КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2022.16.98112
УДК 004.94:519.21

Романюк Олександр Миколайович
студент Факультету інформаційних технологій та управління
Київський університет імені Бориса Грінченка, м. Київ
ORCID ID: 0000-0002-1214-9406
ombabych.fitu18@kubg.edu.ua

Складанний Павло Миколайович
кандидат технічних наук,
завідувач кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Шевченко Світлана Миколаївна
канд. пед. наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки
місце роботи: Київський університет імені Бориса Грінченка, м. Київ, Україна
ORCID ID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

ПОРІВНЯЛЬНИЙ АНАЛІЗ РІШЕНЬ ДЛЯ ЗАБЕЗПЕЧЕННЯ КОНТРОЛЮ ТА УПРАВЛІННЯ ПРИВІЛЕЙОВАНИМ ДОСТУПОМ В IT-СЕРЕДОВИЩІ

Анотація. Зловживання привілеями в IT-середовищі визначається як одна із загроз інформаційним активам бізнесу на сучасному етапі. У статті досліджено і проаналізовано дані проблеми, які тісно пов'язані з витоком інформації внаслідок легітимного доступу до не її та/або несанкціонованого доступу до неї. Звіти, дослідження, акти, опитування на різних підприємствах містять великий обсяг аналітико-статистичних матеріалів, які підтверджують актуальність та важливість даної роботи.

Спираючись на наукову літературу, здійснено огляд ключових означень з даної проблеми, а саме: охарактеризовано дефініцію «привілейований доступ»; розглянуто основні приклади привілейованого доступу в IT-середовищі; описані ризики і загрози інформації від векторів атак, пов'язаних з привілейованим доступом до IT-середовища. Представлено механізм для забезпечення контролю та управління привілейованим доступом – PAM, висвітлені кроки цього процесу та обґрунтовано його доцільність. Експериментальні методики дозволили вибрати найбільш застосовні рішення PAM: WALLIX Bastion PAM, One Identity Safeguard PAM, CyberArk PAM. Розкрито сутність і проаналізовано функціонал кожного з даних рішень. Встановлено переваги і недоліки кожної технології. Внаслідок досліджень технічних та функціональних характеристик здійснено порівняльний аналіз даних трьох рішень: обов'язковими компонентами рішення щодо контролю та управління привілейованим доступом є менеджер паролів та менеджер сесій (сеансів), а додатковими – модуль з аналітикою привілейованих сеансів та менеджер доступу, що звільняє компанії від користування VPN для доступу до привілейованих активів. Також можна зазначити, що функціонал у всіх продуктів дуже схожий, тому велику грає роль реалізація, саме практичний підхід протягом експлуатації, внутрішні алгоритми роботи, додаткові можливості щодо інтеграцій та інновації.

PAM-рішення рекомендовано організаціям як засіб для пом'якшення ризиків інформаційної безпеки та загроз внаслідок інсайдерської діяльності працівників компанії, які мають привілейований доступ в IT-середовищі.

Ключові слова: інформаційна безпека; внутрішні загрози; привілейований доступ; несанкціонований доступ; контроль та управління привілейованим доступом.

ВСТУП

◦ **Постановка проблеми.** Збереження конфіденційності, цілісності та доступності інформації – основні принципи політики безпеки бізнесу. Інформаційні ризики є найпотужнішими важелями, що впливають на результативність та ефективність роботи сучасного підприємства. Серед інформаційних загроз найбільш актуальними, як свідчать моніторингові звіти, є витік конфіденційних даних від несанкціонованих дій користувачів. 97% IT-лідерів вважають інсайдерські загрози серйозною проблемою безпеки [1]. Зокрема, привілейовані IT-користувачі становлять найбільший ризик для інсайдерської безпеки організацій – 63% [2]. Серед них 80% усіх випадків зловживання привілеями були фінансово мотивовані [3]. 76% організацій стикаються з порушеннями політики привілейованого доступу щороку, і 60% цих випадків призводять безпосередньо до порушень безпеки, що впливають на бізнес. Опитування свідчить, що лише біля 30% підприємств шукають рішення для забезпечення контролю привілейованим доступом, інші організації покладаються на основні інструменти автентифікації та ідентифікації [4].

Аналіз останніх досліджень і публікацій. Практики і теоретики у сфері безпеки приділяють велику увагу загрозам і ризикам внаслідок порушення привілейованого доступу в інформаційну систему. У дослідженнях [5-12] науковці розуміють привілейований доступ як внутрішню проблему організації. За їх висновками встановлено, що однією з основних причин актуальності загроз інформаційної безпеки є несанкціонований виток інформації за межі захищених інформаційних систем, і мінімізувати такі загрози можливо внаслідок впровадження систем протидії: систем моніторингу та аудиту, систем аутентифікації, засобів шифрування, систем виявлення та прогнозування витоку інформації.

◦ Керування доступом на основі ролей в IT-середовищі є важливою складовою політики безпеки бізнесу, воно виконує роль захисту критичної інфраструктури організації, оскільки суб'єкти загроз націлені на облікові записи з метою зруйнувати всю мережу організації. Так, аналіз практик показав, організації стикаються з низкою проблем із захистом, контролем та моніторингом привілейованого доступу, зокрема найпоширеніші з них представлені на рис. 1:

◦

◦ *Рис. 1. Найпоширеніші проблеми із захистом, контролем, моніторингом привілейованого доступу*

Є очевидним, що бізнес потребує в політиці безпеки серйозні рішення для забезпечення контролю привілейованим доступом, що й підтверджує актуальність даного дослідження.

Мета статті. Метою статті є дослідження технічних і функціональних характеристик PAM-рішень для визначення їх переваг і недолік у процесі забезпечення контролю привілейованим доступом.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Поняття «привілейований доступ»

Щоб дослідити процес управління привілейованим доступом, потрібно визначитися з деякими поняттями у цій сфері.

У корпоративному середовищі «привілейований доступ» — це термін, який використовується для позначення спеціального доступу або можливостей, що виходять за межі стандартного користувача. Привілейований доступ дозволяє організаціям захищати свою інфраструктуру та програми, ефективно вести бізнес і зберігати конфіденційність даних та критичної інфраструктури [13]. Іншими словами, наділення користувача привілеями, які перевищують стандартний доступ. Внаслідок таких привілеїв можна обійти периметр обмежень безпеки, переходити з однієї мережі на іншу, змінити або підлаштувати хмарні облікові записи тощо.

Привілейований доступ або привілейований обліковий запис використовують для позначення доступу або спеціальних навичок, що перевищують можливості стандартного користувача [14].

Привілейований доступ пов'язаний з користувачами-суб’єктами, програмами та ідентифікаторами машин.

На рис. 2 представлені приклади привілейованого доступу, який використовують працівники компаній, та приклади привілейованого доступу, пов’язаного з програмним забезпеченням [13].

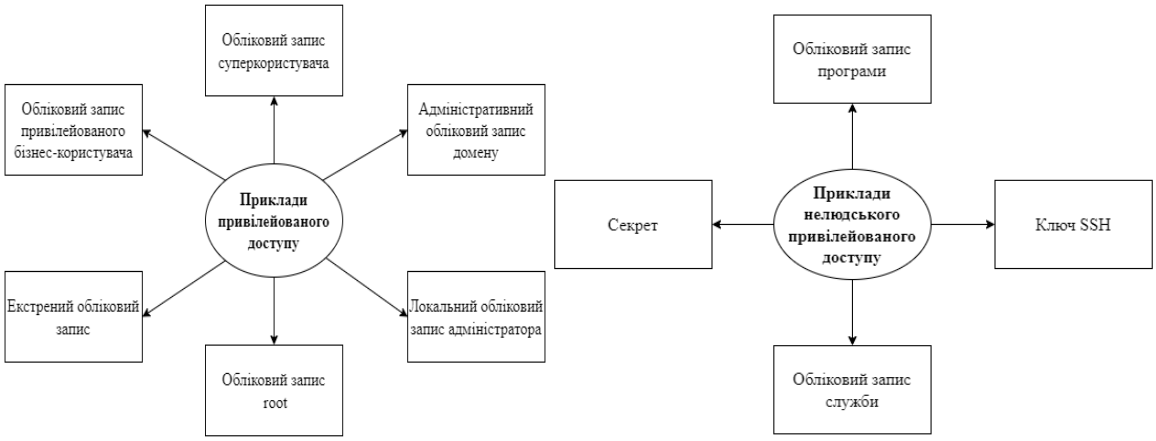

Рис. 2. Приклади привілейованого доступу, який використовують користувачі

Аналітична статистика [3] вказує на те, що на сьогодні визначають чотири типи суб’єктів внутрішніх загроз: привілейовані користувачі та адміністратори; співробітники компанії; треті сторони та тимчасові працівники; привілейовані бізнес-користувачі та

керівники. І саме зловживання привілеями зазначено як основні причини витоку конфіденційної інформації.

Привілейовані користувачі та адміністратори – працівники, що мають усі ключи до інфраструктури організації та конфіденційних даних. Через високий рівень доступу, який мають привілейовані користувачі, інсайдерські атаки, спричинені ними, важко виявити. Привілейовані користувачі знають (і можуть) отримати доступ до конфіденційних ресурсів, не порушуючи жодних правил кібербезпеки.

Привілейовані бізнес-користувачі та керівники мають доступ до найбільш конфіденційної інформації організації – «ядра бізнесу». Ця категорія користувачів може зловживати своїми знаннями для інсайдерської торгівлі, особистої вигоди або корпоративного чи урядового шпигунства.

У сучасному бізнес-середовищі поверхня атак, пов'язаних з привілеями, швидко зростає, оскільки системи, програми, міжмашинні облікові записи, хмарні та гібридні середовища, DevOps, роботизована автоматизація процесів та пристрої Інтернету речей стають все більш взаємопов'язаними. Зловмисники знають це і націлені на привілейований доступ, як шлях до конфіденційних даних компанії, що може завадити як бізнесу, так і репутації.

У дослідженні [9] до загроз, пов'язаних з привілеями, відносять:

- інсайдери, які мають надмірний і неконтрольований доступ до облікових записів, відкриваючи потенціал для неправомірного використання та зловживань;
- інсайдери, чиї облікові записи були скомпрометовані через успішний фішинг, соціальну інженерію чи інші тактики;
- облікові записи, які були скомпрометовані в результаті поганих облікових даних, паролів, пристроїв і моделей програм, що дозволяють зловмисникам скомпрометувати системи та отримувати привілеї для зловмисної діяльності. Враховуючи такі загрози, вони вважають, що привілеї повинні бути вбудовані в операційну систему, файлову систему, програму, базу даних, гіпервізор, платформу управління хмарою і навіть мережу за допомогою сегментації, щоб бути ефективними для взаємодії між користувачами та програмою. Автентифікація надається будь-яким механізмом за допомогою імені користувача та пароля або ключа сертифіката чи пари. Інтерпретація привілеїв ресурсами не може бути по-справжньому ефективною лише на одному рівні.

Підсумовуючи вище викладене, визначаємо, що привілейований доступ до ІТ-середовища має свої ризики і загрози, є очевидним, що організації мають впроваджувати в систему політики безпеки технології та підходи щодо контролю та управлінню привілейованим доступом.

Рішення для контролю та управлінням привілейованим доступом в ІТ-середовищі

●Захист від зловживання привілейованим обліковим записом з боку інсайдерів або інших типів інсайдерських атак вимагає спеціальних рішень.

●Управління привілейованим доступом або PAM – це, в основному, механізм інформаційної безпеки, який поєднує людей, технології та процеси, призначений для відстеження, обробки та контролю привілейованих облікових записів, а також націлений на підтримку організацій у спробах захистити доступ до конфіденційних даних і дотримуватись останніх вимог законодавства [15]. Керування привілейованим доступом засноване на принципі найменших привілеїв, коли користувачам та програмам надається

мінімальний доступ, необхідний для виконання своїх професійних задач. Основні можливості PAM представлені на рис. 3.

Рис. 3. Основні можливості PAM

Сам процес є алгоритмічним, який включає наступні кроки (таблиця 1):

Таблиця 1.

Процес керування привілейованим доступом

Кроки	Характеристика кроків
1 крок	Визначення привілейованих облікових записів в організації
2 крок	Багатофакторна автентифікація для системних адміністраторів та/або реєстрація привілейованих сеансів
3 крок	Автоматизоване рішення PAM: - контроль привілейованим доступом та примусове керування ним; - автоматизована зміна паролів через регулярні проміжки часу або після кожного використання ; - застосування машинного навчання для відстеження відхилень і оцінки ризиків в реальному часі; - попередження адміністратора про небезпечні дії.

На сучасному етапі в Україні стрімко розгортаються рішення та підходи PAM. У той же час організаціям важко визначитися із застосуванням цих рішень. Це пов’язано з нерозумінням або складністю архітектури; впровадженням та реалізацією; заплутаністю ліцензування продукту з прихованими витратами; відсутністю сервісної підтримки; невизначеним питанням щодо інтеграції з іншими елементами системи тощо. У зв’язку з цим, надалі розглянемо три рішення PAM: WALLIX Bastion PAM, One Identity Safeguard PAM, CyberArk PAM, що визнані провідними такими аналітичними компаніями, як Garther, Forrester Research, KuppingerCole

WALLIX Bastion PAM

WALLIX – лідер на ринку керування привілейованим доступом. У розрізі Privilege Access Management першочергово має бути впроваджений продукт WALLIX Bastion,

включаючи в себе такі три модулі: Session Management (WALLIX Bastion Session Manager); Password Management (WALLIX Bastion Password Manager); Remote Access Management (WALLIX Bastion Access Manager). WALLIX Bastion Session Manager забезпечує моніторинг і контроль усіх привілейованих сеансів облікового запису в режимі реального часу для запобігання та виявлення зловмисної активності. WALLIX Bastion Password Manager дозволяє контролювати паролі, секрети, облікові дані та керувати ними, а також надійно зберігати облікові дані в контрольованому сховищі та захищати паролі від крадіжки завдяки високоякісному шифруванню. Слід зазначити, існування інтеграції зі сховищами сторонніх розробників. WALLIX Bastion Access Manager забезпечує захищений віддалений доступ для IT-адміністраторів і зовнішніх користувачів: безпечне підключення з будь-якого місця. Даного функціоналу вистачить багатьом компаніям, як перший крок, а оскільки компанія WALLIX позиціює свій підхід до привілейованого доступу дуже гнучким, то надалі компанії можуть легко інтегрувати інші бажані продукти до власної, вже створеної системи. На рис. 4 представлена схема роботи вищеописаних модулів в одному рішенні WALLIX Bastion PAM [16].

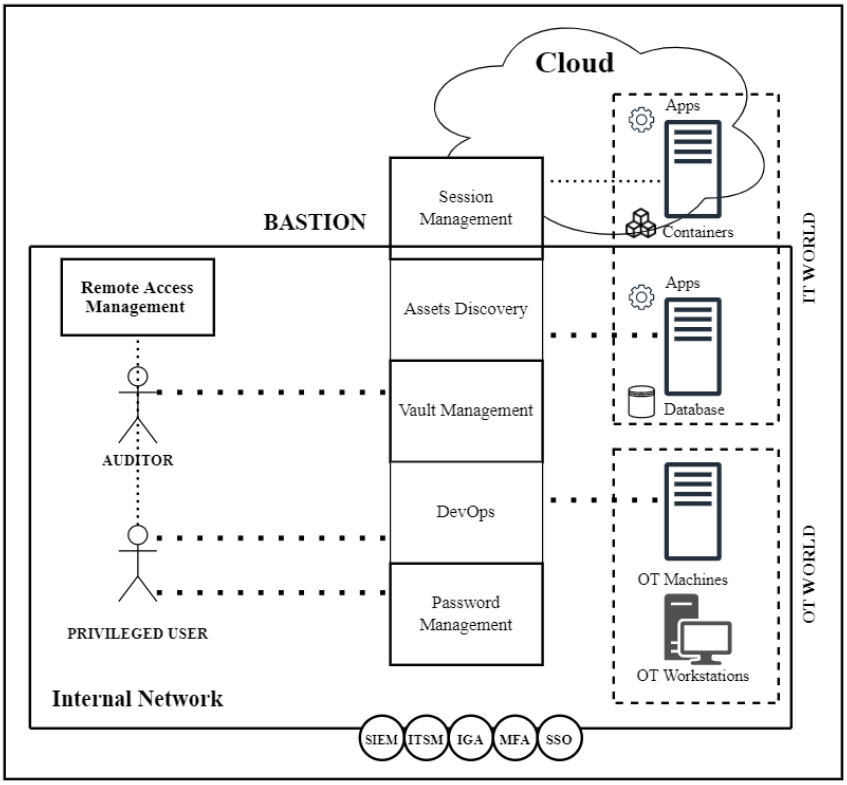

Рис.4. Схема роботи модулів в одному рішенні WALLIX Bastion PAM

На інфографіці зображено два типи активів, відповідно до яких і надається користувачам доступ – це OT WORLD та IT WORLD. Різниця між ними полягає в тому, що IT-системи (information technology) використовуються для обчислень, орієнтованих на дані, а OT-системи (operational technology) відстежують події, процеси та пристрої, а також вносять корективи в роботу підприємства та промисловості [17].

Враховуючи відгуки у впровадженні як малим, так і великим бізнесом [18], визначимо переваги та недоліки рішення WALLIX Bastion PAM (таблиця 2).

ISSN 2663 - 4023

Таблиця 2.

Переваги та недоліки рішення WALLIX Bastion PAM

Переваги	Недоліки
Керування сесіями: забезпечення повного OCR для записаних графічних сеансів, дозволяючи аудиторам зручніше шукати артефакти.	Виявлення облікових записів: функції виявлення облікових записів обмежені та зосереджені переважно на скануванні Active Directory.
Простота розгортання: рішення просте у розгортанні, представлене у кількох формфакторах, включаючи попередньо створені віртуальні образи; присутній функціонал аварійного відновлення та можливості створення умов високої доступності.	Зміна облікових даних: керування обліковими даними WALLIX є на рівні нижче середнього, а підтримка комплексного керування обліковими даними відсутня (немає в запропонованому плані постачальником).
Ціна: ціни є конкурентоспроможними. Для малого бізнесу – це вигідне рішення, аналізуючи ринок. Для великих копаній, ціни є на рівні з основними конкурентами WALLIX.	Географічна стратегія: компанія WALLIX популярна в країнах EMEA, проте її присутність в інших регіонах невелика.
Управління секретами: використання комплексного зняття відбитків з додатків на основі агентів. Цей метод може ефективно видалити будь-які статичні облікові дані з програм або сценаріїв.	Відсутність товстого клієнта: велика кількість вікон з сеансами в браузері буде завантажувати оперативну пам'ять на машині користувача; відсутність альтернатив щодо підключення до активів.

One Identity Safeguard PAM

Каліфорнійська компанія One Identity (Quest Software) спеціалізується на рішеннях PAM і є справжнім лідером на ринку рішень щодо контролю та управлінням привілейованим доступом. У розрізі ж саме Privileged Access Management One Identity пропонує лінійку продукції «Safeguard», зокрема розглянемо такі три основні модулі: Safeguard for Privileged Sessions; Safeguard for Privileged Passwords; Safeguard for Privileged Analytics. Safeguard for Privileged Sessions надає можливість контролювати та записувати привілейовані сеанси адміністраторів, підрядників, рядових користувачів тощо. Safeguard for Privileged Passwords автоматизує, контролює та захищає процес надання привілейованих облікових даних за допомогою керування доступом на основі ролей та автоматизованих робочих процесів. Safeguard for Privileged Analytics аналізує та формує статистику по найбільш ризикованим користувачам, цілодобово стежить за новими внутрішніми та зовнішніми загрозами та виявляє аномальні відхилення від базової активності протягом привілейованого сеансу за допомогою машинного навчання; підвищує безпеку, припиняючи з'єднання, коли надходить сповіщення про потенційно небезпечну діяльність. Додатковий модуль Safeguard Remote Access надає захищений віддалений доступ для привілейованих користувачів. Це хмарне рішення безпечно з’єднує віддалених користувачів із привілейованими ресурсами – без необхідності використання VPN. На рис. 5 представлена схема роботи вищеописаних модулів в одному рішенні One Identity Safeguard.

ISSN 2663 - 4023

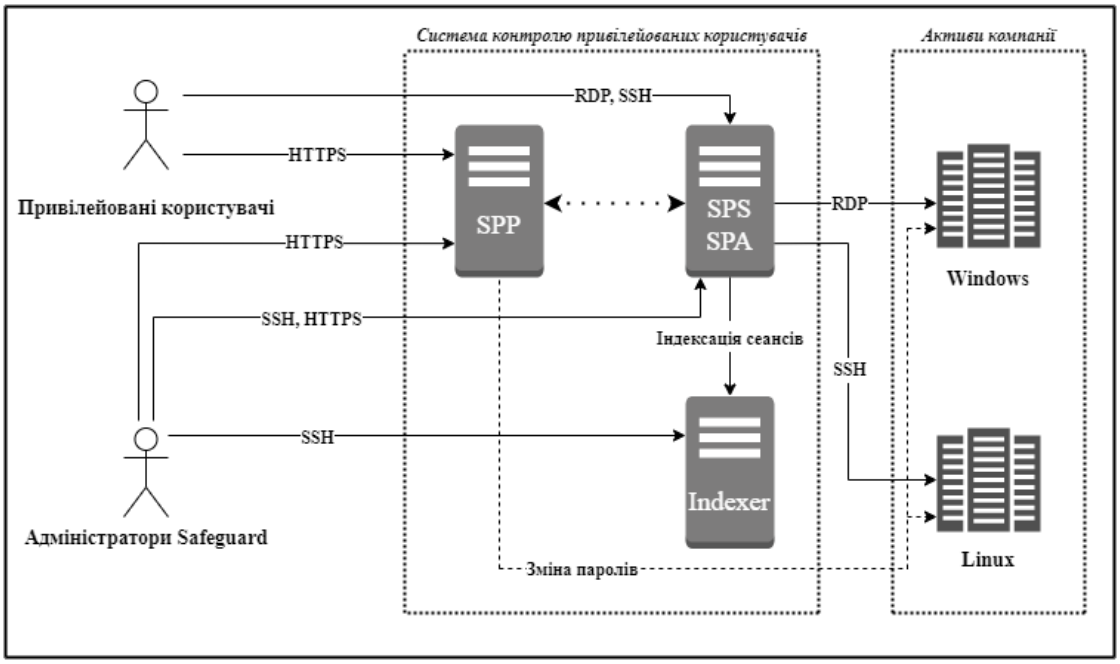

Рис. 5. Схема роботи модулів в одному рішенні One Identity Safeguard

Привілейовані користувачі в основному взаємодіють з Safeguard for Privileged Passwords (SPP) для запиту доступу до активів компанії, а через Safeguard for Privileged Sessions (SPS) із застосуванням певних політик вже приєднуються до кінцевих робочих станцій. Адміністратори відділу ІБ в той час працюють з усіма модулями: з SPP для адміністрування активів, облікових записів, створення політик доступу, надання користувачам певних прав відповідно до розробленої моделі ролей тощо; з SPS для налаштування політик до кожного протоколу з'єднання, перегляду сеансів користувачів, налаштування індексування тощо; з Safeguard for Privileged Analytics (SPA) для аналізу та розслідування аномальних подій. SPP після закінчення або при екстреному припиненню сеансу змінює пароль облікового запису.

Підсумовуючи викладене, визначимо переваги та недоліки продукту One Identity Safeguard (Таблиця 3) [18; 19].

Таблиця 3.

Переваги та недоліки продукту One Identity Safeguard

Переваги	Недоліки
Safeguard for Privileged Sessions: можливість забезпечення повного OCR для записаних графічних сеансів, дозволяючи аудиторам зручніше шукати артефакти.	Додаткові витрати: деякі продукти є додатковими інструментами від Quest Software, які за певних умов буде необхідно придбати.
Аналітика та аудит сеансів: використання машинного навчання для аналізу не лише спроб привілейованого доступу, а й повної діяльності сеансу, включаючи команди; використання пасивного поведінкового біометричного аналізу.	Керування обліковими записами служб: функції керування обліковими записами служб є базовими. Більш розширені функції вимагають створення спеціальної логіки системного роз'єму.

ISSN 2663 - 4023

Розуміння ринку: One Identity розуміє та має стратегію розв'язання проблеми щодо виявлення важкодоступних облікових записів вбудованих служб Windows, проте для цього необхідно придбати додаткові інструменти, такі як Quest Change Auditor і Quest Enterprise Reporter.	Ціна: ціни на продукти One Identity нерівномірні. Наприклад, малий бізнес з менш складними сценаріями отримує вигоду від рішення, а складніші сценарії, як правило, перевищують середні ціни на ринку.
Простий для розуміння інтерфейс: який є загальним для всіх модулів, зокрема з підтримкою CLI і GUI.	Відсутність підтримки LDAPS: Active Directory, що використовується для ідентифікації та автентифікації наразі не підтримує LDAPS у модулі Safeguard for Privileged Passwords.
Гнучкість: плавне розгортання, інтеграції та зручне масштабування для багатьох організацій	Відсутність інновацій: нові можливості найчастіше це вдосконалення наявного функціонала, а не справжні інновації, які очікуються як від одного з лідерів.

CyberArk PAM

CyberArk є безпрецедентним лідером у Gartner Magic Quadrant щодо управління привілейованим доступом за останні кілька років. Протягом дослідження розглянемо саме продукт Privileged Access Manager, як повноцінне рішення для управління привілейованим доступом. Даний менеджер доступний як окреме програмне забезпечення або як SaaS рішення (CyberArk Privilege Cloud) [19–20]. PAM охоплює наступні модулі: Enterprise Password Vault (EPV); Privileged Session Manager (PSM);; Privileged Threat Analytics (PTA); Secrets Manager Credential Providers; On-Demand Privileges Manager (OPM); SSH Key Manager [21]. Перших три задовольняють умові мінімальної реалізації PAM-рішення. Enterprise Password Vault (EPV) дозволяє організаціям захищати, керувати, автоматично змінювати та реєструвати всі дії, пов’язані з усіма типами привілейованих паролів і ключів SSH. Privileged Session Manager (PSM) дозволяє організаціям захищати та контролювати привілейований доступ до мережевих пристроїв. CyberArk Privileged Threat Analytics (PTA) постійно відстежує використання привілейованих облікових записів, якими керує платформа PAM, а також облікових записів, якими ще не керує CyberArk, і шукає ознаки зловживання або неправильного використання платформи. На рис. 6 зображена схема роботи вищеописаних модулів в одному рішенні CyberArk Privileged Access Manager.

ISSN 2663 - 4023

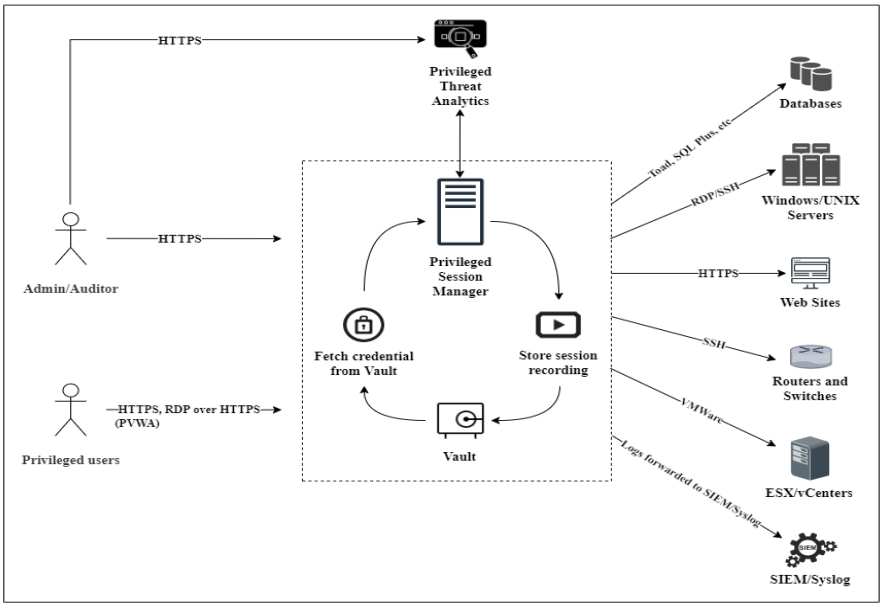

Рис. 6. Схема роботи модулів в одному рішенні CyberArk Privileged Access Manager

Підсумовуючи викладене, визначимо переваги та недоліки продукту CyberArk Privileged Access Manager (Таблиця 4) [18].

Таблиця 4.

Переваги та недоліки продукту CyberArk Privileged Access Manager

Переваги	Недоліки
Успіх на ринку рішень PAM: CyberArk залишається найбільшим брендом PAM з довгою історією в цьому секторі, широким географічним охопленням і найбільшою часткою ринку PAM.	Досвід клієнтів: складність використання та труднощі у розгортані, а оновлення програмного забезпечення часто вимагають професійних послуг. CyberArk тоді ж закликає існуючих і потенційних клієнтів перейти на версії своїх продуктів SaaS.
Інновації: CyberArk перший, хто представив інновації на ринок, та є єдиним, хто пропонує функціональність Cloud Infrastructure Entitlements Management.	Висока доступність: функції аварійного відновлення та високої доступності CyberArk є складними для налаштування та експлуатації.
Інтеграції: CyberArk має велику партнерську екосистему та надає багато конекторів та інтеграцій із суміжними технологіями, такими як ITSM та IGA.	UNIX і Linux: CyberArk PEDM поступається конкурентам як з точки зору механізмів глибокого контролю на основі системних викликів, так і можливості підтримки складніших конфігурацій з AD.
Продукти: CyberArk може підтримувати складні сценарії використання, а його продукти PAM отримують стабільно високі бали в технічних оцінках Gartner.	Ціни: продукти CyberArk є одними з найдорожчих на ринку. Крім того, CyberArk припинив випуск програмної версії свого продукту Windows EPM, що з часом змушує всіх клієнтів підписатися на модель SaaS.

Порівняльний аналіз технологій для контролю привілейованим доступом

Порівняльний аналіз рішень WALLIX Bastion, One Identity Safeguard, CyberArk PAM представлено в таблиці 5.

Таблиця 5.

Порівняльний аналіз рішень PAM

Параметр порівняння	WALLIX Bastion	One Identity Safeguard	CyberArk PAM
Єдина точка входу	Так	Так	Так
Доступ без VPN	Так	Так	Так
Модуль аналітики	Так (Інтеграція зовнішнього рішення CYBERNOVA Operation Center)	Так	Так
Рівень автоматизації	Середній	Високий	Дуже високий
Масштабованість системи	Так	Так	Так
Легкість розгортання	Легко та швидко	Легко та швидко	Легко та швидко
Інтеграція із системами класу SIEM та IdM/IAM	Так	Так	Так
Інтеграція з хмарними середовищами	Так	Так	Так
Середовище для самостійного доопрацювання	Так (відкритий API)	Так (SDK)	Так (SDK)
Інтеграція з каталогами користувачів	Так	Так	Так
Інтеграція з системами класу DLP	Ні	Ні	Ні
Інтеграція з системами класу IDS та IPS	Ні	Ні	Ні
Відповідність стандартам ІБ	PCI DSS, SOX, Basel II, ISO 27001, GDPR, HIPAA, NIST	PCI DSS, SOX, Basel II, ISO 27001, GDPR, HIPAA, NIST	PCI DSS, SOX, Basel II, ISO 27001, GDPR, HIPAA, NIST
Наявність додаткових модулів	Так	Так	Так
Налаштування власних ролей	Так	Так	Так
Двофакторна автентифікація	Так	Так	Так
Налаштування відмовостійкої конфігурації рішення	Так	Так	Так, проте певні налаштування вимагають професійного досвіду
Сховище паролів	Так	Так	Так (запатентована технологія Secure Digital Vault)
Налаштування правил генерації паролів	Так	Так	Так
Автоматична перевірка та /або зміна паролів	Так	Так	Так
Частота оновлень	Часто	Часто	Часто
Технічна підтримка	Так	Так	Так
Гнучкість ціноутворення	Так	Так	Частково для великого бізнесу
Впровадження інноваційних рішень	Ні	Ні	Так
Загальна оцінка Gartner з відгуків користувачів	4.5/5	4.5/5	4.4/5.

Таким чином, провівши порівняльний аналіз технологій та функціоналу рішень PAM, можемо зробити висновки, що обов'язковими компонентами будь-якого рішення є менеджер паролів та менеджер сесій (сеансів), а опціональними – модуль з аналітикою привілейованих сеансів та менеджер доступу. Щодо можливостей, вони дуже схожі у всіх рішень, адже більшість це необхідні функції, без яких продукт буде виглядати неповноцінним. Аналізуючи схеми роботи модулів кожного рішення прослідковується

схожа логіка, але різні підходи, що все одно робить кожне рішення індивідуальним. Маючи такий функціонал як сховище паролів, їх планова перевірка та ротація, моніторинг у реальному часі, підтримка двофакторної аутентифікації, відповідність стандартам та можливості інтеграцій з корпоративними системами – кожне рішення може покривати мінімальні вимоги щодо контролю та управління привілейованим доступом.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

PAM розглядається багатьма аналітиками та технологами як один із найважливіших проєктів безпеки для зниження кіберризиків та досягнення високої рентабельності інвестицій. Керівникам компаній слід пам'ятати, що контроль та керування привілейованими обліковими записами не є додатковим заходом безпеки для організації, а є необхідністю, якій слід віддавати перевагу, вибираючи індивідуально ті рішення та підходи, які задовольняють компанію.

Вектор наступних досліджень спрямовується на модифікацію алгоритму керування привілейованим доступом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1 Infographic: 20 Alarming Insider Threats Statistics https://www.stealthlabs.com/blog/infographic-20-alarming-insider-threats-statistics/
2 2020 Insider Threat Report https://www.cybersecurity-insiders.com/portfolio/2020-insider-threat-report-gurucul/
3 (2022) Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
4 EMA Evaluation Guide to Privileged Access Management (PAM). https://loughtec.com/wp-content/uploads/2022/03/ema_eval_guide_to_privileged_access_management_pam-1.pdf
5 Tep, K. S., Martini, B., Hunt, R., & Choo, K.-K. R. (2015). A Taxonomy of Cloud Attack Consequences and Mitigation Strategies: The Role of Access Control and Privileged Access Management. У *2015 IEEE Trustcom/BigDataSE/ISPA*. IEEE. https://doi.org/10.1109/trustcom.2015.485.
6 Jayabalan, M., & O'Daniel, T. (2016). Access control and privilege management in electronic health record: a systematic literature review. *Journal of Medical Systems*, *40*(12). https://doi.org/10.1007/s10916-016-0589-z
7 Gaehtgens, F., Data, A., Kelley, M., Rakheja, S. (2021). Magic Quadrant for Privileged Access Management.
8 https://www.gartner.com/doc/reprints?id=1-27MYWKG6&ct=211012&st=sb
9 Sindiren, E., Ciylan, B. (2018). Privileged Account Management Approach for Preventing Insider Attacks. *IJCSNS International Journal of Computer Science and Network Security,* 18(1).
10 Haber, M. J. Hibbert, B. (2018). Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations. https://doi.org/10.1007/978-1-4842-3048-0, https://libraff.com/b/w/c979cb0ee57fbbfe6487e2e357d71de8b9526b93/privileged-attack-vectors-building-effective-cyber-defense-strategies-to-protect-organizations.pdf
11 Бурячок, В. Л., Толубко, В. Б., Хорошко, В. О., & Толюпа, С. В. (2015). Інформаційна та кібербезпека: соціотехнічний аспект : підручник. ДУТ.
12 Гулак, Г. М., Козачок, В. А., Складанний, П. М., Бондаренко, М. О., Вовкотруб, Б. В. (2017). Системи захисту персональних даних в сучасних інформаційно-телекомунікаційних системах. *Сучасний захист інформації*, *2*, 65-71. http://nbuv.gov.ua/UJRN/szi_2017_2_12.
13 Shevchenko, S., ZhdanovaY., Skladannyi, P., Boiko, S. (2022). Інсайдери та інсайдерська інформація: суть, загрози, діяльність та правова відповідальність. *Електронне фахове наукове видання "Кібербезпека: освіта, наука, техніка;*, *3*(15), 175-185. https://doi.org/10.28925/2663-4023.2022.15.175185

14 Privileged Access Management (PAM). https://www.cyberark.com/what-is/privileged-access-management/
15 Access Management (PAM). Управління повним циклом використання високопрівілегірованних облікових даних. https://senhasegura.com.ua/products/access-management-pam/
16 What Is Privileged Access Management (PAM)? https://heimdalsecurity.com/blog/privileged-access-management-pam/
17 Secure, Control & Audit Privileged Session Activity https://www.wallix.com/privileged-access-management/session-manager/
18 What is IT/OT convergence? Everything you need to know https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence
19 Magic Quadrant for Privileged Access Management https://www.gartner.com/doc/reprints?id=1-27MYWKG6&ct=211012&st=sb
20 KuppingerCole Leadership Compass PAM 2021 https://lp.cyberark.com/kuppingercole-leadership-compass-pam-2021.html

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (16), 2022
ISSN 2663 - 4023

Oleksandr M. Romaniuk
student of the Faculty of Information Technology and Management
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID ID: 0000-0002-1214-9406
ombabych.fitu18@kubg.edu.ua

Pavlo M. Skladannyi
PhD,
Head of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-7775-6039
p.skladannyi@kubg.edu.ua

Svitlana M. Shevchenko
PhD, Associate Professor,
Associate Professor of the Department of Information and Cybersecurity
named after Professor Volodymyr Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine
ORCID: 0000-0002-9736-8623
s.shevchenko@kubg.edu.ua

COMPARATIVE ANALYSIS OF SOLUTIONS TO PROVIDE CONTROL AND MANAGEMENT OF PRIVILEGED ACCESS IN THE IT ENVIRONMENT

Abstract. Abuse of privileges in the IT environment is defined as one of the threats to the information assets of the business at the present stage. The article examines and analyzes these problems, which are closely related to the leakage of information due to legitimate access to it and / or unauthorized access to it. Reports, research, acts, surveys at various enterprises contain a large amount of analytical and statistical materials that confirm the relevance and importance of this work. Based on the scientific literature, a review of key definitions on this issue, namely: characterized the definition of "privileged access"; the main examples of privileged access in the IT environment are considered; describes the risks and threats of information from attack vectors associated with privileged access to the IT environment. The mechanism for control and management of privileged access - RAM is presented, the steps of this process are highlighted and its expediency is substantiated. Experimental techniques allowed to choose the most applicable solutions of RAM: WALLIX Bastion PAM, One Identity Safeguard PAM, CyberArk PAM. The essence and functionality of each of these solutions are revealed. The advantages and disadvantages of each technology are established. As a result of research of technical and functional characteristics the comparative analysis of data of three decisions is carried out: obligatory components of the decision on control and management of privileged access are the manager of passwords and the manager of sessions (sessions), and additional - the module with analytics of privileged sessions and the access manager. use a VPN to access privileged assets. It can also be noted that the functionality of all products is very similar, so the implementation plays a big role, namely the practical approach during operation, internal algorithms, additional opportunities for integration and innovation. PAM solutions are recommended for organizations as a means to mitigate information security risks and threats due to insider activities of company employees who have privileged access to the IT environment.

Keywords: information security; internal threats; privileged access; unauthorized access; control and management of privileged access.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1 Infographic: 20 Alarming Insider Threats Statistics https://www.stealthlabs.com/blog/infographic-20-alarming-insider-threats-statistics/
2 2020 Insider Threat Report https://www.cybersecurity-insiders.com/portfolio/2020-insider-threat-report-gurucul/
3 (2022) Data Breach Investigations Report. https://www.verizon.com/business/resources/reports/dbir/
4 EMA Evaluation Guide to Privileged Access Management (PAM). https://loughtec.com/wp-content/uploads/2022/03/ema_eval_guide_to_privileged_access_management_pam-1.pdf
5 Tep, K. S., Martini, B., Hunt, R., & Choo, K.-K. R. (2015). A Taxonomy of Cloud Attack Consequences and Mitigation Strategies: The Role of Access Control and Privileged Access Management. У *2015 IEEE Trustcom/BigDataSE/ISPA*. IEEE. https://doi.org/10.1109/trustcom.2015.485.
6 Jayabalan, M., & O'Daniel, T. (2016). Access control and privilege management in electronic health record: a systematic literature review. *Journal of Medical Systems*, *40*(12). https://doi.org/10.1007/s10916-016-0589-z
7 Gaehtgens, F., Data, A., Kelley, M., Rakheja, S. (2021). Magic Quadrant for Privileged Access Management.
8 https://www.gartner.com/doc/reprints?id=1-27MYWKG6&ct=211012&st=sb
9 Sindiren, E., Ciylan, B. (2018). Privileged Account Management Approach for Preventing Insider Attacks. *IJCSNS International Journal of Computer Science and Network Security*, 18(1).
10 Haber, M. J. Hibbert, B. (2018). Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations. https://doi.org/10.1007/978-1-4842-3048-0, https://libraff.com/b/w/c979cb0ee57fbbfe6487e2e357d71de8b9526b93/privileged-attack-vectors-building-effective-cyber-defense-strategies-to-protect-organizations.pdf
11 Buriachok, V. L., Tolubko, V. B., Khoroshko, V. O., & Toliupa, S. V. (2015). Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt : pidruchnyk. DUT.
12 Hulak, H. M., Kozachok, V. A., Skladannyi, P. M., Bondarenko, M. O., Vovkotrub, B. V. (2017). Systemy zakhystu personalnykh danykh v suchasnykh informatsiino-telekomunikatsiinykh systemakh. Suchasnyi zakhyst informatsii, 2, 65-71. http://nbuv.gov.ua/UJRN/szi_2017_2_12.
13 Shevchenko, S., ZhdanovaY., Skladannyi, P., Boiko, S. (2022). Insaidery ta insaiderska informatsiia: sut, zahrozy, diialnist ta pravova vidpovidalnist. Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika; 3(15), 175-185.https://doi.org/10.28925/2663-4023.2022.15.175185
14 Privileged Access Management (PAM). https://www.cyberark.com/what-is/privileged-access-management/
15 Access Management (PAM). Upravlinnia povnym tsyklom vykorystannia vysokoprivilehirovannykh oblikovykh danykh. https://senhasegura.com.ua/products/access-management-pam/
16 What Is Privileged Access Management (PAM)? https://heimdalsecurity.com/blog/privileged-access-management-pam/
17 Secure, Control & Audit Privileged Session Activity https://www.wallix.com/privileged-access-management/session-manager/
18 What is IT/OT convergence? Everything you need to know https://www.techtarget.com/searchitoperations/definition/IT-OT-convergence
19 Magic Quadrant for Privileged Access Management https://www.gartner.com/doc/reprints?id=1-27MYWKG6&ct=211012&st=sb
20 KuppingerCole Leadership Compass PAM 2021 https://lp.cyberark.com/kuppingercole-leadership-compass-pam-2021.html