УДК 004.77
DOI: https://doi.org/10.53920/ITS-2023-2-3

Олександр Іванович ГОЛУБЕНКО,
кандидат технічних наук, доцент,
т. в. о. завідувача кафедри комп'ютерних наук
та інженерії програмного забезпечення,
ЗВО «Міжнародний науково-технічний університет
імені академіка Юрія Бугая»
ORCID ID: 0000-0002-1776-5160
Андрій Вікторович ЛЕМЕШКО,
доктор філософії, доцент,
доцент кафедри комп'ютерної інженерії,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0000-0001-8003-3168
Олександр Сергійович ЦВИК,
аспірант кафедри комп'ютерної інженерії,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0000-0001-7786-1712
Юрій Валентинович МІШКУР,
аспірант кафедри комп'ютерної інженерії,
Державний університет інформаційно-комунікаційних технологій
ORCID ID: 0009-0004-6807-6914

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЛОКАЛЬНИХ МЕРЕЖАХ ЗА ДОПОМОГОЮ КОНТРОЛЮ ТРАФІКУ

Розглянуто основи контролю трафіку й можливості збільшення потужності моніторингу мережі. Проаналізовано способи завдання шкоди мережі й створення інцидентів безпеки. Визначено основні аспекти безпеки, що повинні бути включені в моніторинг за мережею. Визначено, як контроль трафіку працює без додаткових сил моніторингу й основні можливості з новими технологіями. Був проведений аналіз основної мережі з використанням контролю трафіку й з вдосконаленням за допомогою додаткових засобів, що сприяло збільшенню можливостей моніторингу мережі й покращення контролю трафіку. Були розглянуті основні додаткові заходи, щодо використання адміністративних та технічні аспектів, що можливо використовувати в мережі задля безпеки. Розглянуто основні принципи контролю трафіку завдяки Network Traffic Analysis (NTA) й Network Behavior Analysis (NBA), завдяки чого

з'являється можливість виявлення шкідливого програмного забезпечення (ПЗ) й аномалій в мережі. Проаналізований спосіб моніторингу мережі за допомогою Data Leak Prevention (DLP) й приведені основні привелегії його використання та недоліки. Проаналізовані також системи моніторингу логів Security Information and Event Management (SIEM) й Intrusion Detection System (IDS), завдяки яких є можливість аналізувати додатки й периметр мережі для виявлення загроз.

Ключові слова: *контроль трафіку, мережа, моніторинг, інформаційна безпека, програмне забезпечення.*

Oleksandr GOLUBENKO
Candidate of technical sciences, associate professor,
Temporary acting head of the Department
of Computer Science and Software Engineering,
IHE «Academician Yuri Bugay international science
and technical university»
Andrii LEMESHKO
Doctor of Philosophy, Associate Professor,
associate professor of the departmentof computer engineering,
State University ofinformation and communication technologies
Oleksandr TSVYK
graduate student of the Department of Computer Engineering,
State University of information and communication technologies
Yurii MISHKUR
graduate student of the Department of Computer Engineering,
State University of information and communication technologies

ENSURING INFORMATION SECURITY IN LOCAL NETWORKS USING TRAFFIC CONTROL

The basics of traffic control and the possibility of increasing the power of network monitoring are considered. Methods of causing damage to the network and creating security incidents are analyzed. The main security aspects that should be included in network monitoring are defined. Defined how traffic control works without additional monitoring forces and basic capabilities with new technologies. An analysis of the core network using traffic control was performed and enhanced with additional tools, which contributed to increased network monitoring capabilities and improved traffic control. The main additional measures regarding the use of administrative and technical aspects that can be used

in the network for security were considered. The main principles of traffic control through Network Traffic Analysis and Network Behavior Analysis are considered, thanks to which the possibility of detecting malicious software and anomalies in the network appears. The method of network monitoring using Data Leak Prevention (DLP) is analyzed and the main advantages and disadvantages of its use are given. Security Information and Event Management (SIEM) and Intrusion Detection System (IDS) log monitoring systems were also analyzed, thanks to which it is possible to analyze applications and the network perimeter to detect threats.

Keywords: *traffic control, network, monitoring, information security, software.*

Постановка проблеми. Однією з основних проблем інформаційної безпеки (ІБ) є користувачі, які не повністю розуміють «кібер-гігієну» й можуть спровокувати надзвичайну ситуацію з витоком корпоративних даних. Проблемою є й зовнішній вплив на локальну мережу, хакерами чи зловмисниками, які намагаються добратися до даних компанії чи користувачів, та з кожним роком вдосконалюються й випробують різні способи для нанесення шкоди локальній мережі й зменшення супротиву для входу до його ядра – серверу. Тому постійно треба вдосконалювати мережу й основні принципи її безпеки, в тому числі й контроль трафіку.

Традиційна модель контролю трафіку не має переваг перед новими загрозами, що постійно з'являються, й має основну проблему – вона має принцип контролювання периметру мережі, який дозволяє отримувати весь трафік, але не забезпечує безпеку при деяких виняткових ситуаціях. До таких ситуацій відноситься: несанкціонований вхід не з корпоративних пристроїв, підключення флеш-пам'яті до мережевих пристроїв, WEB-сайти з «cryptojacking» або «miner» й передача сек'юрних даних 3-м особам через веб-сайти чи іншим способом. Так для вирішення даних проблеми потрібно використовувати додаткові заходи безпеки й це буде розглянуто в статті.

Аналіз останніх досліджень і публікацій. Більшість компаній, що надають послуги з безпеки мережі, проводять дослідження в яких є можливість визначити основні проблеми мережі на даний час. Також великі інфраструктурні IT компанії, проводять дослідження й надають багато інформації про випадки інцидентів безпеки. Компанія Embroker провела дослідження з кібербезпеки,

яка визначила основні проблеми інформаційної безпеки за останні роки (2020 – 2023), й в 2023 році виділила основні інциденти, які відбулися в мережі й завдали шкоду компаніям. Серед них можна виділити такі, як:

- Порушення регламентів ІБ (знайдено у 100% компаній);
- Підозрілу мережну активність (знайдено у 90% компаній);
- Активність шкідливого програмного забезпечення (знайдено у 68% компаній);
- Спроби експлуатації вразливості у ПЗ (знайдено у 31% компаній);
- Спроби підбору пароля (знайдено у 26% компаній);
- Спроби експлуатації веб-вразливостей (знайдено у 3% компаній);

Завдяки цьому аналізу можемо зробити висновки, як були шляхи завдання шкоди. З цього можемо виділити основу проблеми – недостатній аналіз трафіку й безпеки мережі, й це описано в [1] й вказано, на яких ділянках були основні проблеми.

Мета статті – це дослідження забезпечення інформаційної безпеки в локальних мережах за допомогою контролю трафіку.

Виклад основного матеріалу дослідження. Оскільки на сьогодні дуже важливим елементом є актуальна інформаційна безпека, то відбувається постійно вдосконалення програм й пристроїв, за допомогою яких й забезпечується безпека. Але оновлення відбувається на основі аналізу того, що зловмисниками раніше було розроблено та застосовано з метою не санкціонованого доступу до мережі, зламу мережі через сегменти, які погано захищені. Тому інциденти з безпеки відбуваються щоденно й не можуть бути зупинені. Завдяки застосуванню різних інструментів безпеки – Firewall, VPN, WLAN, контроль трафіку, антивірусів – ми маємо безпечну мережу, й у кожного є свої прошивки, оновлення й нові версії, за допомогою якої ми маємо вдосконаленні засоби захисту, й з кожною новою версією того ж самого Firewall ми й маємо нові спроби злому мережі.

Локальні мережі з кожним роком стають більш технологічними, з'являються нові сервіси та послуги, а разом з ними розвиваються й нові способи загрози інформаційній безпеці. Тому компанії намагаються з кожним разом знайти новий спосіб, як запобігти критичним інцидентам й зробити мережу безпечною. Основний з способів регулювання безпеки є контроль трафіку.

Перш за все розглянемо середовище порушень регламентів ІБ. Можна виділити основні проблеми:

- використання ПЗ для віддаленого доступу;
- використання незахищених протоколів передачі даних;
- використання BitTorrent;
- завантаження з подальшим встановленням потенційно небезпечного стороннього ПЗ;
- встановлення підміненого ПЗ (з прихованим функціоналом);
- застосування протоколів LLMNR, NetBios.

До підозрілої мережної активності можна віднести: приховування трафіку, множинну неуспішну автентифікацію, сканування внутрішньої мережі, спроби підключення до зовнішніх мереж, спроби віддаленого запуску програми, копіювання та передача даних у великих обсягах.

Завдяки вразливості програмного забезпечення зловмисник може використовувати функціонал програми у своїх цілях. У локальній мережі поширені спроби підбору пароля з допомогою методів перебору, це відбувається завдяки «брутфорсу» й може відбуватися як всередині мережі так й поза, завдяки віддаленим серверам. Веб-вразливості можуть бути використані для доступу до веб-сервера та виконання шкідливого коду.

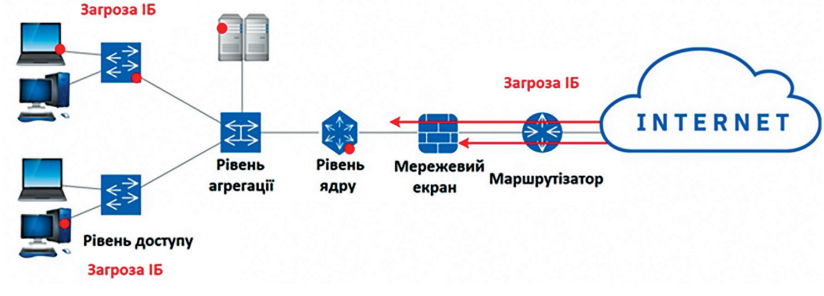

Рис. 1. Вразливі місця локальних мереж

Традиційна модель контролю трафіку на периметрі мережі не справляється з усіма загрозами ІБ з однієї простої причини - вона призначена для контролю периметра, а крім основного шляху, на якому стоїть міжмережевий екран (МЕ), існують обхідні канали отримання доступу до локальної мережі. Такими каналами можуть

бути підключені заражені мобільні пристрої, ноутбуки, флешки та диски. Особливу небезпеку становлять несанкціоновані підключення модемів та Wi-Fi адаптерів до пристроїв локальної мережі. Вони можуть відкрити канали передачі даних, які не контролюються МЕ.

Маючи доступ до всього трафіку в мережі, аналізуючи його та зіставляючи, ми можемо створити поведінковий профіль вузла. У цей профіль входитиме така інформація: які протоколи використовує, з якими сегментами мережі взаємодіє, скільки трафіку передає/отримує тощо. У разі виявлення нетипової поведінки (аномалії) подається сигнал тривоги. Поява нового вузла в мережі не залишиться непоміченою.

Завдяки розподіленій системі моніторингу трафіку локальної мережі є можливість детально провести аналіз поширення загроз ІБ по периметру в пошуку місця їх виникнення. Якщо додати потужності для зберігання трафіку, є можливість зробити аналіз у майбутніх інцидентах і розібратися у минулих. Завдяки цьому легко визначити вузькі місця, неправильну конфігурацію обладнання чи його несправність. Завдяки отриманим результатів є можливість удосконалення мережі й її безпеки.

Для запобігання порушенням регламентів ІБ, підозрілої мережевої активності, використання шкідливого ПЗ та експлуатації вразливості в ПЗ використовуються адміністративні та технічні заходи. Це відбувається за допомогою технічного підрозділу.

Для аналізу трафіку, взятого на периметрі і в самій мережі, на наявність заборонених протоколів і сервісів, використовуються Network Traffic Analysis і Network Behavior Analysis. За допомогою порівняння сигнатур та поведінкового аналізу система NTA/NBA зможе розпізнати роботу шкідливого ПЗ. Завдяки функціональним можливостям роботи з шифрованим трафіком та аналізом протоколів можна виявити аномалії в трафіку. Поведінковий аналіз та машинне навчання системи NTA/NBA дозволить виявити дивну активність у роботі мережі та спроби підбору облікових даних, що породжують велику кількість неуспішних аутентифікацій. Цей факт буде видно у трафіку.

Виявити загрози безпеці мережі та провести аналіз поведінки користувачів можна за допомогою системи Data Leak Prevention, яка використовує збір даних із точок моніторингу локальної мережі та з DLP-агентів, встановлених на мережному та абонентському

устаткуванні. Однак використання DLP-агентів може викликати труднощі, адже є пристрої, на які їх неможливо встановити, й на те є різні причини (відсутній доступ до ОС, немає підтримки з боку ОС, тощо). Існує ризик несанкціонованого підключення до мережі, коли користувачі можуть підключати свої особисті пристрої до мережі. Варто зазначити, що шкідливе програмне забезпечення може обходити моніторинг DLP-агента. Отримуючи трафік з точок моніторингу локальної мережі, система DLP зможе проводити аналіз поведінки всіх пристроїв у мережі незалежно, чи встановлений на них DLP-агент чи ні.

Система Security Information and Event Management збирає, аналізує логи різних додатків і на їх підставі може робити висновки про наявність загроз ІБ: підозрілий трафік та атаки, випадки зараження шкідливим програмним забезпеченням, порушення регламентів ІБ користувачами. Робота системи SIEM із вбудованим модулем NetFlow/sFlow полягає в наступному: трафік з точок моніторингу мережі надходить на модуль NetFlow/sFlow, модуль NetFlow/sFlow аналізує трафік, формує події та відправляє на SIEM, де проводиться аналіз та робиться висновок про наявність загрози ІБ. Таким чином, модуль NetFlow/sFlow збирає мережеву статистику з отриманого трафіку, а застосування його спільно з SIEM дозволяє здійснювати незалежний від інших програм моніторинг мережі на предмет загроз ІБ.

Система Intrusion Detection System призначена для виявлення вторгнень. Серед найпоширеніших видів IDS можна виділити Perimeter Intrusion Detection Systems (PIDS) та Network Intrusion Detection System (NIDS). Система PIDS аналізує трафік, взятий з периметра мережі (даний трафік може бути отриманий як з активного мережного обладнання, так і з моніторингу на мережі). Але не всі загрози ІБ можна виявити на периметрі мережі, вони можуть виникнути всередині мережі та не виходити назовні. Такі загрози найчастіше виникають під час підключення до мережі несанкціонованих пристроїв користувачів, підключення модемів, Wi-Fi адаптерів, зараження локальних пристроїв вірусами. Система NIDS отримує та аналізує трафік з точок моніторингу, розташованих по всій локальній мережі. Використання системи NIDS дозволяє виявити всі описані загрози ІБ.

Висновки та пропозиції. Визначивши основні загрози мережі, з'являється можливість їх нейтралізації й вдосконалення безпеки.

В цій статті були описані основні принципи контролю трафіку і визначені додаткові засоби до моніторингу мережі. Тому такі методи, як NTA/NBA, DLP, системи SIEM й IDS рекомендовано використовувати разом з основним контролем трафіку для запобігання виникнення інцидентів безпеки й для кращого регулювання потоку мережі. Вся система моніторингу, яка вказана вище, допоможе не тільки контролювати трафік, а й робити аналіз мережі з подальшим вдосконаленням мережі й покращенням інформаційно безпеки.

© Голубенко О.І., Лемешко А. І., Цвик О.С., Мішкур Ю.В., 2023

ЛІТЕРАТУРА

1. Ефективна та можлива техніка керування перевантаженнями для High. PerformanceMINs з розподіленою маршрутизацією на основі тегів, Транзакції IEEE у паралельних і розподілених системах, 243.

2. Автономна інженерія трафіку для надійності мережі. IEEE Journal on Selected Areas in Communications, 76.

3. Контроль перевантаження для високошвидкісної дротової мережі: систематичний огляд літератури. Журнал мережевих і комп'ютерних програм, 182.

4. Досягнення в запобіганні перевантаження TCP. 11-й міжнародний симпозіум IEEE з прикладного машинного інтелекту та інформатики, 129.

5. Управління ризиками. Загрози кібербезпеці у 2023 році https://www.embroker.com/blog/top-cybersecurity-threats/.

REFERENCES

1. An Effective and Feasible CongestionManagement Technique for High. PerformanceMINs with Tag-Based Distributed Routing, IEEE Transactions on Parallel and Distributed Systems, 243.

2. Autonomic traffic engineering for network robustness. IEEE Journal on Selected Areas in Communications, 76.

3. Congestion control for highspeed wired network: A systematic literature review. Journal of Network and Computer Applications, 182.

4. Advances in TCP Congestion Prevention. IEEE 11th International Symposium on Applied Machine Intelligence and Informatics, 129.

5. Risk Management Cybersecurity Threats in 2023 https://www.embroker.com/blog/top-cybersecurity-threats/.

СТАТТЯ НАДІЙШЛА ДО РЕДАКЦІЇ 01.12.2023