Защита в облаках

Интервью с генеральным директором компании "Сертифицированные информационные системы" – Сергеем Борисовичем Груздановым.

Груданов Сергей Борисович – генеральный директор компании "Сертифицированные информационные системы".

SN. Что сдерживает продвижение облачных сервисов для корпоративных применений?

С.Г. Облачные сервисы, хотя и имеют множество преимуществ, несут также и дополнительные риски в области ИБ. Основной экономический эффект при использовании облаков удается достичь только в условиях разделяемых/совместно используемых ресурсов с другими компаниями/организациями. Соответственно, к этому добавляется и то, что вся ИТ-инфраструктура со всеми приложениями выносится за охраняемый периметр.

На Западе в полной мере все дополнительные ИБ-риски, связанные с развитием новых облачных технологий, поняли еще в 2010 г. Следствием этого стал ряд регламентирующих и законодательных актов во всех развитых странах, появившихся в 2011 г., и, по сути, запрещающих передачу, обработку и хранение информации без шифрования.

Однако, несмотря на принимаемые меры, ряд крупных скандалов в 2011–12 гг. из-за утечки данных привели к тому, что использование публичных облаков практически было запрещено для размещения чувствительных данных в МО США и многих крупных западных банков (за исключением клиентских сервисов). В последних – и по причине высоких отчислений по рискам. До России эта волна докатилась лишь в 2013 г.: с выходом приказов № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» и № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», в которых устанавливается, что информационные системы, использующие технологии виртуализации, требуют от заказчиков внедрения сертифицированных решений.

Причины, сдерживающие миграцию в облачную инфраструктуру (публичное облако либо частное облако с разделением полномочий отдела безопасности и IT), состоят в:

- контроле трафика как на уровне периметра, так и внутри виртуальной инфраструктуры;
- контроле доступа к узлам виртуальной инфраструктуры из неконтролируемой зоны (включая применение мобильных устройств);
- защите данных в виртуальной инфраструктуре в процессе хранения и обработки (оптимальный вариант – прозрачно для гипервизора, приложений и пользователей);
- усилении функций аутентификации при организации доступа к виртуальной инфраструктуре (включая доступ с мобильных устройств).

SN. Каким же образом решаются поставленные задачи и насколько они применимы к российскому рынку?

С.Г. Защита сетевой инфраструктуры осуществляется, например, с использованием решений одного из лидеров сетевой безопасности – компании CheckPoint. Данные решения неоднократно подтверждали свой функционал как в физической инфраструктуре (выступая в качестве шлюза безопасности и сервера доступа с организацией VPN-соединения с использованием ГОСТ'овой криптографии; более того, CheckPoint предоставляет доступ и с мобильных устройств без необходимости получения рутового доступа), так и в виртуальной (решение может быть развернуто внутри виртуальной инфраструктуры и может контролировать трафик между виртуальными машинами).

Компания SafeNet уделяет большое внимание защите информации, размещаемой в виртуальной инфраструктуре. Решение ProtectV позволяет выполнять прозрачное шифрование виртуальных жестких дисков машин, функционирующих на базе гипервизоров VMware vSphere и Amazon. Ключевой особенностью решения является возможность организации доверенной загрузки, а также управление жизненным циклом ключей шифрования с возможностью размещения хранилища ключей в контролируемой зоне.

Так как в компаниях все больше и больше появляется мобильных пользователей, которые хотели бы получить доступ к информации с мобильных устройств, то и возможность атаки сильно увеличивается – начиная от перехвата трафика, содержащего персональную информацию для аутентификации, до создания фейкового ресурса с возможностью атаки DNS spoofing. Для предотвращения данного типа атак компания SafeNet предоставляет решения для обеспечения двухфакторной аутентификации. Однако в силу того, что применимость PKI-инфраструктуры не всегда доступна для мобильных платформ, наибольшую популярность приобретают бесконтактные аутентификаторы – генераторы одноразовых паролей (аппаратные, программные, генерируемые на стороне сервера). Решение SafeNet Authentication Service позволяет внедрить механизмы двухфакторной аутентификации в компанию (как в физическую среду, так и в виртуальную), не изменяя архитектуру, развернутую в компании.

Если затрагивать вопрос сертификации, то решения Check Point успешно прошли сертификацию ФСТЭК. Процесс сертификации SafeNet Authnetication Service находится в финальной стадии. К сожалению, решение ProtectV на текущий момент не может пройти сертификацию в силу отсутствия ГОСТ'овой криптографии, однако есть множество заказчиков, которым необходимо выполнить требования регуляторов в соответствии с требованиями PCI DSS.

Рассмотренные выше решения позволяют мигрировать инфраструктуру в облачную среду, сохраняя при этом высокий уровень безопасности, как с точки зрения внутренних, так и внешних угроз. При этом остается гибкость облачных решений, которая может быть представлена средой виртуализации, не нарушающей при этом функциональность решения в целом.

VI Уральский форум "Информационная безопасность банков"

Декабрь 2013 г. – С 17 по 22 февраля 2014 г. в Республике Башкортостан в ДЦ "Юбилейный" состоится VI Уральский форум "Информационная безопасность банков". Форум проводит Ассоциация российских банков совместно с компанией "АВАНГАРД ЦЕНТР" при официальной поддержке Банка России.

Программа Форума предполагает проведение тематических секций, круглых столов и дискуссий по следующим направлениям:

- инновационные банковские технологии (мобильный офис, облачные вы-