Защита компьютерной сети применительно к облачным средам

Автор: *С.М. Божаткин, Национальный университет кораблестроения имени адмирала Макарова, г. Николаев; И.Н. Журавская, к.т.н., Черноморский государственный университет им. П. Могилы*

В последнее время широкое распространение получают облачные технологии. Многие специалисты считают, что облачные технологии в будущем станут основой ИТ-структуры компаний, но не меньшая группа специалистов обеспокоена вопросами безопасной эксплуатации подобных сервисов, предотвращения потери контроля над трафиком и возможностью использования привычных инструментов [1].

В небольших организациях мощность установленных компьютеров превосходит потребности пользователей. Но бывают задачи, для которых требуется большая мощность вычисления. Как выход можно рассматривать создание локального «облака», в котором одним компьютеры используют мощности других компьютеров, незагруженных собственными процессами.

Сама концепция размещения приложений и данных на распределённых ресурсах показывает, что задача обеспечения безопасности имеет совсем другие корни, а поэтому решать ее необходимо несколько иначе. Кроме классических угроз, присущих локальной сети, добавляются и специфические угрозы целостности, доступности и конфиденциальности информации в случае перевода как физических, так и виртуальных машин (VM) в спящий режим. Но, в этом случае становится актуальной проблема защиты Instant-On – спящих виртуальных машин и шаблонов. Через некоторый период времени их установки уже могут не соответствовать конфигурации безопасности, и после включения VM или создании новой VM из такого шаблона они уже будут иметь уязвимости. Имеющиеся системы обновлений вроде WSUS умеют работать только с запущенными машинами, поэтому здесь нужны специализированные инструменты. Для решения этой проблемы может быть использовано такое ПО как Microsoft Offline Virtual Machine Servicing Tool, System Center Virtual Machine Manager 2012, VMware Update Manager и т.п. Все перечисленные программы умеют обновлять остановленные и спящие VM и шаблоны на хостах Hyper-V.

Угрозы безопасности можно разделить на две категории:

а) внутренние – которые исходят от администраторов сервиса и становятся возможными из-за просчетов в построении системы управления и аудита;

б) внешние — исходящие из глобальной сети и от других клиентов облака.

Локальное облако имеет свой периметр, поэтому все усилия по защите должны быть направлены на защиту этого периметра.

Одним из распространённых классов задач является работа над одним проектом нескольких исполнителей при наличии в организации нескольких проектов. В этом случае нет четко обозначенного периметра, но обязательно введение среди исполнителей системы иерархий. Исполнитель, работающий над одним проектом («человек за стеной»), имеет доступ только к определенным узлам, внесенным в так называемый «белый список». Исполнитель, работаюй над несколькими проектами, имеет статус «человек над стеной».

Практически все аспекты безопасности с появлением облака новы и требуют пересмотра, но сказать, что они уникальны, тоже нельзя. В таком случае требуется несколько иной подход для решения проблем безопасности. Учитывая, что вариантов облаков на сегодня существует много, а сама проблема изучена далеко неполностью, универсального совета, как и решения, никто не дает. К тому же, здесь нет многолетних наработок. Поэтому, в отличие от классических систем обеспечения безопасности, где в ближайшее время вряд ли стоит ожидать чего-либо интересного, рынок решений для защиты виртуализации только набирает обороты. Каждый разработчик ПО видит и соответственно решает проблему по-своему. А любые и особенно новые продукты на рынке требуют некоторой обкатки в реальных условиях, прежде, чем они будут максимально удовлетворять пользователя по надежности и функциональности.

Так как правила доступа теперь нельзя привязать к физической топологии сети, к IP-адресам пользователей, а сервис может быть распределен между несколькими физическими машинами, то особенно важным становится аудит всех событий, инициированных каждым пользователем. Требования протоколирования всех процессов, запущенных на ПК и обращений к серверам напрямую прописан в НД ТЗИ 2.5-004-99 [2].

Необходимо отметить расширение потребности пользователя выхода за пределы украинской сети обмена интернет-трафиком (UA-IX). Однако, за пределами UA-IX аудит событий не является обязательным в соответствии с Гармонизированными критериями европейских стран (ITSEC), в которых используются только три критерия защищенности, включенные в TRIAD_CIA (конфиденциальность, целостность и доступность информации).

Чаще всего защита каналов связи реализуется при помощи VPN-серверов или SSH-туннелей [3]. В настоящее время VPN-серверы более популярны, чем SSH-туннели хотя и те, и те в избытке продаются в интернете. Что разворачивать на своём сервере, каждая организация принимает собственное решение, но следует заметить, что при использовании

SSH-туннеля информационная скорость передачи данных будет практически в 3 раза больше. Согласно проведённым исследованиям, при информационной скорости передачи информации в локальной сети 96.5 Mbps скорость в SSH-туннеле будет достигать 94.2 Mbps, а network/VPN – всего 32.4 Mbps [4]. Поэтому актуальность использования SSH-соединений со временем будет повышаться.

В облаке могут быть задействованы и сервисы on-line. Серьёзной угрозой безопасности всего облака является также неучтённый трафик. Достаточно сложно помешать злоумышленнику создать ложный облачный сервис и получить доступ к конфиденциальной информации. Поэтому вероятность использования облака хакерами (технология Exploits as a Service - EaaS) также должна учитываться.

Облачные технологии все больше проникают в нашу жизнь. Улучшаются инструменты защиты, но и улучшаются инструменты атак. На сегодняшнем этапе использования облачных технологий для обеспечения безопасности информации, обрабатываемой в организации, можно порекомендовать:

- создание своего облака с ограниченным количеством участников, т.е. построения периметра с организацией его защиты;
- создание VPN-каналов или SSH-туннелей для всех участников облака;
- поднятие всех используемых сервисов на своём сервере.

В сети интернет довольно много предложений по аренде сторонних мощностей. Перед использованием в своих проектах облачных технологий необходимо оценить используемый ресурс на уязвимость к атакам.

Список литературы:

1. Трудности защиты облачных сред и возможности существующих решений для защиты облаков [Электронный ресурс] // Наброски админа. – Режим доступа: URL: http://wpcon-fig.ru/?p=1086. – Загл. с экрана.

2. НД ТЗИ 2.5-004-99. Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа [Электронный ресурс] // Веб-сайт Держспецзв'язку Украины. – Режим доступа : URL : http://www.dstszi.gov.ua/dstszi/.../document?id=4164. – Загл. с экрана.

3. Методы анонимности сети [Электронный ресурс] // Посты интернет-сообщества Хабрахабр. – Режим доступа : URL : http://habrahabr.ru/post/190396/. – Загл. с экрана.

4. SSH or VPN? / Jiang Yio [Электронный ресурс] // Inportb. – Режим доступа : URL : http://inportb.com/2009/09/04/ssh-or-vpn/. – Загл. с экрана.