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

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Дослідження шляхів та розробка рекомендацій щодо впровадження PAM для захисту інформаційної системи організації від несанкціонованого доступу на прикладі Wallix Bastion»

зі спеціальності *125 Кібербезпека*
(код, найменування спеціальності)

освітньо-професійної програми *Інформаційна та кібернетична безпека*
(назва програми)

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

_____ Ярослав ШАНДРОВСЬКИЙ
(підпис)

Виконав: здобувач вищої освіти групи БСД-41
ШАНДРОВСЬКИЙ Ярослав
(прізвище, ім'я)

Керівник професор д.т.н. ГАЙДУР Галина
(науковий ступінь, вчене звання, прізвище, ім'я)

Рецензент _____
(науковий ступінь, вчене звання, прізвище, ім'я)

Київ 2024

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

API – Application Programming Interface

CIEM - Cloud Infrastructure Entitlement Management

DMZs – Demilitarized Zones

EMEA - Europe, Middle East, and Africa

IAM – Identity And Access Management

IDM – Identity Management

IT – Information Technologies

ITSM – IT-Services Management

OT – Operational Technologies

PaaS – Platform as a Service

PAM – Privileged Access Management

PASM - Privileged Account and Session Management

PEDM - Privilege Elevation and Delegation Management

PPM – Privileged Password Management

PUM – Privileged User Management

RBAC – Role-Based Access Control

SIEM – Security Information and Event Monitoring

SSO – Single Sign-On

VPN – Virtual Private Network

ІС – Інформаційні Системи

НСД – Несанкціонований Доступ

ВСТУП

Акутальність дослідження. Інформаційні системи відіграють ключову роль у забезпеченні безперервної діяльності сучасних організацій. Вони містять цінні та конфіденційні дані, порушення конфіденційності, цілісності та/або доступності яких може завдати серйозної шкоди організації. Захист цих систем від несанкціонованого доступу є критично важливим завданням для забезпечення інформаційної безпеки організації.

Одним з найбільших ризиків для інформаційних систем є компрометація привілейованих облікових записів, які надають широкі повноваження для управління системними ресурсами та конфігураціями. Зловмисники часто прагнуть отримати доступ до цих облікових записів, щоб здійснювати шкідливу діяльність, розповсюджувати шкідливе програмне забезпечення або викрадати конфіденційні дані.

Управління привілейованим доступом (PAM) є ефективним підходом для захисту інформаційних систем від цих загроз. Впровадження рішень PAM, таких як Wallix Bastion, дозволяє організаціям контролювати та відстежувати використання привілейованих облікових записів, забезпечуючи ізоляцію, аудит і підвищений рівень безпеки цих критично важливих ресурсів. Дослідження методів та засобів впровадження PAM на прикладі Wallix Bastion є актуальним для підвищення захисту інформаційних систем організацій від зловмисників.

Об'єкт дослідження – захист привілейованих облікових записів інформаційної системи організації від несанкціонованого доступу.

Предмет дослідження – методи та засоби захисту привілейованих облікових записів інформаційної системи організації від несанкціонованого доступу на прикладі Wallix Bastion.

Мета роботи – розробка рекомендацій щодо впровадження PAM-системи для захисту привілейованих облікових записів інформаційної системи організації від несанкціонованого доступу.

Наукові завдання:

дослідити сутність проблеми захисту інформаційної системи організації від несанкціонованого доступу;

проаналізувати основні підходи до захисту інформаційної системи організації від несанкціонованого доступу;

проаналізувати існуючі рішення PAM із захисту інформаційної системи організації від несанкціонованого доступу;

проаналізувати методи та засоби впровадження PAM для захисту інформаційної системи організації від несанкціонованого доступу на прикладі Wallix Bastion;

розробити рекомендацій щодо впровадження PAM для захисту інформаційної системи організації від несанкціонованого доступу.

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

Практичне значення одержаних результатів: розроблено рекомендації щодо застосування методів та засобів захисту інформаційної системи організації від несанкціонованого доступу, а також розроблено рекомендації фахівцям з кібербезпеки щодо їх реалізації.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Цифрова трансформація кібербезпеки», яка відбулася 26 квітня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ПРИВІЛЕЙОВАНИХ ОБЛІКОВИХ ЗАПИСІВ В ІС ОРГАНІЗАЦІЇ

1.1. Аналіз поняття та змісту привілейованих облікових записів в ІС організації

Несприятливі наслідки кібератак продовжують ставати серйозною загрозою для сучасних організацій, незважаючи на величезні зусилля, які вони вкладають у забезпечення безпеки своєї інфраструктури. Зловмисникам все ще вдається отримати несанкціонований доступ до корпоративних інформаційних систем, що часто призводить до крадіжки або знищення конфіденційних даних та інших важливих ресурсів.

Крім того, як це свідчить звіт компанії Apple, спостерігається тенденція зростання кількості таких інцидентів з кожним роком (у глобальному масштабі кількість жертв у 2023 році зросла вдвічі порівняно з 2022 роком), що свідчить про недостатню ефективність захисних заходів та потребу в удосконаленні підходів до реалізації захисту інформації [1].

Проте, чому не вдається повністю захистити інформаційні системи від кіберзагроз? Що саме перешкоджає всім цим колосальним зусиллям у досягненні мети? Ці запитання є на чолі досліджень та обговорень у галузі інформаційної безпеки. Нерідко вони ведуть до відкриття ключових причин, які лежать в основі зростання тенденції до інцидентів несанкціонованого доступу до інформаційних систем організацій, що призводить до витоків даних.

Першою із цих причин є постійне ускладнення IT-середовища, де кожен користувач отримує все більший функціонал налаштування систем, а процеси автоматизації зробили системи ще вразливішими.

По-друге, зловмисники використовують нові технології, атакуючи системи інноваційними методами для здійснення більш ефективних атак.

По-третє, різноманіття технологічних постачальників рішень захисту може створювати додаткові проблеми та невизначеність.

Такий ландшафт створює різноманітні точки вразливості для несанкціонованого доступу (рис. 1.1), що становить серйозну загрозу безпеці даних та систем, а беручи до уваги той факт, що найслабшим ланцюгом у всій інфраструктурі – є сам користувач, то за принципом найменшого опору - основним вектором атаки виявляється привілейований доступ та облікові записи, що пов’язані з ним [2].

Рис. 1.1. Стан проблеми несанкціонованого доступу [2]

Морей Хейбер, головний радник з питань безпеки (Chief Security Advisor) в компанії BeyondTrust, пропонує таке основне визначення поняття привілеїв: «Спеціальне право або дозвіл, наданий або доступний лише певній особі чи групі осіб для виконання особливих або чутливих операцій над ресурсом або в його межах. В контексті інформаційних технологій, вони зазвичай асоціюються з обліковими записами чи групами адміністраторів або root-обліковими записами, а також з будь-якими обліковими записами, яким можуть бути надані підвищені повноваження.» [3].

Таким чином, звідси виходить, що привілеї - це особливі права чи переваги,

які виходять за рамки звичайних норм чи дозволів і надаються лише обмеженій групі осіб. Це піднесення над загальноприйнятими правилами та нормативами, характерне для вузького кола користувачів або суб'єктів.

У реальному житті, це поняття можна пов’язати з поняттям освіта. Освіта - це право, доступне для всіх, а не привілей для обраних. Екстраполюючи це на IT-середовище: стандартні користувачі в організації мають базовий набір прав доступу, передбачений для більшості автентифікованих користувачів системи. Стандартний користувач має ті ж самі основні права, що й майже всі інші; він не є привілейованим. Тому в типовій організації стандартні користувачі мають права, які є глобальними для всіх автентифікованих користувачів - так само, як і з освітою.

Натомість привілейовані облікові записи - це ті, які наділені розширеними правами та можливостями, що виходять за рамки стандартних користувацьких прав, доступних для більшості. Вони потрібні лише невеликій групі адміністраторів, розробників чи IT-персоналу для виконання специфічних завдань.

Деталізація розрізнення загальних типів користувачів за рівнем їх привілеїв може мати стільки рівнів, скільки сама організація вважає за потрібне, виходячи з ролей і посад, обов’язків своїх користувачів. У найпростішій ієрархічній схемі інтерпретації привілеїв міститься лише два рівні:

Стандартні користувачі: відповідно загальні та спільні права, що надані всім користувачам для виконання довірених завдань;

Користувачі-адміністратори: закономірно володіння широким набором привілейованих прав, наданих для управління всіма аспектами системи та її ресурсами. Це може включати встановлення програмного забезпечення, керування параметрами конфігурацій, застосування виправлень, керування користувачами тощо.

Представлена ієрархічній схемі має загальне відображення, однак не підкреслює основних тонкощів розподілу привілейованих прав. Тож на практиці, більшість організацій визначають ієрархію привілеїв за п'ятьма основними рівнями (рис. 1.2):

Жодного доступу: це означає, що у користувача немає облікового запису, або

існуючий обліковий запис було вимкнено чи видалено. Це відмова в будь-якій формі доступу, навіть анонімного;

Гостьовий обліковий запис користувача: обліковий запис, що має обмежений доступ і права нижчі за звичайного (стандартного) користувача. Часто цей вид облікових записів пов’язано із анонімним доступом;

Стандартний користувач: обліковий запис, що має спільні права, надані всім користувачам для виконання довірених завдань;

Привілейований користувач: обліковий запис, що має всі права стандартного користувача, за виключенням додаткових привілеїв для виконання певних завдань. Цей тип облікових записів – не є адміністраторським або обліковим записом суперкористувача, однак йому довіряють виконання певних завдань, які зазвичай асоціюються з адміністраторами;

Обліковий запис адміністратора: обліковий запис, що має авторизовані дозволи (у формі привілеїв) для зміни процесів, конфігурацій, налаштувань, керуваннями користувачами та встановленим програмним забезпеченням і ресурсами інформаційних систем тощо. Для уточнення, цей тип облікових записів також можна розбити на підкатегорії - локальні адміністратори (для одного ресурсу) та адміністратора домену (для багатьох ресурсів). Відповідно, права цього типу облікових записів, на відміну від прав вище зазначених облікових записів - дають значно ширші можливості впливу та зміни в корпоративних інформаційних системах.

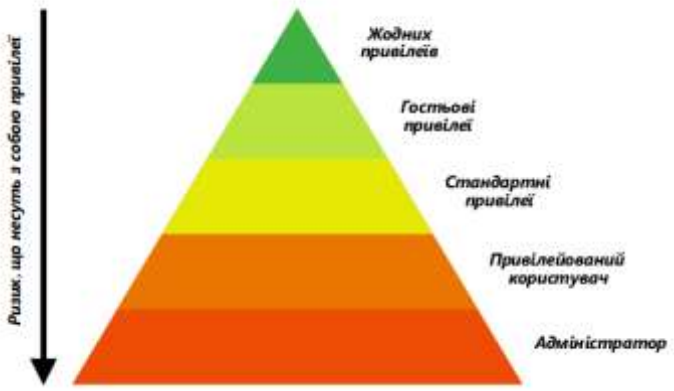

Рис. 1.2. Ієрархічна схема привілейованих облікових записів

Хоча такий розгляд у макромасштабі надає певне розуміння ризику, що несуть із собою певні рівні привілеїв користувачів - важливо також зосередитися на мікрорівні дозволів, зокрема на рівнях файлів, окремих функцій та самої інформації, для забезпечення належного захисту. Обмежувати розуміння привілеїв лише правами виконання певних програм буде надто вузьким підходом.

Концепцію привілейованого доступу необхідно реалізовувати у всіх компонентах IT-інфраструктури – бази даних, додатки, гіпервізори, файлові системи, операційні системи, платформи управління хмарними ресурсами та навіть мережеву інфраструктуру через механізми сегментації. Лише за такого комплексного підходу привілеї будуть ефективно реалізовуватися як для користувачів, так і у процесах комунікації між додатками.

Однак, слід також зазначити, що ці принципи справедливі, у разі, якщо здійснюється автентифікація, за допомогою будь-якого механізму, починаючи від імені користувача і пароля і закінчуючи парою ключів сертифіката. Належний контроль привілеїв інформаційного ресурсу може бути ефективним лише у тому разі, коли вони продумані та застосовані на кожному рівні інфраструктури.

З цією метою, повстає необхідність детальнішого розгляду привілеїв кожного рівня (за виключенням того, що зовсім не має повноважень) (рис. 1.3):

Гостьовий обліковий запис користувача

Гостьовим користувачам надаються суворо обмежені привілеї, що дозволяють виконувати лише деякі обмежені функції та завдання. У багатьох компаніях гостьові користувачі ізолюються в окремі сегменти мережі з базовим доступом, наприклад до мережі Інтернет, але без доступу до внутрішніх корпоративних ресурсів. Ця ізоляція мінімізує ризики у випадку компрометації гостьових систем, обмежуючи можливості бічних переміщень зловмисників всередині IT-середовища організації.

Наприклад, скомпрометована гостьова система не повинна отримувати прямий доступ до внутрішніх корпоративних систем і даних у разі сканування мережі, незалежно від типу мережевого підключення, чи то було підключення через Ethernet або бездротове з'єднання.

Стандартний користувач

Стандартний обліковий запис користувача – відповідно має деякі привілеї, що перевищують можливості гостьового користувача, щоб задовольняти вимогам базових завдань в організації, пов’язану з роботою та роллю. Не зважаючи на той факт, що організація може у своїй практиці відмовитися від застосування гостьових облікових записів як таких, від стандартних – неможливо, оскільки існує певна градація між цим, а також наступним рівнем – привілейованим користувачем.

Типові організації можуть мати сотні або тисячі різних шаблонів стандартних користувачів, призначених для збалансування доступу та ефективності боротьби з ризиком. Кожній ролі надано доступ до певних систем, додатків, ресурсів і даних, необхідних для виконання конкретної роботи.

У багатьох випадках користувач може бути членом кількох груп, залежно від його конкретних посадових обов'язків. Наприклад, ролі з обмеженим доступом (також звані базовими ролями, базовими правами та правами при «народженні» у контексті управління ідентичностями) зазвичай надаються кожному користувачеві організації (працівнику, підряднику) для забезпечення базового доступу.

Наприклад, це може бути доступ до електронної пошти та корпоративної Інтрамережі. Далі цього рівня вже йдуть конкретні привілеї, які надають додатковий доступ на основі посадових обов'язків або самої специфіки ролі.

Привілейований користувач

Привілейований користувач - це підвищений випадок використання стандартного користувача, який взаємодіє з програмами та ресурсами, що потребують унікальних, чутливих або розширених функцій, які не мають права використовувати «пересічні» користувачі. Привілейований користувач може не володіти глибокими технічними знаннями про ресурси, з якими він працює, але має компетенцію або роль, що дозволяє йому діяти в рамках привілейованих інструкцій для виконання конкретних завдань.

Крім того, в організації привілейований користувач може мати формальну роль, відведену окремій особі, і може вважатися фахівцем з певного програмного забезпечення, ролі або ресурсу. Часто це люди, які навчені виконувати розширені

функції, що виходять за рамки їхніх типових посадових обов'язків, і, таким чином, мають відповідні привілеї. Привілейовані користувачі представляють множину, що є проміжною між стандартними користувачами та повноцінними адміністраторами на основі явних привілеїв, наданих для виконання конкретних завдань.

Знову ж таки, вони не є адміністраторами, але на основі наданих їм привілеїв можуть бути джерелом привілейованих векторів атак. Це особливо актуально, якщо їм надано надмірні права, які повинні контролюватися на зловживання ними, оскільки їхні привілеї дозволяють отримувати доступ до потенційно чутливих можливостей.

Нарешті, деякі типові ролі, які асоціюються з привілейованими користувачами, зазвичай зустрічаються серед розробників, співробітників служби підтримки, адміністраторів додатків і баз даних (навіть якщо вони не мають адміністративних або root-привілеїв), і навіть серед інженерів.

Обліковий запис адміністратора

Адміністратор або Root-користувач - "володіє" системою та всіма її ресурсами. Всі функції, конфігурації та можливості потенційно знаходяться під їхнім контролем, оскільки привласнення адміністративних привілеїв суб'єктом ефективно нівелює застосовність засобів безпеки та контролю доступу для відповідної обчислювальної системи або середовища. Здобуття статусу адміністратора, так чи інакше, надає можливість обходити існуючі механізми обмеження прав і політики безпеки, анулюючи їхню дієвість та захисну спроможність щодо суб'єкта з отриманими повноваженнями.

Таким чином, отримання прав адміністратора або root-доступу, що надає повний привілейований доступ – вважається головною ціллю для зловмисника. Якщо суб'єкт загрози має привілейований доступ і може діяти непомітно, то будь-яка система, додаток або дані потенційно опиняються в межах його досяжності. Отже, отримання привілеїв - це основний вектор атаки для проникнення в організацію, або комп'ютерного пристрою кінцевого користувача.

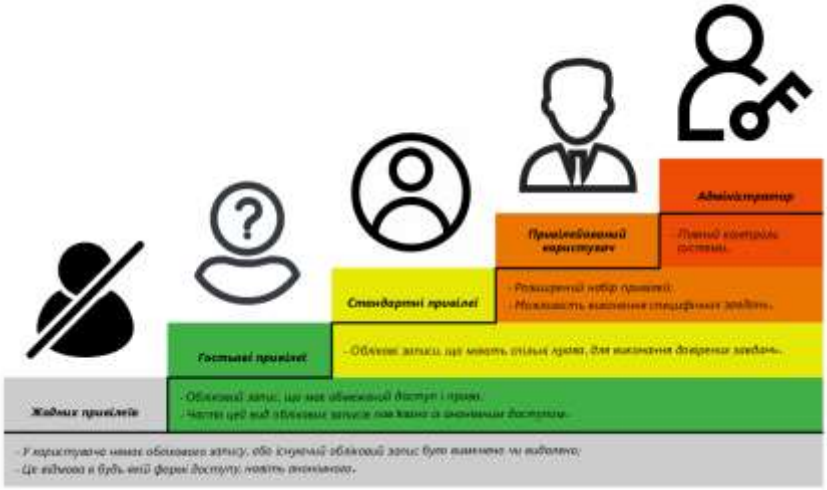

Рис. 1.3. Загальні класи користувачів

Привілейований доступ у контексті інформаційних систем та автоматизації бізнес-процесів розглядається з нової перспективи. Попри традиційну ієрархічну структуру облікових записів користувачів з різними рівнями прав доступу, зростаюча автоматизація вносить свої корективи.

З одного боку, класичний підхід із чітким розподілом привілеїв між обліковими записами адміністраторів, технічного персоналу та звичайних користувачів залишається актуальним. Проте, автоматизовані системи та програмні рішення також потребують власних привілейованих облікових записів для коректного функціонування та виконання делегованих їм завдань і бізнес-процесів.

У сучасному середовищі інформаційних технологій привілейований доступ не обмежується лише людськими користувачами. Системам та програмним агентам також надаються спеціальні права та повноваження, необхідні для автоматизації робочих процесів, інтеграції з іншими системами, управління ресурсами та даними. Ретельне планування, налаштування та моніторинг таких привілейованих облікових записів стає невід'ємною частиною належного управління та забезпечення безпеки автоматизованих середовищ.

Відповідно до людських облікових записів, з не-людських також можна побудувати, як скорочену дворівневу, так і загальну розширену – ієрархічну схему

(рис. 1.4):

Жодного доступу: відповідно до назви, як і у разі людського типу облікового запису - це означає, що у користувача немає облікового запису, або існуючий обліковий запис було вимкнено чи видалено;

Сервісні облікові записи: є одним із найнижчих рівнів привілеїв для автоматизованих процесів і систем. Їх призначено для надання обмежених прав доступу, необхідних для виконання певних сервісних функцій або задач у системі. Ці облікові записи зазвичай використовуються для фонових процесів, системних служб або утиліт. Приклади прав, що надаються сервісним обліковим записам, можуть включати доступ на читання/запис у визначених каталогах, доступ до специфічних системних ресурсів (наприклад, мережевих служб або пристроїв вводу-виводу) або виконання обмежених адміністративних завдань. Привілеї ретельно обмежуються лише тими операціями, які необхідні для належного функціонування відповідного сервісу чи утиліти;

Облікові записи застосунків: надають привілеї, необхідні для належної роботи різних програмних рішень та застосунків в системі. Ці привілеї можуть бути досить різноманітними, залежно від вимог конкретного застосунку та його функціональності. Наприклад, обліковий запис веб-застосунку може потребувати доступу до бази даних для зчитування та запису інформації, доступу до системних бібліотек для взаємодії з операційною системою, мережевого доступу для обміну даними з іншими системами тощо. Окремий застосунок для обробки зображень може вимагати прав на читання та запис у визначених каталогах для зберігання та маніпулювання файлами зображень;

Системні облікові записи: мають високий рівень привілейованого доступу, що дозволяє їм виконувати критичні операції з управління та адміністрування системними компонентами, конфігураціями та безпекою. Ці облікові записи зазвичай використовуються системними службами або процесами автоматизації для підтримки належної роботи та безпеки операційних систем, середовищ або складних програмних рішень. Привілеї системних облікових записів можуть включати можливість встановлювати системні оновлення та патчі, управляти

користувачами та їхніми дозволами, налаштовувати системні служби та компоненти, аналізувати журнали подій та виконувати різноманітні завдання з адміністрування та моніторингу системи. Доступ системних облікових записів є досить широким, оскільки вони повинні мати можливість отримувати доступ до системних файлів, конфігурацій, реєстрів та інших критичних ресурсів для забезпечення належного функціонування та безпеки всієї системи;

Машинні облікові записи: мають найвищий рівень привілейованого доступу в ієрархії автоматизованих систем та процесів. Вони можуть мати практично необмежені повноваження для управління ресурсами, даними, конфігураціями та критичними операціями в межах свого домену чи середовища. Такі потужні облікові записи часто використовуються для високорівневих системних процесів, служб або агентів автоматизації, які відповідають за управління життєво важливими функціями, інтеграцію з іншими системами, забезпечення безперервності бізнес-процесів тощо. Приклади привілеїв машинних облікових записів можуть включати повний доступ до системних файлів та конфігурацій, можливість запускати та зупиняти критичні процеси, встановлювати оновлення та виправлення на найвищому рівні, керувати розподілом ресурсів та виконувати операції з високим рівнем ризику.

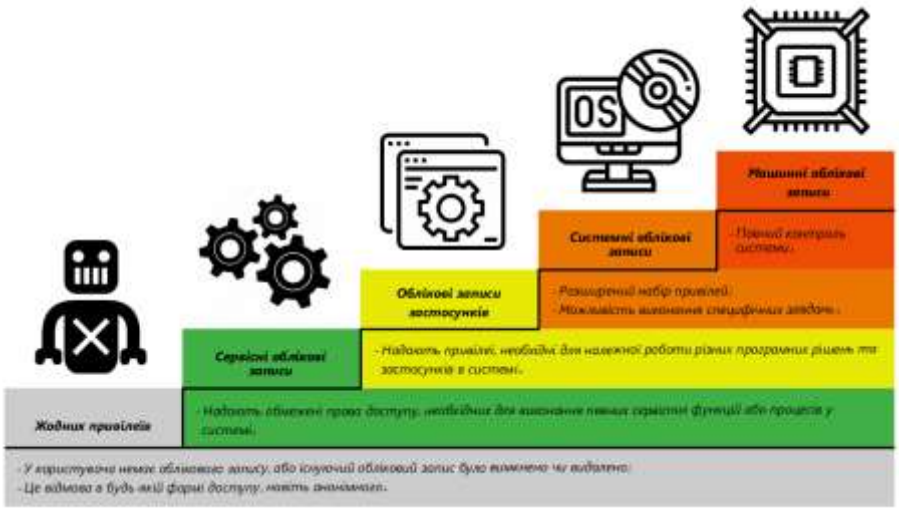

Рис. 1.4. Загальні класи не-людських користувачів

В решті решт, незалежно від того, чи йдеться про людський обліковий запис, чи програмний, для забезпечення належного розмежування контролю доступу та безпеки, використовуються облікові дані.

Облікові дані - це сукупність облікового запису з пов'язаним з ним паролем, кодом, сертифікатом або іншим типом потенційно секретного ключа. Облікові дані можуть мати більше одного механізму безпеки, призначеного для подвійної або багатофакторної автентифікації, або бути базовими гостьовими обліковими даними, до яких може отримати доступ будь-хто - без потреби в секретному ключі або за допомогою звичайного, відомого ключа. Облікові дані - це лише просте представлення комбінації облікового запису та пароля, необхідної для автентифікації. Тим не менш, вони є головним ресурсом, що дає змогу будь-якому зловмиснику розпочати ескалацію привілеїв.

Відповідно, привілейовані облікові дані (також звані привілейованими паролями) - це підгрупа облікових даних, які надають підвищений доступ і дозволи в облікових записах, програмах і системах.

1.2. Аналіз загроз НСД до привілейованих облікових записів в ІС організації

У світі кібербезпеки привілейовані облікові записи є одним із найбільших джерел вразливостей та ризиків. Зловмисники часто зосереджуються саме на них, оскільки це найпростіший спосіб отримати доступ до критичних ресурсів та, зрештою, заволодіти всім середовищем.

Останні дослідження підкреслюють масштаби проблеми. Згідно зі звітом IDSA "2023 Trends in Securing Digital Identities", 90% організацій зазнали принаймні одного несанкціонованого втручання в інформаційну систему, пов'язаного з привілейованими обліковими даними, протягом 2022-2023 років. Ця тривожна статистика свідчить про те, наскільки поширеними є атаки, що експлуатують привілейовані облікові записи [4].

Крім того, згідно з "2023 Data Breach Investigations Report" від Verizon, 74% усіх витоків інформації включають людський фактор, через помилки, неправильне

використання привілеїв, використання викрадених облікових даних або соціальну інженерію [5].

Зловмисники добре усвідомлюють, що привілейовані облікові записи є найпростішим способом отримати доступ до критичних систем та даних організації. Тому захист цих облікових записів має бути пріоритетним завданням для забезпечення належного рівня кібербезпеки та стійкості IT-інфраструктури.

Сучасні способи несанкціонованого доступу до інформаційних систем з використанням привілейованих облікових записів часто реалізуються за схожим сценарієм і може приймати наступний вигляд вектору атаки, який в загальному випадку може мати наступну форму (рис. 1.5).

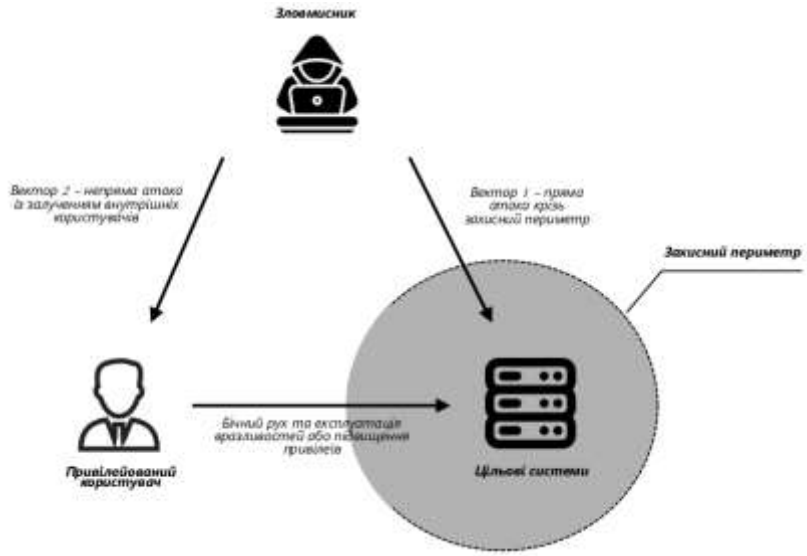

Рис. 1.5 Загальний (макро) вигляд вектору атаки на інформаційні системи

Виходячи з наведеної ілюстрації, загалом можна виділити два основні вектори атаки, доступні для зловмисника:

1. Спроба прямої атаки на чутливий інформаційний ресурс, який містить в собі конфіденційні дані. Такі системи, як правило, мають регулярні оновлення, належний рівень моніторингу та захисту, використовуючи передові технології виявлення загроз через їхню чутливість і відповідність регуляторним вимогам. Тому на сьогодні цей варіант є найменш імовірним для реалізації атаки;

2. Спроба непрямої атаки на чутливий інформаційний ресурс, із

залученням внутрішніх користувачів та їх облікових записів, виконання бічного руху з метою підвищення привілейованих прав. В такому разі, зловмисник оминає більшість існуючих засобів захисту, оскільки для них він діє як внутрішній законний користувач.

Основна ціль зловмисника буде цілком досягнена у тому разі, коли привілейований доступ до програми, її бази даних або допоміжної файлової системи – буде його досяжності. Цей вектор атаки також потенційно може дозволити зловмиснику виконувати команди, здійснювати бічні переміщення та викрадати додаткові дані, незалежно від того, чи є виступає він зовнішнім або внутрішнім порушником для інформаційної системи. Крім того, багато організацій надають більше привілеїв, ніж потрібно для конкретної роботи, що призводить до збільшення площини атаки і підвищує ризики для інформаційної безпеки.

Наприклад, багато організацій все ще дозволяють користувачам мати адміністративний контроль над своїми інформаційними системами просто для зручності або через застарілі програми, які вимагають адміністративних прав. Важливо також відзначити, що останнім часом атаки починають зосереджуватися на нетрадиційних активах, яким може не вистачати гнучкості та контролю, необхідних у сучасному складному середовищі загроз.

Причиною цього може бути той факт, що у деяких системах параметри контролю доступу – бінарні, що відображає дві опції, або повного, абсолютного доступу, або його повна відсутність. Це в першу чергу стосується споживчих пристроїв, які не мають концепції рольового доступу, але це також застосовно і до багатьох пристроїв Інтернету речей (IoT), застарілих систем і навіть технологій наступного покоління, що використовуються для виробництва, автоматизації та управління OT-технологіями.

Таким чином, щоб зрозуміти, де саме і на якому етапі виникають вразливості, необхідно детально розглянути вектор сучасних способів несанкціонованого доступу до інформаційних систем з використанням привілейованих облікових записів на мікрорівні (рис 1.6).

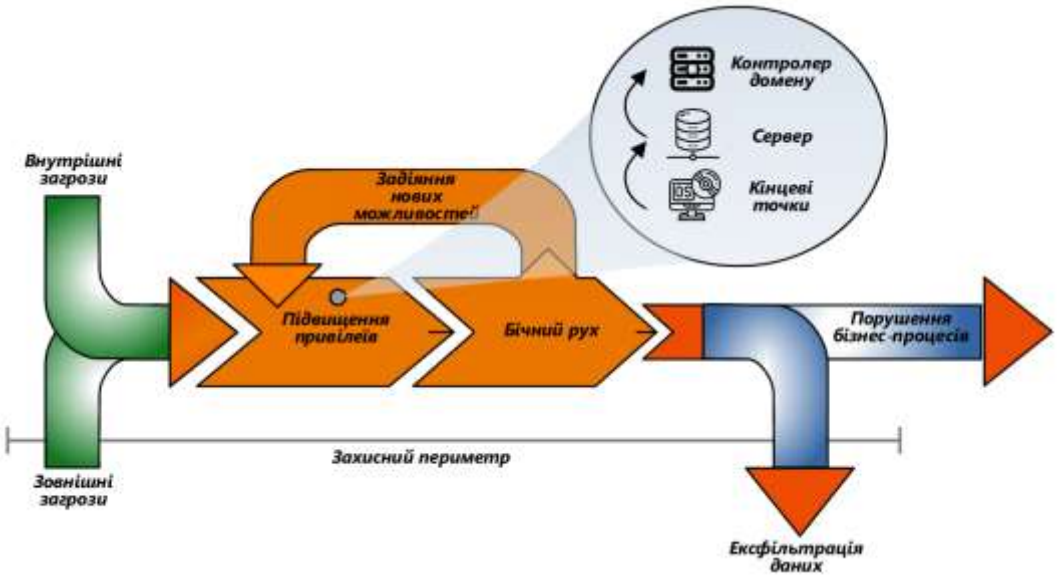

Рис. 1.6. Вузький (мікро) вигляд вектору атаки на інформаційні системи

Як можна це бачити з ілюстрації – атаку можна розбити на 6 основних етапів:

1. Проникнення (внутрішні та зовнішні загрози). Як це було сказано раніше, відійшли ті часи, коли зловмисники намагалися безпосередньо атакувати периметр захисту, натомість зараз вони фокусуються на більш витончених методах. Більш ніж ймовірно, що вони проведуть успішну кампанію, експлуатуючи неправильно налаштовані ресурси через скомпрометовані привілейовані облікові записи, або фішингові атаки з метою компрометації користувачів зсередини. Їх мета - потрапити в середину, залишаючись непоміченими системами безпеки та створивши стійкий внутрішній плацдарм. Крім того, ризик проникнення зростає через збільшення кількості віддалених працівників та різноманітність загроз, які складніше контролювати.

2. Командування та управління через Інтернет. Якщо це не програма-вимагач або автономне шкідливе програмне забезпечення, зловмисник швидко встановлює зв'язок із сервером управління, щоб завантажити набір інструментів і додаткове корисне навантаження. Це дозволяє йому оцінити обстановку і спланувати свій наступний крок.

3. Виявлення привілейованих облікових записів і спроба привілейованої ескалації. Суб'єкти загроз починають вивчати мережу, інфраструктуру,

привілейовані облікові записи, облікові дані та активи, що виконують щоденні та критичні функції (рис. 1.7). Вони починають шукати можливості отримати додаткові облікові дані, підвищити привілеї або просто використовувати вже скомпрометовані привілеї для доступу до ресурсів, додатків і даних.

4. Бічне переміщення між активами, обліковими записами та ресурсами. Зловмисники використовують викрадені облікові дані і знання про середовище, щоб скомпрометувати додаткові активи, ресурси та ідентичності (облікові записи) за допомогою бічного переміщення. Це продовжує їхню кампанію розповсюдження та навігації в середовищі жертви.

5. Пошук додаткових можливостей закріплення. Продовжуючи з'ясовувати інші слабкі місця, такі як вразливості, неправильно налаштовані хости та додаткові привілейовані облікові дані, суб'єкт загрози має на меті залишитися непоміченим. Якщо їхнє пересування або присутність буде виявлено, більшість організацій негайно намагатимуться пом'якшити наслідки інциденту. Таким чином, діючи в стелс-режимі, суб'єкт загрози може визначити більше цілей, встановити більше шкідливого програмного забезпечення або хакерських інструментів і розширити свою присутність, використовуючи додаткові вектори атаки - від вразливостей до скомпрометованих ідентифікаційних даних.

6. Витік або знищення даних. Нарешті, зловмисник збирає, сегментує і, зрештою, викрадає дані або, в найгіршому випадку, зазвичай знищує активи та ресурси відповідно до своєї місії (наприклад, програми-вимагачі). Важливо пам'ятати, що весь цей ланцюжок атак може бути виконаний інсайдером або зовнішнім зловмисником. Знання інсайдера можуть прискорити всі ці кроки і обійти засоби контролю безпеки, оскільки такі користувачі можуть вважатися такими, що заслуговують на довіру.

Згідно Нормативного документу технічного захисту інформації 1.4-001-2000 "Типове положення про службу захисту інформації в автоматизованій системі", цей тип загроз інформаційній системі визначається як "маскарад". Під "маскарадом" розуміється виконання одним користувачем інформаційної системи дій від імені іншого користувача, що може бути дозволено для останнього. Порушення полягає

у несанкціонованому присвоєнні прав і привілеїв іншого користувача, що називається симуляцією або моделюванням [6].

Цілі "маскараду" - приховування власних дій під ім'ям іншого користувача або отримання доступу до його даних/привілеїв. Успішна реалізація "маскараду" зловмисниками дозволяє їм приховати сліди своїх дій та отримати несанкціоновані права й привілеї в інформаційній системі.

Таким чином, після того, як було встановлено автентифікований сеанс будь-якого типу, незалежно від того, легітимний він чи зламаний, типова мета зловмисника - підвищити привілеї та витягти дані. Рисунок 6 ілюструє це на основі моделі, яку було представлено раніше.

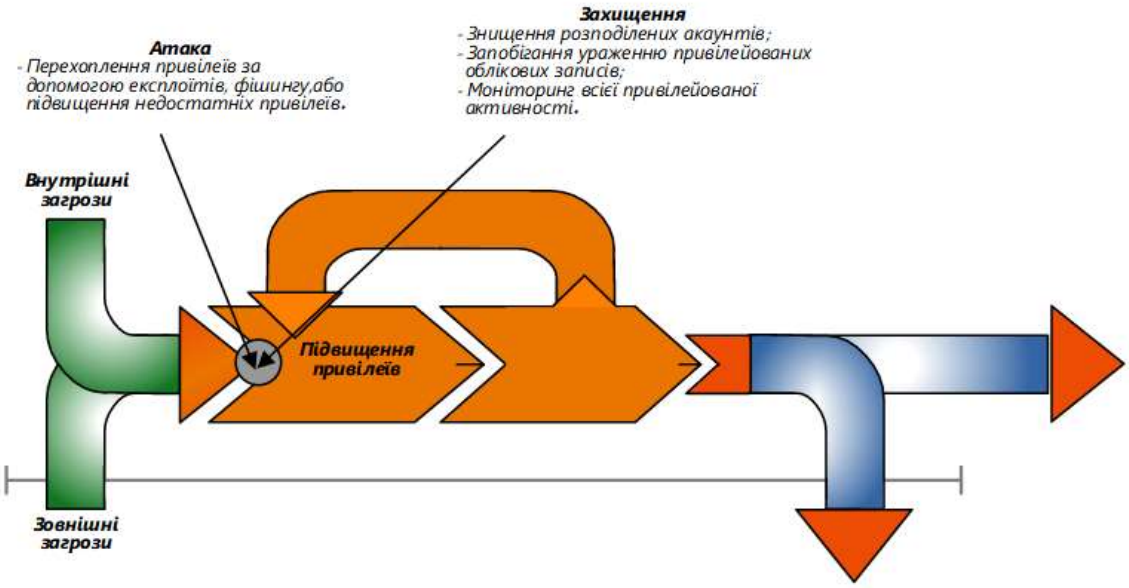

Рис. 1.7. Перехоплення привілеїв та їх підвищення

Звичайний користувач, як правило, не має прав на будь-які чутливі ресурси інформаційної системи. Отже, як зловмисник орієнтується в середовищі і отримує права адміністратора або root-користувача, щоб використовувати їх як вектор атаки? Так, існує п'ять основних загроз несанкціонованого доступу до привілейованих облікових записів інформаційної системи організації:

- Експлуатація облікових даних;
- Вразливості та експлоїти;

- Неправильна конфігурація;
- Шкідливе програмне забезпечення;
- Соціальна інженерія.

Експлуатація облікових даних. Успішна автентифікація із використанням легітимних облікових даних надає зловмиснику доступ до ресурсу. Проте, навіть за відомого імені користувача, отримання пароля стає лише питанням часу для досвідченого хакера. Зазвичай вони цілеспрямовано обирають адміністраторів або керівників, оскільки їхні облікові записи мають розширені привілеї для прямого доступу до конфіденційних даних і систем. Це дозволяє кіберзлочинцю просуватися далі, не викликаючи підозр.

Ключовим для успіху зловмисників є залишатися непоміченими. Після проникнення вони повинні закріпитися в інфраструктурі жертви. Встановлення цього плацдарму може бути результатом різних векторів - від експлуатації невстановлених оновлень безпеки до соціальної інженерії. Досягнувши успіху, зловмисники, як правило, ведуть спостереження та чекають слушної нагоди для подальшого розвитку атаки. При цьому вони намагаються йти шляхом найменшого опору і приховувати будь-які сліди своєї присутності.

Скомпрометовані облікові дані є найпростішим вектором привілейованої атаки для зловмисника, а пов'язані з ними облікові записи контролюють майже всі аспекти сучасного інформаційно-технологічного середовища, від адміністраторів до службових облікових записів.

Крадіжка облікових даних може здійснюватися різними способами: від банального повторного використання пароля до впровадження шкідливого ПЗ, яке вичитує їх з пам'яті. Викрадені адміністративні облікові дані дозволяють зловмиснику безпосередньо експлуатувати критичні ресурси. Навіть стандартні облікові дані користувача можуть надати доступ до конфіденційних даних відповідно до його ролі та посади в організації. Подальша ескалація привілеїв від рівня звичайного користувача до адміністратора може відбуватися за допомогою різних методів.

Вразливості та експлоїти. Сама по собі вразливість не гарантує успіху

привілейованого вектору атаки. Насправді, вразливість лише вказує на існування ризику та можливість успішної реалізації певного типу атаки. Вразливості є наслідком помилок у коді, дизайні, реалізації чи налаштуваннях, які потенційно дозволяють зловмиснику здійснити шкідливу дію шляхом експлуатації.

Отже, без наявності відповідного експлуатаційного коду (експлойту) вразливість залишається лише потенційною проблемою, що враховується під час оцінювання ризиків для визначення можливих наслідків. Залежно від характеру вразливості, доступних експлойтів та критичності ресурсу, на який вона впливає, фактичний ризик може бути незначним або ж катастрофічним. Хоча це спрощена модель оцінки реального ризику, вона формує основу для розуміння привілейованих векторів атаки.

Не всі вразливості та експлойти є рівноцінними. В залежності від привілеїв користувача чи програми, де наявна вразливість, ефективність та потенціал ескалації для певного вектору атаки можуть істотно відрізнятися. Тому характеристики конкретної вразливості безпосередньо впливають на ризики та наслідки її експлуатації.

Наприклад, вразливість операційної системи, яка може бути використана під час сеансу звичайного користувача або адміністратора, може мати дві абсолютно різні сукупності ризиків. Для звичайного користувача експлойт може взагалі не спрацювати, може бути обмежений лише привілеями звичайного користувача, або ж він може мати повний адміністративний доступ до інформаційної системи. Насправді, за даними BeyondTrust, 75% вразливостей Microsoft можна було б усунути, працюючи як звичайний користувач, а не як адміністратор. А якщо користувач використовує обліковий запис адміністратора домену або інші підвищені привілеї, експлойт може мати дозволи на все середовище [7].

Вразливості бувають різноманітними: в операційних системах, додатках, веб-застосунках, інфраструктурі тощо. Їх можуть використовувати для атак на протоколи, мережі, зв'язок між ресурсами. Проте не всі вразливості мають експлойти. Деякі з них є лише концепцією, деякі ненадійні, а деякі легко використовувати і навіть включені в комерційні інструменти тестування на

проникнення або безкоштовні хакерські інструменти з відкритим вихідним кодом. Частину вразливостей продають на чорних ринках для кіберзлочинців.

Таким чином, вразливості можуть бути будь-де і будь-коли. Важливим є те, як вони використовуються, і якщо вразливість сама по собі призводить до експлойту, який може змінити привілеї (підвищення привілеїв від одного користувача до іншого), то ризик є цілком реальним вектором привілейованої атаки. На сьогоднішній день 40% всіх вразливостей Microsoft дозволяють підвищити привілеї, що свідчить про те, що ця категорія є досить критичною для безпеки систем [7].

Неправильна конфігурація. Конфігураційні вади є різновидом вразливостей, які не потребують традиційного виправлення, а лише пом'якшення. Важливо розрізняти процеси виправлення та пом'якшення. Виправлення передбачає розгортання оновлень програмного чи апаратного забезпечення для усунення самої вразливості. Цей процес відомий як управління виправленнями. Натомість пом'якшення - це просто зміна на певному рівні в існуючій системі для зменшення ризику її використання зловмисниками. Це може бути зміна налаштувань у файлах, політиках безпеки, оновлення сертифікатів тощо. По суті, конфігураційні вади пов'язані із слабкими за замовчуванням налаштуваннями безпеки або неналежним захистом системи, що дозволяє легко використати їх для отримання привілейованого доступу.

Найпоширенішими є конфігураційні вади у налаштуваннях облікових записів, які ігнорують кращі практики безпеки. Наприклад, це може бути відсутність пароля або використання наперед відомого пароля за замовчуванням для адміністративних облікових записів. Або незахищений доступ, який не блокується після початкового встановлення системи через відсутність досвіду або навмисно залишений бекдор.

Шкідливе програмне забезпечення. Шкідливе програмне забезпечення - це загальний термін для будь-якого небажаного чи несанкціонованого програмного забезпечення, створеного із зловмисними намірами щодо комп'ютерної системи або мережі. Воно охоплює широкий спектр загроз, таких як віруси, шпигунські

програми, хробаки, програми-вимагачі, рекламні програми тощо. Головна мета шкідливого ПЗ може варіюватися від стеження, витоку конфіденційних даних, порушення роботи системи до повного її контролю та вимагання грошей. Фактично, шкідливе ПЗ може бути інструментом для вчинення будь-якого кіберзлочину залежно від наміру зловмисника.

Шкідливе ПЗ, як і будь-яка інша програма, може виконуватись із різними рівнями привілеїв - від обмежених прав користувача до адміністративних. Залежно від способу створення, наміру та отриманих привілеїв, шкода від нього, як і у разі вразливостей та експлоїтів, може коливатися від незначної до катастрофічної для системи. Воно може потрапити на комп'ютер через експлуатацію вразливостей, легітимні інсталятори, недоліки ланцюжка постачання або соціальну інженерію тощо. Але метою завжди є отримання несанкціонованого коду, що працює на скомпрометованій системі.

Залежно від мети, воно може виконувати функції реєстрації натискань клавіш, крадіжки паролів та іншої інформації для подальших атак з підвищенням привілеїв або розгортання додаткового шкідливого коду. Отже, шкідливе ПЗ є транспортним засобом для забезпечення постійного доступу зловмисників із метою крадіжки даних, вимагання або інших злочинів.

Соціальна інженерія. Соціальна інженерія залишається серйозною проблемою в кібербезпеці, оскільки жодна технологія не може повністю захистити від атак, які використовують людський фактор. Навіть якщо спам-фільтри блокують шкідливі електронні листи, а рішення для захисту кінцевих точок виявляють відоме або підозріле шкідливе програмне забезпечення, вони не можуть повністю зупинити соціальну інженерію та інсайдерські загрози.

Найкращим захистом від таких атак є освіта та глибоке розуміння того, як зловмисники використовують притаманні людям риси для досягнення своїх злочинних цілей. Тільки при умові усвідомлення власних вразливостей та реагування на них належним чином, можна мінімізувати можливості зловмисників компрометувати системи та отримувати привілейований доступ.

У соціальній інженерії зловмисники намагаються експлуатувати кілька

ключових людських якостей для успіху атак:

Довірливість - сприйняття змісту повідомлення, навіть якщо він виглядає абсурдним чи нелогічним. Зловмисники часто використовують неправдоподібні історії чи обіцянки, розраховуючи на схильність жертви довіряти. Вони покладаються на те, що жертва сприйматиме все на віру замість критичного аналізу ситуації;

Цікавість - незнайомість із технікою атаки чи нездатність її впізнати та відреагувати відповідно. Люди часто потрапляють в пастку через природну цікавість до нового чи незвичного. Зловмисники використовують це, щоб заохотити відкрити шкідливі вкладення чи перейти на зловмисні сайти. Нездатність розпізнати загрозу також грає на руку атакуючим;

Лінь - небажання витрачати зусилля на перевірку URL, вмісту тощо на наявність зловмисної активності. Люди часто йдуть шляхом найменшого опору, уникаючи додаткових кроків безпеки. Зловмисники розраховують на це, створюючи ситуації, коли перевірка вимагає більших зусиль, ніж здається виправданим;

Довіра - віра в те, що комунікація надходить з надійного джерела. Атаки соціальної інженерії часто імітують легітимність, щоб користуватися схильністю довіряти авторитетам. Зловмисники використовують фірмові логотипи, стилі листування тощо для видавання себе за дійсних користувачів. Сліпа довіра до начебто надійних джерел підриває пильність.

1.3. Підхід щодо захисту привілейованих облікових записів

Сьогодні в індустрії кібербезпеки не існує єдиного продукту, який забезпечить необхідний захист від усіх етапів атак, що було розглянуто у попередньому підрозділі. І хоча деякі нові та інноваційні рішення допоможуть захиститися від початкового зараження або виявити його, вони не гарантують, що зупинять 100% зловмисної активності. Насправді, питання не в тому, чи буде, а в тому, коли здійсниться успішний злам інформаційної системи організації.

Привілейовані акаунти та пов'язані з ними вектори атак завжди будуть лежати в основі будь-якого успішного злому, незалежно від комбінації вразливостей та експлойтів, чи інших інструментів, що є у досяжності зловмисників.

Таким чином, про виконання таких базових дій як от управління вразливостями, встановлення виправлень, захист кінцевих точок, виявлення загроз тощо – не може бути й мови. Це є базовою вимогою. Однак, також потрібно захищати, контролювати і перевіряти привілеї в середовищі. Правильне управління привілеями може допомогти на всіх етапах атаки. Від зменшення поверхні атаки до захисту від бічного руху, виявлення порушення в процесі, активного реагування та пом'якшення наслідків цього порушення.

Очевидно, що вже існують добре відомі рішення для цього завдання, найчастіше воно реалізується за допомогою служби каталогів, де в ієрархічному вигляді зберігаються записи про ресурси, користувачів і привілеї користувачів на дії щодо ресурсів.

Як правило, управління привілеями реалізується на основі ролей користувача, де кожній ролі дозволяється певний набір дій з певним ресурсом. Цей підхід називається RBAC (Role-Based Access Control). Ролі формуються відповідно до обов'язків і повноважень співробітників в організації, що спрощує адміністрування привілеїв. Замість призначення прав кожному користувачеві індивідуально, достатньо пов'язати користувача з відповідною роллю.

Доступ до служб каталогів, що зберігають інформацію про користувачів, ролі та привілеї, реалізується за допомогою протоколу LDAP (Lightweight Directory Access Protocol). LDAP забезпечує ефективний механізм для читання і запису атрибутів, пов'язаних із записами каталогу. Багато додатків та операційних систем інтегруються зі службами каталогів на основі LDAP для автентифікації користувачів і управління доступом до ресурсів.

На практиці використовують такі реалізації LDAP:

1. OpenLDAP;
2. MSAD;
3. SAMBA;

4. IBMDomino.

Для автоматизації управління службами каталогів є класи рішень IDM (Identity Management) - системи управління ідентифікаційними даними, які відповідають за управління обліковими записами або електронними уявленнями користувачів.

Однак останнім часом, говорячи про IDM, зазвичай мають на увазі IAM (Identity and Access Management) - комплексні системи управління ідентифікаційними даними та доступом. IAM розв'язують не тільки завдання управління обліковими записами, а й завдання управління привілеями і доступом користувачів до різних ресурсів і додатків відповідно до заданих політик безпеки. Таким чином, терміни IDM і IAM по суті стали синонімами, що відображають розширення функціональності таких систем.

Системи IAM можуть охоплювати такі компоненти, як центральний каталог ідентифікаційних даних, модулі автентифікації та авторизації, засоби управління доступом на основі ролей (RBAC), інструменти звітності та аудиту, інтерфейси для самообслуговування користувачів тощо. Вони покликані забезпечити централізоване управління всім життєвим циклом ідентифікаційних даних і привілеїв у масштабах організації, підвищити безпеку і скоротити операційні витрати.

У зв'язку з відомими подіями співробітники розподілені в просторі, все частіше працюють віддалено і часто використовують свої власні пристрої як робочі станції. Для здешевлення експлуатації дедалі частіше залучаються приватні підрядники, тож кількість віддалених співробітників зростає, і вони потребують підвищеної уваги. На адміністраторів безпеки лягає підвищене навантаження з контролю віддалених користувачів усіх типів, як бізнес-користувачів з рутинними правами, так і користувачів, що мають права на дії, які становлять серйозну загрозу компанії.

На додачу самі інформаційні системи підприємств все більше переїжджають у хмару, що ставить нові питання до контролю доступу. Це може бути ефемерність ресурсів, коли сервери живуть у хмарі короткий і невизначений час, потрібне

прискорення впровадження нових технологій, потрібно передбачити швидке масштабування систем. На випадок поглинань і злиттів організацій потрібно володіти інструментарієм для швидкого вбудовування систем контролю доступу на інформаційні системи поглинених компаній.

Географічна розподіленість користувачів і використання особистих пристроїв створюють додаткові ризики для безпеки даних і дотримання нормативних вимог. Необхідно забезпечити суворий контроль над тим, хто має доступ до конфіденційної інформації, а також можливість відстежувати на легітимність всі дії користувачів.

Слід зазначити, що хоча служби каталогів ефективно розмежовують права доступу, вони не надто добре реалізують часове управління доступом. Це означає, що привілейовані облікові записи активні цілодобово (168 годин на тиждень), але на практиці вони використовуються лише протягом декількох хвилин для виконання робочих завдань.

Для скорочення поверхні атаки було б доцільно обмежити дію привілейованих облікових записів тільки тими періодами часу, коли вони справді потрібні, тобто цими кількома хвилинами.

Таким чином, необхідність відокремити управління привілейованими обліковими записами від управління іншими обліковими записами, а також потреба в часовому управлінні доступом привілейованих облікових записів – призвели до появи рішень класу PAM (Privileged access management)

IDM/IAM - це загальні системи управління цифровими ідентифікаційними даними та доступом користувачів. Вони відповідають за управління робочими обліковими записами, забезпечуючи надійну ідентифікацію кожного користувача.

PAM (Privileged Access Management) є підмножиною IDM/IAM, яка спеціалізується на контролі над привілейованими обліковими записами, що мають розширені права для внесення змін до мереж, систем або додатків.

Основна мета PAM - реалізувати принцип найменших привілеїв (Least Privilege), надаючи підвищені права доступу тільки для виконання конкретних завдань і на обмежений час.

До складу комплексних PAM рішень зазвичай входять такі компоненти:

- PIM (Privileged Identity Management) - управління паролями і життєвим циклом привілейованих облікових записів.
- PUM (Privileged User Management) - управління привілейованими користувачами.
- PSM (Privileged Session Management) - управління привілейованими сесіями, брокер сесій.
- AAPM (Application-to-Application Privileged Management) - управління привілеями для взаємодії між додатками.
- ShAPM (Shared Account Password Management) - управління спільними привілейованими обліковими записами.
- SUPM (SuperUser Privilege Management) - управління суперкористувацькими привілеями.

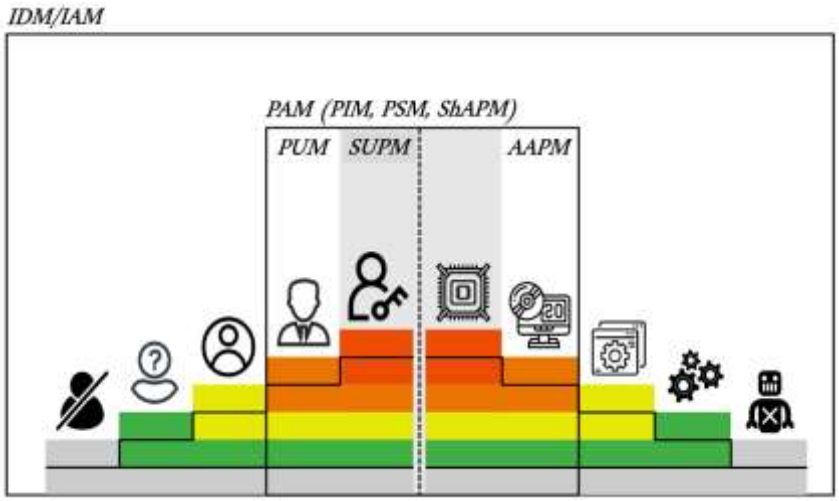

Рис. 1.8. Ієрархія компонентів рішень управління привілейованими обліковими записами

1.4. Аналіз існуючих рішень PAM

У своєму останньому звіті «Magic Quadrant for Privileged Access Management», провідна дослідницька та консалтингова компанія Gartner – проаналізувала основні тенденції сучаного ринку рішень класу PAM (рис. 1.9) [8].

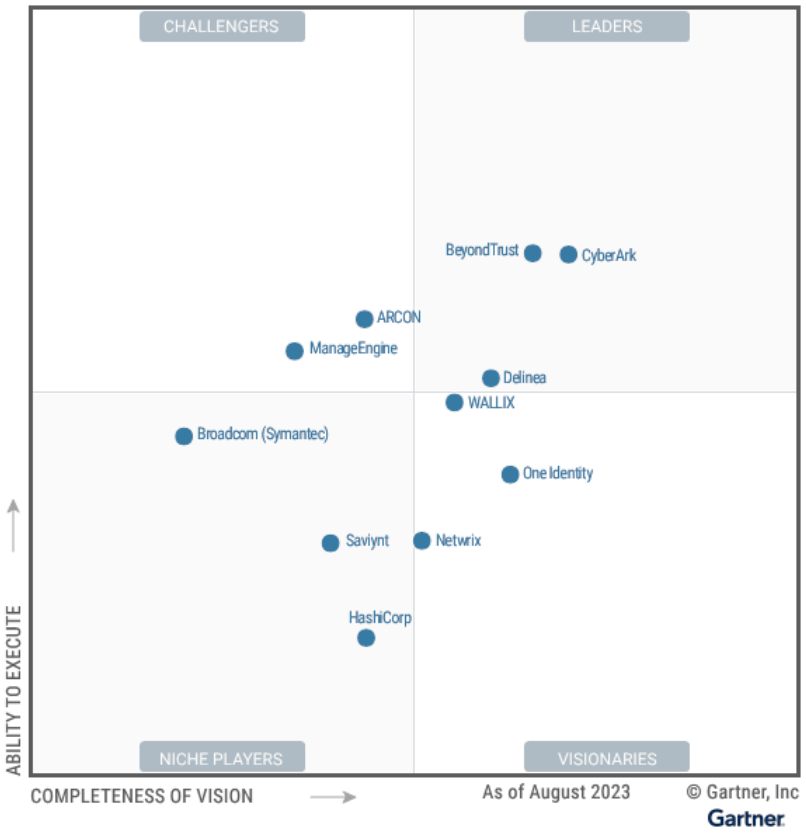

Рис. 1.9. Магічний квадрант для PAM [8]

Gartner визначає управління привілейованим доступом (PAM) як інструменти, що керують і захищають облікові записи, облікові дані і команди, які пропонують підвищений рівень технічного доступу, тобто адміністрування або конфігурування систем і додатків. Доступні у вигляді програмного забезпечення, SaaS або апаратних пристроїв, інструменти PAM керують привілейованим доступом для людей (системних адміністраторів та інших) і машин (систем або додатків).

Gartner виділяє чотири окремі категорії інструментів PAM:

- Управління привілейованими обліковими записами і сеансами (PASM) - зберігання облікових даних привілейованих облікових записів і управління сеансами для привілейованих користувачів;
- Управління підвищенням привілеїв і делегуванням (PEDM) - хост-агенти, які забезпечують фільтрацію команд і підвищення привілеїв для користувачів macOS, UNIX/Linux і Windows;

- Управління секретами - спеціалізоване сховище, орієнтоване на управління обліковими даними для програмного забезпечення і робочих навантажень;
- Управління правами доступу до хмарної інфраструктури (CIEM) - управління правами доступу до інфраструктури хмарних провайдерів послуг.

Друга категорія інструментів PAM забезпечує контроль над командами, дозволяючи виконувати лише певні дії, а також може тимчасово підвищувати привілеї користувача, щоб дозволити виконання команд у привілейованому контексті.

Всі інструменти PAM забезпечують видимість і спостережливість використання привілейованих облікових записів і команд, відстежуючи і записуючи привілейований доступ для аудиту. Це може включати детальний запис сеансів, щоб допомогти зрозуміти не тільки те, хто і коли використовував привілейований обліковий запис, але й те, що він робив.

Комбінація технічних засобів контролю, що надаються інструментами PAM, може реалізувати управління привілеями "точно вчасно", щоб забезпечити дотримання принципу найменших привілеїв: Користувачі повинні мати лише мінімальний рівень привілеїв на час, необхідний для досягнення конкретної мети.

Обов'язковими можливостями для PAM є

- Централізоване управління та забезпечення привілейованого доступу шляхом контролю доступу до привілейованих облікових записів та облікових даних або виконання привілейованих команд (або і того, і іншого);
- Керування та надання привілейованого доступу авторизованим користувачам (тобто системним адміністраторам, операторам, співробітникам служби підтримки тощо) на тимчасовій основі.

Стандартні можливості включають

- Сховище облікових даних і управління привілейованими обліковими записами;
- Контрольоване підвищення привілеїв на основі агентів для команд, що виконуються в операційних системах Windows, UNIX/Linux або macOS;

- Виявлення привілейованих облікових записів у різних системах, додатках і продуктах хмарної інфраструктури;
- Управління, моніторинг, запис і віддалений доступ до привілейованих сеансів;
- Можливості аудиту, щоб встановити, хто, коли і де використовував привілейований доступ.

Додаткові можливості включають

- Керування секретами для додатків і служб;
- Управління життєвим циклом привілейованих облікових записів і віддалений привілейований доступ для постачальників послуг та інших зовнішніх користувачів, яким потрібен технічний доступ;
- Управління привілеями "точно вчасно" (Just-in-Time), щоб скоротити час і обсяг, на який користувачеві надаються привілеї, до мінімально можливого;
- Управління правами доступу до хмарної інфраструктури (CIEM) та виявлення загроз.

CyberArk

CyberArk є лідером у цьому магічному квадранті. CyberArk запатентувала технологію сховищ більше двох десятиліть тому і була першим постачальником PAM, який представив у своєму портфоліо функції управління секретами та CIEM. CyberArk пропонує функціональність PASM за допомогою Privileged Access Manager (SaaS або програмне забезпечення), функціональність PEDM за допомогою Endpoint Privilege Manager для Windows, UNIX/Linux і macOS (SaaS або програмне забезпечення), управління секретами і AAPM за допомогою Conjur і функціональність CIEM за допомогою Cloud Entitlements Manager. Компанія також пропонує віддалений інструмент PAM під назвою Vendor Privileged Access Manager.

Сильні сторони

- Продукт: CyberArk має велику партнерську екосистему і забезпечила багато з'єднувачів та інтеграцій з суміжними технологіями, такими як управління IT-послугами (ITSM) та інструменти управління ідентифікацією та

адміністрування (IGA). Продукти PAM від CyberArk є одними з найдосконаліших на ринку. Вони мають високі оцінки за ідентифікацію робочих навантажень і управління секретами, управління обліковими даними, ведення журналів і звітності, інтеграцію та автоматизацію суміжних технологій, а також CIEM.

- Загальна життєздатність: CyberArk продовжує займати найбільшу частку ринку PAM. З моменту публікації останнього "Магічного квадранту" зростання кількості клієнтів і доходів продовжувало залишатися високим.
- Інновації: CyberArk впровадив низку значних оновлень з часу публікації минулорічного "Магічного квадранту", зокрема, інтегрував свій менеджер секретів з Amazon Web Services (AWS) та розширив функціональність JIT для охоплення більшої кількості сценаріїв використання.
- Реагування на потреби ринку: CyberArk додав функцію прозорого управління секретами, яка дозволяє керувати секретами як у сховищах CyberArk, так і в сховищах секретів AWS.

BeyondTrust

BeyondTrust є лідером у цьому магічному квадранті. Послуги PASM надаються двома продуктами, Password Safe (PS) та Privileged Remote Access (PRA), обидва доступні як SaaS, або програмне забезпечення у вигляді апаратного чи віртуального пристрою. Ці два продукти продаються окремо, але BeyondTrust тепер пропонує їх у пакеті під назвою Total PASM, і Gartner оцінив його саме так. Функціональність PEDM забезпечується продуктами управління привілеями, які доступні у вигляді програмного забезпечення (UNIX/Linux, macOS і Windows) і SaaS (для macOS і Windows). BeyondTrust також надає програмне забезпечення для з'єднання з Active Directory (AD). Управління секретами раніше було окремим продуктом, але тепер входить до складу Total PASM. BeyondTrust також пропонує функціональність CIEM за допомогою інструменту Cloud Privilege Broker. Клієнти BeyondTrust географічно диверсифіковані, з великою концентрацією в Північній Америці та Європі.

Сильні сторони

- Стратегія продукту: Пакет PS і PRA надає потужні можливості,

особливо у сферах відкриття облікових записів і реєстрації, управління привілейованими сесіями та віддаленого доступу. Однак, це не так, якщо розгорнути лише один з цих продуктів: PRA зосереджений на управлінні привілейованими сеансами, в чому автономна версія PS не сильна;

- Продукт: BeyondTrust є найкращим у своєму класі для UNIX/Linux та macOS PEDM, а також найкращим для Windows PEDM. Щодо пакета Total PASM, клієнти позитивно відгукуються про можливості виявлення, розумні правила та простоту використання;
- Клієнтський досвід: BeyondTrust дуже тісно співпрацює зі своїми клієнтами, маючи кілька команд, від успішних клієнтів до технічної підтримки;
- Оперативність реагування на ринок: BeyondTrust додав до свого продукту PRA можливості доступу до мережі з нульовою довірою (ZTNA) і тепер пропонує ефективний інструмент доступу до IT-інфраструктури для розробників та інженерів. Компанія також додала більше інструментів, які допоможуть клієнтам оцінити рівень зрілості PAM.

WALLIX

Компанія WALLIX є «провидцем» у цьому магічному квадранті. Заснована у Франції в 2003 році, компанія WALLIX представила свій продукт PAM у 2007 році. WALLIX Bastion забезпечує функціональність PASM і доступний як програмне забезпечення, віртуальний чи фізичний пристрій або як керована послуга. WALLIX BestSafe забезпечує функціональність PEDM і доступний лише у вигляді програмного забезпечення. WALLIX також пропонує SaaS-сервіс для віддаленого доступу до PAM. WALLIX не надає функціонал CIEM. Клієнти в основному знаходяться в регіоні EMEA, деякі з них розташовані в Північній Америці. Компанія інвестувала значні кошти в залучення та підтримку клієнтів, які використовують промислові системи управління та операційні технології (OT).

Сильні сторони

- Продукт: WALLIX пропонує зрілий і багатофункціональний продукт для управління сеансами і має широкі можливості для фільтрації елементів керування сеансами, запису та аудиту сеансів у реальному часі. Він також добре

підходить для інтеграції з суміжними системами і має розширені можливості для управління передачею файлів, включаючи можливість авторизації вхідних і вихідних передач через робочі процеси та автоматичне сканування файлів.

- Продукт: WALLIX - найкращий у своєму класі інструмент для мереж ОТ/мереж управління процесами з можливістю тунелювання через власні протоколи ОТ. Оскільки дані від компанії Flashpoint показують, що промисловість є найбільш вразливою до загроз витоку інформації та несанкціонованого доступу, а вся її інфраструктура базується на ОТ-технологіях, то саме здатність WALLIX забезпечувати належний захист ОТ-систем робить це рішення найкращим вибором для боротьби з такими загрозами в промисловому секторі [1];
- Відповідність державному законодавству: Наявність висновку відповідності до вимог технічного захисту інформації від ДССЗЗІ означає, що рішення WALLIX відповідає вимогам безпеки для використання в державних установах та організаціях України [9];
- Ціноутворення: Ціни є висококонкурентними, з котируваннями нижче середнього для всіх оцінених сценаріїв;
- Клієнтський досвід: Клієнти часто відзначають ефективну та своєчасну підтримку, а також позитивно відгукуються про простоту використання рішення.

Отже, завдяки комбінації найкращої підтримки ОТ-інфраструктури, конкурентних цін, потужного функціоналу управління привілейованим доступом, позитивного клієнтського досвіду та відповідності вимогам державних органів безпеки, рішення WALLIX може бути ідеальним вибором для захисту промислових компаній та організацій від загроз витоку даних та несанкціонованого доступу.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЩОДО ВПРОВАДЖЕННЯ PAM В ІС ОРГАНІЗАЦІЇ НА ОСНОВІ WALLIX BASTION

2.1. Архітектура Wallix Bastion

Успішна архітектура системи управління привілейованим доступом (PAM) повинна захищати привілеї для кожного користувача, сеансу та ресурсу.

Традиційно, досягається це основними елементами рішення, що формують його базовий функціонал – є PIM, PUM, PSM та PPM. Саме ці модулі забезпечують безпечний контроль доступу, аудит, оповіщення та запис для будь-якого привілейованого сеансу.

Інщі компоненти PAM-системи будуть виступати у якості функціонального доповнення для розширення та комплексності підходу.

Однак перш ніж заглибитися у внутрішню архітектуру та компоненти рішення Wallix Bastion, варто розглянути загальний контекст - типову IT-інфраструктуру сучасної організації. Це допоможе краще зрозуміти, як Bastion інтегрується та взаємодіє з різними елементами розподіленого середовища для забезпечення комплексного управління привілейованим доступом. Приклад такої корпоративної архітектури зображено на рисунку 2.1.

Так, можна виділити кілька ключових складових, характерних для сучасного корпоративного IT-середовища:

1. Зовнішні з'єднання, що забезпечують доступ до глобальних мереж та хмарних сервісів, а також під'єднання віддалених користувачів через периметр безпеки організації;
2. Безпосередньо периметри безпеки, реалізований комплексом захисних пристроїв, таких як брандмауери тощо, що відокремлюють внутрішні ресурси від загроз.
3. Мережеве обладнання для підключення всіх пристроїв до єдиної

мережі;

4. Численні серверні системи, призначені для різних служб та додатків, таких як веб-сервери, бази даних, поштові та файлові сховища;

5. Кінцеві точки користувачів: робочі станції та інші клієнтські пристрої, що підключаються до внутрішньої мережі.

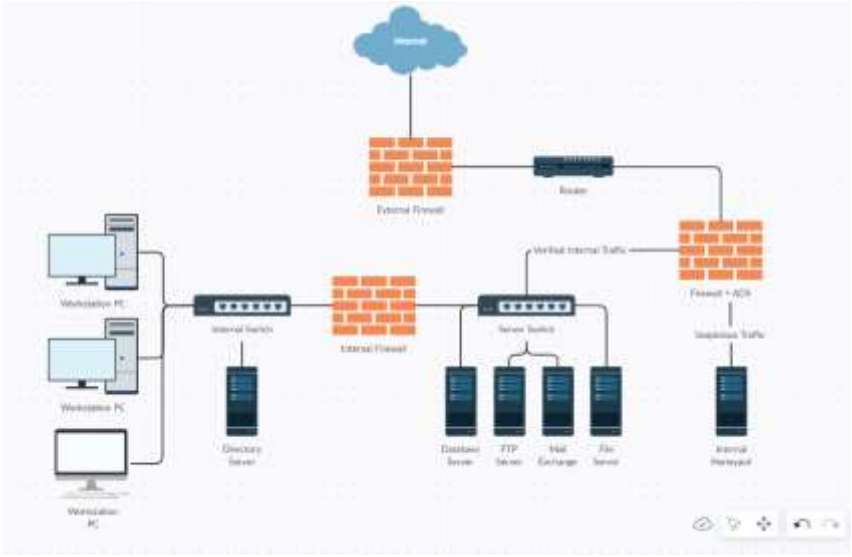

Рис. 2.1. Загальний вигляд архітектура IT-інфраструктури організації

Спроба реалізувати управління привілейованим доступом безпосередньо в існуючій багаторівневій та розгалуженій IT-інфраструктурі, як ця, з використанням тільки тих штатних засобів, що реалізують наявні засоби захисту, мережеве обладнання та кінцеві пристрої – є складним і недоцільним завданням. Такий підхід буде дорогим, неефективним для основних бізнес-процесів та складним в обслуговуванні.

Таким чином, для впровадження процесу управління привілейованим доступом організація має модифікувати існуючу мережеву архітектуру. Ключовою зміною є підключення брокера сесій Wallix Bastion в ролі проксі-сервера між користувачами та цільовими системами (рис. 2.2). Це унеможливлює прямий доступ до критичних ресурсів.

Розглянувши загальний контекст впровадження системи в корпоративну IT-інфраструктури, тепер можна заглибитися у внутрішню будову самого рішення

Wallix Bastion. Його модульна архітектура охоплює всі ключові аспекти комплексного управління привілейованим доступом, про які було зазначено вище.

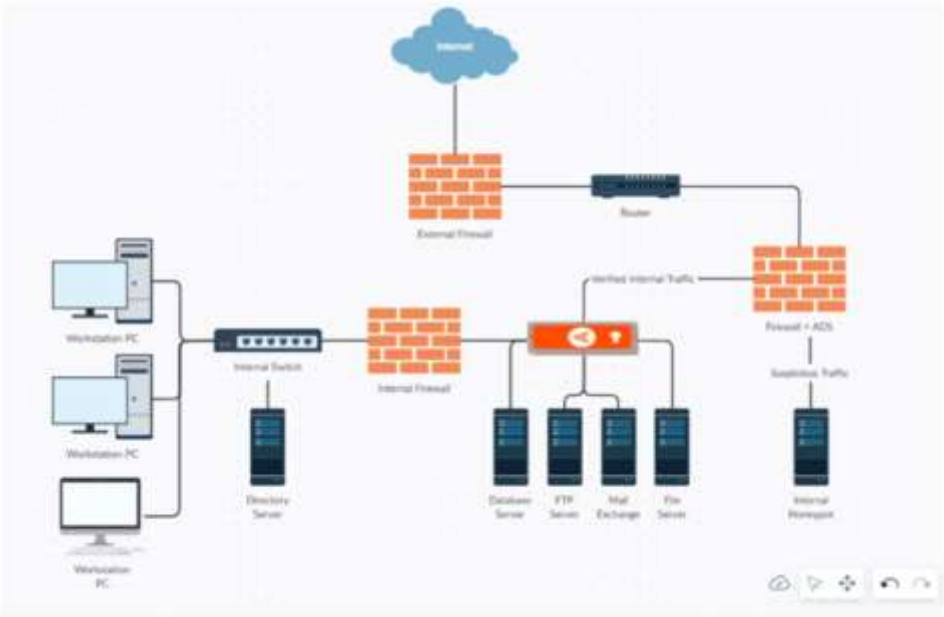

Рис. 2.2. Загальний вигляд архітектура IT-інфраструктури організації з реалізацією системи управління привілейованим доступом.

Одним з центральних компонентів виступає менеджер сесій (Session Manager), який забезпечує безпечне встановлення, контроль та аудит привілейованих з'єднань користувачів із цільовими системами (рис. 2.3).

Другим - є парольний менеджер (Password Manager) - репозиторій для зберігання та керування обліковими даними цільових систем. Він дозволяє ізолювати привілейовані облікові дані від кінцевих користувачів, посилюючи безпеку.

До нього також належать такі напівмодулі, як менеджер привілеїв від застосунку до застосунку (AAPM), а також сховище облікових даних (Vault).

Модулі тісно інтегровані між собою, утворюючи цілісну платформу з широким функціоналом для забезпечення прозорості, підзвітності та безпеки усіх привілейованих операцій в розподіленому середовищі організації.

Рис. 2.3. Внутрішня архітектура рішення [10]

Усі вхідні підключення привілейованих користувачів, спрямовані на Wallix Bastion, або через веб-інтерфейс за протоколом HTTPS (реалізоване через допоміжний продукт Access Manager), або напряму з використанням протоколів RDP чи SSH – оброблюються менеджером сесій.

Відповідно, на підставі дозволів розмежування доступу – користувач має можливість підключатися до цільових систем, використовуючи такі протоколи як RDP, SSH, неспецифікована реалізація трафіку TCP/IP, RLOGIN, VNC та TELNET.

Відповідно для розширення цього списку підтриманих протоколів для будь-яких інших специфічних застосунків та сервісів – існує можливість впровадження Jump-сервера на базі Windows Server, на якому буде розгорнутий допоміжний клієнт-застосунок такий як веб-браузер, командний рядок тощо, що утилізує відповідний необхідний протокол (рис. 2.4).

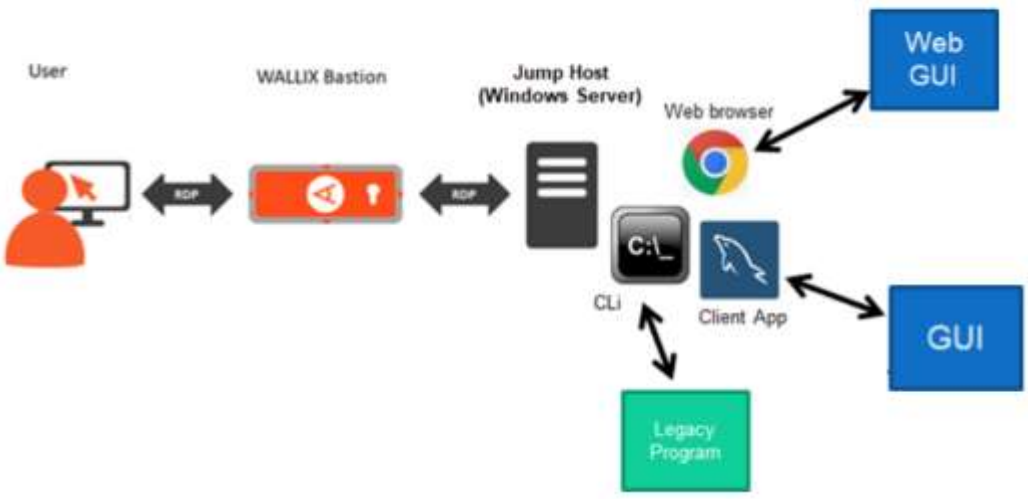

Рис. 2.4. Принцип дії Jump-сервера з рішенням [11]

Менеджер паролів забезпечує повний життєвий цикл управління паролями. Він ін'єктує паролі безпосередньо в сесії доступу, періодично змінює їх за потребою, не розкриваючи привілейованим користувачам.

Так наприклад, щоб унеможливити обхід брокера сесій, в найпростішому випадку реалізації архітектури, організація може позбавити привілейованих користувачів знання паролів до цільових систем. Для цього до архітектури самого рішення Wallix Bastion додане сховище паролів Vault.

Виключення людського фактору з парольної політики дозволяє суттєво підвищити складність паролів до рівня криптографічних ключів (128+ символів). Це додатково посилює безпеку системи.

Менеджер сесій також добре інтегрується з системою управління IT-сервісами (ITSM), для того щоб підтверджувати заявки на підключення відповідним квитком на роботи.

Крім цього, менеджер сесій має можливість підключати адміністраторів безпеки, по-перше, для того, щоб схвалювати заявки на доступ привілейованих користувачів, і, по-друге, щоб отримати можливість контролювати всередині сесій їх дії, так званий режим роботи "чотири ока".

Водночас для перевірки автентичності та підтримки життєвого циклу робочих облікових записів є можливість інтеграції IDM/IAM, а для реалізації поведінкового аналізу – інтеграція з системами SIEM.

2.2. Призначення та функція менеджера сесій

Як було зазначено раніше, менеджер сесій (Session Manager) є одним з ключових компонентів рішення Wallix Bastion для управління привілейованим доступом. Його основне призначення - забезпечувати безпечний контроль та моніторинг з'єднань привілейованих користувачів до критичних систем та ресурсів організації.

Відповідно, для виконання всіх покладених на нього задач, менеджер сесій

Wallix Bastion має відповідні функції, кожну з яких можна віднести до того чи іншого аспекту контролю, делегування та аудиту доступу (Рис. 2.5):

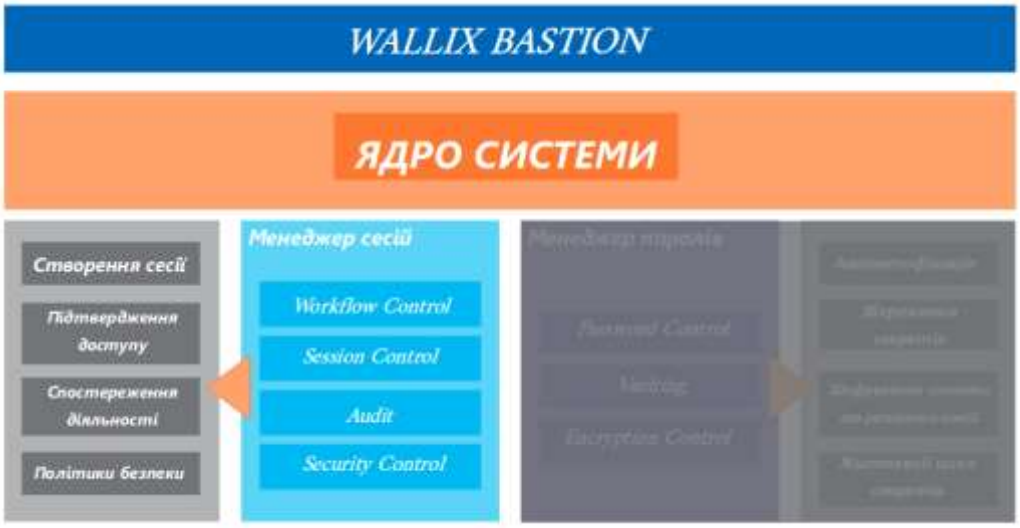

Рис. 2.5. Основні компоненти менеджер сесій

1. Функція контролю робочого процесу (Workflow Control);
2. Функція контролю сесій (Session Control);
3. Функція аудиту (Audit);
4. Функція контролю безпеки (Security Control).

Взаємодія згаданих функцій менеджера сесій Wallix Bastion реалізує комплексний алгоритм управління та контролю привілейованого доступу до інформаційних систем організації. При детальнішому розгляді, можна виділити основний алгоритм дій, за яким відбувається оброблення запитів привілейованих користувачів (рис. 2.6):

1. Першочергово, ініціатор сесії повинен пройти перевірку автентичності та підтвердження доцільності підстави на отримання привілейованого доступу:

a. Сукупність функцій, що виконують контроль робочого процесу, із взаємодією з модулем парольного менеджера (Password Manager) – здійснюють перевірку автентичності користувача, або на підставі облікової інформації, що було надано як локально (Wallix Bastion), так і системами IDM/IAM, або з задіянням додаткових факторів перевірки автентичності (MFA);

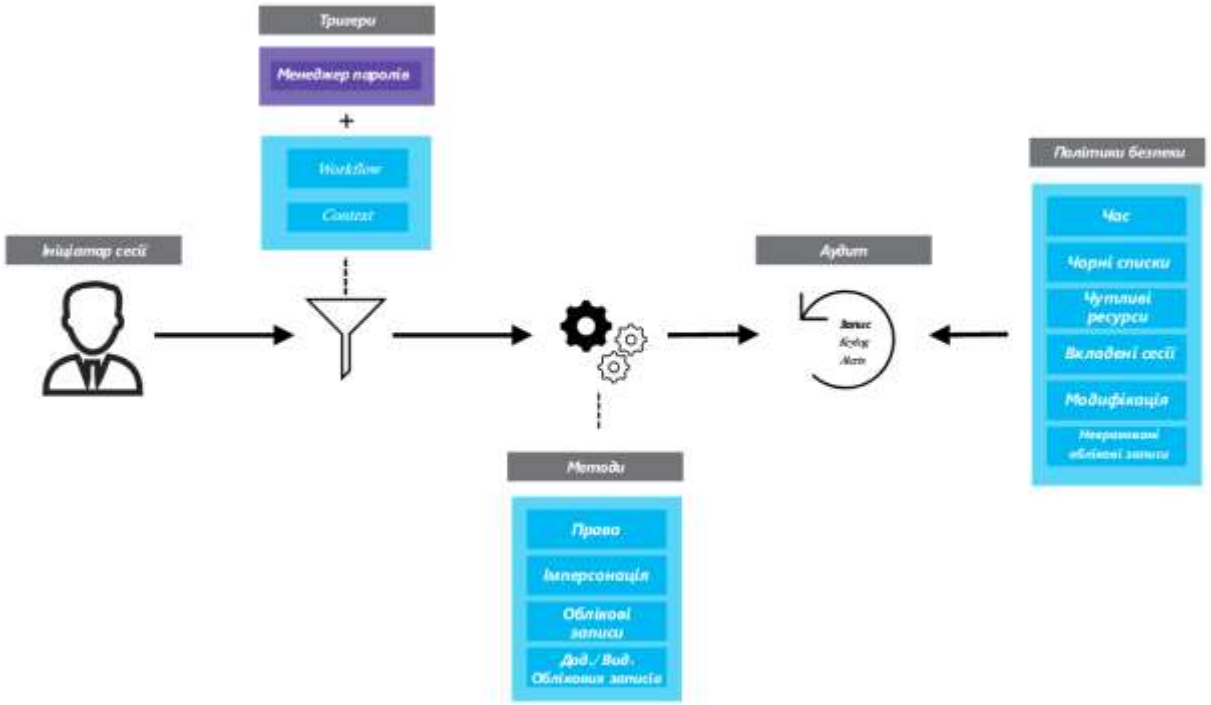

Рис. 2.6. Процес обробки запиту та встановлення сесії

b. Друга частина перевірки – перевірка доцільності підстави на отримання привілейованого доступу. У цьому разі підтвердження необхідності доступу можна отримати, або шляхом обробки заявки через наявну в організації системи менеджменту сервісів IT (ITSM), або реалізованою за допомогою самого Wallix Bastion процесу підтвердження заявок на отримання доступу системними адміністраторами та/або персоналом з підтвердження доступу (Approver).

c. При цьому, під час цього етапу процесу створення сесії – обов’язково перевіряється контекст доступу, по типу: чи запит прийшов з дозволеної IP-адреси, чи в дозволений робочий час тощо.

2. Надалі обробка запиту на сесію передається множині функцій контролю сесій, які виконують безпосередньо встановлення сесії у такий спосіб:

a. Шляхом маніпуляції обліковими записами, наприклад спочатку створити (чи увімкнути), а потім, після закінчення відведеного строку на виконання необхідних робіт – видалити його (чи вимкнути);

b. Шляхом маніпуляції правами, наприклад спочатку дати відповідний

рівень прав доступу до інформаційної системи чи застосунку, а по зникненню необхідності – забрати;

c. Шляхом імперсонації – можливості працювати під іменем привілейованого користувача, без знання пароля від неї, як наприклад, вбудовані механізми операційної системи – SUDO (Unix) чи RUN AS (Win);

d. Шляхом додавання і видалення облікових записів з привілейованих груп користувачів.

3. Після створення привілейованої сесії одним з перерахованих вище методів – наступає фаза аудиту, під час якої здійснюється:

a. Відеоспостереження та запис з фіксацією всіх дій користувачів для спостереження у реальному часі, чи подальшого зберігання та аналізу поведінки;

b. Журналювання натискань клавіш – спостереження у реальному часі та зберігання, з подальшим аналізом детального звіту команд, які були застосовані ініціатором сесії.

4. Відповідно в одночас із початком фази аудиту – набирають сили і функції контролю безпеки, які на основі регулярних виразів та журналювання натискань клавіш автоматизують системи реалізації політик безпеки, зокрема інформування чи відкликання доступу тощо, на будь-яку неправомірну діяльність:

a. У разі виконання в невизначений час;

b. Застосовуються команди, які були визначені небезпечними та внесені до чорного списку;

c. Була спроба отримання доступу до чутливих ресурсів – не типових для виконувальної роботи користувача;

d. Була спроба зробити вкладену віддалену сесію до іншої віддаленої інформаційної системи;

e. Була спроба несанкціонованої модифікації системи;

f. Була спроба створити неврахований обліковий запис.

На рівні операційної архітектури модуля менеджера сесій – якщо говорити спрощено, взаємодія основних компонентів здійснюється наступним чином (рис. 2.7):

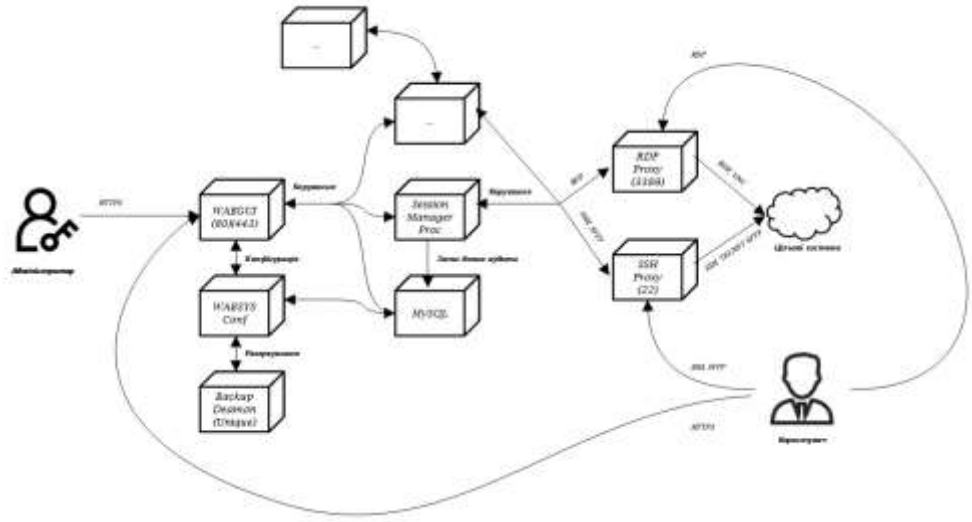

Рис. 2.7. Операційна архітектура модуля менеджера сесій

Адміністратори самої системи Wallix Bastion та інші користувачі IT-інфраструктури організації отримують доступ до Web-сервера Apache, який розгортається для можливості входу до Web-консолі керування за портами 80 і 443, за протоколом HTTP та HTTPS відповідно.

Сама консоль керування “WABGUI” – дає змогу виконувати управління модулями-процесами:

- Session Manager Proc – представляє функціонал менеджера сесій;
- Password Manager Proc – представляє функціонал менеджера паролів;
- WAB System Configuration – представляє функціонал конфігурації самої системи Wallix Bastion;
- Backup Deamon – процес, що ініціює за потреби створення резервних копій важливих даних системи.

Відповідно, Session Manager Proc має зв’язок із основними проксі-серверами, розгорнутими в системі для виконання процесів ініціації, обліку та закриття сесій:

- SSH-proxy – для доступу за протоколами SSH, SFTP, Telnet до цільових систем;
- RDP-proxy – для доступу за протоколами RDP, VNC до цільових систем.

Відповідно облік інформації, необхідної для створення, підтримання та

аудиту сесії зберігається у MySQL базі даних.

2.3. Призначення та функція парольного менеджера

Відповідно, як це також було зазначено раніше, менеджер паролів (Session Manager) є ще одним з ключових компонентів рішення Wallix Bastion для управління привілейованим доступом. Його основне призначення - забезпечувати автентифікацію привілейованих користувачів та захист і керування їх обліковими даними.

Так само, для виконання всіх покладених на нього задач, менеджер паролів Wallix Bastion має відповідні функції, кожну з яких можна віднести до того чи іншого аспекту управління процесом життєвого циклу облікових даних (Рис. 2.8):

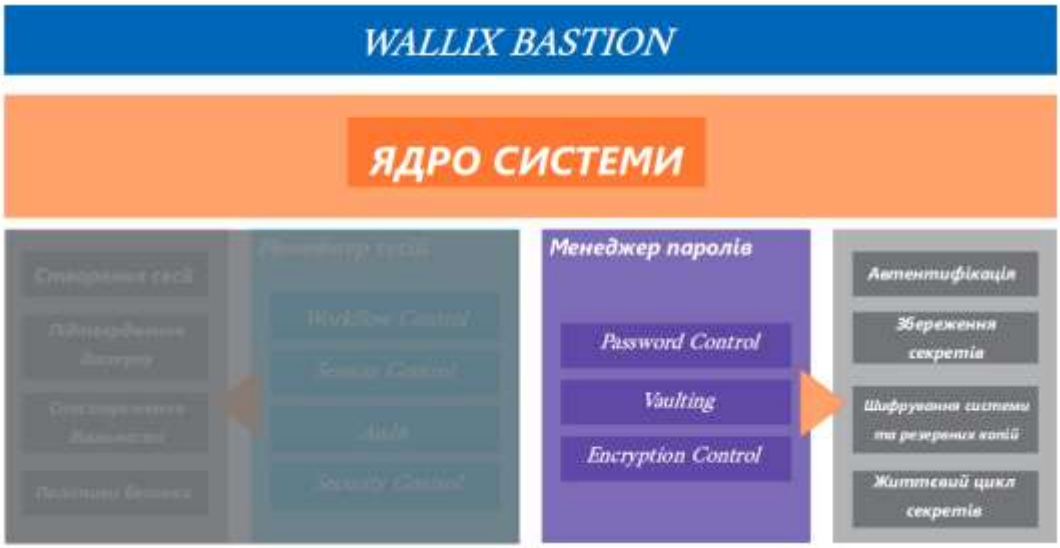

Рис. 2.8. Основні компоненти менеджер паролів

1. Функції контролю паролів (Password Control);
2. Функції сховища (Vaulting);
3. Функції контролю шифрування (Encryption Control).

Взаємодія згаданих компонентів менеджера паролів Wallix Bastion реалізує комплексний алгоритм управління та контролю життєвого циклу привілейованих облікових даних користувачів та інформаційних систем організації. При

детальнішому розгляді, можна виділити основний алгоритм дій, за яким відбувається оброблення запитів привілейованих користувачів (рис. 2.9):

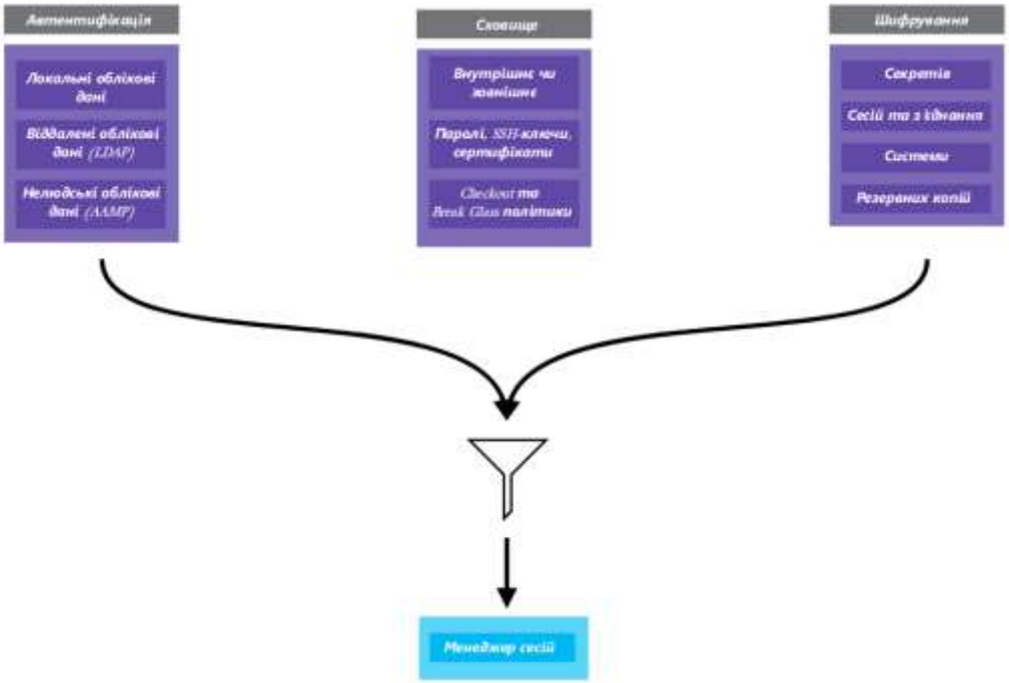

Рис. 2.9. Процес обробки запиту та встановлення сесії

1. Під час ініціації сесії користувача, вступає в силу процес перевірка його автентичності. Відповідно, порівняння облікових даних введених користувачем проводиться з тими, що:

a. Збережені у локальній базі даних самого рішення Wallix Bastion, доданих самим адміністратором системи;

b. Отримані із зовнішньої IDM/IAM системи, з використанням протоколу LDAP;

Однак, слід зазначити, що крім людських облікових записів – застосовуватися можуть і не людські, роботу з якими по автентифікації проводить відповідний підмодуль AAPM.

2. Сховище секретів Vault – виконує функції зберігання, та при необхідності відтворення паролів, забезпечуючи повний цикл керування паролями:

a. Сховище може бути як внутрішнє, так зовнішнє, надані іншими виробниками захисних рішень (CyberArk, HashiCorp, IBM);

b. Секретами можуть виступати, як логіни, паролі користувачів, так і SSH-ключи, а також сертифікати (підписані відкриті ключі SSH);

c. Існує можливість налаштування Checkout-політики для можливості короткострокового ознайомлення користувачів із обліковими даними. Також є функція випадкового змінення облікових даних після закінчення відведеного періоду;

d. Реалізується механізм "розбитого скла" (Break Glass), який дозволяє користувачеві отримати облікові дані привілейованих записів, зібраних в системі Wallix Bastion, тобто логін, загальні імена (CN), паролі та SSH-ключі. Це може стати в нагоді у випадку недоступності Wallix Bastion. Облікові дані в системі автоматично надсилаються користувачеві щоночі о 2:34 в часовому поясі, в якому знаходиться Wallix Bastion – він отримує зашифрований його GPG ключем електронний лист, що містить список всіх облікових даних для цільових груп, зібраних в системі, в залежності від обсягу обмежень, встановлених для їх профілю.

3. Функція шифрування в Bastion забезпечує захист конфіденційних даних не тільки таких як паролі привілейованих облікових записів, а й підключення через веб-інтерфейс, RDP та SSH-з'єднання тощо. Цей алгоритм застосовує унікальний конфіденційний ключ шифрування, який адміністратор безпеки рішення Wallix Bastion визначає під час первинного налаштування системи.

Крім того, після кожного перезавантаження системи з'єднання через проксі-сервери Bastion будуть недоступні до моменту, поки адміністратор не введе ключ-парольну фразу в веб-інтерфейсі адміністрування.

Слід зазначити, що після завершення фази ініціалізації шифрування, рекомендується створити резервну копію Bastion принаймні один раз. Це дозволить зберегти копію ключа шифрування в безпечному місці.

На рівні операційної архітектури модуля менеджера паролів – взаємодія основних компонентів здійснюється наступним чином (рис. 2.10):

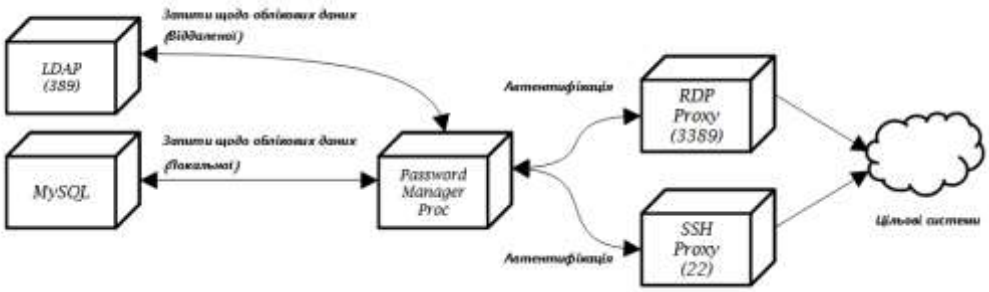

Рис. 2.10. Операційна архітектура модуля менеджера паролів

Доповнюючи функціонал, що було зазначено у попередньому розділі, Password Manager Proc також має зв’язок із основними проксі-серверами, розгорнутими в системі для виконання процесів автентифікації та обліку привілейованих користувачів. Для виконання цієї задачі, застосовується або вже зазаначена раніше локальна база даних MySQL, або відбувається підключення до зовнішньої системи за протоколом LDAP.

3 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЩОДО ВПРОВАДЖЕННЯ PAM В ІС ОРГАНІЗАЦІЇ НА ОСНОВІ WALLIX BASTION

3.1. Рекомендації щодо встановлення та налаштування Wallix Bastion

У відповідності до передових практик на ринку сучасних рішень з інформаційної безпеки, компанія Wallix пропонує три варіанти розгортання свого продукту Bastion [12]:

- On-Premise розгортання, що передбачає встановлення рішення на внутрішніх ресурсах замовника з можливістю повної конфігурації програмної та апаратної складової відповідно до індивідуальних вимог та можливостей;
- Appliance-based реалізація на спеціалізованому апаратному забезпеченні, що вироблене компанією Wallix. Цей варіант не потребує складного розгортання з боку замовника, необхідно лише інтегрувати пристрій до існуючої мережевої інфраструктури, однак все ж потребує підтримки з боку замовника;
- Cloud-based, або хмарна реалізація, за якою всі аспекти розгортання, налаштування та підтримки рішення забезпечуються безпосередньо компанією Wallix.

У разі розгортання рішення типу On-Premise, Wallix надає образ рішення розширення .iso, яке поті розгортається на фізичному серверному обладнанні, або на віртуальному. Bastion розгортається на операційній системі типу Unix – Debian.

Первинне встановлення проходить у інтерактивному режимі, покроково, за допомогою завантажувача GRUB.

Відповідно, як можна бачити з рисунку 3.1 та 3.2, первинне налаштування проходить такі етапи:

1. Вибір мови розкладки клавіатури для вводу даних;
2. Створення пароля для внутрішнього базового користувача системи Wallix Bastion – wabadmin, який наділений мінімальними привілеями;

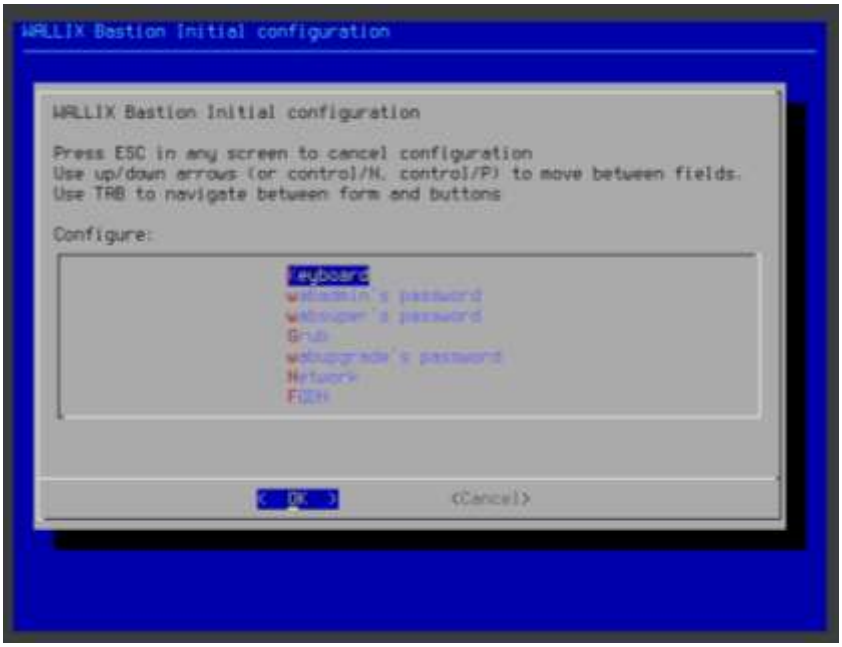

Рис. 3.1. Первинна конфігурація (кроки виконання)

3. Створення пароля для внутрішнього суперкористувача системи Wallix Bastion – wabsuperuser, який має максимальні привілеї та може виконувати будь який скрипт, а також будь які команди системи;

4. Створення пароля для користувача інтерфейсу GRUB Wallix Bastion – wabbootadmin;

5. Створення пароля для користувача функції безпечного оновлення системи Wallix Bastion – wabupgrade;

6. Комплексне налаштування мережі, куди входить:

a. Конфігурація хостового ім’я системи Wallix Bastion;

b. Конфігурація IP-адресації внутрішніх мережевих адаптерів системи (як IPv4, так і IPv6) та DNS;

c. Конфігурація шлюзу за замовчуванням;

d. Конфігурація маршрутизації та VLAN, у разі ускладненої реалізації мережевого зв’язку з цільовими інформаційними системами;

e. Конфігурація FQDN для можливості застосування доменних імен при звернені до системи.

Рис. 3.2. Первинна конфігурація (мережеві налаштування)

Слід зазначити, що паролі для вище згаданих внутрішніх користувачів системи, в цілях безпеки повинні бути унікальними, неменше чотирнадцяти символів, та налічувати в собі великі та маленькі літери алфавіту, цифри та спеціальні знаки (рис. 3.3).

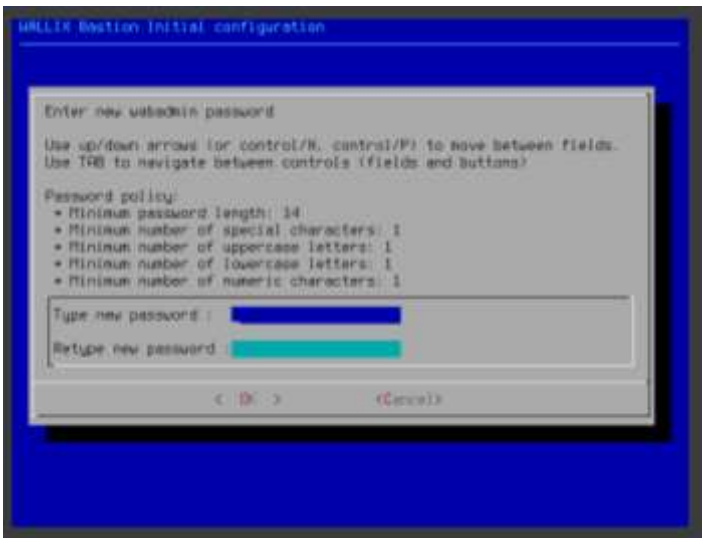

Рис. 3.3. Процес створення паролю для внутрішнього користувача

Первинне налаштування може вважатися завершеним після того, як адміністратор системи вперше ввійде до свого облікового запису у веб-інтерфейсі, та надасть парольну фразу, за допомогою якої ініціюється загальна функція шифрування системи (рис. 3.4).

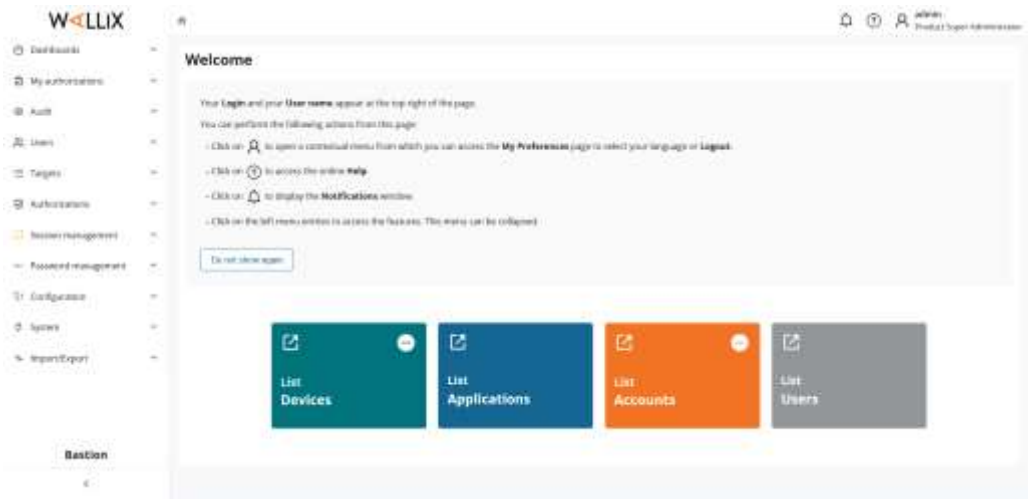

Рис. 3.4. Веб інтерфейс Wallix Bastion

Користувацький інтерфейс рішення Wallix Bastion відрізняється інтуїтивною та зрозумілою структурою, дотримуючись принципів зручності та лаконічності. Меню розділене на окремі секції, кожна з яких відповідає за специфічний аспект налаштувань та управління системою:

1. Dashboards (Інформаційні панелі) – Меню «Dashboards» надає детальний аналіз усіх з'єднань, здійснених через Wallix Bastion в контексті адміністрування або аудиту, у вигляді числових даних, табличних подань і графіків за певний період часу;

2. My authorizations (Мої повноваження) – Меню «My authorizations» надає інформацію користувачу про всі наявні сесії, де користувач був успішно автентифікований та має можливість ініціювати сеанс з відповідною кінцевою точкою;

3. Audit (Аудит) – Меню «Audit» дозволяє аудитору переглядати дані аудиту Wallix Bastion і, головним чином, історії з'єднань. В контексті користувачів та ролей Wallix Bastion, аудитор - це користувач, якому адміністратором Wallix Bastion призначив права аудиту: в його профілі встановлено право «Перегляд» для функції «Аудит сесії»;

4. Users (Користувачі) – Меню «Users» дозволяє створювати та керувати користувачами/адміністраторами Wallix Bastion, групувати їх. Крім цього, тонко налаштовувати, які пункти меню може бачити користувач у своєму кабінеті,

заборонені дії тощо;

5. Targets (Цільові системи) – Меню «Targets» надає можливість створювати та керувати пристроями, додатками, доменами, обліковими записами та групами, до яких можна отримати доступ з Wallix Bastion;

6. Authorizations (Повноваження) – Меню «Authorizations» дозволяє визначати повноваження. Ці повноваження визначають, які цільові облікові записи та протоколи користувачі можуть використовувати для доступу до пристроїв. Повноваження застосовуються до груп користувачів, пов'язаних з цільовими групами. Всі користувачі в одній групі успадковують однакові повноваження.

7. Session management (Керування сесіями) – Меню «Session management» надає можливість керування механізмами автентифікації для проксі-серверів (RDP, VNC, SSH, TELNET, RLOGIN і RAW TCP/IP), а також параметрами зберігання записів сеансів. Можна ввімкнути або вимкнути шифрування та цифровий підпис записів сеансів. Ці записи можна переглянути на сторінці «Session History» в меню «Audit». Зашифровані записи може прочитати лише той екземпляр Wallix Bastion, який їх створив. Використовуваний алгоритм шифрування - AES 256 CBC. Підпис виконується шляхом обчислення HMAC SHA 256. Підпис перевіряється при відтворенні.

8. Password management (Керування паролями) – Меню «Password management» дозволяє керувати політиками та плагінами зміни паролів. Політика зміни пароля визначає параметри зміни пароля (тобто пароля, ключа SSH).

9. Configuration (Конфігурація) – Меню «Configuration» надає широкі можливості для налаштування різних аспектів роботи Wallix Bastion: конфігурації специфічних параметрів (опцій графічного інтерфейсу, проксі-серверів RDP, SSH тощо), управління часовими проміжками доступу для користувачів та груп користувачів, налаштування зовнішніх методів автентифікації (LDAP, Active Directory, Kerberos, RADIUS), інтеграції облікових записів через імпорт з LDAP/AD, налаштування механізму сповіщень, локальної політики паролів, банера з повідомленням при вході в сесію чи веб-інтерфейс, автентифікації через X509 сертифікати, управління API-ключами тощо;

10. System (Система) – Меню «System» надає сукупність можливостей: відображати загальну інформацію про стан системи, конфігурувати мережеві налаштування, налаштовувати службу часу (NTP), управляти віддаленим сховищем для зберігання записів сесій, управляти агентом SNMP, конфігурувати поштовий сервер для відправки сповіщень, визначати відображення сервісів на мережеві інтерфейси та ввімкнення/вимкнення сервісів Wallix Bastion, переглядати вміст файлу «syslog» з журналами сесій, повідомленнями про роботу проксі та використання веб-інтерфейсу адміністратора, переглядати вміст файлу «dmesg» з логами завантаження системи, а також зберігати та відновлювати конфігурацію Wallix Bastion;

11. Import/Export (Імпорт/Експорт) – Меню «Import/Export» надає можливості імпортувати дані з файлу .csv, експортувати дані у форматі .csv, .zip чи .tar.gz архіву, а також імпортувати облікові записи користувачів з каталогів LDAP або Active Directory.

Таким чином, комплексний функціонал рішення Wallix Bastion надає адміністраторам безпеки організацій потужний інструментарій для ефективного захисту критично важливих інформаційних систем від загроз несанкціонованого доступу. Завдяки наступним рекомендаціям, адміністратори мають можливість належним чином контролювати та захищати привілейовані облікові записи користувачів, що пов'язані з цільовими системами, а також забезпечувати безпеку їхніх облікових даних:

1. Рекомендації «Оброблення сесій»

Внутрішні сесії. Адміністратори системи повинні реалізувати для внутрішніх користувачів один з наступних можливостей налаштувань створення сесій підключення до кінцевих станцій:

1. Через веб-інтерфейс самої системи Wallix Bastion, з використанням власного облікового запису до рішення, без знання паролю до кінцевої системи;

2. Застосування власних інструментів для входу, таких як Putty, або вбудованих у Windows засобів підключення по RDP, з можливістю підключення до Wallix Bastion через внутрішню IP-адресу (рис. 3.5);

3. Автентифікування до застосунку, використовуючи той чи інший набор інструментів, перелічений вище.

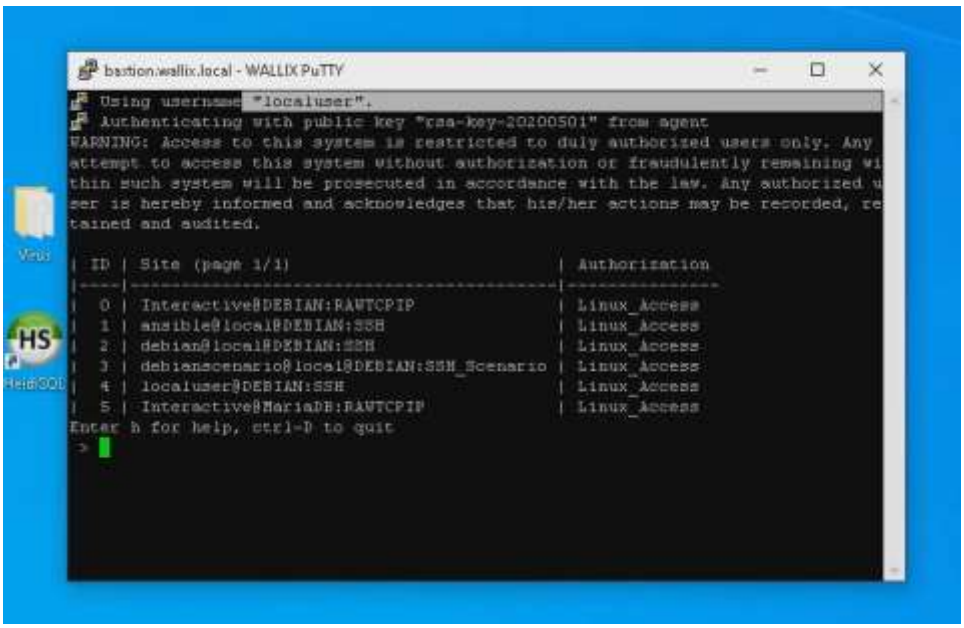

Рис. 3.5. Реалізація створення сесії через інструмент Putty

Зовнішні сесії. Відповідно для під'єднання зовнішніх користувачів, адміністратори системи повинні спочатку налаштувати захищене віддалене з'єднання (наприклад через VPN), провести їх ідентифікацію та автентифікацію до рішення Wallix Bastion, і тільки потім регулювати привілейований доступ до цільових систем. Тобто таким чином, прямого доступу до цільових систем – не має бути (рис. 3.6).

Рис. 3.6. Сторінка входу до системи користувачів

2. Рекомендації «Аудит»

Дозволи. Адміністратори системи повинні налаштувати підтримку динамічної авторизації за допомогою процедури дозволу. Коли користувач хоче ініціювати з'єднання з об'єктом або отримати доступ до облікових даних об'єкта, він спочатку надсилає запит на затвердження. Цей механізм ґрунтується на часових рамках, визначених для доступу до об'єктів або облікових даних об'єктів, а також необхідності розгляду запиту на підтвердження аудиторами (рис. 3.7).

Рис. 3.7. Процес підтвердження заявки аудитором

Обліковість. Відповідно, на додачу до процедури розгляду запитів аудиторами, адміністратори системи можуть автоматизувати цей процес системою ITSM, тим самим підвищуючи обліковість. Користувачі зможуть отримати доступ до цільових об’єктів тільки при наявності відкритого відповідного Ticket-запиту в системі керування IT-сервісами (рис. 3.8).

Рис. 3.8. Процес підтвердження заявки ITSM системою

Обірвання сесій. Wallix Bastion надає можливість аудиторам та адміністраторам системи, при підозрі на виконання несанкціонованих дій привілейованим користувачем на цільовій системі – спостереження всіх його дій в реальному часі. Крім самого факту фіксації дій користувача – можливе примусове обривання сесії (рис. 3.9).

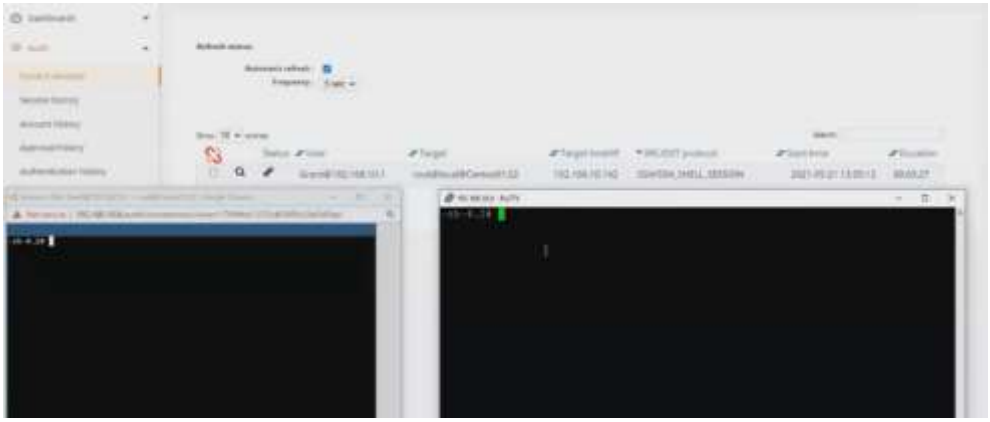

Рис. 3.9. Процес аудиту сесії в реальному часі

Аудит архівних записів. Відповідно, аудит реального часу можна архівувати, та зберігати для подальшого оброблення чи застосування при розслідуванні інцидентів. Wallix Bastion надає можливість перегляду мета даних, транскрипту виконуваних команд під час сесії, та безпосередньо відеозапис у вбудованому плеєрі – для будь якої сесії (рис. 3.10).

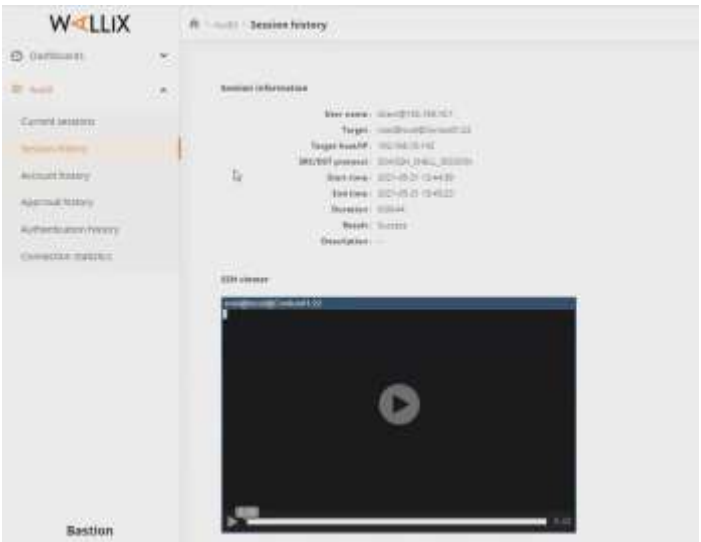

Рис. 3.10. Процес перегляду історії сесії

Виконання автоматичних правил. Адміністратор системи повинен, для особливо чутливих груп кінцевих пристроях, або для вибіркових сукупностей привілейованих користувачів ініціювати правила, які при детектуванні певної поведінки у налаштованій сесії – або обривати сесію, або робити сповіщення відповідальних осіб по електронній пошті (рис. 3.11).

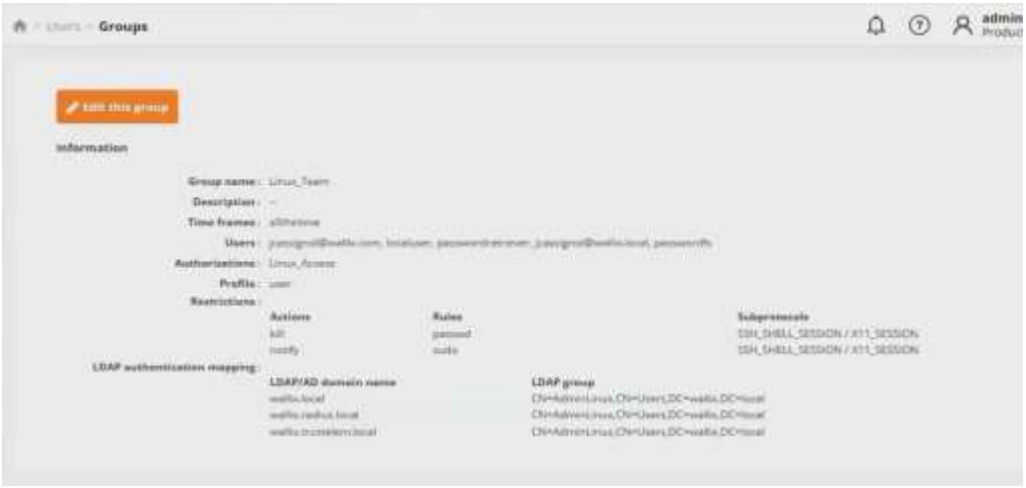

Рис. 3.11. Налаштування обмеження для користувачів

3. Рекомендації «Інтеграція з іншими захисними рішеннями»

Antivirus & DLP. У разі роботи користувачів із файлами у буфері обміну на налаштованих сесіях, існує можливість передачі цих файлів до зовнішніх антивірусних програм, або систем запобігання витоків інформації. ICAP-сервери відповідних антивірусних та DLP рішень можуть бути налаштовані на перевірку дійсності файлів, що передаються під час RDP- та SSH-сесій. Відповідно, у разі детектування, відповідні сповіщення надходять у мета дані сесії та передаються до інтегрованої SIEM-системи, а передача цього файлу блокується (рис.3.12).

Рис. 3.12. Налаштування верифікації файлів при передачі

SIEM. Як це зазначалося раніше, рішення Wallix Bastion має можливість інтеграції з існуючою SIEM системою організації для відвантаження всіх журналів подій (рис . 3.13).

Рис. 3.13. Налаштування інтеграції з SIEM-системою

4. Рекомендації «Відновлення та резервування»

High-Availability. Відповідно до назви, налаштування цієї функції відповідає за надання користувачам системи Wallix Bastion найбільшої доступності. Досягається це завдяки налаштування декіількох екземплярів рішення з увімкненою реплікацією даних, тобто формування їх у кластери (рис. 3.14).

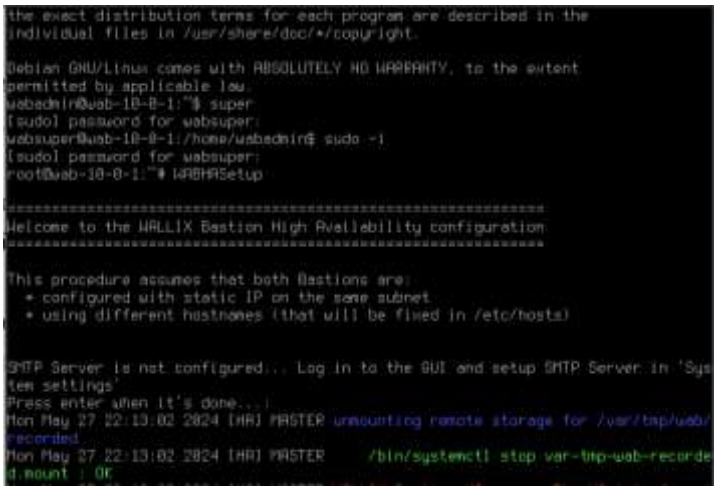

Рис. 3.14. Налаштування High-Availability через вбудований сценарій командного рядка

Backup. Аміністратори системи обов’язково повинні виконувати регулярні процедури резервного копіювання системи Wallix Bastion для того, щоб у разі аварійної ситуації відновити її роботу. Резевні копії відповідно захищаються шифруванням із використанням парольної фрази–ключа (рис. 3.15).

Рис. 3.15. Налаштування High-Availability

Break Glass. Адміністратори системи, для налаштування безперервності критичних процесів організації - можуть реалізувати механізм «розбитого скла» (Break Glass), який дозволяє користувачеві отримати облікові дані груп цільових систем, зібраних в Wallix Bastion, тобто логін, загальне ім'я (CN), паролі та SSH-ключі. Це може стати в нагоді у випадку недоступності WALLIX Bastion (рис. 3.16).

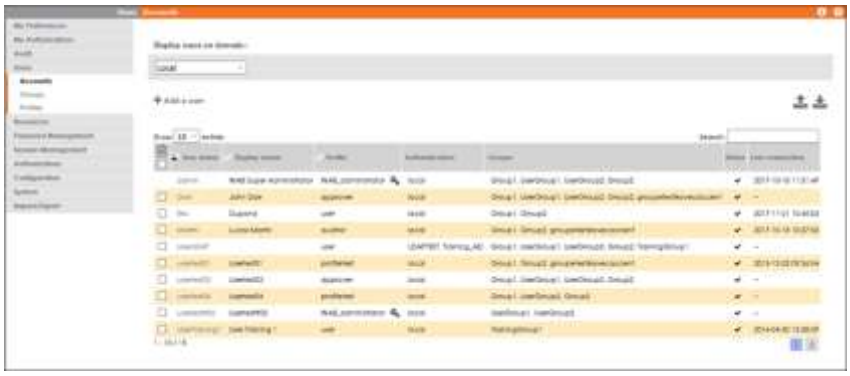

Рис. 3.16. Налаштування механізму «розбітого скла»

5. Рекомендації «Сповіщення та звітність»

Сповіщення на пошту. Адміністратор системи має змогу підлаштувати під себе інформаційні сповіщення, що можуть надсилатися електронною поштою, за різними категоріями (рис. 3.17).

Рис. 3.17. Налаштування сповіщень електронної пошти

Інформаційні панелі. Така форма звітності надає можливості повного контролю загального стану системи, а також моніторинг можливих несправностей чи потенційних порушень (рис. 3.18).

Рис. 3.18. Вигляд інформаційної панелі

3.2. Рекомендації щодо розширення функціональних можливостей Wallix Bastion

Як було продемонстровано в попередніх розділах, рішення Wallix Bastion спрощує і реалізує ключові аспекти управління привілейованим доступом і відповідно захищає привілейовані облікові записи та пов'язані з ними ресурси – на достатньому рівні. Однак, відповідно до основної аксіоми галузі захисту інформації, жодне окреме рішення не здатне повністю вирішити всі потреби безпеки. Захист - це завжди комплексний підхід. Не є виключенням і загрози несанкціонованого доступу до привілейованих облікових записів в інформаційних системах організації.

Компанія Wallix також це усвідомлювала і тому розробила комплексну екосистему продуктів для посилення безпеки та спрощення управління ідентичностями та привілейованим доступом до критичних ресурсів організації. Відповідно, крім основного рішення Wallix Bastion, ця екосистема включає додаткові продукти, що розширюють функціонал та забезпечують всебічний захист від векторів загроз, пов'язаних з несанкціонованим використанням привілейованих облікових записів (рис. 3.19).

Рис. 3.19. Всі продукти в екосистемі Wallix [13]

Серед ключових компонентів екосистеми Wallix варто відзначити рішення [13]:

1. Access Manager - для прозорого та безпечного підключення віддалених користувачів до інформаційних систем організації;

2. Trustelem та Authenticator – хмарний сервіс централізованого управління ідентичностями та доступом (IDaaS) та додаток для багатофакторної автентифікації (MFA) відповідно;

3. BestSafe - спеціалізований продукти для підвищення привілеїв та делегуванням ними на кінцевих точках (PEDM та EPM).

Ці додаткові рішення тісно інтегровані з Wallix Bastion, забезпечуючи цілісний підхід до безпеки привілейованого доступу та автентифікацією та управлінням ідентичностями в організації.

Wallix Access Management [14].

У зв'язку з різким зростанням віддалених користувачів, залучення аутсорсингових потужностей а також необхідності підтвердження відповідності комплаєнсу перед зовнішніми аудиторами та партнерами, забезпечення безпечного віддаленого доступу для співробітників та сторонніх організацій стало ключовою вимогою для IT-індустрії. Компанія Wallix відреагувала на цю потребу, розробивши спеціалізований додатковий продукт Access Manager, який тісно інтегрується з іншими продуктами виробника.

Wallix Access Manager замінює традиційний в своєму роді VPN-з'єднання, яке застосовується для надання доступу віддаленим користувачам. Натомість цей продукт створює єдиний централізований мережевий сервіс, який забезпечує захист з'єднання за рахунок інтеграції виключно HTTPS протоколу (рис. 3.20).

Спрощення встановлення та експлуатації досягається за рахунок того, що сам продукт достатньо розгорнути на будь-якому Unix чи Windows сервері, і вивести у Інтернет білий IP чи доменне ім'я, за яким користувачі зможуть його знайти у будь-якому веб-браузері.

Серед інших функціональних можливостей та переваг – виділяють:

1. Зменшення поверхні атаки:

- Інтеграція з SSO або MFA (через Wallix Authenticator або інших провайдерів);
- Можливість надавати тимчасовий віддалений доступ третім особам і віддаленим співробітникам.

2. Спрощення зовнішнього доступу:

- Використання переваг SSH/RDP консолей, вбудованих у веб-браузер;
- Використання кількох джерел аутентифікації, як локально заведених, так і тих, що постачаються самою системою Wallix Bastion, чи навіть за протоколом LDAP;
- Веб-реалізація надає можливість уникнення розгортання та обслуговування товстих клієнтів.

3. Контрольна та аудиторська діяльність:

- Існує можливість збереження записів та перевірка всієї активність користувачів для усіх сесій;
- Контроль та перевірка зовнішній доступ до всіх пристроїв Wallix Bastion з єдиної консолі.

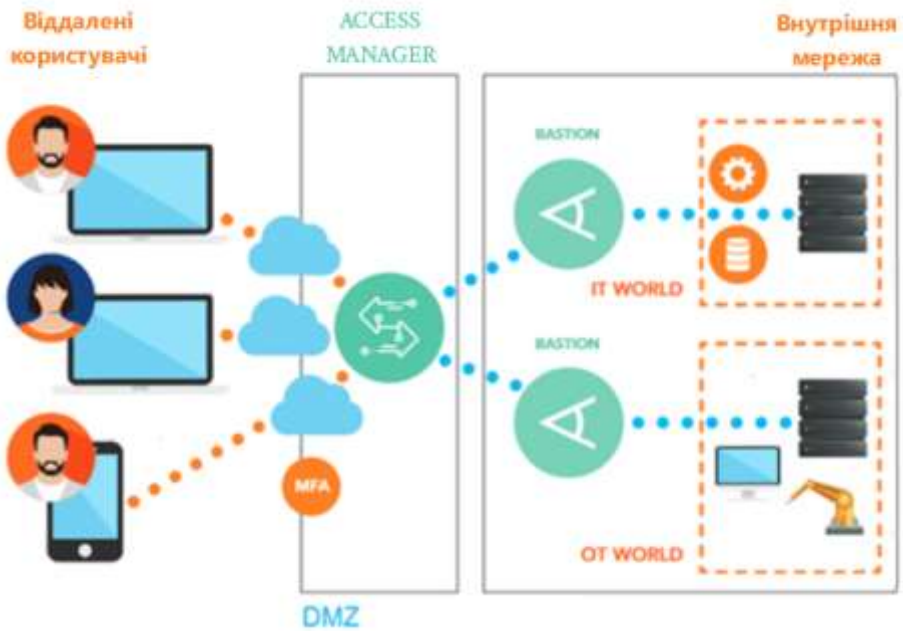

Рис. 3.20. Архітектура продукту Access Manager [14]

Таким чином, Wallix Access Manager стає ключовим доповненням до Wallix Bastion, забезпечуючи безпечний зовнішній доступ для виконання адміністративних завдань та завдань обслуговування. Ця комбінація продуктів дозволяє організаціям впоратися з викликами, пов'язаними зі зростанням віддаленої роботи, зберігаючи високі стандарти безпеки та керованості привілейованих облікових записів.

Wallix Trutelem and Authenticator [15-17].

Підтверджуючи твердження про те, що будь яка система класу PAM – є частиною загальної системи керуванням ідентичностями та доступом IAM/IDM, успішність реалізації та застосовування першої – прямо залежить від успішності реалізації другої. Усвідомлюючи цю взаємозалежність, компанія Wallix розробила рішення Trustelem для забезпечення комплексного управління ідентифікацією в межах своєї продуктової екосистеми.

Wallix Trustelem - це рішення для управління ідентичностями та доступом як сервіс (IDaaS), що пропонує хмарні можливості єдиного входу SSO та багатофакторної автентифікації MFA. Основна мета Trustelem - уніфікувати, забезпечити та спростити доступ користувачів до їхніх додатків. Платформа дозволяє блокувати атаки, такі як фішинг та соціальна інженерія, а також захищати

стратегічні активи за допомогою MFA.

Архітектура рішення максимально проста, воно зчитує відповідну інформацію про існуючі облікові записи користувачів, як з власної бази, так з можливістю інтеграції з такими службами каталогів як Microsoft Active Directory, а також її хмарна реалізація в Azure, Google Suite, інші сервіси що аперують протоколом LDAP тощо (рис. 3.21).

Багатофакторна аутентифікація реалізовано в свою чергу із застосуванням таких можливостей як відправка СМС-повідомлень за номером телефона, надіслання Email-листів з додатковим аутентифікатором, реалізація тимчасово згенерованих одноразових кодів TOTP у додатку Wallix Authenticator чи будь-якому іншому представленому на ринку тощо.

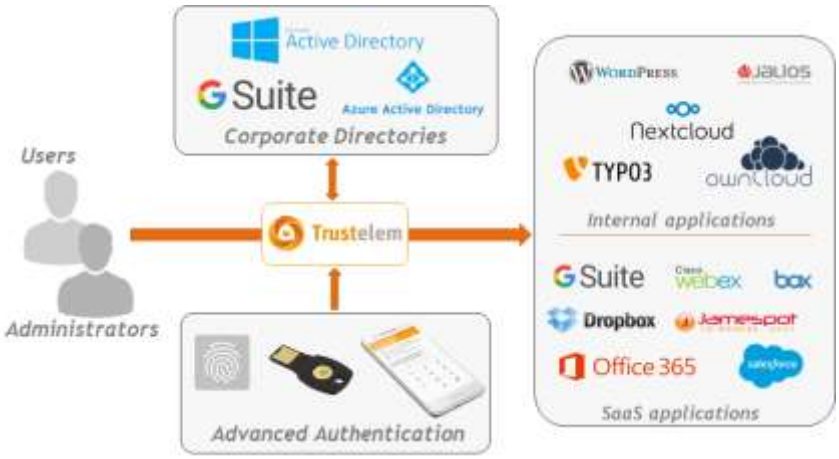

Рис. 3.21. Архітектура продукту Trustelem [15]

Налаштування Trustelem передбачає три основні кроки: додавання користувачів, додавання додатків до яких здійснюється вхід та налаштування правил доступу. Крім того, платформа пропонує додаткові функції, такі як автентифікація без паролів, самостійне скидання паролів, API та інші. Trustelem також надає інструменти для відстеження всіх подій у межах сесії, що дозволяє здійснювати моніторинг та аудит використання системи.

Wallix BestSafe [18].

Wallix Bastion покриває ключові аспекти управління привілейованим доступом, але не має функцій для гнучкого налаштування рівнів привілеїв

користувачів безпосередньо на кінцевих інформаційних системах організації. Для вирішення цього було розроблено рішення Wallix BestSafe.

Рішення BestSafe доповнює екосистему Wallix функціоналом із підвищенням привілеїв та делегуванням ними на кінцевих точках (PEDM та EPM). Це рішення тісно інтегроване з Bastion і дозволяє гнучко налаштовувати рівні привілеїв локальних користувачів та додатків на серверах та робочих станціях в інфраструктурі організації згідно із принципами мінімальних привілеїв та права доступу.

Деякі інформаційні системи, які відносяться до традиційних систем, користувач з адміністративними правами має абсолютний доступ до всіх функцій підвищеного привілею. BestSafe дозволяє точно обмежити привілейований доступ лише до необхідного мінімуму для роботи. Рішення надає можливість гранулярного налаштування рівню привілеїв, що гарантує обмежити привілейований доступ тільки до тих функцій та процесів, які необхідні для виконання тільки службових обов’язків.

Продукт інтегрується в два етапи:

1. Розгортання основного рішення для керування у вигляді розширення до оснасток контролера домену, для можливості створення правил для застосунків та користувачів, з подальшим інтегруванням їх на кінцевих точках з іншими груповими політиками на кінцевій точці;

2. Безпосереднє розгортання агент-модуля на кінцевій точці, який буде перехоплювати керування процесами та застосунками до того, як вони почнуть реалізовувати функції ядра чи операційної системи, перевіряючи на дозвіл, чи блокування, або моніторинг цього процесу на предмет підозрілої активності.

Правила обмеження привілейованого доступу формуються на основі створених білих, сірих чи чорних списків. Білі списки групують перелік дозволених корпоративних програм; сірі списки – відведені для програм, потенційно небезпечних і мають деякі обмеження функціоналу; Чорні – відповідно для застосунків, які повністю заборонені до використання (рис. 3.22).

Рис. 3.22. Алгоритм дії продукту BestSafe [18]

Це допомагає усунути зайвих привілеїв на рівні застосунків та процесів, чи захист від виконання шкідливих процесів з правами привілейованого користувача.

Крім того, ще серед додаткових переваг продукту виділяють:

1. Можливість ротації паролів:

- Гарантія унікальності кожного пароля для кожного комп'ютера, облікового запису та дня;
- Просте й ефективне керування ротацією паролів - один пароль дійсний тільки на певному комп'ютері, у конкретний день і час;
- Відстеження спроб змінити пароль;
- Прогнозування майбутніх змін пароля без під'єднання до мережі.

2. Централізоване управління та аудит привілейованого доступу:

- Вимкнення привілеїв в облікових записах користувачів;
- Керування привілеями на рівні користувача на додаток до привілеїв додатків і процесів;
- Розподіл облікових записів користувачів за групами;
- Встановлення часових обмежень для сеансів користувачів з автоматичним завершенням сеансу після досягнення встановленого терміну;
- Скорочення навантаження на IT-адміністраторів.

3. Проактивний захист від шкідливих програм:

- Автоматичне виявлення намірів виконати шифрування, до початку

самого процесу;

- Зупинка шкідливих процесів і запуск автоматизованих правил відповіді;
- Визначення дій за правилами на основі стандартів або порогових значень адміністратора;
- Збереження ключів шифрування для подальшого розшифрування.

Таким чином, комбінація Wallix Bastion та BestSafe забезпечує цілісне середовище для централізованого управління привілейованим доступом як на рівні мережевих підключень, так і безпосередньо на кінцевих системах, підвищуючи безпеку та полегшуючи процеси адміністрування в організації.

3.3. Розробка загальних рекомендацій щодо захисту від НСД привілейованих облікових записів в ІС організації

Забезпечення належного захисту привілейованих облікових записів в інформаційних системах організацій є критично важливим завданням в епоху зростаючих кіберзагроз. Привілейовані облікові записи, що надають розширені права доступу до критичних ресурсів та систем, є привабливою ціллю для зловмисників. Успішна компрометація таких облікових записів може призвести до катастрофічних наслідків, включаючи витік конфіденційних даних, порушення цілісності систем та навіть повний контроль над ними.

Незважаючи на те, що розробка ефективної стратегії захисту може здаватися складним завданням, існують перевірені практики та рекомендації, які допоможуть організаціям мінімізувати ризики, пов'язані з привілейованим доступом. Впровадження комплексного підходу до управління привілейованими обліковими записами є критично важливим для забезпечення безпеки інформаційних систем та захисту бізнес процесів від зловмисних атак.

Ретельне дотримання рекомендацій щодо захисту привілейованого доступу дозволить організаціям досягти кількох ключових цілей. По-перше, це допоможе суттєво знизити ризики компрометації критичних систем та витоку

конфіденційних даних. По-друге, впровадження належних заходів безпеки забезпечить відповідність вимогам регулюючих органів та галузевим стандартам, що є особливо важливим для організацій, які працюють у регульованих секторах. Нарешті, ефективний захист привілейованих облікових записів підвищить загальний рівень кібербезпеки організації та допоможе зберегти репутацію надійного та безпечного партнера.

Не варто недооцінювати важливість захисту привілейованих облікових записів. Хоча процес розробки та впровадження відповідної стратегії може здаватися складним, представлені рекомендації допоможуть організаціям досягти своїх цілей безпеки та мінімізувати ризики для бізнесу, пов'язані з компрометацією привілейованого доступу [19-21]:

1. Використання стандартних облікових записів: важливо забезпечити використання стандартних облікових записів користувачів для щоденних операцій. Усі користувачі, включно з адміністраторами, повинні мати звичайні облікові записі без підвищених привілеїв для виконання типових завдань, таких як перегляд електронної пошти, доступ до інтернет-банкінгу тощо. Адміністративні облікові записі з розширеними правами доступу слід використовувати виключно для здійснення спеціалізованих адміністративних функцій.

Коли адміністративні привілеї дійсно вимагаються, всі дії, що виконуються з їх використанням, мають бути належним чином контрольовані та захищені за допомогою рішень для управління привілейованим доступом PAM. Ці технології забезпечують прозорість і підзвітність при роботі з адміністративними обліковими записами, допомагаючи організаціям підтримувати принцип найменших привілеїв та мінімізувати ризики зловживання розширеними правами доступу.

2. Уникнення використання спільних облікових записів: важливо уникати практики спільного використання облікових даних та паролів між співробітниками організації або із зовнішніми постачальниками послуг. Такий підхід значно підвищує ризики компрометації облікових записів та зловживання ними. Якщо доступ до системи надається багатьом особам через спільний обліковий запис, то зловмисник, який отримає ці облікові дані, зможе безперешкодно проникнути до

ресурсів організації.

Крім того, спільне використання облікових записів створює серйозні проблеми для забезпечення належного аудиту та відстеження дій користувачів у системі. За наявності загального облікового запису стає неможливим достовірно визначити, хто саме і які операції виконував. Це унеможливлює притягнення користувачів до відповідальності за будь-які неналежні або зловмисні дії.

3. Уникнення повторного використання паролів: одним з ключових правил безпеки є уникнення повторного використання одних і тих самих паролів для різних облікових записів та ресурсів. Якщо зловмисник зможе розгадати або іншим чином отримати пароль для одного ресурсу, то всі інші системи, де використовується такий самий пароль, одразу стануть вразливими для несанкціонованого доступу.

Загроза стає актуальною навіть у тих випадках, коли імена користувачів або облікові записи відрізняються. Головним фактором ризику є однаковий пароль, який зловмисник вже має у своєму розпорядженні. Саме тому надзвичайно важливо уникати використання повторюваних паролів та забезпечити унікальні, складні та регулярно змінювані, у разі потреби, автентифікаційні дані для кожного облікового запису.

4. Уникнення зберігання паролів у відкритому тексті: забезпечення конфіденційності облікових даних є критично важливим для безпеки будь-якої інформаційної системи. Паролі та інші облікові дані в жодному разі не повинні зберігатися у відкритому, незашифрованому вигляді. Незалежно від методу чи місця їх зберігання, вони мають залишатися захищеними та недоступними для несанкціонованих осіб.

Відкрите зберігання паролів створює серйозні ризики їх розголошення та компрометації. Зловмисники, які отримають доступ до незахищених автентифікаційних даних, зможуть безперешкодно проникати у системи від імені легітимних користувачів. Саме тому забезпечення належного захисту та шифрування паролів під час їх передачі, обробки та зберігання має бути пріоритетним завданням для організацій, які серйозно ставляться до кібербезпеки.

5. Мінімізація кількості привілейованих облікових записів: мінімізація кількості привілейованих облікових записів допоможе значно знизити ризики, пов'язані з привілейованим доступом. Чим менше адміністративних облікових записів існує в системі, тим меншою є потенційна поверхня атаки для зловмисників. Відповідно, організація матиме менше можливих векторів для компрометації та зловживання розширеними правами доступу.

Обмежена кількість привілейованих обліків також спрощує процеси контролю, моніторингу та аудиту їх використання. Адміністраторам безпеки доведеться стежити і перевіряти значно меншу кількість активності, пов'язаної з адміністративними обліковими записами. Це підвищить ефективність виявлення та реагування на будь-які підозрілі або зловмисні дії в режимі реального часу.

6. Регулярна зміна паролів для привілейованих облікових записів: регулярна зміна паролів для привілейованих облікових записів є важливим заходом безпеки, який допоможе запобігти їх компрометації та зловживанню. Рекомендується змінювати паролі привілейованих обліків після кожного використання для виконання адміністративних дій або принаймні на регулярній основі за визначеним графіком.

Своєчасна зміна паролів не дозволить їм застаріти та стати частиною атак шляхом повторного використання вже відомих зловмисникам облікових даних. Крім того, часта ротація паролів значно знижує ризики їх витоку протягом тривалого періоду часу. Навіть якщо пароль стане відомим зловмиснику, обмежений термін його дії зведе нанівець можливість його подальшого використання.

7. Забезпечення належної складності паролів для привілейованих облікових записів є критично важливим заходом безпеки. Привілейовані паролі в жодному разі не повинні бути легко читабельними для людини або нагадувати звичайні слова чи фрази. Використання складних, випадкових комбінацій символів допоможе захиститися від спроб їх підбору або усного розголошення.

При виборі паролів для привілейованих облікових записів необхідно дотримуватися найвищих стандартів складності. Деякі з них мають бути ще

складнішими, ніж інші, для мінімізації ризиків, пов'язаних із людським фактором. Це може включати використання спеціальних символів, випадкових цифрових послідовностей тощо.

8. Впровадження багатофакторної автентифікації: впровадження багатофакторної автентифікації є важливим кроком для підвищення безпеки доступу до внутрішніх систем, додатків та конфіденційних даних організації. Замість покладання лише на один фактор автентифікації, такий як пароль, багатофакторна автентифікація вимагає додаткових елементів підтвердження, наприклад, одноразових токенів, біометричних даних або фізичних носіїв.

При розгортанні багатофакторної автентифікації слід враховувати не лише статичні фактори, такі як тип системи чи додатку, але і динамічні ризики, пов'язані з контекстом доступу. Наприклад, якщо користувач намагається виконати критично важливу операцію у незвичний час, з нового місця або на системі з невстановленими критичними оновленнями безпеки, доцільно вимагати додаткового етапу автентифікації. Такий контекстний підхід допоможе мінімізувати ризики, не обмежуючи користувачів під час звичайної діяльності.

9. Важливим заходом безпеки є впровадження контролю репутації додатків, що дозволяє організаціям визначати, які програми є безпечними для використання, а які потенційно небезпечними. Це досягається шляхом використання білих, чорних та сірих списків.

Білі списки містять перелік дозволених додатків, які вважаються безпечними. Чорні списки включають програми, визнані шкідливими або можуть бути задіяні у зловмисній діяльності, запуск яких має бути заблокований. Сірі списки призначені для додатків із невизначеною репутацією, які потребують додаткового аналізу та контролю.

ВИСНОВКИ

В результаті виконання кваліфікаційної роботи було проведено ґрунтовний аналіз проблеми захисту привілейованих облікових записів в інформаційних системах організацій. Ця проблема є надзвичайно актуальною, оскільки привілейовані облікові записи є критично важливими для забезпечення безпеки та безперервної роботи ІС, а їх компрометація може призвести до серйозних наслідків, включаючи втрату конфіденційних даних, порушення цілісності та доступності систем.

Було досліджено різноманітні методи та засоби для впровадження системи привілейованого доступу (PAM) в інформаційні системи організацій. Особливу увагу приділено реалізації рішенню Wallix Bastion, а також інших рішень цієї екосистеми, які є потужним інструментом для управління привілейованим доступом та забезпечення належного рівня безпеки.

На основі проведеного аналізу та досліджень були розроблені рекомендації щодо успішного впровадження PAM для захисту інформаційних систем організацій від несанкціонованого доступу. Ці рекомендації охоплюють різні аспекти, такі як вибір та налаштування відповідного рішення PAM, організація процесів управління привілейованим доступом, навчання персоналу та моніторинг і аудит дій привілейованих користувачів.

Впровадження системи привілейованого доступу відповідно до розроблених рекомендацій дозволить організаціям підвищити рівень безпеки своїх інформаційних систем, зміцнити захист від несанкціонованого доступу та забезпечити відповідність нормативним вимогам у сфері інформаційної безпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Madnick S. The continued threat to personal data: key factors behind the 2023 increase. 2023.

2. Flashpoint. Data breach. URL: https://flashpoint.io/intelligence-101/data-breach/ (date of access: 01.05.2024).

3. Haber M. J. Privileged attack vectors: building effective cyber-defense strategies to protect organizations. Apress, 2020. 419 p.

4. IDSA. 2023 trends in securing digital identities. 2023.

5. Verizon. 2023 Data Breach Investigations Report. URL: https://www.verizon.com/business/resources/reports/dbir/ (date of access: 01.05.2024).

6. НД ТЗІ: Типове положення про службу захисту інформації в автоматизованій системі від 04.12.2000 р. № 1.4-001-2000 : станом на 28 груд. 2012 р.

7. BeyondTrust. Microsoft vulnerabilities report 2024. 2024.

8. Gartner. Magic quadrant for privileged access management. URL: https://www.gartner.com/doc/reprints?id=1-2GFGKSOO&ct=240201&st=sb (date of access: 01.05.2024).

9. Державна служба спеціального зв’язку та захисту інформації України. Засоби ТЗІ, які мають експертний висновок про відповідність до вимог технічного захисту інформації. 09.2023.

10. Inteligent IT Destribution. The WALLIX bastion hardware and software system is certified by the state service of special communications and information protection of ukraine. Intelligent IT Distribution. URL: https://iitd.com.ua/en/news/wallix-bastion-sertifikovano-dzi/ (date of access: 01.05.2024).

11. Wallix PAM privileged access management. URL: https://vntek.vn/vi/san-pham/wallix-giai-phap-quan-ly-tai-khoan-dac-quyen-pam.html (date of access: 01.05.2024).

12. Wallix. Privileged access management - WALLIX. URL: https://www.wallix.com/privileged-access-management/ (date of access: 01.05.2024).

13. Golicense. The importance of network security: why businesses need wallix. Golicense. URL: https://golicense.net/product-category/security-license/wallix/ (date of access: 01.05.2024).

14. Wallix. Wallix datasheet Access Manager. 2023.

15. Wallix. Doc Trustelem. URL: https://trustelem-doc.wallix.com/ (date of access: 01.05.2024).

16. Wallix. Wallix datasheet Trustelem. 2023.

17. Wallix. Wallix datasheet Authenticator. 2023.

18. Wallix. Wallix datasheet BestSafe. 2023.

19. Microsoft. What is privileged access management (PAM) | microsoft security. URL: https://www.microsoft.com/en/security/business/security-101/what-is-privileged-access-management-pam (date of access: 01.05.2024).

20. Delinea. What is privileged access management (PAM)? | delinea. URL: https://delinea.com/what-is/privileged-access-management-pam#expert (date of access: 01.05.2024).

21. SenhaSegura. Ebook - privileged access management 101. Brazil, Brasília, 2023. 24 p.

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)