ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи
на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Бєлих Р.К.
(прізвище та ініціали)
Керівник Чумак Н.С.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПЗ – програмне забезпечення

ПК – персональний комп’ютер

AD – Active Directory

APIs – Application Programming Interfaces

IAM – Identity and Access Management

IDS – Intrusion Detection System

IoT – Internet of Things

IP – Internet Protocol

IPsec – IP security

LDAP – Lightweight Directory Access Protocol

MFA – Multi-Factor Authentication

OTP – One Time Password

RADIUS – Remote Authentication in Dial-In User Service

SaaS – Software as a Service

SAML – Security Assertion Markup Language

SSO – Single Sign-On

VPN – Virtual Private Networks

ВСТУП

Актуальність дослідження. Призначення систем управління ідентифікацією та доступом користувачів до інформаційних систем – дозвіл або блокування доступу до захищених даних і додатків. Більш складні рішення IAM дозволяють підприємствам ще більш деталізовано призначати дозволи. Наприклад, можна задавати час доби, коли конкретний користувач має право взаємодіяти з сервісом, і місце, з якого може здійснюватися доступ.

Системи IAM допомагають організаціям привести безпеку і конфіденційність даних у відповідність до нормативних вимог. Підприємства можуть використовувати методи IAM, такі як єдиний вхід (SSO), багатофакторна автентифікація (MFA), управління доступом на основі ролей (RBAC) і «правило найменших привілеїв» (надання користувачам та об'єктам, таким як програмні додатки, мінімального обсягу доступу, необхідного для виконання завдання), щоб відповідати вимогам регуляторів.

За допомогою таких заходів безпеки, як SSO, MFA або RBAC, організації можуть підвищити безпеку, а також знизити бар'єри, що заважають співробітникам ефективно працювати. Співробітники отримують швидкий доступ до ресурсів, які їм необхідні для виконання своєї роботи, де б вони не знаходилися. З IAM співробітники можуть відчувати себе більш впевнено, працюючи в безпечному середовищі.

Система IAM, яка забезпечує автоматичну підготовку робочих місць користувачів, також спрощує для співробітників процедуру запиту і отримання авторизованого доступу до різних ресурсів, коли це необхідно, що знижує навантаження на IT-середовище і складність взаємодії з нею, а також підвищує продуктивність персоналу.

Опитування Forrester, проведене в серпні 2020 року, показало, що 53% працівників інформаційних служб зберігають свої паролі ненадійно. Ще одне опитування споживачів у США, проведене компанією Transmit Security у березні

2023 року, показало, що більше половини з них перестали користуватися веб-сайтом, оскільки процес їх входу був занадто складним [12].

Сучасні системи IAM виходять за рамки захисту користувачів, включаючи автентифікацію нелюдських сутностей, таких як ключі додатків, API та секрети, агенти та контейнери.

Вищесказане визначає актуальність теми даної бакалаврської роботи, основний зміст якої становлять дослідження методів та засобів управління ідентифікацією та доступом користувачів до інформаційних систем підприємства.

Об'єкт дослідження – управління ідентифікацією та доступом до інформаційної системи підприємства.

Предмет дослідження – методи та засоби управління ідентифікацією та доступом до інформаційної системи підприємства.

Мета роботи – розробити рекомендації щодо застосування методів та засобів управління ідентифікацією та доступом до інформаційної системи підприємства.

Наукові завдання:

проаналізувати існуючі загрози безпечному доступу користувачів до корпоративних даних;

визначити зміст проблеми управління ідентифікацією та доступом до інформаційної системи підприємства;

дослідити існуючі методи та засоби управління ідентифікацією та доступом до інформаційної системи підприємства;

розробити рекомендації щодо управління ідентифікацією та доступом до інформаційної системи підприємства.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів полягає в розробці рекомендацій щодо застосування методів та засобів управління ідентифікацією та доступом до інформаційної системи підприємства.

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

1.1. Аналіз загроз безпечному доступу користувачів до корпоративних даних

Більше 80% порушень безпеки є результатом «використання вкрадених облікових даних» або застосування методу грубої сили. Password Dumper – це найбільш поширений варіант шкідливого ПЗ, що спеціалізується на крадіжці облікових даних. 44 мільйони облікових записів залишилися вразливими через злом облікових записів або крадіжки облікових даних [11].

Пандемія COVID-19 зумовила широке застосування віддаленої роботи працівників організацій та підприємств. При цьому на перший план вийшло забезпечення правильного рівня доступу потрібних людей до потрібних ресурсів в потрібному контексті. Ця тенденція буде зберігатися ще довгий час після закінчення кризи. Зазначається, що треба змінити традиційний погляд на безпеку, орієнтований на периметр мережі, на мислення, орієнтоване на ідентифікацію, яке забезпечує безпечний доступ для різних типів користувачів незалежно від їх місця розташування, пристрою або мережі [10].

Стек технологій нульової довіри розширюється, але остаточного рішення немає. Проте, далекоглядні компанії використовують системи управління ідентифікацією та доступом (Identity and access management, IAM) для підключення і оптимізації захисту у своїй архітектурі наскрізної безпеки. Наприклад, 76% організацій за межами Північної Америки планують інвестувати в системи управління інформацією і подіями безпеки (SIEM) протягом наступних 12-18 місяців. У Північній Америці найбільш запланованої інтеграцією IAM є оркестровка і автоматизація [10].

У [10] зазначається, що 90% постачальників медичних послуг вже впроваджують систему єдиного входу для співробітників, а більше 40% планують впровадити систему єдиного входу для зовнішніх користувачів в наступному році.

індустрія. Цікаво, що володіння технологіями IAM повністю знаходиться в руках груп безпеки в 40% цих організацій (більш ніж в два рази більше, ніж в будь-якій іншій галузі).

Рішення з управління ідентифікацією та доступом надають фахівцям з безпеки методи, процеси і технології для управління ідентифікаційними даними і правами користувачів, послуг і речей. Ці програми також охоплюють відносини і довіру між цими людьми, послугами та речами. У сучасних складних і розподілених IT-середовищах сучасні програми IAM повинні робити набагато більше, ніж просто надавати ідентифікаційні дані користувачам і надавати доступ. Програми IAM лежать в основі досягнення критичних бізнес-цілей і актуальні для кожної високоефективної організації. В результаті деякі ініціативи в галузі IT або безпеки вимагають такого ретельного обговорення і вивчення IAM [1].

Сучасне рішення IAM виходить за рамки встановленого інструментарію і фокусується на результатах і усуненні технічного боргу або важких налаштувань, які заважають організації розгортати в масштабі. Сучасні програми IAM зміщують акцент з тактичних або ручних операцій на більш стратегічну функцію, оптимізовану для цілей бізнесу. Крім того, відмінні риси IAM можуть допомогти знизити ризик витоку даних, пов'язаних з ідентифікаційними даними та обліковими даними [1].

Ці програми можуть допомогти підвищити продуктивність і спільну роботу, забезпечуючи конкурентну перевагу на ринку. Нарешті, сучасна програма може допомогти забезпечити більш систематичне здійснення і підтримання нормативно-правової відповідності, знижуючи при цьому витрати на виправлення результатів аудиту, пов'язаних з IAM. Багато підприємств, які прагнуть до цифрової трансформації, вважають, що програми IAM є ключем до цієї ініціативи змін. Стратегії оптимізації цифрової трансформації включають модернізацію інструментів на робочому місці, міграцію в хмару, інтеграцію програмного забезпечення як послуги (SaaS) і локальних додатків, ініціативи по роботі з дому і розширення каналів взаємодії з клієнтами. Ці імперативи можуть забезпечити визнану цінність для бізнесу і конкурентну перевагу [1].

В [1] зазначається, що багато організацій не можуть досягти своїх цілей через фрагментовані, застійні та неповні програм IAM, які з часом розроблялися з використанням монолітних точкових технологічних рішень. В результаті підприємства стикаються зі значними ризиками невдач і можуть втратити конкурентну перевагу гнучкої підключеної робочої сили [1].

Недоліки традиційних рішень IAM [1]:

підвищена складність. Компанії зазвичай додають більше додатків, інформації, методів доступу і користувальницьких прав у міру необхідності;

висока увага до користувача. Підвищення очікувань щодо захисту інформації, що дозволяє встановити особу (Personally Identifiable Information, PII), і забезпечення безперебійної взаємодії з користувачем;

додаткові правила. Нові стандарти, необхідні для доступу та спільного використання PII і конфіденційної інформації;

більше інструментів безпеки. В середньому організації використовують від 25 до 49 різних інструментів безпеки від 10 різних постачальників;

Усвідомлений підхід до модернізації існуючої програми IAM може привести до переваг, які безпосередньо покращують продуктивність бізнесу і стан безпеки, наприклад такі результати [1]:

зниження витрат за рахунок автоматизації;

забезпечення операційної ефективності для людей і систем за рахунок інтегрованої технологічної структури;

допомога в підтримці більш успішних впроваджень за рахунок правильного планування;

поліпшення аналізу ризиків;

зниження витрат на дотримання вимог;

підвищення якості обслуговування клієнтів і співробітників.

Рішення IAM, яке оптимізоване для задоволення потреб і унікальних умов організації, допомагає розширити можливості управління дотриманням нормативних вимог, надати зручний доступ авторизованим користувачам і

захистити цінні дані. Але без використання сучасної структури програми IAM бізнес може зіткнутися з такими серйозними перешкодами [1]:

часові і витрати на ручні процеси IAM;

поганий користувальницький досвід;

відсутність навичок розгортання сучасних рішень;

високі технічні витрати з монолітними настройками;

слабкі інновації і низька продуктивність співробітників.

Можливе зростання витрат також є фактором, який особливо турбує підприємства, які не мають сучасної програми IAM. Згідно зі звітом Ponemon Cost of an Insider Threat за 2020 рік, найдорожча інсайдерська загроза – це крадіжка облікових даних [1].

Ці інциденти значно збільшилися за частотою і вартостю. Фактично, частота інцидентів на компанію потроїлася з 2016 року – в середньому з 1 до 3,2, а середня вартість майже подвоїлася з 493 093 доларів США за той же період [1].

Більше 871 тис. дол. США – середня вартість інциденту крадіжки облікових даних для підприємств в 2019 році [1].

Для організацій, які хочуть підвищити точність і швидкість надання доступу потрібній людині в потрібний час і в потрібних умовах, існує потреба в сучасній програмі IAM та має першорядне значення. Але існують і інші вагомі причини для впровадження, які також повинні враховувати керівники служб безпеки і IT на підприємствах [1].

Серед стимулів до переходу на сучасні IAM – сприяння майбутнього зростання. Відмовившись від традиційної програми IAM, керівники підприємства виходять за рамки інструментів, щоб більше зосередитися на результатах і усунення технічних вад або надмірно індивідуалізованих рішень. Завдяки гнучкому підходу організації можуть швидко розгорнути сучасне рішення IAM для автоматизації робочих процесів. Перехід до більш стратегічних варіантів використання вивільняє ресурси IAM для інших важливих проектів [1].

В результаті підприємства можуть підготуватися до використання мікросервісов, які принесуть більше користі, забезпечать перевагу на ринку і

зроблять IAM розумніші за рахунок використання автоматизації, щоб відповідати суворим вимогам бізнесу. Ще один важливий фактор, який слід враховувати, – це безпроблемна взаємодія з кінцевим користувачем як для корпоративних співробітників, так і для споживачів [1].

Gartner повідомляє, що 70 відсотків проектів IAM зазнають невдачі через те, що їх не приймають користувачі. При використанні сучасної програми IAM користувачі повинні відчувати себе причетними до розгортання нових рішень. Цей досвід може сприяти широкому поширенню і успіху ініціативи програми IAM в цілому [1].

Системи управління ідентифікацією та доступом (IAM) можна розділити на дві категорії: управління ідентифікацією (IDM) і управління доступом (AM) [2].

IDM – це адміністрування профілів користувачів і дозволів. Він керує, наприклад, можливостями ініціалізації і деініціалізації через робочі процеси. AM – це використання профілів користувачів для контролю доступу. Він керує, наприклад, автентифікацією, єдиним входом (SSO), авторизацією користувачів. Користувачі можуть бути ким завгодно: клієнтом, членом екосистеми, співробітником або сутністю, яка не є людиною [2].

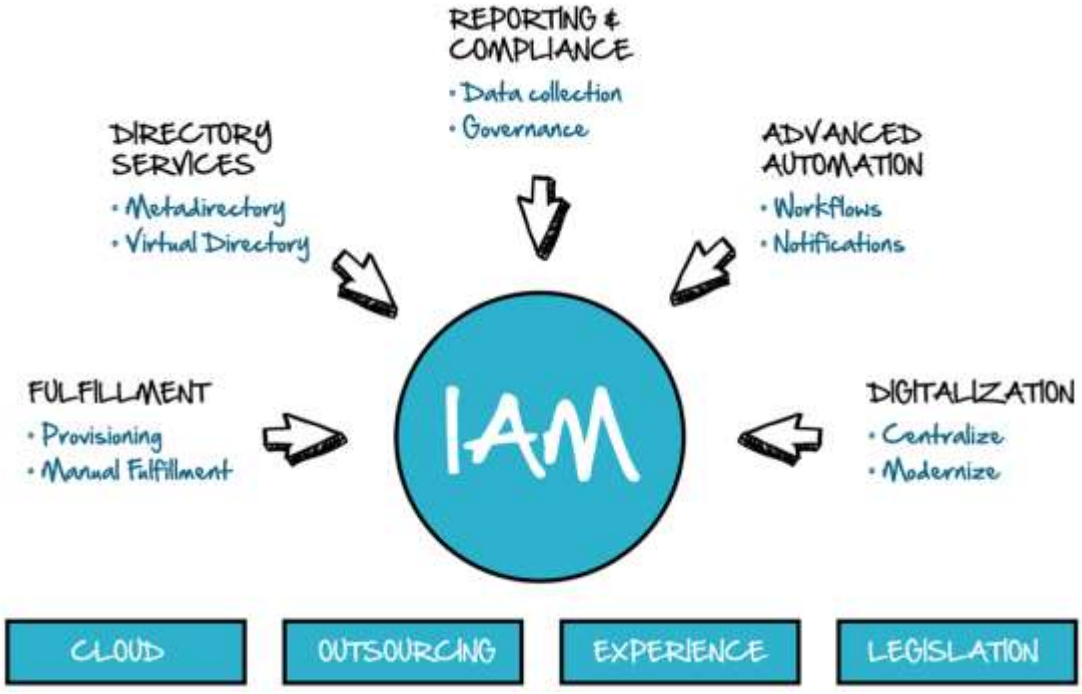

Рис. 1.1. Складові частини IAM [2]

Основна ідея будь-якого рішення IAM – діяти як централізоване сховище ідентифікаційних даних. Залежно від потреб клієнта, користувачі можуть мати кілька ідентифікаторів, які контролюються і відслідковуються, а також максимально автоматизовані. Централізоване рішення IAM може забезпечити гнучкість для бізнесу, підвищену безпеку і дотримання нормативних вимог [2].

Спочатку IAM можна управляти і контролювати без автоматизації для цільових систем, на цьому етапі треба докласти зусиль для процесів запиту та затвердження і стежити за журналом аудиту за допомогою ручного виділення ресурсів.

Інструменти IAM розрізняються залежно від потреби (рис. 1.1). Однак при створенні успішного рішення для управління ідентифікацією і доступом необхідно дотримуватися певних стандартів. Рішення IAM можна впроваджувати поступово. Це робить процес більш гнучким і адаптованим до потреб організації.

1.2. Підходи до управління ідентифікацією та доступом користувачів до корпоративних даних

У [3] зазначається, що компрометовані облікові дані користувачів є однією з найпоширеніших цілей для хакерів отримати доступ до мереж організацій за допомогою зловмисного програмного забезпечення, фішингу та атак програм-вимагачів. Тому для підприємств життєво важливо зберігати свої найцінніші ресурси. Для цього в корпоративних мережах втілюються рішення з управління ідентифікацією та доступом (Identity and Access Management, IAM) для захисту корпоративних даних та користувачів.

Розглянемо визначення управління ідентифікацією та доступом. *IAM – це система політик, процесів та технологій, що дозволяють організаціям керувати цифровими посвідченнями та контролювати доступ користувачів до важливої корпоративної інформації.* Призначаючи користувачам конкретні ролі та забезпечуючи належний рівень доступу до корпоративних ресурсів та мереж, IAM покращує безпеку та зручність роботи користувачів, забезпечує кращі результати

бізнесу та підвищує життєздатність мобільної та віддаленої роботи, використання хмарних технологій [3].

Основною метою рішення IAM є присвоєння однієї цифрової ідентифікації кожній особі чи пристрою. Потім рішення підтримує, модифікує та контролює рівні доступу та привілеї протягом життєвого циклу кожного користувача.

Основними функціями системи IAM є [3]:

перевірка та автентифікація користувачів на основі їх ролей та контекстної інформації, таких як локація, час доби або мережі (довірені чи інші);

захоплення та запис подій для входу користувачів;

управління та забезпечення видимості бази ідентифікаційних даних компанії;

керування призначенням та видаленням прав доступу користувачів;

надання дозволу системним адміністраторам керувати та обмежувати доступ користувачів та контролювати зміни в привілеях користувачів.

Аспекти нульової довіри охоплюють все: від типу ресурсів, якими управляє організація, до того, як вони готують і деініціалізують користувачів, які методи автентифікації розгортають і багато іншого.

Компанії з фрагментованим підходом до ідентифікації (рис. 1.2) ще не почали свій шлях. На етапі 0 вони можуть почати використовувати хмарні технології, але ще не інтегрують ці рішення з платформою IAM або локальними ресурсами. На етапі 1 команди починають працювати над єдиною екосистемою IAM, реалізуючи такі проекти, як усунення неякісних паролів за рахунок впровадження єдиного входу (SSO) та багатофакторної автентифікації (MFA) для доступу співробітників до ключових ресурсів [10].

Переходячи до етапу 2, підприємства впроваджують додаткові передові методи безпеки, розширюючи контроль доступу на інші ресурси, такі як їх API-інтерфейси, а також використовуючи багатий контекст і різні фактори для більш обґрунтованого прийняття рішень щодо автентифікації. Варто зазначити, що захист API особливо важливий на даному етапі, оскільки Gartner виявив, що «до 2023 року 90% веб-додатків матимуть велику поверхню для атаки у вигляді

відкритих API, а не призначеного для користувача інтерфейсу, порівняно від 40% в 2019 році» [10].

Коли компанії досягають стадії 3, вони успішно впроваджують підхід повної автентифікації, заснованої на оцінці ризиків, з нульовим довірою, з рішеннями безпарольного і безперервного доступу.

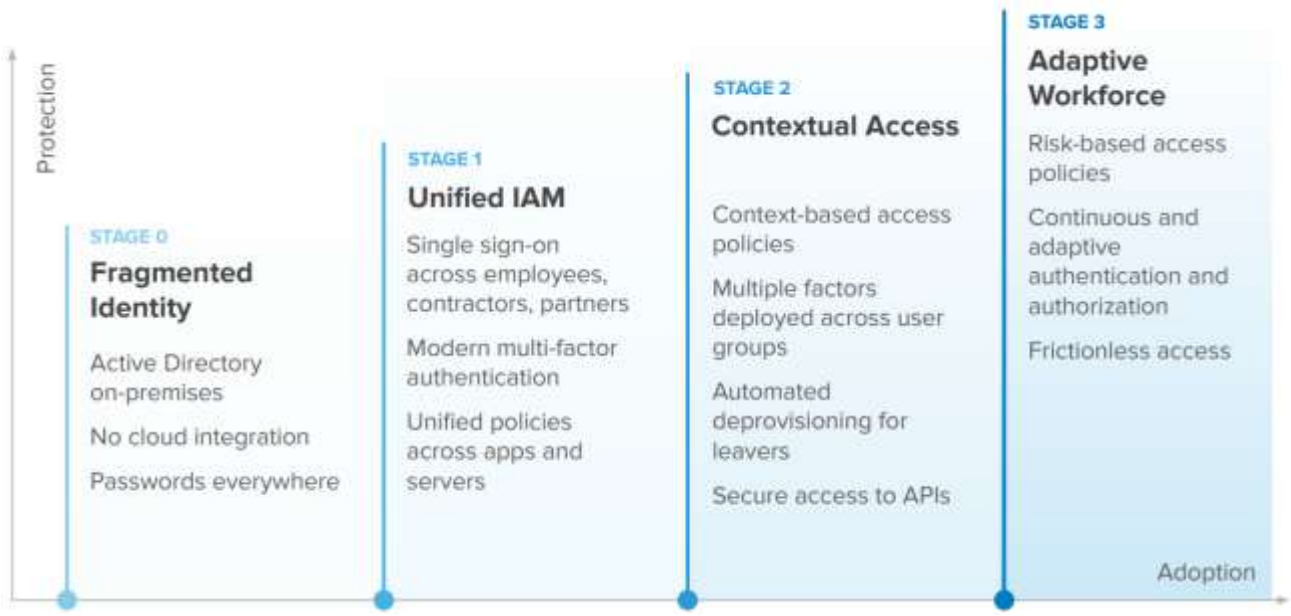

Рис. 1.2. Крива зрілості ідентифікації та доступу [10]

1.3. Модель управління доступом на основі ролей

Розглянемо модель управління доступом на основі ролей (Role Based Access Control, RBAC).

Еталонна модель RBAC визначає набори основних елементів RBAC (таких як користувачі, ролі, дозволи, операції і об'єкти) і відносин, такі як типи і функції. Еталонна модель RBAC служить двом цілям. По-перше, еталонна модель визначає обсяг функцій RBAC. Це визначає мінімальний набір функцій, включених в усі системи RBAC, аспекти ієрархій ролей, аспекти відносин статичних обмежень і аспекти відносин динамічних обмежень. По-друге, еталонна модель забезпечує точну і узгоджену мову з точки зору наборів елементів і функцій для використання при визначенні функціональної специфікації [9].

Набори і відносини основних елементів моделі RBAC визначені на рис. 1.3 Ядро RBAC включає в себе набори з п'яти основних елементів даних, які називаються користувачі (USERS), ролі (ROLES), об’єкти (OBS), операції (OPS) та дозволи (PRMS) [9].

Модель RBAC в цілому визначається в термінах окремих користувачів, яким призначаються ролі, а дозволи призначаються ролям. Таким чином, роль – це засіб для позначення відносин «many-to-many» між окремими користувачами та дозволами. Крім того, базова модель RBAC включає набір сеансів (SESSIONS), де кожен сеанс являє собою зіставлення між користувачем і активованою підмножиною ролей, призначених користувачеві [9].

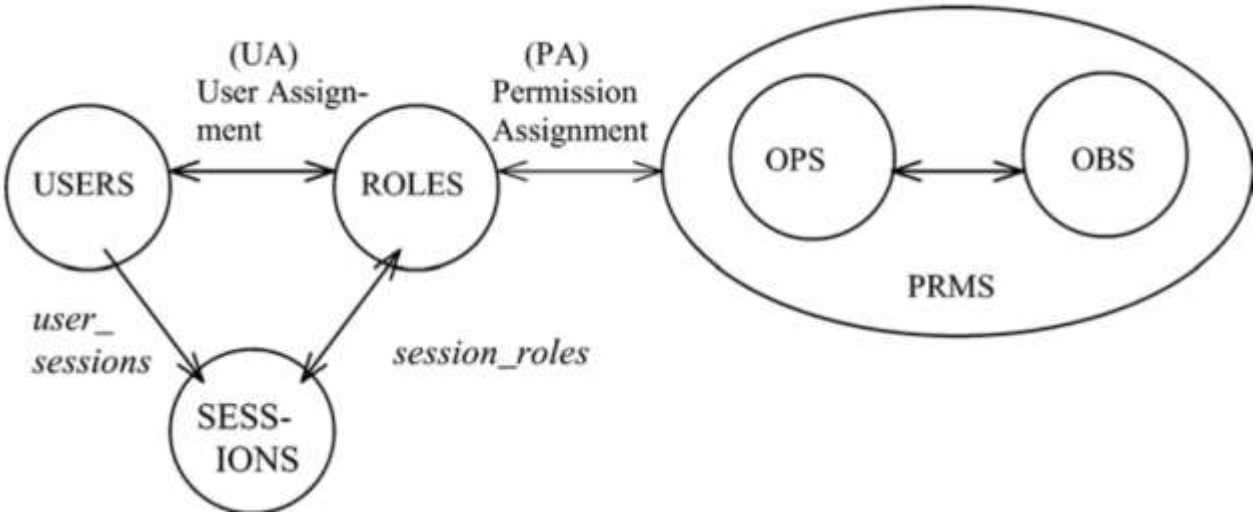

Рис. 1.3. Ядро моделі RBAC [9]

Користувач визначається як людина. Хоча поняття користувач може бути розширено, щоб включити в нього машини, мережі або інтелектуальні автономні агенти.

Роль – це службова функція в контексті організації з деякою пов'язаною семантикою, що стосується повноважень і відповідальності, наданих користувачеві, якому призначена роль.

Дозвіл – це дозвіл на виконання операції з одним або декількома об'єктами, захищеними RBAC.

Операція – це виконуваний образ програми, який при виклику виконує деяку функцію для користувача.

Типи операцій і об'єктів, якими управляє RBAC, залежать від типу системи, в якій вона буде реалізований. Наприклад, в файловій системі операції можуть включати читання, запис і виконання; в системі управління базою даних операції можуть включати вставку, видалення, додавання та оновлення [9].

Мета будь-якого механізму управління доступом – захистити системні ресурси (тобто захищені об'єкти). Відповідно до більш ранніх моделей управління доступом об'єкт – це об'єкт, який містить або приймає інформацію [9].

Для системи, яка реалізує RBAC, об'єкти можуть представляти інформаційні контейнери (наприклад, файли, каталоги в операційній системі та/або стовпці, рядки, таблиці та подання в системі управління базами даних) або об'єкти можуть представляти вичерпні системні ресурси, такі як принтери, дисковий простір і цикли процесорів [9].

Набір об'єктів, які охоплюються RBAC, включає всі об'єкти, перераховані в дозволах, призначених ролям. Центральне місце в RBAC займає концепція рольових відносин, навколо яких роль є семантичної конструкцією для формулювання політики [9].

На рис. 1.3 показані відносини призначення користувачів (UA) та призначення дозволів (PA). Стрілки вказують на ставлення «many-to-many» (наприклад, користувачеві може бути призначена одна або декілька ролей, а роль може бути призначена одному або декільком користувачам). Таке розташування забезпечує більшу гнучкість і детальність призначення дозволів ролям і користувачів ролям. Без цих зручностей існує підвищена небезпека того, що користувачеві може бути наданий більший доступ до ресурсів, ніж це необхідно, через обмежений контроль над типом доступу, який може бути пов'язаний з користувачами і ресурсами. Користувачам може знадобитися перерахувати каталоги і змінити існуючі файли, наприклад, без створення нових файлів, або їм може знадобитися додати записи в файл без зміни існуючих записів. Будь-яке збільшення гнучкості контролю доступу до ресурсів також підсилює застосування принципу найменших привілеїв [9].

Кожен сеанс являє собою зіставлення одного користувача з можливою множиною ролей, тобто користувач встановлює сеанс, під час якого користувач активує деяку підмножину ролей, які йому призначено. Кожен сеанс пов'язаний з одним користувачем і кожен користувач пов'язаний з одним або декількома сеансами. Функція *session_roles* дає нам ролі, активовані сеансом, а функція *session_users* дає нам користувача, пов'язаного з сеансом. Доступні користувачеві дозволи – це дозволи, призначені ролям, які в даний момент активні у всіх сеансах користувача [9].

Рольовий контроль доступу. Фреймворки IAM мають не лише вирішальне значення для контролю доступу користувачів до важливої інформації, але й реалізації контролю доступу на основі ролей. Це дозволяє системним адміністраторам регулювати доступ до корпоративних мереж або систем на основі ролей окремих користувачів, які визначаються їх посадою, рівнем повноважень та відповідальністю в бізнесі [3].

Рішення IAM також має вирішальне значення для запобігання ризикам безпеки, коли працівники покидають бізнес. Скасування вручну привілеїв доступу до програм та послуг, якими користувався колишній співробітник, часто може зайняти час або навіть забути повністю, залишаючи хакерам прогалину в безпеці. IAM запобігає цьому, автоматично припиняючи надання прав доступу після того, як користувач покидає компанію або коли змінюється його роль в організації.

Цифрові ідентичності існують не тільки для людей, оскільки IAM також управляє ідентифікацією пристроїв та додатків. Це створює подальшу довіру та забезпечує глибший контекст навколо того, чи є користувач тим, ким він є, і програмами, до яких користувач має право доступу.

Рішення IAM складається з різних компонентів та систем. Найчастіше розгортаються [3]:

Єдиний вхід (SSO) – це форма контролю доступу, яка дозволяє користувачам проходити автентифікацію за допомогою декількох програм або систем, використовуючи лише один логін та один набір облікових даних. Додаток або веб-сайт, до якого користувач намагається отримати доступ, покладається на

довірену третю сторону, щоб підтвердити, що користувач є тим, ким вони називаються, в результаті чого забезпечується покращений інтерфейс користувача, знижена втомлюваність паролем, прощене управління паролями, мінімізовані ризики безпеки для клієнтів, партнерів та постачальників, обмежене використання облікових даних та покращений захист особистості.

Багатофакторна автентифікація перевіряє особу користувача, вимагаючи від них введення декількох облікових даних та надання різних факторів:

щось, що користувач знає: пароль;

щось, що є у користувача: токен або код, надісланий користувачеві електронною поштою або SMS, апаратний генератор токенів або програму автентифікації, встановлену на смартфоні користувача;

щось специфічне для користувача, наприклад, біометрична інформація.

Управління привілейованим доступом захищає бізнес як від кібератак, так і від інсайдерських атак, призначаючи вищі рівні дозволів обліковим записам з доступом до важливих корпоративних ресурсів та засобів управління на рівні адміністратора. Ці рахунки зазвичай є цілями для кіберзлочинців і, як такі, високим ризиком для організацій.

Автентифікація на основі ризику – коли користувач намагається увійти в програму, рішення для автентифікації на основі ризику розглядає контекстні функції, такі як їх поточний пристрій, IP-адреса, місцезнаходження або мережа, щоб оцінити рівень ризику. На основі цього він вирішить, дозволити користувачеві доступ до програми, запропонувати йому подати додатковий коефіцієнт автентифікації або заборонити їм доступ. Це допомагає компаніям негайно виявляти потенційні ризики безпеки, глибше розуміти контекст користувача та підвищувати рівень безпеки за допомогою додаткових факторів автентифікації.

Управління даними – це процес, який дозволяє компаніям управляти доступністю, цілісністю, безпекою та зручністю використання своїх даних. Сюди входить використання політик та стандартів щодо використання даних, щоб забезпечити їх узгодженість, надійність та не зловживати ними. Управління

даними важливо в рамках рішення IAM, оскільки засоби штучного інтелекту та машинного навчання покладаються на підприємства, які мають якісні дані.

Федеративне управління ідентифікацією – це процес спільного використання автентифікації, за допомогою якого підприємства діляться цифровими посвідченнями з надійними партнерами. Це дозволяє користувачам користуватися послугами декількох партнерів, що використовують однакові облікові дані. Єдиний вхід є прикладом цього процесу на практиці.

Нульова довіра – підхід Zero-Trust віддаляє бізнес від традиційної ідеї довіри всім або всьому, що підключено до мережі або за брандмауером. Ця думка вже неприйнятна, враховуючи прийняття хмарних та мобільних пристроїв, які розширюють робоче місце за межі чотирьох стін офісу та дозволяють людям працювати з будь-якого місця. IAM є вирішальним у цьому підході, оскільки він дозволяє компаніям постійно оцінювати та перевіряти людей, які мають доступ до їх ресурсів.

Розглянемо переваги системи управління ідентифікацією та доступом. Впровадження рішення IAM забезпечує широкий спектр переваг для організацій, таких як [3]:

безпечний доступ: відкриття мереж для більшої кількості співробітників, нових підрядників, клієнтів та партнерів забезпечує більшу ефективність та продуктивність, але це також збільшує ризик. Рішення IAM дозволяє компаніям розширити доступ до своїх додатків, мереж та систем локально та в хмарі без шкоди для безпеки;

скорочення запитів довідкової служби. Рішення IAM позбавляє користувачів потреби надсилати скидання паролів та запити довідкової служби, автоматизуючи їх. Це дозволяє користувачам швидко та легко підтвердити свою особу, не турбуючи адміністраторів системи, які, в свою чергу, можуть зосередитись на завданнях, які додають більшої ділової цінності;

знижений ризик. Покращений контроль доступу користувачів означає зменшення ризику порушення внутрішніх та зовнішніх даних. Це життєво важливо, оскільки хакери все частіше націлюють облікові дані користувачів як

ключовий метод доступу до корпоративних мереж та ресурсів;

дотримання вимог. Ефективна система IAM допомагає бізнесу задовольнити потреби у відповідності до вимог, що стосуються все більш суворих правил щодо даних та конфіденційності.

1.4. Підходи до реалізації технології управління ідентифікацією та доступом користувачів до інформаційних систем

Можливості управління ідентифікацією та доступом (IAM) мають вирішальне значення в захисті клієнтів від захоплення облікових записів, крадіжки особистих даних і порушень конфіденційності. Керівники бізнесу, IT-директори і директори з інформаційної безпеки використовують технології IAM як для взаємодії з клієнтами, так і для їх захисту протягом усього шляху. Ці ж технології також життєво важливі для захисту досвіду співробітників, підвищення їх як операційної ефективності, так і продуктивності [12].

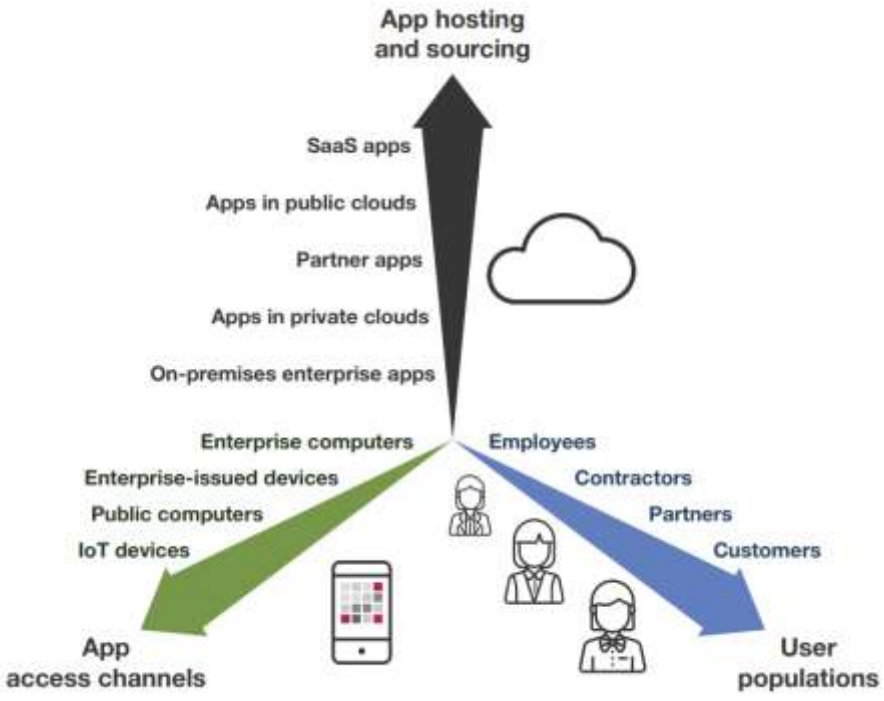

Рис. 1.4. IAM повинен обслуговувати моделі хостингу керованих додатків, групи користувачів і різноманітність кінцевих точок [12]

Методи та засоби IAM повинні підтримувати нові цифрові бізнес-моделі і вимоги. Оскільки компанії використовують цифрові технології для створення нових джерел цінності для клієнтів і підвищення оперативності, життєво важливі

бізнес-процеси будуть проходити через різні групи користувачів, моделі хостингу, а також канали і пристрої доступу (рис. 1.4) [12].

Корпоративна стратегія та архітектура IAM повинні забезпечувати необхідний рівень контрольованого доступу з будь-якого пристрою до будь-якого внутрішнього або зовнішнього додатку і ресурсу даних, незалежно від моделі хостингу, для співробітників і підрядників (сценарії IAM для персоналу), ділових партнерів (сценарії IAM партнерів), клієнтів (сценарії IAM споживача і додаткових партнерів) і пристроїв (сценарії підключеного пристрою IAM) (рис. 1.5) [12].

Підключення пристрою і ідентифікатори машин, такі як боти, ще більше ускладнюють ці вимоги через їх величезну кількість, множину типів і обсягів даних, якими повинні керувати і управляти групи безпеки. Це матиме неабиякий вплив на дизайн інтерфейсу IAM-систем і архітектуру сучасних рішень, які інтегруються з IAM-системами.

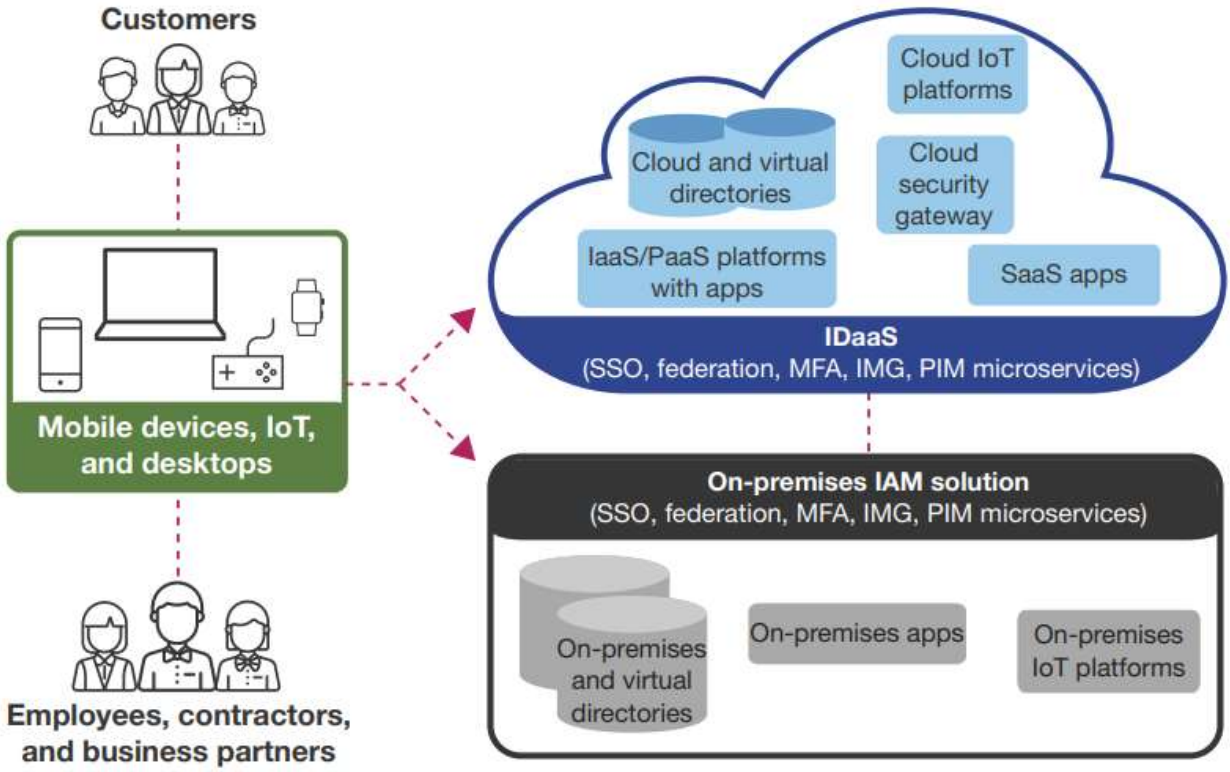

Рис. 1.5. Еталонна архітектура IAM на основі мікросервісів і API [12]

Сучасні середовища корпоративної ідентифікації складаються з різних систем записів, починаючи від мережевих пристроїв, серверів, служб каталогів та

хмарних додатків. Управління ідентифікацією, яка знаходиться в цих різних системах, може швидко перерости в таку велику адміністративну проблему, що негативно впливає на користувачів, адміністраторів та розробників додатків [4].

Крім того, багато найбільш шкідливих порушень безпеки на сьогоднішній день спричинені скомпрометованими обліковими записами користувачів та паролями, погіршеними тим, що користувачі отримують невідповідні рівні доступу. Безпечне та ефективне управління автентифікацією та авторизацією ідентифікаційних даних для всіх систем та додатків має вирішальне значення для мінімізації порушень безпеки [4].

Fortinet IAM надає послуги, необхідні для надійного підтвердження особи користувачів та пристроїв під час їх входу в мережу. За допомогою даного надійного рішення можна контролювати і керувати ідентифікацією, щоб надійно підключити потрібних користувачів лише до відповідних ресурсів.

Рішення Fortinet IAM включає такі продукти [4]:

FortiAuthenticator захищає від несанкціонованого доступу до корпоративних ресурсів, надаючи централізовані послуги автентифікації для Fortinet Security Fabric, включаючи послуги єдиного входу, управління сертифікатами та управління доступом гостей;

FortiToken підтверджує особистість користувачів, додаючи другий фактор до процесу автентифікації за допомогою фізичних або мобільних маркерів додатків;

FortiToken Cloud пропонує як послугу багатофакторну автентифікацію (MFA). Організації можуть використовувати інтуїтивно зрозумілу інформаційну панель для управління MFA.

Поєднання FortiAuthenticator та FortiToken або FortiToken Cloud ефективно вирішує проблеми, пов’язані з ідентифікацією та управлінням доступом, з якими стикаються організації в цю епоху швидко зростаючого зв’язку між користувачами та пристроями [4].

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА НА БАЗІ FortiAuthenticator

2.1. Призначення та основні функції рішення FortiAuthenticator

Причиною багатьох найбільш небезпечних порушень безпеки є доступ неавторизованих користувачів до мережі або надання дійсним користувачам доступу на рівні, який не відповідає їх реальним повноваженням.

Основне призначення рішення FortiAuthenticator – управління доступом з функцією ідентифікації для адаптивної системи мережевої безпеки. FortiAuthenticator підтримує функції, які забезпечують ефективну реалізацію політик безпеки і підвищують рівень захищеності мережі. Доступ до конфіденційних мереж і даних при необхідності зможуть отримати тільки користувачі з відповідними повноваженнями.

Основними функціями рішення FortiAuthenticator є:

прозора ідентифікація користувачів мережі і реалізація політик на основі посвідчень в корпоративній мережі, оснащеної системою Fortinet;

надійна двофакторна перевірка справжності/перевірка справжності за допомогою одноразового пароля за підтримки рішення FortiToken;

управління сертифікатами для корпоративних безпроводових підключень і підключень VPN;

управління гостьовим доступом для проводових і безпроводових мереж;

функції єдиного входу для внутрішніх і хмарних мереж.

Особливостями управління ідентифікацією користувачів і технології єдиного входу (SSO) рішення Fortinet є [5]:

включає політики безпеки на основі ідентифікаційних даних і ролей в захищеній корпоративної мережі Fortinet без необхідності додаткової автентифікації за рахунок інтеграції з Active Directory;

підвищує безпеку підприємства за рахунок спрощення та централізації

управління ідентифікаційною інформацією користувачів;

безпечна багатофакторна автентифікація/OTP (One Time Password, OTP) з повною підтримкою FortiToken;

автентифікація за протоколами RADIUS і LDAP;

управління сертифікатами для розгортання корпоративної VPN;

підтримка IEEE802.1X для забезпечення безпеки проводових і безпроводових мереж;

SAML SP/IdP (Service Provider/Identity Provider) Web SSO.

Розглянемо політику корпоративної мережевої ідентифікації.

Доступ до мережі та Інтернет є ключовим фактором практично для кожної ролі на підприємстві. Однак ця вимога повинна бути збалансовано з ризиком, який вона несе. *Ключова мета кожного підприємства – забезпечити безпечний, але контрольований доступ до мережі, що дозволяє потрібній людині отримати потрібний доступ в потрібний час без шкоди для безпеки* [5].

Єдиний вхід Fortinet (FSSO) – це метод забезпечення безпечного доступу до мережі, підключеної до Fortinet, і доступу на основі ролей. Завдяки інтеграції з існуючими системами автентифікації Active Directory або LDAP, він забезпечує безпеку корпоративних користувачів на основі ідентифікації, не заважаючи користувачеві і не створюючи роботи для мережевих адміністраторів [5].

FortiAuthenticator заснований на принципах єдиного входу Fortinet, додаючи більш широкий спектр методів ідентифікації користувачів і велику масштабованість. FortiAuthenticator – це функціональний компонент авторизації в захищеній корпоративної мережі Fortinet, який ідентифікує користувачів, запитує дозволу на доступ у сторонніх систем і передає цю інформацію на пристрої FortiGate для використання в політиках на основі ідентифікації [5].

FortiAuthenticator забезпечує прозору ідентифікацію за допомогою широкого набору методів [5]:

опитування контролера домену Active Directory;

інтеграція з FortiAuthenticator Single Sign-On Mobility Agent, який визначає вхід в систему, зміну IP-адреси і вихід з системи;

автентифікація на основі порталу FSSO з віджетами відстеження для зменшення необхідності повторної автентифікації;

моніторинг RADIUS Accounting Start записів.

Ключові особливості та переваги рішення FortiAuthenticator [5]:

прозора ідентифікація користувачів FSSO – нульовий вплив на корпоративних користувачів;

інтеграція з LDAP і AD для членства в групах – використовує існуючі системи для мережевої авторизації, скорочуючи час розгортання і оптимізуючи процеси управління. Інтеграція з існуючими процедурами управління користувачами;

широкий спектр методів ідентифікації користувачів – гнучкі методи ідентифікації користувачів для інтеграції з найрізноманітнішими корпоративними середовищами;

включення ідентифікації та безпеки на основі ролей – дозволяє адміністратору безпеки надавати користувачам доступ до відповідної мережі та ресурсів додатків, що відповідають їх ролі, зберігаючи при цьому контроль і мінімізуючи ризики.

Роглянемо методи ідентифікації користувачів для єдиного входу в FortiAuthenticator.

Рішення FortiAuthenticator може ідентифікувати користувачів за допомогою різноманітних методів і інтегруватися зі сторонніми системами LDAP або Active Directory для застосування даних груп або ролей до користувача і зв'язку з FortiGate для використання в політиках на основі ідентифікації. FortiAuthenticator повністю гнучкий і може використовувати ці методи в поєднанні. Наприклад, на великому підприємстві в якості основного методу прозорої автентифікації з відкатом до порталу для систем, що не відносяться до домену, або гостьових користувачів можна вибрати опитування AD або FortiAuthenticator SSO Mobility Agent [5].

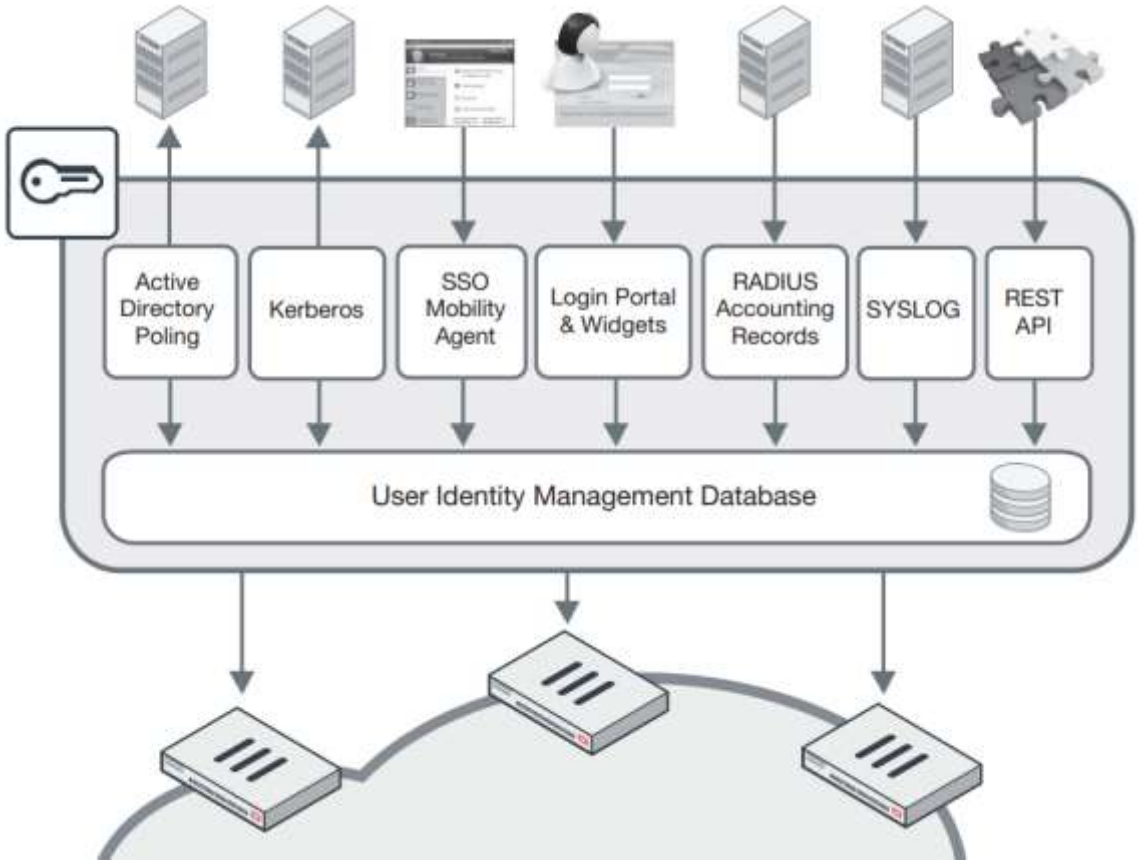

Рис. 2.1. Методи управління ідентифікацією користувачів, які застосовуються [5]

Опитування Active Directory. Перевірка автентичності користувача в активному каталозі можна знайти шляхом регулярного опитування контролерів домену. При виявленні входу в систему ім'я користувача, IP-адреса і відомості про групу вводяться в базу даних управління ідентифікацією користувачів FortiAuthenticator і відповідно до локальної політикою можуть використовуватися спільно з декількома пристроями FortiGate (рис. 2.1, 2.2) [5].

FortiAuthenticator SSO Mobility Agent. Для складних розподілених доменних архітектур, де опитування контролерів домену неможливий або небажаний, альтернативою є клієнт єдиного входу FortiAuthenticator. Розповсюджуваний як частина FortiClient або як окрема установка для ПК з Windows, клієнт передає FortiAuthenticator інформацію про вхід в систему, зміни стека IP (проводовий/ безпроводовий, бездротовий мережевий роумінг) і вихід з системи, усуваючи необхідність в методах опитування (рис. 2.1) [5].

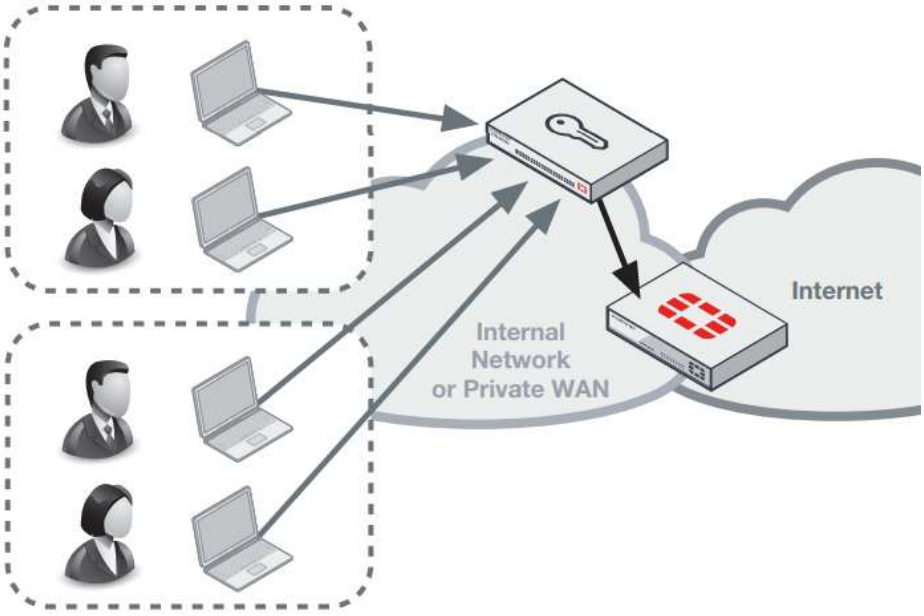

Рис. 2.2. Опитування Active Directory [5]

Портал логінів та віджети FortiAuthenticator. Для систем, які не підтримують опитування AD або де клієнт недоступний, FortiAuthenticator надає портал явної автентифікації. Цей портал дозволяє користувачам вручну автентифікуватися в FortiAuthenticator, а потім в мережі. Щоб звести до мінімуму вплив повторних входів в систему, необхідних для ручної автентифікації, надається набір віджетів для вбудовування в мережі організації, які автоматично реєструють користувачів за допомогою файлів cookie браузера щоразу, коли вони заходять на домашню сторінку інтрамережі (рис. 2.1, 2.3) [5].

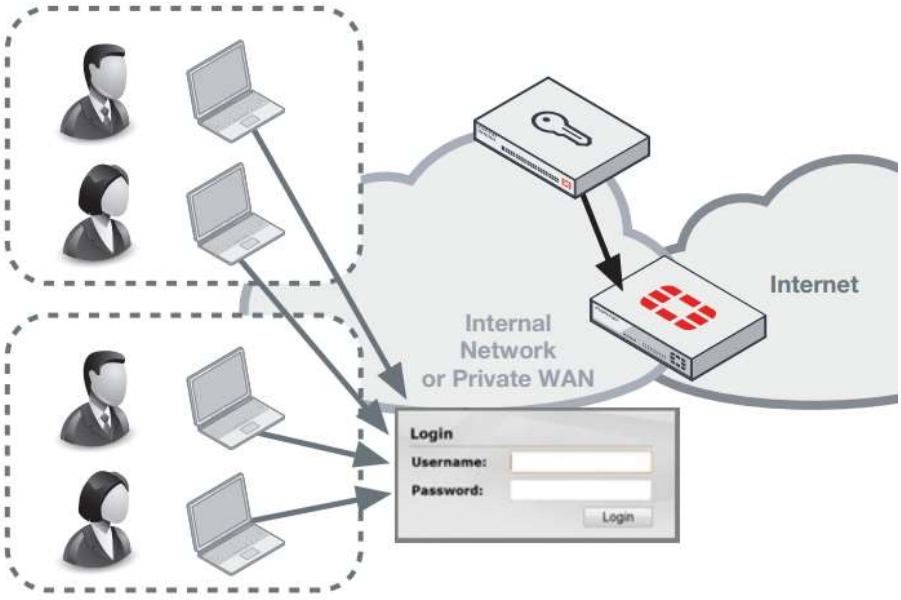

Рис. 2.3. Портал логінів та віджети FortiAuthenticator [5]

Вхід в обліковий запис RADIUS. У мережі, яка використовує автентифікацію за протоколом RADIUS (наприклад, безпроводову автентифікацію або автентифікацію VPN), облік RADIUS може використовуватися як метод ідентифікації користувача. Ця інформація використовується для запуску входу користувача в систему і надання інформації про IP-адресу і групу, усуваючи необхідність у другому рівні автентифікації (рис. 2.1, 2.4) [5].

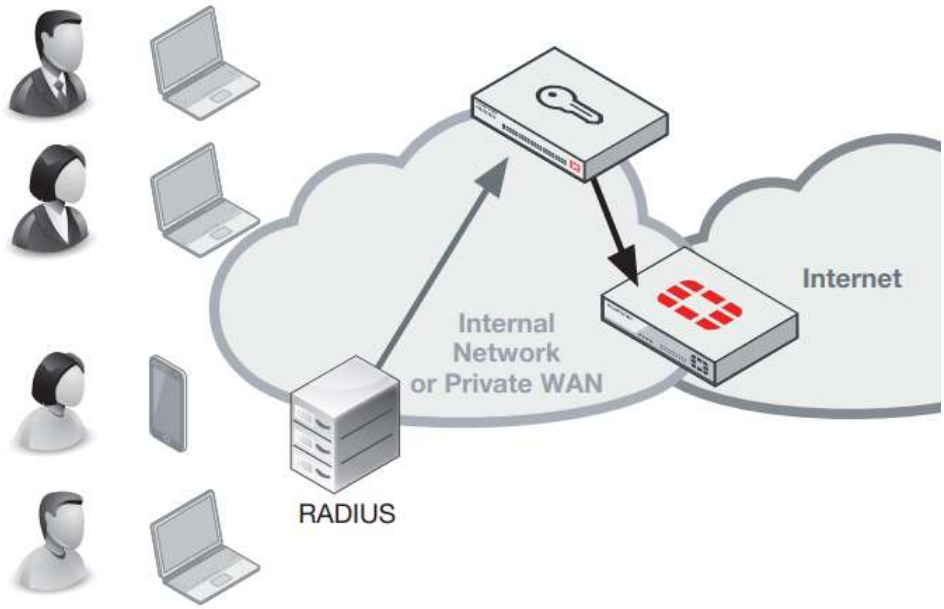

Рис. 2.4. Вхід в обліковий запис RADIUS [5]

Розглянемо додаткову функціональність рішення FortiAuthenticator.

Надійна ідентифікація користувача з багатофакторною автентифікацію.

FortiAuthenticator розширює можливості багатофакторної автентифікації на кілька пристроїв FortiGate і сторонні рішення, що підтримують автентифікацію за протоколами RADIUS або LDAP. Ідентифікаційна інформація користувача з FortiAuthenticator в поєднанні з автентифікаційною інформацією з FortiToken гарантує, що тільки авторизованим особам буде надано доступ до конфіденційної інформації організації. Цей додатковий рівень безпеки значно знижує ймовірність витоку даних, допомагаючи компаніям виконувати вимоги аудиту, пов'язані з державними та комерційними правилами конфіденційності [5].

FortiAuthenticator підтримує найширший спектр токенов, який може задовольнити вимоги користувача. FortiAuthenticator надає можливість використовувати фізичні одноразові токени FortiToken 200, FortiToken Mobile

(для iOS і Android), e-mail- і SMS-токени, а також використовувати токени для всіх користувачів і сценаріїв. Багатофакторна автентифікація може використовуватися для управління доступом до таких додатків, як управління FortiGate, SSL і IPsec VPN, вхід в портал безпродового доступу та мережеве обладнання сторонніх виробників, сумісний з RADIUS. Для спрощення управління локальними користувачами FortiAuthenticator включає функції саморегистрації користувачів і відновлення пароля [5].

Корпоративні VPN на основі сертифікатів. VPN типу «мережу-мережа» часто забезпечують прямий доступ до серцевини корпоративної мережі з багатьох віддалених місць. Часто ці віртуальні приватні мережі захищаються просто заздалегідь наданим ключем, який в разі злому може надати доступ до всієї мережі. FortiOS підтримує VPN на основі сертифікатів. Однак використання захищених сертифікатами мереж VPN було обмежено, в першу чергу через накладні витрати і складності, пов'язаних з управлінням сертифікатами. FortiAuthenticator усуває ці накладні витрати, оптимізуючи масове розгортання сертифікатів для використання VPN в середовищі FortiGate, співпрацюючи з FortiManager для настройки і автоматизації доставки безпечних сертифікатів по протоколу SCEP [5].

Для клієнтських VPN сертифікатів сертифікати можуть бути створені і збережені в сховище сертифікатів USB FortiToken 300. Це безпечне сховище сертифікатів, захищене контактами, сумісно з FortiClient і може використовуватися для підвищення безпеки клієнтських VPN-підключень в поєднанні з FortiAuthenticator [5].

Додаткові функції і переваги рішення FortiAuthenticator [5]:

автентифікація користувачів за протоколами RADIUS і LDAP – локальна база даних автентифікації з інтерфейсами RADIUS і LDAP централізує управління користувачами;

широкий спектр надійних методів автентифікації – надійна автентифікація, що забезпечується FortiAuthenticator за допомогою апаратних токенів, токенів електронної пошти, SMS, електронної пошти і цифрових сертифікатів, допомагає

підвищити безпеку паролів і знизити ризик розкриття пароля, відтворення або перебору паролів;

самостійна реєстрація користувача і відновлення пароля – знижує необхідність втручання адміністратора, дозволяючи користувачеві виконувати власну реєстрацію і вирішувати свої проблеми з паролями, що також підвищує задоволеність користувачів;

інтеграція з Active Directory і LDAP. Інтеграція з існуючими каталогом спрощує розгортання, прискорює установку і дозволяє повторно використовувати існуючі розробки;

управління сертифікатами – оптимізоване управління сертифікатами забезпечує швидке та економічне розгортання методів перевірки справжності на основі сертифікатів, таких як VPN;

автентифікація 802.1X – управління доступом до корпоративних портів для перевірки підключення користувачів до локальної і безпроводової локальної мережі для запобігання несанкціонованому доступу до мережі.

2.2. Призначення та основні функції рішення FortiToken 200

Рішення FortiToken 200 є токеном з одноразовим паролем.

Перевірка справжності виключно за допомогою пароля може спричинити за собою порушення безпеки, зараження шкідливим ПЗ і проблеми реалізації політик. *Двофакторна перевірка справжності передбачає використання пароля спільно з токеном і сервером перевірки автентичності, що істотно підвищує рівень захисту.* Авторизовані співробітники отримують захищений доступ до корпоративних ресурсів за допомогою різних пристроїв: від ноутбуків до мобільних телефонів. Серія FortiToken 200 включає доступні за ціною і зручні в експлуатації апаратні токени, призначені для застосування в середовищах, які потребують ефективної перевірки автентичності.

Серія FortiToken 200 має наступні переваги (рис. 2.5):

ефективний засіб перевірки автентичності, який масштабується, з низькою вхідною вартістю і низькою сукупною вартістю володіння;

зручність використання завдяки унікальному параметру активації по мережі;

зниження експлуатаційних витрат за рахунок застосування існуючого засобу FortiGate як серверу перевірки автентичності;

зручний великий ЖК-дисплей.

Рис. 2.5 Вигляд FortiToken 200

Fortinet FortiToken Mobile (FTM) і апаратні OTP-токени (FTK200, FTK-200CD і FTK-220) повністю інтегровані з FortiClient, захищені FortiGuard і забезпечують пряме управління і використання в платформах безпеки FortiGate і FortiAuthenticator. Ці токени застосовуються для захисту корпоративної мережі за допомогою простих в управлінні і простих у використанні рішень для двофакторної автентифікації.

FortiToken 200/200CD FortiToken 200 є частиною широкої і гнучкої пропозиції Fortinet для двофакторної автентифікації. Це протокол TOTP (Time-based one-time Password algorithm), що відповідає вимогам OATH (Initiative For Open Authentication). Це невеликий пристрій розміром з брелок для ключів, який забезпечує реальну мобільність і гнучкість для кінцевого користувача. Клієнтське програмне забезпечення для установки не потрібно – просто натисніть кнопку, FortiToken 200 генерує і відображає безпечний одноразовий пароль кожні 60 секунд для перевірки особистості користувача для доступу до критично важливих мереж і додатків.

Великий ЖК-екран FortiToken 200 набагато легше читається, ніж інші маркери OTP, і на екрані є індикатор, який показує час, що залишився до наступного OTP. Токени FortiToken 200CD поставляються з зашифрованим

активаційним компакт-диском для максимальної безпеки початкового числа токенов OTP.

Розглянемо переваги рішення FortiToken 200.

Надійна автентифікація під рукою. Це клієнтський компонент високонадійний, простий у використанні і адмініструванні Fortinet, надзвичайно економічне рішення з двома факторами, що відповідає вимогам строгої автентифікації. Апаратний OTP-токен запобігає крадіжці паролів користувачів, фішинговим, словниковим і атакам методом перебору.

Крім готової можливості взаємодії з будь-яким OATH-сумісним сервером автентифікації на основі часу, таким як FortiAuthenticator від Fortinet, FortiToken також можна використовувати безпосередньо з консолідованою платформою безпеки FortiGate, включаючи конфігурації високої доступності. FortiGate має вбудований сервер автентифікації для перевірки OTP в якості другого фактора автентифікації для SSL VPN, IPsecVPN, Captive Portal і адміністративного входу, що усуває необхідність у зовнішньому сервері RADIUS, який зазвичай потрібно при реалізації двофакторних рішень [6].

Онлайн-активація за допомогою FortiGuard

Існує можливість активувати FortiToken онлайн безпосередньо з FortiGate або FortiAuthenticator, використовуючи FortiGuard Center, який підтримує початкові значення токенов в керованому репозиторії сервісів. Після активації токену до них більше не можна буде отримати доступ з FortiGuard, що гарантує безпеку токенів від компрометації.

Переваги FortiToken 200 [6]:

унікальна служба надання токенов через FortiGuard зводить до мінімуму накладні витрати на підготовку і забезпечує максимальну безпеку початкового числа;

безстрокова ліцензія на токен і необмежену кількість передач пристроїв виключають щорічну абонентську плату;

масштабоване рішення, що використовує існуючі пристрої кінцевих користувачів, пропонує низьку початкову вартість і сукупну вартість володіння;

зниження витрат і складності за рахунок використання існуючого рішення FortiGate як сервера двофакторної автентифікації.

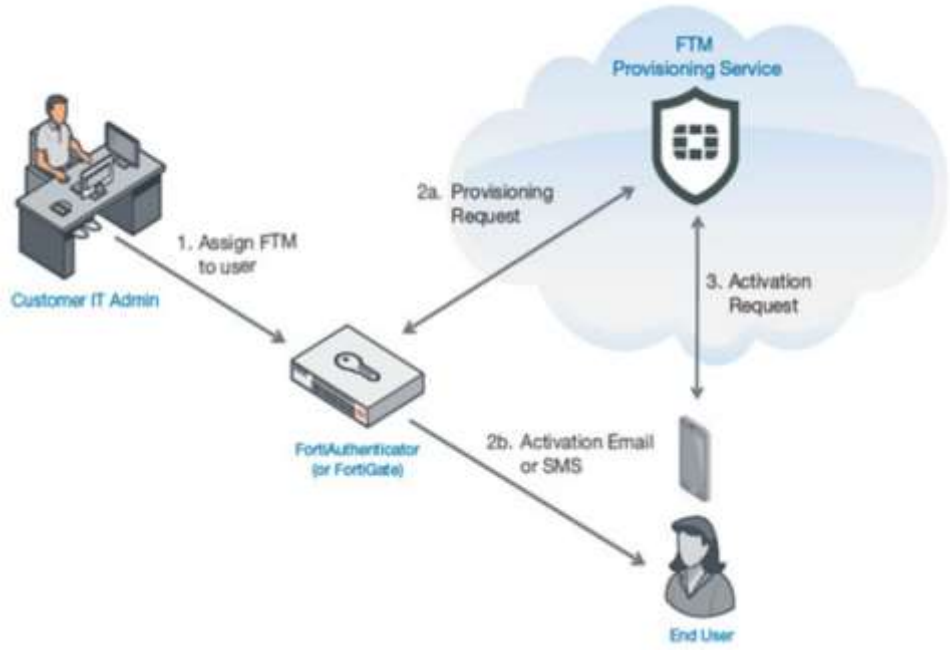

Рис. 2.6. Реалізація двофакторної автентифікації [6]

2.3. Застосування FortiAuthenticator для реалізації автентифікації в корпоративній мережі

Пристрій FortiAuthenticator – це рішення для *управління ідентифікацією та доступом*. Рішення для управління ідентифікацією та доступом є важливою частиною корпоративної мережі, забезпечуючи доступ до захищених мережевих активів та відстежуючи дії користувачів на відповідність політиці безпеки [8].

FortiAuthenticator надає послуги з ідентифікації користувачів в лінійці продуктів Fortinet, а також сторонніх пристроїв.

FortiAuthenticator надає певні функції, включаючи [8]:

автентифікація: FortiAuthenticator включає за протоколами RADIUS (Remote Authentication Dial In User Service), TACACS+ (Terminal Access Controller Access-Control System Plus), LDAP (Lightweight Directory Access Protocol) методи автентифікації сервера та SAML (Security Assertion Markup Language), які використовується для обміну даними автентифікації та авторизації між

постачальником ідентифікаційних даних IdP (Identity Provider) та постачальником послуг SP (Service Provider);

двофакторна автентифікація: FortiAuthenticator може виступати як двофакторний сервер автентифікації з підтримкою одноразових паролів (one-time password, OTP) за допомогою апаратного забезпечення FortiToken, FortiToken Mobile, Short Message Service (SMS) або електронної пошти. Двофакторна автентифікація FortiAuthenticator сумісна з будь-якою системою, що підтримує протокол RADIUS;

підтримка IEEE802.1X: FortiAuthenticator підтримує 802.1X для використання в безпроводових та проводових мережах FortiGate;

ідентифікація користувача: FortiAuthenticator може ідентифікувати користувачів за допомогою кількох джерел даних, включаючи Active Directory (AD), робочий стіл клієнта, вхід гостьового порталу, облік RADIUS, Kerberos та API REST (Representational State Transfer). Потім він може передавати цю інформацію в компоненти FortiGate або FortiMail для використання в політиках на основі ідентифікаційних даних;

керування сертифікатами: FortiAuthenticator може створювати та підписувати цифрові сертифікати для використання, наприклад, у VPN FortiGate та за допомогою магазину сертифікатів FortiToken 300 USB;

інтеграція: FortiAuthenticator може інтегрувати зі сторонніми системами автентифікації RADIUS, LDAP та SAML, що дозволяє повторно використовувати існуючі джерела інформації. API REST також може бути використаний для інтеграції із зовнішніми системами забезпечення.

FortiAuthenticator є критично важливою системою і її слід ізолювати на мережевому інтерфейсі, який відділений від інших хостів, щоб полегшити захист міжмережевого екрану сервера. Необхідно вжити заходів для запобігання несанкціонованому доступу до FortiAuthenticator.

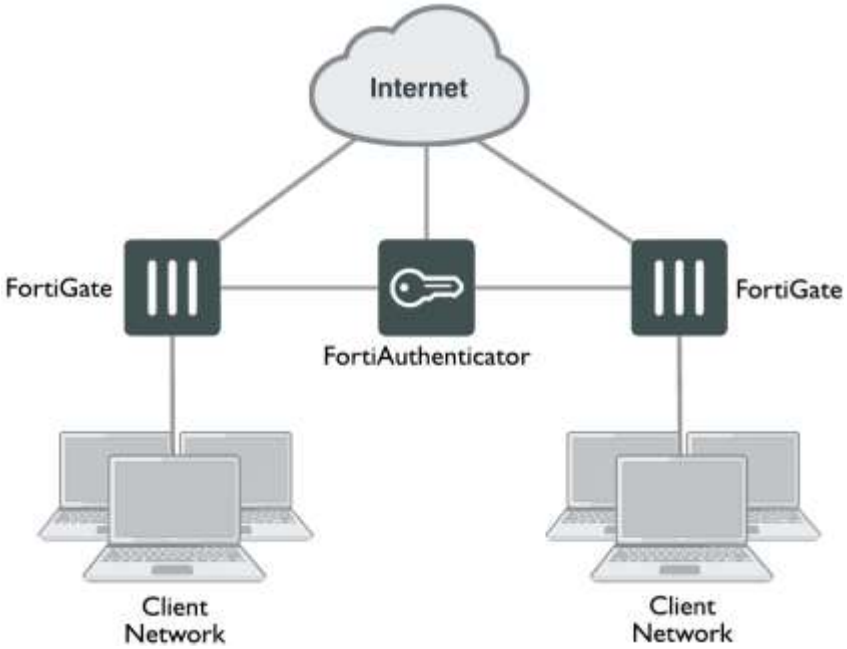

Рис. 2.7. FortiAuthenticator у декількох мережах пристроїв FortiGate [8]

Серія приладів управління ідентифікацією та доступом FortiAuthenticator доповнює лінійку двофакторної автентифікації FortiToken для безпечного віддаленого доступу. FortiAuthenticator дозволяє розширити підтримку FortiTokens на всіх інформаційних системах підприємства, увімкнувши автентифікацію за допомогою декількох пристроїв FortiGate та сторонніх виробників пристроїв. FortiAuthenticator та FortiToken забезпечують економічно вигідну, масштабовану та безпечну автентифікацію для всієї корпоративної мережевої інфраструктури [8].

Пристрій FortiAuthenticator надає просту у налаштуванні опцію віддаленої автентифікації для користувачів FortiGate. Крім того, він може замінити агент Fortinet Single Sign-On (FSSO) в мережі Windows AD [8].

Розглянемо налаштування автентифікації в FortiAuthenticator.

По-переш, необхідно вирішити, які елементи конфігурації FortiAuthenticator потрібні [8]:

необхідно визначити тип автентифікації, який буде використовуватися: на основі пароля або токена. За бажанням можна ввімкнути обидва типи. *Це називається двофакторною автентифікацією*;

необхідно визначити тип сервера автентифікації, який буде

використовуватися: RADIUS, TACACS+, вбудований LDAP або віддалений LDAP. Необхідно буде використовувати принаймні один із цих типів серверів;

необхідно визначити, які компонети FortiGate чи сторонні пристрої використовуватимуть FortiAuthenticator. FortiAuthenticator повинен бути налаштований на кожному блоці FortiGate в якості сервера автентифікації, або RADIUS, або LDAP. Для автентифікації RADIUS кожен FortiGate або сторонній пристрій необхідно налаштувати на FortiAuthenticator як клієнт автентифікації [8].

Автентифікація на основі пароля

Облікові записи користувачів можна створювати на пристрої FortiAuthenticator кількома способами [8]:

адміністратор створює користувача та вказує його ім'я користувача та пароль;

адміністратор створює ім'я користувача і випадковий пароль автоматично надсилається користувачеві;

користувачі створюються шляхом імпортування файлу CSV або із зовнішнього сервера LDAP.

Користувачі можуть самостійно зареєструватися для автентифікація на основі пароля. Це зменшує навантаження для системного адміністратора. Користувачі можуть вибирати власні паролі або мати випадково сформований пароль, який надається у браузері або надсилається їм по електронній пошті або SMS. Самореєстрація може бути миттєвою або вимагати схвалення адміністратора [8].

Після створення користувачі автоматично становляться частиною система автентифікації RADIUS і можуть бути автентифіковані віддалено.

Двофакторна автентифікація

Двофакторна автентифікація підвищує безпеку, вимагаючи декілька відомостей поверх імені користувача та пароля. Як правило, є два фактори [8]:

щось, що користувач знає, як правило, пароль;

щось, що є у користувача, наприклад пристрій FortiToken.

Потребування двох факторів збільшує труднощі для несанкціонованої особи

видати себе за законного користувача.

Щоб увімкнути двофакторну автентифікацію, необхідно налаштувати в обліковому записі користувача автентифікацію на основі пароля та токена.

На основі токена FortiAuthenticator автентифікація вимагає від користувача введення цифрового токена або одноразового пароля (OTP) при вході в систему. Підтримуються два типи числових токенов [8]:

Заснований на часі (TOTP): пароль токена генерується з використанням комбінації часу та секретного ключа, який відомий лише токену та пристрою FortiAuthenticator. Пароль токена змінюється через регулярні проміжки часу і FortiAuthenticator може перевірити введений код доступу, використовуючи час і секретну інформацію про зміст для цього токена.

Паролі можна використовувати лише один раз (одноразові паролі), щоб запобігти повторним атакам. Fortinet має наступні часові токени [8]:

обладнання FortiToken;

FortiToken Mobile, що працює на сумісному смартфоні.

На основі подій або на основі HMAC (HOTP): токен пароль генерується за допомогою тригера події та секретного ключа. Токен подій підтримуються за допомогою дійсного облікового запису електронної пошти та номера мобільного телефону із послугою SMS.

Пристрої FortiToken, додатки FortiToken Mobile, адреси електронної пошти та номери телефонів повинні бути налаштовані в обліковому записі користувача.

Тільки адміністратор може налаштувати автентифікацію на основі токенів.

Двофакторна конкатенація токена та пароля

Клієнт може надати об'єднані паролі та одноразові коди паролів (OTP) у полі пароля, щоб не було другого кроку для введення коду OTP. Це підтримується всіма методами автентифікації на FortiAuthenticator, які також підтримують автентифікацію лише за допомогою пароля.

Сервери автентифікації

FortiAuthenticator має вбудовані сервери RADIUS та LDAP. Він також підтримує використання віддаленого RADIUS та LDAP (що може включати

сервери Windows AD).

Вбудовані сервери найкраще використовувати там, де немає їх інфраструктури автентифікації або коли потрібен окремий набір облікових даних. Необхідно створювати базу даних облікових записів користувачів на FortiAuthenticator. База даних може містити додаткову інформацію про користувача, таку як вуличні адреси та номери телефонів, які неможливо зберегти у базі даних автентифікації користувачів пристрою FortiGate. Для автентифікації можна використовувати LDAP або RADIUS. Параметр віддаленого LDAP додає пристрої FortiGate до існуючої структури LDAP. За бажанням можна додати двофакторну автентифікацію до віддаленого LDAP [8].

Автентифікація за протоколом RADIUS

Якщо використовується RADIUS, то необхідно ввімкнути RADIUS в кожному обліковому записі користувача. Пристрої FortiGate повинні бути зареєстровано як клієнти автентифікації RADIUS у розділі Автентифікація> Служба RADIUS> Клієнти. На кожному пристрої FortiGate, який використовуватиме протокол RADIUS, FortiAuthenticator повинен бути налаштований як сервер RADIUS у розділі Користувачі та пристрій> Сервери RADIUS [8].

Вбудований LDAP

Якщо використовується вбудований протокол LDAP, то потрібно буде налаштувати дерево каталогів LDAP. Необхідно додати користувачів із бази даних користувачів до відповідних вузлів в ієрархії LDAP. На кожному блоці FortiGate, який використовуватиме протокол LDAP, FortiAuthenticator повинен бути налаштований як сервер LDAP у розділі Користувачі та пристрій> Сервери LDAP [8].

Віддалений LDAP

Віддалений LDAP використовується, коли є існуючий каталог LDAP і його слід використовувати для автентифікації. Інформація про користувача може бути вибірково синхронізовано з FortiAuthenticator, але облікові дані користувача (паролі) залишаються увімкненими та перевіряються щодо каталогу LDAP.

Щоб використовувати віддалений LDAP, клієнт автентифікації (наприклад, пристрій FortiGate) повинен підключитися до пристрою FortiAuthenticator за допомогою RADIUS для автентифікації інформації про користувача. Потім пароль надається для перевірки проксі-сервером LDAP, у той час як будь-який пов'язаний пароль токена перевіряється локально.

Розглянемо методи автентифікації.

RADIUS і TACACS+ з PAP, портали користувачів, SAML IdP та REST API [8]:

пароль кінцевого користувача надається FortiAuthenticator як чистий текст;

будь-який тип облікового запису користувача (тобто локальний або віддалений) може автентифікуватися.

RADIUS із CHAP/MSCHAPv2 [8]:

пароль кінцевого користувача надається FortiAuthenticator як хеш-дайджест;

тільки локальні облікові записи користувачів з паролями, що зберігаються за допомогою зворотної криптографії, можуть автентифікуватися.

Машинна автентифікація

Машинна (або комп’ютерна) автентифікація – це функція супліканта Windows, яка дозволяє машині Windows виконувати автентифікацію в мережі через 802.1X до автентифікації користувача.

Машинна автентифікація виконується самим комп’ютером, який надсилає свої облікові дані об’єкта комп’ютера перед тим, як з’явиться екран входу в систему Windows. Автентифікація користувача виконується після входу користувача до Windows [8].

На підставі облікових даних комп'ютера, наданих під час автентифікації машини, може бути наданий обмежений доступ до мережі. Наприклад, доступ може бути наданий лише серверу Active Directory, щоб увімкнути автентифікацію користувачів.

Після машинної автентифікації може відбутися автентифікація користувача, щоб підтвердити, що користувач також є дійсним, а потім надати подальший доступ до мережі.

Автентифікація машини зазвичай відбувається під час завантаження або виходу з системи, а не, наприклад, коли пристрій виходить із режиму глибокого сну. Через це FortiAuthenticator кешує автентифіковані пристрої на основі їх MAC-адрес протягом певного періоду [8].

2.4. Застосування FortiToken для реалізації двофакторної автентифікації

Приклад: двофакторна автентифікація IPsec VPN з FortiToken-200 (рис. 2.8) [7].

У цьому випадку налаштовується двофакторна автентифікація за допомогою FortiToken-200 для підключень IPsec VPN.

Ця конфігурація передбачає, що ви вже створили користувача і групу користувачів (FTK-users). Ви додасте FortiToken-200 в FortiGate, призначите токен користувачеві і додасте користувача в групу. Потім ви скористаєтеся майстром для створення тунелю IPsec VPN, який дозволить користувачам FortiToken-200 отримати безпечний доступ до внутрішньої мережі та Інтернету. Ви протестуєте настройку, надавши користувачу доступ до VPN з віддаленого пристрою за допомогою FortiClient.

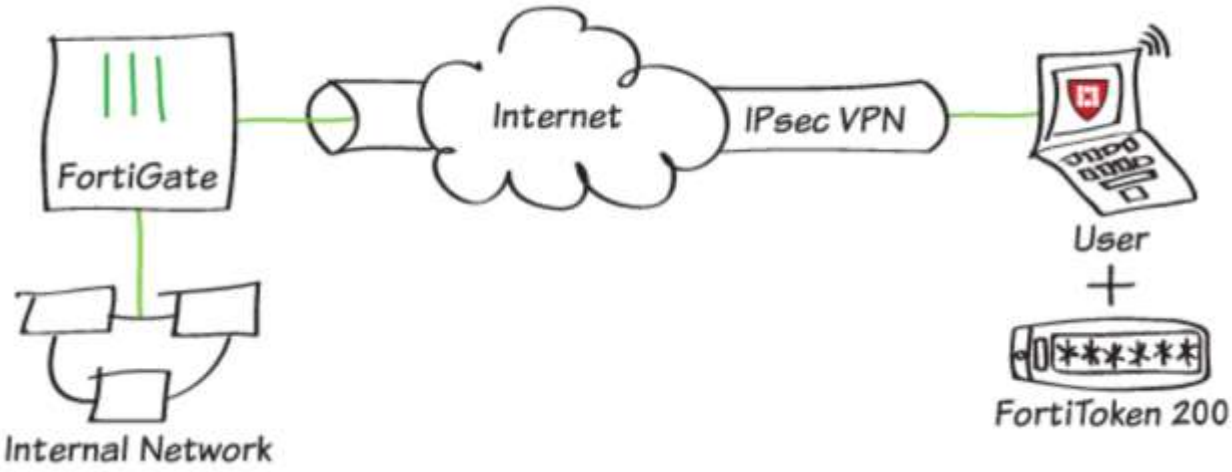

Рис. 2.8. Схема двофакторної автентифікації IPsec VPN з FortiToken-200 [7]

Приклад: доступ до адаптивного порталу Wi-Fi за допомогою FortiToken-200 (рис. 2.9) [7].

У цьому сценарії ви будете застосовувати двухфакторную аутентифікацію для користувачів Wi-Fi, у яких є пристрої FortiToken-200, через прихований портал. Користувачі FortiToken-200, які спробують вийти в Інтернет, будуть перенаправлені на сторінку входу в портал авторизації і попросять ввести своє ім'я користувача, пароль і шестизначний код аутентифікації.

У цьому сценарії припускається, що у вас вже є пристрій FortiAP, підключений і авторизоване до FortiGate, і що SSID був налаштований і налаштований для використання адаптивного порталу. Щоб дізнатися, як налаштувати бездротову мережу за допомогою адаптивного порталу, см. Конфігурацію нашої онлайн-книги рецептів: Управління доступом Wi-Fi на адаптивному порталі.

Ця конфігурація призначена для генератора фізичних ключів FortiToken-200. Див. Крок 2 для отримання інформації про використання FortiToken Mobile.

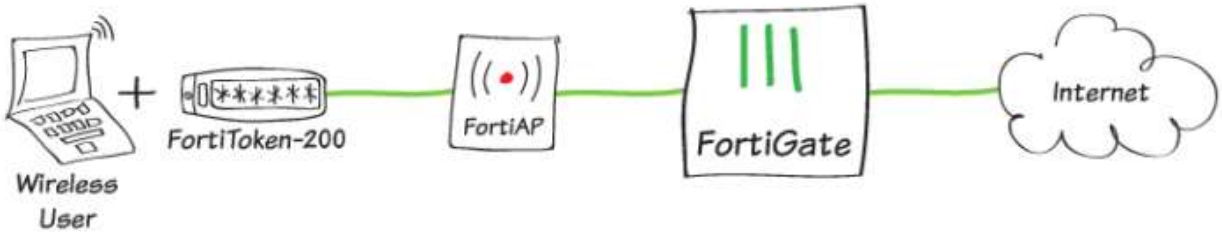

Рис. 2.9. Схема доступу до адаптивного порталу Wi-Fi за допомогою FortiToken-200 [7]

Приклад: двофакторна автентифікація FortiToken з RADIUS на FortiAuthenticator (рис. 2.10) [7].

У цьому сценарії ви налаштуєте FortiAuthenticator для роботи в якості сервера RADIUS, щоб дозволити користувачам SSL VPN аутентифицироваться за допомогою FortiToken-200.

У цьому сценарії припускається, що ви вже додали FortiToken, призначили його користувачеві і додали користувача в групу для користувачів FortiToken на FortiAuthenticator.

Ви налаштуєте користувача FortiToken-200, клієнта RADIUS на FortiAuthenticator і FortiGate для використання FortiAuthenticator як сервер

RADIUS. Потім ви створите тунель SSL VPN.

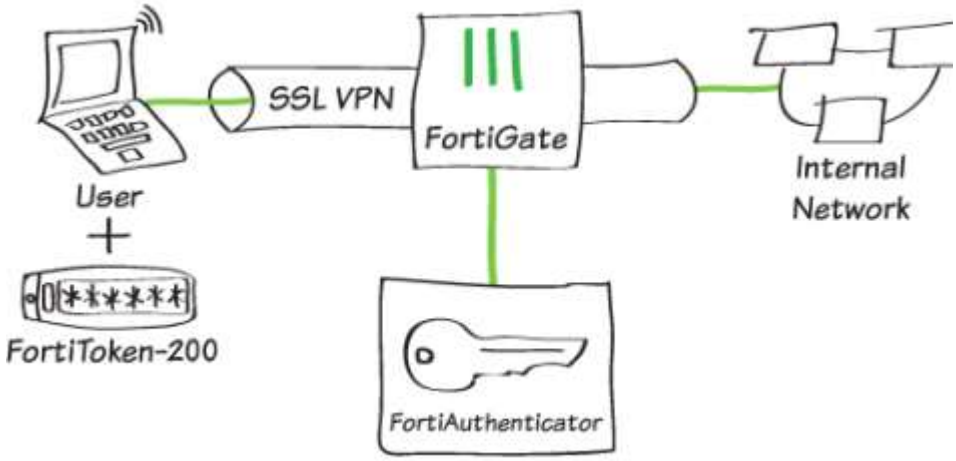

Рис. 2.10. Схема двофакторної автентифікації FortiToken з RADIUS на FortiAuthenticator [7]

3 РОЗРОБЛЕННЯ РЕКОМЕНДАЦІЙ ЩОДО УПРАВЛІННЯ ІДЕНТИФІКАЦІЄЮ ТА ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ПІДПРИЄМСТВА

3.1. Рекомендації із застосування рішень Fortinet в IAM-системі підприємства

Управління ідентифікацією і правами доступу при забезпеченні простої автентифікації, доступності додатків і оптимальної взаємодії з кінцевими користувачами стає все більш складним завданням в швидко мінливому бізнес-середовищі і IT-середовищі. Ці проблеми посилюються змінами суспільства і бізнесу через пандемію COVID-19. В результаті співробітники багатьох організацій стали ще більш віддаленими і мобільними [11].

Забезпечення ефективних прав доступу для кожного користувача для захисту організації від кіберзлочинців має розвиватися. Вони повинні не відставати, оскільки кордони організації швидко переміщуються з захищених периметрів мережі на нову філію домашнього офісу [11].

Згідно DBIR Verizon 2020 року, паролі залишаються слабкою ланкою. Використання вкрадених облікових даних займає перше місце серед хакерських атак, а шкідливе ПЗ для скидання паролів знаходиться в списку найбільш небезпечних дій [11].

Рішення Fortinet для управління ідентифікацією і доступом (IAM) дає організаціям можливість централізовано контролювати і управляти життєвим циклом доступу користувачів до критично важливої інформації як в хмарі, так і локально. Воно забезпечує надійну автентифікацію за рахунок використання багатофакторної автентифікації (MFA) для підтвердження особи, контрольних журналів для відповідності нормативним вимогам, єдиного входу кінцевого користувача (SSO) до різних ресурсів без повторної автентифікації для підвищення безпеки при одночасному поліпшенні роботи кінцевого користувача та управління сертифікатами X.509 для підключення гостей і політик

використання власного пристрою (BYOD) [11].

Рішення Fortinet IAM є в фізичному, віртуальному та хмарному форм-факторах для розгортання локально або в хмарі, яке відповідає бізнес-потребам організації.

Рішення для розрізнених систем управління доступом. Більшість організацій використовують безліч розрізнених систем в різних відділах для управління співробітниками, підрядниками, партнерами, ідентифікаційними даними гостей і доступом до даних. Наприклад, відділ кадрів може використовувати різні програмні рішення для ідентифікації співробітників і підрядників і надання доступу до різних ресурсів. Відділ маркетингу може бути інтегрований зі сторонніми партнерськими програмами та використовувати різне програмне забезпечення для аналізу і виконання даних і робочих процесів на основі даних про ідентичність користувачів, зібраних в рамках спільних партнерських ініціатив. Тим часом IT-відділ може використовувати кілька систем, в тому числі кілька систем IAM, для забезпечення безпечного доступу до організації для безлічі користувачів і пристроїв [11].

В цілому, кількість розрізнених систем і результуючі розрізнені дані, розміщені на сучасному підприємстві, викликають тривогу. Розрізнені системи не тільки створюють виснажливий, неуніфікований досвід для кінцевих користувачів, але і підвищують ризик і ускладнюють оцінку ризиків. Крім того, управління розрізненими системами вимагає від IT-фахівців значної кількості часу і ресурсів [11].

Ефективна система IAM забезпечує централізовану автентифікацію, єдиний вхід і примусову авторизацію для цільових програм, розміщених локально або в хмарі. Ці та аналогічні функції спрощують IT-операції, адміністрування та обслуговування, усувають ризики непередбачених розривів між системами і забезпечують безпечний доступ для організації, забезпечуючи при цьому узгоджені і поліпшені можливості для кінцевих користувачів в процесі автентифікації і входу в систему.

Організації по всьому світу і у всіх вертикалях все частіше використовують

рішення Fortinet IAM.

Fortinet IAM складається з FortiAuthenticator, FortiToken і FortiToken Cloud – рішення «MFA-as-a-service», яке допомагає організаціям впроваджувати і впроваджувати передові методи IAM.

Fortinet IAM: FortiAuthenticator – джерело ідентифікації з централізованим управлінням. У центрі Fortinet IAM знаходиться FortiAuthenticator. FortiAuthenticator функціонує як джерело ідентифікації організації і глибоко інтегрований в Fortinet Security Fabric.

FortiAuthenticator підсилює доступ користувачів в організації за рахунок спрощення та централізації управління життєвим циклом і зберігання ідентифікаційної інформації користувачів, отриманої з різних систем запису. Завдяки інтеграції з існуючими системами автентифікації Active Directory (AD), Lightweight Directory Access Protocol (LDAP) або хмарними сховищами посвідчень, FortiAuthenticator забезпечує автентифікацію користувачів, включаючи MFA, сертифікаційну та адаптивну автентифікацію, а також елементи керування єдиним входом для організацій, щоб забезпечити ідентифікацію та забезпечити права доступу для всіх користувачів, у будь-який час та з будь-якого місця, будь то через корпоративну проводову, безпроводову мережу або віддалену віртуальну приватну мережу (VPN) з'єднання.

FortiAuthenticator підтримує високу доступність (HA), що забезпечує безперервність і відмовостійкість бізнесу. Розгортання високої доступності просте і працює без проблем під час аварійного перемикання, будь то для обслуговування або під час несподіваного збою. FortiAuthenticator також включає параметри самостійної реєстрації користувачів і відновлення пароля, що дозволяють користувачам скидати свій пароль без звернення до служби підтримки, що може дати значну економію коштів для багатьох організацій.

FortiAuthenticator доступний для розгортання локально, в віртуальному середовищі або через загальнодоступну хмару. Ліцензування FortiAuthenticator має просту структуру, що передбачає постійні, одноразові витрати на всі функції. Звіти FortiAuthenticator також дозволяють легко продемонструвати рентабельність

інвестицій (ROI) протягом усього процесу прийняття рішення і розгортання.

Завдяки гнучким форм-факторам FortiAuthenticator організації можуть вибрати будь-який метод розгортання, який найкраще відповідає їх ініціативам і бюджетам IAM. Завдяки інтегрованому набору рішень і потужним механізмам організації можуть щорічно економити понад 50% в порівнянні з альтернативними рішеннями.

FortiAuthenticator захищає доступ користувачів за допомогою розширених, оптимізованих функцій управління доступом для посвідчень, таких як централізована політика доступу користувачів, управління привілеями користувачів, MFA, SSO, контрольні журнали і багато іншого. За рахунок підвищення захисту доступу користувачів FortiAuthenticator ускладнює зловмисникам крадіжку облікових даних, видачу себе за користувачів або пристрої та отримання несанкціонованого доступу до додатків або мережевих ресурсів. Крім того, його централізоване управління спрощує IT-операції і скорочує непередбачені проломи в безпеці, які можна не помітити при управлінні непов'язаними системами IAM.

Fortinet IAM: FortiToken – комплексний варіант для MFA. MFA – важлива функція безпеки для будь-якого рішення IAM, оскільки вона вимагає перевірки декількох облікових даних. MFA повинна включати як мінімум два з наступного [11]:

щось, що знає користувач: ім'я користувача і пароль;

щось, що є у користувача: одноразовий пароль (OTP) у вигляді токена або коду. Він відправляється користувачеві по електронній пошті або SMS на апаратний генератор токенів або в додаток для перевірки автентичності, встановлене на смартфоні користувача;

щось специфічне для користувача: біометрична інформація, така як відбиток пальця користувача, розпізнавання особи або сканування райдужної оболонки ока.

FortiToken (FTK) пропонує широкий спектр токенів OTP і сценаріїв використання MFA для задоволення потреб будь-якої організації. FTK також

поставляється в різних форм-факторах:

додаток: засноване на часі і зручне для користувача, з PUSH для прийому/відхилення облікових даних під час процесу MFA. Він підтримує платформи iOS або Android;

автономний: фізичний пристрій з захистом від несанкціонованого доступу з OTP на основі часу. Ці маркери бувають у вигляді USB-накопичувача, половинного розміру кредитної картки або невеликого розміру зв'язки ключів, кожен з яких має великий екран для відображення токена;

жетони електронної пошти та SMS: активація токена може бути виконана онлайн або офлайн (що робить її придатною для закритих середовищ). FTK також можуть передаватися між пристроями автентифікації, такими як FortiGate або FortiAuthenticator, або між мобільними пристроями (наприклад, iOS або Android). Це забезпечує видимість, спрощує управління двофакторною автентифікацією і підвищує безпеку для захисту організацій від зловмисників, які шукають несанкціонований доступ (навіть якщо у кіберзлочинця є ім'я користувача і пароль, вони не можуть отримати доступ до системи без іншої інформації).

FortiAuthenticator пропонує варіанти токенів для всіх користувачів і сценаріїв для підтвердження особи користувача за допомогою MFA. Завдяки централізованому управлінню FortiAuthenticator і FTK надають організаціям можливість гарантувати ідентифікацію та контролювати доступ користувачів до корпоративних VPN, мережевих пристроїв і ресурсів, а також локальним або хмарним додаткам.

Fortinet IAM: FortiToken Cloud – хмарне «MFA-as-a-Service». FortiToken Cloud (FTC) надає все необхідне для впровадження та управління багатофакторної автентифікації в середовищі FortiGate або FortiAuthenticator. Ніякого додаткового обладнання або програмного забезпечення автентифікатора не потрібно, а також будь-яких змін існуючої політики безпеки на FortiGate або FortiAuthenticator. FTC – це послуга підписки, доступна при покупці балів. Бали FTC можуть легко збільшуватися в міру зміни потреб організації. Завдяки інтуїтивно зрозумілій панелі інструментів організації можуть отримати зведення

корисних показників, таких як спільне використання, активні користувачі, що залишилися точки і журнали, в яких фіксується основна інформація як про активні, так і закриті сеанси [11].

FortiToken Cloud полегшує організаціям впровадження MFA, розширюючи ідентифікацію користувача за рахунок перевірки того, що у користувача є. MFA ускладнює доступ зловмисників до корпоративних ресурсів, навіть якщо у них є і використовуються вкрадені облікові дані, а це основні дії по злому і основні дії по загрозам, які призводять до порушень мережі.

Fortinet – визнаний лідер в області мережевих технологій і технологій кібербезпеки. Рішення Fortinet IAM – відмінне рішення для організацій. Воно надає правильні інструменти IAM в поєднанні з перевагами гнучкого розгортання, щоб надати права доступу для кожного користувача, в кінцевому підсумку захищаючи бізнес від порушень кібербезпеки. Той факт, що він забезпечує управління життєвим циклом і централізовані операції, адміністрування та обслуговування, а також простоту використання для кінцевих користувачів, робить Fortinet IAM легким вибором для передових методів організації IAM [11].

3.2. Рекомендації щодо впровадження системи управління доступом на підприємстві

Для ефективного впровадження системи управління доступом на підприємстві необхідно враховувати розмір та тип бізнесу. Системи IAM життєво важливі для бізнесу для автоматичного управління ідентифікацією та привілеями доступу користувачів у різних місцях, обчислювальних середовищах та на декількох пристроях. Системи IAM однаково ефективні як для великих підприємств, так і для середнього та малого бізнесу. Для організацій та підприємств різного розміру доступні рішення для вибору інструментів, що спрощують доступ користувачів, скасовують опору на паролі та автентифікують користувачів, де б вони не знаходились та на будь-якому пристрої.

Необхідно створити стратегію інтеграції IAM. Загальними ризиками, пов’язаними з впровадженням IAM, є інтеграція рішення з існуючими рішеннями,

перехід до хмари та співробітники, які використовують продукти та інструменти, не схвалені організацією, також відомою як Shadow IT. Цього можна уникнути, повністю прийнявши перехід до IAM, витративши час і зусилля на створення цілісної стратегії управління ідентичністю та заохочуючи співпрацю у бізнесі.

Необхідно знаходити та застосовувати правильні рішення IAM. До найважливіших компонентів системи IAM належать:

доступ до продуктів управління, які визначають і керують ідентифікацією користувачів і вмикають такі інструменти, як єдиний вхід для хмарних, мережевих та веб-ресурсів;

процеси автентифікації, такі як багатофакторна автентифікація та автентифікація на основі ризиків, які допомагають користувачам легко перевірити свою особу;

токени паролів, які додають додатковий захист простому використанню паролів.

Збільшення хмарних додатків та підключених пристроїв змінило наш спосіб роботи. Це також розширило поверхню атаки, надавши кіберзлочинцям більше можливостей для цілеспрямованих атак. Щоб уникнути порушень, організації повинні забезпечити доступ правильних користувачів до потрібних мережевих ресурсів.

Fortinet User Authentication надає інструменти та можливості для ефективного управління ідентифікацією та автентифікацією користувачів, пристроїв та гостей чи партнерів. Гнучкі варіанти розгортання дозволяють вибрати найкращий спосіб розгортання рішення залежно від потреб підприємства. Необхідно обирати відповідне рішення: локальне готове до використання обладнання, віртуальну машину, керовану хмару або ідентифікацію як послугу (IDaaS). Необхідно інтегрувати рішення Fortinet IAM із існуючою інфраструктурою автентифікації, такою як активний каталог (AD) або LDAP, або з новими службами через постачальників хмарних послуг [4].

Застосовуйте багатофакторну автентифікацію (MFA) для підвищення безпеки корпоративних даних. Надання безпечного доступу до програм, послуг

або розробки програмного забезпечення, розміщених локально або в хмарі, і одночасно пропонуючи зручність використання для кінцевих користувачів, є постійною проблемою.

Можна значно ускладнити отримання хакерами доступу до захищеної інформації, використовуючи додаткові облікові дані, такі як одноразовий пароль (OTP). OTP є одним із компонентів MFA. MFA є важливою функцією безпеки будь-якого рішення IAM, оскільки вимагає перевірки кількох облікових даних [4].

Fortinet MFA забезпечує простий у використанні захищений доступ до корпоративних VPN, Wi-Fi, локальних або хмарних додатків. Користувачі можуть швидко ввійти в систему, реагуючи на push-повідомлення на своєму смарт-пристрої під час процесу автентифікації.

Підвищити безпеку корпоративних даних та забезпечити легший доступ для користувачів можна за допомогою єдиного входу (SSO).

Централізоване управління ідентифікаторами користувачів та їх доступом до організаційних ресурсів є найефективнішою практикою управління ідентифікацією та доступом (IAM). За допомогою централізованого рішення IAM IT-адміністратори можуть виконувати вимоги щодо складності паролів та багатофакторну автентифікацію. Крім того, Fortinet IAM забезпечує кращу взаємодію з користувачем при доступі до сервісів та програм у хмарі або в приміщенні [4].

Єдиний вхід (SSO) – це ключовий компонент IAM (рис. 3.1), який дозволяє користувачам надійно автентифікуватися за допомогою декількох програм та веб-сайтів, увійшовши лише один раз.

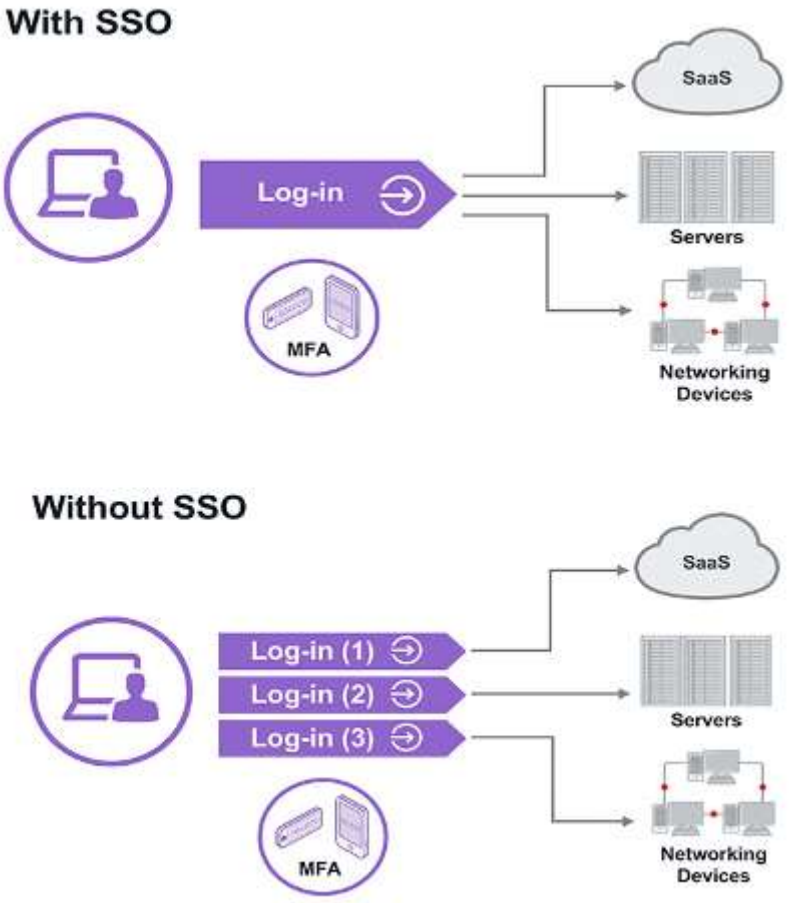

Рис. 3.1. Переваги SSO [4]

Однак не всі рішення SSO будуються однаково. Деякі провайдери пропонують рішення SSO для веб-програм, а інші використовують загальнодоступну хмарну інфраструктуру. Однак інші рішення SSO розроблені для локальних служб, включаючи програми, сховище файлів, сервери та мережі. Одноосібне рішення веб-додатку SSO є неефективним для ефективної безпеки ідентичності, оскільки хмарна інфраструктура та локальні служби матимуть різні вимоги до єдиного входу. Як результат, управління та об'єднання ідентифікаційних даних в основному залишатиметься децентралізованим і потребуватиме зусиль щодо інтеграції різних рішень SSO, щоб забезпечити справжні можливості SSO [4].

Fortinet FortiAuthenticator забезпечує комплексний підхід до єдиного входу за допомогою централізованого управління ідентифікацією. Він автентифікує користувачів за допомогою традиційних локальних, а також сучасних веб- і

хмарних протоколів автентифікації. Для отримання повний контролю за доступом необхідно підключити користувачів до відповідних ресурсів у хмарі або в своїй інфраструктурі, одночасно покращуючи їх досвід.

ВИСНОВКИ

В роботі проведено дослідження та аналіз проблеми забезпечення безпечного доступу користувачів до корпоративних даних.

Проаналізовано існуючі загрози безпечному доступу користувачів до корпоративних даних. Встановлено, що більше 80% порушень безпеки є результатом використання вкрадених облікових даних або застосування методу грубої сили. Дане положення ускладнено пандемія COVID-19, що зумовило широке застосування віддаленої роботи працівників організацій та підприємств.

Визначено зміст проблеми управління ідентифікацією та доступом до інформаційної системи підприємства. Системи IAM допомагають організаціям привести безпеку і конфіденційність даних у відповідність до нормативних вимог. Підприємства можуть використовувати методи IAM, такі як єдиний вхід (SSO), багатофакторна автентифікація (MFA), управління доступом на основі ролей (RBAC) і «правило найменших привілеїв» (надання користувачам та об'єктам, таким як програмні додатки, мінімального обсягу доступу, необхідного для виконання завдання), щоб відповідати вимогам регуляторів.

Досліджено існуючі методи та засоби управління ідентифікацією та доступом до інформаційної системи підприємства на прикладі рішень FortiAuthenticator 200E та FortiToken 200 series. Основне призначення рішення FortiAuthenticator – управління доступом з функцією ідентифікації для адаптивної системи мережевої безпеки. FortiAuthenticator підтримує функції, які забезпечують ефективну реалізацію політик безпеки і підвищують рівень захищеності мережі. Доступ до конфіденційних мереж і даних при необхідності зможуть отримати тільки користувачі з відповідними повноваженнями.

Перевірка справжності виключно за допомогою пароля може спричинити за собою порушення безпеки, зараження шкідливим ПЗ і проблеми реалізації політик. Двофакторна перевірка справжності передбачає використання пароля спільно з токеном і сервером перевірки автентичності, що істотно підвищує

рівень захисту. Авторизовані співробітники отримують захищений доступ до корпоративних ресурсів за допомогою різних пристроїв: від ноутбуків до мобільних телефонів. Серія FortiToken 200 включає доступні за ціною і зручні в експлуатації апаратні токени, призначені для застосування в середовищах, які потребують ефективної перевірки автентичності.

Запропоновано рекомендації із застосування рішень Fortinet в IAM-системі підприємства.

Розроблено рекомендації керівникам підприємств та фахівцям з кібербезпеки щодо впровадження системи управління доступом на підприємстві.

Таким чином, запропоновані в роботі рекомендації мають сприяти ефективному створенню та функціонуванню системи управління ідентифікацією та доступом до інформаційної системи підприємства.

ПЕРЕЛІК ПОСИЛАНЬ

1. Designing a modern IAM program for your business. IBM Security [Електронний ресурс] – Режим доступу: https://www.ibm.com/downloads/cas/9YBEK41O.

2. Identity Management (IDM) and Access Management (AM) [Електронний ресурс] – Режим доступу: https://www.efecte.com/about-iam.

3. What is Identity and Access Management (IAM)? [Електронний ресурс] – Режим доступу: https://www.fortinet.com/resources/cyberglossary/identity-and-access-management.

4. Identity and Access Management Use Cases [Електронний ресурс] – Режим доступу: https://www.fortinet.com/products/identity-access-management?tab=models-specs#usecases.

5. FortiAuthenticator. Data Sheet [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiAuthenticator.pdf.

6. FortiToken One-Time Password Token. Data Sheet [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortitoken.pdf.

7. FortiToken – Comprehensive Guide. Version 4.5.3 [Електронний ресурс] – Режим доступу: https://fortinetweb.s3.amazonaws.com/docs.fortinet.com/v2/attachments/a3e2887c-20eb-11e9-94bf-00505692583a/ftk-admin-guide.pdf.

8. FortiAuthenticator 6.2.1 Administration Guide [Електронний ресурс] – Режим доступу: https://docs.fortinet.com/document/fortiauthenticator/6.2.1/administration-guide/473473/whats-new-in-fortiauthenticator.

9. Role Based Access Control. ANSI INCITS 359-2004 [Електронний ресурс] – Режим доступу:

https://www.cs.purdue.edu/homes/ninghui/readings/AccessControl/ANSI+INCITS+359-2004.pdf.

10. The State of Zero Trust Security in Global Organizations. Identity and access management maturity in 2020 [Електронний ресурс] – Режим доступу: https://www.okta.com/sites/default/files/pdf/zero-trust-security-in-global-org.pdf.

11. Identity and Access Management (IAM). Advanced Practices with Fortinet [Електронний ресурс] – Режим доступу: https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-identity-and-access-management.pdf.

12. The Future Of Identity And Access Management Vision: The Identity And Access Management. Playbook by Andras Cser and Merritt Maxim June 26, 2019 [Електронний ресурс] – Режим доступу: https://sectigo.com/uploads/resources/The-Future-Of-Identity-And-Access-Management.pdf.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)