УДК 004.056:355.451]:004.75

НОВІТНІ СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ І КЕРОВАНИЙ ЗАХИСТ В ХМАРНІЙ ІНФРАСТРУКТУРІ

Белозьоров С. Ю.
Науковий керівник – к.т.н., проф. Марчук В.С.
Харківський національний університет радіоелектроніки, каф. ІКІ імені В.В.Поповського,
м. Харків, Україна
тел. +380(50)-301-66-25.

The presented work is devoted to the analysis of modern intrusion detection systems and managed information protection in cloud infrastructures. Google Corporation has developed Cloud IDS intrusion detection system for its GCP cloud technologies. This system provides detection of intrusion threats, malware, spyware, and command attacks on the network. Peer-to-peer traffic is mirrored and then inspected by Palo Alto Networks threat protection technologies. To act against threats detected by Cloud IDS, Google developed the Google Cloud Armor system.

Хмарні технології в останні роки стають все популярнішими: багато компаній переносять свої сервіси на cloud-сховища і використовують хмари провайдерів для розміщення критично важливої інформації. Таке рішення є максимально практичним та доступним, проте не варто забувати про можливі проблеми, з якими можна зіткнутися у процесі його використання. Хмарна інфраструктура піддається тим самим загрозам, як і традиційна фізична.

Корпорація Google для своїх хмарних технологій GCP розробила систему виявлення вторгнень Cloud IDS [1].

Cloud IDS (Cloud Intrusion Detection System) - це служба виявлення вторгнень, яка забезпечує виявлення загроз вторгнень, зловмисного та шпигунського програмного забезпечення і командних атак у мережі. Cloud IDS працює шляхом створення однорангової мережі, якою керує Google із дзеркальними віртуальними машинами. Трафік у одноранговій мережі віддзеркалюється, а потім перевіряється технологіями захисту від загроз Palo Alto Networks, щоб забезпечити розширене виявлення загроз. Є можливість віддзеркалювати весь трафік або відфільтрований трафік на основі: протоколу, діапазону IP-адрес або його напрямку.

Cloud IDS забезпечує повну видимість мережевого трафіку, дозволяючи відстежувати зв'язок між віртуальними машинами для виявлення переміщення всередині периметра. Це забезпечує інспекційний механізм, який перевіряє трафік у середині підмережі.

Cloud IDS можна також використовувати, щоб відповідати розширеним вимогам щодо виявлення загроз і відповідності існуючим стандартам.

Cloud IDS автоматично оновлює сигнатури вразливостей та антишпигунських програм без будь-якого втручання користувача, що дозволяє користувачам зосередитися на аналізі та усуненні загроз, не керуючи сигнатурами та не оновлюючи їх.

Cloud IDS щодня отримує оновлення від Palo Alto Networks та передає їх на всі існуючі кінцеві точки IDS.

В хмарній системі захисту є можливість встановлювати три рівня серйозності загроз: високий, середній і низький. Окрім того можна відключати не потрібні, з точки зору користувача, ідентифікатори загроз використовуючи прапор --threat-exceptions.

Щоб діяти проти загроз, які виявляє Cloud IDS Google розробив систему Google Cloud Armor [2].

Google Cloud Armor допомагає захистити сервіси Google Cloud від різних типів загроз, включаючи: розподілені атаки типу «відмова в обслуговуванні» (DDoS), атаки на програми, такі як міжсайтовий скриптинг (XSS) та впровадження SQL (SQLi). У Google Cloud Armor є як автоматичні засоби захисту, так і засоби захисту, які потрібно настроїти вручну.

Попередньо налаштовані правила WAF (Web Application Firewall) Google Cloud Armor – це складні правила брандмауера веб-застосунків WAF з десятками сигнатур, складені згідно галузевих стандартів з відкритим вихідним кодом.

У Google Cloud Armor є керована служба захисту програм Managed Protection.

У Google Cloud Armor також вбудовано адаптивний механізм захисту. від розподілених атак типу «відмова в обслуговуванні» (DDoS) за рахунок аналізу шаблонів трафіку серверних служб, виявляючи та попереджаючи передбачувані атаки. Правила WAF можна настроїти відповідно до потреб користувача. Адаптивний захист можна включити для кожної політики безпеки, але для цього потрібна активна підписка Managed Protection.

Список використаних джерел:

1. Google. Cloud IDS overview. https://cloud.google.com/intrusion-detection-system/docs/overview

2. Google Cloud Armor overview. https://cloud.google.com/armor/docs/cloud-armor-overview