В результаті злагодженої роботи всіх блоків забезпечується комплексний захист інформації в критичній інфраструктурі. Механізми безпеки, використані в системі захисту інформації повинні відповідати вимогам пристроїв по продуктивності, щоб не забирати все процесорний час. Щоб довести доступність методів для використання на пристроях з обмеженою пам'яттю і продуктивністю, використовувані методи були протестовані. Тестування механізмів безпеки проводилося на емуляторі Raspberry Pi 3.

Для тестування були обрані алгоритми HMAC, хешування SHA-256, електронного підпису ECDSA. Також були поставлені експерименти з різною довжиною переданого повідомлення M на Raspberry Pi 3. Їх результати наведені в таблиці 1. На їх основі довжина в 100 байт обрана як стандартна довжина повідомлення, а довжина 1000 байт як довжина блоку поновлення.

Таблиця

Швидкість обраних алгоритмів в залежності від розміру блоку

Processor model	ECDSA-256 signatures/min	ECDSA-256 verifications/min	HMAC operations/min	SHA-256 operations/min
M=100b	220 000	131 000	3 000 000	25 850 000
M=1000b	200 000	130 000	1 500 000	5 000 000
M=10000b	108 000	122 000	255 000	822 000

На основі цих спостережень можна зробити висновок, що всі ці операції не займуть багато процесорного часу пристрою Raspberry Pi 3, дозволивши йому виконувати основну роботу по виконанню команд і посилці сигналів. З цього випливає, що перераховані вище механізми можна безболісно застосовувати для пристроїв в даній залізничній критичної інфраструктури і в багатьох інших.

Список використаних джерел

1. Merabti M. Critical Infrastructure Protection: A 21st Century Challenge / M. Kennedy, W. Hurst // Conference paper May 2011 - 7 p.
2. Ateniese G. Critical Infrastructure Protection: Threats, Attacks and Countermeasures / R. Baldoni, D. Bloisi, A. Bondavalli, F. Buccafurri, etc. // Tenace March 2014. - 169 p.

Сєвєрінов О. В., к.т.н. доцент,
Овчаренко М. Ю., бакалавр (ХНУРЕ)

АНАЛІЗ СИСТЕМ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Управління інцидентами інформаційної безпеки грає важливу роль в рішенні питань інформаційної безпеки систем критичної інфраструктури. Інцидент інформаційної безпеки це одиночна подію або ряд небажаних та непередбачених подій інформаційної безпеки, через які існує ймовірність компрометації бізнес-інформації і загрози інформаційній безпеці [1].

При забезпеченні інформаційної безпеки систем критичної інфраструктури одним з найважливіших видів діяльності є виявлення інцидентів інформаційної безпеки. При цьому актуальною є задача автоматизації процесу управління інцидентами. На сьогоднішній день відомо багато різноманітних систем управління інцидентами, серед яких найбільш поширені DLP (Data Leack Prevention), EDR (Endpoint Detection and Response), UEBA (User and Entity Behavior Analytics) та SIEM (Security Information and Event Management) системи .

User and Entity Behavior Analytics (UEBA) – клас систем, що збирають інформацію не лише про користувачів та їх ролі у системі, а також про системне оточення (робочі станції, сервери, програмне забезпечення, мережевий трафік), що дає можливість ідентифікувати більш широкий клас загроз, та формує відповідно них моделі нормальної поведінки користувача та його взаємодії з корпоративними системами [2]. Якщо дії користувача виходять за рамки побудованої моделі, UEBA-система визначає цю поведінку як аномальну та створює відповідне попередження для адміністратора безпеки. Також система надає інформацію про те, до яких систем та з якими правами певний користувач здійснював доступ, що в свою чергу дозволяє редагувати права доступу користувачів до певних цільових систем.

SIEM (Security information and event management) - програмні продукти, які об'єднують управління інформаційною безпекою SIM (Security Information Management) та управління подіями безпеки SEM (Security Event Management) та забезпечують аналіз в реальному часі подій, отриманих від мережевих пристроїв та додатків, а також журналювання даних і генерацію звітів для подальшого їх аналізу [2].

DLP (Data Leak Prevention) - технології запобігання витоку конфіденційної інформації з інформаційної

системи назовні, а також програмні або програмно-апаратні засоби для такого запобігання витокам. DLP-системи будуються на аналізі потоків даних, які перетинають периметр інформаційної системи, що захищається. При виявленні в цьому потоці конфіденційної інформації спрацьовує спеціальне програмне забезпечення системи і потік блокується.

EDR (Endpoint Detection and Response) - це нова платформа, здатна виявляти атаки на кінцеві точки і оперативно на них реагувати. Платформа EDR не тільки захищає інформаційну систему від шкідників, але і вміє моментально помічати нові загрози високої складності і одночасно проявляти реакцію на ситуацію, що виникла. Данні системи підвергають перевірці всі файли, що запускаються на кінцевій точці.

На сьогоднішній день існує велика кількість загроз інформаційній безпеці, тому використання систем управління інцидентами інформаційної безпеки є доцільним в інформаційних системах будь-якого розміру та сфери використання. Системи управління інцидентами дозволяють виявити, реагувати та аналізувати події та інциденти інформаційної безпеки, без наявності яких неможливо реалізувати рівень захищеності системи який би відповідав сучасним стандартам та галузевим вимогам [3].

Проведений аналіз показав, що системи управління інцидентами інформаційної безпеки - це наступний крок у визначенні невідомих типів загроз, цілеспрямованих атак і внутрішніх порушників. На перший план в даний час виходять SIEM-системи. Ґрунтуючись на поведінковому аналізі, ці системи здатні виявляти аномалії і неочевидні взаємодії користувачів з корпоративними системами, що дозволяє адміністраторам безпеки бачити розширену картину безпеки підприємства та оперативно реагувати на загрози.

Сьогодні лідируючі UEBA-системи мають механізми тісної інтеграції з існуючими SIEM-системами, що відкриває перед ними куди більш широкий простір для застосування. Світовий ринок UEBA-систем досить молодий і перспективний, тому виробники SIEM, EDR і DLP будуть розширювати аналітичні здібності своїх систем, в тому числі з використанням методів поведінкової аналітики або відповідних продуктів сторонніх виробників.

Список використаних джерел

1. What is User and Entity Behavior Analytics? A Definition of UEBA, Benefits, How It Works, and More. Режим доступу: https://digitalguardian.com/blog/what-user-and-entity-behavior-analytics-definition-ueba-benefits-how-it-works-and-more.
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. ISO/IEC 27001:2013 - Informational technology – Security techniques – Informational security management systems – Requirements.

Петренко Т. Г., к.т.н., доцент,
Дзюба А. А., PhD студент (УкрДУЗТ)

УДК 656.2:004

МОНІТОРИНГ РІВНЯ ВІБРАЦІЇ ЗА ДОПОМОГОЮ РОЗУМНИХ СЕНСОРІВ

Моніторинг рівня вібрації в реальному часі є актуальним. Періодичне вимірювання рівня вібрації використовується у таких галузях як будівництво та транспорт. За допомогою цих вимірювань визначається справність споруд та механізмів. Крім того рівень допустимої вібрації регулюється в Україні Держстандартом ДСН 3.3.6. 039-99. Стандарту повинні дотримуватись всі виробники та будівельники. Вимірювання параметрів вібрації є важливим і для залізничного транспорту, адже необхідно дотримуватись санітарно-гігієнічних норм у потягах та спорудах. Використовується багато різних систем моніторингу параметрів вібрації (Аврора-2000, SenSystem, LAP-LASER, Q-500, ВСВ-700). Ці системи використовують як контактні (електродинамічні та п'єзоелектричні), так і безконтактні (оптичні, електромагнітні, електричні, радіохвильові та ін.) типи датчиків. Також використовується спеціальне програмне забезпечення для аналізу даних та попередження користувача про можливі несправності. Але ці системи не є системами віддаленого моніторінгу у реальному часі.

Моніторинг рівня вібрації в реальному часу потребує впровадження нових інформаційних технологій. На залізничному транспорті моніторинг рівня вібрації в реальному часу може виявити погіршення стану залізничного полотна, безпосередньо рейок та також механізмів вагону.

Пропонуєма модель моніторингу та аналізу включає набір розумних сенсорів. Розумний сенсор це пристрій з бездротовим зв'язком що безпосередньо проводить зчитування з відповідного датчика (або кількох), виконує запис даних на запам'ятовуючий пристрій та передає дані у хмарне сховище, проводить попередній миттєвий аналіз. Тобто, у разі різкої зміни параметрів розумний сенсор може подати сигнал тривоги людині. Використання хмарного сховища дозволяє зберігати дані за потребний період часу та аналізувати як поточні дані у режимі реального часу, так і проводити аналіз за довгий час. Програми аналізу даних спроможні оцінювати поточний стан об'єкта що спостерігається, та прогнозувати подальшу динаміку розвитку показань.