ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розроблення рекомендацій щодо управління привілейованим доступом інформаційної системи організації на базі рішення Delinea»

на здобуття освітнього ступеня бакалавра
зі спеціальності ____*125 Кібербезпека*_____
(код, найменування спеціальності)
освітньо-професійної програми _*Інформаційна та кібернетична безпека*_
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ Ігор БРИКСА

Виконав: здобувачка вищої освіти групи БСД-43
БРИКСА Ігор
(ПРІЗВИЩЕ, Ім'я)

Керівник: КУЗНЕЦОВ Олександр
д.т.н, професор (ПРІЗВИЩЕ, Ім'я)

Рецензент: ВИШНІВСЬКИЙ Віктор
д.т.н., професор (ПРІЗВИЩЕ, Ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

PUM - управління привілейованими користувачами

PIM - управління привілейованою ідентифікацією

PAM - управління привілейованим доступом

PTA - привілейована аналітика загроз

ВСТУП

Актуальність дослідження. Управління привілейованим доступом (PAM) має вирішальне значення для організацій, щоб покращити кібербезпеку та захистити конфіденційні дані та критично важливі системи. Впровадження технології привілейованого доступу може зменшити внутрішні загрози в організаціях. Це може бути досягнення за рахунок обмеження доступу до конфіденційних систем і даних лише авторизованим особам. Це зменшує ризик навмисного чи ненавмисного зловживання працівниками або підрядниками своїми привілеями.

Технологія управління привілейованого доступу зменшує поверхню атаки зодо заовнішньої загрози. Зовнішні зловмисники часто націлюються на привілейовані облікові записи, оскільки вони забезпечують шлях до конфіденційної інформації та критичних систем організації. PAM допомагає захищати та контролювати ці облікові записи, що ускладнює компрометацію системи для зовнішніх загроз.

Сьогодні організації повинні відповідати вимогам закону, таким як Закон України «Про захист персональних даних», GDPR, та PCI DSS, які зобов'язують запровадити жорсткий контроль доступу та моніторинг. PAM допомагає організаціям відповідати цим вимогам відповідності, запроваджуючи найменш привілейований доступ і зберігаючи контрольний слід привілейованих дій.

Крім цього PAM використовує принцип найменших привілеїв, гарантуючи, що користувачі мають лише мінімальний рівень доступу, необхідний для виконання своїх робочих функцій. Це зменшує поверхню атаки та обмежує потенційний вплив інцидентів безпеки.

Рішення PAM надають надійні функції обліковими обліковими записами, такі як зберігання, ротація та розподіл привілейованих облікових записів. Це допомагає запобігти неавторизованому доступу через скомпрометовані або витік облікових записів.

Особливістю використання технології PAM є можливість відстежувати та записувати привілейовані сеанси в реальному часі. Це не тільки допомагає виявляти підозрілу діяльність, але й забезпечує виявлення кіберслідів для розслідування інцидентів безпеки.

Впровадження PAM зменшує ризик несанкціонованого доступу, зловживання привілеями та витоку даних. Контролюючи та відстежуючи привілейований доступ, організації можуть проактивно виявляти та усунути загрози безпеці до їх ескалації.

Таким чином, можна стверджувати що управління привілейованим доступом відіграє велике значення для підтримки надійної безпеки інформаційної системи організації, відповідності вимогам і захисту від широкого спектру внутрішніх і зовнішніх загроз. Тому тема кваліфікаційної роботи на освітній ступінь «Магістра» є актуальною.

Об'єкт дослідження –управління привілейованим доступом до інформаційної системи організації.

Предмет дослідження – методи та засоби управління привілейованим доступом до інформаційної системи організації на прикладі рішення Delinea.

Мета роботи – розробити варіант розгортання управління привілейованим доступом до інформаційної системи організації на базі рішення Delinea та рекомендації щодо застосування рішення в інформаційній системі організації.

Наукові завдання:

- провести аналіз проблеми управління привілейованим доступом до інформаційної системи організації;
- проаналізувати основні загрози інформаційній системі організації;
- провести аналіз існуючих рішень щодо управління привілейованим доступом до інформаційної системи організації;
- проаналізувати методи та засоби управління привілейованим доступом до інформаційної системи організації на базі рішення Delinea;

- розробити варіант розгортання управління привілейованим доступом до інформаційної системи організації на базі рішення Delinea та рекомендації щодо застосування даної технології.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання процесу управління привілейованим доступом до інформаційної системи організації.

Практичне значення одержаних результатів полягає в розробці технології управління привілейованим доступом до інформаційної системи організації на базі рішення Delinea та рекомендації фахівцям з кібербезпеки щодо застосування технології в інформаційній системі організації.

Апробація результатів. Результати даного дослідження доповідались на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ПРОБЛЕМИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ ДО ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЙ

1.1. Аналіз змісту поняття привілейованого доступу до інформаційної системи організації

Привілейований доступ до інформаційної системи організації відноситься до рівня доступу, який надає користувачеві розширені або спеціальні права для виконання певних операцій або функцій в системі, які не доступні звичайним користувачам. Це може включати доступ до конфіденційної інформації, можливість внесення змін в налаштування системи, керування правами доступу і т.д.

Користувачі з привілейованим доступом, як правило, включають адміністраторів системи, які відповідають за її конфігурацію, безпеку, резервне копіювання і загальний нагляд. Вони можуть мати повний доступ до всіх ресурсів системи, включаючи файли, бази даних, мережеві налаштування тощо.

Важливо зазначити, що доступ з привілеями повинен бути обмеженим і контрольованим. Це забезпечить безпеку інформаційної системи та запобігатиме можливості зловживання адміністративними привілеями. Для цього можуть застосовуватися методи аутентифікації та авторизації, а також ведення журналів дій користувачів з привілеями для виявлення ненормальної або небезпечної активності.

Сьогодні будь-яка компанія для своєї роботи має свою інфраструктуру на бізі якої працює інформаційна система (рис 1.1). Таку архітектуру можна представити як декілька рівнів. Для кожного рівня можуть бути різні користувачі. З визначених користувачів такої інфраструктури повинні бути користувачі, які є її адміністраторами і мають спеціальні права. Тобто у таких користувачів є вищі привілеї доступу, ніж у звичайного працівника компанії. Отже надалі спробуємо надати зміст поняття привілейованого доступу до інформаційної системи організації.

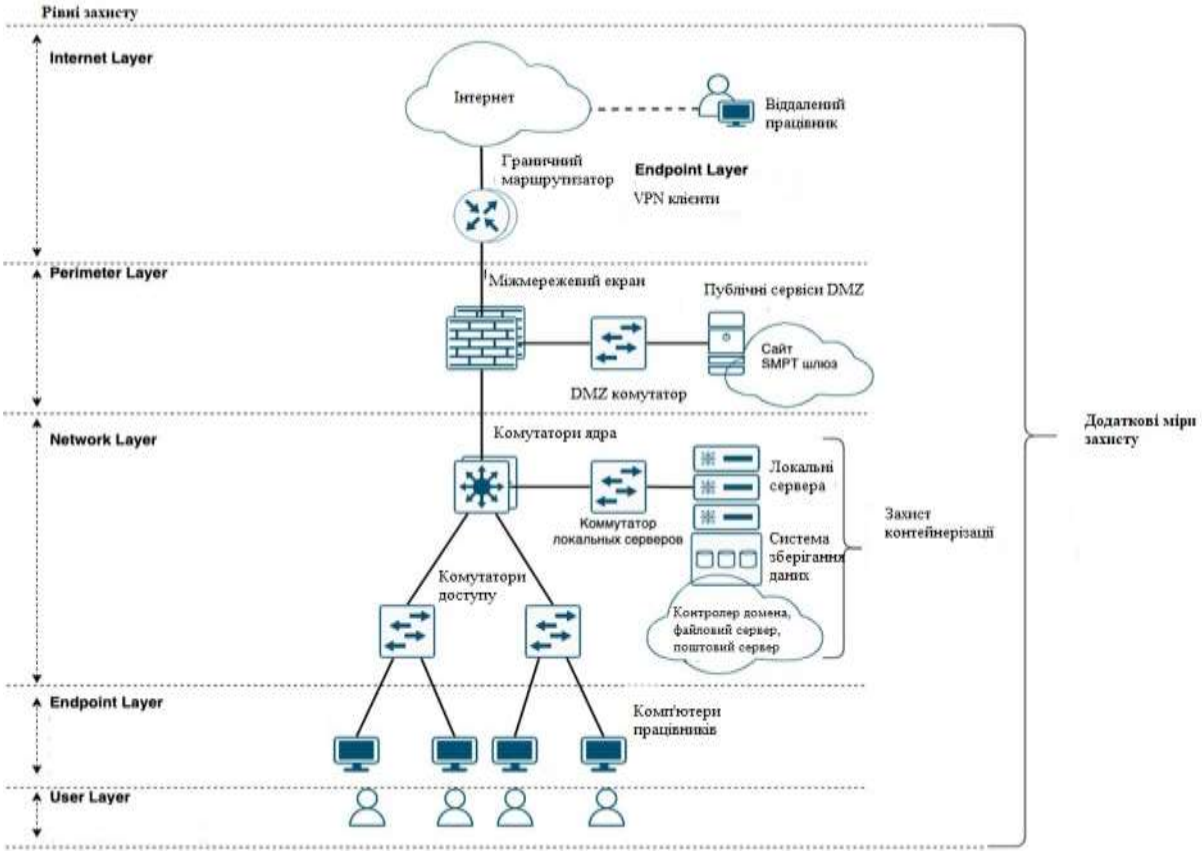

Рис.1.1. Архітектура інформаційної системи організації

Управління привілейованими користувачами, яке іноді називають PUM — це процес управління обліковими записами привілейованих користувачів, пов’язаних із певними активами. [1, 9]

Іноді PUM є синонімом управління привілейованою ідентифікацією (PIM). В обох випадках привілейований обліковий запис не пов’язано з конкретною особою, а скоріше є цифровою ідентифікацією, яку можна передати.

Привілейовані облікові записи покладаються на облікові дані для контролю доступу та поведінки. Створюючи та зберігаючи привілейовані облікові дані (паролі, ключі та секрети) у безпечному сховищі та керуючи ними, рішення PAM контролюють авторизований доступ користувача, процесу чи систем до захищених ресурсів у IT-середовищі.[1]

PAM включає рішення для управління повним життєвим циклом усіх типів привілейованих облікових записів, від виявлення до надання та зміни, а також виведення з експлуатації. За допомогою PAM компанії можуть впроваджувати рівні доступу, включаючи затвердження, моніторинг сеансів та запис. Аналітика корпоративного рівня та реагування на інциденти, включені в комплексний PAM, дозволяють звітувати про відповідність аудиторам і керівникам, а також підтримувати спільну роботу команди IT і безпеки, щоб запобігти атакам на кібербезпеку привілеїв і реагувати на них.

Управління привілейованим доступом (PAM) містить інструменти контролю безпеки та керування політикою для управління та контролю доступу до привілейованих облікових записів, робочих станцій і серверів. Привілейовані облікові записи - це облікові записи з підвищеними дозволами, наприклад облікові записи адміністратора. PAM контролює, хто може використовувати ці облікові записи для виконання критично важливих завдань, таких як встановлення програмного забезпечення, внесення змін до налаштувань системи або доступ до конфіденційних даних.

Ось ключові терміни, які потрібно знати, щоб зрозуміти зміст поняття PAM.

Індустрія PAM почалася з основних можливостей управління привілейованими обліковими записами. Управління привілейованими обліковими записами – це процес IT-безпеки за допомогою програмного забезпечення на основі політик і політик для контролю того, хто може отримати доступ до конфіденційних систем і інформації.

Привілейовані облікові записи покладаються на секрети (паролі, ключі та сертифікати) для контролю доступу. Створюючи, зберігаючи та керуючи цими секретами в захищеному сховищі, засоби керування привілейованими обліковими записами дозволяють авторизувати доступ привілейованого користувача або ідентифікатора машини до захищених ресурсів у IT-середовищі.

З перших днів PAM стратегії привілейованої безпеки розширилися, а загальне визначення PAM змінилося. Сьогодні більшість людей визначають PAM як керування

привілейованим доступом . Це визначення PAM відображає ширшу категорію безпеки, ніж керування привілейованим обліковим записом . Він визначає не лише те, які люди та системи можуть отримати доступ до привілейованого облікового запису, а й те, що вони можуть робити після входу в систему.

Це визначення PAM містить стратегії, які забезпечують командам безпеки більш детальний контроль і нагляд за діями, які виконуються під час привілейованих сеансів. Він включає в себе керування паролями привілейованих облікових записів за допомогою таких тактик, як керування обліковими даними, застосування найменших привілеїв і керування обліковим записом. Наприклад, затвердження привілейованого доступу та робочі процеси, двофакторна/багатофакторна автентифікація, моніторинг та запис привілейованого сеансу та віддалений запуск є критично важливими елементами комплексної програми керування привілейованим доступом.

Як правило, організації починають свою стратегію PAM з рішень для керування привілейованими обліковими записами та сеансами (PASM), щоб отримати видимість і контролювати поверхню атак своїх привілейованих облікових записів і зменшити кількість привілейованих облікових записів.

Як було сказано, організаціям необхідно застосувати проактивний, цілісний підхід до управління привілейованим доступом, щоб досягти успіху у впровадженні PAM.

Розглянемо 10 ключових кроків щодо впровадження повністю керованої стратегії PAM (рис.1.2):

Рис.1.2. Ключові кроки до створення комплексного PAM

1. Залучення системи автоматизації до управління привілейованими паролями сприяє покращенню огляду і забезпеченню автоматичної зміни облікових записів та їх паролів. Це виключає потребу вручного втручання з боку IT-персоналу та мінімізує ймовірність помилок в адміністративних процесах. Також, завдяки коротшому життєвому циклу паролів, користувачі ніколи не отримують доступ до привілейованих паролів у будь-який момент.

2. Впровадження концепції мінімального привілеювання дозволу виконання для користувачів, призначених лише необхідні дозволи для щоденних робочих завдань. При запиті на розширення доступу, привілеї можуть надаватися тимчасово та обмежено на період виконання завдання, з подальшим відкликанням.

3. Проведення аналізу вразливостей програмного забезпечення допомагає приймати обґрунтовані рішення щодо надання привілеїв. Включення елементів

керування додатками та привілеїв у систему управління вразливістю може допомогти зменшити ризики, пов'язані з потенційними загрозами.

4. Врахування мережевих пристроїв у системі безпеки, оскільки вони також можуть стати точкою входу для зловмисників. Налаштування PAM на мережевих пристроях дозволить зменшити ризик використання стандартних облікових даних та підвищить загальний рівень безпеки.

5. Розгляд безпеки у хмарному середовищі, включаючи впровадження локальних принципів PAM у хмарну інфраструктуру, забезпечить захист конфіденційної інформації та забезпечить безпеку даних під час їх переміщення в хмару.

6. Захист пристроїв Інтернету речей (IoT) шляхом впровадження автоматизованих рішень PAM допоможе знизити ризик кібератак і зберегти конфіденційні дані.

7. Запобігання вбудовуванню облікових даних у програми і веб-сайти може бути досягнуто за допомогою належної політики PAM, що дозволяє керувати доступом до облікових даних з точністю і безпекою.

8. Використання привілейованої аналітики загроз (PTA) для моніторингу та оцінки ризиків поведінки користувачів, а також надання сповіщень у разі виявлення підозрілої або ризикованої діяльності.

9. Інтеграція привілейованих облікових записів для спільного керування користувачами між системами на базі Unix і Windows.

10. Інтеграція стеку ідентифікаційних даних для спільної роботи інструментів керування ідентифікацією та доступом, з метою посилення контролю доступу та зменшення ризику атак.

Реалізація вищезазначених кроків може допомогти мінімізувати зловживання привілеями, але це не буде остаточним рішенням безпеки. Оскільки використання привілейованих облікових записів зростає, організаціям вкрай необхідно співпрацювати з постачальниками рішень для кібербезпеки, які розглянемо в

наступному підрозділі, щоб розробити ще більш досконалу стратегію PAM, яка встановлює ширші межі та створює відповідний кіберзахист.

Привілейовані облікові записи є ключем до інформаційної інфраструктури організації, оскільки їх можна використовувати для доступу до таких ресурсів, як сервери, бази даних, програми або робочі станції.

Привілейовані облікові записи, яким потрібні підвищені дозволи, включають:

- Облікові записи адміністратора домену, які керують користувачами Active Directory;
- Облікові записи системного адміністратора, які керують серверами, хмарними платформами та базами даних;
- Кореневі облікові записи для суперкористувачів, які керують платформами Unix/Linux;
- Облікові записи, які запускають і керують програмами, службами та запланованими завданнями, пулами програм IIS (програми .NET) і мережевим обладнанням, таким як брандмауери, маршрутизатори та комутатори.

Причини надання привілейованих облікових записів або надання підвищених привілеїв:

- встановлення апаратного/програмного забезпечення системи;
- доступ до конфіденційних даних;
- скидання паролів для інших;
- доступ до всіх машини в середовищі;
- внесення змін в систему IT-інфраструктури.

Привілейовані облікові записи використовуються системними адміністраторами для розгортання та обслуговування IT-систем, тому вони існують майже на кожному підключеному пристрої, сервері, базі даних і програмі. Привілейовані облікові записи виходять далеко за межі локальної або хмарної корпоративної інфраструктури й включають облікові записи маркетингу, продажів,

фінансів і соціальних мереж, якими керують співробітники. Тому важливо, щоб навіть малі та середні підприємства мали ефективний процес керування привілейованими обліковими записами.

Приклади PAM-записів

Будь-який обліковий запис із підвищеними дозволами або статусом у вашій компанії є привілейованим обліковим записом. Вам потрібно стежити за кожним обліковим записом системного адміністратора, рівня С або обліковим записом служби інакше, ніж за іншими обліковими записами користувачів. Ось список звичайних привілейованих облікових записів.

1. Облікові записи локальних адміністраторів: будь-який обліковий запис, який входить до групи локальних адміністраторів на будь-якому комп'ютері, є привілейованим обліковим записом.

2. Сервісні облікові записи: облікові записи, які ви використовуєте для керування програмами, є сервісними обліковими записами. Загалом вони існують лише для того, щоб дозволити програмі виконувати свою роботу, і не мають дозволів за межами цієї відповідальності. Ці облікові записи можуть мати доступ до ОС, файлів і папок і/або баз даних.

3. Облікові записи адміністратора домену: адміністратори домену мають привілеї для всіх систем і користувачів у домені мережі. Ці облікові записи мають привілеї божественного режиму.

4. Облікові записи привілейованих користувачів : Ви знаєте того користувача, якому ви надали локальний адміністративний доступ до цього одного комп'ютера? Тепер цей обліковий запис є привілейованим.

5. Облікові записи рівня С: привілеї означають не лише доступ до комп'ютерних систем, це також може означати вплив. Подумайте про це: ви реагуєте інакше, якщо отримуєте електронний лист від IT-директора, ніж ваші колеги. Хакери використовують цей вплив у своїх фішингових атаках.

Рис.1.3. PAM-записи [5]

1.2. Аналіз ризиків використання некерованих привілеїв

За статистикою Майже 80% організацій не впровадили — або впровадили лише частково — рішення для керування привілейованим доступом. Багато зломів мають одну спільну рису: їх було здійснено через компрометацію привілейованих облікових даних. За оцінками аналітиків, до 80% усіх порушень безпеки пов’язані з компрометацією привілейованих облікових записів (рис.1.4) [3, 4].

Рис.1.4. Статистика впровадження привілейованих облікових записів в організаціях

Зловживання привілейованим обліковим записом відбувається, коли привілеї, пов'язані з певним обліковим записом користувача, використовуються неналежним чином або шахрайським шляхом, навмисно, випадково або через умисне ігнорування політик. Згідно зі звітом Verizon [3] про розслідування витоку даних за 2023 рік , зловживання привілейованими обліковими записами зараз є другою за поширеністю причиною інцидентів безпеки та третьою за поширеністю причиною зломів (рис.1.5).

У типовому сценарії зловживання привілеями є прямим результатом поганого контролю доступу: користувачі мають більше прав доступу, ніж їм потрібно для виконання своєї роботи, а організація не в змозі належним чином відстежувати діяльність привілейованих облікових записів і встановлювати належний контроль [3].

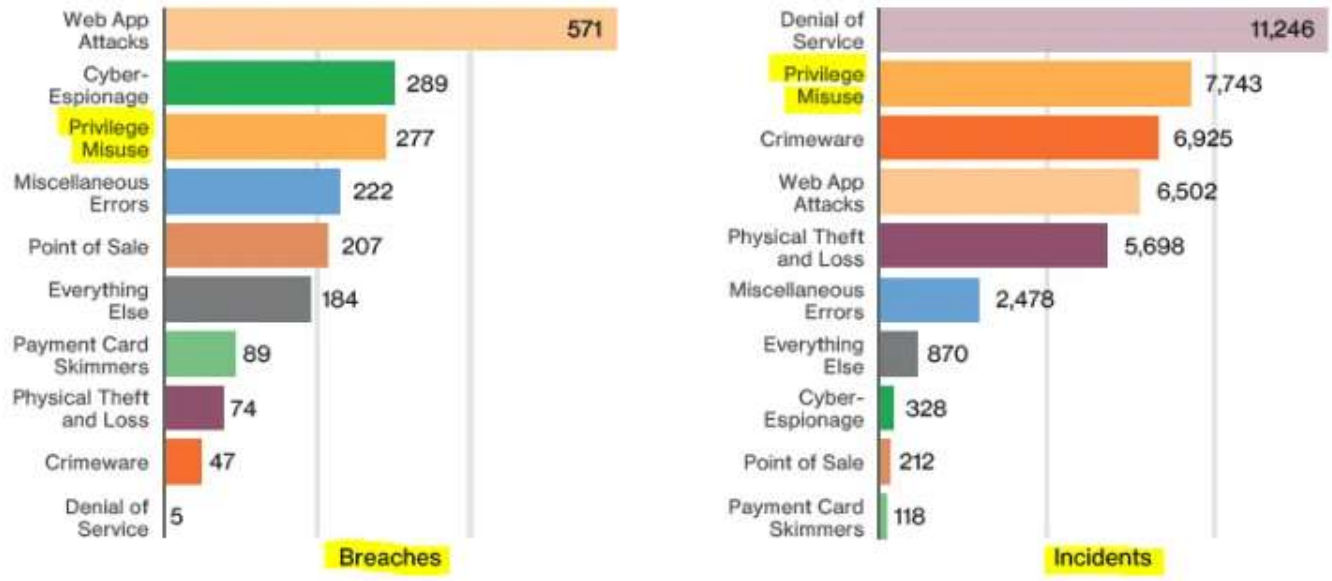

Рис.1.5. Зловживання привілейованими обліковими [3]

Привілейовані облікові записи є шлюзом до критично важливих систем і даних. Зловживання цими потужними обліковими записами може призвести до втрати конфіденційних даних і бізнес-аналітики, а також до простою систем і програм, необхідних для бізнес-операцій. Крім прямої шкоди для бізнесу, ці проблеми можуть призвести до поганої реклами та втрати клієнтів і судових процесів, які можуть тривати роками, а також до недотримання вимог і пов’язаних із цим покарань, які можуть включати як великі штрафи, так і тюремне ув’язнення для вищого керівництва [3].

Незважаючи на ризик, традиційні методи ідентифікації та керування привілейованими обліковими записами все ще покладаються на ручні, трудомісткі завдання, які виконуються нечасто або раз за разом. Ці методи можуть легко поставити під загрозу безпеку, оскільки для більшості зловмисників захоплення облікових записів користувачів низького рівня є лише першим кроком. Їхня справжня мета — заволодіти привілейованими обліковими записами, щоб вони могли розширити свій доступ до програм, даних і ключових адміністративних функцій.

Наприклад, у багатьох випадках облікові записи локального домену на пристроях кінцевих користувачів спочатку зламуються за допомогою різних методів соціальної інженерії. Потім атаки посилюються, щоб отримати доступ до більшої кількості систем.

Практично всі організації мають деякі невідомі або некеровані привілейовані облікові записи, що підвищує їхній ризик.

Це може статися з різних причин:

- доступ для колишнього співробітника ніколи не відключався.
- обліковий запис використовується все рідше і рідше, поки він не застарів і не буде залишений.
- облікові записи за умовчанням для нових пристроїв ніколи не вимикалися.

Управління ризиками для привілейованих користувачів

Одна третина всіх зломів, незалежно від типу атаки, передбачає використання вкрадених облікових даних. Минулого року 71% інцидентів були мотивовані фінансово, а 25% були мотивовані стратегічними важелями (тобто шпигунством).

Згідно зі звітом Verizon про розслідування витоку даних за 2023 рік , 34% зломів ініційовано внутрішньою загрозою, якою може бути незадоволений співробітник, навмисне внутрішнє шпигунство або просто неакуратна гігієна безпеки. Майже 30% зареєстрованих інцидентів були пов’язані з неправильним використанням привілеїв, а 20% порушень – через неправильне використання пароля.

Рис.1.5. Статистика інцидентів пов’язаних з PAM [1]

Незважаючи на цю статистику, навіть у найскладніших IT-середовищах привілейованими обліковими записами користувачів занадто часто керують за допомогою загальних паролів у кількох системах, неавторизованого обміну обліковими даними та паролів за замовчуванням, які ніколи не змінюються, що робить їх основними цілями для атак.

Людей часто вважають найслабшою ланкою в стратегії безпеки

Домінує в інцидентах пов'язаних з компрометацією привілейованих записів – внутрішні користувачі інформаційної системи організації (таблиця 1.1). Більшість мотивується фінансовою вигодою, а особисті дані залишаються улюбленою метою.

Таблиця 1.1.

Інциденти пов'язані з компрометацією привілейованих записів внутрішніми користувачами

Частота	406 інцидентів, 288 з підтвердженим розкриттям даних
Види загрози	Внутрішні (99%), численні (7%), зовнішні (6%), партнерські (2%)
Мотиви	Фінансовий (89%), образа (13%), шпигунство (5%), зручність (3%), веселощі (3%), ідеологія (2%)
Дані скомпрометовані	Особисті (73%), медичні (34%), інші (18%), банківські (12%), платіжні (12%)

Отже ключовим фактором у захисті даних організації є впровадження стратегій керування привілейованим доступом (PAM), які іноді називають керуванням привілейованими обліковими записами. Ці привілейовані користувачі можуть мати повноваження встановлювати програмне забезпечення та змінювати або видаляти облікові записи користувачів. Їхній статус також може надати їм доступ до конфіденційної або безпечної інформації.

1.3. Аналіз рішень управління привілейованим доступом до інформаційної системи організації

Більшість організацій структурують свої системи за рівнями відповідно до серйозності можливих наслідків в разі порушення або неправильного використання. Чим вищий рівень, тим більші наслідки може мати подібне порушення.

Рішення PAM допомагають IT-адміністраторам і адміністраторам безпеки контролювати та захищати привілейований доступ, дозволяючи їм надавати «точно вчасно» доступ до систем високого рівня. Це означає, що користувачам надаються підвищені дозволи лише до тих пір, поки вони потрібні для виконання їхньої роботи.

Після виходу з системи високого рівня дозволи скасовуються. Ці дозволи також можуть бути обмежені за часом; користувач матиме доступ протягом певного періоду часу, перш ніж йому доведеться шукати оновлений дозвіл. Це захищає критично важливі бізнес-системи від несанкціонованого доступу та сприяє кращому управлінню відповідно до норм захисту даних.

Розглянемо найбільш відомі рішення привілейованого доступу.

Рішення ARCON для управління ризиками розроблені для захисту даних і конфіденційності шляхом прогнозування ситуацій ризику, захисту організацій від цих ризиків і запобігання їх прогресуванню в інциденти. Управління привілейованим доступом (PAM) ARCON дозволяє групам безпеки підприємства захищати та керувати всім життєвим циклом своїх привілейованих облікових записів. Він захищає привілейовані облікові дані від атак скомпрометованих інсайдерів і сторонніх кіберзлочинів. [3, 7, 8]

ARCON PAM має безпечне сховище паролів, яке автоматизує часті зміни паролів. Сховище генерує та зберігає надійні динамічні паролі, доступ до яких мають лише авторизовані користувачі. Користувачі повинні пройти багатофакторну автентифікацію (MFA), щоб отримати доступ до сховища. ARCON пропонує власну програмну перевірку одноразового пароля (OTP) для перевірки особи користувачів, і цей інструмент інтегрується зі сторонніми рішеннями автентифікації, якщо організація хоче створити рівні автентифікації навколо сховища. Безпека MFA дозволяє ARCON PAM запуск єдиного входу (SSO) для доступу до всіх критично важливих систем без користувачів, які повинні ділитися своїми обліковими даними. Це робить процес входу більш ефективним, водночас захищаючи важливі дані від загрози злому пароля. Нарешті, увесь привілейований доступ здійснюється точно вчасно, що зменшує поверхню загрози, віддаючи перевагу доступу за потреби над постійними привілеями.[3]

Розширений моніторинг сеансів дає адміністраторам повне уявлення про те, хто використовує середовище привілейованого доступу та чому, що дозволяє швидше

зменшувати ризики. ARCON PAM також забезпечує повний контрольний журнал привілейованих дій, а також звіти та аналітику результатів за допомогою механізму звітності рішення. Це дозволяє керівникам і аудиторам за потреби оцінювати статус відповідності організації.

Рішення *BeyondTrust* є провідним постачальником на ринку управління привілейованим доступом. *BeyondTrust* пропонує низку рішень, які забезпечують високий рівень видимості та безпеки в середовищах кінцевих точок, серверів, хмар, DevOps і мережевих пристроїв. Привілейований віддалений доступ — це рішення BeyondTrust для керування та аудиту внутрішнього та стороннього віддаленого привілейованого доступу без потреби у VPN. Його розроблено, щоб підвищити продуктивність співробітників, незалежно від їхнього місцезнаходження, і водночас не дати зловмисникам отримати доступ до критично важливих бізнес-систем. [3]

Привілейований віддалений доступ зберігає паролі в безпечному хмарному сховищі на пристрої. Крім того, це рішення інтегрується з BeyondTrust Password Safe, який постачається як програмне забезпечення. Обидва параметри дають змогу BeyondTrust вводити облікові дані, що дозволяє BeyondTrust безпечно вводити облікові дані зі сховища безпосередньо в сеанс. Це означає, що користувачі не відкривають облікові дані в жодному моменті під час входу. Рішення також має потужні можливості моніторингу з можливостями відстеження та аудиту, доступними в одному інтерфейсі. Адміністратори можуть установити параметри авторизації та сповіщень, щоб отримувати сповіщення, коли користувач отримує доступ до привілейованого віддаленого доступу. Ці сповіщення також зручні для віддаленого працівника, тому адміністратори можуть схвалювати запити на доступ і контролювати використання своїх мобільних пристроїв з будь-якого місця. Комплексні журнали аудиту та криміналістика сеансів дозволяють IT-групам переглядати та контролювати використання привілейованих облікових записів, а також створювати звіти для підтвердження відповідності.

Symantec є провідним виробником рішень для запобігання втраті корпоративних даних (DLP), захисту кінцевих точок і веб-безпеки. Symantec Privileged Account Management (PAM) — це рішення PAM, створене для того, щоб допомогти організаціям легше відстежувати та керувати доступом до корпоративних облікових записів високого рівня, щоб зменшити ризик порушення облікових даних і забезпечити відповідність галузевим стандартам, таким як PCI-DSS. [3]

Symantec PAM зберігає всі привілейовані облікові дані, включаючи паролі адміністратора та адміністратора, а також ключі SSH, у безпечному сховищі. Користувачі повинні підтвердити свою особу за допомогою двофакторної автентифікації, перш ніж їм буде надано доступ до сховища, а облікові дані автоматично змінюються відповідно до налаштованих адміністратором політик, щоб забезпечити дотримання стандартів захисту даних і допомогти запобігти порушенням у результаті використання постійних облікових даних. Symantec PAM постійно стежить за діяльністю привілейованих користувачів, застосовуючи методи машинного навчання для порівняння поточних дій з минулими діями, щоб виявити підозрілу або аномальну поведінку. Адміністратори можуть налаштувати автоматичне виправлення такої поведінки, щоб обмежити поперечне поширення атак у мережі. Нарешті, платформа фіксує дані аудиту з кожного привілейованого сеансу, пов’язуючи всі дії з іменованим користувачем і зберігаючи ці дані в зашифрованому сховищі, де їх можна використовувати для аудиту та відповідності або використовувати як криміналістичний доказ ризикованої поведінки. Адміністратори також можуть вибрати відеозапис усіх привілейованих сеансів для тих самих цілей.

Symantec Privileged Access Management для середніх і великих організацій, які бажають запровадити рішення PAM, щоб запобігти витоку облікових даних і боковим атакам компрометації облікових записів. Платформа також добре підходить для підприємств, які вже використовують інші технології безпеки Symantec, оскільки вони виграють від простоти інтеграції та уніфікованого огляду своїх інструментів безпеки.

CyberArk займає одну з найбільших часток ринку PAM, пропонуючи керовані політиками рішення корпоративного рівня, які дозволяють IT-командам захищати, керувати та записувати дії привілейованих облікових записів. Їхнє рішення Core Privilege Access Security (PAS) забезпечує багаторівневу безпеку доступу для привілейованих облікових записів і містить понад 500 готових інтеграцій. Централізоване керування та звітування дають адміністраторам чітке уявлення про те, хто і чому отримує доступ до критично важливих систем.[3]

Core PAS постійно сканує мережу, щоб виявити привілейований доступ. IT-команди можуть вибрати перевірку спроб доступу, додавши їх до черги, або автоматично ротувати облікові записи та облікові дані відповідно до політики компанії. Облікові дані для доступу до критично важливих активів ізольовано в безпечному сховищі, що допомагає запобігти розкриттю облікових даних. З центральної консолі керування IT-команди можуть вибрати запис і аудит привілейованих сеансів у зашифрованому сховищі. Записи включають відтворення відео, тому адміністратори можуть переглядати конкретні дії та натискання клавіш і контролювати їх на предмет підозрілої активності. Якщо виявлено підозрілу поведінку, Core PAS автоматично призупиняє або припиняє привілейований сеанс залежно від рівня ризику. Автоматична зміна облікових даних у разі призупинення або припинення дії гарантує, що зловмисники або скомпрометовані облікові записи не зможуть повторно отримати доступ до системи.

CyberArk також пропонує розширену версію своєї Core Privileged Access Security, яка включає централізовано керовані детальні засоби контролю доступу для захисту серверів із найменшими привілеями та моніторингу мережі на наявність загроз для контролерів домену. Обидва ці модулі повністю інтегруються зі стандартним рішенням. Рішення CyberArk пропонує варіанти локального, хмарного та SaaS розгортання, що робить його придатним для всіх організацій, незалежно від стану переходу на хмару.

Delinea, провайдер кібербезпеки, що народився в результаті злиття Thycotic і Centrify у 2020 році, є спеціалістом у наданні рішень для керування доступом на рівні підприємства. *Secret Server* — це інструмент управління привілейованим доступом від Delinea, розроблений, щоб допомогти організаціям відстежувати, керувати та захищати доступ до найбільш чутливих корпоративних баз даних, додатків, гіпервізорів, інструментів безпеки та мережевих пристроїв. Secret Server пропонує низку потужних функцій безпеки, а також надійні засоби моніторингу та аудиту сеансів, щоб допомогти компаніям захистити дані компанії від атак захоплення облікових записів і забезпечити дотримання правил захисту даних. [3]

Secret Server зберігає всі привілейовані облікові дані в зашифрованому централізованому сховищі, до якого користувачі можуть отримати доступ лише через процес двофакторної автентифікації. Після перевірки користувачі можуть переглядати лише ті паролі, які їм потрібні для виконання своєї роботи, призначені засобами контролю доступу, налаштованими адміністратором. На порталі централізованого керування адміністратори можуть надавати та скасовувати привілеї для своєчасного доступу, а також налаштовувати політики щодо складності пароля та ротації облікових даних. Це усуває слабкі та статичні паролі, зменшуючи ризик крадіжки пароля. Адміністратори також можуть налаштувати спеціальний робочий процес для делегування запитів на доступ, зокрема для третіх сторін. Потужні можливості запису сеансів дозволяють організаціям відстежувати привілейовані дії, щоб забезпечити відповідність і виявити джерело будь-якої шахрайської або підозрілої діяльності.

Secret Server доступний для розгортання локально або в хмарі за допомогою двох пакетів: пакет Professional пропонує зашифроване сховище паролів з інтеграцією AD, аудитом і звітністю, а також інтеграціями CRM, SAML і HS; пакет Platinum пропонує все вищезазначене, а також робочі процеси затвердження, захист Unix, розширені сценарії та аварійне відновлення. Загалом Secret Server від Delinea є надійним рішенням для підприємств, які хочуть забезпечити захист і централізоване

керування доступом до своїх критично важливих систем, облікових записів і додатків, як для запобігання атакам захоплення облікових записів, так і для забезпечення дотримання стандартів захисту даних.

Для подальшого дослідження буде розглянуто архітектуру та функції основних компонентів рішення Delinea PAM.

Висновки до розділу 1

1. Проведено аналіз поняття управління привілейованим доступом, яке дозволяє контролювати та захищати привілейований доступ, дозволяючи надавати «точно вчасно» доступ до систем високого рівня.

2. Проведено аналіз загроз, які впливають на ризик використання некерованих привілеїв і приводять до компрометації привілейованих облікових даних.

3. Проведено обґрунтування рішення на основі аналізу найбільш відомих рішень привілейованого доступу, які дозволяють організаціям управляти привілейованими записами. Для подальшого дослідження було обрано рішення Delinea PAM.

2 МЕТОДИ ТА ЗАСОБИ УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ НА БАЗІ РІШЕННЯ DELINEA

2.1. Етапи планування привілейованого доступу рішення Delinea

Правильне налаштування управління привілейованим доступом вимагає початкового плану і постійної програми. Першим кроком є визначення того, які привілейовані облікові записи мають бути пріоритетними організації, і переконайтися, що люди, відповідальні за керування привілейованими обліковими записами, чітко розуміють їх прийнятне використання та обов'язки.

Керування привілейованим доступом (PAM) є головним пріоритетом для багатьох організацій у всьому світі, оскільки кіберзлочинці продовжують націлюватися на привілейовані облікові записи, щоб отримати доступ, пересуватися по мережі та здійснювати зловмисну діяльність.

У зв'язку з критичним впливом привілейованих облікових записів організації повинні впроваджувати найкращі практики PAM для захисту та зменшення ризиків привілейованих облікових записів у традиційних середовищах і хмарній інфраструктурі.

Організації з найпривілейованішими обліковими записами повинні захистити:

Адміністраторів домену

Місцевіх адміністратори

Кореневі облікові записи

Сервісні облікові записи

Мережеві облікові записи, такі як CISCO Enable

Облікові записи програми

Облікові записи автоматизації для виконання робочих навантажень.

Перед тим як впровадити рішення керування привілейованим доступом, необхідно провести планування основних кроків [1].

1. Визначити, які важливі функції залежать від даних, систем і доступу.

2. Визначити кому потрібен доступ до ваших привілейованих облікових записів.

3. Визначити сторонніх підрядників, яким потрібен доступ.

4. Встановити часові вікна для використання привілейованого облікового запису.

5. Розуміти шляхи вирішення, якщо станеться злам системи привілейованого доступу.

Багато організацій є не готовими до зламу облікового запиу, і зазвичай за умовчанням просто змінюють паролі привілейованого облікового запису або вимикають привілейований обліковий запис. Цього недостатньо безпеки. Комплексний набір інструментів реагування на інциденти допоможе запобігти перетворенню кібератаки в кіберкатастрофу, забезпечуючи врахування ключових питань, таких як:

– кроки, які необхідно вжити до того, як станеться інцидент, щоб переконатися, що люди готові діяти;

– індикатори компрометації, які допомагають виявити привілейовану атаку;

– дії, які необхідно вжити під час кожної фази інциденту, щоб стримати збиток;

– стратегії, які допоможуть вам продовжувати нормальний бізнес навіть під час нападу.

6. Визначити ризик того, що привілейовані облікові записи будуть викриті або зловживаються інсайдером.

7. Знати політику IT-безпеки, яка чітко охоплює керування привілейованим доступом.

8. Розуміти як дотримуватися державних чи галузевих норм.

2.2. Життєвий цикл управління привілейованим доступом

Після того, як складено план впровадження PAM, який включає права доступу, наступним кроком є дотримання життєвого циклу управління привілейованим доступом Delinea. Це допоможе вам швидко рухатися на шляху до захисту та забезпечення привілейованого доступу.[4]

Рис.2.1. Життєвий цикл управління привілейованим доступом Delinea [4]

Ось етапи життєвого циклу PAM:

1. Визначити

Визначіть та класифікуйте привілейовані облікові записи. Ваші бізнес-функції залежать від даних, систем і доступу, і залежність від цих об’єктів різна від однієї організації до іншої. Якщо ви не впевнені, як почати це завдання, перегляньте свій план відновлення, оскільки він зазвичай класифікує ваші критичні системи. Потім не забудьте узгодити ваші привілейовані облікові записи з вашим бізнес-ризиком і бізнес-операціями.

Розробіть політику IT-безпеки, яка чітко охоплює привілейовані облікові записи. Чи є у вашій організації політика, яка докладно визначає прийнятне використання та обов'язки для привілейованих облікових записів? Ви повинні мати робоче розуміння того, хто має привілейований доступ і коли він використовується. З цієї причини ви повинні розглядати привілейовані облікові записи окремо, чітко визначаючи привілейований обліковий запис і викладаючи правила прийнятного використання.

2. Виявляйте

Виявляйте для себе свої привілейовані облікові записи. Автоматизоване програмне забезпечення для керування привілейованим доступом дає змогу ідентифікувати ваші привілейовані облікові записи, здійснювати безперервне виявлення, щоб стримувати розповсюдження привілейованих облікових записів, виявляти потенційні внутрішні зловживання та виявляти зовнішні загрози. Ця повна постійна видимість ландшафту вашого привілейованого облікового запису є ключовою для боротьби із загрозами кібербезпеці.

3. Управляйте та захищайте

Захистіть паролі своїх привілейованих облікових записів. Завчасно керуйте, відстежуйте та контролюйте доступ до привілейованого облікового запису за допомогою програмного забезпечення для захисту паролем. Переконайтеся, що ваше рішення для керування паролями може автоматично виявляти та зберігати привілейовані облікові записи; розклад ротації паролів; перевіряти, аналізувати та керувати діяльністю окремого привілейованого сеансу; і відстежуйте паролі облікових записів, щоб швидко виявляти зловмисну діяльність і реагувати на неї.

Обмежте доступ IT-адміністраторів до систем. Розробіть політику найменших привілеїв, щоб забезпечити найменші привілеї на кінцевих точках, не порушуючи бізнес-операції. Привілеї слід надавати лише тоді, коли вони потрібні та схвалені. Рішення з найменшими привілеями та керування програмами дозволяють

безперебійно підвищувати рівень затверджених, надійних і дозволених програм, мінімізуючи ризик запуску неавторизованих програм.

4. Моніторинг

Відстежуйте та записуйте сеанси для активності привілейованого облікового запису. Ваше рішення для керування привілейованим доступом повинно мати можливість відстежувати та записувати дії привілейованого облікового запису. Це допомагає забезпечити належну поведінку та уникнути помилок користувачів, оскільки вони знають, що їх діяльність контролюється. У разі злому моніторинг використання привілейованого облікового запису також допомагає аналітикам з кібербезпеки виявити першопричину та визначити критичні засоби контролю, які можна покращити, щоб зменшити ризик майбутніх загроз кібербезпеці.

5. Виявлення ненормального використання

Відстеження та сповіщення про поведінку користувачів . До 80% порушень стосуються скомпрометованого користувача або привілейованого облікового запису. Не недооцінюйте значення отримання інформації про привілейований доступ до облікового запису та поведінку користувачів. Відстеження доступу та активності ваших привілейованих облікових записів у режимі реального часу допомагає виявити ймовірну компрометацію облікового запису та потенційне зловживання користувачами. Поведінкова аналітика зосереджується на ключових точках даних для встановлення індивідуальних базових показників користувачів, включаючи активність користувачів, доступ із паролем, подібну поведінку користувачів і час доступу для ідентифікації та попередження про підозрілу активність.

6. Реагувати на інциденти

Підготуйте план реагування на інцидент , якщо привілейований обліковий запис буде зламано. Проста зміна паролів привілейованого облікового запису або вимкнення привілейованого облікового запису недостатня, якщо привілейований обліковий запис зламано. Потрапивши у вашу систему, кіберзлочинці можуть інсталювати зловмисне програмне забезпечення та навіть створити власні

привілейовані облікові записи. Якщо обліковий запис адміністратора домену скомпрометовано, наприклад, ви повинні припустити, що весь ваш Active Directory також скомпрометовано.

7. Аналіз та аудит

Аудит та аналіз активності привілейованого облікового запису. Постійний моніторинг використання привілейованого облікового запису за допомогою перевірок і звітів допомагає виявити незвичайну поведінку. Це може свідчити про порушення або неправильне використання. Ці автоматизовані звіти допомагають відстежувати причини інцидентів безпеки, а також демонструють відповідність політикам і нормам. Крім того, привілейовані аудити облікових записів надають вам відповідні показники кібербезпеки та важливу інформацію організації, яка потрібна керівнику для прийняття більш обґрунтованих бізнес-рішень.

2.3. Архітектура та компоненти рішення Delinea PAM

Архітектура платформи Delinea PAM – це хмарна архітектура, яка може підвищити стійкість організацій до кібернетичного середовища за умови дотримання певних умов. Хмарні обчислення пропонують високомасштабовану та гнучку інфраструктуру для IT та безпеки. Власні хмарні архітектури мають потенціал для покращення аварійного відновлення та безперервності бізнесу, забезпечуючи безперервне резервне копіювання, відновлення після відмови та відновлення даних.

Однак якщо основні компоненти інфраструктури, які інтегруються хмарною архітектурою, не можуть задовольнити потреби в масштабованості, гнучкості та резервуванні, тоді системи організації не такі стійка. Нехмарні компоненти можуть створювати перешкоди та сповільнювати роботу. Ці компоненти можуть створювати вразливості, які можуть відкрити двері для кібератак. Найважливіше те, що вони збільшують вірогідність і обсяг простоїв ваших критичних IT-систем і бізнес-операцій.

Щоб захистити вашу організацію від збоїв, хмарні архітектори повинні створити міцну та надійну архітектуру, яка може протистояти викликам і підтримувати потреби бізнесу.

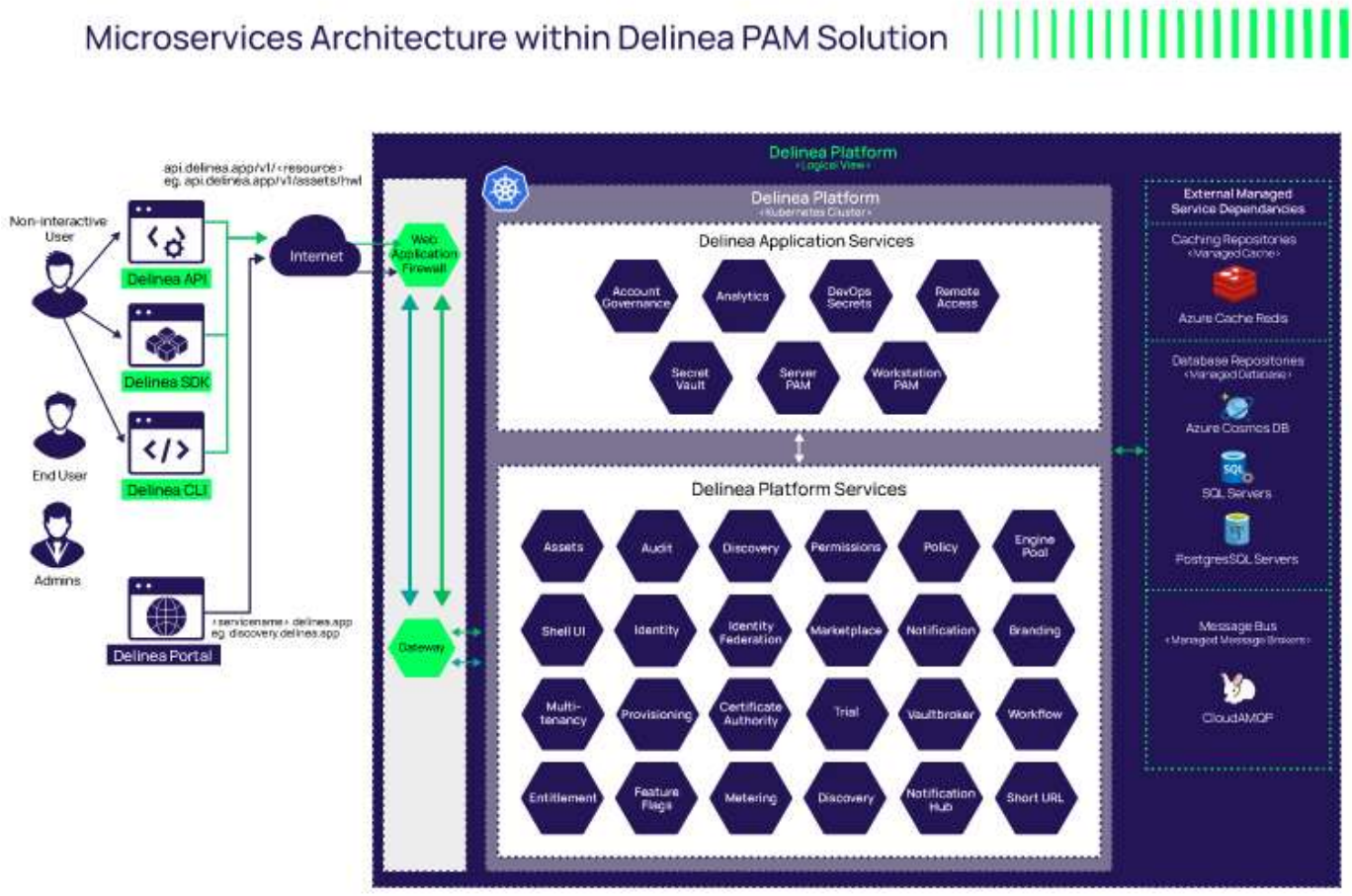

Рис. 2.2 Архітектура Delinea PAM

Архітектуру Delinea PAM розбито на понад 70 різних сервісів. Кожен із сервісів повністю ізольований і незалежний від інших сервісів. У цій моделі, якщо одна з цих служб виходить з ладу, інші служби продовжують працювати.

Розглянемо основні компненти Delinea PAM.

1. Секретний сервер

Дозволяє виявляти, керувати, захищати та перевіряти доступ до привілейованого облікового запису.

Delinea Secret Server — це корпоративне рішення для керування паролями, розроблене для того, щоб допомогти організаціям безпечно зберігати, керувати та контролювати доступ до привілейованих облікових даних. Він спрямований на покращення безпеки конфіденційних даних, зниження ризику витоку даних і спрощення процесу керування паролями.

2. Менеджер життєвого циклу облікового запису - дозволяє знаходити, захищати, створювати та виводити з експлуатації облікові записи служби.

Аналітика привілейованої поведінки - дозволяє виявляти аномалії в поведінці привілейованого облікового запису.

Менеджер привілеїв - управляє привілеями робочої станції та контроль додатків.

3. Сервер PAM - керує ідентифікаторами та політиками на серверах.

2.4. Опис функцій компонентів рішення Delinea PAM

До основних функцій Delinea Secret Server відноситься:

Безпечне зберігання паролів: *Secret Server* зберігає привілейовані облікові дані в зашифрованому форматі, захищаючи конфіденційну інформацію від несанкціонованого доступу.

Контроль доступу: Secret Server реалізує контроль доступу на основі ролей, дозволяючи адміністраторам встановлювати дозволи та контролювати, хто має доступ до конфіденційної інформації.

Керування підвищенням привілеїв: Secret Server інтегрується з системами Windows, щоб забезпечити керування підвищенням привілеїв, допомагаючи зменшити ризик порушення даних.

Аудит і звітність: Secret Server надає детальні журнали аудиту та звіти, що полегшує організаціям відстеження доступу до конфіденційної інформації та виявлення будь-якої несанкціонованої діяльності.

Автоматичне керування паролями: Secret Server підтримує автоматичне керування паролями, допомагаючи оптимізувати процес керування паролями та зменшити ризик помилок, зроблених вручну.

Багатофакторна автентифікація: Secret Server підтримує багатофакторну автентифікацію, допомагаючи покращити безпеку конфіденційної інформації.

Інтеграція з іншими інструментами: Secret Server інтегрується з багатьма іншими інструментами, включаючи Active Directory, Microsoft Azure та хмарні програми, що полегшує організаціям керування своїми паролями та контролем доступу.

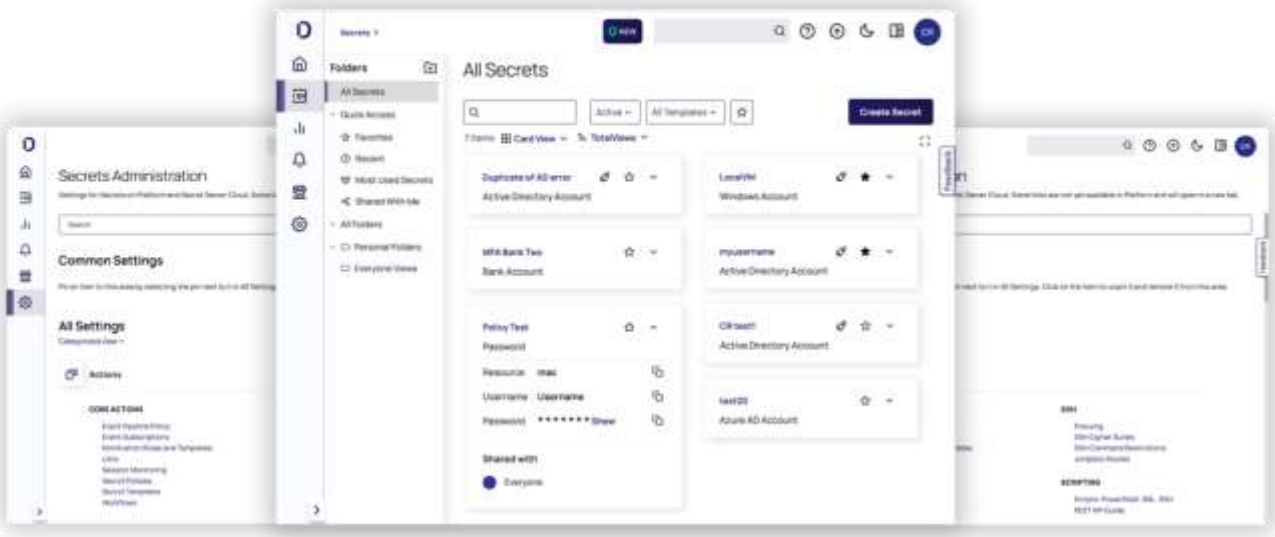

Рис. 2.3. Секретний сервер [4, 6]

Менеджер привілеїв надає наступні функції [6]:

Можливість розгорнути одного агента. Це дозволяє знаходити програми з правами адміністратора навіть на комп'ютерах поза доменом і застосовувати політики.

Визначати гнучку політику. Надає можливість підвищувати, дозволяти, забороняти та обмежувати програми лише кількома командами за допомогою майстра політики. Легке створення перших політик за допомогою The Workstation Policy Framework.

Управління/вилучення прав локального адміністратора. Створює правила для постійного визначення членства в локальній групі та автоматичної ротації привілейованих облікових даних.

Застосовувати програми. Дозволяє довіреним програмам запускати, блокувати інші або використовувати їх у ізольованому середовищі, зберігаючи модель найменших привілеїв.

Підвищити продуктивності IT і кінцевих користувачів. Дані служби підтримки зменшуються завдяки автоматизованим масовим або повторюваним операціям; люди автоматично отримують доступ до потрібних програм і систем.

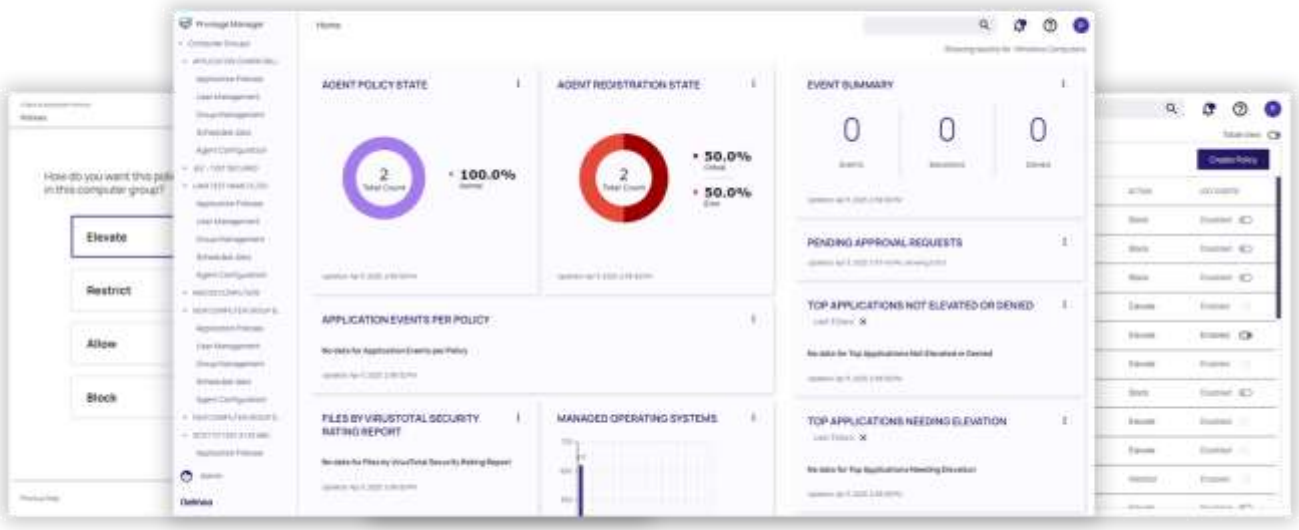

Рис.2.4. Панель менеджеру привілеїв [6]

Менеджер життєвого циклу облікового запису такі основні функції [4, 6]:

Знаходити приховані облікові записи. Це дозволяє знайти та ідентифікувати облікові записи служби.

Встановлювати робочі процеси, в основу яких покладено делегування право власності за допомогою дозволів на основі ролей.

Налаштовувати облікові записи автоматично.

Забезпечує управління на основі встановлення права власності та відповідальність за облікові записи.

Видаляти облікові записи без збоїв.

Сервер PAM виконує наступні функції:

Централізовано керує політиками входу, виконання та MFA в Active Directory (AD) (запатентовані зони) або від постачальників хмарних ідентифікаторів.

Мінімізує ризик за на основі нормативних актів і найкращих практик, таких як «нульова довіра» та «нульові постійні привілеї», щоб захистити від програм-вимагачів і атак зловживання даними.

Застосувати найменші привілеї на основі контролю доступу на основі ролей (RBAC) на рівні хоста для детального контролю та підвищення привілеїв.

Застосувати адаптивний MFA. Політики MFA застосовуються під час входу та виконання програми в Windows і Linux для більшої надійності ідентифікації та вимог страхування кіберризиків.

Покращення безпеки та відповідності. Аудиторські журнали та записи сеансів для перевірки безпеки, реагування на інциденти, відповідності та повної відповідальності.

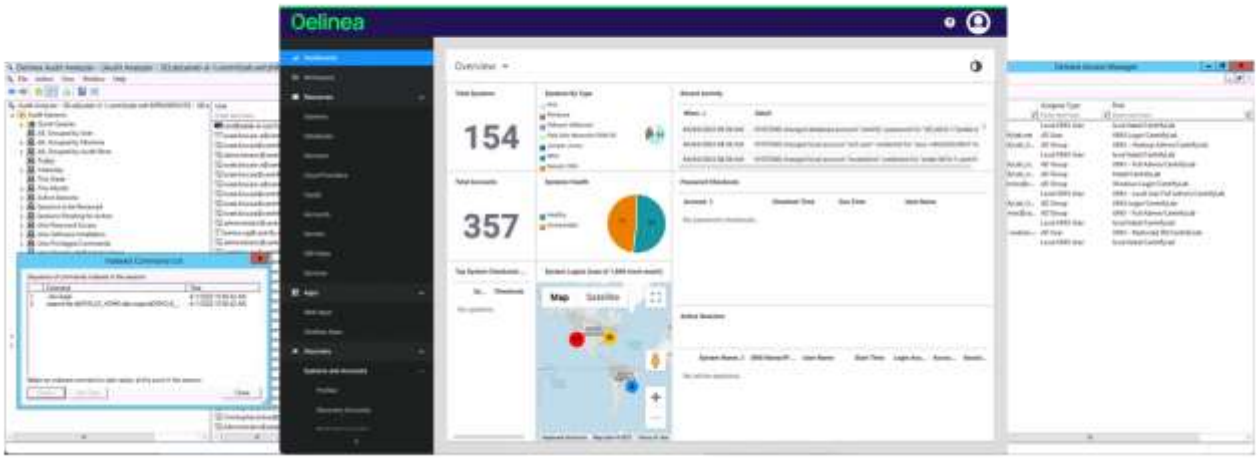

Рис. 2.5. Панель серверу PAM

За допомогою аналітика привілейованої поведінки за допомогою платформи PAM фахівці з кібербезпеки можуть виявляйте аномалії в привілейованих облікових записах в інформаційній системі організації.

Рис. 2.6. Панель аналітики привілейованої поведінки

Аналітика привілейованої поведінки Analytics використовує розширене машинне навчання для аналізу активності привілейованих облікових записів у режимі

реального часу, щоб виявити аномалії та забезпечити оцінку загроз і настроювані сповіщення.

Розширене машинне навчання аналізує всю активність привілейованого облікового запису, щоб ви могли виявляти проблеми та вимірювати ступінь порушення.

Висновки до розділу 2

1. Показано план і етапи впровадження PAM платформи, яке надає краще розуміння необхідності застосування управління привілейованим доступом.

2. Проаналізовано життєвий цикл PAM, в результаті чого визначено основні дії щодо до захисту та забезпечення привілейованого доступу.

3. Проаналізовано архітектуру платформи Delinea PAM, що дозволить підвищити стійкість організацій до загроз.

4. Визначено основні компоненти та описано основні функції платформи PAM.

3 РОЗРОБЛЕННЯ ВАРІАНТА РОЗГОРТАННЯ РІШЕННЯ PAM ПЛАТФОРМИ DELINEA УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ

3.1. Розроблення варіанта розгортання компонентів PAM платформи

Основним компонентом PAM платформи є Secret Server — це комплексне рішення для керування привілейованим доступом (PAM), призначене для захисту, контролю та керування привілейованими обліковими записами та обліковими даними в організації. Він пропонує безпечне централізоване сховище для зберігання конфіденційної інформації, такої як паролі, ключі та сертифікати, гарантуючи, що доступ до цих критичних активів надається лише авторизованому персоналу. [9]

Залежно від того, як ваші адміністратори налаштували секретний серве , ви можете увійти або за допомогою свого облікового запису Active Directory, або локального облікового запису.

Секрети — це пакети конфіденційної інформації з індивідуальними назвами, наприклад паролі. Секрети стосуються широкого спектру захищених даних, кожен тип представлений і створений секретним шаблоном , який визначає параметри всіх секретів на його основі. Секрети дуже потужні та надають багато способів контролю та захисту своїх даних, наприклад:

Переконайтеся, що паролі довгі, складні та часто змінюються.

Звільнення користувачів від необхідності запам’ятовувати численні складні паролі або коли їх потрібно змінювати. Вам потрібно лише запам'ятати свій пароль для доступу до Secret Server . Усі ваші секретні паролі керуються за вас.

Автоматична зміна паролів через задані проміжки часу без втручання користувача.

Визначення того, хто має доступ до секрету.

Переконайтеся, що особа, яка має доступ до секретного сервера чи секрету, це дійсно ви.

Запис того, хто насправді отримав доступ до секрету.

Уся секретна інформація полів для введення тексту надійно шифрується перед збереженням у базі даних, включаючи детальний контрольний журнал для доступу та історії.

До основних відомостей про секрети відноситься:

- перегляд секретів (включає перевірку терміну дії та історії)й;
- створення секретів;
- секретні параметри конфігурації;
- редагування секретів (включає зміну паролів вручну, замість очікування закінчення терміну дії);
- деактивація та повторна активація секретів.

Створена за механізмом керування доступом на основі ролей (RBAC), безпека на основі ролей (RBS) є методом Secret Server для регулювання дозволу на доступ до системи. Кожному користувачеві та групі має бути призначена роль. Secret Server постачається з трьома ролями: адміністратор, користувач і користувач лише для читання. Кожна роль містить різні дозволи, які відповідають посадовій функції користувача. За допомогою RBS забезпечується суворий детальний доступ до Secret Server.

Ролі можна призначити декілька дозволів. Наприклад, ви можете призначити ролі права адміністрування користувачів, редагування секрету, власного секрету та перегляду Active Directory. Потім цю роль можна призначити користувачу або групі.

Базова схема та конфігурація Secret Server показано на рис 3.1 :

- Додавання ліцензій
- Основні налаштування безпеки
- Налаштування автоматичного резервного копіювання
    - Heartbeat
    - Налаштування доступу для локальних і AD користувачів.

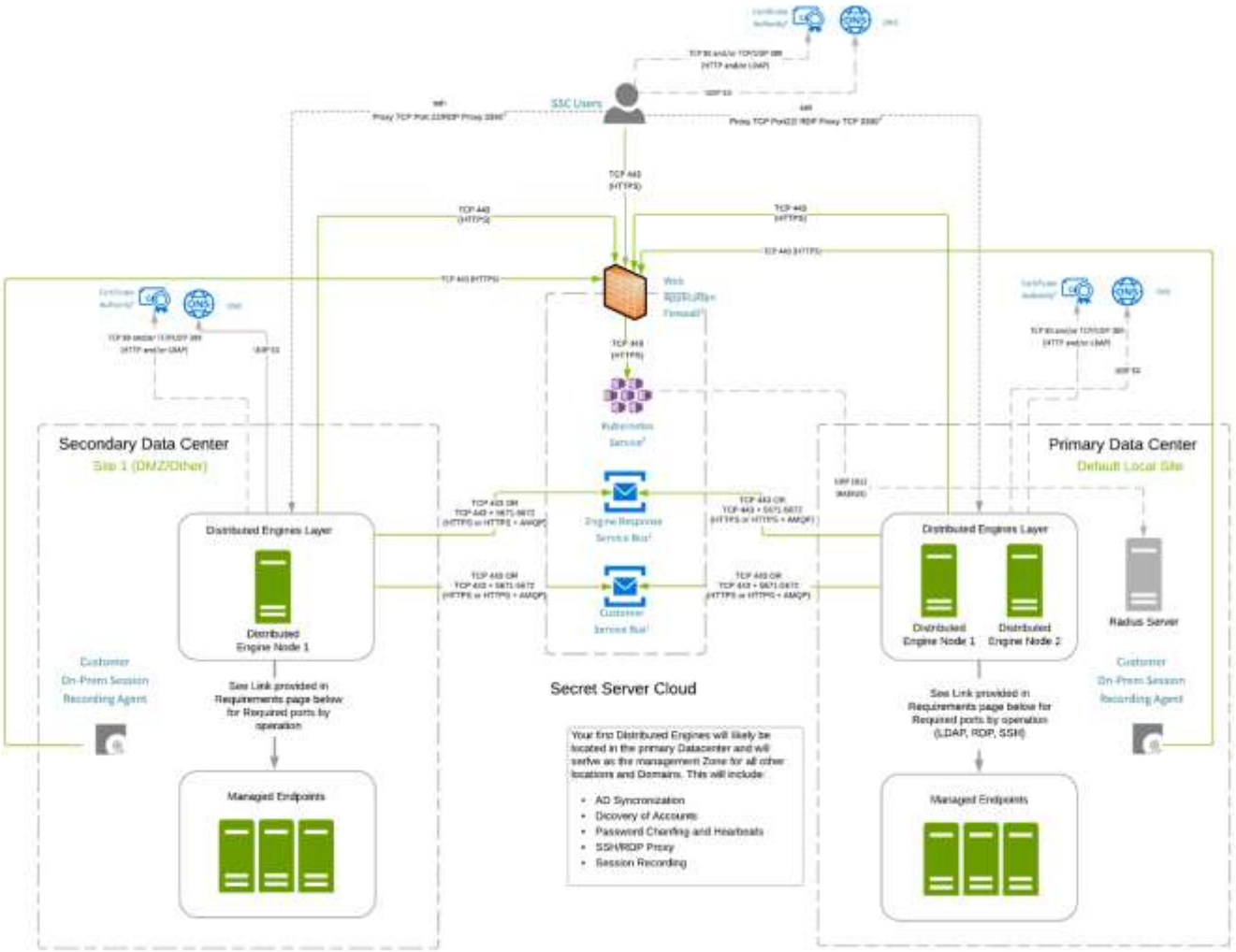

Рис.3.1. Схема розгортання серверу секретів [9]

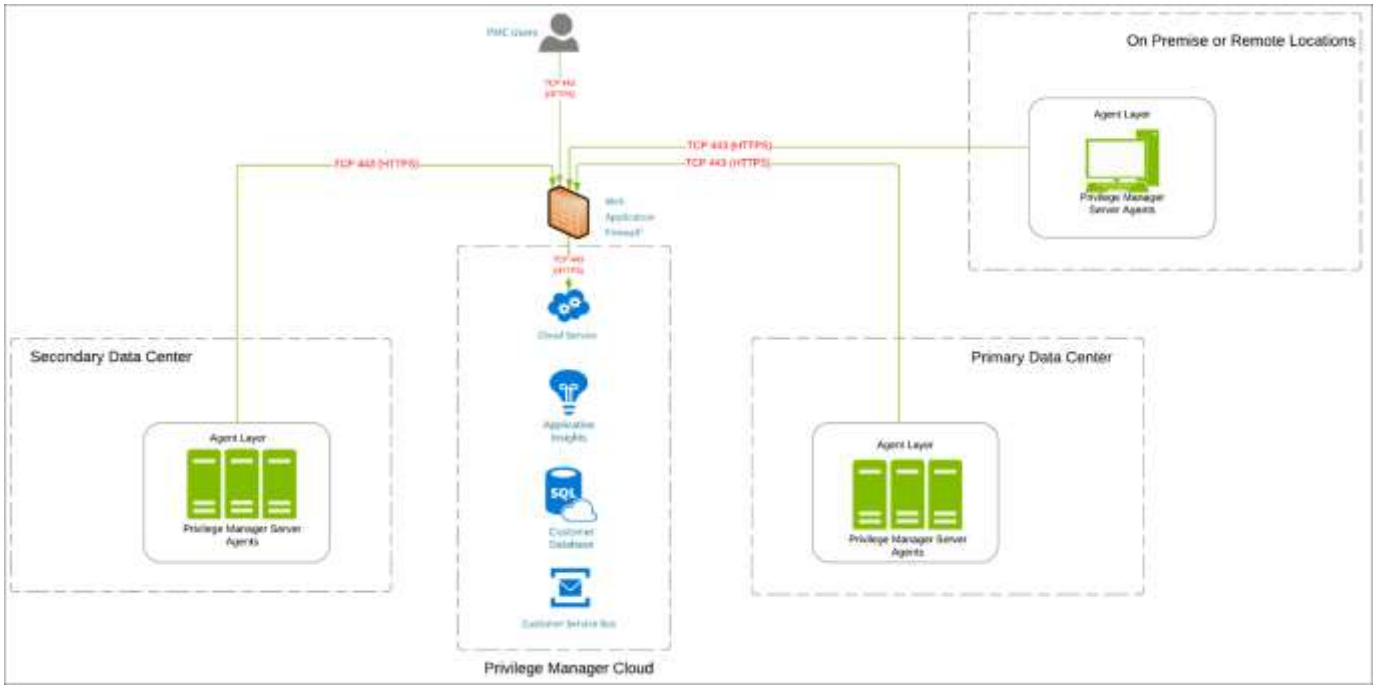

Рис. 3.2. Схема розгортання менеджеру паролів [9]

Базовий запис сеансу є ліцензованою функцією Secret Server . Він налаштований на клієнтських машинах через засіб запуску Secret Server. За допомогою програми запуску Secret Server робить посекундні знімки екрана на клієнтській машині під час записаного сеансу користувача. Ці зображення екрана користувача компілюються у відео, яке можна завантажити та відтворити з метою аудиту та безпеки. Діяльність, записана під час сеансу, базується лише на змінах екрана.

Моніторинг сеансів дозволяє адміністраторам із дозволом на моніторинг сеансів переглядати всі активні запущені сеанси в межах Secret Server. Якщо запис сеансу ввімкнено на секреті, адміністратор може спостерігати за сеансом користувача в режимі реального часу.

Адміністратори можуть здійснювати пошук сеансів серед активних і завершених сеансів. Для перегляду та пошуку сеансів перейдіть до вкладки *Адміністратора > Моніторинг сеансів* .

Для деяких пошукових фільтрів потрібно встановити або налаштувати додаткові компоненти:

Дані клієнта проксі-сеансу - пошук у даних про натискання клавіш проксі-сеансів SSH. Потрібно, щоб проксі-сервер SSH був увімкнений і сеанси SSH використовували його.

Дані про натискання клавіш RD : вимагає встановлення агента моніторингу сеансу RDP.

Ім’я програми RDP - вимагає встановлення додаткового агента моніторингу сеансу RDP на цільовому пристрої.

Щоб переглянути запис, необхідно натиснути значок камери на сеансі. З’явиться сторінка перегляду запису сеансу.

Якщо є зареєстрована активність сеансу, як-от натискання клавіш або дані програми від агента RDP або проксі-сервера SSH, тоді ви можете здійснювати пошук серед активності сеансу та переходити до точок під час відтворення відео. Під час відтворення також відображається карта активності, щоб показати моменти високої активності, такі як зміни екрана, натискання клавіш, запущені та зупинені процеси.

Хмарна архітектура життєвого циклу облікового запису складається з наступних компонентів [10]:

Менеджер життєвого циклу облікового запису : забезпечує дизайн хмарної програми та інтуїтивно зрозумілий користувальницький інтерфейс як інтерфейс Active Directory, що дозволяє корпоративним IT-користувачам легше та ефективніше запитувати, затверджувати, надавати привілеї, керувати обліковими записами служб і припиняти їх, делегуючи тонкощі Active Directory хмарній програмі.

Thycotic One Identity: облікові записи, які використовуються для надання доступу користувачам до екземпляра ALM.

ALM Remote Engine : служба Windows, яка працює на апаратному забезпеченні вашої організації. Ця служба керує взаємодією між хмарною службою ALM і

інсталяцією Active Directory. она також підтримує інтеграцію ALM з примірником Secret Server/DSV вашої організації.

Бази даних : вони не залежать від клієнта для кожного екземпляра ALM.

Сервер Active Directory. Це сервер Active Directory, з яким ви збираєтеся інтегрувати ALM Remote Engine. Зв'язки між ALM Remote Engine і доменом у вашому середовищі є відображенням 1:1. Це означає, що ALM Remote Engines може одночасно керувати лише одним доменом.

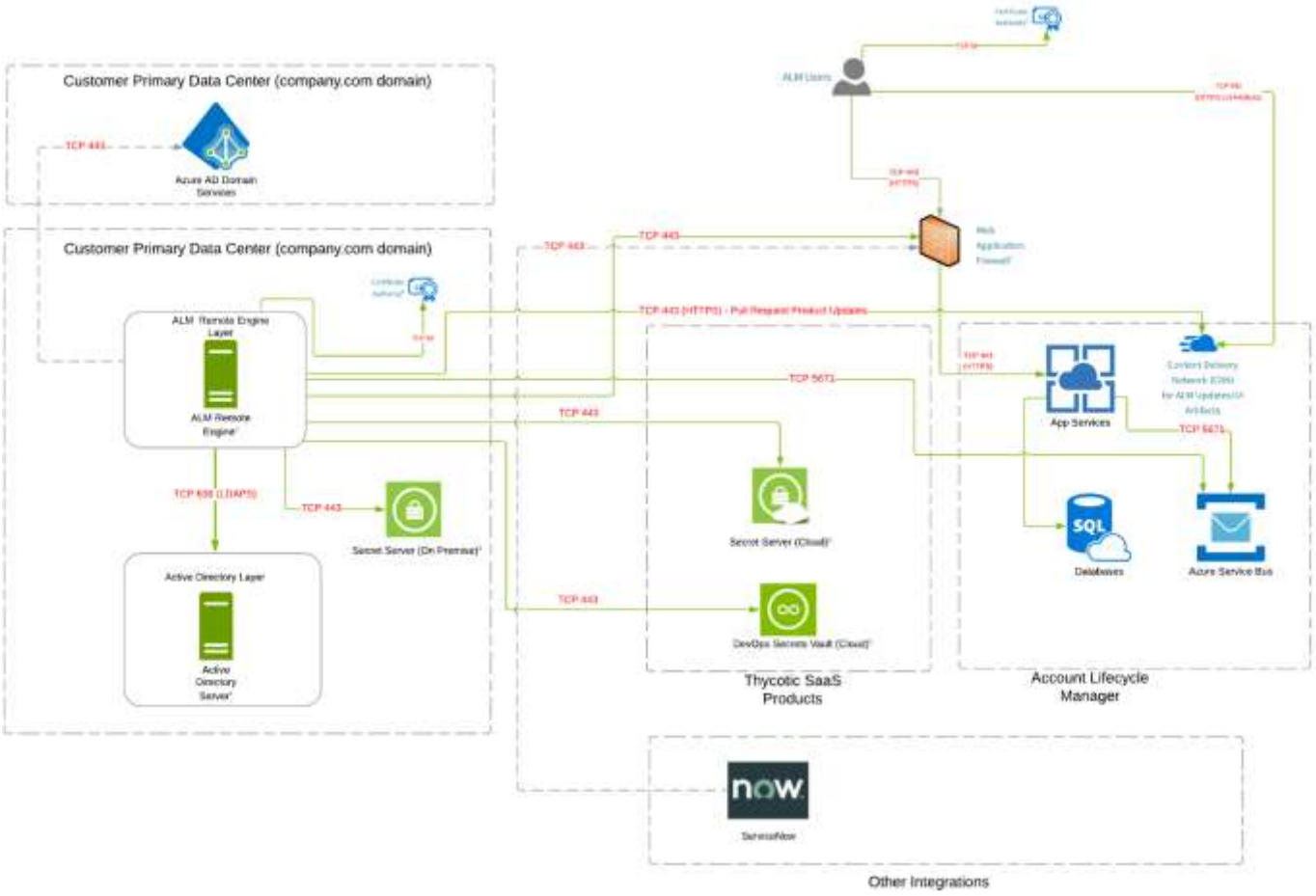

Рис. 3.3. Схема налаштування менеджера життєвого циклу облікового запису [10]

Для підключення компонентів менеджера життєвого циклу облікового запису треба виконати наступні вимоги до еталонної архітектури:

Потрібні лінії зв'язку зеленого кольору. Лінії, які є сірими та пунктирними, можуть бути або не потрібні залежно від індивідуальних вимог клієнта.

Цей дизайн повністю підтримується Delinea.

Усі сервери ALM Remote Engine мають працювати на Windows Server 2012 або новішої версії з .NET 4.7.1 або новішої версії.

ALM Remote Engine

Мінімальні системні вимоги: 2 ядра, 2 ГБ оперативної пам'яті

Рекомендовані вимоги: 4 ядра, 4 ГБ оперативної пам'яті.

Диспетчер життєвого циклу облікових записів (Account Lifecycle Manager ALM) контролює створення, керування та виведення з експлуатації облікових записів служби Active Directory, які працюють у мережі вашої організації. ALM зменшує розповсюдження облікових записів служби та підвищує безпеку, посилюючи керування та створюючи підзвітність за допомогою дозволів на основі ролей. Залежно від ролі користувача, він може запитувати, затверджувати, надавати, керувати обліковими записами служб і видаляти їх.

ALM керує обліковими записами служби, призначаючи кожен обліковий запис користувачеві у організації. ALM використовує чотири ролі для визначення дозволів користувача та визначення підзвітності. Роль користувача визначає, як він взаємодіє з ALM і обліковими записами служби.

Власник облікового запису – усім користувачам ALM надається роль власника облікового запису. Власники облікових записів можуть читати та оновлювати керовані облікові записи, призначені їм.

Системний адміністратор – системний адміністратор має повний доступ до конфігурації та керування ALM. Вони можуть створювати користувачів, ролі, групи та робочі процеси та керувати ними.

Запитувач – Запитувачі можуть подати запит на створення нових облікових записів служби.

Схвалювач – схвалювачі переглядають запити на нові сервісні облікові записи та схвалюють або відхиляють їх надання.

3.2. Розробка рекомендацій щодо застосування рішення управління привілейованим доступом в організації

Застосування технології управління привілейованим доступом надає низку переваг, які дозволять підвищити кібербезпеку інформаційної системи організації.

Необхідно постійно проводити оцінку привілейованих облікових записів. Регулярний перегляд та оновлення списку привілейованих облікових записів забезпечить точність їх оцінки та надають можливість визначити основні рівні привілеїв.

Для визначення основних рівнів привілеїв, чітко визначте та класифікуйте рівні привілеїв на основі посадових ролей та обов'язків. Після чого необхідно встановити принцип найменших привілеїв, надаючи мінімальний рівень доступу, необхідний для кожної ролі. Регулярно переглядайте та оновлюйте рівні привілеїв у міру розвитку посадових ролей.

Реалізуйте багатофакторну автентифікації (MFA) для всіх для всіх привілейованих облікових записів. Необхідно MFA реалізовати в усіх системах і програмах, до яких мають доступ привілейовані користувачі. Крім цього необхідно регулярно оновлювати конфігурації та технології MFA для відповідності останнім стандартам безпеки.

Регулярна зміна паролю та управління ними підвищує безпеку привілейованих облікових даних. Для цього застосовуйте менеджери паролю, які допоможуть виконувати і знаходити паролі, які необхідно змінювати.

Проводьте аналітику щодо користувачів паролів, це дозволить вчасно виявляти аномальні дії привілейованих користувачів, невдалі спроби входу та незвичні дії.

Регулярно проводите перевірки привілейованого доступу, щоб забезпечити відповідність політикам безпеки та нормам. Зберігайте детальні записи дій із

привілейованим доступом для цілей аудиту. Негайно усувайте будь-які прогалини у відповідності та вживайте коригувальні заходи.

Застосовуйте моніторинг і запис сеансів для всіх привілейованих сеансів. Переконайтеся, що журнали надійно зберігаються та регулярно перевіряються на наявність підозрілих дій. Використовуйте сповіщення в режимі реального часу, щоб повідомляти адміністраторів про будь-які незвичайні шаблони доступу.

Проводьте регулярне навчання привілейованих користувачів щодо найкращих практик безпеки та важливості PAM.

Підготуйте заздалегідь змодельовані вправи та навчальні сесії, щоб підвищити обізнаність користувачів. Постійно інформуйте користувачів про останні загрози безпеці та оновлення системи PAM.

На основі перевірки секретів і доступу до них проводьте регулярні перевірки привілейованого доступу, щоб переконатися, що користувачам усе ще потрібні призначені привілеї.

Підтримуйте рішення PAM в актуальному стані за допомогою останніх виправлень безпеки та оновлень.

Регулярно оцінюйте й оновлюйте технологію PAM, щоб отримати переваги від нових функцій і покращених заходів безпеки.

Розробіть комплексний план реагування на інциденти, специфічні для порушень привілейованого доступу.

Чітко визначте ролі та обов’язки щодо реагування та пом’якшення інцидентів, пов’язаних із привілейованими обліковими записами.

Проводьте регулярні навчання, щоб перевірити ефективність плану реагування на інциденти.

Висновки до розділу 3

1. В роботі запропоновано варіанти розгортання та налаштування компонентів платформи Delinea PAM.

2. Розроблено налаштування секретів Secret Server на основі ролей RBAC та застосування менеджера життєвого циклу облікового запису .

3. Розроблено рекомендації щодо застосування методів та засобів управління привілейованим доступом в організації для фахівців з кібербезпеки. В рекомендаціях надано основні шляхи, які дозволять вирішити проблему захисту привілейованих облікових записів інформаційної системи організації.

ВИСНОВКИ

При виконання кваліфікаційної роботи отримано наступні результати:

1. Проведено аналіз поняття управління привілейованим доступом, яке дозволяє контролювати та захищати привілейований доступ, дозволяючи надавати «точно вчасно» доступ до систем високого рівня.

2. Визначено основні загрози, які впливають на ризики використання некерованих привілеїв і приводять до компрометації привілейованих облікових даних.

3. Проведено вибір рішення на основі аналізу найбільш відомих рішень привілейованого доступу, які дозволяють організаціям управляти привілейованим доступом. Для подальшого дослідження було обрано технологію Delinea PAM, як надійне рішення безпеки.

4. Показано план і етапи впровадження PAM платформи, яке надає краще розуміння необхідності застосування управління привілейованим доступом.

5. Проаналізовано життєвий цикл PAM, в результаті чого визначено основні дії щодо до захисту та забезпечення привілейованого доступу.

6. Проаналізовано архітектуру платформи Delinea PAM, яка може підвищити стійкість організацій до кібернетичного середовища.

7. Визначено основні компоненти та функції платформи PAM.

8. В роботі запропоновано схеми налаштування компонентів платформи Delinea PAM.

9. Розроблено технологі. управління привілейованим доступом користувачів до інформаційної системи, яка дозволяє налаштовувати секрети на основі Secret Server на основі ролей RBAC та використання менеджера життєвого циклу облікового запису .

10. Розроблено налаштування секретів Secret Server на основі ролей RBAC та застосування менеджера життєвого циклу облікового запису .

11. Розроблено рекомендації щодо застосування методів та засобів управління привілейованим доступом в організації для фахівців з кібербезпеки. В рекомендаціях надано основні шляхи, які дозволять вирішити проблему захисту привілейованих облікових записів інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Призначення PAM URL: https://delinea.com/blog/privileged-users (дата звернення 07.03.2024).

2. Звіт Verizon. Класифікація інцидентів URL: https://www.verizon.com/business/resources/reports/dbir/2023/incident-classification-patterns-intro/ (дата звернення 18.03.2024).).

3. Jones, C. (2023). Discover the top ten best privileged access management solutions. URL: https://expertinsights.com/insights/the-top-10-privileged-access-management-pam-solutions (дата звернення 28.03.2024).

4. Staff, V. B. Report: Privileged access management still absent in 80% of organizations. VentureBeat. URL: https://venturebeat.com/business/report-privileged-access-management-still-absent-in-80-of-organizations (дата звернення 05.04.2024).

5. Delinea Inc. (2023, November 11). URL: https://delinea.com/blog/privileged-access-management-lifecycle-path-to-maturity (дата звернення 16.04.2024).

6. Privileged Access Management For Dummies®, Delinea Special Edition URL: https://delinea.com/hubfs/Delinea/ebooks/delinea-ebook-privileged-access-management-for-dummies.pdf (дата звернення 21.04.2023).

7. Privilege Manager URL: https://delinea.com/products/privilege-manager (дата звернення 27.04.2024).).

8. Звіт Gartner; Магічний квадрант управління привілейованим доступом URL : https://www.gartner.com/doc/reprints?id=1-26UE4193&ct=210719&st=sb]/ (дата звернення 04.05.2024).

9. Morey J. Haber, Darran Roll Identity Attack Vectors: Implementing an Effective Identity and Access. - 2020. 200p.

10. Secret Server Documentation URL: https://docs.delinea.com/online-help/secret-server/start.htm (дата звернення 06.05.2024).

11. Introduction to Account Lifecycle Manager. URL: https://docs.delinea.com/online-help/account-lifecycle-manager/start.htm (дата звернення 07.05.2024).

12. Privileged Behavior Analytics URL: https://docs.delinea.com/online-help/privileged-behavior-analytics/start.htm#WelcometoPrivilegedBehaviorAnalyticsTechnicalAssistance (дата звернення 08.05.2024).

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація)