Способы сетевой защиты облачной информации.

Облачные вычисления являются одной из наиболее быстро развивающихся областей информационных технологий. Это сетевая модель вычислений, в которой клиент входит в облако, чтобы получить доступ к данным и приложениям, хранящимся на удаленном сервере, а оплачивает соответственно использованию. Gartner [2] подсчитала, что рынок облачных вычислений мог быть порядка 150 миллиардов долларов в 2013 году. По данным исследования мульти сервисного оператора Orange Business Services, в 2012 году объем российского рынка облачных сервисов составил 4,5 млрд рублей [3]. Скорость роста и процветание этой отрасли привели к некоторым проблемам безопасности. Насколько безопасно хранение информации о клиентах в облачных сервисах вызывает обеспокоенность. Поскольку вход в облако, как правило, бесплатен, то высока вероятность того, что злоумышленники также могли получить доступ к серверам и поставить под угрозу безопасность. Организации обычно используют системы обнаружения вторжений (IDS), чтобы смягчить такие сетевые атаки. В этих системах обнаружения вторжений используются методологии аномалий активности, подписи и приманок. Исследователи также соединяют методологии аномалий с подписями, подписи с приманками и синтезируют математические модели представления программного обеспечения в терминах теории графов и теории множеств, позволяющие анализировать процесс выполнения ПО и его инструкции. Предложен способ формального описания классифицирующего признака программного обеспечения, основанный на синтезированной модели представления ПО [4] и новый алгоритм классификации программного обеспечения с заданным признаком и без такового. Там же предложен подход к оценке подобия различных экземпляров программного обеспечения, основанный на мере Дамерау – Левенштейна. Уже синтезирована методика верификации программного обеспечения на деструктивность для сред облачных вычислений, использующая оценку подобия различных экземпляров программного обеспечения. Но очень немногие пробовали работать на аномалиях активности на приманке. В [1] сочетают преимущества методов анализа аномальной активности с технологией приманки для разработки гибридных технологий обнаружения вторжений и систем предотвращения, IDS. Интеллектуальная программная система защиты систем облачных вычислений от атак [5] содержит программные сенсоры сбора информации о пакетах данных, циркулирующих в сети, на основе библиотеки libpcap (осуществляет собственно перехват пакетов). В качестве базовой программной системы может быть использована хорошо зарекомендовавшая себя система обнаружения и предупреждения вторжений Snort [6]. Блок анализа ситуаций, использующий информацию от программных сетевых сенсоров и базы знаний системы, состоящий из модуля корреляционного анализа и модуля принятия решения на основе методов искусственного интеллекта; предназначен для обработки собранных сенсорами данных с целью обнаружения информационных атак и вторжений. Модуль реакции на обнаруженные атаки и вторжения оперативно реагирует на угрозы (сетевые атаки, вирусная активность и пр.) согласно профилю сетевой безопасности (отсылка уведомлений в графический интерфейс визуализации обнаруженных атак и вторжений, информирование ответственных лиц по электронной почте, SMS и др.).

Модуль управления компонентами средств обнаружения атак, который представляет собой графический интерфейс для визуализации обнаруженных атак и вторжений, и управления функционированием системы обнаружения и предотвращения распределенных сетевых атак. Модуль хранения, основанный на системе управления базами данных, позволяет обеспечить доступ модулей истории обнаружения сетевых атак, базе настроек и профилям безопасности, обучающей выборке и др.

[1]. Ajeet Kumar Gautam et al, “ Improved Hybrid Intrusion Detection System (HIDS): Mitigating false alarm in Cloud Computing”, Journal of Computing Technologies, 2012. Pp. 7-12.

[2]. http://www.gartner.com/technology/home.jsp

[3]. http://www.rg.ru/2013/07/09/uslugi.html

[4]. http://mephi.ru/upload/avtoreferat/Tumanov.pdf

[5]. Ю. Г. Емельянова, В. П. Фраленко. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления // Программные системы: теория и приложения : электрон. научн. журн. 2011. № 4(8), с. 17–31. URL: http://psta.psiras.ru/read/psta2011_4_17-31.pdf

[6]. Cloud Security Alliance, URL: https://cloudsecurityalliance.org/.