуствен интелект за подпомагане на управлението на идентичност и достъп чрез удостоверяване на потребители, контрол на достъпа, осигуряване на потребители, управление на пароли, откриване на аномалии и интерфейси на естествен език. Освен това се подчертава значението на IAM В метавселената, където потребителите ще се нуждаят от сигурни и надеждни начини за управление на своите самоличности и достъп до ресурси значението на управлението на идентичност и достъп има критична роля

Резултатите от авторско проучване проведено с анкетиране на глобални корпорации потвърждават, че повечето компании считат, че разполагат с надеждно решение за управление и администриране на идентичности по отношение на управлението на вътрешните идентичности като съществува разнообразни обхванати процеси и граници между вътрешно и външно управление на решенията като е стартирано разширяване на обхванатите идентичности с външни идентичности.

ГЛАВА 2. ВОДЕЩИ ДОСТАВЧИЦИ НА ТЕХНОЛОГИИ ЗА УПРАВЛЕНИЕ НА ИДЕНТИЧНОСТТА И ДОСТЪПА И УПРАВЛЕНИЕ НА ИДЕНТИЧНОСТТА И ДОСТЪПА НА КЛИЕНТИТЕ

В тази глава на дисертационния труд е представен обстоен анализ на водещите доставчици на технологии в областта на управление на идентичност и достъп и управление на идентичност и достъп на клиенти.

2.1. Водещи доставчици на технологии за управление на идентичност и достъп

Според проучването, представено в предишната глава, много фактори влияят върху поведенческите намерения при избор на решения за управление и администриране на идентичност, в това число полезност, простота на използване, съответствие между задачи и технология, нагласи за доверие, доверие в Интернет (включително обмен на информация), опасения за неприкосновеност на личния живот и разходи. Резултатите от проведеното анкетиране на 24 глобални корпорации показват, че 11 от 22 (50%) от участниците използват SailPoint, 6 от тях използват SailPoint IdentityIQ; 2 използват SailPoint IdentityNow. От останалите 11 анкетирани компании, които не използват SailPoint, 2 използват Oracle Identity Management, а другите 9 използват различни решения или комбинации от решения.

2.1.1. SailPoint е водещ доставчик на технологии в областта на управление на идентичност и достъп. Цялостните решения на SailPoint помагат на организациите да управляват и защитават идентичности в различни системи и приложения и за насочени към подобряване на сигурността, осигуряване на съответствие и повишаване на оперативната ефективност. Основните характеристики и предимства на решенията на SailPoint за управление на идентичност и достъп включват възможност да рационализират управлението на идентичности, да автоматизират процесите за управление на достъпа и да предоставят надеждни възможности за отчитане и анализ. Решенията за управление на идентичност и достъп на SailPoint са изградени върху облачна платформа, което позволява мащабируемост и гъвкавост. Платформата използва усъвършенствани технологии базирани на изкуствен интелект и машинно обучение за да повиши сигурността и ефективността. Решенията на SailPoint поддържат и широк набор от интеграции с други корпоративни системи, което улеснява организациите при управление на идентичностите в цялата им ИТ екосистема. Организациите се сблъскват и с няколко предизвикателства при внедряване на решения за управление на идентичност и достъп. Решенията на SailPoint са насочени към сложността на управление на идентичности в хибридна ИТ среда, необходимост от непрекъснато съответствие и важност на потребителското изживяване. Управлението на идентичност и достъп изисква цялостен подход, който включва не само технологии, но и процеси и политики.

2.1.2. Oracle Management Cloud (OMC) е цялостен пакет от услуги за управление, предназначен да осигури пълна видимост, контрол и автоматизация на приложения и инфраструктура. OMC използва машинно обучение и анализ на големи обеми данни за да предостави информация и да повиши оперативната ефективност. Възможностите на OMC включват мониторинг, управление и анализ на приложения, инфраструктура и логове, които помагат на организациите да оптимизират производителността, да предотвратяват прекъсвания и да намаляват оперативните разходи. Възможностите на OMC за мониторинг на производителността на приложенията позволяват на организациите да получат дълбока прозрачност за производителността на приложенията и потребителското изживяване. Като осигурява мониторинг и диагностика в реално време, OMC помага да се идентифицират и решават проблеми с производителността преди те да се отразят на потребителите, което осигурява надеждност и наличност на критични бизнес приложения.

Възможностите на ОМС за мониторинг и управление на инфраструктура осигуряват цялостна видимост за състоянието и производителността на ИТ инфраструктурата. Инструментите за мониторинг на инфраструктурата на ОМС помагат на организациите да откриват и разрешават проблеми в сървъри, бази данни и други инфраструктурни компоненти. Възможностите за анализ на логове на ОМС позволяват на организациите да събират, анализират и визуализират данни от логове от различни източници, което позволява на организациите да получат представа за оперативни проблеми, заплахи за сигурността и нарушения на съответствие с регулации.

2.1.3. Omada е един от водещите доставчици на технологии в областта на управление на идентичност и достъп като предлага цялостни решения, предназначени да помогнат на организациите да управляват и защитават идентичности в различни системи и приложения. Решенията на Omada са насочени към подобряване на сигурността, осигуряване на съответствие и повишаване на оперативната ефективност. Основните характеристики и предимства на предложенията на Omada за управление на идентичност и достъп включват възможност да се рационализира управлението на идентичност, да се автоматизират процесите за управление на достъп и да се предоставят надеждни възможности за отчитане и анализ. Решенията за управление на идентичност и достъп на Omada са изградени върху платформа, базирана на облачни технологии, която позволява мащабируемост и гъвкавост. Платформата използва изкуствен интелект и машинно обучение за да повиши сигурността и ефективността. Решенията на Omada поддържат и широк набор от интеграции с други корпоративни системи, което улеснява организациите при управление на идентичности в цялата им ИТ екосистема. Освен това решенията на Omada се справят със сложността на управление на идентичности в хибридна ИТ среда, необходимостта от непрекъснато съответствие с регулации и важността на потребителското изживяване. По този начин решенията на Omada подпомагат организациите да се ориентират в сложността на управлението на идентичности и достъп в съвременната цифрова ера.

2.2. Водещи доставчици на технологии за управление на идентичност и достъп на клиенти

Изискванията за управление на идентичност и достъп на клиенти са много различни от тези за управление на идентичност и достъп. Основните характеристики на управление на идентичност и достъп на клиенти включват хостинг в облак, платформено базирана функционалност, силна автентификация и синдикация, интеграция, мащабируемост и възможност за персонализиране на интерфейса. Според проучването, представено в предишната глава, тези особености са водещи за организациите да приемат допълнителни решения, които да подпомагат в управлението на външни идентичности. Резултатите от проведеното анкетиране на 24 глобални корпорации показват, че 14 от 22 (64%) от участниците използват най-много едно решение за управление на идентичност и достъп на клиенти заедно с решения за управление на идентичност и достъп за да поддържат идентичности на външните потребители: 5 от 14 (36%) от респондентите използват SAP Customer Data Cloud (преди известен като Gigya), като една компания (във фармацевтична промишленост), която понастоящем използва MS Azure също мигрира към SAP Customer Data Cloud; 3 от 14 компании (21%) използват Okta, други 3 – Ping Identity, една компания (в областта на услуги за човешки ресурси) използва CA Siteminder, а друга компания (във фармацевтичната индустрия) използва SailPoint. Сред компаниите, които в момента не използват никакво решение за управление на идентичност и достъп на клиенти, една компания (в автомобилна индустрия) проучва внедряване на Azure AD, а друга компания (в енергетиката) инвестира в изграждането на собствено решение за управление на външни идентичности.

2.2.1. SAP е основен доставчик на технологии в областта на управление на идентичност и достъп на клиенти. Цялостните решения на SAP за управление на идентичност и достъп на клиенти са предназначени да помогнат на организациите да управляват и защитават идентичностите на клиенти в различни системи и приложения. Решението на SAP за управление на идентичност и достъп на клиенти е SAP Customer Data Cloud, което обхваща SAP CIAM за B2C и SAP Enterprise Consent and Preference Management (SAP ECPM). SAP CIAM и SAP ECPM са публични облачни решения (SaaS), които предоставят услуги интегрирани в клиентски приложения и бекенд решения. За да се даде възможност за внедряване и използване на съответните услуги в съответствие с регионални разпоредби за защита на данните, решенията са достъпни в световен мащаб с центрове за данни в Австралия, Европейския съюз и САЩ (включително CIAM за B2B Add-On), както и в Русия и Китай (с изключение на CIAM за B2B Add-On). За Европейския съюз съществува допълнителна възможност за използване на център за данни, базиран на MS Azure. SAP Customer Identity предоставя функционалността на решението SAP CIAM за да помогне на компаниите да превърнат непознати онлайн посетители в познати лоялни клиенти като ги ангажират на ранен етап като същевременно повишат сигурността свеждайки до минимум рискови трансакции, базирани на пароли.

2.2.2. Microsoft предлага стратегия с четири стълба на цифровата трансформация за внедряване на управление на идентичност и достъп на клиенти: ангажиране на клиентите, овластяване на служителите, оптимизиране на операциите и трансформиране на продуктите. Тези четири основни стълба, както и техният цифров цикъл за обратна връзка позволяват на клиентите да концептуализират, усъвършенстват и реализират своите идеи за бизнес трансформация. Решенията за управление на идентичност и достъп на клиенти на Microsoft осигуряват самостоятелна регистрация на потребители, управление на акаунти и възстановяване на пароли. Вградената възможност за персонализиране на потребителското изживяване позволява на клиентите на Microsoft да персонализират брандинг и тема на интерфейсите за крайни потребители според своите предпочитания. Друга функция, осигурена чрез решенията за управление на идентичност и достъп на клиенти на Microsoft, е възможността за активиране на потребителски домейн към услугата, така че потребителите да не виждат адреса microsoftonline.com в url лентата на уебстраниците B2C. При постоянно променящата се ситуация на киберзаплахи са необходими експерти по сигурността, които да изпълняват тази роля. Microsoft не позволява нарушаване на паролата на потребителя да създаде възможност за влизане в системата на клиента, а вместо това дава възможност на разработчиците да използват облачна услуга за идентификация, която непрекъснато се усъвършенства срещу нови заплахи.

2.2.3. Okta има визия да бъде платформа, която позволява на всяка компания да внедри всяка технология. Okta предоставя напълно мултитенант облачна услуга, което е едно от основните нововъведения, отличаващия е от другите конкуренти на решения за управление на идентичност и достъп и решения базирани на идентификация като услуга (Identity as a Service, IDaaS). Според Okta изборът на подходящ доставчик на решение за управление на идентичност и достъп на клиенти изисква в допълнение осигуряване на цялостно положително преживяване на клиента. Лекотата на използване за включване на нови потребители и самостоятелната регистрация са ключови фактори, които пряко влияят върху приемането на нови цифрови услуги и предложения, а оттам и върху произтичащите от това приходи. Затова от съществено значение са силни експертни познания в областта на технологиите и цялостно разбиране на преживяването на клиентите и основните процеси. В допълнение модерното управление на съгласия е необходимо за всеки успешен цифров бизнес. Okta предоставя услуги за директории, единично влизане, силно удостоверяване, работни процеси за осигуряване, управление на достъп до API, управление на достъп до сървъри и вградени отчети.

Работи в облак върху сигурна, надеждна и обстойно одитирана платформа и се интегрира с локални приложения, директории и системи за управление на идентичност.

2.2.4. Ping предлага решения за администриране и цялостна защита на потребителски данни и права на достъп за компании и организации от всички области на икономиката и публичната администрация. Опитът на компанията гарантира най-висока ефективност и е в основата на иновативни и устойчиви решения. Ping допълва собствените си методи с иновативни продукти от избрани технологични партньори като по този начин постига решаващи конкурентни предимства, реализира индивидуални решения и гарантира най-високо качество. Архитектурата на решенията е основната разлика между Ping и другите доставчици на решения за управление на идентичност и достъп на клиенти. Наследените архитектури имат тежки топологии на агентни сървъри, проектирани и разработени през миналия век и насочени към корпоративни еднодойменни уеб SSO изисквания. Решението на Ping Identity Platform е предназначено да възприеме текущите стандарти и да избегне обвързването с доставчик. Клиентите могат да опростят и да подобрят достъпа на потребителите до интегрираните уеб, мобилни и API услуги по сигурен начин, но на цена, която е по-малка от цената и сложността на алтернативните решения, включително възможността за вътрешна разработка.

2.3. Изводи към втора глава

Управлението на идентичност и достъп е адекватно покрито от надеждни решения, поддържани от реномирани доставчици, които инвестират в подобрения на предлаганите платформи и решения. Въз основа на направения анализ на три компании, предоставящи решения за управление на идентичност и достъп (SailPoint, Oracle Management Cloud и Omada) могат да бъдат обобщени критерии за избор на решение за управление на идентичност и достъп на клиенти:

- Решението за управление на идентичност и достъп на клиенти трябва да подкрепя дългосрочната визия на компанията. Работните процеси трябва да са достатъчно гъвкави, за да отговарят на настоящите и очакваните нужди.
- Решението за управление на идентичност и достъп на клиенти е елемент от цялостната технологична архитектура на компанията, което обуславя важността за управлението на идентичност и достъп на клиенти да бъде добре интегрирано в цялостната ИТ среда на компанията.
- Тъй като нуждите се променят с времето от основно значение е да се определи структурата за поддръжка на решението за управление на идентичност и достъп на клиенти от самото начало. Изборът между вътрешно разработени и управлявани от доставчика подобрения може да доведе до избор на различно решение.
- Спецификата на индустрията и географският контекст определят регулаторните, данъчните и правните съображения, които често са важни и не трябва да бъдат пренебрегвани при избор на решение за управление на идентичност и достъп на клиенти.
- Всички налични решения за управление на идентичност и достъп на клиенти в еднаква степен решават въпросите за сигурността на достъпа и най-вече за въвеждането на собствена идентичност. Но определянето на крайния потребител (B2B, B2C, B2B2C и т.н.) води до различни изисквания за взаимоотношения, които трябва да бъдат анализирани и обхванати при избор на решение за управление на идентичност и достъп на клиенти.
- Във всички случаи внедряването на платформа за управление на идентичност и достъп на клиенти трябва да предлага цялостно преживяване за клиента, да укрепва опита на потребителите в областта на сигурността и да допринася за ефективното намаляване на измами.

Направеният сравнителен анализ на решения за управление на идентичност и достъп на клиенти потвърждава, че съществуват множество надеждни и функционални решения. Очакваното развитие в близко бъдеще е свързано с изследвания върху критичните възможности за управлението на идентичност и достъп на клиенти в областта на метавселената и върху възможностите идентичностите да преминават от виртуалното към материалното пространство и обратно.

ГЛАВА 3. АТАКИ СРЕЩУ МНОГОФАКТОРНА АВТЕНТИКАЦИЯ

Трета глава от дисертационния труд има за цел да представи преглед на наличните инструменти за таксономия на атаки при многофакторна автентикация и да предложи теоретична рамка, подобряваща академичното разбиране за уязвимостите и потенциалните възможности за използване на механизмите за многофакторна автентикация като по този начин допринася за по-широкото познаване на предизвикателствата пред киберсигурността и намаляването на заплахите за сигурността при управление на идентичност и достъп.

3.1. Основни атаки на многофакторна автентикация

Няколко значими атаки на многофакторната автентикация в последните години свидетелстват за уязвимостта ѝ. През 2012 г. европейският банков сектор беше разтърсен от появата на Eurograbber, който от зловреден банков софтуер се разрасна до мобилен зловреден софтуер способен да открадне втория фактор на защита – доставените чрез SMS еднократни пароли, което позволи на нападателя да придобие контрол над двата фактора и да причини значителни финансови загуби и щети на репутацията. Подобна атака беше осъществена през 2017 г. срещу германски банкови институции, при която първият фактор за сигурността беше компрометиран със злонамерен софтуер, а вторият фактор с експлоатиране на пропуски в сигурността на система за мобилни съобщения и повиквания, чрез които нападателите променят информацията за маршрутизиране и пренасочват съобщенията за еднократни пароли. Ботове за прихващане на OTP, появили се през 2021 г. по същество автоматизират атаките за прихващане на еднократни пароли чрез компрометиране на идентификационни данни и подвеждане на жертвите да предоставят следващия фактор на сигурността. Хакерската група Lapsus$ извърши атака срещу Uber през 2022 г. се основава на затрупване на жертвата със съобщения за „push“ известия. През 2022 г. беше осъществена поредица атаки срещу персонала по поддръжка на компанията за сигурност на идентичността Okta за компрометиране на пароли и използване на пропуск в сигурността на Twilio като услуга за доставка на еднократни пароли чрез SMS, базирана на регистриране на всяка еднократна парола. Компрометирането на административни акаунти в Twilio осигурява достъп на нападателите до административните конзоли и съхранените еднократни пароли, с което и достъпа до двата фактора за потребителска автентикация. Версията на инструмента от вида adversary-in-the-middle Evilginx от 2023 позволява кражба на потребителски идентификатори, пароли, OTP и сесийни бисквитки.

3.2. Инструменти за таксономия на атаки към многофакторна автентикация

3.2.1. Data Breach Investigations Report (DBIR) е доклад на Verizon за разследване на нарушения на сигурността на данните през 2023 г., в който са посочени седем категории действия на заплаха или вектори на атака: социална, хакерска, злонамерен софтуер, злоупотреба, физическа, грешка и околна среда. Няколко атаки на многофакторна автентикация могат да се отнесат към тези категории.

3.2.1. MITRE ATT&CK предлага таксономия „Credential Access“, според която достъпът до удостоверителни данни включва 17 техники за кражба на идентификационни данни, като имена на акаунти и пароли, в това число Adversary-in-the-middle, Brute force, Credentials from Password stores, Forced Authentication, MFA Interception и други.

3.2.3. Хакерска многофакторна автентификация е таксономия, предложена от Роджър Граймс, съгласно която всичко започва от потребителя, тъй като потребителите също са компонент на инфраструктурата. Социално-инженерна атака може да компрометира потребителя и целия поток за многофакторна автентикация, в същото време устройствата и хардуерът също имат голямо значение при многофакторното удостоверяване като устройствата се разделят на три категории за удостоверяване: крайни, придружаващи и специализирани.

3.2.4. Алтернативи на скала на доверието: Горните три таксономични модела могат да се комбинират за да се създаде по-пълна картина за внедряване на многофакторното удостоверяване. Въвеждането на скала на доверието е добър инструмент за оценка на частта от модела, която ще се използва. В зависимост от критичността на приложението и необходимото ниво на доверие могат да се изберат различни методи за удостоверяване, като например: (1) Много ниско ниво на доверие: пароли; (2) Ниско ниво на доверие: настолни, гласови, SMS еднократни пароли (one-time password, OTP); (3) Средно ниво на доверие: мобилни еднократни пароли и пуш (push) известия; (4) Високо ниво на доверие: автентификатор на платформата FIDO2, ключ за сигурност и софтуерен роуминг; (5) Много високо ниво на доверие: хардуерен токен X.509.

Допълнителна възможност за повишаване нивото на сигурност е използване на конкретен метод за удостоверяване, който е с по-ниско ниво на сигурност и прилагане на допълнителни механизми за контрол, които да повишат сигурността. Например съвместното използване на съвпадение на номер и местоположение увеличава защитата срещу груба сила при атаки от типа „push-bombing“.

3.3. Бъдещо развитие

Исторически първият модел за достъп извършва удостоверяването преди началото на сесия: преглеждат се пълномощията и контекстуалната информация и се взема решение за оценка на риска. Въвеждането на поетапно удостоверяване с оценка на риска и потребителят в отделни моменти от сесията определя изискване за допълнително удостоверяване.

Преходът към непрекъснато адаптивно удостоверяване изисква оценяване на риска при всяка заявка и дори по време на една и съща сесия в това число с използване на пасивна поведенческа биометрия. За прилагане на надеждно управление на удостоверенията трябва да се приложи надеждна защита на всяко ниво: ако процесът на възстановяване на акаунти или записване на пълномощия е слаб, използването на силно пълномощно е без значение, тъй като нападателят ще премести атаката на друг етап.

Многофакторната автентикация използва допълнителен фактор за удостоверяване, но повечето организации не инвестират в осигуряване на множество фактори за удостоверяване за своите потребители, затова търсят алтернативи за доказване на самоличност или удостоверяване на автентичност с други средства. Най-популярният начин за удостоверяване на самоличност е ориентиран към използване на документи или проверка на самоличността от доставчик от трета страна. Разликата между удостоверяването на самоличността и проверката на самоличността е, че няма стъпка за обвързване на самоличността: налице е доказателство, че тази самоличност съществува, но не е задължително да се докаже, че тази самоличност се отнася за конкретно лице.

Когато всички други възможности за удостоверяване са изчерпани код за достъп може да гарантира достъп за ограничено време. Всички тези подходи обаче създават зависимост, каквато не би трябвало да има при многофакторното удостоверяване. Първоначалната формула „нещо, което знаете“, „нещо, което имате“ и „нещо, което сте“ гарантира, че факторите са напълно отделни и ако нападателят компрометира един от факторите, не може да компрометира цялата система. Но освен откриването и реагирането на компрометиране на всички фактори трябва да се осигури превенция или управление на сигурността на идентичността. При избора на инструмент трябва да бъдат изпълнени конкретни предварителни условия като например конфигурация на многофакторната автентикация, политики и обхват, както и интегриране с управлението на информация и събития в областта на сигурността.

3.4. Защита на отдалечен привилегирован достъп за външни потребители

Често нарушенията на сигурността на организациите се дължи не на лош подход към сигурността, а на хакерски атаки към доставчици на услуги, което води до нарушаване на сигурността на компаниите. Такива нарушения на сигурността от трети страни се увеличават: хакерите преследват лесни цели, а доставчиците са лесни мишени, тъй като организациите изразходват време, средства и ресурси за защита на привилегирования достъп на вътрешните потребители. Предизвикателство и проблем за сигурността на достъпа е третирането на външните потребители по същия начин като вътрешните потребители.

Няколко доставчици на услуги за управление на привилегирован достъп (Privileged Access Management, PAM) предлагат инструменти за управление на отдалечен привилегирован достъп (Remote Privileged Access Management, R-PAM) за защита на отдалечен привилегирован достъп за външни доставчици. Според прогнозни оценки до 2026 г. организациите, прилагащи инструменти за R-PAM, ще намалят излагането на риск с повече от 50%. Инструментите за управление на отдалечен привилегирован достъп са предназначени за преодоляване на предизвикателства за общ отдалечен достъп. Достъпни са онлайн и осигуряват лесен и сигурен метод за достъп за външни потребители като се предлагат в две алтернативи: add-on и самостоятелни приложения. Традиционните средства за управление на привилегировани акаунти и сесии (Privileged Account and Session Management, PASM) се справят с откриване на привилегировани акаунти, съхраняване на пароли, автоматично въвеждане на пълномощия, записване на сесии, управление на сесии и възможности „точно навреме“ (just-in-time) като осигуряват всички тези възможности за вътрешни потребители. Допълнителните средства RPAM влизат в действие с допълнителни възможности за достъп без VPN, силно удостоверяване и по-добро управление на идентичност за външни потребители. Комбинацията на PASM и RPAM позволява да бъдат решени проблемите с отдалечен привилегирован достъп за всички вътрешни и външни потребители.

3.5. Изводи към трета глава

Многофакторното удостоверяване е важна мярка за сигурност, но не е безотказна и може да бъде уязвима за различни видове атаки, за което свидетелстват множество значими атаки срещу многофакторното удостоверяване. Наличните инструменти за таксономия класифицират атаките срещу многофакторно удостоверяване според различни критериални характеристики. За защита от атаки срещу многофакторно удостоверяване могат да бъдат приложени различни стратегии, в това число надеждно управление на пълномощия, доказване на самоличност и използване на сигнали за риск и разпознаване. Защитата на отдалечения привилегирован достъп за външни потребители се превръща в критичен приоритет.

ГЛАВА 4. ГЕНЕРИТИВЕН ИЗКУСТВЕН ИНТЕЛЕКТ В УПРАВЛЕНИЕТО НА ИДЕНТИЧНОСТТА И ДОСТЪПА

През последните години появата на генеративния изкуствен интелект (GenAI) оказа значително влияние върху управлението на идентичността и достъпа. Генеративният изкуствен интелект демократизира използването на големи езикови модели като даде възможност за различни случаи на използване при управлението на идентичност и достъп – от адаптивен достъп до откриване и реагиране на заплахи за идентичността. Но от друга страна развитието на генеративния изкуствен интелект доведе до нови предизвикателства. Настоящата глава на дисертационния труд разглежда баланса между използването на изкуствен интелект за подобряване на управлението на идентичността и достъпа и преодоляването на свързаните с това рискове.

4.1. Генеративен ИИ

Подходите за машинно обучение са важна част от управлението на идентичност и достъп от много години. Развитието и постиженията на генеративния изкуствен интелект и демократизирането му дадоха възможност за широкото използване на големи езикови модели за различни случаи на употреба при управлението на идентичността и достъпа. Един от първите случаи на употреба на анализ с машинно обучение е адаптивния достъп, но днес много други случаи на употреба са свързани с управлението и администрирането на идентичност, които се различават по използването на изкуствен интелект.

4.2. Случаи на използване на генеративен изкуствен интелект при управление на идентичност и достъп

Анализът базиран на машинно обучение подпомага управлението на идентичността и достъпа с възможността да се настройва за конкретни случаи на употреба.

4.2.1. Заявките за достъп могат да използват усъвършенствани техники за клъстериране за групиране на правата в роли. Ако заявката е с достатъчно нисък риск, то достъпът може да бъде предоставен автоматично, ако е с по-висок риск се изисква да получи одобрение. По този начин автоматизираното предоставяне на достъп основано на риска спестява време както на потребителя, който бързо получава достъп, така и на оторизираните да предоставят достъп.

4.2.2. Поведенческа биометрия при управление на идентичност и достъп се базира на пасивни поведенчески биометрични данни, които разглеждат начина, по който потребителя взаимодейства с мишка или клавиатура на своето устройство и позволява да се определи дали потребителят е робот, друг човек, който наподобява обичайното поведение на потребител или измама с превземане на акаунт. Анализите базирани на машинно обучение позволяват да се гарантира, че потребителите са тези, за които се представят.

4.2.3. Управление на права за облачна инфраструктура: машинно обучение се използва проверяване и осигуряване на адекватни конфигурации за достъп за краен потребител или организация с много различни софтуерни разработки в облак и особено в мулти-облак с много изчислителни ресурси и ресурси за съхранение. Неподходящите конфигурации за достъп са един от основните източници на нарушения в облака. Някои доставчици разглеждат тази възможност за управление на правата за облачната инфраструктура като част от управлението на привилегирования достъп, но други като част от управлението и администрирането на идентичностите.

4.2.4. Откриване и реакция на заплахи за идентичността използва аналитични техники за защита на самите системи за идентичност. Анализи с машинно обучение се използват за откриване на аномалии. Източниците на данни за идентичност, които се използват за обучение на модели за машинно обучение произхождат от много инструменти за идентичност и обхващат както данни за самите идентичности, така и политики и роли, права или журнални файлове. Заплаха при използването на машинно обучение е инжектирането на вредни данни в моделите за машинно обучение поради което анализът на обучаващите данни за откриване на аномалии предотвратява заплахи за сигурността .

4.3. Тенденции в областта на машинното обучение, изкуствения интелект и генеративния изкуствен интелект

Съществуват няколко тенденции в прилагането на машинното обучение, изкуствения интелект и генеративните модели в системите за идентификация с изразена тенденция към федеративно използване, което превръща системите за идентификация в по-отзивчиви и адаптивни.

Три различни тенденции оказват влияние върху еволюцията на анализите базирани на машинно обучение и изкуствен интелект за управление на идентичността и достъпа и в системите за сигурност.

4.3.1. Управление на събития, свързани с информация за сигурността: Системите за управление на информационни събития в областта на сигурността събират логове с данни, които могат да бъдат анализирани. Анализът на поведението на потребителски единици позволява на тези системи да анализират лог-файлове с използване на машинно обучение.

4.3.2. Усъвършенстван анализ и откриване на измами се използва в банковата индустрия за предотвратяване на измами като се развива за да отговори на по-специфични случаи на употреба за управление на идентичност, например измами при създаване на нови банкови акаунти и измами с превземане на банкови акаунти.

4.3.3. Генеративен изкуствен интелект е сравнително нова тенденция на развитие на изкуствения интелект, която има голям потенциал за съвместно използване с други техники за управление на идентичността и достъпа. Използването на естествен език при генеративния изкуствен интелект позволява по-ефективно общуване с компютрите и дава възможност на системите за идентификация да подават сигнали и отговори по естествен за хората начин: изречения, параграфи и номерирани списъци със задачи. Съществено предимство, което стимулира използването на изкуствения интелект в областта на идентичността е възможността да се използват големи езикови модели за промяна на самите модели, така че моделите за случаи на употреба за управление на идентичност са съставни модели комбиниращи модели с машинно обучение или модели с генеративен изкуствен интелект и машинно обучение.

4.4. Доставчици на услуги и възможности за компаниите

Много доставчици използват анализ с машинно обучение и предоставят генеративни функции на изкуствен интелект за случаи на употреба при управление на идентичност и достъп. Агенти или копилоти на различни доставчици като Microsoft, Radiant Logic и Axiomatics предоставят специфични възможности за използване на генеративен изкуствен интелект за подпомагане на управлението на идентичността и достъпа.

Както анализите базирани на машинното обучение, така генеративният изкуствен интелект могат да подпомогнат процеса на автоматизация за управление на идентичност и достъп, но генеративният изкуствен интелект има предимства за потребителското изживяване, комуникацията и взаимодействието. И двата подхода са свързани със сложност при използването им и могат да бъдат чувствителни на обучение с некоректни или дефектни данни или неправилно проектирани модели, което изисква сериозна валидация и верификация на моделите.

Машинното обучение е жизненоважна част от архитектурните решения за проверка на идентичност и заемат важно място в съвременните системи за идентификация. Системите за идентичност се развиват така, че да подпомагат самоконфигурирането си.

Непрекъснатата оценка на риска е от решаващо значение за цялото управление на достъпа, особено за управление на отдалечен достъп. Управлението на риска от трети страни е ключова област с голяма важност за компаниите. Откриването на заплахи е свързано с отделяне на сигнала за опасност от налични шумове в средата, което изисква специално внимание към „чистота“ на идентичността: не трябва да има излишни права, не трябва да съществуват неизползвани акаунти, а политиките за достъп не трябва да предоставят възможност за заплахи за сигурността.

Друг критичен аспект в поддържането на системите за идентификация в компаниите е гарантиране на механизъм за откриване на заплахи с достатъчно фина настройка, така че да дава надеждни предупреждения и да минимизира фалшивите предупреждения. Съгласно последни проучвания 67% от компаниите вече са внедрили системи за откриване и реагиране на заплахи за идентичността (Identity Threat Detection and Response, ITDR) или са в процес на внедряване, което е значителна промяна през последните две години. Развитието им е в посока на предупреждения от приложения за възможност за неправомерно използване с автоматизиране на отговора на сигналите за сигурност и идентичност. До 2023 г. този процес не е автоматизиран, но очакванията са през 2025 г. голяма част от компаниите да използват автоматизирани системи за откриване и реагиране на заплахи за идентичността с използване на машинно обучение, генеративен изкуствен интелект и големи езикови модели, които позволяват бързо приоритизиране, обработване и действие при сигнали от системите за сигурност.

4.5. Бъдещи перспективи на изкуствения интелект в управлението на идентичността

Заплахите за сигурността на идентичността трябва да се преодоляват с модел за сигурност ориентиран към идентичността. Подходящото използване на изкуствен интелект с подходящи защитни средства и под надзора на хора и машини подпомага откриване на заплахи, приоритизиране и реагиране за да помогнат за по-бързото развитие спрямо развитието на нарушителите.

Понастоящем управлението на идентичността и достъпа е сложна и бързо променяща се област с много среди, права и субекти. Идентифицирането на всички тези субекти и управлението на техния достъп е предизвикателство за хората. Въпреки автоматизацията на инструментите за управление на идентичност и достъп, все още голяма част от тази автоматизация зависи от хората.

Интелигентната автоматизация позволява да се намали степента на сложност при управлението на идентичност и достъп. Системите и потребителите трябва да изпълняват повечето от задачите с помощта на интелигентни междинни агенти. Генеративен изкуствен интелект дава възможност за нови по-ефективни атаки срещу системите за управление на идентичност и достъп.

Но от друга страна това е предпоставка за фалшиви самоличности и фалшиви данни, които могат да предизвикат хаос в системата за управление на идентичност като увреждат основата на доверието, върху която се изгражда контрола на управлението на идентичността и достъпа.

При използване на генеративен изкуствен интелект за контрол на управление на идентичност и достъп моделите се обучават на базата на данни за компанията и контекста на компанията. Това позволява моделите да се прецизират с данни свързани с управлението на идентичността и достъпа и да се дообучат за контекста на компанията, например организационна структура, оперативен модел, правила и разпоредби, политики и процедури. Генеративните модели използват допълнителните данни и ги сравняват и противопоставят на политиките и процедурите за да се идентифицират областите, в които има пропуски. В допълнение моделите могат да се прецизират с данни за бизнес процесите и приложенията, които автоматизират тези бизнес процеси в компаниите.

4.6. Изводи към четвърта глава

Интегрирането на генеративния изкуствен интелект в управлението на идентичност и достъп предоставя както значителни възможности, така и важни предизвикателства. От една страна генеративният изкуствен интелект демократизира използването на големи езикови модели, което дава възможност за различни случаи на използване при управлението на идентичност и достъп като например адаптивен достъп и откриване на заплахи за идентичността. Тази технология може да повиши сигурността и оперативната използваемост чрез автоматизиране на процесите и осигуряване на по-ефективен потребителски опит. От друга страна се въвеждат и нови рискове като например създаване на дълбоки фалшификати и сложни фишинг атаки. За да се справят с тези предизвикателства организациите трябва внимателно да избират доставчици, да поддържат езикови модели и да гарантират неприкосновеността на личните данни. Бъдещето на управлението на идентичност и достъп е в интелигентната автоматизация, при която инструментите управлявани от изкуствен интелект могат да се самоконфигурират и адаптират към променящите се заплахи. Непрекъснатото обучение и адаптиране са от решаващо значение за успешното използване на възможностите на изкуствения интелект при управлението на идентичност и достъп.

ГЛАВА 5. ДЕЦЕНТРАЛИЗИРАНА ИДЕНТИЧНОСТ И ПРОВЕРИМИ УДОСТОВЕРЕНИЯ

Традиционните централизирани платформи за идентификация, макар и ефективни, показват ограничения по отношение на сигурността, неприкосновеността на личните данни и контрола на потребителите. Настоящата глава на дисертационния труд е посветена на изследване на потенциала на децентрализираната идентичност и проверимите удостоверения за управление на цифровата идентичност.

5.1. Анализ на децентрализираната идентичност и проверимите удостоверения

5.1.1. Модели за цифрова идентичност: Цифровата идентичност се развива чрез няколко модела: централизирана идентичност, федеративна идентичност, идентичност ориентирана към потребителя, суверенна идентичност. Основният недостатък на централизираната идентичност, управлявана от централен орган и използваща за идентификация на потребителите потребителски имена и пароли е наличието на единствена точка на отказ и несигурност на личните данни.

Федеративната идентичност позволява на потребителите да използват една и съща идентичност в множество приложения, което намалява необходимостта от множество акаунти, но запазва използването на централизирани доставчици на идентичност и свързаните с това предизвикателства за поверителността. Моделът базиран на идентичност ориентирана към потребителя предоставя по-голям контрол върху личните данни като позволява управление на идентичността без наличие на централизирана федеративност. Например OpenID и OAuth дават възможност на потребителите да контролират своите данни чрез различни удостоверения и сертификати. Суверенната идентичност (Self-Sovereign Identity, SSI) е най-новият модел в развитието на цифровата идентичност, който предоставя пълен контрол на потребителите върху тяхната идентичност като използва децентрализирани технологии като блокчейн, децентрализирани идентификатори (Decentralized Identifiers, DID) и проверими удостоверения (Verifiable Credentials, VC) и напълно елиминира необходимостта от централни органи като гарантира, че данните са криптографски защитени и проверими.

5.1.2. Абстрактен модел за цифрови идентичности е надежден модел за абстракция, в това число абстракция на акаунти или абстракция на идентичности. Организации, които използват абстрактен модел за цифрова идентичност поддържат централизирана платформа за идентичност и имат контрол върху идентичността, което води контрол и притежаване на данните, свързани с тази идентичност.

5.1.3. Децентрализираната идентичност и проверимите удостоверенията предлагат алтернативен модел за цифрова идентичност като прехвърлят контрола върху субектите, с което се трансформира архитектурата на бизнес отношенията от организационен към ориентиран към субектите подход. Децентрализираната идентичност позволява на потребителя да свърже свой портфейл за идентичност с конкретни услуги и да инжектира необходимите данни за да извърши транзакция. Работният процес за създаване и проверка на децентрализирани идентификатори и проверими удостоверения включва три основни участника: издател, който създава DID, актуализира документа DID, събира и проверява DID на получателя, издава VC и го отменя; получател, който създава DID, споделя го с издателя, получава VC, създава проверимо представяне (Verifiable Presentation, VP) и споделя VP с проверяващия орган; проверител, които получава VP, разрешава DID на издателя и получателя, проверява техните подписи, проверява състоянието на отмяна и проверява самоличността на издателя и получателя.

5.1.4. Неутралност и контролируемост. Преминаването към модел, ориентиран към субекта изисква привеждане на цифровата идентичност в съответствие с принципите за неутралност и контролируемост. Неутралността предполага независимост, сигурност, всеобхватност, прозрачност и оперативна съвместимост. Контролируемостта осигурява достъп и неприкосновеност на личните данни, сигурност, устойчивост, постоянство и преносимост. Критичен компонент за осигуряване на принципите за неутралност и контролируемост е независима и обща доверителна инфраструктура.

5.1.5. Портфейлите за идентичност осигуряват създаване идентификатори и съхраняване на частни ключове и всички други удостоверителни или криптографски данни, които могат да бъдат проверени. Понякога портфейлите за идентичност се разглеждат само като начин за удостоверяване или оторизация като част от услугите, но могат да се използват не само за основните функции за идентичност, а като преход към извършването на много повече услуги от гледна точка на бизнеса като плащания, управление на собственост и цифрови подписи.

5.1.6. Протоколите осигуряват свързването на регистрацията, сертифицирането, съхранението на цифровата идентичност като осигуряват стандартизация, така че проверимите удостоверения да работят със съществуващата инфраструктура за управление на идентичност и достъп.

5.2. Текущо състояние

Децентрализацията се развива постепенно като започва с портфейл за идентификация и набор от протоколи за контрол, които да направят този портфейл функционален. Следващата стъпка е децентрализирането на доверителната инфраструктурата. Създадената през 2022 г. Фондацията за отворени портфейли, която е част от Фондацията на Linux развива инициатива за стандартизиране на портфейли за идентичност.

Редица организации обединяват усилията си за управление на корпоративен блокчейн. Например в Канада седемте най-големи финансови институции създават блокчейн среда за цялата страна, която да действа като доверителна инфраструктура. Анонимността на блокчейн не само означава, че няма централен орган, който да блокира даден акаунт в случай на кражба на самоличност или неправомерно поведение, но и че всеки потребител трябва да се предпази от забравяне (или загуба) на частния ключ. На практика блокчейн може да доведе до нови проблеми за потребителите, тъй като всеки потребител самостоятелно управлява криптографските данни за защита на идентичността му.

5.3. Бъдещо развитие

Въвеждането на стандарти за оперативна съвместимост между всички доверителни инфраструктури става ключов аспект на децентрализираната идентичност. Потребителят трябва да има универсален профил, който да позволява навигиране между различните екосистеми. Екосистемите се формират около определена доверителна рамка, която обединява различни страни, като например издатели, притежатели, проверители, органи за гарантиране, разработчици, оператори или одитори и определя състоянието на доверителната инфраструктура като централизирана, споделена или публична. Децентрализираната идентичност може да бъде полезна в много различни случаи на употреба, а не само за управление на идентичност и достъп на клиенти и може да се приложи за плащания, управление на активи, управление на собственост и други. Проверимите идентификатори на юридически лица са от съществено значение за децентрализираната идентичност на даден стопански субект и за осигуряване на възможност на този юридически субект да извършва транзакции с други субекти чрез притежавания от него портфейл. Наличието на универсален портфейл не е единственият начин за прилагане на децентрализирана идентичност и проверими удостоверения: все повече вертикални приложения вграждат децентрализираната идентичност. Въпреки развитието на стандартизацията на децентрализираните идентичности и проверимите удостоверения се въвеждат алтернативни решения от производители на мобилни устройства със собствени портфейли, които използват предимството на вече изградената екосистема.

5.4. Изводи към пета глава

Преходът към децентрализирана идентичност и проверими удостоверения представлява значителен напредък в управлението на цифровата идентичност. Преминаването от централизиран към ориентиран към субекта модел повишава сигурността, неприкосновеността на личните данни и контрола на потребителите като се съгласува по-добре с цифровизацията и намалява затрудненията в бизнес процесите. Децентрализираната идентичност действа като надежден конектор между данните и услугите като позволява на потребителите да управляват своите данни и да извършват транзакции без услугите да съхраняват данни. Проверимите удостоверения гарантират, че издателите на данни могат да издават криптографски подписана информация на притежателите на данни, които могат да я представят на проверителите на данни за независимо потвърждаване. Този модел е съобразен с разпоредбите за защита на личните данни и подобрява сигурността.

Успехът на екосистемата зависи от неутралността, възможността за контрол и оперативната съвместимост като портфейлите за идентификация играят ключова роля в управлението на идентификаторите и проверимите пълномощия. Стандартизираните протоколи и общата доверителна инфраструктура са от съществено значение за осигуряване на оперативна съвместимост и осигуряване на възможност на потребителите да навигират в различни екосистеми с универсален профил. Съществуващите случаи на употреба като например плащания и управление на активи демонстрират практическите приложения на децентрализираната идентичност. Използването на децентрализирана идентичност и проверими пълномощия стимулира иновациите и подобрява управлението на цифровата идентичност.

ГЛАВА 6. МЕТОДОЛОГИЯ ЗА ОПТИМИЗИРАНЕ НА СЕРТИФИЦИРАНЕТО ЗА УПРАВЛЕНИЕ И АДМИНИСТРИРАНЕ НА ИДЕНТИЧНОСТ

Настоящата глава на дисертационния труд изследва традиционния подход към сертифицирането на достъпа, който повечето организации използват днес, неговите основни проблеми и предизвикателства и представя методология за оптимизирането му, която включва три последователни етапа: (1) анализ на идентичността; (2) кампании за сертифициране; (3) комуникация и обучение.

6.1. Анализ на идентичността

Използването на анализ на идентичността осигурява допълнителен контекст за проверяващите. Анализът на идентичността обработва данни от различни източници за генериране на полезна информация, която да се използва от проверяващите. Анализът на идентичността включва адаптиран отговор с изкуствен интелект за допълване на човешката интелигентност с машинна интелигентност, сертифициране ориентирано към риск с динамично изчисляване на рискови оценки, почистване на непознати акаунти и неизползвани права, анализи на поведение за задействане на предупреждение при странно поведение, което не съответства на обичайното.

6.2. Кампании за сертифициране

Съществуват няколко вида кампании за сертифициране, които могат да се провеждат за ефективно намаляване на риска:

6.2.1.Сертифициране основано на честота: извършва се същото сертифициране на база честота, но с няколко нива, в зависимост от хората, които имат повече познания за своя достъп.

6.2.2. Непрекъснато микро-сертифициране: целенасочено сертифициране, което не се отнася за всички потребители, а силно фокусирано върху отделни потребители и използва два вида микро-сертификати: базирани на конкретни събития или базирани на риск.

6.2.3. Определяне на оптимален обхват и обем: управление на баланса между минимизиране на сертифициране базирано на честота и допълване с автоматизирано сертифициране и микро-сертифициране, т.е. намаляване на броя на елементите за достъп, които трябва да бъдат сертифицирани като същевременно се разшири обхвата на това, което трябва да бъде сертифицирано.

6.3. Комуникация и обучение

Добри практики за подобряване на комуникацията и обучението при сертифициране включват: (i) усъвършенстване на шаблоните за имейли; (ii) подобряване на преговорите с одиторите; (iii) повишаване на отговорността на проверяващите; (iv) овластяване на помощния отдел.

6.4. Изводи към шеста глава

Традиционният подход за сертифициране на достъпа в организациите е свързан с редица проблеми и предизвикателства. Повечето организации са ориентирани към спазване на изискванията, при който одиторите определят какво трябва да се сертифицира и колко често. Този подход често води до умора от сертифицирането сред мениджърите и проверяващите, които в крайна сметка одобряват достъп без задълбочен преглед поради липса на контекст и мотивация.

За да се оптимизира сертифицирането на достъпа се предлага използването на анализ на идентичността за предоставяне на допълнителен контекст на проверяващите, преминаване от сертифициране, основано на съответствието, към сертифициране, основано на риска, и изчистване на неправомерни или осиротели акаунти. Анализът на идентичността може да помогне за генериране на полезна информация, изчисляване на динамични оценки на риска и автоматизиране на някои процеси на сертифициране като по този начин се намали умората от сертифицирането и подобри вземането на решения за сигурността.

Като втора стъпка се предлагат ефективни кампании за сертифициране. Такива кампании включват сертифициране на базата на честота с нива, непрекъснато микро-сертифициране въз основа на конкретни събития или рискове, както и определяне на оптимален обхват и обем на сертифицирането.

Последният етап от предложената методология за оптимизиране на сертифицирането за управление и администриране на идентичност е свързана със значението на комуникацията и обучението за подобряване на процесите на сертифициране на достъпа. В нея се предлага усъвършенстване на шаблоните на имейли, подобряване на преговорите с одиторите, повишаване на отчетността на проверяващите и предоставяне на необходимата информация и ресурси на помощния отдел. Тези нетехнически, но практични добри практики имат за цел да повишат цялостната ефективност на сертифицирането на достъпа в организациите.

ЗАКЛЮЧЕНИЕ

Дисертационният труд разглежда многостранната област на управлението на идентичност и достъп в многокорпоративни среди като подчертава критичната роля, която то играе в цифровата трансформация на големите организации. Изследването представя сложността и предизвикателствата, свързани с управлението на идентичност и достъп, особено в контекста на хибридната работна среда и нарастващата зависимост от облачни приложения. На базата на направените анализи се подчертава необходимостта от съвременни решения за управление на идентичност и достъп, които не само повишават сигурността, но и подпомагат гъвкавостта и ефективността на бизнеса.

Основните рискови фактори и предизвикателства при управлението на идентичност и достъп са определени на базата на цялостен преглед и анализ на текущото състояние на областта. Бързата цифрова трансформация и възприемането на хибридни модели на работа значително усложняват процесите на управлението на идентичност и достъп, което налага стратегически подход към управлението на идентичността. Авторско проучване чрез анкетиране на големи корпорации допълнително потвърди тези констатации, разкривайки широко разпространената нужда от подобрени решения за управление на идентичност и достъп.

Анализът на водещите доставчици на технологии в областта на управлението на идентичност и достъп и управлението на идентичността и достъпа на клиенти като SailPoint, Oracle Management Cloud и Microsoft подчертава разнообразната гама от налични решения и важността на избора на правилен доставчик, който да отговаря на специфичните организационни нужди. Развитието на пазар на решения за управление на идентичност и достъп е стимулирано от нарастващото признаване на важността на сигурност на идентичността.

Изследването на атаките за многофакторна автентикация представя различните видове атаки и наличните таксономични инструменти за тяхното класифициране и разбиране. Значението на надеждните решения за многофакторна автентикация е от съществена важност за намаляване на рисковете за сигурността и за защита на чувствителната информация. Анализът на бъдещите тенденции подчертават необходимостта от непрекъснато развитие и адаптиране на стратегиите за управление на идентичност и достъп за да се отговори на нововъзникващите заплахи.

В дисертационния труд е анализиран потенциала на изкуствения интелект за усъвършенстване на процесите на управление на идентичност и достъп чрез автоматизация и анализ базиран на машинно обучение и генеративния изкуствен интелект, като са изведени основните свързани с това предизвикателства и рискове и необходимостта от балансиран подход при използването на изкуствен интелект при управление на идентичност и достъп.

Трансформационният потенциал на децентрализираната идентичност и проверимите удостоверения са обстойно анализирани като са изведени предимствата на решения за децентрализирана идентичност при осигуряването на сигурно и мащабируемо управление на идентичността. Предложено е разглеждането на цифровите идентичности като надежден абстрактен модел за свързване на субекти и управление на взаимоотношения, както и нововъзникващите концепции за децентрализирани идентификатори и проверими удостоверения и тяхното приложение за управление на идентичност и достъп.

Предложена е методология за оптимизиране на сертифицирането на достъпа за управление и администриране на идентичност, която има за цел да рационализира процеса на сертифициране, да подобри видимостта и да повиши цялостната ефективност на решенията за управление на идентичност и достъп с подчертаване на значението на непрекъснатия мониторинг и одит за осигуряване на съответствие и намаляване на рисковете.

Цялостният анализ на управлението на идентичност и достъп в многокорпоративни среди и основните предизвикателства, тенденции и решения представени в изследването показват критичната роля на управление на идентичност и достъп в подкрепа на цифровата трансформация и гарантирането на сигурността на организационните активи., Представените изводи и препоръки за организациите, които се стремят да подобрят своите стратегии за управление на идентичност и достъп са предпоставка за постигане на сигурна и ефективна рамка за управление на идентичността в многокорпоративна среда. Предложените методология и добри практики могат да послужат като пътна карта за организациите, които искат да модернизират своите решения за управление на идентичност и достъп и да се справят с непрекъснато променящата се обстановка за сигурност.

НАУЧНО-ПРИЛОЖНИ И ПРИЛОЖНИ ПРИНОСИ

Научни приноси:

- Предложена е методология за сертифициране на управлението и администрирането на идентичности, която оптимизира сертифицирането на достъпа при администриране на идентичности като свързва теоретичните рамки със стратегиите за практическо имплементиране, подобрява видимостта и рационализира процеса на сертифициране като осигурява систематичен подход за практическо прилагане;
- Предложена е нова рамка за сигурно и мащабируемо управление на идентичност основана на децентрализирани модели на идентичност и парадигми за управление на идентичността ориентирани към доверието, включително децентрализирани идентификатори и проверими удостоверения;

Научно-приложни приноси:

- Предложена е класификация на многофакторна автентификация, която определя структурирана таксономия на различни видове атаки при многофакторна автентификация и предлага теоретична рамка, подобряваща академичното разбиране за уязвимостите и потенциалните експлойти на механизмите за многофакторна автентификация и по този начин допринася за по-широко познаване на предизвикателствата пред киберсигурността и намаляването на заплахите за сигурността в управлението на идентичността и достъпа;
- Предложени са стратегии за интегриране на изкуствен интелект (ИИ) в различни рамки за управление на идентичност и достъп, които позволяват намаляване на риска при управлението на идентичността и достъпа като се отчитат мащабируемостта, автоматизацията и непрекъснатото адаптиране към нововъзникващи заплахи;

Приложни приноси:

- Направен е обстоен анализ на водещите доставчици на технологии за управление на идентичността и достъпа и за управление на идентичността и достъпа на клиентите, който предлага научно обоснован подход за организациите при избор на решения, съответстващи на техните специфични нужди и организационни цели.

СПИСЪК НА ПУБЛИКАЦИИТЕ ПО ДИСЕРТАЦИОННИЯ ТРУД

1. **Liveretos, A.**, Draganov, I. (2022) *Customer Identity and Access Management (CIAM): An Overview of the Main Technology Vendors*. International Journal of Economics and Management Systems, Vol. 7, pp. 464–475, ISSN: 2367-8925, https://www.iaras.org/home/caijems/customer-identity-and-access-management-ciam-an-overview-of-the-main-technology-vendors

2. **Liveretos, A.**, Draganov, I. (2022) *Identity & Access Management (IAM) and Customer IAM (CIAM): A Pulse Survey of Several Global Corporations Over Their Current Usage and Exploitation of Automated IAM and CIAM Solutions*. International Journal of Computers, Vol. 7, pp. 95–103, ISSN: 2367-8895, https://www.iaras.org/home/cijc/identity-access-management-iam-and-customer-iam-ciam-a-pulse-survey-of-several-global-corporations-over-their-current-usage-and-exploitation-of-automated-iam-and-ciam-solutions

3. **Liveretos, A.**, Lazarova, M. (2024) *Generative Artificial Intelligence and Machine Learning for Identity and Access Management*. Proceedings of the Technical University of Sofia, ISSN: 2738–8549, 2738–8530, Vol. 74, No. 3, https://doi.org/10.47978/TUS.2024.74.03.019

4. **Liveretos, A.**, Lazarova, M. (2024) *Attacks Against Multi-Factor Authentication*. International Journal of Advances in Computer Science and Technology, Vol. 13, No. 10, pp. 118–122, ISSN: 2320–2602, https://doi.org/10.30534/ijacst/2024/0113102024

5. **Liveretos, A.**, Lazarova, M. (2024) *Decentralized Identity and Verifiable Credentials – Trends and Advancement*. Proc. of 32nd IEEE National Conference with International Participation TELECOM'2024, 21–22 November 2024, Sofia, Bulgaria, https://doi.org/10.1109/TELECOM63374.2024.10812293 (индексирана в Scopus)

SUMMARY

IDENTITY AND ACCESS MANAGEMENT IN A MULTICORPORATE ENVIRONMENT

Anastasios Liveretos

The thesis explores the multifaceted domain of Identity and Access Management (IAM) within multicorporate environments, emphasizing the critical role it plays in the digital transformation of large organizations. The research has highlighted the complexities and challenges associated with IAM particularly in the context of a hybrid workforce and the increasing reliance on cloud-based applications. The findings underscore the necessity for modern solutions for identity and access management that not only enhance security but also support business agility and efficiency.

The comprehensive overview of the current state of IAM identified the key risk factors and challenges. The rapid digital transformation and the adoption of hybrid work models have significantly complicated the processes, necessitating a strategic approach to identity governance. The survey conducted among large corporations further validated these findings, revealing a widespread need for improved IAM solutions. The analysis of leading technology vendors in the IAM and Customer Identity and Access Management (CIAM) space such as SailPoint, Oracle Management Cloud, and Microsoft highlighted the diverse range of solutions available and the importance of selecting the right vendor to meet specific organizational needs. The growing market for IAM solutions is driven by the increasing recognition of identity security's value. The exploration of multi-factor authentication (MFA) attacks provides valuable insights into the various types of attacks and the taxonomy tools available to classify and understand them and underscores the importance of robust MFA solutions in mitigating security risks and protecting sensitive information. The future considerations discussed also emphasize the need for continuous evolution and adaptation of IAM strategies to address emerging threats. The potential of Artificial Intelligence (AI) to enhance IAM processes through automation, analytics, and machine learning is thoroughly examined also addressing the associated risks and the need for a balanced approach to leveraging AI in IAM. The transformative potential of decentralized identity and verifiable credentials is explored highlighting the benefits of decentralized identity solutions in providing secure and scalable identity management. The emphasis on digital identities as a trusted abstraction model for connecting entities and managing relationships is particularly noteworthy as well as the emerging concepts of decentralized identifiers (DIDs) and verifiable credentials (VCs) and their implications for IAM. A methodology for optimizing Identity Governance and Administration (IGA) access certification is proposed that aims to streamline the certification process, improve visibility, and enhance the overall efficiency of IAM solutions emphasizing the importance of continuous monitoring and auditing to ensure compliance and mitigate risks.

The thesis provides a comprehensive analysis of IAM in multicorporate environments, addressing the key challenges, trends, and solutions. The research demonstrates the critical role of IAM in supporting digital transformation and ensuring the security of organizational assets. The findings and recommendations presented offer valuable insights for organizations seeking to enhance their IAM strategies and achieve a secure and efficient identity management framework. The contributions offer practical guidance for IAM practitioners and decision-makers. The proposed methodologies and best practices can serve as a roadmap for organizations looking to modernize their IAM solutions and address the evolving security landscape.