

УДК 004.75

ТЕЛЕНИК А.М.,
ЖАРИКОВ Е.В.

БІЗНЕС-АНАЛІЗ БЕЗПЕКИ КОМП'ЮТЕРНИХ МЕРЕЖ

Сучасні загрози підприємствам з боку кіберзлочинців потребують покращення технологій і методів підвищення безпеки. Запропоновано систематизувати загрози для комп'ютерних мереж спираючись на принципи опису структури комп'ютерної мережі згідно рівнів еталонної моделі OSI. Виконано огляд та класифікацію загроз роботі комп'ютерних мереж відповідно до рівнів моделі OSI, проаналізовано вразливості на кожному рівні відповідно до сучасних методів бізнес-аналізу. З використанням таблиці вразливості виявлено особливий рівень загроз мережевому рівню через комбінацію небезпечних наслідків та широкого спектру вразливостей мережі.

КЛЮЧОВІ СЛОВА: комп'ютерна мережа; рівень моделі OSI; загроза рівню; бізнес-аналіз; кібератака; аналіз загроз

BUSINESS ANALYSIS OF COMPUTER NETWORK SECURITY

Today's threats to businesses from cybercriminals require improved security technologies and techniques. It is proposed to systematize threats to computer networks based on the principles of describing the structure of the computer network according to the levels of the OSI reference model. An overview and classification of threats to computer networks according to the levels of the OSI model, vulnerabilities at each level are analyzed in accordance with modern methods of business analysis. Using the vulnerability table, a special level of threats to the network layer was identified due to a combination of dangerous consequences and a wide range of network vulnerabilities.

KEYWORDS: computer network; OSI model level; level threat; business analysis; cyberattack; threat analysis

1. Вступ

Цифрова трансформація ставить інформаційні технології в основу сучасних продуктів, послуг та операцій. При цьому відбувається постійне зростання обсягів використання і впровадження комп'ютерних мереж у всіх сферах життя. За останні тридцять років використання комп'ютерних мереж для підвищення швидкості та поліпшення координації роботи стало звичним явищем у промисловості, на підприємствах, в учбових закладах, урядових установах, при створенні військових автоматизованих систем управління та, зрештою, у повсякденному побуті широких верств населення. Найвищим та найбільш відомим проявом цього масового поширення комп'ютерних мереж є охоплення більшості території планети глобальною мережею Internet [1].

Разом з тим за ці ж тридцять років відбулося багатократне зростання кількості

та якості різноманітних загроз комп'ютерним мережам.

У 2021 році кіберзлочинність стала більш складною та поширеною. Злочинці все частіше атакують критично важливу інфраструктуру — охорону здоров'я, фінансові установи, енергетичний сектор, що завдає значної шкоди споживачам. Аналіз масштабів та нових тенденцій розповсюдження кібератак показав, що найпоширеніші кібератаки здійснюються із застосуванням програм-вимагачів (Ransomware), шкідливої електронної пошти (Phishing attacks), шкідливого програмного забезпечення (Malware). Такий висновок зроблений у звіті Microsoft Digital Defense Report 2021 (MDDR 2021) [2]. Спираючись на понад 24 трильйони щоденних сигналів безпеки в хмарі Microsoft, кінцевих точках та інтелектуальних периферіях, звіт MDDR 2021 доповнює минулорічний аналогічний звіт і

містить внески від понад 8500 експертів з безпеки з 77 країн [2].

Усі ці чинники змушують користувачів, як корпоративних так і приватних, враховувати у своїй діяльності ці дві тенденції – розширення використання комп'ютерних мереж та збільшення різноманітних кіберзагроз. Отже, технології та інструменти захисту від кібератак мають забезпечувати максимально можливий і разом з тим адекватний наявним засобам рівень захисту комп'ютерних мереж.

2. Класифікація загроз з використанням моделі OSI

Розв'язання поставленої задачі неможливе без детального опису та оцінки можливих типів та видів загроз, які можуть виникнути. Найбільш логічним способом класифікації загроз, що можуть виникнути, є розділення їх за рівнями еталонної моделі OSI (*Open Systems Interconnection*) – універсального та загальноприйнятого на даний момент принципу опису структури комп'ютерної мережі. Цей принцип для класифікації загроз обрано через те, що його застосування дозволяє визначити, який саме компонент комп'ютерної мережі перебуває під загрозою.

Фізичний рівень моделі OSI є базовим рівнем фізичного обладнання мереж, що забезпечують передачу потоків даних. У першу чергу це фізичні порти, кабельні та радіохвильові лінії зв'язку [3]. Характер обладнання цього рівня зумовлює і природу загроз, які полягають у використанні природних для цього рівня вразливостей мережі, таких як неадекватний фізичний захист обладнання, можливість передачі даних у незашифрованому вигляді у середовищі передачі, вразливість обладнання до впливу електромагнітних випромінювань. Ці фактори роблять актуальними загрози перехоплення, пошкодження або запису трафіку ліній зв'язку як шляхом фізичного підключення до лінії зв'язку, так і впливу на сигнал засобами його подавлення та перехоплення.

На каналному рівні відбувається фізична адресація абонентів мережі, тож незахищеною є передача даних у відкритому вигляді та відсутність надійних механізмів

аутентифікації чи електронно-цифрового підпису повідомлень, що передаються. Це зумовлює характер загроз, які перш за все полягають у можливості підміни зловмисниками пакетів, як при отриманні повідомлення замаскувавшись під адресата, так і при відправленні їх, маскуючись під відправника.

Третім рівнем моделі є мережевий рівень – рівень маршрутизації та логічної адресації абонентів мережі. Він забезпечує взаємодію процесів, що розташовані на вищих рівнях (Host layers), з нижчими рівнями (Media layers) моделі. Це відображає і характер загроз, які можуть виникати на цьому рівні – це і фізичні (можливість доступу сторонніх осіб до обладнання, перш за все до маршрутизаторів), і логічні (можливість віддаленого управління та впливу на комутатори та маршрутизатори). Кіберзагрози на цьому рівні – це відключення або вивід з ладу маршрутизаторів, дезорганізація та дестабілізація роботи мережі шляхом відключення від мережі магістральних комутаторів, інфільтрація до мережі сторонніх структурних компонентів з навіязуванням хибних маршрутів передачі даних.

На транспортному рівні відбувається сегментація даних на блоки та пакети і їх передача між абонентами мережі [3]. Вразливостями на цьому рівні є можливість підміни повідомлень, помилки сегментації, а також ненадійність з'єднання. На використанні цих вразливостей ґрунтуються типові атаки на протоколи транспортного рівня: підміна UDP-пакетів, перевантаження мережі «важкими» сегментами, а також та так звані «циклічні» атаки з заміною номера порту отримувача на номер порту відправника.

Три найвищих рівня моделі OSI – сеансовий, презентаційний та прикладний, з точки зору безпеки зазвичай об'єднуються через спільний характер та арсенал загроз мережі на цих рівнях. Треба акцентувати увагу на прикладний рівень, тому що саме на ньому зазвичай розташовується ціль зловмисників – персональні дані та сервіси користувачів мережі. До того ж, величезне різноманіття протоколів, що використовуються на цих рівнях, надає

зловмисникам великий вибір методів впливу на мережу. Завдяки цьому, на цих рівнях фізичні загрози остаточно змінюються програмними. Найбільш розповсюдженими є Peer-to-Peer (P2P) атаки, що базуються на встановленні неавторизованого P2P-з'єднання з комп'ютером-ціллю, атаки з використанням надвеликих заголовків HTTP-пакетів та DDoS-атаки (Distributed Denial-of-Oervice).

Таким чином, загрози для комп'ютерних мереж можна описати та систематизувати, орієнтуючись на їх класифікацію за рівнем еталонної моделі.

По-перше, загрози відповідають умовам та технічним особливостям рівнів, на які вони націлені. По-друге, загрози прив'язані до конкретних вразливостей мереж та мережевого обладнання. По-третє, загрози поступово змінюють свій характер з підвищенням рівня від фізичних методів на першому рівні до виключно програмних на прикладному. Така систематизація має практичне втілення.

3. Практичне використання

Актуальною є завдання розробки комплексу засобів та методів захисту комп'ютерних мереж від широкого спектру

кібератак. Продемонстрований характер загроз, які мають як фізичну, так і програмну природу, зумовлює поєднання у розроблюваній технології як апаратних, так і програмних методів захисту.

Розроблення комплексу методів і засобів у складі технології захисту потребує проведення бізнес-аналізу загроз з метою визначення вимог, яким він повинен відповідати. Аналіз загроз визначає загрози та визначає найбільш економічно ефективну політику зменшення ризику для конкретної архітектури, функціональності та конфігурації системи. Аналіз загроз має виконуватися як постійний процес протягом усього життєвого циклу системи розробки, інтеграції, запитів на зміни та управління проблемами [4].

Одним із методів збору даних про безпеку та конфіденційність системи є перелік загроз та активів ІТ інфраструктури на так званому робочому аркуші. Розроблюваний робочий аркуш аналізу загроз може бути розповсюджений серед користувачів, адміністрації та керівництва навіть як частина процесу аналізу вимог, щоб зібрати інформацію про потенційні проблеми безпеки [5]. Приклад такого аркуша представлено у таблиці.

Таблиця – Робочий аркуш загроз мережі. Літерами показаний ефект від атаки: А – руйнівний, Б – вивід системи з ладу, В – порушення роботи, Г – відсутній; Вірогідність: А – висока, Б – вірогідність існує, В – мала вірогідність, Г – атака практично неможлива.

Ефект/вірогідність	Обладнання користувача	Сервери	Мережеві пристрої	Програмне забезпечення	Сервіси	Дані
Несанкціонований доступ	Б/А	Б/Б	В/Б	А/Б	Б/В	А/Б
Несанкціоноване використання	Б/В	Б/Б	В/В	А/Б	Б/В	А/Б
Denial of Service	Б/Б	Б/Б	Б/Б	Б/Б	Б/Б	Г/Г
Спуфінг	А/Г	Б/Г	Б/Г	А/Б	В/В	А/Б
Викривлення даних	А/В	Б/В	В/В	А/Б	Г/Г	А/Б
Зараження вірусом	Б/Б	Б/Б	Б/Б	Б/Б	Б/В	Г/Г
Фізичне ушкодження	А/Г	Б/В	В/В	Г/Г	Г/Г	Г/Г

З наведеного прикладу випливає, що найбільш важкі наслідки матиме атака на мережевий рівень, саме на ньому найбільший ризик руйнівної атаки. Більш того, в результаті атаки на мережевому рівні існує

загроза для обладнання та програмного забезпечення. Усі ці фактори і дозволяють зробити припущення про першочергову важливість захисту саме мережевого рівня.

Висновки

У статті систематизовано загрози для комп'ютерних мереж згідно рівнів еталонної моделі OSI. Проведено попередній бізнес-аналіз загроз безпеці комп'ютерних мереж, окреслено можливі загрози у залежності від рівня еталонної моделі OSI та зроблено висновки про характер та сутність загроз. Побудовано таблицю вразливостей мережі та зроблено висновки про найбільш вразливий рівень моделі OSI до атак.

Список літератури

1. Дж. Скотт Хогдал Анализ и диагностика компьютерных сетей, — Москва: Лори, 2007. 352 с.
2. Microsoft Digital Defense Report [Електронний ресурс] – Режим доступу до ресурсу: <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report> (дата звернення: 17.11.2021).
3. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. 4-е издание. — Санкт-Петербург, Питер, 2010. 944 с.
4. Business Analysis Body of Knowledge – Toronto, Ontario, Canada, IIBA, 2015. 502 p.
5. Babok v3: бизнес-анализ для управления изменениями [Електронний ресурс] – Режим доступу до ресурсу: <https://analytics.infozone.pro/tag/babok-3/> (дата звернення: 17.11.2021).

УДК 004.75

*АНТОНЕНКО А.А.,
ЖАРИКОВ Е.В.*

ПРАКТИЧНЕ ВИКОРИСТАННЯ ANSIBLE ЯК ІНСТРУМЕНТУ РЕАЛІЗАЦІЇ ПІДХОДУ «ІНФРАСТРУКТУРА ЯК КОД»

У статті розглянуто практичне використання Ansible як інструменту реалізації підходу «Інфраструктура як код» на прикладі розгортання сервісу «Apache2». Розглянуто підходи до опису ІТ інфраструктури та верифікації налагодження сервісу.

КЛЮЧОВІ СЛОВА: Ansible, інфраструктура як код, сервісна ІТ інфраструктура

PRACTICAL ANSIBLE USAGE AS A TOOL FOR IMPLEMENTING THE "INFRASTRUCTURE AS A CODE" APPROACH

This article considers the practical use of Ansible as a tool of the Infrastructure as a code approach on the example of service deployment. Approaches to infrastructure description, testing, and verification of service debugging are considered.

KEYWORDS: Ansible, infrastructure as a code, service IT infrastructure

1. Вступ

У сучасних центрах оброблення даних (ЦОД) широко застосовуються асоби централізованого управління, верифікації та опису конфігурацій об'єктів ІТ-інфраструктури. Одним з інструментів реалізації підходу «Інфраструктура як код» (Infrastructure as code, IaC) є Ansible.. Постійно зростаюча потреба у ефективному управлінні кодом для забезпечення сучасних вимог з боку бізнесу та споживачів змусила велику кількість підприємств переосмислити шаблони розробки.

Основною проблемою внесення змін у код для швидкого процесу доставки до серверів і середовищ виконання є відома проблема сумісності роботи програмістів та системних адміністраторів, які безпосередньо впроваджують розроблені застосунки.

Зазвичай розгортання та запуск застосунків здійснюється за допомогою засобів автоматизації, іншими словами скриптів. При зміні потреб та вимог до впроваджуваної частини інфраструктури зазвичай необхідно зробити відповідні зміни до скриптів, застосувати зміни та перевірити