УДК 004.5-004.8

АВТОМАТИЗИРОВАННАЯ СИСТЕМА АНАЛИЗА БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ И СЕРВИСОВ В РАМКАХ ПОПУЛЯРНЫХ ОБЛАЧЫХ ПЛАТФОРМ

Дербан А.Н., Дербан Д.Н.
Белорусский национальный технический университет;
Минск, Республика Беларусь

С каждым годом растет популярность облачных платформ и решений для развертывания инфраструктуры информационных ресурсов крупных и средних организаций. В подавляющем большинстве случаев на предприятиях используется довольно обширный перечень программных продуктов, которые функционируют в облаке в рамках совокупности виртуальных серверов и сервисов, администрируемых на базе множества учетных записей. С течением времени осуществляется обновление и адаптация программного обеспечения под постоянно изменяющиеся условия функционирования современных предприятий. Очевидно, что чем более развита инфраструктура организации, чем дольше она функционирует и чем обширней функционал системного и прикладного программного обеспечения, тем все сложнее осуществить комплексную оценку проблем информационной безопасности.

Одним из современных подходов в области анализа кибербезопастности облачных решений являются так называемые CloudBots - автономные программные модули. В случае наступления определенного события активируется соответствующий CloudBot, который способен протоколировать или даже блокировать выявленную уязвимость. Типичными примерами правил могут выступать ситуации, связанные с активность приложения на определенном сетевом порту, сбои и ошибки авторизации и т.д.

Реализованные в CloudBots технологии базируется на программных платформах с открытым исходным кодом, что позволяет их использовать в популярных облачных решениях: Amazon Web Services (AWS), Microsoft Azure и Google Cloud Platform (GCP). Для развертывания в рамках AWS необходимо использовать сервис Amazon Simple Notification Service (SNS), который запускает на выполнение так называемую лямбда функцию, которая в свою очередь инициирует вызов необходимого CloudBot. Возникшие ошибки в процессе функционирования (не выполняется набор правил, связанных с ботом) регистрируются средствами SNS, кроме того протоколируются все необходимые параметры, выявленной ботом проблемы.

Инициируя запуск как стандартных, так и разработанных самостоятельно CloudBots в совокупности с сервисом регистрации и обработки событий, можно существенно повысить уровень безопасности сетевой инфраструктуры организации, функционирующей в облаке.