УДК 004.056.53 https://doi.org/10.35546/kntu2078-4481.2023.1.16

Є. М. БАЙЛЮК
старший викладач кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»
ORCID: 0000-0002-4961-7816

О. А. ПОКОТИЛО
старший викладач кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»
ORCID: 0000-0002-1587-235X

О. С. ГОЛОВНЯ
кандидат педагогічних наук,
доцент кафедри комп'ютерної інженерії та кібербезпеки
Державний університет «Житомирська політехніка»
ORCID: 0000-0003-0095-7585

І. С. ХІМІЧУК
студент
Державний університет «Житомирська політехніка»
ORCID: 0009-0000-4456-0868

АНАЛІЗ КІБЕРАТАК НА ACTIVE DIRECTORY ТА МЕТОДІВ ПІДВИЩЕННЯ РІВНЯ ЗАХИЩЕНОСТІ ОПЕРАЦІЙНОЇ СИСТЕМИ WINDOWS SERVER

У статті розглянуто кібератаки на Active Directory операційної системи Windows Server та досліджено можливі способи протидії таким атакам та пом'якшення їх наслідків.

Враховуючи популярність Active Directory для побудови корпоративних мереж, високою є й зацікавленість кіберзлочинців в атаках з метою порушення роботи таких систем чи одержання конфіденційної інформації, а отже, зростає потреба запобігання таким атакам та мінімізації їх впливу. У статті здійснено огляд наявних публікацій, присвячених цій проблематиці. Водночас, наголошується на необхідності дослідження різних видів атак на Active Directory, зокрема нових, а також на важливості володіння комплексом методів та інструментів для захисту від цих атак. Досліджено та проаналізовано такі види кібератак на Active Directory, як «розпилення» пароля, передача хешу, атаки з «золотим» та «срібним квитком», DNS-спуфінг, атаки на об'єкт групової політики, розширення DNS, атаки DCSync та SMB Relay. Розглянуто низку інструментів, які можуть використовуватися кіберзлочинцями і які повинні братися до уваги фахівцями з кібербезпеки під час налаштування та тестування захисту корпоративної мережі на базі Active Directory (Mimikatz, Bloodhound, Empire, CrackMapExec, Nmap, Metasploit, Responder, PowerUp, LaZagne). У ході проведення аналізу різних видів кібератак та інструментів, доступних зловмисникам, визначено загальні вразливості Active Directory та вектори відповідних атак. Наведено можливі стратегії пом'якшення ризиків успішного проведення атак, зокрема впровадження політики надійних паролів, багатофакторної автентифікації, контролю доступу з найменшими привілеями, оновлення програмного забезпечення та виправлень безпеки і моніторингу та виявлення підозрілої активності. Загалом стаття містить інформацію про ризики безпеки, пов'язані з Active Directory, і в ній запропоновано практичні поради для IT-фахівців, які прагнуть посилити захист від кібератак, спрямованих на цю критично важливу систему.

Ключові слова: *вразливості, кібератаки, Active Directory, інструменти проведення атак, запобігання атакам, зменшення ризиків, пом'якшення наслідків кібератак.*

Y. M. BAILIUK
Senior Lecturer at the Department of Computer Engineering and Cyber Security
Zhytomyr Polytechnic State University
ORCID: 0000-0002-4961-7816

O. A. POKOTYLO
Senior Lecturer at the Department of Computer Engineering and Cyber Security
Zhytomyr Polytechnic State University
ORCID: 0000-0002-1587-235X

O. S. HOLOVNIA
Candidate of Pedagogical Sciences,
Associate Professor at the Department of Computer Engineering and Cyber Security
Zhytomyr Polytechnic State University
ORCID: 0000-0003-0095-7585

I. S. KHIMICHUK
Student
Zhytomyr Polytechnic State University
ORCID: 0009-0000-4456-0868

ANALYSIS OF CYBER ATTACKS ON ACTIVE DIRECTORY AND METHODS OF INCREASING THE SECURITY LEVEL OF THE WINDOWS SERVER OPERATING SYSTEM

The article examines cyber-attacks on Active Directory of Windows Server operating system and investigates possible ways to prevent and mitigate them.

Considering the popularity of Active Directory for building corporate networks, cyber criminals are highly interested in attacking it to disrupt its work or gain access to confidential information, and therefore, there is an increasing need for preventing and mitigating these attacks. The paper gives an overview of available publications on these issues. At the same time, the authors of the article emphasize the necessity of studying different types of attacks on Active Directory, in particular, new attacks, as well as the importance of being aware of versatile methods and tools for mitigating these attacks. The work studies and analyses the cyber-attacks on Active Directory, including Password Spraying, Pass-the-Hash, Golden Ticket and Silver Ticket Attacks, DNS Spoofing, attacks on group policy objects, DNS amplification, DCSync and SMB Relay attacks. The authors consider instruments available to cyber criminals and should be factored in by cybersecurity professionals while configuring and testing the defense of corporate networks based on Active Directory (Mimikatz, Bloodhound, Empire, CrackMapExec, Nmap, Metasploit, Responder, PowerUp, LaZagne). Through the analysis of different types of cyber-attacks and tools possibly exploited by intruders, the study determines general vulnerabilities of Active Directory, and corresponding attack vectors. In addition, possible strategies to mitigate the risks of successful attacks are considered, including implementing strong password policies, multi-factor authentication, least-privilege access control, software updates and security patches, and monitoring and suspicious activity detection. Consequently, the article provides information on the security risks associated with Active Directory and suggests practical advice for IT professionals who want to strengthen their defenses against cyber-attacks targeting this mission-critical system.

Key words: *vulnerabilities, cyber-attacks, Active Directory, attack tools, attacks prevention, risk reduction, mitigating the consequences of cyber-attacks.*

Постановка проблеми

Оскільки технології прогресують і організації все більше покладаються на цифрову інфраструктуру, безпека інформаційно-комунікаційних систем стає все більш важливою. Active Directory операційної системи Windows Server є критично важливим компонентом IT-інфраструктури багатьох організацій, забезпечуючи централізовану платформу для керування обліковими записами користувачів, груповими політиками та ресурсами комп'ютера. Однак із такою критичністю зростає ризик кібератак, оскільки зловмисники намагаються використовувати вразливості в AD, щоб отримати доступ до конфіденційної інформації або порушити роботу системи.

Враховуючи критичну роль AD в управлінні IT-інфраструктурою організації, важливо розуміти природу цих атак і методи, які можна використовувати для запобігання або їх пом'якшення. Тому аналіз кібератак на Active Directory є важливою областю дослідження для IT-фахівців та адміністраторів безпеки.

Цей аналіз може надати цінну інформацію про ризики, пов'язані з атаками AD, зокрема про тактику, методи та процедури, які використовують зловмисники. Це також може допомогти виявити слабкі місця в інфраструктурі AD організації та надати вказівки щодо заходів, які можна вжити для їх усунення. Розуміючи природу цих атак і застосовуючи належні заходи безпеки, організації можуть зменшити ризик стати мішенню кіберзлочинців і забезпечити безпеку та цілісність своєї IT-інфраструктури.

Формулювання мети дослідження

Метою даної роботи є дослідження різних типів атак на Active Directory ОС Windows, інструментів, які можуть використовувати кіберзлочинці для їх проведення, методів запобігання та пропонування стратегій пом'якшення ризиків успішного проведення атак.

Аналіз останніх досліджень та публікацій

Під час проведення досліджень з даної теми було проаналізовано ряд публікацій, що стосуються атак на Active Directory. Зокрема, у статті Lukas Kotlaba, Simona Buchovecka та Robert Lorencz [1] основною темою є виявлення атаки Kerberoasting у середовищі Active Directory. Мета атаки полягає в тому, щоб отримати паролі облікових записів сервісів без потреби в будь-яких спеціальних правах доступу користувача чи ескалації привілеїв, що

робить її придатною для початкових фаз компрометації мережі та подальшого повороту для більш привілейованих облікових записів. Основною метою статті є обговорення можливостей моніторингу, налаштування правил виявлення, побудованих на основі вбудованих можливостей аудиту Active Directory, включаючи можливі способи мінімізації помилкових спрацьовувань.

У роботі Muthuraj S., Sethumadhavan M., Amritha P. P. та Santhya, R. [2] розглянуто виявлення відомих атак, спрямованих на служби домену з боку зловмисника за допомогою SIEM. Також запропоновано методи запобігання цим атакам. SIEM широко використовуються в багатьох організаціях аналітиками безпеки для моніторингу їхньої мережі за допомогою журналів подій. Правила виявлення були розроблені та реалізовані в Splunk. Оцінювання правил і атак були виконані у віртуальному середовищі.

Дослідження авторів Basem Ibrahim Mokhtar, Anca D. Jurcut, Mahmoud Said ElSayed та Marianne A. Azer [3] надає уявлення про критичність, вплив і виявлення атак Active Directory. У статті розглянуто різні атаки на Active Directory. Також представлено етапи атаки Active Directory і робочий процес автентифікації Kerberos, яким зловживають в більшості атак для компрометації середовища Active Directory. Крім того, проведено експерименти з двома атаками, які базуються на підвищенні привілеїв, щоб перевірити сигнатури атак у журналах подій Windows.

У статті Giuseppe Nebbione та Maria Carla Calzarossa [4] запропоновано методологічну структуру за допомогою штучного інтелекту, спрямовану на оцінювання того, є цільове середовище вразливим чи безпечним. Фреймворк заснований на комбінованому застосуванні методів на основі графів і машинного навчання. Компоненти цілі разом із їхніми вразливими місцями представлені графіками, аналіз яких ідентифікує шляхи атак, пов'язані з потенційними загрозами безпеці. Методи машинного навчання класифікують ці шляхи та забезпечують оцінювання безпеки цілі. Експериментальне оцінювання запропонованого фреймворку була проведена на 220 штучно створених середовищах Active Directory, половина з яких містила вразливості.

У роботі Charlie Clark [5] зазначено, що Microsoft Active Directory була представлена для вирішення безлічі мережевих проблем. Але відкритість і широке поширення також зробили її основною мішенню для кібератак. У цій статті розглядається одна конкретна вразливість і те, як вона демонструє ключову роль Active Directory і її потенціал як слабкого місця у ваших мережах.

Ціль статті Bamidele Oni та Aboubakar Kpelafiya [6] полягає в аналізі компонентів архітектури серверів та загроз безпеці, які можуть виникнути проти серверів Windows і Linux. Крім того, у статті наведено загальний опис контрзаходів, які можна застосувати для захисту від різних загроз і вразливостей в обох операційних систем.

У статті авторів Ільєнко А. В., Ільєнко С. С. та Куліш Т. [7] розглянуто проблеми забезпечення інформаційної безпеки операційної системи Windows та визначення перспективних методів забезпечення захисту. Також зроблено аналіз та проведено класифікацію сучасних вразливостей операційної системи та на прикладах наведено наслідки їх дії. Крім того, визначено основні підходи і методи щодо організації захисту операційної системи. Розглянуто стандартні підходи, а саме використання вбудованих засобів захисту програмного забезпечення, захист Active Directory, віртуалізація для стримування атак. В роботі показані власні приклади реалізації Blockchain для перевірки сертифікатів, враховуючи деякі із варіацій перевірок. Приклади реалізовано на Python 3.0.

В дослідженні Струкова В. М. та Гуділіна В. В. [8] були розглянуті деякі з актуальних можливих методів проведення атак на корпоративні інформаційні системи, які засновані на використанні служби каталогів Active Directory і метою яких є отримання прав адміністратора домену, а також було надано практичні рекомендації із захисту та детектування проаналізованих видів атак.

В роботі Юкальчук А. І., Загоруйко Л. В., та Мартьянової Т. А. [9] наводиться приклад дослідження реалізації комп'ютерної атаки у типовій інформаційній інфраструктурі, яка вміщує корпоративну мережу з доменною архітектурою та автоматизовану систему управління технологічним процесом. Для розглянутого прикладу визначено оптимальні значення часових параметрів безпеки.

Під час аналізу публікацій, присвячених даній темі, було виявлено, що в них описано невелику кількість атак та не враховано нові типи атак. Крім того, розглянуті в цих дослідженнях методи та засоби захисту від цих атак є досить обмеженими. В даній статті, окрім аналізу атак на Active Directory, описано спеціалізовані інструменти, за допомогою яких зловмисники можуть успішно реалізовувати ці атаки. Знаючи про ці інструменти, адміністраторам безпеки буде значно легше захистити систему від вторгнень. Також у цій статті наведено методи та засоби, які можуть забезпечити високий рівень захисту системи чи значно зменшити ризик успішної реалізації таких атак.

Викладення основного матеріалу дослідження

Кібератаки на Active Directory (AD) можуть приймати різні форми, включаючи атаки на паролі, підвищення привілеїв і прослуховування мережного трафіку. Зловмисники часто використовують тактику соціальної інженерії, наприклад фішинг, щоб отримати доступ до облікових даних AD, які вони можуть використовувати для отримання доступу до мережі та конфіденційних ресурсів. Отримавши доступ, зловмисники можуть виконувати команди, встановлювати зловмисне програмне забезпечення та виконувати інші шкідливі дії, часто з метою викрадання конфіденційних даних або зриву бізнес-операцій. Розглянемо основні типи кібератак на Active Directory, які найчастіше проводяться зловмисниками.

«Розпилення» пароля (Password Spraying) є одним із найпоширеніших типів атак на Active Directory. Зловмисник намагається увійти в AD за допомогою списку часто використовуваних паролів, сподіваючись отримати доступ до одного або кількох облікових записів. Він може використовувати автоматизовані інструменти для перевірки великої кількості паролів зі списком імен користувачів. Отримавши доступ до облікового запису, зловмисники потенційно можуть викрасти конфіденційну інформацію або встановити зловмисне програмне забезпечення на скомпрометованій машині. Щоб запобігти атакам з «розпиленням» паролів, організації повинні заохочувати використання надійних паролів і впроваджувати політику блокування облікових записів, яка запобігає атакам підбору. Крім того, багатофакторна автентифікація може ускладнити зловмисникам отримання доступу до облікових записів, навіть якщо вони мають правильний пароль.

Іншим типом атаки, спрямованої на Active Directory, є передача хешу (Pass-the-Hash). У цьому типі атаки зловмисник викрадає хеш пароля облікового запису AD і використовує його для автентифікації користувача, не знаючи фактичного пароля. Цю атаку можна здійснити шляхом перехоплення мережевого трафіку, доступу до скомпрометованої машини або використання шкідливого програмного забезпечення. Коли зловмисник отримує доступ до облікового запису, він може видати себе за законного користувача та отримати доступ до конфіденційних ресурсів. Щоб запобігти атакам передачі хешу, організації повинні використовувати надійні алгоритми шифрування для захисту хешів паролів, наприклад шифрування Kerberos. Вони також повинні використовувати ізоляцію домену, щоб запобігти доступу зловмисників до інших машин у мережі після того, як вони скомпрометували одну машину.

Атака з «золотим квитком» (Golden Ticket Attack) – це тип атаки, у якому зловмисник отримує хеш пароля облікового запису KRBTGT і використовує його для створення підробленого квитка для видачі квитків (TGT), який може надати йому доступ до будь-якої служби в домені. Маючи Golden Ticket, зловмисник може отримати повний контроль над доменом і скомпрометувати будь-який сервіс. Атаки з Golden Ticket важко виявити, і їх можна здійснити, навіть якщо організація має потужні механізми автентифікації. Щоб запобігти атакам з Golden Ticket, організації повинні забезпечити безпеку своїх контролерів домену AD і захист облікових даних адміністратора. Вони також повинні стежити за діяльністю облікового запису KRBTGT і використовувати засоби контролю доступу з найменшими привілеями, щоб обмежити збитки, які може завдати зловмисник, якщо йому вдасться отримати Golden Ticket.

Атака зі «срібним квитком» (Silver Ticket Attack) – це тип атаки, у якій зловмисник створює підроблений TGT для певного облікового запису служби. За допомогою Silver Ticket зловмисник може отримати доступ до певних служб, не будучи виявленим. Цей тип атаки часто використовується зловмисниками, які вже скомпрометували мережу та хочуть зберегти доступ до певної служби чи ресурсу. Щоб запобігти атакам з Silver Ticket, необхідно використовувати надійні алгоритми шифрування для захисту облікових даних сервісного облікового запису, наприклад AES-256. Також потрібно використовувати засоби контролю доступу з найменшими привілеями.

Атака DCSync – це тип атаки, у якій зловмисник імітує контролер домену та запитує реплікацію даних облікового запису AD. Ці дані можуть містити конфіденційну інформацію, таку як паролі та хеші. Отримавши ці дані, зловмисник може використовувати їх для подальших атак на мережу. Щоб запобігти атакам DCSync, організації повинні використовувати безпечні протоколи зв'язку, такі як LDAP через SSL/TLS, щоб захистити конфіденційні дані AD під час передачі. Крім того, потрібно використовувати шифрування для захисту конфіденційних даних у стані зберігання, наприклад вмісту бази даних AD.

DNS-спуфінг (DNS Spoofing) – це тип атаки, під час якої зловмисник перенаправляє DNS-запити на підроблений сервер, що дозволяє йому перехоплювати трафік і потенційно отримувати доступ до конфіденційної інформації. У контексті Active Directory, підробка DNS може використовуватися для перенаправлення запитів автентифікації на підроблений сервер, дозволяючи зловмиснику перехоплювати облікові дані для входу. Для того, щоб запобігти атакам DNS-спуфінгу, слід запровадити безпечні протоколи DNS, наприклад DNSSEC, і регулярно перевіряти свої журнали DNS на наявність підозрілої активності.

Атаки на об'єкт групової політики (GPO). GPO є ключовою функцією Active Directory, яка використовується для керування налаштуваннями користувачів і комп'ютера. Зловмисники можуть використовувати вразливості в GPO, щоб отримати підвищені привілеї або встановити шкідливе програмне забезпечення на цільових машинах. Наприклад, зловмисник може змінити GPO, щоб встановити бекдор на всіх машинах у домені. Щоб запобігти атакам на GPO, організаціям слід регулярно переглядати налаштування своїх GPO та переконатися, що вони використовують найновіші рекомендації щодо безпеки від Microsoft. Також необхідно обмежити доступ до інструментів керування GPO довіреним адміністраторам і використовувати інструменти аудиту для моніторингу змін GPO.

Розширення DNS (DNS Amplification) – це тип атаки, під час якої зловмисник надсилає DNS-запит на сервер, підробляючи вихідну IP-адресу, щоб виглядати так, ніби запит надходить з комп'ютера легального користувача. Потім сервер відповідає набагато більшим пакетом, ніж початковий запит, переповнюючи машину легального користувача трафіком і потенційно викликаючи атаку на відмову в обслуговуванні (DoS). Щоб запобігти атакам

посилення DNS, необхідно впроваджувати такі заходи безпеки, як брандмауери та системи виявлення вторгнень, які можуть ідентифікувати та блокувати підроблені запити DNS. Крім того, необхідно налаштувати свої DNS-сервери, щоб відповідати лише на законні запити та обмежити розмір відповідей, щоб запобігти розширенню DNS.

SMB Relay – це тип атаки, яка використовує слабкість у протоколі SMB (Server Message Block), який використовується системами Windows для спільного використання файлів і принтерів. Атака працює шляхом перехоплення та передачі запитів автентифікації SMB між клієнтом і цільовим сервером. Зловмисник спочатку визначає цільову систему в мережі, яка вразлива до атак SMB Relay, потім перехоплює запити автентифікації SMB від інших систем у мережі. Далі зловмисник передає запит автентифікації на контролер домену в мережі для отримання облікових даних домену для користувача, який спочатку зробив запит на автентифікацію. Маючи доступ до облікових даних домену, зловмисник може виконувати різноманітні зловмисні дії в мережі, наприклад створювати нові облікові записи користувачів, підвищувати привілеї та отримувати доступ до конфіденційних даних. Щоб запобігти атакам SMB Relay на Active Directory, необхідно переконатися, що всі системи в мережі оновлені з останніми виправленнями безпеки. Крім того, потрібно запровадити сегментацію мережі та контроль доступу, щоб обмежити поширення атак. Також необхідно відстежувати мережевий трафік на наявність ознак атак SMB Relay, таких як численні запити автентифікації з однієї IP-адреси, та використовувати такі технології, як підписання SMB і шифрування SMB [10], [11].

Для проведення атак на Active Directory зловмисники можуть використовувати різноманітні інструменти. Далі розглянемо найпопулярніші з них.

Mimikatz – це інструмент, який дозволяє зловмиснику отримувати з пам'яті чисті текстові паролі, хеші та інші облікові дані автентифікації. Його також можна використовувати для підвищення привілеїв і виконання команд у скомпрометованій системі.

Bloodhound – інструмент, який допомагає визначати вразливості в середовищах Active Directory. Він відображає зв'язки між користувачами, групами, комп'ютерами та іншими ресурсами в межах домену, що допомагає зловмисникам визначити потенційні шляхи для проведення атаки.

Empire – це пост-експлуатаційний інструмент, який дозволяє зловмисникам контролювати скомпрометовані системи та виконувати різні дії, такі як: виконання команд, завантаження та завантаження файлів, а також перехід до інших систем.

CrackMapExec – це інструмент тестування на проникнення, який дозволяє зловмисникам перевіряти безпеку середовищ Active Directory, виконуючи різні атаки, такі як «розпилення» пароля, передача хешу та атаки Golden Ticket.

Nmap – це популярний інструмент відображення мережі та сканування портів, який можна використовувати для визначення відкритих портів і служб у системах у мережі. Його можна використовувати для прослуховування мережі, щоб зібрати інформацію про середовище Active Directory та виявити потенційні вразливості.

Metasploit – це фреймворк для тестування на проникнення, який включає низку інструментів для використання вразливостей у системах. Він містить модулі для атак на середовища Active Directory, такі як атака SMB relay, яка дозволяє зловмисникам перехоплювати та ретранслювати запити автентифікації SMB, щоб отримати доступ до системи жертви.

Responder – це інструмент, який можна використовувати для отримання облікових даних із систем у мережі. Він працює шляхом підробки мережевих служб і захоплення облікових даних, надісланих системами, які намагаються автентифікуватися за допомогою цих служб. Це можна використовувати для збору облікових даних для облікових записів Active Directory.

PowerUp – це сценарій PowerShell, який використовується для підвищення привілеїв у середовищах Windows. Він містить модулі для виявлення неправильно налаштованих ACL, пошуку шляхів обслуговування та виявлення інших уразливостей, які можна використати для отримання вищих привілеїв у Active Directory.

LaZagne – інструмент відновлення пароля, який можна використовувати для вилучення паролів, що зберігаються в системі. Він містить модулі для відновлення паролів, що зберігаються в різних програмах і службах, у тому числі тих, що використовуються Active Directory, наприклад у файлі NTDS.dit [12], [13].

Наслідки кібератак на Active Directory можуть бути серйозними. Успішна атака може призвести до витоку даних, крадіжки конфіденційної інформації та збоїв у роботі служби. Щоб пом'якшити наслідки кібератак на Active Directory, організації повинні мати плани реагування на інциденти, у яких описано кроки, які необхідно вжити в разі атаки. Також необхідно проводити регулярні перевірки безпеки та оцінки уразливостей, щоб виявити потенційні недоліки в інфраструктурі AD.

Профілактичні заходи включають впровадження політики надійних паролів, багатофакторну автентифікацію та контроль доступу з найменшими привілеями. Багатофакторна автентифікація (MFA) може допомогти захистити систему від крадіжки облікових даних, яка є поширеним вектором атак на Active Directory. Вимагаючи другий фактор, наприклад мобільний пристрій або біометричну автентифікацію, на додаток до пароля, MFA може значно збільшити складність компрометації облікових даних користувача. Для контролю доступу з найменшими

привілеями необхідно запровадити керування привілейованим доступом (PAM). Також PAM можна використовувати для обмеження доступу до адміністративних облікових записів і моніторингу активності в цих облікових записах. Обмеживши доступ до привілейованих облікових записів, організації можуть зменшити ризик того, що ці облікові записи будуть скомпрометовані та використані для здійснення атак на Active Directory. Крім того, організації повинні регулярно виправляти та оновлювати свою інфраструктуру AD для усунення будь-яких відомих уразливостей. Також необхідно проводити регулярні тренінги з безпеки для співробітників, щоб ознайомити їх з ризиками кібератак та як їх уникнути.

Оновлення програмного забезпечення та виправлень безпеки має вагоме значення для пом'якшення атак Active Directory. Зловмисники часто використовують відомі вразливості в застарілому програмному забезпеченні чи системах, щоб отримати доступ до інфраструктури організації. Регулярно оновлюючи програмне забезпечення та виправлення безпеки, організації можуть закрити ці вразливості та запобігти використання їх зловмисниками.

Можливості виявлення є важливими для ідентифікації та реагування на кібератаки на Active Directory. Організації повинні запроваджувати інструменти та методи моніторингу та виявлення підозрілої активності в інфраструктурі AD, наприклад аналіз журналів і виявлення аномалій. Аудит дозволяє організаціям відстежувати зміни, внесені в об'єкти Active Directory, такі як облікові записи користувачів, членство в групах і GPO. Також потрібно регулярно проводити тестування на проникнення, щоб виявити потенційні недоліки в інфраструктурі AD.

Плани реагування на інциденти мають вирішальне значення для мінімізації збитків, спричинених кібератаками на Active Directory. Організації повинні мати чітко визначені плани реагування на інциденти, які окреслюють кроки, яких необхідно вжити у випадку атаки. Ці плани повинні включати процедури стримування атаки, дослідження масштабів атаки та відновлення нормальної роботи [14], [15].

Висновки

Аналіз кібератак на Active Directory ОС Windows Server має вирішальне значення для організацій в плані підвищення рівня безпеки та захисту IT-інфраструктури від зловмисників. Кібератаки на Active Directory можуть мати серйозні наслідки, і організації повинні вжити належних заходів для пом'якшення цих ризиків. Першим кроком до зменшення ризиків атак на AD є розуміння природи цих атак і методів, які використовують зловмисники. Проводячи ретельний аналіз атак, які були здійснені на систему, організації можуть ідентифікувати загальні вразливості та шаблони поведінки зловмисників, що дозволяє їм вживати профілактичних заходів для запобігання майбутнім атакам. Крім того, адміністраторам безпеки організації важливо знати про інструменти, які можуть використовувати зловмисники при проведенні атак. Це дасть можливість значно знизити ризик їх успішної реалізації. Одним із ефективних методів захисту від атак на AD є впровадження багатофакторної автентифікації (MFA) для всіх облікових записів користувачів. MFA додає до AD додатковий рівень безпеки, вимагаючи від користувачів надання двох або більше форм автентифікації для доступу до ресурсів. Це може допомогти запобігти несанкціонованому доступу до AD і зменшити ризик викрадення облікових даних. Інший важливий аспект безпеки AD – це гарантія того, що всі системи та програмне забезпечення постійно оновлюються з останніми виправленнями безпеки. Багато атак на AD здійснюються з використанням відомих уразливостей у застарілому програмному забезпеченні, але, підтримуючи системи та програмне забезпечення в актуальному стані, організації можуть зменшити ризик реалізації цих атак. Організації також повинні регулярно відстежувати діяльність AD на наявність ознак підозрілої поведінки, як-от незвичайні спроби входу, невдалі спроби автентифікації або зміни дозволів користувача. Це може допомогти виявити та запобігти атакам до того, як вони завдадуть значної шкоди системі та організації в цілому. Крім того, важливо переконатися, що всі співробітники регулярно проходять навчання з питань безпеки, щоб допомогти їм розпізнавати та уникати атак соціальної інженерії, наприклад, таких як фішинг. Розповідаючи співробітникам про ризики, пов'язані з атаками на AD, і надаючи їм інструменти та знання для виявлення підозрілої поведінки та повідомлення про неї, організації можуть зменшити ризик успішних атак. Хоч атаки AD становлять значну загрозу для IT-інфраструктури організацій, існують методи та засоби захисту, які організації можуть вжити, щоб зменшити ці ризики. Розуміючи природу цих атак і застосовуючи належні заходи безпеки, організації можуть зменшити ризик стати мішенню кіберзлочинців і забезпечити безпеку та цілісність своєї IT-інфраструктури.

Список використаної літератури

1. Kotlaba Lukas, Buchovecka Simona, Lorencz Robert. Active Directory Kerberoasting Attack: Monitoring and Detection Techniques. In *ICISSP*. 2020 p. 432-439. https://doi.org/10.5220/0008955004320439

2. Muthuraj S., Sethumadhavan M., Amritha P. P., Santhya, R. Detection and prevention of attacks on active directory using SIEM. In *Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2020, Volume 2.* Springer Singapore, 2021. p. 533-541. https://doi.org/10.1007/978-981-15-7062-9_53

3. Mokhtar Basem Ibrahim, Jurcut Anca D., ElSayed Mahmoud Said, Azer Marianne A. Active Directory Attacks – Steps, Types, and Signatures. *Electronics*, 2022, 11(16): 2629. https://doi.org/10.3390/electronics11162629

4. Nebbione Giuseppe, Calzarossa Maria Carla. A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments. *IEEE Access*, 2023, 11: 15119-15130. https://doi.org/10.1109/ACCESS.2023.3244490

5. Clark Charlie. Analysis of a new AD vulnerability. *Network Security*, *2022*, 2022.12. https://doi.org/10.12968/S1353-4858(22)70069-4

6. Oni Bamidele, Kpelafiya Aboubakar. Windows Active Directory vs. Linux Directory Services, 2023.

7. Ільєнко А.В., Ільєнко С., Куліш Т. Перспективні методи захисту операційної системи Windows. Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка», 2020, 4(8). С. 124-134.

8. Струков В. М., Гуділін, В. В. Захист від атак підвищення привілеїв в корпоративних інформаційних системах. Протидія кіберзлочинності та торгівлі людьми: зб. матеріалів Міжнар. наук.-практ. конф.(м. Харків, 18 трав. 2021 р.). Харків: ХНУВС, 2021. С. 79-82.

9. Юкальчук, А. І., Загоруйко, Л. В., & Мартьянова, Т. А. Моделювання apt-атак, що експлуатують вразливість Zerologon. *Прикладні аспекти сучасних міждисциплінарних досліджень*, 2022. С. 231-234.

10. Philip Robinson. Top 10 Active Directory Attack Methods. URL: https://www.lepide.com/blog/top-10-active-directory-attack-methods/

11. Jason Morano. The anatomy of Active Directory attacks. URL: https://blog.quest.com/the-anatomy-of-active-directory-attacks/

12. Carlos Polop. Hack Tricks. Active Directory Methodology. URL: https://book.hacktricks.xyz/windows-hardening/active-directory-methodology

13. Darren Mar-Elia Attacking Active Directory: Tools and Techniques for Using your AD Against You. URL: https://www.semperis.com/blog/tools-attacking-active-directory/

14. Microsoft. Windows Server. Active Directory Domain Services. Security principals. URL: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-principals

15. Active Directory Security. URL: https://www.quest.com/solutions/active-directory/active-directory-security.aspx

References

1. Kotlaba, L., Buchovecká, S., & Lórencz, R. (2020). Active Directory Kerberoasting Attack: Monitoring and Detection Techniques. In ICISSP (pp. 432-439). https://doi.org/10.5220/0008955004320439

2. Muthuraj, S., Sethumadhavan, M., Amritha, P. P., & Santhya, R. (2021). Detection and prevention of attacks on active directory using SIEM. In Information and Communication Technology for Intelligent Systems: Proceedings of ICTIS 2020, Volume 2 (pp. 533-541). Springer Singapore. https://doi.org/10.1007/978-981-15-7062-9_53

3. Mokhtar, B. I., Jurcut, A. D., ElSayed, M. S., & Azer, M. A. (2022). Active Directory Attacks–Steps, Types, and Signatures. Electronics, 11(16), 2629. https://doi.org/10.3390/electronics11162629

4. Nebbione, G., & Calzarossa, M. C. (2023). A Methodological Framework for AI-Assisted Security Assessments of Active Directory Environments. IEEE Access, 11, 15119-15130. https://doi.org/10.1109/ACCESS.2023.3244490

5. Clark, C. (2022). Analysis of a new AD vulnerability. Network Security, 2022(12). https://doi.org/10.12968/S1353-4858(22)70069-4

6. Oni, B., & Kpelafiya, A. (2023) Windows Active Directory vs. Linux Directory Services, 2023.

7. Ilyenko, A., Ilyenko, S., & Kulish, T. (2020). Promising methods of protecting the Windows operating system. Electronic professional scientific publication "Cybersecurity: education, science, technology", 4(8), 124-134. https://doi.org/10.28925/2663-4023.2020.8.124134. [in Ukrainian].

8. Strukov, V. M., & Gudilin, V. V. (2021). Protection against privilege escalation attacks in corporate information systems. Combating cybercrime and human trafficking: coll. materials of the International science and practice conference (Kharkov, May 18, 2021). – Kharkiv: KhNUVS, 2021. – P. 79-82. [in Ukrainian].

9. Yukalchuk, A. I., Zagoruyko, L. V., & Martyanova, T. A. (2022). Simulating apt-attacks exploiting the Zerologon vulnerability. Applied aspects of modern interdisciplinary research, 231-234. [in Ukrainian].

10. Philip Robinson. (2022). Top 10 Active Directory Attack Methods. Retrieved from: https://www.lepide.com/blog/top-10-active-directory-attack-methods/

11. Jason Morano. (2022). The anatomy of Active Directory attacks. Retrieved from: https://blog.quest.com/the-anatomy-of-active-directory-attacks/

12. Carlos Polop. Hack Tricks. Active Directory Methodology. Retrieved from: https://book.hacktricks.xyz/windows-hardening/active-directory-methodology

13. Darren Mar-Elia. (2017). Attacking Active Directory: Tools and Techniques for Using your AD Against You. Retrieved from: https://www.semperis.com/blog/tools-attacking-active-directory/

14. Microsoft. Windows Server. Active Directory Domain Services. (2022). Security principals. Retrieved from: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/manage/understand-security-principals

15. Active Directory Security. Retrieved from: https://www.quest.com/solutions/active-directory/active-directory-security.aspx