Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки

Владислав Ушатов[1], Олександр Сєвєрінов[2]

1. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м Харків, пр. Науки, 14, E-mail: vladyslav.ushatov@nure.ua

2. Кафедра безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, УКРАЇНА, м Харків, пр. Науки, 14, E-mail: oleksandr.sievierinov@nure.ua

Коротка анотація – The issues of the effective use of information protection and event management systems are considered. The analysis of the problems arising when using these systems in organizations is carried out. Possible solutions to these problems used in the latest versions of SIEM systems are considered.

Ключові слова - управління інформаційною безпекою, подіями безпеки, інциденти інформаційної безпеки, SIEM.

I. Вступ

Розвиток інформаційних технологій призводить до збільшення випадків витоку інформації. Результати глобального дослідження компанії InfoWatch витоків конфіденційної інформації в першому півріччі 2019 року показали, що за даний період аналітиками було зареєстровано тисяча двісті сімдесят шість випадків витоку конфіденційної інформації, з яких 55,6% відбулися в результаті внутрішніх порушень, а 44,4% через зовнішній вплив [1]. Сукупна кількість скомпрометованих призначених для користувача даних перевищила показник першого півріччя 2018 року більш ніж в 3,6 рази і склала 8,74 млрд записів. На рисунку 1 представлений зріст числа зареєстрованих випадків витоку інформації за останні 12 років (прогноз на 2019 рік за підсумком результатів першого півріччя).

В цих умовах, а також враховуючи вимоги міжнародних стандартів, однією з важливих засобів захисту інформації стає система управління інцидентами інформаційної безпеки [2].

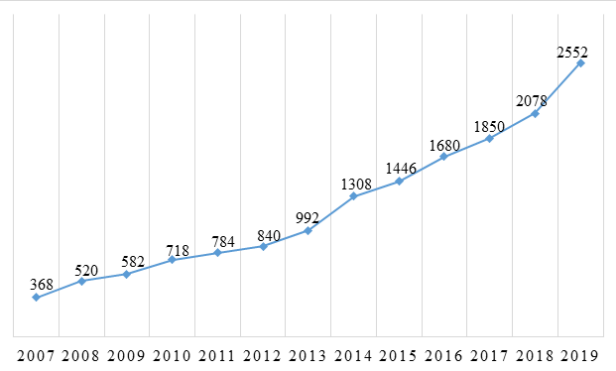

Рисунок 1 - Число зареєстрованих витоків інформації

Тому актуальним є проведення аналізу проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки.

II. SIEM - системи управління інформаційною безпекою та подіями безпеки

Незалежно від кількості вже проваджених засобів захисту в організації, якщо своєчасно не реагувати на виникаючі загрози інформаційної безпеки (ІБ), то їх ефективність буде прагнути до нуля. При цьому з ростом обсягів інформаційних потоків стрімко зростає і кількість засобів ІБ, від яких надходять дані про події інформаційної безпеки, тому встежити за рівнем безпеки організації стає все складніше і складніше.

Через величезні обсяги оброблюваних даних стає складно сфокусуватися на важливих аспектах інформаційної безпеки підприємства. Тому для оперативного виявлення і реагування на інциденти ІБ в сучасних великих підприємствах використовуються рішення класу SIEM (Security Information and Event Management, системи управління інформаційною безпекою та подіями безпеки) [3, 4] .

Функціональна модель системи SIEM об'єднує підсистеми: збору даних, попередньої їх обробки, зберігання, аналізу, уявлення. Виходячи з цього узагальнена послідовність обробки подій безпеки в рішеннях SIEM представлена на рисунку 2 [3].

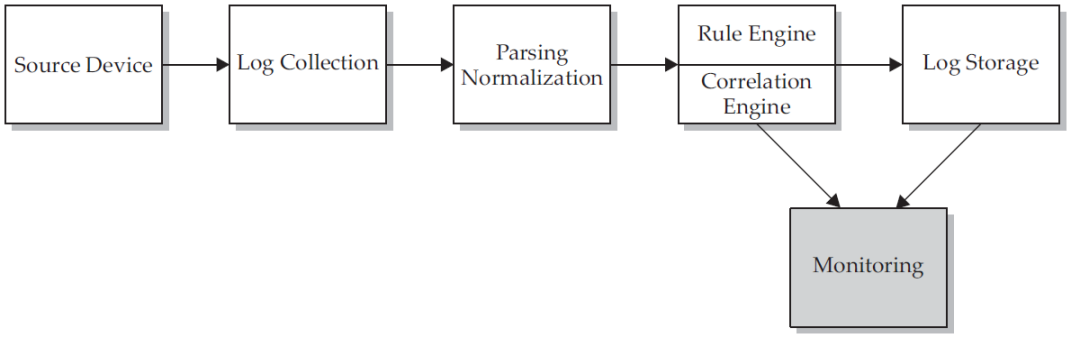

Рисунок 2 - Узагальнена послідовність обробки подій безпеки в системах SIEM

Застосовувані методи і засоби в системах SIEM розділити по функціональності на наступні основні групи: збір і агрегація (об'єднання елементів); аналіз і кореляція (знаходження взаємозв'язку); оповіщення; візуалізація; зберігання; експертний аналіз і пошук; допоміжні методи і засоби.

Системи SIEM забезпечують аналіз в реальному часі подій (інцидентів) безпеки, отриманих від мережевих пристроїв і додатків.

Через високу складність системи SIEM мають велику кількість проблем, що заважають їх ефективному застосуванню.

III. Проблеми застосування систем SIEM

Проведений аналіз показав, що одним з перших недоліків систем управління інформаційною безпекою та подіями безпеки, що заважає широкому використанню їх в малому і середньому бізнесі, є висока вартість.

Другим проблемним питанням є те, що через складність і високі вимоги системи безпеки SIEM часто не виправдовують очікування керівництва організацій і користувачів, і мета їх використання не досягається за рік і більше. За даними Gartner, компанії часто купують друге або третє SIEM-рішення, тому що чинне рішення не виправдало очікувань [5]. Відсутність необхідних ресурсів і навичок обслуговуючого персоналу (фахівців з досвідом з розслідування інцидентів, аудиту і тестів на проникнення) - найпоширеніші причини невдалих SIEM-проектів.

Наступними э низька проблем, пов'язаних з технічними питаннями застосування систем управління інформаційною безпекою та подіями безпеки. Однією з причин низької ефективності використання SIEM-систем є те, що необхідно постійно змінювати налаштування системи - для того щоб вона продовжувала збирати актуальні дані з джерел і виявляти інциденти. Ще однією проблемою – є непрацюючі правила кореляції. В інфраструктурі організації постійно відбуваються конфігураційні зміни (зміна структури мережі, підключення нових засобів, оновлення продуктів), що призводять до недійсності правил, помилкових спрацьовувань або пропуску безлічі подій. Зі змінами в інформаційній структурі доводиться додавати нові правила нормалізації, кореляції і агрегації в систему SIEM. І не завжди фахівці організації це можуть зробити самостійно – не мають досвіду або система SIEM не має такого функціоналу.

Проблемним питанням для більшості організацій є також трудовитрати на роботу з SIEM-системою. Найчастіше розмір персоналу, що обслуговує систему SIEM складає від двох до п'яти осіб, а їх час роботи з системою постійно зростає.

IV. Шляхи вирішення проблем застосування SIEM-систем

Дослідження компанії Positive Technologies показало, що на думку респондентів, знизити трудовитрати на SIEM-систему допоможуть: поставка вендором способів детектування загроз (53%); керівництво по донастройці правил для зниження кількості помилкових спрацьовувань (49%); можливість писати власні правила кореляції без вивчення спеціальної мови (44%).

Деякі розробники SIEM-систем впроваджують ці побажання в своїх виробах. Нові версії SIEM-систем мають в своєму функціоналі конструктор правил кореляції, за допомогою якого фахівці організації можуть створювати власні правила, не використовуючи будь-якої спеціальної мови програмування.

В системах SIEM з'явилася можливість проводити ретроспективний аналіз за індикаторами компрометації, що дозволяє виявляти атаки, що сталися в минулому, і запобігти їх подальшому розвитку.

Для виявлення нових загроз компанія Positive Technologies запропонувала хмарну базу знань Positive Technologies Knowledge Base (PT KB). Вона автоматично наповнює підключені SIEM новими способами виявлення компрометації в вигляді правил кореляції, агрегації, нормалізації, а також інформації про способи розслідування інцидентів.

Також останнім часом в функціонал SIEM-систем має можливості отримувати актуальні дані про стан ІБ у великій організації в будь-який момент і виявляти розподілені атаки на інфраструктуру окремого підрозділу або цілого підприємства.

Висновки

Таким чином, незважаючи на достатню кількість проблем застосування SIEM-систем ведеться активна робота по їх модернізації, що дозволяє організаціям ефективно використовувати ці системи для оперативного виявлення і реагування на інциденти інформаційної безпеки.

Література

[1] Сайт компанії InfoWatch [Електронний ресурс]. – Режим доступу: https://infowatch.com.

[2] Сєвєрінов О.В. Управління інформаційною безпекою згідно міжнародних стандартів / О.В. Сєвєрінов, В.І. Черниш, М.Є. Молчанова // Системи управління, навігації та зв'язку. – К: ДП «ЦНДІ НіУ». - 2011. – Вип. 4(20). – С. 250-253.

[3] Miller D. et al. Security information and event management (SIEM) implementation. – McGraw-Hill, 2011.

[4] Сєвєрінов О.В. Управління інцидентами інформаційної безпеки на основі використання SIEM систем / О.В. Севєрінов, В.В. Ушатов // Інформатика, управління та штучний інтелект. Тези шостої міжнародної науково-технічної конференції – Х.: НТУ «ХПІ», 2019. – С. 109.

[5] Сайт компанії Gartner [Електронний ресурс]. – Режим доступу: https://www.gartner.com/.

[6] Трудозатраты на работу в SIEM выросли у 62% специалистов по ИБ [Електронний ресурс]. – Режим доступу: https://ko.com.ua/taxonomy/term/8247.