Давидов Петро

Рев'ю на тему

«Забезпечення безпеки облікових записів корпоративних користувачів»

Вступ

У статті «Забезпечення безпеки облікових записів корпоративних користувачів» Іван Ярославович Тишик, кандидат технічних наук, доцент кафедри захисту інформації Національного університету «Львівська політехніка», досліджує актуальну проблему захисту облікових даних у корпоративних мережах. Основна тема публікації - забезпечення безпеки облікових записів користувачів у мережевих операційних системах, зокрема в середовищі Windows Server та Active Directory (AD).

Автор ставить перед собою мету, визначити базовий набір правил щодо створення, призначення та використання облікових записів, організувати комплекс утиліт для адміністрування AD, провести діагностику його захищеності та запропонувати серверну ОС, яка забезпечує додатковий захист привілейованих облікових записів. Приділяється увага практичному аспекту адміністрування, виявлення вразливостей, протидія атакам та впровадження інструментів моніторингу.

Методологія

Дослідження має прикладний характер, базується на аналізі актуальних загроз, практик адміністрування та функціональних можливостей Windows Server.

У статті використовуються такі методи:

- Огляд статистичних даних щодо вразливостей ОС (зокрема, згадано про1428 вразливостей у Windows Server 2019 за останні 4 роки)
- Аналіз інструментів тестування та моніторингу (Kali Linux, Metasploit, rdpscan)
- Моделювання атак (наприклад, ескалація прав через mimikatz)
- Практичне використання утиліт: Netwrix Auditor, Account Lockout Examiner, Semperis DSP, SolarWinds Permissions Analyzer

- Впровадження політик безпеки AD, включаючи параметри групових політик, захищені групи користувачів, парольні обмеження

Методи збору даних включають емпіричне тестування(тобто на практичному досвіді), спостереження за поведінкою системи при атаках, а також аналіз функціональності утиліт у реальному середовищі.

Результати

Формується низка практичних рекомендацій, які дозволяють значно підвищити рівень захисту облікових записів у корпоративному середовищі:

1. *Визначено базові правила створення облікових записів:*

   - ✓ Мінімізація адміністративних привілеїв
   - ✓ Персоніфікація акаунтів адміністраторів
   - ✓ Заборона запуску сервісів під обліковими записами адміністраторів

2. *Розроблено політику паролів:*

   - ✓ Мінімальна довжина пароля: 10 символів для користувачів, 14 - для адміністраторів
   - ✓ Вимога унікальності: новий пароль має відрізнятись від попереднього на більше ніж 3 (три) символи
   - ✓ Термін дії пароля: 5 - 7 днів
   - ✓ Використання генераторів випадкових паролів та мобільних додатків для їх зберігання (Sticky Password)

3. *Запропоновано комплекс утиліт для моніторингу AD:*
   - ✓ Account Lockout Examiner - аналіз спроб входу з неправильним паролем
   - ✓ Netwrix Auditor - виявлення несанкціонованих змін, пошкодження файлів
   - ✓ Semperis DSP - фіксація змін навіть при вимкненому журналюванні

4. *Впроваджено механізм захищеної групи користувачів (Protected Users):*
   - ✓ Автентифікація лише через Kerberos
   - ✓ Вимога AES-шифрування
   - ✓ Відсутність кешованих облікових даних
   - ✓ Обмеження дії TGT-квитків - повторна автентифікація кожні 4 години

5. *Проведено моделювання атаки з використанням mimikatz та демонстрацію її виявлення через Semperis DSP.*

6. *Висвітлено ризики, пов'язані з кешованими обліковими даними, та способи їх контролю через групові політики.*

Ключові інсайти

1. Використання групи Protected Users - механізм захисту привілейованих облікових записів

Цей інсайт є важливим для побудови безпечної IAM архітектури. Він дозволяє обмежити використання слабких протоколів автентифікації, зменшити ризик компрометації та забезпечити контроль над життєвим циклом облікових записів. Може бути застосовано для сегментації доступу до критичних ресурсів.

2. *Semperis DSP - інструмент для виявлення змін навіть при вимкненому журналюванні*

Це відкриває нові можливості для моніторингу AD у складних умовах, коли стандартні засоби не працюють. Можна сказати, що, цей інсайт є одним з ключових для побудови системи реагування на інциденти, особливо в середовищах з високими вимогами до доступності та прозорості.

3. *Строга політика паролів, генератори, мобільні сховища, та їх використання у зв'язці, створює баланс між безпекою і зручністю.*

Це рішення дозволяє реалізувати захист від атак типу Kerberoasting, не створюючи надмірного навантаження на користувачів. Це може бути підставою для впровадження password hygiene framework у середовищі з великою кількістю кінцевих користувачів.

Висновок

Стаття є цінним внеском у прикладну кібербезпеку корпоративного рівня. Вона поєднує теоретичні засади інформаційного захисту з практичними інструментами адміністрування та моніторингу. Розуміння автором архітектури Windows Server та Active Directory, дає автору можливість висвітлювати та пропонувати конкретні рішення для підвищення захищеності облікових записів.

У публікації треба звернути увагу на слідуючи вектори:

- ✓ Формалізація правил створення та використання облікових записів
- ✓ Впровадження комплексного інструментарію для моніторингу AD
- ✓ Аналіз механізмів автентифікації та кешування
- ✓ Практичне моделювання атак і демонстрація реагування

Подальші дослідження можна сконцентрувати на таких пунктах:

- ✓ Розширення номенклатури утиліт для моніторингу (наприклад, Quest Change Auditor)
- ✓ Вивчення поведінки системи при складних атаках
- ✓ Автоматизацію аудиту змін у глибоко вкладених групах користувачів

Ця публікація є джерелом практичних рішень, які можуть бути інтегровані в реальні корпоративні середовища для підвищення рівня захисту, прозорості та керованості доступом.