УДК 004.056.5:338.24-047.36

МОНІТОРИНГ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СЕГМЕНТІВ КОРПОРАТИВНИХ МЕРЕЖ СУЧАСНОГО БІЗНЕСУ

Н. В. Гуленко, Т. М. Яворська

Анотація. У даному дослідженні представлена інформація про важливість забезпечення інформаційної безпеки на сучасних підприємствах. Наведені можливості та головні переваги корпоративних мереж, названі основні загрози корпоративним мережам у сфері інформаційної безпеки. Визначено сучасні засоби забезпечення інформаційної безпеки на прикладі SIEM-систем, наведені найбільш популярні виробники і постачальники послуг SIEM-систем. Висвітлено перспективи впровадження цих систем у діяльність сучасних підприємств.

Ключові слова. Корпоративна мережа, моніторинг, інформаційна безпека, SIEM-система.

Вступ. Сучасні інформаційні технології повністю інтегрувалися в усі сфери людської діяльності. Всесвітня мережа Інтернет об'єднує не лише окремих користувачів зі своїми персональними комп'ютерами та смартфонами, а й корпоративні мережі. З метою підвищення ефективності своєї діяльності підприємства, бізнес-структури через власні корпоративні мережі цілодобово обмінюються інформацією, документами між своїми підрозділами, постачальниками, партнерами та клієнтами.

З розвитком технологій підвищується і рівень загроз у сфері використання інформаційних технологій. Мережі та сервіси передачі даних піддаються ризику масштабних атак з боку зловмисників. Зловмисники вже більше десятка років активно здійснюють різні правопорушення та злочинні дії у сфері інформаційних технологій. У відповідь на нові атаки розробляються нові або удосконалюються старі методи захисту інформації та інформаційно-технічної інфраструктури підприємств.

Дослідженням питань інформаційної безпеки займається ряд як вітчизняних, так і закордонних дослідників, а також значна кількість державних і недержавних наукових установ, дослідницьких та аналітичних центрів. Серед науковців, що досліджують проблеми інформаційної безпеки: А. Грамші, К. Кубечка, М. Зубок, Я. Жарков, Р. Калюжний, Б. Кормич, В. Ліпкан. В. Макаренко, Ю. Максименко, О. Барановський та ін.

Виклад основного матеріалу. Сьогодні існує безліч загроз інформаційній безпеці підприємств, бізнесовим структурам. Серед загроз з якими стикаються підприємства — зовнішні вторгнення в корпоративні мережі і, як результат, – недоступність до корпоративних сервісів, викрадення конфіденційних даних та інформації, неможливість контролю web-трафіку, проникнення вірусів і, так званих, «троянських» програм, різні види внутрішніх і зовнішніх загроз підприємству та його діяльності.

Інформаційна безпека – стан захищеності потреб особи, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз. Захист інформації передбачає систему заходів, спрямованих на недопущення несанкціонованого доступу до інформації, несанкціонованої її модифікації, втрати, знищення, порушення цілісності [1].

Корпоративна мережа – мережа, ресурси якої доступні працівникам однієї компанії, підприємства чи навчального закладу [2].

VPN (Virtual Private Network) – узагальнена назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри. Ці технології дозволяють організовувати безпечний доступ до корпоративної мережі для віддалених співробітників компанії. Мережа VPN об'єднує підрозділи компанії в єдину мережеву інфраструктуру, забезпечує безперебійність роботи її ресурсів і захист внутрішнього трафіку [2].

Переваги корпоративних мереж: можливість централізованого дистанційного навчання; скорочення витрат на експлуатацію мереж та підвищення цінності інвестицій в мережеву інфраструктуру; прозорість роботи компанії, контроль над корпоративними

мережевими ресурсами; повний контроль за діяльністю всіх служб та структурних підрозділів; автономність мережі та високий рівень безпеки; безперервне оновлення інформації між співробітниками підприємства дозволить приймати їм своєчасні та правильні рішення; гнучкість корпоративної мережі на внутрішні та зовнішні зміни в середині компанії; доступ до всіх інформаційних ресурсів підприємства в реальному часі, незалежно від місця знаходження співробітників: в офісі, в іншому місті, дома або в дорозі [3].

В межах єдиної корпоративної мережі можна [3]:

- організувати централізований доступ до мережі інтернет;
- відео-, конференц зв'язок в межах компанії;
- корпоративну електронну пошту, голосову пошту, факси для підвищення ефективності та продуктивності роботи співробітників; єдиний електронний документообіг компанії;
- створення корпоративної IP-телефонії;
- загальні архіви документів, єдині корпоративні довідники та сервіси;
- автоматичний збір даних систем відео нагляду;
- комплексну автоматизацію робочих місць;
- дистанційний режим доступу до файлів, до сервер із базами даних, пристроїв друку; безпеку передачі даних та захисту корпоративної інформації від несанкціонованого доступу.

Для захисту від ненадійного доступу до даних корпоративних мереж в умовах сучасного розвитку бізнесу необхідно використовувати сучасні засоби забезпечення безпеки такі, як:

- захист периметра мережі;
- системи запобігання вторгненням;
- Web-фільтрація даних;
- антиспам-системи;
- антивірусний захист.

Для забезпечення інформаційної безпеки і керування інцидентами безпеки використовують SIEM-системи (Security information and event management). SIEM-системи представлені додатками, приладами і послугами.

SIEM-система моніторингу дозволяє звести всі події та інциденти інформаційної безпеки в єдиній структурі, виконує інтелектуальний аналіз атак та їх наслідків і допомагає адміністраторам виробити контрзаходи по інформаційній безпеці корпоративних мереж [4].

Крім цього, система моніторингу інформаційної безпеки виконує реєстрацію та зберігання всіх інцидентів інформаційної безпеки, що робить можливим використання отриманого матеріалу в якості доказового при виконанні розслідувань інцидентів та в судочинстві [4].

Робота цієї системи дозволяє побачити більш повну картину активності мережі і інцидентів інформаційної безпеки. Але разом з тим, цю систему використовують як додатковий спосіб захисту від цілеспрямованих атак на корпоративну мережу.

SIEM-система повинна збирати, аналізувати, моніторити і представляти інформацію із мережевих приладів і приладів безпеки.

Функції SIEM-системи спрямовані на моніторинг основних подій і станів інформаційної безпеки всередині компанії та її діяльності.

Основними функціями можна назвати [5]:

- моніторинг автентифікації та знаходження компроментуючих аккаунтів користувачів корпоративної мережі та адміністраторів;
- моніторинг випадків зараження корпоративних мереж;
- моніторинг підозрілого вихідного трафіку мереж і передання по мережі даних с використанням журналів веб-проксі;

- відстеження системи змін і інших адміністративних дій у внутрішніх мережах на їх відповідність дозволеного протоколу даних компанії;
- моніторинг атак на веб-додатки шляхом аналізу різних звітів;
- відстеження крадіжок даних та інших підозрілих зовнішніх підключень.

Слід приділити особливу увагу налаштуванню SIEM під клієнта, його інфраструктуру і системи безпеки. Правильно налаштовані правила використання системи дозволять спеціалісту аналізувати дійсно важливі повідомлення про інциденти порушення інформаційної безпеки, фільтруючи зайві дані.

SIEM-системи використовують інформацію з таких джерел, як [6]:

- системи автентифікації і системи контролю і управління доступом (Access Control);
- антивірусні засоби;
- міжмережеві екрани; системи виявлення / запобігання вторгнень;
- системи проксінг доступу в інтернет і веб-фільтрації; активні мережеві пристрої;
- системні журнали подій інформаційної безпеки серверів і робочих станцій користувачів;
- журнали аудиту систем управління базами даних;
- ключові корпоративні ресурси: поштові сервери, файлообмінні сервери, CRM- і ERP-системи;
- інші бізнес-додатки відповідно до вимог інформаційної безпеки компаній і стандартів.

Отриману інформацію SIEM аналізує за допомогою правил, що містять набір умов, тригерів, лічильників і сценаріїв дій у відповідь (в сукупності складових Use Cases). SIEM не протидіє зловмисним діям порушників, однак рішення дозволяє отримати найбільш повне уявлення про виникаючі події безпеки [5].

Великі підприємства, холдинги, мульти та транснаціональні компанії різних галузей – основна категорія споживачів SIEM-систем. SIEM дозволяють виявити порушення безпеки серед величезної кількості подій і оперативно відреагувати на виявлені проблеми. Крім того, SIEM-системи при необхідності беруть участь в проведенні аудитів відповідності.

Все більша увага приділяється дрібним постачальникам, оскільки організації малого і середнього бізнесу шукають послуги або варіанти надання SIEM для скорочення внутрішніх ресурсів і витрат, необхідних для дотримання вимог безпеки, використовують послуги аутсорсингу.

Сьогодні світовий ринок SIEM можна назвати зрілим і конкурентоспроможним. Постачальники в змозі задовольнити основні вимоги будь-якого клієнта, проте залишаються проблеми, пов’язані з виявленням цілеспрямованих атак і порушень в сфері інформаційної безпеки.

Ситуація може бути поліпшена завдяки додатковій розвідці загроз, профілізації поведінки користувачів і додатків, ефективній аналітиці. На даний момент спостерігається активне впровадження поведінкової аналітики користувачів і сутностей (User and Entity Behavior Analytics, UEBA), що позиціонується постачальниками як доповнення до SIEM, що володіє більш високою точністю виявлення цілеспрямованих атак [6].

Серед світових лідерів-постачальників SIEM систем можна назвати такі як:

SolarWinds Inc. – американська компанія, яка розробляє програмне забезпечення для бізнесу, яке допомагає керувати їх мережами, системами та інфраструктурою інформаційних технологій [7].

Netwrix – це приватна компанія, що займається інформаційною безпекою, яка дає можливість фахівцям з інформаційної безпеки та управління відновлювати контроль над чутливими, регульованими та критично важливими для бізнесу даними, незалежно від місця їх проживання [8].

Rapid7 – лідер в розробці рішення для управління уявленнями і тестування на просування. Допомога полягає в повному представленні безпеки інформаційної інфраструктури [9].

Одними з найбільш популярними SIEM-систем в Україні на теперішній час є [10]:

- QRadar Security Intelligence Platform (виробника IBM), основними перевагами є єдина платформа для всіх дій, які виконуються; гнучка архітектура; велика кількість безкоштовних додатків, контенту і модулів;
- McAfee (від виробника ESM), основні переваги це великий обхват промислових систем управління; інтеграція зі сторонніми технологіями; постійне джерело оновлення даних;
- HP ArcSight, основні переваги це повний набір можливостей, які дають можливість використання всіх функцій системи; проведення різноманітних аналіз; наявність бази знань загроз; наявність правил і додаткових продуктів.

Висновки. Отже, інформаційна безпека сучасних підприємств та бізнес-структур є одним з найважливіших компонентів інтегральної безпеки, на якому б рівні вона не розглядалась – національному, галузевому, корпоративному або персональному.

У сфері забезпечення інформаційної безпеки систем важливі не тільки окремі рішення, а й механізми генерації нових рішень, що дозволяють працювати і розвиватися в темпі технічного прогресу. Наявність засобів захисту інформації не є гарантією захисту всіх корпоративних ресурсів.

Для забезпечення оптимального рівня захисту необхідна система моніторингу інформаційної безпеки підприємства, якими є SIEM-системи, що спрямовані на моніторинг основних подій і інцидентів інформаційної безпеки всередині компанії та її діяльності.

В умовах сьогодення, сучасні технології програмування інформаційних систем не дозволяють створювати безпомилкові програми, що не підтримує швидкий розвиток засобів забезпечення інформаційної безпеки. Важливо починати з того, що необхідно створювати надійні системи інформаційної безпеки із залученням підозрілих компонентів (програм). Це стає цілком можливим, але потребує дотримання певних принципів і контролю за станом захищеності протягом усього життєвого циклу інформаційної системи.

Аннотация. В данном исследовании представлена информация о важности обеспечения информационной безопасности на современных предприятиях. Приведенные возможности и главные преимущества корпоративных сетей, названы основные угрозы корпоративным сетям в сфере информационной безопасности. Определены современные средства обеспечения информационной безопасности на примере SIEM-систем, приведены наиболее популярные производители и поставщики услуг SIEM-систем. Освещены перспективы внедрения этих систем в деятельность современных предприятий.

Ключевые слова. Корпоративная сеть, мониторинг, информационная безопасность, SIEM-система.

Abstract. This study provides information on the importance of information security in modern enterprises. The main opportunities and advantages of corporate networks are given, the main threats to corporate networks in the field of information security are named. Modern means of information security are identified on the example of SIEM-systems, the most popular manufacturers and service providers of SIEM-systems are given. Prospects for the introduction of these systems in the activities of enterprises are highlighted.

Key words. Corporate network, monitoring, information security, SIEM system.

СПИСОК ЛІТЕРАТУРИ

1. Інформаційна безпека. URL: http://www.ukr.vipreshebnik.ru/entsiklopediya/55-i/1943-informatsijna-bezpeka.html.
2. Комп'ютерні мережі. Основні терміни класифікації. URL: https://sites.google.com/site/mijsajtmerezainternet/komputerni-merezi-osnovni-termini-klasifikaciie.
3. Практикум з програмування на VBA. Навч. посібник / П. І. Каленюк, А. Ф. Обшта, Н. М. Гоблик, Н. Ф. Клочко, С. М. Ментинський. Львів: Видавництво Національного університету «Львівська політехніка», 2005. 208 с.
4. Системи моніторингу та управління безпекою. URL: http://integritysys.com.ua/security/siem/.
5. Что такое SIEM-системы и для чего они нужны? URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Popular-SIEM-Starter-Use-Cases
6. Огляд світового і російського ринку SIEM – систем. URL: https://www.anti-malware.ru/analytics/Market_Analysis/overview-global-and-russian-market-siem#part6
7. Solar Winds. URL: https://www.solarwinds.com/
8. Netwix. URL: https://www.netwrix.com/
9. Rapid7. URL: https://www.rapid7.com/
10. Які SIEM лідирують на ринку кібербезпеки в Україні? URL: https://channel4it.com/publications/Kakie-SIEM-lidiruyut-na-rynke-kiberbezopasnosti-v-Ukraine-14717.html