«Инфофорум 2016»: угрозы ИБ в банковском секторе достигли критических масштабов

Угрозы информационной безопасности бизнеса приближаются к критическому масштабу. К такому неутешительному выводу пришли участники панельной дискуссии «Мобильная безопасность и управление безопасностью ИТ-инфраструктуры», состоявшейся в рамках прошедшего в Москве 4–5 февраля «Инфофорума 2016».

В двухчасовой дискуссии, которую вели Дмитрий Фролов, глава Центра реагирования на компьютерные атаки Банка России, и Тимур Аитов, эксперт Ассоциации «Россия», приняли участие целый ряд экспертов в области безопасности, представляющих российские и международные ИТ-компании, банки, правоохранительные органы и иные властные структуры. Среди ключевых тем – противодействие новейшим типам кибератак на кредитно-финансовые организации России, развитие инновационных платежных инструментов и противодействие преступности в кредитно-финансовой сфере, безопасность в сфере мобильных платежей и систем ДБО, а также ряд других.

Обеспечение ИБ и запуск проектов: egg or chicken?

Как отметила **Мария Воронова**, ведущий эксперт по информационной безопасности компании InfoWatch, обсуждая вопрос совмещения интересов бизнеса, диктующих как можно более быстрый запуск на рынок нового сервиса, и необходимости обеспечить при этом максимально возможный уровень безопасности, «здесь правила игры диктует именно бизнес». По ее словам, зачастую бизнес изначально предпочитает брать на себя все потенциальные риски, лишь бы проект оперативно был запущен в коммерческую эксплуатацию, а вопросы безопасности решать задним числом, по мере выявления проблем. Как подчеркнула М. Воронова, во многом такая ситуация представляется ей оправданной, однако уже на этапе запуска сервисов необходимо инвестировать в некую ИТ-базу, которая впоследствии, по мере развития проекта, позволит обеспечивать безопасность на всех его этапах.

В свою очередь, **Михаил Левашов**, зам. генерального директора ГК «Инфосекьюрити», отметил, что на практике вопросы обеспечения безопасности в новых проектах решаются на стадии подготовки далеко не всегда. В результате известны примеры, когда буквально через несколько недель после запуска того или иного платежного сервиса компании сталкиваются с многомиллионными убытками, и только после этого обращаются за помощью к специализированным структурам, в том числе в рамках аутсорсинга, поскольку сами, как правило, не располагают ни штатом соответствующих специалистов, ни необходимыми компетенциями.

Лев Шумский, начальник управления информационной безопасности Связного Банка, подчеркнул, что в решении рассматриваемой дилеммы «интересы бизнеса – обеспечение безопасности» все зависит исключительно от зрелости бизнеса: «зрелый бизнес в обязательном порядке привлекает службу информационной безопасности во все свои процессы». Немаловажен, по его словам, и уровень зрелости самой службы ИБ – при этом развитому бизнесу вполне по силам решать эти задачи силами внутренних подразделений.

Со своей стороны, **Валерий Конявский**, заведующий кафедрой «Защита информации» МФТИ, научный руководитель ОАО «КБПМ», добавил, что в своей стратегии ИБ участникам рынка следует четко различать такие понятия, как угрозы и атаки. По его словам, именно угрозы, на которые своевременно не обратили внимания, очень быстро преобразуются в атаки. При этом он отметил, что самым слабым звеном в системах ДБО по-прежнему остается клиент, на которого нацелено большинство успешных атак преступников. На этом фоне, по мнению В. Конявского, клиента необходимо обеспечить средствами, которые позволят ему в случае мошенничества обезопасить себя от неправомерных претензий банка. В ходе своего выступления он продемонстрировал аудитории мини-компьютер российской разработки, который в первый день «Инфофорума 2016» вместе с другим решением – так называемым «Лучом Чемизова» – был показан президенту РФ Владимиру Путину. Главным достоинством представленной разработки В. Конявский назвал принципиальное отсутствие возможности заражения вирусами благодаря применению уникального типа аппаратной архитектуры, что позволяет эффективно использовать решение в системах ДБО на стороне клиента.

Зав. кафедрой «Защита информации» МФТИ отметил, что сегодня на запуск эффективного информационного сервиса может потребоваться не более нескольких недель, в то время как на то, чтобы сделать этот сервис действительно защищенным, действующие документы регуляторов заставляют тратить годы. Этот разрыв не зависит от разработчиков и целиком обусловлен текущей нормативной базой. На этом фоне нужно как можно скорее адаптировать требования регуляторов к реалиям современного рынка.

ЦБ РФ: ущерб от хакерских атак может быть сопоставим с последствиями применения ядерного оружия

Дмитрий Фролов, глава Центра реагирования на компьютерные атаки Банка России, отметил значительно возросшие за последнее время компетенции преступников, которые делают сегодня акцент на сканирование организационной и технологической составляющей ИБ-структуры банков, что позволяет им открывать все новые потенциальные уязвимости.

М. Воронова: «Уже на этапе запуска проекта необходимо инвестировать в ИТ-базу, которая позволит обеспечивать ИБ»

Последние давно уже стали предметом активной купли-продажи, в том числе на уровне государств, не говоря уже о преступных сообществах. При этом Дмитрий Фролов подчеркнул: «StaffNet использовал только 4 уязвимости и аналогичное количество эксплойтов, если же в сфере промышленного ПО будет задействовано 2000 эксплойтов, ущерб от такого рода атак будет сопоставим с применением ядерного оружия».

С 1 января 2016 г. в России выявлено уже не менее трех преступных атак на ИТ-системы банков, целью которых было хищение денежных средств на общую сумму 2 млрд рублей. Такие данные привел участвующий в дискуссии представитель Управления «К» МВД России **Евгений Михалев**. При этом он уточнил, что в результате мошенникам удалось похитить не более 300 млн рублей, в том числе благодаря четкой работе правоохранительных органов. В качестве примера он привел недавний инцидент, когда полицейские пресекли деятельность преступной организации, целью которой являлось масштабное хищение средств, находящихся на счетах целого ряда банков страны.

В свою очередь ведущий панельной дискуссии эксперт Ассоциации «Россия» Тимур Аитов отметил, что суммарные потери банков от действий преступников в 4-м квартале 2015 г. составили не менее 1,5 млрд рублей.

Microsoft: импортозамещение в сфере ПО не решит задачу обеспечения национальной безопасности?

Одной из ключевых тем двухчасовой дискуссии стали задачи импортозамещения и альтернативные сценарии, позволяющие обеспечить безопасность российской экономики, включая банковский бизнес, в сегодняшних геополитических условиях.

Отвечая на вопрос, заинтересованы ли отечественные ИТ-структуры в самостоятельной разработке безопасных

▸ **Панельная дискуссия «Мобильная безопасность и управление безопасностью ИТ-инфраструктуры» состоялась 5 февраля 2016 года в рамках прошедшего в Москве «Инфофорума 2016»**