Кушнір І.В., магістрант,
Фальковський І.Г., ст. викладач,
Державний університет «Житомирська політехніка»

РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ ІНФРАСТРУКТУРИ КЕРУВАННЯ ЛОГАМИ

В умовах постійного зростання обсягів даних, що генеруються пристроями та програмним забезпеченням, зберігання, обробка й моніторинг логів стають основою для своєчасного виявлення аномалій, усунення несправностей і захисту від потенційних загроз. Впровадження ефективної інфраструктури централізованого журналювання є важливим етапом у забезпеченні безпеки та стабільності IT-систем. У тезах представлено низку рекомендацій, що дозволяють оптимізувати цей процес [1].

Централізація журналювання. Дані журналів з різних джерел, таких як програми, мережеві пристрої та сервери, повинні збиратися в центральному місці для зручності аналізу та кореляції. Це допомагає спеціалістам ефективно виявляти проблеми, запобігати втраті даних та забезпечувати безпеку, знижуючи ризик видалення журналів зловмисниками та збереження їх у середовищі з автоматичним масштабуванням.

Моніторинг важливих подій. Створення списку важливих подій для моніторингу допомагає визначити, які дані потрібно фіксувати в журналах, що забезпечує зручність у відстеженні та аналізі подій. Такий список служить орієнтиром для команд, що займаються впровадженням і підтримкою систем керування логами, гарантуючи, що всі важливі дані будуть зафіксовані.

Уникання конфіденційної та непотрібної інформації. Важливо визначити, які дані потрібно журналювати, а які — ні. Залишення поза увагою конфіденційних або непотрібних даних, наприклад, особистих даних або вихідного коду, зменшує навантаження на системи і знижує ризики для витоку персональних даних і тим самим забезпечуючи відповідність стандартам безпеки, таким як GDPR або PCI DSS.

Активний моніторинг і реагування. Регулярний моніторинг журналів дозволяє виявляти аномалії та загрози в реальному часі. Це дає змогу швидко реагувати на інциденти, запобігаючи їх ескалації, і забезпечує стабільність систем, підтримуючи безперервну роботу організації [2].

Структуроване журналювання. Структуровані журнали, що записуються за визначеними форматами (наприклад, з мітками часу та рівнем важливості подій), полегшують обробку даних, роблячи їх легшими для аналізу. Це дозволяє використовувати інструменти для запитів та аналізу даних, такі як SQL, Splunk або Elastic Stack, що значно прискорює процес усунення несправностей та діагностики.

Індексація логів. Індексація журналів дозволяє швидко знаходити необхідну інформацію, що значно скорочує час реагування на проблеми. Це особливо важливо при роботі з великими обсягами даних, адже індексація допомагає виявляти тенденції, які можуть бути важко помітні у невеликих наборах інформації.

Масштабоване зберігання. Хмарне зберігання є ефективним рішенням для великих обсягів журналів, надаючи гнучкість у масштабуванні і забезпечуючи надійне зберігання даних. Це дозволяє організаціям зберігати логи тривалий час, забезпечуючи безпеку та ефективний доступ до даних для аналізу і моніторингу.

Оптимізація політики зберігання. Організації повинні розробити політики зберігання для різних типів журналів, враховуючи вимоги законодавства і власні потреби. Це включає зберігання логів для забезпечення відповідності нормативам, а також для аналізу історичних даних, що можуть бути корисні для прогнозування майбутніх навантажень або оцінки ефективності систем.

Збір з різних джерел. Для отримання повної картини подій і забезпечення ефективного моніторингу важливо збирати логи з різних джерел, таких як мережеві пристрої (комутатори, маршрутизатори), системи безпеки (міжмережеві екрани, IDS/IPS), веб-сервери, додатки і хмарна інфраструктура. Це дає змогу комплексно оцінювати стан систем та вчасно реагувати на інциденти.

В доповіді буде представлено використання рекомендацій щодо впровадження інфраструктури керування логами для застосування централізованої системи збору і обробку логів в IT-інфраструктурі.

Список використаних джерел

1. K. Kent, M. Souppaya. Guide to Computer Security Log Management // NIST Special Publication 800-92. 2006
2. Security Log Management: Challenges and Best Practices. Exabeam. URL: https://www.exabeam.com/explainers/event-logging/security-log-management-challenges-and-best-practices/ (date of access: 02.12.2024).