УДК 004.056.5: 004.7

Г. В. Олійник, С. В. Грибков
Національний університет харчових технологій,
кафедра інформаційних систем

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ ІНТЕЛЕКТУАЛЬНОГО ПРОГРАМНОГО КОМПЛЕКСУ ДЛЯ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Розглянуто основні проблеми захисту комп'ютерних мереж та запропоновано використання інтелектуального програмного комплексу QRadar для моніторингу інформаційної безпеки з метою виявлення загроз захисту елементів комп'ютерних мереж. Використання QRadar адміністраторами підвищує ефективність обслуговування комп'ютерної мережі у декілька разів завдяки застосуванню функцій автоматичного пошуку й аналізу виникнення загроз, попередження їх виникнення, а також надання повної інформації про вузли, виконання процесів та передавання пакетів у мережі.

Ключові слова: захист комп'ютерної мережі, аналіз подій та порушень, аналіз загроз, QRadar.

A STUDY OF USING QRADAR FOR COMPUTER NETWORK PROTECTION

The paper considers main problems of computer network protection and proposes to use QRadar Security Intelligence Platform to monitor information security for the purpose of detecting threats to protection of computer network elements. Using QRadar by the administrators ensures the increase of computer network service effectiveness by several times. It happens due to applying functions of automatic search and analysis of threat occurence, threat prevention, and providing complete information about the nodes, process execution, and packet transfer in a network.

Key words: computer network protection, event analysis, violation analysis, threat analysis, QRadar.

Вступ

Сучасний етап розвитку цивілізації характеризується впливом інформаційних і телекомунікаційних технологій, які сприяють змінам в економіці, соціальних структурах, культурі, державному управлінні тощо. Для України дуже важливим є той факт, що застосування інформаційних технологій дає можливість підвищити якість підготовки і прийняття управлінських рішень у різних сферах діяльності. Якість, надійність та безпечність інформаційного обміну – це ті критерії, що повинні бути основою всіх новостворюваних інформаційно-телекомунікаційних систем. Їх реалізація стала однією з пріоритетних задач для всіх державних та недержавних організацій.

З розвитком інформаційних технологій збільшились потреби щодо вирішення проблем захисту інформації, оскільки вона стала найважливішим стратегічним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Такі показники постійно ускладнюються, якісно змінюються, безперервно зростає кількість джерел інформації та її споживачів. Водночас збільшується вразливість сучасного інформаційного суспільства до недостовірної інформації, несвоєчасного надходження інформації, промислового шпигунства, комп'ютерної злочинності тощо.

Важливість миттєвого отримання точних даних під час управління безпекою комп'ютерної мережі важко переоцінити. Швидкість виявлення загрози є однією з актуальних проблем. Наприклад, один із корпоративних серверів заражений вірусом, а співробітники намагаються переглянути web-сайт зі шкідливим вмістом – рахунок часу ведеться на секунди. У таких випадках слід застосовувати сучасні комплексні інтелектуальні програмні засоби категорії SIEM (Security Information and Event Management – управління інформацією та подіями безпеки), що забезпечують можливість оперативно отримувати та аналізувати дані для негайного реагування в небезпечних ситуаціях [1]. Головними завданнями систем SIEM є збирання, зберігання й агрегація інформації про події безпеки з різних джерел комп'ютерної мережі, її нормалізація та кореляція, виявлення загроз і порушень політики безпеки, а також ведення звітності.

Огляд літературних джерел

Бурхливий розвиток інформаційних технологій спонукає до удосконалення методів захисту комп'ютерних систем та мереж, оскільки постійно виникають нові способи й методи їх ураження. Усе це зумовлює швидку втрату актуальності публікацій за цим напрямом.

У публікаціях [2, 3] описано проблеми захисту комп'ютерних мереж та можливих підходів до їх вирішення. У роботі [4] розглянуто найпоширеніші мережеві атаки та способи їх виявлення. Регулярно аналітичні статті та квартальні/річні звіти за адресою [5] випускає Arbor Networks, що займається захистом інформації. У публікації [6] розглянуто питання інформаційної безпеки та захисту даних, зокрема в інформаційно-обчислювальних системах та мережах. У [7] розглянуто проблематику оцінювання рівня захисту комп'ютерних мереж із врахуванням коефіцієнта емерджентності, що дає змогу визначити необхідний рівень захисту інформаційних потоків для певного класу архітектури комп'ютерної мережі. Публікації [8–10] присвячені огляду систем SIEM, що функціонують на уніфікованій операційній платформі та управляються з єдиної консолі.

На жаль, в публікаціях недостатньо висвітлено використання мережевого програмного комплексу QRadar, що належать до систем SIEM та має єдину архітектуру для аналізу журналів реєстрації, потоків, даних про кожний компонент комп'ютерної мережі.

Постановка задачі

Для підвищення ефективності захисту корпоративних інформаційних мереж та систем важливо дослідити основні проблеми їх захисту та застосування програмного комплексу QRadar для моніторингу інформаційної безпеки в реальному часі з метою виявлення уражень та атак на елементи комп'ютерної мережі, зокрема не відомих до цього.

Проблема захисту комп'ютерних мереж

Інформаційна безпека, згідно з визначенням, запропонованим "Узгодженими критеріями оцінки безпеки інформаційних технологій Європейських країн (ITSEC)", містить три складові: конфіденційність – захист від несанкціонованого отримання інформації; цілісність – захист від несанкціонованої зміни інформації; доступність – захист від несанкціонованого утримання інформації та ресурсів.

Під загрозою безпеці інформації в комп'ютерній мережі розуміють подію або дію, яка може викликати зміну функціонування її елементів, пов'язану з порушенням захищеності інформації, особливо під час її передавання чи оброблення. Вразливість інформації означає можливість настання такого стану, коли створюються умови для виникнення загроз безпеці інформації. Атака на комп'ютерну мережу – це комплекс дій, здійснених порушником, для пошуку та використання певної вразливості. Атака може мати форму вірусів, хробаків або бути результатом протиправних дій зловмисників, які намагаються отримати конфіденційні дані чи зашкодити роботі мережевих служб. Оскільки мережеві служби є найбільш фундаментальними елементами інфраструктури, будь-яка атака, скерована на них, може призвести до збитків підприємства, а тому основною задачею адміністраторів є їх захист [1].

Для підтримки взаємодії між комп'ютерами у мережі існує значна кількість апаратних та програмних засобів. Вразливими є усі основні структурно-функціональні елементи комп'ютерної мережі: робочі станції, сервери (host-машини), міжмережеві мости, шлюзи, центри комутації, канали зв'язку тощо. Велика кількість засобів для обміну даними у мережі загрожує безпеці системи. Сучасні комп'ютерні мережі містять багато різноманітних систем та пристроїв, а тому керування доступом до елементів мережі може стати складною нестандартною задачею. Для захисту серверів від несанкціонованого доступу необхідно застосовувати комплексні засоби захисту на кожному з них для запобігання незаконному доступу до інформаційних ресурсів. Надійні інструменти безпеки можуть зменшити складність і покращити власне безпеку, не порушуючи доступності. Вважається, що найбезпечніша система – це та, до якої ніхто не має доступу, але на практиці вона не може приносити користі. Отже, загрози безпеці мають визначатися й усуватися без порушення роботи чинних служб.

Проблеми безпеки передавання інформації під час роботи в комп'ютерних мережах доцільно поділити на три основні типи [1, 2]:

– перехоплення інформації – цілісність інформації зберігається, але її конфіденційність порушується;

– модифікація інформації – вихідне повідомлення змінюється і надсилається адресату;

– підміна авторства інформації – має серйозні наслідки: наприклад, хтось може надсилати електронні листи від іншого імені або web-сервер може видавати себе за електронний магазин, приймати замовлення, номери кредитних карт, але не відправляти товари.

Втрата інформації та несанкціонований доступ в системах і мережах пов'язані з:

- можливістю зчитування залишкової інформації в пам'яті системи після виконання санкціонованих запитів;
- копіюванням носіїв інформації та файлів інформації без застосування заходів захисту;
- маскуванням під зареєстрованого користувача;
- маскуванням під запит системи;
- використанням програмних пасток;
- використанням недоліків операційної системи;
- незаконним підключенням до апаратури та ліній зв'язку;
- злочинним виведенням з ладу механізмів захисту;
- проникненням комп'ютерних вірусів.

Різнопланові загрози безпеці інформації мають різне походження. У літературі описано різноманітні класифікації, в яких як критерії розподілу використовують види породжуваних небезпек, ступінь злочинного наміру, джерела появи загроз тощо.

Система безпеки повинна насамперед гарантувати доступність і цілісність інформації, а потім вже її конфіденційність. Доступність полягає у тому, що будь-який файл або ресурс системи повинен бути доступним у будь-який час за умови дотримання прав доступу. Цілісність полягає у забезпеченні незмінності інформації під час її зберігання або передавання. Важливим принципом сучасного захисту інформації є оптимальне співвідношення між доступністю і безпекою, що можна реалізувати використанням комплексного програмного рішення.

Безпеки інформації в комп'ютерних мережах можна досягти лише комплексним підходом до постійного підтримання організаційних, організаційно-технічних, апаратних та програмних заходів на належному рівні. Забезпечення безпеки – це безперервний процес, а не разові заходи, що виконуються за необхідності.

Для надійності захисту ресурсів комп'ютерних мереж необхідно постійно удосконалювати існуючі та впроваджувати сучасні прогресивні й перспективні технології інформаційної безпеки. Основними задачами та підходами до цього є:

- комплексний підхід до формування інформаційної безпеки, що забезпечує раціональне об'єднання технологій і засобів інформаційного захисту;
- застосування захищених віртуальних мереж для захисту інформації, переданої у відкритих каналах зв'язку;

• криптографічне перетворення даних для забезпечення цілісності, дійсності та конфіденційності інформації;

• застосування міжмережевих екранів для захисту корпоративної мережі від зовнішніх загроз у разі підключення до загальнодоступних мереж зв'язку;

• керування доступом на рівні користувачів та захист від несанкціонованого доступу до інформації;

• гарантована ідентифікація користувачів шляхом застосування токенів (смарт-карт, touch-memory, ключів для USB-портів та ін.) та інших засобів аутентифікації;

• надійний захист інформації шифруванням файлів і каталогів;

• захист від вірусів з використанням спеціалізованих комплексів антивірусної профілактики й захисту;

• технологія виявлення вторгнень і активного дослідження захищеності інформаційних ресурсів;

• централізоване керування засобами інформаційної безпеки.

Наявність централізованих засобів керування продуктами безпеки є обов'язковою вимогою для можливості їхнього застосування в корпоративному масштабі. Необхідно зауважити, що системи централізованого керування продуктами безпеки різних виробників переважно не сумісні одна з однією.

Комплексне рішення QRadar

Компанія IBM, один з лідерів у створенні програмних рішень, пропонує сучасний інтелектуальний комплекс моніторингу інформаційної безпеки підприємства – IBM QRadar. Цей комплекс надає можливість кореляційного аналізу даних у реальному часі для отримання актуальних знань про загрози безпеці. Комплекс QRadar забезпечує високий рівень масштабування та продуктивності, централізоване управління, можливість конфігурації та адаптації до специфічних вимог на основі сервісних майстрів та інші переваги. Продукт QRadar належав компанії Q1Labs, яка увійшла до корпорації IBM в 2011 році.

Основними функціями програмного комплексу QRadar є:

• збирання та аналіз повідомлень, що надходять від різних джерел – системи виявлення вторгнень, міжмережевих екранів, операційних систем, різних додатків, баз даних, антивірусних систем тощо;

• ранжування інформації про події інформаційної безпеки, що дає змогу розглядати насамперед найбільш критичні інциденти для функціонування інформаційної інфраструктури;

• кореляційний аналіз отриманих даних на предмет визначення комплексних мережевих атак, а також атак, розподілених за часом;

• автоматичне виявлення проблем, пов'язаних з порушенням безпеки, визначення їх причин та реагування на них;

• візуалізація отриманих даних у реальному часі та повідомлення адміністраторів комп'ютерної мережі про підозри на порушення безпеки та цілісності елементів мережі, що використані для цього.

QRadar складається з трьох сумісно функціонуючих додатків, які призначені для реалізації такої загальної функціональності: управління логами – QRadar Log Manager, управління подіями та інцидентами – QRadar SIEM і управління ризиками – QRadar Risk Manager [8].

QRadar Log Manager є комплексним рішенням для управління логами, яке забезпечує збирання, зберігання та аналіз журналів мережевих подій і журналів безпеки.

QRadar SIEM забезпечує повну прозорість мережі, відстежуючи та контролюючи активність всіх користувачів, пристроїв і додатків, що дозволяє виявляти не тільки існуючі, а й потенційні загрози для мережевої інфраструктури.

QRadar Risk Manager забезпечує управління загрозами, журналами подій, аналіз поведінки мережі з використанням функцій автоматизованого управління ризиками в критичних місцях. QRadar Risk Manager дає змогу оцінювати стан безпеки в автоматизовану режимі, застосовуючи

цілу низку індикаторів загроз щодо конфігурації мережі, мережевої активності, подій безпеки та результатів сканування наявності загроз.

Інтерфейс користувача QRadar реалізований через web-інтерфейс та містить набір інформаційних панелей для перегляду детальної інформації про події, мережеві потоки, зареєстровані порушення. Основні інформаційні панелі представлені такими елементами: порушення, зареєстровані в системі, а також налаштування правил кореляції; перегляд і аналіз зареєстрованих подій безпеки; перегляд і аналіз мережевих потоків; перегляд та налаштування профілів пристроїв, виявлення серверів та управління сканерами пошуку вразливостей; створення, редагування, розповсюдження звітів; управління параметрами налаштування системи, користувачами, джерелами подій [8].

Інформаційні панелі подій забезпечують можливість швидкого візуального аналізу багатьох аспектів подій та потоків, виявлених системою QRadar. Дані для відображення на інформаційних панелях генеруються на основі пошукових шаблонів за подіями або потоками з бази даних QRadar. Адміністратори мають можливість відредагувати існуючі або створити нові структури відображення даних на інформаційних панелях, а також змінити вид відображення інформації (графік, діаграма, таблиця тощо).

Фіксація порушення автоматично генерується системою при спрацьовуванні одного з відповідних кореляційних правил, що складається з однієї окремої умови або з цілої низки умов, які спрацьовують у результаті аналізу різнорідних подій та мережевих потоків. Одне порушення або інцидент може складатися з десятків тисяч проаналізованих подій і/або потоків. Кожне зафіксоване порушення містить вичерпну інформацію про інцидент: IP-адреси джерел і цілей, номери портів, MAC адреси, ім’я та групу користувача тощо.

Адміністратор мережі має можливість переглянути детальну інформацію про порушення, що виникло, та отримати повний опис будь-якої події або потоку, що стали причиною створення інциденту. Широкий спектр можливостей налаштування забезпечує формування повідомлення адміністратору про певні події тільки тоді, коли буде накопичено відповідну кількість таких повідомлень. Найпростішим і водночас яскравим прикладом може слугувати подія неправильного введення пароля. Система не буде попереджати, якщо було зафіксовано лише одну спробу ввести неправильний пароль – це трапляється часто. Однак, якщо система реєструє повторні спроби введення неправильного пароля до одного і того самого облікового запису більше заданої кількості разів за короткий проміжок часу, подія переходить у статус загрози, оскільки це може свідчити про спробу несанкціонованого проникнення до системи за допомогою підбору пароля.

Модуль представлення і аналізу інформації про події безпеки, зареєстровані та нормалізовані системою, забезпечує розв’язання таких задач: пошук певної події; пошук підмножини подій; збереження і управління критеріями та результатами пошуку; перегляд подій у реальному часі; перегляд згрупованих за різними критеріями подій; створення, перегляд та аналіз графіків часових рядів; перегляд та управління даними перехоплення пакетів; асоціювання невідомої події з категоріями високого та низького рівня; налаштування параметрів помилкових спрацювань для запобігання створенню інцидентів; експорт подій у формати XML або CSV. Цей модуль дає змогу контролювати й досліджувати події інформаційної безпеки в режимі реального часу, а також виконувати складні пошукові запити для розширеного аналізу. Необхідно зазначити, що події, введені до складу будь-якого інциденту, зазначаються, що дає змогу провести повний та швидкий аналіз.

Модулем представлення і аналізу мережевих потоків візуально відстежують та досліджують мережеві потоки даних у режимі реального часу, а також застосовують складні параметри фільтрації для їх відображення. Крім цього, є можливість проаналізувати мережевий потік для визначення типу передавання даних та типу повідомлення.

Використовуючи пасивний потік даних та дані про вразливості, QRadar автоматично виявляє ресурси, що працюють в мережі, та створює профілі пристроїв, які надають інформацію про кожний відомий ресурс, зокрема інформацію про кожну працюючу мережеву службу для кожного ресурсу. Вони використовуються для кореляції даних, щоби зменшити кількість помилкових

спрацьовувань. За наявності сканера вразливості в мережевій інфраструктурі до профілю пристрою автоматично додається інформація про можливі вразливості. Дані з профілів пристроїв також використовуються системою для визначення відповідності до зареєстрованих подій та порушень.

Модуль створення, редагування, розповсюдження, управління звітами містить значну кількість стандартних видів звітів, розбитих на десять основних груп. Звіти, що відповідають восьми основним міжнародним нормам, доступні відразу, а за необхідності є можливість змінити їх форми представлення. Вбудований фільтр дає змогу створювати різні форми звітів. Будь-який зі звітів можна налаштувати для автоматичного формування за графіком та розсилання визначеним адресатам у форматах PDF, HTML, RTF, XLS та XML.

Модуль управління налаштуваннями системи, користувачами, джерелами подій дозволяє запланувати автоматичні оновлення всієї системи, модулів підтримки пристроїв, резервне копіювання та відновлення, внесення змін у глобальні налаштування системи, побудувати ієрархію мережевих сегментів. Управління користувачами і ролями дає змогу гнучко налаштувати права доступу кожного користувача системи до конкретних об'єктів або звітів.

Висновок

Використання розглянутого комплексного програмного рішення IBM QRadar забезпечить комплексний захист у комп'ютерних мережах будь-якої складності. Програмне рішення дає змогу відслідковувати та аналізувати виникнення загроз, попереджувати їх виникнення, а також надавати адміністраторам повну інформацію про вузли, виконання процесів та передавання пакетів у мережі.

Комплексне програмне рішення IBM QRadar повністю інтегрується в інфраструктуру підприємства, що забезпечує швидкий та надійний моніторинг корпоративної безпеки, а також масштабується з її розвитком, застосовуючи досвід взаємодії з конкретними користувачами до груп користувачів усієї організації. Можливість всебічного перегляду та аналізу інформації підвищує ефективність обслуговування комп'ютерної мережі в декілька разів. Основними перевагами застосування IBM QRadar є: підвищення рівня захищеності інформаційної інфраструктури внаслідок оперативного реагування на інциденти інформаційної безпеки; прискорення і автоматизація процесу ідентифікації, а також подальше дослідження інцидентів; централізований підхід до задач обробки та зберігання подій інформаційної безпеки.

1. Биячуев Т.А. Безопасность корпоративных сетей. – СПб: Издательство ГУ ИТМО, 2004. 2. M. Abliz Internet Denial of Service Attacks and Defense // Pittsburgh: University of Pittsburgh Technical Report [Электронный ресурс]. – Режим доступу: http://people.cs.pitt.edu/~mehmud/docs/abliz11-TR-11-178.pdf. 3. Гайворонський М. В., Новіков О. М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2009. – 608 с. 4. Приходько Т. А. Исследование вопросов безопасности локальных сетей на канальном уровне модели OSI [Электронный ресурс]. – Режим доступу: http://ea.donntu.edu.ua:8080/jspui/handle/123456789/2068. 5. Worldwide Infrastructure Security Report // Arbor Networks [Электронный ресурс]. – Режим доступа: http://www.arbornetworks.com/report 6. Емельянова Н. З., Партыка Т. Л., Попов И. И. Защита информации в персональном компьютере. – М.: Форум, 2009. – 368 с. 7. Якименко І. З. Критерії оцінки рівня захисту комп'ютерних мереж з врахуванням їх архітектури // Інформатика та математичні методи в моделюванні, 2013 – Т. 3. – №1 – С. 82–90. 8. David R. Miller, Shon Harris, Stephen Vandyke Security Information and Event Management (SIEM) implementation, McGrawHill, 2011. 9. Security Intelligence Operations [Электронный ресурс]. – Режим доступа: http://tools.cisco.com/security/center/home.x 10. SAS® Security Intelligence [Электронный ресурс]. – Режим доступа: https://www.sas.com/software/security-intelligence.