СТИМУЛ В ДЕЙСТВИИ

ПЛАТЕЖИ ПОД ЗАЩИТОЙ ПОЛОЖЕНИЯ БАНКА РОССИИ №382-П

Антон СВИНЦИЦКИЙ
директор по консалтингу АО «ДиалогНаука»

Как мы знаем, банковская отрасль России является одной из наиболее продвинутых в части регламентации со стороны регуляторов в вопросах обеспечения информационной безопасности. Уже начиная с 2006 года активно развивается комплекс документов Банка России по обеспечению информационной безопасности, а с 2015 года стал функционировать центр реагирования на инциденты FinCERT.

Положение Банка России от 9 июня 2012 года № 382-П устанавливает требования к защите информации при осуществлении переводов денежных средств. Этот документ существует с 2012 года и его требования неоднократно актуализировались и пересматривались для соответствия с текущими реалиями. Положение предполагает, в том числе, проведение регулярной оценки соответствия участника платежной системы определенным требованиям. Компания «ДиалогНаука» проводит аудит в соответствии с этим Положением достаточно давно — за прошедшие 5 лет компания провела более 50 аудитов, поэтому нам хотелось бы поделиться полученными результатами этих работ.

ПРОБЛЕМА КАДРОВ

Основной проблемой, приводящей к недостаточно высокому уровню соответствия организации требованиям Положения 382-П, по нашему опыту, является недостаточность кадровых ресурсов, необходимых для выполнения всех задач в области информационной безопасности (ИБ). Так, например, в 25% случаев в кредитной организации (именно кредитные организации являются основным заказчиком проведения внешней оценки соответствия) количество сотрудников, задействованных в реализации процессов обеспечения ИБ, не превышало трех специалистов, а чаще всего был просто один человек, ответственный за безопасность. Он занимался всем и решал все задачи, связанные с ИБ. В основном это была разработка документов, иногда согласование правил доступа, также на него была возложена проверка соответствия требованиям регулятора и учет носителей ключевой информации. При этом администрирование средств защиты информации в этом случае находилось в ведении ИТ-подразделений.

ДРУГИЕ ПРОБЛЕМЫ

Однако даже в случаях, когда сотрудников, отвечающих за информационную безопасность своей компании, было 10–15 человек, они не решали задач, связанных с глубокой интеграцией процессов обеспечения ИБ в банковские технологические процессы и задач, связанных с выявлением инцидентов — обрабатывались только простые инциденты, не затрагивающие технологические и бизнес-процессы организации.

Среди выявленных «ДиалогНаукой» несоответствий можно выделить следующие группы, которые оказывали непосредственное влияние при формировании оценки уровня соответствия:

I. Нереализованные (не формализованные) требования по обеспечению информационной безопасности в системах ДБО: в первую очередь это отсутствие внутренних документов, определяющих требования к таким системам, в том числе требования к регистрации событий безопасности. В половине проектов представители кредитной организации не смогли продемонстрировать журналы регистрации событий, содержащие всю необходимую в соответствии с требованиями Положения 382-П информацию.

II. Отсутствующие свидетельства вовлеченности ответственных за обеспечение информационной безопасности в процессы разработки/приобретения/модернизации автоматизированных банковских систем и компонент среды обработки защищаемой информации: в основном это отсутствие технических заданий (требований), содержащих формализованные требования по необходимым к реализации мерам защиты информации, а также отсутствие контроля реализованных мер защиты при вводе в эксплуатацию.

ОСНОВНОЙ ПРОБЛЕМОЙ, ПО НАШЕМУ ОПЫТУ, ЯВЛЯЕТСЯ НЕДОСТАТОЧНОСТЬ КАДРОВЫХ РЕСУРСОВ, НЕОБХОДИМЫХ ДЛЯ ВЫПОЛНЕНИЯ ВСЕХ ЗАДАЧ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

СТАТИСТИКА

Ниже приведена статистика по используемым средствам защиты, полученная по результатам проведенных аудитов:

- только 60% заказчиков используют продукты двух и более вендоров для организации антивирусной защиты. Самый популярный антивирус — это продукты «Лаборатории Касперского», но также встречаются ESET, Trend Micro и Sophos. У большинства заказчиков антивирус также выполняет задачи контроля периферийных устройств. Дополнительные системы контроля USB и периферийных устройств используются крайне редко;
- системы защиты от утечек информации (DLP) по факту используются редко, а если и используются, то не самым эффективном образом — мониторинг (не блокировка) по общим правилам, таким как отслеживание номеров карт или паспортных данных, в отдельных случаях — оцифровка типовых договоров. Полностью настроенных процессов практически не встречается. Используются в основном решения трех производителей: InfoWatch, McAfee и Forcepoint (WebSense);
- межсетевые экраны — это в основном либо Cisco ASA, либо встроенные механизмы сетевого оборудования, хотя в последнее время все больше клиентов начинают применять специализированные межсетевые экраны;
- только 40% заказчиков используют сертифицированные средства криптографической защиты информации для защиты каналов связи;
- средства анализа защищенности, которые должны проверять наличие уязвимостей, используются у не более чем 60% заказчиков. По сканерам безопасности лидерами являются Nessus, Qualys, XSpider и MaxPatrol. В каждом пятом проекте сканирование безопасности было отдано на аутсорсинг;
- наконец, тесты на проникновение проводят менее половины заказчиков. При этом со следующей редакции 382-П проведение тестов на проникновение становится обязательным.

Другие средства защиты используются крайне редко. Единицы используют WAF (Web Application Firewall) и только в рамках выполнения требований PCI DSS.

* * *

В завершение хотелось бы обратить внимание на то, что в новой редакции Положения 382-П усиливаются требования в части контроля состояния информационной безопасности: предполагается формализация необходимости проведения ежегодных тестирований на проникновение, аудита кода приложений на уязвимости и оценки только в форме внешней оценки соответствия, выполняемой лицензиатами ФСТЭК России. Данный фактор дает возможность за счет привлечения сторонней специализированной компании-интегратора даже при небольшом количестве сотрудников в отделе информационной безопасности реализовать полный спектр требований Банка России. В целом, с нашей точки зрения, принятие Банком России Положения № 382-П позволило повысить внимание кредитных организаций к вопросам информационной безопасности и послужило стимулом в реализации мероприятий, направленных на повышение уровня защищенности как от внешних, так и внутренних угроз.