УДК 621.396:004.056

АНАЛІЗ ПОТЕНЦІЙНИХ РИЗИКІВ КОМПЛЕКСНОЇ СИСТЕМИ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

Даниленко М.С., Соколюк В.А., Клушин Д.Д., Безрук В.М.
e-mail: mykyta.danylenko1@nure.ua, vadym.sokoliuk@nure.ua, daniil.klushyn@nure.ua, valerii.bezruk@nure.ua
Харківський національний університет радіоелектроніки, каф. IMI
м. Харків, Україна

The modern technological base provides a fairly wide range of software and hardware tools to counteract malicious influences that pose a potential threat to network infrastructure and data in file storage. However, based on the existing world experience in protecting against cyber threats, it can be stated that only a multi-level complex system can provide a significant level of security. On the other hand, any complex system has potential vulnerabilities that can be used by an attacker to successfully implement an attack. Therefore, to maintain network information security, it is necessary not only to deploy a protection system, but also to audit its possible vulnerabilities and localize each of them.

Переважна більшість сучасних комплексних систем протидії кіберзагрозам містить у собі такі компоненти, як:

- засоби захисту мережевого периметру (зазвичай це міжмережевий екран або NGFW);
- платформа контролю процесів, які мають перебіг усередині мережі (IDS/IPS-системи);
- програмний засіб захисту на рівні кінцевого вузла (локальні екземпляри IDS/IPS, антивірусне ПЗ тощо);
- засоби логування.

При цьому, якщо така мережа не є об’єктом інтересу з боку потенційних зловмисників, теоретично її можна вважати захищеною.

Розглянемо потенційні сценарії реалізації атак з боку зловмисників за умов, що мережа вважається захищеною.

По-перше, атаку може бути реалізовано з середини мережі, за участю персоналу, як наслідок їхніх некваліфікованих (або цілеспрямованих зловмисних) дій. Передумовами для цього є:

1. Можливість фізичного доступу співробітників до програмно-технічних засобів підтримки та контролю захищеності мережі, що дає змогу впливу на регламент їх роботи, у т.ч. повної деактивації.
2. Можливість локального мережевого доступу до програмно-технічних засобів підтримки та контролю захищеності мережі особами, які не мають відповідної кваліфікації та привілеїв; це дає змогу впливу на регламент їх роботи, у т.ч. відключення.
3. Відсутність вимог щодо використання у системі виключно довірених змінних носіїв (наприклад, flash) з блокуванням пристроїв, які не

внесено у перелік довірених. Це дає можливість як крадіжки даних, так і розміщення на клієнтських терміналах зловмисних модулів в обхід багатьох компонент захисту

4. Можливість неконтрольованого підключення та використання співробітниками точок доступу WiFi (т.з. «чужинців»), що створює умови для проведення атак Evil Twin та зводить нанівець ефективність усіх засобів протидії кіберзагрозам.

Разом з тим, на рівні мережевого периметру можна виокремити ряд загроз, більшість з яких на базі поширеного технологічного базису не виявляються, або ігноруються адміністраторами безпеки. Це, зокрема:

1. Неявний та/або прихований зміст. У першому випадку мова може йти про зловмисний контент, наприклад, глибокого рівня вкладеності. Для його виявлення може бути використано механізми DPI (deep packet inspection). Водночас, глибокого аналізу пакетів недостатньо, коли зловмисний контент вимагає для активації певних умов, або коли мова йде про загрози на кшталт ZeroT та подібні. Для їх виявлення необхідно додатково застосовувати засоби стегоаналізу, а також моделювати ізольоване «робоче» середовище – пісочницю (sandbox) для безпечного запуску підозрілих файлів.

2. Новітні загрози. У загальному випадку це стосується зловмисних механізмів, сигнатури або характерні ознаки впливу яких відсутні у базах відповідного ПЗ. Такі загрози є «прозорими» для NGFW, IDS/IPS та антивірусних засобів. Виявити їх вплив досить складно і, зазвичай, це можливо лише після самого вторгнення, шляхом аналізу лог-файлів та виявлення аномалій технічного регламенту роботи мережі, її окремих вузлів та служб.

Окрім зазначеного, існує певний ризик інфільтрації зловмисних модулів через веб-інфраструктуру підприємства, як наслідок експлуатації зловмисником уразливостей CMS, недоліків налаштувань модулів безпеки на рівні сайту, а також можливість неконтрольованого розміщення відвідувачами зовнішніх посилань (блог, коментарі тощо), які можуть містити, у т.ч., посилання на потенційно небезпечні ресурси.

Список використаних джерел:

1. Deny Write Access to Unprotected Removable Drives in Windows 11. URL: https://geekrewind.com/how-to-deny-write-access-to-removable-drives-not-protected-by-bitlocker-in-windows-11/?ysclid=m7rg33wuah909468332/ (дата звернення: 07.11.2024).

2. Research on unsecured Wi-Fi networks across the world. URL: https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/ (дата звернення: 07.11.2024).

3. Oops, they did it again: APT Targets with ZeroT and PlugX | Proofpoint US. URL: https://www.proofpoint.com/us/threat-insight/post/APT-targets-zerot-plugx (дата звернення: 09.11.2024).