Таким чином, порівнявши кількість найдених випадків вразливих місць коду (рис. 1). видно, що сканер, розроблений на основі удосконаленого методу, показав кращий результат, ніж аналог ZAP.

Отримані результати сканувань можна легко використати для покращення роботи просканованих web – сайтів, оскільки вони уже містять опис причин вразливостей та шляхи боротьби з ними. Усунення знайдених вразливостей неодмінно підвищить рівень безпеки перевірених сайтів.

УДК 004.56.5(043.2)

УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗА ДОПОМОГОЮ SIEM

Богдан Карачун
Державний університет телекомунікацій
info@dut.edu.ua

Жоден найдосконаліший спосіб зниження ризиків інформаційної безпеки, будь це політика безпеки, що досконально опрацьована, або найсучасніший брандмауер, не може захистити від виникнення в інформаційному середовищі подій, що потенційно несуть загрозу діяльності організації. Складність і різноманітність середовища діяльності сучасного підприємства зумовлюють наявність залишкових ризиків незалежно від якості підготовки і впровадження заходів протидії. Також завжди існує вірогідність реалізації нових, невідомих до теперішнього часу, загроз інформаційній безпеці. Неготовність організації до обробки подібного роду ситуацій може істотно ускладнити відновлення бізнес-процесів та потенційно збільшити завдані збитки.

Кількість потенційних каналів витоку інформації достатньо велика. Найбільш поширені з них відносяться до категорії ненавмисного розкриття інформації співробітниками організації з причин непоінформованості або недисциплінованості. Відсутність уявлень щодо правил роботи з конфіденційними документами, невміння визначити, які документи є конфіденційними, та звичайна неуважність при роботі з інформацією – все це може призвести до виникнення події або інциденту інформаційної безпеки.

Розглянемо декілька визначень понять події та інциденту ІБ:

1. Під подією інформаційної безпеки (ПІБ) розуміється стан системи, сервісу або мережі, котрий свідчить про можливе порушення політики безпеки, або про невідому ситуацію, яка може мати відношення до безпеки, тоді як інцидент інформаційної безпеки (ІІБ) – це одна або серія подій інформаційної безпеки, які можуть призвести до збитків та втрат для організації. Втрати можуть бути, як матеріальними(вартість інформації, експлуатаційні витрати і т.д.) так і нематеріальними (репутація організації, зміна морально-психологічного клімату і т.д.).

2. Подія інформаційної безпеки – це ідентифікований випадок стану системи або мережі, який вказує на можливе порушення політики інформаційної безпеки або відмову засобів захисту, або раніше невідому ситуацію, яка може бути суттєвою для політики безпеки. Інцидент інформаційної безпеки відповідно – це одинична

подія або ряд небажаних та непередбачених подій інформаційної безпеки, із-за яких велика ймовірність розкриття конфіденційної бізнес-інформації.

Розглянемо SIEM (Security Information and Event Management) для попередження та фіксування інцидентів:

SIEM-система може виявити можливу загрозу безпеки навіть якщо ця загроза добре замаскована під звичайну подію. Зробити це дозволяє те, що система аналізує не кожну окрему подію, а всі події в комплексі та та-ким чином може «побачити» повну картину подій зі сторони. Ця властивість може бути дуже корисною коли мова йде про систему аналізу загроз конфіденційній інформації користувачів відкритих соціальних мереж.

Така система призначена для аналізу інформації, що надходить від різних інших систем, таких як DLP, IDS, антивірусів і подальшого вияв-лення відхилення від норм за якимись критеріями. Як тільки виявлено від-хилення – генерується інцидент. В основі роботи SIEM лежить, як не див-но, майже гола математика і статистика. Будь-яких захисних функцій «го-ла» SIEM в собі не несе.

SIEM потрібна саме для збору та аналізу інформації. Інформація на-дходить з різних джерел – таких, як DLP-системи, IDS, маршрутизатори, міжмережні екрани, АРМ користувачів, серверів...

Досить клопітно вручну переглядати логи з великої кількості джерел. До того ж бувають ситуації, коли зовні нешкідливі події, отримані з різних джерел, у сукупності несуть у собі загрозу. Припустимо, коли відбувається посилання листа з чутливими для компанії даними людиною, що має на це право, але на адресу, що знаходиться поза його звичайного кола адрес, на які він відправляє. DLP система цього може не відловити, але SIEM, вико-ристовуючи накопичену статистику, на підставі цього вже згенерує інци-дент. Аналогічно, якщо один з працівників IT відділу відкритої соціа-льної мережі почав проводити листування та повідомляти третім особам, що не мають допуску до інформації, відомості про користувачів, структу-ру соціальної мережі чи програмне та технічне забезпечення, що використовується для забезпечення роботи мережі, то це відразу буде помічено си-стемою SIEM та адміністратори отримають відповідне сповіщення.

Система SIEM може виконувати такі основні функції:

- аналізувати події та створювати оповіщення при якихось ано-маліях: мережного трафіку, несподіваних дій користувача, невпізнаних пристроях і т. д.;
- перевірити на відповідність стандартам безпеки;
- створити красивий звіт. У тому числі налаштований безпосере-дньо для ваших потреб. Наприклад, щоденний звіт про інциденти, щотиж-невий звіт TOP-10 порушників, звіт з працездатності пристроїв і т. д.;
- відстежувати події, що спровоковані пристроя-ми / серверами / критично важливими системами, створювати відповідні оповіщення для зацікавлених осіб;
- зібрати доказову базу з приводу інцидентів;
- надати звіт про події в мережі без надання доступу до самої мережі, тобто адміністратор з відділу захисту інформації може відстежува-ти поведінку користувачів при тому, що не матиме ніякої можливості ознайомитися з конфіденційною інформацією власника аккаунту.

Загалом може скластися таке хибне враження, що SIEM-система є панацеєю для запобігання будь-яких загроз, але це не так. Ця система мо-же відстежувати всі

події в мережі, проте не може виконувати якихось дій крім створення попередження для адміністраторів цієї мережі, а адміністратор вже спираючись на отриманий звіт приймає рішення про подальші дії. Та все ж таки ця система може відстежувати поведінку користувачів та спираючись на статистику подій вирішити, чи потрібно адміністратору звернути більше уваги тому чи іншому користувачу. Причиною тому мо-же бути як нетипова для користувача поведінка, так і певні маркери в повідомленнях, що можуть вказувати на можливу діяльність користувача, що пов'язана з тероризмом, розповсюдженням наркотичних речовин тощо.

До того ж система SIEM лише аналізує отримані дані і працює тим краще, чим більше до неї надходить інформації з різних джерел (IDS/IPS, DLP, маршрутизатори, сервери тощо) в вигляді логів.

Література

1. Кримінальний Кодекс України, ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах(комп'ютерах), автоматизованих системах, комп'ютерних мережах, або зберігається на носіях такої інформації, вчиненні особою, яка має право доступу до неї».

2. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020-q3/Slyusar V.I. Blockchain technology in future multi-domain operations.

3. Методи виявлення інцидентів/Ukrainian Information Security journal. http://jrnl.nau.edu.ua/index.php/ZI/article/view/8798.

4. Кассето О. What is UBA, UEBA, & SIEM? Security Management Terms Defined [Електронний ресурс] / Оріон Кассето. https://www.exabeam.com/siem/uba-ueba-siem-security-management-terms-defined-exabeam/.

5. Incident Response Automation and Security Orchestration with SOAR. https://www.exabeam.com/siem-guide/incident-response-and-automation/.

УДК 004.056.53

ВИЯВЛЕННЯ РАДІОЗАКЛАДНИХ ПРИСТРОЇВ ЗА РАХУНОК ПОЄДНАННЯ МЕТОДІВ ЛОКАЛІЗАЦІЇ ЗА РІВНЕМ ПОЛЯ ТА АКУСТИЧНОГО ЗВ'ЯЗУВАННЯ

Павло Павловський, Дмитро Присяжний, Віталій Гудзь
Вінницький національний технічний університет
prepod@vntu.net, dimpris@gmail.com

Проаналізовано існуючі методи захисту інформації від витоку акустичним каналом, а також методи та засоби захисту від закладних пристроїв. Доведено доцільність поєднання методів локалізації за рівнем поля та акустичного зв'язування з метою мінімізації часових витрат на виявлення радіозакладних пристроїв. Обґрунтовано необхідність розроблення пристрою, який буде виконувати функції кількох пристроїв водночас, що визначає не лише його функціональну, але й економічну доцільність.