Полігон протестований та випробуваний під час проведення практичних навчань здобувачів освіти та перших в Україні навчаннях із кібербезпеки Grid NetWars і повністю готовий до використання.

УДК 004.77

ДОСЛІДЖЕННЯ ТА ПОРІВНЯННЯ СИСТЕМ МОНІТОРИНГУ КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

Олег Карабан
Харківський національний економічний університет імені Семена Кузнеця, oleg.karaban034@gmail.com

Сьогодні інформаційні технології (ІТ) знайшли своє місце практично у всіх сферах людської діяльності. Повсюдне використання ІТ є характерною рисою ведення сучасного бізнесу. Це пояснюється тим, що цифрові технології надають швидкий шлях для виходу продукту на ринок, ефективні зв'язки з постачальниками та клієнтами, засоби комунікації та взаємодії робітників тощо. У своєї більшості мережеві взаємодії та Інтернет стає головною складовою сучасних ІТ. Важливою рисою застосування таких ІТ є забезпечення їх кібербезпеки.

Для ефективної роботи та підтримки безпеки комп'ютерних систем і мереж слід впроваджувати системний підхід та комплекс заходів на рівні окремого комп'ютеру, серверу та мережі. Важливою складовою такого забезпечення безпеки є засоби моніторингу стану ІТ-інфраструктури.

Метою даної роботи є дослідження та порівняння систем моніторингу комп'ютерних систем і мереж шляхом розроблення та впровадження моделей та засобів інформаційних технологій й інструментів керування ІТ-інфраструктурою за умов раціонального використання її інформаційно-обчислювальних ресурсів.

Незалежно від розміру компанії, не можна ігнорувати необхідність моніторингу серверів, баз даних, мережі, безпеки, інфраструктури тощо. При цьому важливо використовувати якісні інструменти моніторингу. Моніторинг необхідний компаніям, щоб бути впевненими, що кожна система працює належним чином. Але процес моніторингу ІТ-інфраструктури буває досить клопітким й іноді викликає труднощі, якщо моніторинг не налаштований належним чином. Також, сама система моніторингу завжди є ціллю для зловмисників як потенційна точка для втручання в певний сервіс, систему тощо.

Чим активніше розвиваються ІТ-технології в окремо взятій компанії, тим виразніше можна визначити коло завдань системних адміністраторів, яким доводиться контролювати все більше процесів і стежити за станом все більшої кількості систем. Поруч з цим, для невеличкої компанії, налаштування одного серверу та забезпечення його безпеки може бути досить критичним для ефективного рішення бізнес-завдань. Тому, проблема вибору та впровадження систем моніторингу комп'ютерних систем і мереж буде актуальною незалежно від масштабу ІТ-інфраструктури підприємства чи компанії.

Можна визначити декілька рівнів систем моніторингу за сферою їх призначення та масштабу впровадження. На рівні серверу завжди є примітивні

засоби спостереження за утилізацією процесорного часу, пам'яті, процесів та мережевого трафіку й ін. Ці системи фактично є утилітами операційної системи, які на рівні окремого серверу доцільно розширити на певну кількість основних засобів, що надають дані у реальному часі. Наприклад, для операційних систем Linux є застосунок htop, що надає поточні відомості щодо роботи вузла. Наступним за масштабом та кількості спостережених даних є застосування систем моніторингу на основі циклічних баз даних (Round-robin Database, RRD). Такою є система моніторингу Cacti, яка дозволяє аналізувати дані про стан вузла та мережі. Також можна відзначити інші системи, що фактично виконують моніторинг вузла.

Для аналізу стану багатьох серверів та мереж на рівні IT-інфраструктури доцільним є впровадження спеціалізованих рішень моніторингу Nagios, Zabbix та ін. Ці системи не обмежені границями циклічних баз даних, а застосовують рішення, наприклад, реляційних баз даних промислового рівня. Також відповідні системи є модульними, завдяки застосуванню проксі-серверів дозволяють побудувати ієрархічну модель системи моніторингу й тим самим розвантажити головний вузол, що надає агреговані дані по всій мережі підприємства. Поруч з цим, слід розглянути доцільність застосування рішення Prometheus та Grafana. Фактично, це системи нового покоління, яким характерна модульність, сумісність за протоколами передачі даних, вони дозволяють налаштувати збір необхідних метрик та побудувати персоналізований інтерфейс відбиття даних.

Більшість сучасних систем моніторингу мають модель збору даних на основі залучення агентів, тому важливим є налаштування шифрування трафіку між агентом, який виконується на стороні вузла та системи моніторингу. Також для запобігання несанкціонованому втручанню слід налагоджувати ефективну систему на основі ролей користувачів, які отримають доступ до системи моніторингу та ін.

Поруч з традиційними системами моніторингу комп'ютерних систем і мереж слід враховувати важливу складову безпеки та розслідувань інцидентів – аналіз стану журналів систем та застосунків. Раніше обробку файлів логування можна було виконати тільки вручну, зараз одним з ефективних рішень є впровадження пошукових систем для аналізу текстових даних та систем відбиття результатів у зручній формі таблиць, діаграм, графіків та ін., наприклад, ELK Stack.

Для забезпечення безпеки мереж корпоративного рівня доцільно застосовувати не тільки системи моніторингу стану вузлів та складових IT-інфраструктури, а й залучати засоби, що аналізують трафік на схожість до відомих сігнатур атак, аномалії, ін. - системи запобігання вторгненням (Intrusion Prevention System, IPS) та системи виявлення атак (Intrusion Detection System, IDS). Наприклад, Snort, Suricata та ін.

Ключовим завданням систем моніторингу IT є отримання, збереження та аналіз інформації про стан елементів IT-структури компанії. Спеціальні програми моніторингу дозволяють швидко відреагувати на проблеми, що виникають в роботі IT-сервісів, а також ефективно запобігати виникненню неполадок. Від вибору комплексу рішень з моніторингу залежить ефективність та працездатність IT-інфраструктури та загальний рівень кібербезпеки компанії.

Науковий керівник – д.т.н., професор, Алексієв В.О.