Не так страшно облако, как его малюют

беседовала **Софья Мороз**

Основным сдерживающим фактором облачного бума в российских банках, который предсказывали аналитики, является миф о небезопасности хранения данных в облаках. О ключевых аспектах защиты частного облака в интервью NBJ рассказал начальник отдела информационной безопасности «Амтел-Сервис» Алексей ЗАЛЕЦКИЙ.

NBJ: Алексей Викторович, какие данные действительно можно хранить и обрабатывать с помощью облачных сервисов?

А. ЗАЛЕЦКИЙ: Сегодня в облаке можно хранить любые данные, за исключением государственной тайны. Однако, по результатам проведенного «Амтел-Сервис» опроса, перенести абсолютно все приложения в облако готовы только 10% компаний, в то время как отдельные, менее критичные для бизнеса системы – 91% респондентов. Так, банки чаще хранят в облаке приложения для контакт-центров, корпоративных соцсетей, и только единицы перенесли в свое облако системы, в которых хранятся и обрабатываются критичные для бизнеса данные, а также обработку персональных данных. Хотя на самом деле сегодня вполне реально обеспечить не только надежный уровень защиты, но и выполнить все требования регуляторов к защите персональных данных в частном облаке, что подтверждают реализованные нами проекты. Безусловно, есть ряд сложностей технического и организационного характера, но все они преодолимы.

NBJ: На какие аспекты стоит обратить внимание при работе с облаками?

А. ЗАЛЕЦКИЙ: Необходимо уделять внимание как техническим мерам защиты, так и организационно-распорядительной документации. Основные риски, с которыми мы чаще всего сталкиваемся, в том числе в банках, – это неправомерный доступ пользователей, например операционистов, к данным. Как пример можно привести проект в одном из розничных банков, где в результате проведенного нами обследования были выявлены существенные недостатки системы защиты облака. Несмотря на наличие необходимых средств защиты, в комплексе система защиты информации была совершенно неэффективна как из-за малого внимания к внутренним организационно-распорядительным документам, так и из-за непродуманности защиты всех аспектов взаимодействия пользователей и администраторов с облаком.

Помимо шифрования канала связи, не менее важно обеспечить шифрование информации в самом облаке. К сожалению, сегодня к данной мере защиты прибегает лишь небольшой процент компаний, воспринимая ее как дополнительную, необязательную меру. Также важно реализовать инструменты, позволяющие видеть и реагировать на различные инциденты, выявлять слабые места как самого облака, так и системы его защиты.

NBJ: С какими проблемами вы сталкиваетесь на проектах по защите облаков?

А. ЗАЛЕЦКИЙ: В отсутствие наработанного опыта и отечественных стандартов многие российские организации при создании системы защиты чаще всего использовали продуктовый подход, основанный на лучших технических средствах, представленных на рынке. Основная проблема такого подхода – невозможность обеспечить комплексную систему защиты в облаке. Так, проводя аудит, мы зачастую сталкиваемся с тем, что заказчик делает большой упор на один из уровней защиты: клиентский уровень, приложения, платформы/инфраструктуры. Например, на высоком уровне выполнена защита среды виртуализации, но при этом не решен вопрос по защите на клиентском уровне, не решены вопросы с обеспечением безопасности при получении доступа с мобильных устройств к облаку. Это приводит к крайне низкому общему уровню защищенности. Собственно, наша задача – помочь заказчику увидеть всю картину безопасности облака и устранить уязвимости.

NBJ: Получается, у вас есть готовое решение по защите облака?

А. ЗАЛЕЦКИЙ: Универсального типового решения по обеспечению защиты облака в принципе быть не может, так как вариантов построения облаков очень много. Всестороннюю безопасность облака можно обеспечить только в рамках комплексного проекта. Мы применяем наработанную и проверенную методологию, основным этапом которой является детальное обследование с анализом угроз для каждого уровня. Важнейшие задачи, которые нам приходится решать, – это обеспечение конфиденциальности обрабатываемых данных, разграничение доступа, защита от вредоносного кода и различных типов атак, а также управление системой и событиями безопасности облака. NBJ