АНАЛІЗ МЕТОДІВ ЗАХИСТУ ВІД ЗАГРОЗИ CVE-2020-1472

Сєвєрінов О.В., Федоров І.А.
Харківський національний університет радіоелектроніки, Харків, Україна

Використання служби каталогів Active Directory (AD) має вирішальне значення для безпеки інформаційних систем багатьох підприємств. Можливі атаки на вразливості AD можуть мати серйозні наслідки для безпеки організації [1].

Одна з таких вразливостей - CVE-2020-1472, також відома як Zerologon, дозволяє зловмиснику зламати механізм автентифікації в службі AD [2]. Тому актуальним напрямом є розгляд методів захисту від атак через вразливість CVE-2020-1472.

Метою доповіді є аналіз методів захисту від вразливості CVE-2020-1472, які допоможуть знизити ризик зламу контролера домену Active Directory.

Проведений аналіз показав, що одним з методів захисту є використання надійних паролів, чітка політика безпеки стосовно паролів в організації. Другим засобом є використання багатофакторних методів автентифікації для підвищення рівня захисту. Необхідно також своєчасно встановлювати патчі Microsoft для оновлення безпеки.

Одним з основних методів захисту є застосування систем виявлення вторгнень (IDS) для протидії та повідомлення про системні атаки [3, 4]. Необхідно використовувати рішення для моніторингу подій, які дозволяють відстежувати й аналізувати системні журнали, щоб своєчасно виявляти незвичні події та підозрілі дії. Детектори вторгнень забезпечать захист від відомих атак, а також дозволять виявляти аномалії, які можуть бути пов'язані з новими атаками, про які можуть знати лише експерти з безпеки.

Регулярні перевірки безпеки в інформаційній системі організації дозволить виявити потенційні слабкі місця в системі захисту.

Таким чином, використання інструментів моніторингу подій і детекторів вторгнень може допомогти виявити атаки на контролер домену та зменшити ризики. Однак для ефективного використання цих інструментів необхідні правильні налаштування та належна підтримка експертів інформаційної безпеки.

Список літератури

1. Сєвєрінов О. В., Хрєнов А. Г. Аналіз сучасних систем виявлення вторгнень //Системи обробки інформації. – 2014. – №. 6. – С. 122-124.

2. Netlogon Elevation of Privilege Vulnerability CVE-2020-1472 [Електронний ресурс] – Режим доступу: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-1472.

3. Intrusion Detection System (IDS) [Електронний ресурс] – Режим доступу: https://www.geeksforgeeks.org/intrusion-detection-system-ids.

4. Федоров І.А., Сєвєрінов О.В. Виявлення загрози CVE-2020-1472 за допомогою IDS/IPS SNORT, НТУ «ХПІ», 2022.