МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВАСИЛЯ СТУСА

В. Г. Крижановський, С. П. Сергієнко

Апаратно-програмні засоби захисту інформації у корпораціях

Навчально-методичний посібник

Вінниця
ДонНУ імені Василя Стуса
2019

УДК 004.056.53
К 85

Рекомендовано до друку вченою радою фізико-технічного факультету (протокол № 10 від 21.06.2019 р.)

Автори:
В. Г. Крижановський, проф. кафедри радіофізики та кібербезпеки,
С. П. Сергієнко, доц. кафедри радіофізики та кібербезпеки.

Рецензент: *П. К. Ніколюк,* д-р фіз.-мат. наук, проф., проф. кафедри комп'ютерних технологій.

Крижановський В. Г., Сергієнко С. П.
К 85 Апаратно-програмні засоби захисту інформації у корпораціях: навчально-методичний посібник. Вінниця : ДонНУ імені Василя Стуса, 2019.–36 с.

Розглядаються основи функціонування корпоративних систем управління інформаційною безпекою та контролю інформаційних подій, на прикладі відомої системи фірми IBM QRadar SIEM.

Посібник рекомендовано для студентів вищих навчальних закладів за напрямом «Кібербезпека (Cybersecurity)».

УДК 004.056.53

ВСТУП

Питання інформаційної безпеки для сучасного світу є вкрай актуальним, важко визначити пріоритетні напрями для реагування на загрози кібербезпеки, але питання захисту інформації у корпораціях, які є основою сучасної економіки, завжди залишаються на перших місцях у розробників безпечних інформаційних технологій. Це, безумовно, пов’язано з великим обсягом залучених людських та грошових ресурсів. Метою цього посібника є дати уявлення про деякі важливі аспекти систем захисту інформації для корпорацій (великих підприємств) та їх складових частин – систем моніторингу трафіку та аналізу мережевої активності.

Англійською мовою існує загально прийнята абревіатура для назви таких систем – SIEM (Security Information and Event Management, українською – управління подіями безпеки та управління інформаційною безпекою). Значення терміна змінювалося з часу його введення у 2005 році [1] і зараз його розуміють як опис мережевої активності в одному структурованому наборі даних [2], який призначено для аналізу та прийняття рішень фахівцем з інформаційної безпеки.

1. Види та застосування систем SIEM

Існує багато систем SIEM, які розробляються різними фірмами-розробниками систем обробки даних та комп'ютерної безпеки [3]. На рис. 1 показано рекламний звіт фірми Gartner із вказівкою на продукти деяких інших розробників. Бачимо, що коло виробників досить широке та містить доволі відомих вендорів. Поясненням цього може бути практична обов'язковість використання подібних програмних засобів у сучасній практиці інформаційної безпеки, у деяких країнах ця обов'язковість записана у стандартах та нормативних документах та може бути вимогою страхових компаній [4]. У певному сенсі SIEM є поліпшеною системою виявлення шкідливої активності та різних системних аномалій. Робота SIEM дає можливість побачити більш повну картину активності мережі і подій безпеки. Коли звичайні засоби виявлення, взяті окремо, не бачать атаки, вона може бути виявлена за умови ретельного аналізу та кореляції інформації з різних джерел. Тому багато корпорацій розглядають використання SIEM-систем як додатковий і дуже важливий елемент захисту від цілеспрямованих атак.

На рис. 2 представлено функції SIEM-систем, які відповідають типовим сценаріям використання таких систем.

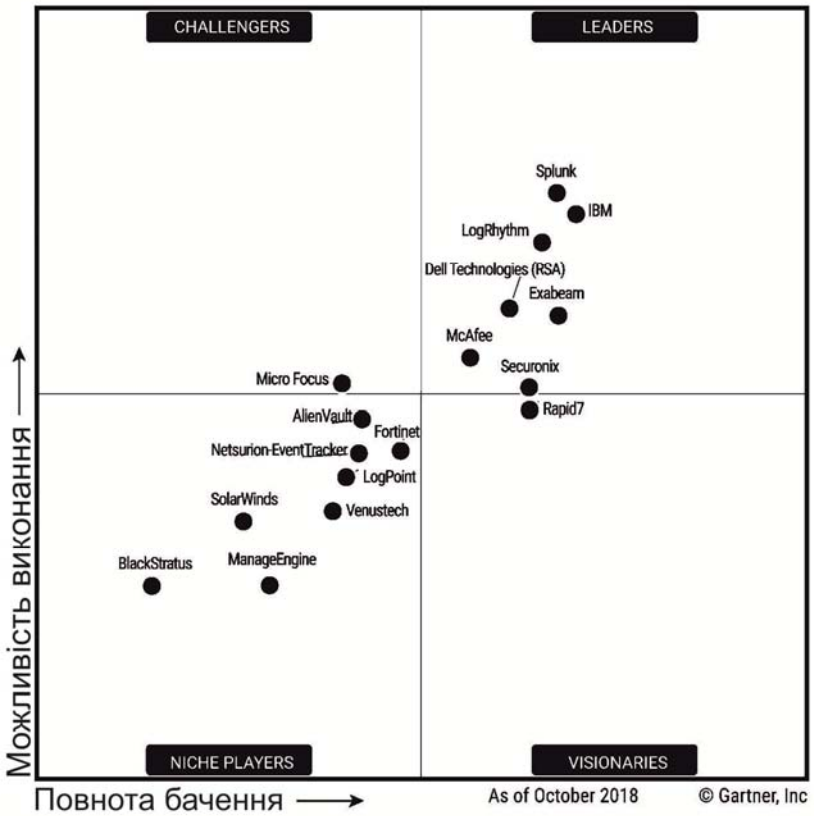

Рис. 1 Деякі характеристики поширених систем SIEM [1]

Рис. 2 Функції, які виконує SIEM-система

1. Відстеження аутентифікації та виявлення компрометування акаунтів користувачів та адміністраторів.
2. Відстеження випадків зараження. Виявлення шкідливих програм із використанням вихідних журналів брандмауерів та журналів веб-проксі, а також внутрішніх журналів підключення та мережевих потоків.
3. Моніторинг підозрілого вихідного трафіку та даних, що передаються в мережі, з використанням журналів брандмауеру та журналів веб-проксі і NetFlow. Виявлення крадіжки даних та інших підозрілих зовнішніх з'єднань.
4. Відстеження змін у системі та інших адміністративних дій у внутрішніх системах та їх відповідність політиці дозволів підприємства.
5. Відстеження атак на веб-додатки та їх наслідків з використанням журналів веб-серверів, WAF (Web Application Firewall, екран для захисту веб-додатків) і логів додатків. Виявлення спроб компрометації веб-додатків шляхом аналізу різних звітів.

SIEM-системи продовжують розвиватися і з часом можуть стати частиною чогось більш досконалого, але зараз без використання SIEM неможливо побудувати такі системи і центри моніторингу і реагування як SOC (Security Operation Centre) і під'єднатися до FinCert або подіб-

них організацій, тому що SIEM дає можливість вирішити цілу низку ключових завдань: збирати та зберігати лог-файли в єдиному централізованому сховищі, надавати спеціалізовані звіти аудиторам для перевірки відповідності вимогам законодавства та відомчим стандартам, досліджувати кореляцію між різними джерелами даних.

Особливо потрібно звернути увагу на налаштовування SIEM під вимоги користувача, його інфраструктури та системи безпеки. Добре налаштовані правила кореляції дають змогу оператору аналізувати справді важливі повідомлення про інциденти, відсіюючи зайве. Важливо, щоб система брала на себе максимум рутинних операцій.

IT-інфраструктура сучасних корпорацій вельми різноманітна. При цьому, з розвитком технологій, головною проблемою побудови захисту стає не відсутність інформації, а її обробка. Кількість джерел, які забезпечують надходження актуальної інформації за поточним станом захищеності, безперервно зростає. Дійсно, зараз усе корпоративне програмне забезпечення веде записи у журнал та фіксує свій стан і події. Але разом зі збільшенням обсягів інформації, адміністраторам інформаційної безпеки стає складніше відстежувати загальний стан справ. Тому якщо вчасно не аналізувати загрози, що виникають, та не намагатися попередити їх, то будь-яка система захисту виявиться марною.

Крім того, зловмисники все частіше переходять від атак «в лоб» до більш складних та розподілених сценаріїв (APT – Advance Persistent Threat). Загальні принципи, на яких будуються APT, давно відомі. Наприклад, використовуються методи соціальної інженерії для того, щоб спровокувати користувача відкрити посилання або файл, що додається. Або використання вразливостей заради отримання доступу до системи, на яку здійснюється атака. Проблема полягає у тому, що у разі подібної атаки всі засоби захисту можуть «мовчати», оскільки «вирвані з контексту» інциденти не будуть сприйматися як серйозна загроза. Але водночас аналіз сукупності інцидентів може наочно вказати на атаку. Саме такі «магічні» властивості приписуються сучасним SIEM-системам – здатність виявляти атаки по «крупинках», за аномаліями, постаналізом подій та інше.

Треба розуміти, що SIEM-системи не призначені та і не можуть попереджати інциденти порушення інформаційної безпеки. Їх сутність закладе у назві: аналіз інформації, яка надходить із різних джерел (DPL, IDS, антивіруси, міжмережеві екрани та інше), та подальше виявлення різних відхилень від норм за призначеними критеріями.

Перед системою SIEM ставлять такі завдання:

- Консолідація та зберігання журналів з різних джерел.
- Надання інструментів для аналізу подій та розборки інцидентів.

- Виконання кореляційного аналізу та обробки подій за правилами.
- Автоматичне сповіщення та інцидент-менеджмент.

1.1. Принцип роботи системи SIEM

В теорії все просто: система збирає інформацію, аналізує в режимі реального часу та/або аналізує поведінку на основі попередніх спостережень і генерує повідомлення про попередження.

На практиці ця схема реалізується за допомогою таких компонентів:

- Агенти (збір даних з різних джерел).
- Сервери-колектори (акумуляція інформації, що надійшла від агентів).
- Сервер баз даних (зберігання інформації).
- Сервер кореляції (аналіз інформації).

Для SIEM-систем вхідною може бути будь-яка інформація. Головне – правильне її подання. Збір даних може виконуватися за допомогою програм – це спеціальні агенти, що локально збирають журнали подій і за можливості передають їх на сервер. Для «прочитання» того чи іншого джерела даних агент використовує колектори – бібліотеки для розуміння конкретного журналу подій або системи. Колектори відіграють важливу роль, тому що різні джерела можуть іменувати одну і ту саму подію по-різному. Наприклад, Firewall одного виробника може записувати у звіт «deny», іншого «discard», третього «drop». Хоча це одна і та сама подія. Колектори допомагають привести всі ці події до загального знаменника.

Якщо ж для джерела нема відповідного колектора, події можна спробувати відправляти як SYSLOG (при умові, що джерело може це робити). Але тут можна зіткнутися з «проблемою синонімів» та необхідністю написати додаткову програму обробки для приведення даних у єдиний формат.

Також інформацію можливо збирати віддалено за допомогою з'єднання за протоколами NetBIOS, RPC, TFTP, FTP. Однак і тут може виникнути проблема з навантаженням на мережу, тому що частина систем дає можливість передавати тільки журнал цілком, а не «свіжі» записи.

SIEM-системи можуть використовувати такі джерела інформації:

- Access Control, Authentication. Застосовуються для моніторингу контроля доступу до інформаційних систем та використання привілеїв.

• DLP-системи. Відомості про спроби витоку інформації від інсайдерів, порушення прав доступу.

• IDS/IPS-системи. Містять дані про мережеві атаки, зміни конфігурації та доступу до пристроїв.

• Антивірусні програми. Генерують події про працездатність програмного забезпечення (ПЗ), бази даних, зміни конфігурацій та політик, про шкідливий код.

• Журнали подій серверів і робочих станцій. Використовуються для контролю доступу, забезпечення безперервності, виконання політик інформаційної безпеки.

• Міжмережеві екрани. Відомості про атаки, шкідливе ПЗ та про інше.

• Мережеве активне обладнання. Дані про інвентаризацію активів, сервісів, програмного забезпечення, вразливостей, подання інвентаризаційних даних та топологічної структури.

• Системи інвентаризації та asset-management. Надають дані для контролю активів в інфраструктурі та виявлення нових.

• Системи веб-фільтрації. Надають дані про відвідування співробітниками підозрілих або заборонених веб-сайтів.

Отримавши інформацію, система може її проаналізувати. За основу аналізу відповідає практично «чиста» математика та статистика. Але відправною точкою є правила, які задаються користувачем. Наприклад, одноразова подія «Login failed» нічого не значить, тоді як три чи більше таких подій від одного облікового запису вже може свідчити про спроби підбору пароля.

У найпростішому випадку у SIEM-системах правила представлені у форматі RBR (Rule Based Reasoning) і містять набір умов, тригери, лічильники, сценарії дій. Наприклад, враховувати параметри віддаленості двох останніх місць використання банківської карти за невеликий проміжок часу: якщо о 15:00 її використовували для сплати за каву у Києві, а через 10 хвилин намагаються зняти готівку у максимальній сумі у Макао, то це явно спроба шахрайства.

SIEM-системи здатні виявляти:

• мережеві атаки у внутрішньому та зовнішньому периметрах;

• вірусні епідемії або окремі вірусні зараження;

• спроби несанкціонованого доступу до конфіденціальної інформації;

• шахрайство;

• помилки та наявність збоїв у роботі інформаційних систем;

• вразливості;

• помилки конфігурації у засобах захисту та інформаційних системах;

• цільові атаки (ATP).

Наразі класичне SIEM-рішення, яке містить у собі тільки інструменти з роботи з журналами подій, що надходять від компонентів IT-інфраструктури (збір, зберігання, кореляція, перевірка на відповідність вимогам, повідомлення), є застарілим і не може задовольнити усі потреби зрілої компанії.

Зараз поняття SIEM стало ширше. Від SIEM-системи вимагаються нові функції та механізми, здатні більш швидше та точно не тільки виявляти, але і попереджати інциденти інформаційної безпеки, водночас не обмежуючись аналізом лише журналів подій. SIEM-рішення нового покоління прагне поєднувати у собі «традиційні» функціональні якості SIEM, а також функції аналізу мережевого трафіку та управління ризиками.

1.2. Приклади комерційних систем SIEM

На ринку SIEM як і раніше домінують великі вендори – IBM, Splunk, HPE, McAfee (раніше Intel Security), які володіють більш як 60 % доходів від ринку. LogRhythm – приклад постачальника точкового рішення, який продовжує займати важливі позиції на ринку. RSA активно наступає на п’яти лідерам і прагне вирватися з другого ешелону.

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. Треба зазначити, що постачальники SIEM, як великі, так і малі, все частіше звертаються до провайдерів інформаційної безпеки – MSSP (Managed Security Service Provider) – для запуску послуг на базі своїх SIEM або ж самостійно пропонують користувачам сервіси.

Провідні виробники SIEM інтегрують свої рішення з платформами Big Data (власні розробки або вільне програмне забезпечення, таке як Hadoop). Низка вендорів, що володіють власними можливостями досліджень в області безпеки (IBM, HPE, McAfee (Intel Security), RSA і Trustwave), забезпечують інтеграцію SIEM з даними кіберрозвідки. Постачальники (EventTracker, HPE, IBM і Trustwave), які пропонують замовникам як SIEM, так і MSSP (Managed Security Service Provider), займаються маркетингом спільно використовуваних технологій розгортання SIEM, які включають в себе низку послуг моніторингу та реагування. Так, наприклад, IBM надає послуги не тільки моніторингу, а й експертного аналізу і реагування на інциденти ІБ, а RSA забезпечує загальну платформу для управління журналами і перехоп-

лення мережевих пакетів, а також інтегрує свій SIEM з технологією GRC (Governance, Risk management, and Compliance).

Закордонні SIEM-системи

HPE ArcSight

Hewlett Packard Enterprise (HPE) ArcSight – одна з найкорисніших SIEM-систем. Довгий час вона вважалася еталоном. Платформа HPE ArcSight орієнтована на середні і великі підприємства та постачальників послуг. Платформа доступна в трьох різних варіантах:

- Платформа даних Arcsight Data Platform, яка забезпечує збір журналів, управління і генерацію звітів.
- Програмне забезпечення Arcsight Enterprise Security Management (ESM), призначене для розгортання широкомасштабного моніторингу безпеки.
- Програмно-апаратний комплекс Arcsight Express, заснований на пристроях «все в одному» і орієнтований на використання з попередньо сконфігурованим моніторингом і звітністю, а також спрощеним управлінням даними.

Платформа HPE ArcSight може бути розгорнута як пристрій, програмне забезпечення або віртуальний екземпляр. HPE ArcSight підтримує масштабовану n-рівневу архітектуру з HPE ArcSight Management Center. HPE ArcSight Express доступний тільки як пристрій.

ArcSight Express треба розглядати як SIEM середнього рівня, розгортання якої вимагає великої підтримки конекторів сторонніх постачальників. HPE ArcSight ESM добре підходить для великомасштабного розгортання і для організацій, які хочуть побудувати виділений SOC.

У 2017 році вийшов новий продукт ArcSight Investigate, який можна використовувати як посилення аналітичних можливостей HPE ArcSight. Додатково HPE ArcSight розвивається в бік вирішення прикладних завдань, таких як боротьба з фінансовим шахрайством в банках, оперативне управління ІБ / IT, контроль метрик ефективності СЗІ, інтеграція з SAP, і соціалізацію (ArcSight Marketplace).

Переваги HPE ArcSight:

- Arcsight ESM надає повний набір можливостей SIEM, які можуть використовуватися для підтримки великомасштабного SOC, включно з повним робочим процесом розслідування інцидентів та управління, а також спеціальну консоль управління розгортанням.

• HPE User Behavior Analytics виявляє аномалії на основі аналізу поведінки користувачів і доповнює традиційну кореляцію, яка є базовою функцією arcsight.

• DNS Malware Analytics аналізує DNS-трафік і забезпечує повну видимість IT-інфраструктури, що допомагає виявити уразливі місця ще до того, як ними скористаються зловмисники. Ідея аналізу DNS-трафіку з метою виявлення зловмисної активності зародилася в дослідницькому підрозділі HP Labs більше п'яти років тому.

• Arcsight Threat Central містить інтерактивну базу знань загроз і дає змогу обмінюватися відомостями про способи їх виявлення та ліквідації.

• На порталі ArcSight Marketplace містяться правила (пакети безпеки) і додаткові додатки. Розробники з HPE сподіваються, що до формування таких пакетів безпеки і створення додаткових додатків будуть підключатися і партнери компанії.

• HPE arcsight має широкий вибір готових до використання сторонніх технологій і конекторів.

IBM QRadar Security Intelligence Platform

IBM QRadar Security Intelligence Platform включає в себе ряд інтегрованих між собою систем збору подій, моніторингу, аналізу захищеності і розслідування інцидентів:

- Log Manager;
- SIEM;
- Flow Processor;
- Vulnerability Manager;
- Risk Manager;
- Network Insights;
- Watson Advisor for Cyber Security;
- Packet Capture and Incidents Forensics.

На додаток до платних компонентів клієнти IBM QRadar отримують доступ до безкоштовного контенту, додатків та репутаційних баз з X-Force and App Exchange, де можна знайти програми для розширеної візуалізації інцидентів, UBA, інтеграційні модулі з іншими системами безпеки від IBM (наприклад, i2 Analysis Notebook) та інших виробників, а також додаткові правила кореляції у вигляді готового SIEM-контенту.

QRadar може бути розгорнуто з використанням фізичних і віртуальних пристроїв, представлений як служба IaaS (Infrastructure-as-a-

Service) в державних або приватних хмарних сервісах або як пропозиція SaaS (Software-as-a-Service) IBM QRadar on Cloud, яке повністю управляється IBM разом із додатковим моніторингом подій IBM Managed Security Services.

Платформа QRadar дає можливість збирати й обробляти дані про події ІБ з журналів аудиту безпеки, аналізувати мережеву статистику (NetFlow та ін.), здійснювати самостійний аналіз мережевого трафіку і переданої інформації, будувати топологію мережі й емулювати зміни в конфігураційних файлах мережного обладнання, виявляти уразливості і небезпечні настройки систем, повністю захоплювати трафік і відтворювати ланцюжок комунікацій між вузлами мережі.

За останній час IBM представила кілька нових функцій і нові можливості, включно з IBM Watson Advisor for Cyber Security, та інтеграцію з платформою реагування на інциденти IBM Resilient, щоб знизити навантаження на аналітиків SOC, систематизувати й автоматизувати процеси реагування на інциденти.

Переваги IBM QRadar Security Intelligence Platform:

- Єдина платформа для планомірного створення SOC: починаючи зі збору та аналізу подій ІБ, виявлення аномальної мережевої активності, сканування вразливостей і виявлення небезпечних конфігурацій, закінчуючи інтеграцією зі штучним інтелектом IBM Watson, комп'ютерною криміналістикою (форензіка) і переходом до процесів реагування на інциденти в IBM Resilient.
- Гнучка архітектура QRadar Platform дає змогу наново визначати роль і функції модулів платформи і не обмежує компанії-клієнтів жорсткими рамками одного разу обраної схеми.
- Велика кількість безкоштовних додатків, контенту та інтеграційних модулів, включно з UBA і репутаційними базами недовірених IP від команди IBM X-Force.
- Велика кількість інсталяцій по всьому світу з високими показниками навантаження і вимогами до працездатності.

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager (ESM) поставляється як фізичні і віртуальні пристрої і програмне забезпечення. Три основні компоненти, що входять до складу SIEM, – ESM, Event Receiver і Enterprise Log Manager, які можуть бути розгорнуті разом як один екземпляр або окремо для розподілених або великомасштабних середовищ. Додатковими компонентами є Advanced Correlation Engine, Database Event Monitor, Application Data Monitor і Global Threat Intelligence.

Розширення, впроваджені за останній час, включають можливість динамічного заповнення списків спостережень із додаткових внутрішніх або зовнішніх джерел, більш глибоку двосторонню інтеграцію з Hadoop і підтримку додаткового доступу до джерел інформації про загрози і управління ними. Інтеграція ESM з McAfee Active Response тепер забезпечує більшу видимість кінцевих точок.

Переваги McAfee Enterprise Security Manager:

- Enterprise Security Manager має гарне охоплення промислових систем управління (ICS) і пристроїв диспетчерського управління та збору даних (SCADA).
- McAfee Data Exchange Layer (DXL) від Intel Security забезпечує інтеграцію із сторонніми технологіями без використання API. Цей підхід дає можливість для використання ESM в якості платформи SIEM.
- McAfee Global Threat Intelligence дає змогу розширити можливості SIEM-системи Enterprise Security Manager, додавши джерело інформації, яка безперервно оновлюється, про загрози, що дає можливість швидко виявляти події, які включають в себе сеанси зв'язку з підозрілими або шкідливими IP-адресами.

RSA NetWitness Suite

У липні 2016 року RSA, підрозділ безпеки EMC[1], повторно представив свою SIEM-систему як платформу RSA NetWitness Suite, яка включає в себе:

- управління журналами RSA NetWitness Logs & Packets (раніше RSA Security Analytics);
- засіб виявлення загроз на робочих станціях RSA NetWitness Endpoint (раніше RSA Enterprise Compromise Assessment Tool);
- менеджер центру оперативного управління RSA NetWitness SecOps Manager (раніше RSA SecOps).

RSA NetWitness Suite забезпечує видимість загроз із використанням даних з подій безпеки та інших джерел журналів, повного захоплення пакетів, NetFlow і кінцевих точок (через RSA NetWitness Endpoint). Система RSA NetWitness орієнтована на моніторинг, аналіз та оприлюднення в режимі реального часу на додаток до підтримки попереджувальної загрози, а також реагування на інциденти і судового розслідування. Платформа використовує комбінацію одного або кіль-

[1] EMC – американська компанія, одна з найбільших виробників систем зберігання даних для організацій і пов'язаних з ними продуктів. Заснована в 1979 р., в 2016 р. поглинена корпорацією Dell.

кох фізичних або віртуальних пристроїв для реєстрації журналів і пакетів (декодер), запитів і пошуку необроблених даних (концентратори), аналітики в реальному часі (Event Stream Analysis) і довготривалого зберігання журналів і звітів (Archiver). Гібридні пристрої, що поєднують декодери і концентратори в одну систему, доступні для невеликих середовищ. Декодери і концентратори доступні для підтримки великих і регіональних розподілених архітектур. Сервер NetWitness надає уніфікований інтерфейс для адміністрування й аналізу. Він також надає інтерфейс для звітів і аналітики шкідливих програм.

RSA Live Connect – це хмарна служба, яка забезпечує автоматичне оновлення контенту, включно з правилами виявлення, парсерами[2] пакетів і журналів, звітами і джерелами загроз. Користувачі RSA NetWitness Suite також можуть використовувати RSA NetWitness SecOps Management (модуль у рішенні RSA Archer Governance, Risk and Compliance), який додає розширений процес управління інцидентами, панелі управління і звіти.

Переваги RSA NetWitness Suite:

- Платформа RSA NetWitness об'єднує аналітику виявлення загроз і моніторинг подій, розслідування та аналіз загроз у мережевому трафіку, кінцевих точках та інших джерелах подій безпеки і журналів.
- Модульні варіанти розгортання дають змогу клієнтам вибирати моніторинг мережевого трафіку, а також можливості моніторингу та аналізу подій і журналів у міру необхідності.
- RSA Live забезпечує простий і автоматизований підхід для забезпечення безперебійної доставки інформації про загрози, контенту та інших оновлень.
- Інтеграція з RSA NetWitness SecOps Manager забезпечує уніфіковані можливості SOC.

Splunk Enterprise Security

Splunk – це багатофункціональна платформа для збору, зберігання, обробки й аналізу машинних даних. На сьогодні вона є вкрай популярною в США і в Європі і поступово виходить на інші ринки. Однією з головних особливостей платформи є те, що вона може працювати з даними практично з будь-яких джерел, що дає змогу широко застосовувати платформу в різних галузях. Одним з ключових напрямків розвитку є SIEM-система Splunk Enterprise Security.

[2] Парсери – ПЗ, що збирає та аналізує (переважно синтаксично) дані.

До складу Splunk Enterprise Security входять такі функціональні рішення:

- Incident Review – гнучкий інструмент перегляду та упорядковування інцидентів, збагачений інформацією із зовнішніх джерел.
- Investigator – візуальний інструмент виявлення Kill Chain і створення нових кореляційних пошуків на базі зібраного досвіду.
- Glass Tables – наочна побудова логічних схем ресурсів, що захищаються, з вбудованим редактором. Можливість створення індивідуально налаштованих візуалізацій з ключовими показниками роботи SOC, які змінюються в масштабі реального часу.
- Security Intelligence – великий набір наперед налаштованих інтеграцій із зовнішніми джерелами інформації про загрози, включно з інтеграцією з Facebook Threat Exchange.

Платформа Splunk може бути розгорнута як на фізичних, так і на віртуальних серверах, також користувачам доступна хмарна версія рішення. Splunk пропонує два види ліцензій: постійну і річну передплату, вартість яких прямо пропорційна обсягу оброблених даних за день, у гігабайтах.

За останні роки у зв'язку з сильним розвитком напрямків Machine Learning і Artificial Intelligence Splunk розробив та інтегрував у свій продукт окремий модуль – Splunk Machine Learning Toolkit, що дає можливість будувати розширену аналітику в області прогнозування, виявлення аномалій, кластеризації та ін. Цей модуль підвищує аналітичні можливості SIEM-системи Splunk Enterprise Security.

У середині 2015 року Splunk додав власну функціональність UEBA з придбанням Caspida, яка була перейменована в Splunk UBA (Splunk також працює з низкою інших продуктів UEBA). Більш жорстка інтеграція між продуктами Enterprise Security і UBA була введена на початку 2016 року.

Переваги Splunk:

- Splunk здійснює збір, пошук, моніторинг та аналіз різних і досить великих за обсягами даних як в режимі історичного пошуку, так і в реальному часі, видаючи швидкий результат і високу інтерактивність пошукових запитів на надзвичайно великих обсягах даних. Splunk є повноцінною Big Data платформою.
- Splunk є універсальною системою для машинних даних, яка забезпечує комплексний збір даних, їх обробку та аналіз. У такий спосіб система здатна об'єднати в собі машинні дані, бізнес-дані, призначені для користувача дані і будувати аналітику в різних розрізах, що робить її вкрай універсальною.

- Splunk використовує технологію MapReduce, що забезпечує розподіл навантажень і швидку горизонтальну масштабованість системи. Також завдяки технології MapReduce зростає її продуктивність.

Trustwave SIEM Enterprise

Trustwave пропонує два варіанти продуктів SIEM: SIEM Enterprise і Log Management Enterprise (LME), обидва доступні як у вигляді фізичних, так і віртуальних пристроїв. Trustwave LME і SIEM Enterprise надають низку опцій, що підходять для середнього та великого бізнесу. Крім того, Trustwave пропонує безліч спільно керованих або гібридних послуг, що доповнюють дані продукти управління безпекою.

За останній час Trustwave внесла низку поліпшень для основних функцій продуктів, включно з параметрами зберігання, призначеними для користувача інтерфейсом і механізмами пошуку, а також удосконаленнями, орієнтованими на керовані і багаторівневі розгортання.

Trustwave – хороший варіант для покупців, що вже використовують продукти і послуги з портфеля Trustwave, або для власників середнього бізнесу, які шукають SIEM-систему, здатну доповнити широкий набір технологій безпеки від одного постачальника.

Переваги Trustwave:

- Користувачі інших продуктів безпеки Trustwave отримають переваги від поліпшення двобічної інтеграції з технологіями у своєму портфелі, які підтримують можливості автоматичного реагування, наприклад, ізоляція скомпрометованих кінцевих точок або блокування облікових записів користувачів.
- Trustwave має один із найпростіших зразків архітектури, яка знижує навантаження на клієнтів під час розгортання і подальшого розширення.

Як зазначено в роботі [5], неможливим є порівняння систем тільки за однією ознакою, потрібна багатокритеріальна оптимізація, і результатом є не одне рішення, а парето-множина рішень. За приклад візьмемо розгляд систем від HP та IBM і зробимо висновок, що для великих організацій, холдингових структур платформами для побудови центру захисту інформації (англ. – secure operation centre (SOC)) використовується рішення від компанії HP, зважаючи на його гнучкість, багатий функціонал та стійкість до великих навантажень. Організаціям меншого масштабу рекомендовано розглянути рішення від компанії IBM. Це рішення підходить тим організаціям, що використо-

вують стандартні технології обробки інформації, і яким не потрібна специфічна гнучкість платформи для реалізації функцій SOC.

2. SIEM-система від IBM

В Україні в банківській сфері використовується система QRadar SIEM фірми IBM, про яку було подано певні загальні відомості. Розглянемо деякі більш конкретні особливості роботи з цією системою. Враховуючи досвід компанії IBM в інформаційних технологіях, можна сподіватися, що дані про роботу SIEM-системи QRadar будуть мати загальну цінність для вивчення функціонування, розгортання та роботи з SIEM-системами.

2.1. Установка QRadar SIEM

Установка системи IBM QRadar SIEM All-in-One у віртуальному середовищі VMware ESX.

Властивості системи QRadar SIEM All-in-One Virtual 3199

- До 1 000 мережевих об’єктів.
- 50 000 мережевих потоків за хвилину, залежно від ліцензії.
- 1 000 подій за секунду (EPS), залежно від ліцензії.
- 750 каналів подій (кількість пристроїв).
- Зовнішні джерела потоків NetFlow, sFlow, J-Flow.
- Колектор QFlow та моніторинг активності Layer 7.

Конфігурація ВМ для QRadar SIEM All-in-One Virtual 3199

Створюємо ВМ з такими параметрами:

- Operating System (OS) – Red Hat Enterprise Linux 6 (64-bit).
- CPU – 4 (Number of virtual sockets = 2; Number of cores per virtual socket = 2).
- Memory Size – 24 Gb (це мінімальна системні вимоги, хоча і при 16 Gb працювати буде).
- SCSI controller – VMware Paravirtual.
- Disk – 256 Gb чи вище (залежить від обсягу подій, які потрібно зберегти).

Установка системи QRadar SIEM All-in-One Virtual 3199

Підключаємо ISO файл та завантажуємося з нього. Тест медіа можна пропустити.

Далі почнеться автоматична установка. Після закінчення отримаємо повідомлення:

```
OK: qsetup is completed.
Type HALT to shutdown or SETUP to login and configure
system
```

Вводимо команду SETUP для початкової конфігурації системи. При запиті авторизації вводимо root (пароль не запитується). Уважно прочитуємо ліцензійну угоду або тиснемо Alt+Q та погоджуємося.

Далі потрібно ввести ключ продукту. Саме цей ключ визначає який модуль (модулі) буде функціонувати на конкретно цій системі.

Система перевірить відповідність ключа та доступність системних ресурсів (якщо системних ресурсів недостатньо – ключ не буде прийнято).

Наступним кроком обираємо звичайне налаштування (а не відновлення).

Також обираємо (хоча він у нас всього один) шаблон тюнінгу (tuning template).

Налаштування дати і часу; використовуємо NTP сервер (ntp.time.in.ua – stratum 1).

Обираємо часовий пояс.

Обираємо версію IP протоколу та менеджмент-інтерфейс.

Вказуємо ім'я хоста та налаштування мережевого інтерфейсу.

Вказуємо пароль для root, а потім і його підтвердження.

Тепер система буде застосовувати наші налаштування та конфігурувати обрані ключем модулі. Це займає досить багато часу, але не більше години.

Перевірка встановленої QRadar SIEM All-in-One Virtual 3199.

Після завершення відбудеться перезавантаження, і консоль буде доступна за адресою https://<ip>. Для авторизації потрібно використовувати логін admin і пароль, який ми задавали для root.

Детальніше про установку можна дізнатися з офіційної документації: **IBM Security QRadar Installation Guide.**

2.2. Мета QRadar SIEM

Завдання ліцензійної програми IBM Security QRadar SIEM:

- Оголошення про підозрілі дії та порушення у IT-середовищі.
- Забезпечення прозорості дій у мережі, активності користувачів та додатків.
- Зіставлення важливих для безпеки даних із різних джерел у контексті один з одним.
- Надання шаблонів звітів для оперативності та відповідності вимогам.
- Забезпечення надійного, захищеного від зламу, сховища для журналів, що призначені для криміналістичних досліджень та використані як докази у суді.

Виявлення можливих атак та порушень політики безпеки

QRadar SIEM дає відповідь на такі ключові питання:

- Що є метою нападу?
- Який вплив надає небезпека?
- Хто атакує?
- Де має бути зосереджене розслідування?

- Коли відбувалися атаки?
- Як атака проникає у систему?
- Можлива атака / порушення є дійсною чи хибною тривогою?

Основні можливості QRadar SIEM

- Можливість обробляти дані за напрямом безпеки від широкого спектру джерел, наприклад:
  - брандмауери;
  - каталоги користувачів;
  - проксі;
  - додатки;
  - маршрутизатори.
- Збір, нормалізація, кореляційна обробка та безпечне збереження подій без обробки, мережеві потоки, вразливості, активи та дані розвідки.
- Захоплення корисного навантаження 7 рівня до визначеної кількості байтів з незашифрованого трафіку.
- Можливості пошуку за комплексом параметрів
- Моніторинг поведінки хосту та мережі, які можуть вказувати на атаку або порушення політики безпеки, наприклад:
  - використання додатків або у неробочий час або невідповідно до шаблонів мережевої активності, які задокументовані раніше;
  - визначення пріоритетів можливих атак або порушень політики безпеки.
- Повідомлення в електронній пошті, SNMP та інші.
- Багато загальних шаблонів звітів.
- Архітектура, що може масштабуватися задля підтримки великих систем.
- Однаковий інтерфейс користувача .

2.3. Збір та обробка подій та потоків

Нормалізація необроблених подій

- Подія – це запис з пристрою, який описує дію на мережу або хост.
- QRadar SIEM нормалізує різноманітну інформацію, яку було знайдено у необробленій події.
  - Нормалізація означає відображення інформації на загальні імена полів, наприклад:
    – SRC_IP, Source, IP та інші нормалізуються до Source IP;
    – user_name, username, login та інші нормалізуються до User.
  - Нормалізовані події відображаються у категорії вищого або нижчого рівня задля полегшення подальшої обробки.
- Після нормалізації необроблених подій можна легко виконати пошук, запис та взаємну кореляційну обробку подій.

Збирання та обробка подій

- Джерела журналів здебільшого відправляють повідомлення у форматі системного журналу, але можливе використання й інших протоколів.

- Збирачі подій отримують необроблені події у вигляді журналу повідомлень від різноманітних джерел.
  - Модулі підтримки пристроїв (Device Support Modules – DSM) у складі збирачів подій розбирають та нормалізують необроблені події, журнал необроблених подій залишається недоторканими.
- Оброблювачі подій отримують нормалізовані події а також необроблені події для аналізу та зберігання .
- Вузли даних забезпечують додаткове зберігання для подій та потоків даних.
- Магістрат виконує кореляційний аналіз в обробнику даних та створює повідомлення про порушення (рис. 3).

Збирання та обробка потоків

- Потік – сесія зв'язку між двома хостами.
- Колектори QFlow читають пакети з ліній або ті, що отримані іншими пристроями.
- Коллектори QFlow перетворюють вусі зібрані мережеві дані у записи потоків, подібні до записів нормалізованих подій; вони містять такі деталі: у який спосіб, хто, коли, скільки, за якими протоколами та з якими опціями передавав дані (рис. 4).

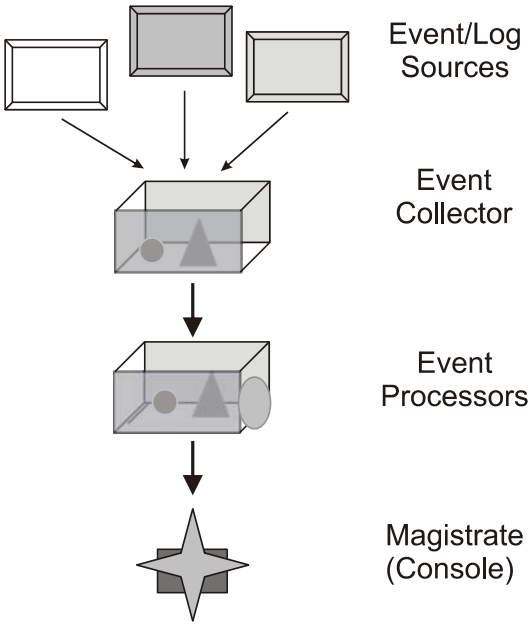

Рис. 3. Збирання подій

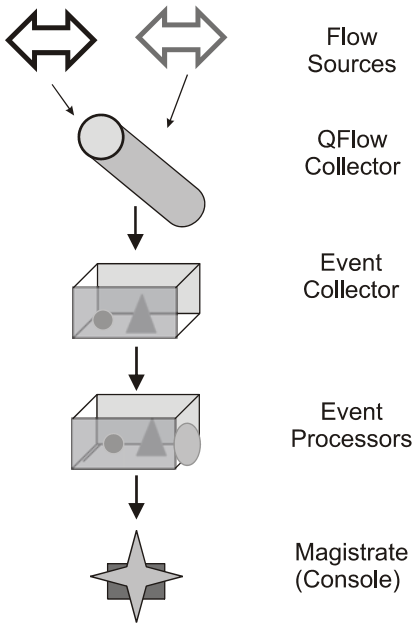

Рис. 4. Збирання потоків

Складання звітів

- Уся зібрана інформація може використовуватися для складання звітів.
- У наявності є тисячі шаблонів звітів.
- Використовуючи «майстра звітів» ви можете створювати нові шаблони звітів та змінювати наявні.

Профілі активів

QRadar SIEM підтримує профілі активів для систем у мережі; профілі відстежують деталі хосту, наприклад, такі:

- IP-адреси;
- послуги прослуховування на відкритих портах;
- вразливості.

Активні сканери

Для оцінки вразливості (VA) та підтримки профілів активів QRadar SIEM інтегрується з багатьма активними сканерами

- можливо спланувати використання Nessus, Nmap и IBM Security QRadar Сканер Vulnerability Manager безпосереднь у QRadar SIEM;
- для інших сканерів можливо підключення тільки збирання результатів сканування до QRadar SIEM, але не самого процесу сканування.

3. Принципи роботи міжмережевих екранів

Міжмережевий екран являє собою локальний (однокомпонентний) або функціонально-розподілений засіб (комплекс), який реалізує контроль за інформацією, що надходить у комп'ютерну систему і / або виходить з неї, і забезпечує захист комп'ютерної системи за допомогою фільтрації інформації, тобто її аналізу за сукупністю критеріїв і прийняття рішення про її поширення в (з) комп'ютерні системи [6].

Ми будемо використовувати поняття міжмережевий екран (МЕ), брандмауер, firewall, шлюз із встановленим додатковим програмним забезпеченням firewall, як еквівалентні.

Формальна постановка задачі екранування полягає в такому: нехай є дві множини інформаційних систем. Екран – це засіб розмежування доступу клієнтів з однієї множини до серверів з іншої множини. Екран здійснює свої функції, контролюючи всі інформаційні потоки між двома множинами систем (рис. 5). Контроль потоків полягає в їх фільтрації, можливо, з виконанням деяких перетворень.

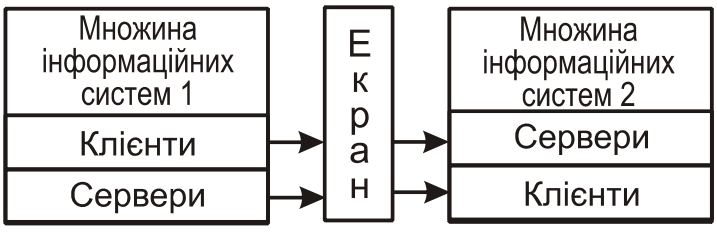

Рис. 5. Екран як засіб розмежування

На наступному рівні деталізації екран (який можна уявити як напівпроникну мембрану) зручно представляти як послідовність філь-

трів. Кожен із фільтрів, проаналізувавши дані, може затримати (не пропустити) їх, а може і відразу перекинути за екран. Крім того, допускається перетворення даних, передача порції даних на наступний фільтр для продовження аналізу або обробка даних від імені адресата і повернення результату відправнику (рис. 6).

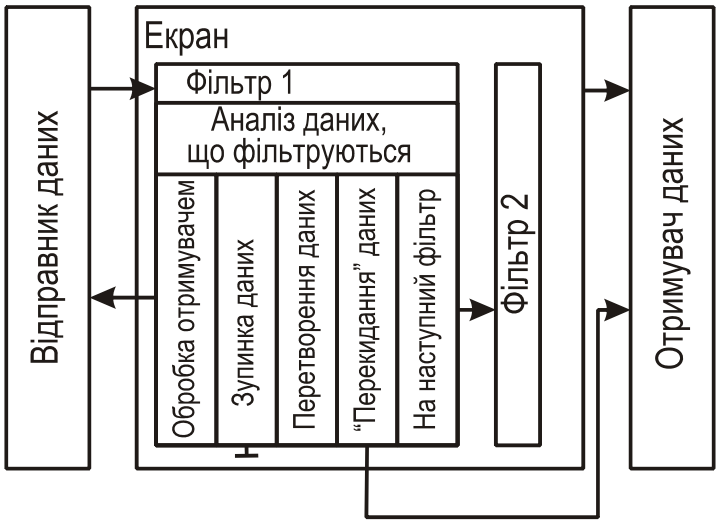

Рис. 6. Екран як послідовність фільтрів

Крім функцій розмежування доступу, екрани здійснюють протоколювання обміну інформацією.

Міжмережевий екран (МЕ) розташовується між тією, що захищається (внутрішньою) мережею і зовнішнім середовищем (зовнішніми мережами або іншими сегментами корпоративної мережі). У першому випадку говорять про зовнішній МЕ, у другому – про внутрішній. Брандмауер – ідеальне місце для вбудовування засобів активного аудиту. МЕ здатний реалізувати як завгодно потужну реакцію на підозрілу активність, аж до розриву зв'язку із зовнішнім середовищем.

На міжмережевий екран доцільно покласти ідентифікацію / аутентифікацію зовнішніх користувачів, які потребують доступу до корпоративних ресурсів (з підтримкою концепції єдиного входу в мережу).

В силу принципів ешелонування оборони для захисту зовнішніх підключень зазвичай використовується двокомпонентне екранування (рис. 6). Первинна фільтрація (наприклад, пакетів з певними IP-адресами, включеними в чорний список) здійснюється граничним маршрутизатором, за яким розташовується так звана демілітаризована зона (мережа з помірною довірою безпеки, куди виносяться зовнішні

інформаційні сервіси організації – Web, електронна пошта тощо) і основний МЕ, що захищає внутрішню частину корпоративної мережі.

Теоретично міжмережевий екран (особливо внутрішній) має бути багатопротокольним, однак на практиці домінування сімейства протоколів TCP / IP настільки велике, що підтримка інших протоколів видається надмірністю, шкідливою для безпеки (чим складніший сервіс, тим він більш вразливий).

Зовнішній і внутрішній міжмережевий екран можуть стати вузьким місцем, оскільки обсяг мережевого трафіку має тенденцію швидкого зростання. Один із підходів до вирішення цієї проблеми передбачає розбиття МЕ на кілька апаратних частин і організацію спеціалізованих серверів-посередників. Основний міжмережевий екран може проводити грубу класифікацію вхідного трафіку за видами і передоручати фільтрацію відповідним посередникам (наприклад, посереднику, що аналізує HTTP-трафік). Вихідний трафік спочатку обробляється сервером-посередником, який може виконувати і функціонально корисні дії – кешування сторінок зовнішніх Web-серверів, що знижує навантаження на мережу взагалі і основний МЕ зокрема.

Ситуації, коли корпоративна мережа містить лише один зовнішній канал, є більше винятком, ніж правилом. Найчастіше корпоративна мережа складається з кількох територіально рознесених сегментів, кожен із яких підключений до Internet. У цьому разі кожне підключення має захищатися своїм екраном. Можна вважати, що корпоративний зовнішній міжмережевий екран є складовим (розподіленим), і потрібно вирішувати задачу погодженого адміністрування всіх компонентів.

Існують також персональні МЕ, призначені для захисту окремих комп'ютерів. Головна відмінність персонального брандмауера від розподіленого – наявність функції централізованого управління. Якщо персональні міжмережеві екрани управляються тільки з того комп'ютера, на якому вони встановлені та ідеально підходять для домашнього застосування, то розподілені міжмережеві екрани можуть управлятися централізовано, з єдиної консолі управління. Такі відмінності дали змогу деяким виробникам випускати свої рішення у двох версіях – персональній (для домашніх користувачів) і розподіленій (для корпоративних користувачів).

Існує два основні способи створення наборів правил брандмауера: «включає» і «виключає». Той міжмережевий екран, що виключає, дозволяє проходження всього трафіку, за винятком трафіку, відповідного набору правил. Міжмережевий екран, що включає, діє прямо протилежним чином. Він пропускає тільки трафік, відповідний правилам, і блокує все інше. Такі міжмережеві екрани зазвичай більш безпечні,

ніж ті, що виключають, оскільки вони суттєво зменшують ризик пропуску фаєрволом небажаного трафіку.

Безпека може бути додатково підвищена з використанням «брандмауера зі збереженням стану». Такий міжмережевий екран зберігає інформацію про відкриті з'єднання і дозволяє тільки трафік через відкриті з'єднання або відкриття нових з'єднань. Недолік брандмауера зі збереженням стану в тому, що він може бути уразливий для атак DoS (Denial of Service, відмова в обслуговуванні), якщо безліч нових з'єднань відкривається дуже швидко. Більшість міжмережевих екранів дають можливість комбінувати поведінку зі збереженням стану і без збереження стану, що оптимально для реальних застосувань.

4. Висновки

У цьому методичному посібнику окреслено основи використання і побудови SIEM систем для збору та обробки інформації про стан інформаційної безпеки, а також розглянуто міжмережеві екрани як один із найпоширеніших засобів захисту інформації. Проблемам інформаційної безпеки приділяється значна увага у вітчизняній науковій періодиці, студентам можуть бути корисні роботи [7-9].

Може бути корисним короткий глосарій термінів з інформаційної безпеки.

Глосарій

Автентифікація (authentication) – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.

Автоматизована система; АС (automated system) – організаційно-технічна система, що реалізує інформаційну технологію таі об'єднує ОС, фізичне середовище, персонал, інформацію, яка обробляється.

Авторизація (authorization) – надання повноважень; встановлення відповідності між повідомленням (пасивним об'єктом) і його джерелом (це користувач або процесс, що створили повідомлення).

Авторизований користувач (authorized user) – користувач, що володіє певними повноваженнями.

Адміністративна конфіденційність (mandatory confidentiality) – послуга, що забезпечує конфіденційність інформації відповідно до принципів адміністративного керування доступом.

Адміністративна цілісність (mandatory integrity) – послуга, що забезпечує цілісність інформації відповідно до принципів адміністративного керування доступом.

Адміністративне керування доступом (mandatory access control) – принцип керування доступом, який полягає в тому, що керувати потоками інформації між користувачами і об'єктами дозволено тільки спеціально авторизованим користувачам, а звичайні користувачі не мають можливості створити потоки інформації, які могли б призвести до порушення встановлених ПРД.

Адміністратор захисту (безпеки) інформації (security administrator) – особа, відповідальна за захист автоматизованої системи від несанкціонованого доступу до інформації.

Активна загроза (active threat) – загроза навмисної несанкціонованої зміни стану системи.

Аналіз прихованих каналів (covert channels analyse) – послуга, яка забезпечує гарантію того, що приховані канали в КС відсутні, знаходяться під наглядом або, принаймні, відомі.

Аналіз процедур захисту (security analysis) – незалежний перегляд і аналіз системних записів і активностей з метою перевірки їх адекватності системним керуючим функціям для забезпечення відповідності з прийнятою стратегією захисту й операційними процедурами, виявлення прогалин у захисті і видачі рекомендацій за будь-якими із зазначених змін в управлінні, стратегії і процедурах.

Аналіз ризику (risk analysis) – систематичне використання інформації для виявлення джерел і оцінки ризику.

Аналіз ризику (risk analysis) – процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеня їх прийнятності для експлуатації АС.

Атака (attack) – спроба реалізації загрози.

Атрибут доступу (tag, access mediation information) – будь-яка зв'язана з об'єктом КС інформація, яка використовується для керування доступом.

Безпека інформації (information security) – стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації.

Відкат (rollback) – послуга, що забезпечує повернення об'єкта КС до відомого попереднього стану після виконання над об'єктом певної операції або серії операцій.

Відкритий текст (clear text) – дані з доступним семантичним змістом.

Відмова в обслуговуванні (denial of service) – будь-яка дія або послідовність дій, що призводять будь-яку частину (компонент) системи до виходу із ладу; нездатність системи виконувати свої функції (надавати декларовані послуги) внаслідок виходу із ладу якого-небудь компонента або інших причин.

Відмова (fault, failure) – втрата здатності КС або її компонента виконувати певну функцію.

Відмова від авторства (repudiation of origin) – заперечення причетності до утворення або передачі якого-небудь документа чи повідомлення.

Відмова від одержання (repudiation of receipt) – заперечення причетності до одержання якого-небудь документа або повідомлення.

Вразливість системи (system vulnerability) – нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Втрата інформації (information leakage) – неконтрольоване розповсюдження інформації, що веде до її несанкціонованого одержання.

Гарантії (assurance) – сукупність вимог (шкала оцінки) для визначення міри упевненості, що КС коректно реалізує політику безпеки.

Диспетчер доступу (reference monitor) – реалізація концепції абстрактного автомата, яка забезпечує дотримання ПРД і характеризується такими трьома особливостями: забезпечує безперервний і повний контроль за доступом, захищений від модифікації і має невеликі розміри.

Довірча конфіденційність (discretionary confidentiality) – послуга, що забезпечує конфіденційність інформації відповідно до принципів довірчого керування доступом.

Довірча цілісність (discretionary integrity) – послуга, що забезпечує цілісність інформації відповідно до принципів довірчого керування доступом.

Довірче керування доступом (discretionary access control) – принцип керування доступом, який полягає в тому, що звичайним користувачам дозволено керувати (довіряють керування) потоками інформації між іншими користувачами і об'єктами свого домена (наприклад, на підставі права володіння об'єктами) без втручання адміністратора.

Домен комп'ютерної системи; домен КС (domain) – ізольована логічна область КС, що характеризується унікальним контекстом, всередині якої об'єкти володіють певними властивостями, повноваженнями і зберігають певні відносини між собою.

Достовірний канал (trusted path) – захищений шлях передачі інформації між користувачем і КЗЗ, що не може бути імітований, а інформація, що передається ним, не може бути отримана або модифікована стороннім користувачем або процесом.

Доступ до інформації (access to information) – вид взаємодії двох об'єктів КС, внаслідок якого створюється потік інформації від одного об'єкта до іншого і / або відбувається зміна стану системи.

Доступність (availability) – властивість ресурсу системи (КС, послуги, об'єкта КС, інформації), яка полягає в тому, що користувач і / або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому необхідний.

Експорт інформації (information export) – виведення інформації з-під керування КЗЗ назовні.

Журнал реєстрації (audit trail) – упорядкована сукупність реєстраційних записів, кожен із яких заноситься КЗЗ за фактом здійснення контрольованої події.

Завірення (notarization) – реєстрація даних у довіреної третьої особи з метою забезпечення надалі впевненості у правильності таких характеристик: зміст, джерело даних, час відправлення чи одержання тощо.

Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і / або нанесення збитків АС.

Залишковий ризик (residual risk) – ризик, що залишається після впровадження заходів забезпечення безпеки.

Запит на доступ (access request) – звернення одного об'єкта КС до іншого з метою отримання певного типу доступу.

Засоби захисту (protection facility) – програмні, програмно-апаратні та апаратні засоби, що реалізують механізми захисту.

Захист від несанкціонованого доступу; захист від НСД (protection from unauthorized access) – запобігання або істотне утруднення несанкціонованого доступу до інформації.

Захист інформації в АС (information protection, information security, computer system security) – діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС загалом, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків внаслідок реалізації загроз.

Захищена комп'ютерна система; захищена КС (trusted computer system, trusted computer product) – комп'ютерна система, яка здатна забезпечувати захист оброблюваної інформації від певних загроз.

Заходи забезпечення безпеки (safeguards) – послуги, функції, механізми, правила і процедури, призначені для забезпечення захисту інформації.

Зашифрування даних (data encryption) – процес перетворення відкритого тексту у шифртекст.

Збирання сміття – загроза, що полягає в захопленні й аналізі користувачем або процесом спільно використовуваних об'єктів, звільнених іншим користувачем чи процесом, з метою одержання інформації, що в них знаходиться.

Ідентифікатор об'єкта КС (object identifier) – унікальний атрибут об'єкта КС, що дозволяє однозначно виділити даний об'єкт серед подібних.

Ідентифікація (identification) – процедура присвоєння ідентифікатора об'єкта КС або встановлення відповідності між об'єктом і його ідентифікатором; впізнання.

Імітовставка (data authentication code) – блок інформації фіксованої довжини, що одержується із відкритого тексту і ключа, однозначно відповідний даному відкритому тексту.

Імпорт інформації (information import) – уведення інформації ззовні під керування КЗЗ.

Ініціалізація (initialization) – встановлення системи або об'єкта у відомий чи визначений стан.

Інформація автентифікації (authentication information) – інформація, що використовується для автентифікації.

Категорія доступу (security level) – комбінація ієрархічних і неієрархічних атрибутів доступу, що відображає рівень критичності (наприклад, конфіденційності) інформації або повноважень користувача щодо доступу до такої інформації.

Квота (quota) – обмеження можливості використання певного ресурсу КС користувачем або процесом.

Керування доступом (access control) – сукупність заходів із визначення повноважень і прав доступу, контролю за додержанням ПРД.

Керування потоками (flow control) – сукупність функцій і процедур, які забезпечують неможливість передачі інформації прихованими каналами, тобто в обхід КЗЗ. У більш вузькому значенні часто розуміється сукупність процедур, які забезпечують неможливість передачі інформації від об'єкта КС з більш високим рівнем доступу до об'єкта КС з більш низьким рівнем доступу.

Керування ризиком (risk management) – сукупність заходів, що проводяться протягом всього життєвого циклу АС щодо оцінки ризику, вибору, реалізації і впровадження заходів забезпечення безпеки, спрямована на досягнення прийнятного рівня залишкового ризику.

Ключ (key) – конкретний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму.

Комп'ютерний вірус (computer virus) – програма, що володіє здатністю до самовідтворення і зазвичай здатна здійснювати дії, які можуть порушити функціонування КС і / або зумовити порушення політики безпеки.

Комплекс засобів захисту; КЗЗ (trusted computing base; TCB) – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Комплексна система захисту інформації; КСЗІ – сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Компрометація (compromise) – порушення політики безпеки; несанкціоноване ознайомлення.

Конфіденційність інформації (information confidentiality) – властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем або процесом.

Користувач (user) – фізична особа, яка може взаємодіяти з КС через наданий їй інтерфейс.

Криптографічне перетворення – перетворення даних, яке полягає в їх шифруванні, вироблення імітовставки або цифрового підпису.

Критерії оцінки захищеності; критерії (security evaluation criteria) – сукупність вимог (шкала оцінки), що використовується для оцінки ефективності функціональних послуг безпеки і коректності їх реалізації.

Критична інформація (sensitive information) – інформація, що вимагає захисту; будь-яка інформація, втрата або неправильне використання якої (модифікація, ознайомлення) може нанести шкоду власникові інформації або АС, або будь-якій іншій фізичній (юридичній) особі чи групі осіб.

Люк (trap door) – залишені розробником недокументовані функції, використання яких дозволяє обминути механізми захисту.

Матриця доступу (access matrix) – n-мірна таблиця, вздовж кожного виміру якої відкладені ідентифікатори об'єктів КС одного типу (суб'єктів-користувачів, об'єктів-процесів чи пасивних об'єктів), і містить як елементи права доступу кожного суб'єкту до кожного із суб'єктів або об'єктів.

Механізми захисту (security mechanism) – конкретні процедури і алгоритми, що використовуються для реалізації певних функцій і послуг безпеки.

Мітка (label) – атрибут доступу, що відображає категорію доступу об'єкта КС.

Модель загроз (model of threats) – абстрактний формалізований або неформалізований опис методів і засобів здійснення загроз.

Модель політики безпеки (security policy model) – абстрактний формалізований або неформалізований опис політики безпеки інформації.

Модель порушника (user violator model) – абстрактний формалізований або неформалізований опис порушника.

Модифікація (modification) – зміна користувачем або процесом інформації, що міститься в об'єкті.

Невизнання участі (repudiation) – відмова одного з об'єктів КС від факту участі в події, що трапилася.

Несанкціонований доступ до інформації; НСД до інформації (unauthorized access to information) – доступ до інформації, здійснюваний з порушенням ПРД.

Об'єкт комп'ютерної системи; об'єкт КС (product object, system object) – елемент ресурсу КС, що знаходиться під керуванням КЗЗ і характеризується певними атрибутами і поводженням.

Об'єкт-користувач (user object) – подання фізичного користувача в КС, що створюється в процесі входження користувача в систему і повністю характеризується своїм контекстом (псевдонімом, ідентифікаційним кодом, повноваженнями і т. ін.).

Об'єкт-процес (process object) – виконувана в цей момент програма, яка повністю характеризується своїм контекстом (поточним станом регістрів обчислювальної системи, адресним простором, повноваженнями і т. ін.).

Оцінка безпеки інформації (information security evaluation) – процес, метою якого є визначення відповідності стану безпеки інформації в КС встановленим вимогам.

Оцінка вразливості (vulnerability assessment) – дослідження об'єкта оцінки з метою визначення можливості реалізації загроз.

Очищення пам'яті (memory clearing) – знищення даних у пам'яті шляхом встановлення полів цих даних у заданий або випадковий стан.

Пароль (password) – секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації.

Пасивний об'єкт (passive object) – об'єкт КС, який в конкретному акті доступу виступає як пасивний компонент системи, над яким виконується дія і / або який служить джерелом чи приймальником інформації.

Персональний ідентифікаційний номер; ПІН (personal identification number, PIN) – вид паролю, що звичайно складається тільки із цифр, і який зазвичай має бути пред'явлений нарівні з фізичним ідентифікатором (карткою або ін.).

Повноваження (privilege) – права користувача або процесу на виконання певних дій, зокрема на одержання певного типу доступу до об'єктів.

Повторне використання об'єкта (object reuse) – послуга, що забезпечує очищення пам'яті і призупинення дії повноважень щодо розділюваного об'єкта, який раніше використовувався одним користувачем або процесом, перед наданням його іншому користувачеві або процесу.

Політика безпеки інформації (information security policy) – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Політика безпеки послуги (service security policy) – правила, згідно з якими функціонують механізми, що реалізують послугу.

Порушник (user violator) – користувач, який здійснює несанкціонований доступ до інформації.

Послуга безпеки (security service) – сукупність функцій, що забезпечують захист від певної загрози або від множини загроз.

Потік інформації (information flow) – передавання інформації від одного до іншого об'єкта КС.

Правила розмежування доступу; ПРД (access mediation rules) – частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів.

Право доступу (access right) – дозвіл або заборона здійснення певного типу доступу.

Прихований канал (covert channel) – спосіб одержання інформації за рахунок використання шляхів передачі інформації, наявних у КС, але не керованих КЗЗ, або спостереження за наявними потоками інформації.

Програмна закладка (program bug) – потайно впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу КЗЗ і / або порушення політики безпеки.

Проникнення (penetration) – успішне подолання механізмів захисту системи.

Пропускна здатність прихованого каналу (covert channel bandwidth) – кількість інформації, що одержується використанням прихованого каналу за одиницю часу.

Реєстрація (audit, auditing) – послуга, що забезпечує збирання і аналіз інформації щодо використання користувачами і процесами функцій і об'єктів, контрольованих КЗЗ.

Рейтинг (rating) – упорядкований перелік рівнів послуг і рівня гарантій, виявлених у процесі оцінки КС.

Ризик (risk) – функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Рівень гарантій (assurance level) – міра упевненості в тому, що КС коректно реалізує політику безпеки.

Рівень допуску (clearance) – ієрархічна частина категорії доступу користувача або процесу, що визначає максимальний рівень доступу пасивного об'єкта, до якого може одержати доступ користувач чи процес.

Рівень доступу (access level) – ієрархічна частина категорії доступу пасивного об'єкта.

Рівень послуги (level of service) – міра ефективності і / або стійкості механізмів, що реалізують послугу, відносно до введеної для цієї послуги шкали оцінки.

Розділюваний об'єкт (shared object) – об'єкт КС, який одночасно або почергово використовується різними користувачами і/або процесами.

Розмежування доступу (access mediation) – сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу.

Розшифрування даних (data decryption) – процес перетворення шифртексту у відкритий текст.

Роль користувача (user role) – сукупність функцій щодо керування КС, КЗЗ і обробки інформації, доступних користувачеві.

Санкціонований доступ до інформації (authorized access to information) – доступ до інформації, що не порушує ПРД.

Список доступу (access control list) – перелік користувачів і / або процесів з зазначенням їх прав доступу до об'єкта КС, з яким пов'язаний цей перелік.

Список повноважень (privilege list, profile) – перелік об'єктів із зазначенням прав доступу до них з боку користувача або процесу, з яким пов'язаний цей перелік.

Спостереженість (accountability) – властивість КС, що дає змогу фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення політики безпеки і / або забезпечення відповідальності за певні дії.

Стійкість до відмов (fault tolerance) – послуга, що забезпечує здатність КС продовжувати функціонування в умовах виникнення збоїв і відмов окремих компонентів.

Тестування на проникання (penetration testing) – випробування, метою яких є здійснення спроби обминути або відключити механізми захисту.

Тип доступу (access type) – суттєвість доступу до об'єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис).

Троянський кінь (Trojan horse) – програма, яка, будучи авторизованим процесом, окрім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми.

Функціональний профіль (functionality profile) – упорядкований перелік рівнів функціональних послуг, який може використовуватись як формальна специфікація функціональності КС.

Цифровий підпис (digital signature) – дані, одержані в результаті криптографічного перетворення блоку даних і / або його параметрів (хеш-функції, довжини, дати утворення, ідентифікатора відправника і т. ін.), що дають змогу приймальнику даних впевнитись у цілісності блоку і справжності джерела даних та забезпечити захист від підробки і фальсифікації.

Цілісність інформації (information integrity) – властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і / або процесом.

Цілісність системи (system integrity) – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий із порушенням політики безпеки.

Шифртекст (ciphertext) – дані, отримані у результаті зашифрування відкритого тексту.

Шифрування даних – процес шифрування або розшифрування.

Ядро захисту (security kernel) – частина КЗЗ, в якій зосереджено мінімально необхідний набір механізмів, що реалізують ПРД.

Література

1. https://www.gartner.com/doc/480703/improve-it-security-vulnerability-management. 11.04.1019
2. https://uk.wikipedia.org/wiki/Security information_and event management (SIEM)
3. http://www.infobezpeka.com/publications/?id=589. 08.08.2019
4. http://www.infobezpeka.com/publications/?id=589
5. Столова О. В. Методика порівняння ефективності сучасних SIEM-систем. http://ela.kpi.ua/bitstream/123456789/20810/1/13.%D0%A1%D1%82%D0%BE%D0%BB%D0%BE%D0%B2%D0%B0.163-164.pdf
6. Інформаційна безпека: навч. посібник /Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник, А.П. Бондарев та ін; за заг. ред. Ю.Я. Бобало та І.В. Горбатого. – Львів: Видавництво Львівської політехніки, 2019.–580 с.
7. Tereykovsky I., Korchenko A., Parashchuk T., Pedchenko Y., Open intrusion detection systems analysis // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 3, pp. 201-216. (In Ukranian)
8. Marushchak A., Skitsko O. The influence of Shadow Information Technology on the cyber security of business entity // Ukrainian Scientific Journal of Information Security, 2018, vol. 24, issue 1, p. 69-74. (In Ukranian)
9. Баглай Р.О. Загрози безпеки хмарних технологій для банків. Системи обробки інформації, 2018, випуск 1 (152). С. 127-135.

ЗМІСТ

Навчальне видання

Крижановський Володимир Григорович
Сергієнко Сергій Петрович

Апаратно-програмні засоби захисту інформації у корпораціях

Навчально-методичний посібник

Редактор Чернов Д. В.
Технічний редактор Колесникова І.М.

Підписано до друку 02.09.2019
Формат 60 х 84/16. Папір офсетний.
Друк – цифровий. Умовн. друк. арк. 1,6
Тираж 10 прим. Зам.

Донецький національний університет імені Василя Стуса
21021, м. Вінниця, 600-річчя, 21
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру серія ДК № 5945 від 15.01.2018