ВОЛКОВ С. Д., ЦАРЕГОРОДЦЕВ А. В., ЦАЦКИНА Е. П.

ОСОБЕННОСТИ ПОСТРОЕНИЯ СИСТЕМ ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК ДЛЯ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ, ФУНКЦИОНИРУЮЩИХ НА ОСНОВЕ ТЕХНОЛОГИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Аннотация. В статье представлен анализ архитектур систем обнаружения атак на информационно-телекоммуникационные системы. Выявляются недостатки данных архитектур при использовании в информационно-телекоммуникационных системах, функционирующих на основе технологии облачных вычислений. Предлагается решение по созданию нейросетевой системы обнаружения атак, не имеющей недостатков проанализированных систем.

Ключевые слова: информационная безопасность, облачные вычисления, система обнаружения атак, искусственные нейронные сети.

VOLKOV S. D., TSAREGORODTSEV A. V., TSATSKINA E. P.

CONSTRUCTION PECULIARITIES OF INTRUSION DETECTION SYSTEMS FOR INFORMATION AND TELECOMMUNICATION SYSTEMS BASED ON CLOUD COMPUTING

Abstract. The article provides an analysis of the intrusion detection systems architectures for information and telecommunication systems. The shortcomings of the architectures in application to the information and telecommunication systems based on cloud computing are identified. As a solution to the problem, the creation of a neural-network-based intrusion detection system is suggested.

Keywords: information security, cloud computing, intrusion detection system, artificial neural networks.

Облачные вычисления (cloud computing) являются сегодня одной из самых активно развиваемых и инновационных сетевых технологий. В соответствии с моделью, рекомендованной Национальным Институтом стандартов и технологий (National Institute of Standards and Technology, NIST) под облачными вычислениями понимается модель предоставления повсеместного, удобного сетевого доступа «по-требованию» к разделяемому пулу конфигурируемых вычислительных ресурсов (например, сети, серверы, память, приложения и сервисы), которые могут быть предоставлены и освобождены в короткие сроки с минимальными усилиями в управлении или с минимальным взаимодействием с поставщиком услуги [1].

В наше время многие компании ограничены в финансовых ресурсах, в результате чего им приходится решать проблему оптимизации затрат. В таких случаях облачные вычисления становятся прекрасным решением этой проблемы: приобретая облачные сервисы, компаниям не обязательно тратить большие средства на создание собственных центров обработки данных, лицензионное программное обеспечение и квалифицированный персонал. Но при всем удобстве, данное преимущество приводит к возникновению новых актуальных угроз информационной безопасности, связанных, прежде всего, с уменьшением возможности контроля процессов обработки информации, а также с динамичностью модели предоставления ресурсов. Таким образом, при внедрении и переходе на использование облачных вычислений возникает противоречие между увеличением эффективности основных производственных процессов в компании – с одной стороны, и возникновением новых угроз информационной безопасности – с другой стороны.

Основная специфика облачных технологий заключается в том, что вместо предоставления «сырых» вычислительных ресурсов и ресурсов хранения, предоставляются более абстрактные ресурсы в виде сервисов [2].

В частности, к особенностям облачных технологий можно отнести следующие моменты.

Во-первых, облачные вычисления фокусируются на подходе «всё как сервис». Причем, исключительно на платном предоставлении вычислительных ресурсов конечному пользователю. Однако ресурсы предоставляется по мере надобности, что позволяет существенно сократить расходы.

Во-вторых, системы, функционирующие на основе облачных вычислений, строятся таким образом, чтобы предоставлять интерфейсы конечным пользователям через веб-доступ или посредством API. Такое повышение уровня абстракции позволяет обеспечить применение облачных вычислений, как на уровне отдельных пользователей, так и на уровне корпоративных клиентов.

В-третьих, технология облачных вычислений построена на базе технологии виртуализации. Она позволяет гибко разделять и гарантировать ресурсы, предоставлять их по требованию и контролировать их использование. С помощью виртуализации возможно создание изолированных виртуальных окружений, которые реализуют определенные сервисы, а также возможно разделение ресурсов (сеть, устройства хранения) на логическом уровне для более гибкого управления.

В последнее время существенный рост количества целенаправленных атак на корпоративные инфраструктуры (в том числе интегрирующие облачные среды) требует четко продуманной стратегии внедрения новых технологий защиты информации. Одним из

действенных подходов является использование средств управления инцидентами и событиями информационной безопасности. В частности, широкое распространение получили автоматизированные системы обнаружения компьютерных атак. Среди них можно выделить такие системы, как Snort, Bro, OSSEC, STAT и Prelude. В общем виде все системы обнаружения атак можно разделить на два класса – network-based (NIDS) и host-based (HIDS).

NIDS-системы (пример, Snort, Bro) основаны на принципе анализа сетевых пакетов данных. Такие системы просматривают сетевой трафик защищаемого сетевого сегмента, защищая тем самым входящие в этот сегмент информационные системы. NIDS-системы, как правило, состоят из декодера пакетов данных, ядра обнаружения атак и подсистемы оповещений. Декодер пакетов отвечает за сбор данных, передаваемых по сети. Ядро обнаружения атак компилирует известные системе сигнатуры и анализирует переданные декодером данные на наличие в них сигнатур атак. При обнаружении атаки создается событие для подсистемы оповещений. На рисунках 1 и 2 приведены обобщенные схемы архитектур сетевых систем обнаружения атак Snort и Bro.

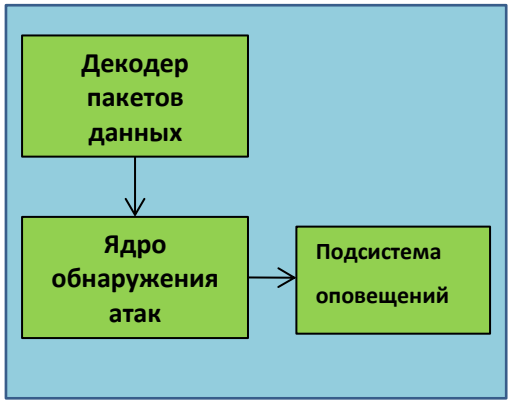

Рис. 1. Обобщенная архитектура системы обнаружения атак Snort.

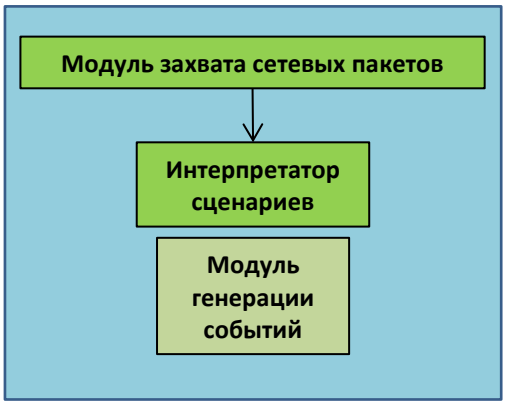

Рис. 2. Обобщенная архитектура системы обнаружения атак Bro.

HIDS-системы (например, OSSEC, STAT) анализируют информацию, расположенную в конкретной информационной системе. Такое расположение позволяет определять только те системные процессы, которые имеют отношение к конкретной атаке, что повышает эффективность работы системы. Системы этого типа, как правило, имеют модульную структуру, состоящую из модулей анализа лог-файлов операционной системы, обнаружения руткитов в системе, контроля целостности системных файлов и т.п. Однако все угрозы HIDS-системы обнаруживают на основе известных им сигнатур, что делает их, с этой точки зрения, похожими на NIDS-системы. На рисунках 2 и 3 приведены обобщенные схемы архитектур сетевых систем обнаружения атак OSSEC и STAT.

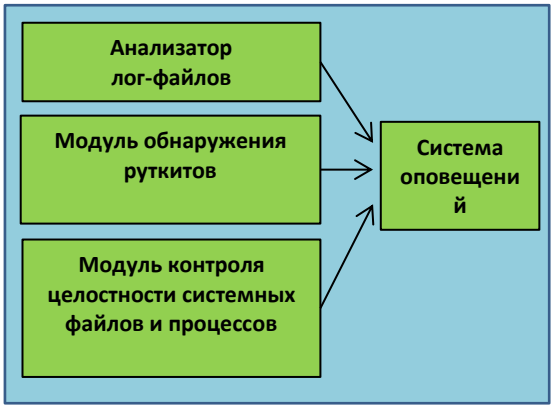

Рис. 3. Обобщенная архитектура системы обнаружения атак OSSEC.

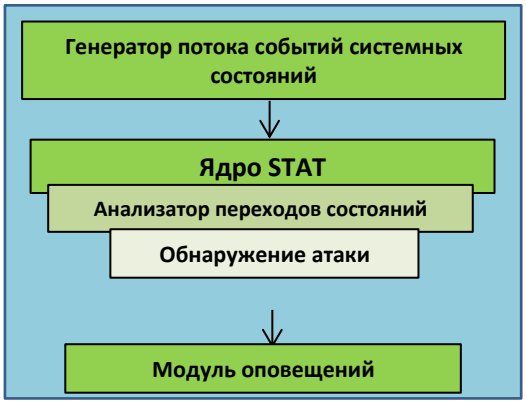

Рис. 4. Обобщенная архитектура системы обнаружения атак STAT.

Кроме того, есть и системы, сочетающие в себе функционал, характерный как для сетевых, так и для узловых систем – гибридные системы обнаружения атак (Hybrid IDS). Примером такой системы является система Prelude. Она позволяет отслеживать активность как на уровне вычислительной сети, так и на уровне отдельных узлов. Система имеет распределенную архитектуру и включает в себя сетевые сенсоры (анализируют данные на уровне сети используя методы сигнатурного анализа) и узловые (анализируют лог-файлы

ОС). Эти сенсоры генерируют сообщения об обнаружении аномалий и отправляют их модулям управления (регистрируют и анализируют сообщения, затем генерируют возможную ответную реакцию системы на атаку). Обобщенная архитектура системы обнаружения атак Prelude представлена на рисунке 5.

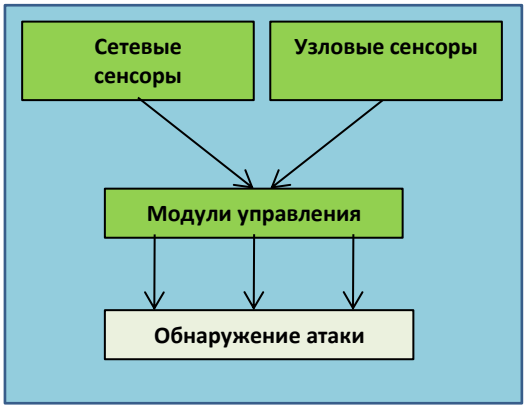

Рис. 5. Обобщенная архитектура системы обнаружения атак Prelude.

Таким образом, можно говорить о том, что оба рассмотренных типа систем, так или иначе, основаны на сигнатурном методе обнаружения атак, а значит, обладают крайне низкой адаптивностью к обнаружению новых (неизвестных системе) атак. Кроме того, принимая во внимание специфику информационно-телекоммуникационных систем, функционирующих на основе технологии облачных вычислений, необходимо учитывать и угрозы целенаправленных атак, которые нарушают функционирование подсистем гипервизора, отвечающие за планирование задач и верификацию команд на их соответствие требованиям информационной безопасности. Такие атаки сложно выявлять и эффективно блокировать используемые ими каналы информационных воздействий, так как эти каналы не доступны для контроля со стороны гостевых операционных систем. Критичность этих атак обуславливается также тем, что их реализация может нанести ущерб не только конкретной гостевой системе, но и всей физической информационно-коммуникационной системе.

Перспективным способом решения данной проблемы является разработка адаптивного метода обнаружения атак, который обеспечит обнаружение не только специфичных для облачных систем атак, но и неизвестных атак. Для создания такого метода можно воспользоваться математической моделью искусственных нейронных сетей. Построенная на их базе нейросетевая система обнаружения атак обучается в течение некоторого периода времени, когда все наблюдаемое поведение считается нормальным. После обучения система запускается в режиме распознавания [3]. В ситуации, когда во входном потоке данных не удается распознать нормальное поведение, фиксируется факт

атаки. Такой механизм обеспечивает обнаружение не только уже известных угроз, но и ранее неизвестных угроз, направленных, в том числе на гипервизор и иные критичные для системы компоненты.

ЛИТЕРАТУРА

1. Емельянова Ю. Г., Фраленко В. П. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления // Программные системы: теория и приложения. – № 4(8). – 2011. – С. 17–31.

2. Радченко Г. И. Распределенные вычислительные системы: учебное пособие. – Челябинск: Фотохудожник, 2012. – 184 с.

3. Rasool Jalili, Fatemeh Imani-Mehr, Morteza Amini, Hamid Reza Shahriari Detection of Distributed Denial of Service Attacks Using Statistical Pre-Processor and Unsupervised Neural Networks // Lecture Notes in Computer Science. – 2005. – Vol. 3439. – pp. 192–203.