УДК 004.056
Б. Калиниченко, І. Грод
Тернопільський національний технічний університет імені Івана Пулюя

ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ МЕРЕЖІ ОФІСУ "ZoomSupport" ТА МЕТОДІВ ЇХ УСУНЕННЯ

UDC 004.056
B. Kalynychenko, I. Grod
(Ternopil Ivan Puluj's National Technical University, Ukraine)

RESEARCH ON THE VULNERABILITIES OF THE "ZoomSupport" OFFICE NETWORK AND THE METHODS OF THEIR REMOVAL

Корпоративна мережа являє собою складну структуру, в якій об'єднані різні сервіси, необхідні для функціонування компанії. Ця структура постійно змінюється - з'являються нові елементи, змінюється конфігурація існуючих. У міру зростання системи забезпечення інформаційної безпеки і захист критично важливих для бізнесу ресурсів стають все більш складним завданням.

Для того щоб виявити недоліки захисту різних компонентів і визначити потенційні вектори атак на інформаційні ресурси, проводиться аналіз захищеності. Ефективний спосіб аналізу - тестування на проникнення, в ході якого моделюється реальна атака зловмисників. Такий підхід дозволяє об'єктивно оцінити рівень захищеності корпоративної інфраструктури і зрозуміти, чи можуть протистояти атакам застосовувані в компанії засоби захисту.

Бездротові мережі є потенційним вектором проникнення у внутрішню інфраструктуру компанії. Зловмиснику досить встановити на ноутбук загальнодоступне ПО для атак на бездротові мережі і придбати недорогий модем, який може працювати в режимі моніторингу трафіку.

На мережевому периметрі компаній основна проблема безпеки полягає в недостатньому захисті веб-додатків. Слід регулярно проводити аналіз захищеності веб-додатків, при цьому найбільш ефективним методом перевірки є метод білого ящика, що має на увазі аналіз вихідного коду. Як превентивний захід рекомендується використовувати міжмережевий екран рівня додатків (web application firewall) для запобігання експлуатації вразливостей, які можуть з'являтися при внесенні змін до коду або додаванні нових функцій.

Тільки своєчасне виявлення спроб атаки дозволить запобігти її до того, як зловмисник завдасть істотної шкоди компанії, тому слід застосовувати технічні рішення, спрямовані на виявлення підозрілої активності. Для ефективного реагування на інциденти інформаційної безпеки рекомендується використовувати системи управління, аналізу і моніторингу подій безпеки (SIEM-системи), які дозволяють виявляти зловмисну активність в мережі, спроби злому інфраструктури, присутність зловмисника і допомагають приймати оперативні заходи по нейтралізації загроз.

Література:

1. Swanson M., Nadya B., Sabato J., Hash J., Graffo L. Security Metrics Guide for Information Technology Systems. National Institute of Standards and Technology Special Publication, No. 800–55, 2003.
2. Гайворонський М.В., Новіков О. М. Безпека інформаційно-комунікаційних систем. — К.: Видавнича група BHV, 2009. — 608с