Управление рисками информационной безопасности в банках: акценты года

Риски всегда присутствуют в банковской деятельности, а в период кризиса их воздействие становится принципиально важным для банка. Мошенники активизируются, поэтому сотрудникам службы безопасности банка нужно быть начеку. О том, как сегодня эффективно управлять рисками безопасности в банках мы беседуем с Виктором Сердюком, генеральным директором ЗАО "ДиалогНаука".

Виктор Сердюк — генеральный директор ЗАО «ДиалогНаука». Его профессиональные качества подтверждены многими сертификатами, включая Certified Information Systems Security Professional, Microsoft Certified Solution Developer, Microsoft Certified Application Developer, Microsoft Certified System Engineer и др.

— Какие риски, связанные с безопасностью банковских информационных систем в настоящее время являются наиболее актуальными?

Виктор Сердюк: В связи с принятием Федерального закона «О персональных данных», требования которого являются обязательными к исполнению, как для государственных, так и коммерческих организаций, в настоящее время, на первый план выходят риски, связанные с несоблюдением действующего законодательства в области защиты информации. Что касается самого процесса управления рисками информационной безопасности в российских кредитно-финансовых организациях, то он становится всё более системным и формализованным. Эта тенденция связана с появлением программных средств, позволяющих автоматизировать процессы оценки и анализа рисков безопасности, а также с принятием стандартов и методик, описывающих алгоритм управления рисками.

Не менее актуальными для российских банков являются риски безопасности, связанные с мошенническими действиями злоумышленников. Это связано с ростом финансовых потерь банков вследствие несанкционированных действий злоумышленников с целью кражи денежных средств со счетов клиентов банка. Потенциальные злоумышленники могут действовать как изнутри, так и извне банка.

— Что делать?

Виктор Сердюк: Я бы порекомендовал банкам попытаться создать полноценную систему управления рисками информационной безопасности, для чего попробовать реализовать комплексный подход, предусматривающий применение организационных, технических и нормативно-методических мер защиты.

В рамах технических мер по защите информации можно предусмотреть использование различных средств безопасности, включая межсетевые экраны, антивирусы, системы защиты от спама, системы обнаружения атак, сканеры безопасности, средства защиты конфиденциальной информации.

Что касается нормативно-методических мер, то они предполагают разработку и внедрение пакета документов, который должен учитывать требования международных и российских стандартов, в частности документов Центрального Банка России.

— Насколько важно использовать модные сегодня сервисы «Cloud computing» в банках, на что стоит обратить внимание?

Виктор Сердюк: При использовании таких сервисов возникают традиционные угрозы информационной безопасности, связанные с нарушением конфиденциальности, целостности и доступности. Специфика защиты данного вида сервисов заключается в том, что за обеспечение безопасности в данном случае отвечает не конечный пользователь, а провайдер, оказывающий услуги «Cloud computing».

— Нужно ли российскому банку соответствовать требованиям стандарта СТО БР ИББС?

Виктор Сердюк: Стандарт носит рекомендательный характер, однако ввод комплекса документов в области стандартизации Банка России внутренним рас-

Текст:
Сергей Советов

порядительным документом организации (приказом или распоряжением), позволяет руководствоваться им при проведении работ по защите информации, отнесенной к персональным данным, банковской и коммерческой тайне, что повышает эффективность и упрощает задачу по реализации требований законодательства к обработке персональных данных.

Комплекс работ по реализации требований СТО БР ИББС это последовательность этапов, являющихся частью общего цикла системы обеспечения информационной безопасности. Во-первых, предварительная оценка соответствия. Целью данного этапа является оценка текущего состояния информационной безопасности, выявление несоответствий требованиям стандарта СТО БР ИББС, а также разработка рекомендаций по устранению обнаруженных несоответствий. Второй этап — внедрение. Здесь осуществляются работы по определению информационных активов, подлежащих защите, оценке актуальных угроз и рисков, разработке комплекта нормативной и регламентирующей документации, внедрению необходимых технических средств защиты с целью приведения в соответствие с требованиями стандарта Банка России. На данном этапе так же применяются «Методические рекомендации по выполнению законодательных требований при обработке персональных данных в организациях БС РФ».

Третий этап, необходимый для оценки достигнутого уровня соответствия требованиям стандарта — Оценка соответствия. Результаты являются основой для совершенствования СОИБ. По результатам этапа выпускается «Подтверждение соответствия организации, банковской системы РФ стандарту Банка России СТО БР ИББС-1.0–2010», который должен быть направлен в адрес Банка России, Роскомнадзор, ФСТЭК России и ФСБ России.

Результатом вышеперечисленных работ, является повышение устойчивости бизнеса за счет снижения рисков информационной безопасности и соответствие не только требованиям признанного отраслевого стандарта, которым является СТО БР ИББС, но и законодательным требованиям, в том числе, требованиям Федерального закона «О персональных данных».

Необходимо отметить, что ЗАО «ДиалогНаука» является членом сообщества ABISS, имеет статус организации-консультанта и располагает необходимым опытом и компетенциями для проведения оценки соответствия информационной безопасности требованиям стандарта СТО БР ИББС.

— Как повысить защищенности автоматизированных банковских систем?

Риски использования услуг «Cloud computing», а также возможные варианты их минимизации:

• Несоответствие требованиям законодательства стандартов в области информационной безопасности. Так, при начале работы с провайдером, необходимо убедиться, что его автоматизированная система соответствует всем необходимым требованиям по безопасности информации, например ФЗ «О персональных данных», PCI DSS, ISO 27002 и др.

• Нарушение работоспособности инфраструктуры провайдера. При планировании применения услуг «Cloud computing» необходимо удостовериться в том, что инфраструктура провайдера защищена от возможных сбоев и отказов. Также необходимо получить гарантии максимального времени восстановления информации, в случае возникновения нештатных ситуаций.

• Несанкционированный доступ к информации, обрабатываемой на стороне провайдера. Как правило, провайдер предоставляет услуги «Cloud computing» одновременно большому количеству организаций, при этом все данные в большинстве случаев содержатся в одном хранилище. Поэтому необходимо проверить, что провайдер использует технологии защиты, обеспечивающие разграничение доступа к данным.

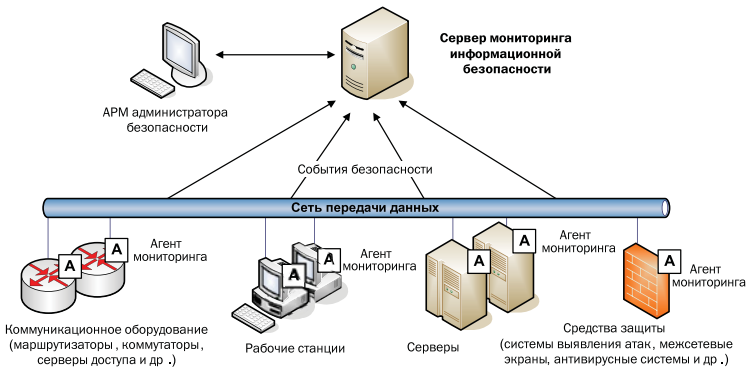
Состав системы мониторинга:

• Агенты мониторинга, предназначенные для сбора информации, поступающей от различных средств защиты;

• Сервер событий, обеспечивающий централизованную обработку информации о событиях безопасности, которая поступает от агентов. Обработка осуществляется в соответствии с правилами, которые задаются администратором безопасности;

• Хранилище данных, содержащее результаты работы системы, а также данные, полученные от агентов;

• Консоль управления системой, позволяющая в реальном масштабе времени просматривать результаты работы системы, а также управлять её параметрами.



Виктор Сердюк: Для повышения эффективности принятия решений по реагированию на события, связанные с нарушением безопасности мы рекомендуем использовать специализированные системы мониторинга, которые могут автоматизировать процесс сбора и анализа информации, поступающей от различных средств защиты. В западной терминологии такие системы мониторинга обозначаются аббревиатурой SIM (Security Information Management) или SIEM (Security Information and Event Management).

В настоящее время наибольшее распространение получили следующие коммерческие системы мониторинга событий информационной безопасности: ArcSight, Cisco MARS, RSA Envision, NetForensics, NetIQ, Symantec, и др. Необходимо отметить, что кроме коммерческих существуют также и бесплатные системы мониторинга с открытым кодом. Примером такой системы является продукт Prelude Universla SIM.

— Каковы особенности внедрения систем мониторинга?

Виктор Сердюк: Процесс внедрения любой системы мониторинга событий информационной безопасности включает обследование автоматизированной системы, когда проводится идентификация основных источников событий безопасности, определение технологии сбора, хранения и обработки данных. По результатам обследования формируются требования к архитектуре и функциональным возможностям системы. При разработке технического проекта, в котором описывается конфигурация оборудования и программного обеспечения, определяется порядок внедрения, схема информационных потоков, требования к внешнему окружению системы мониторинга и т.д.

На основе систем мониторинга могут быть созданы полноценные центры управления информационной безопасностью (SOC, Security Operation Centers). Для создания и внедрения полноценного центра управления необходимо разработать и внедрить комплекс документов, описывающий процессы работы центра, роли сотрудников, работающих в центре, процедуры взаимодействия центра управления информационной безопасностью с другими подразделениями, например, с центром сетевого управления (Network Operation Center, NOC) и т.д. Кроме этого, для эффективной работы SOC необходимо обеспечить выделение сотрудников, ответственных за работу с центром управления.

— Как защитить банк от фрода?

Виктор Сердюк: Сегодня проблема защиты от мошеннических действий злоумышленников является одной из наиболее актуальных задач для большинства российских банков. Для своевременного выявления фактов мошенничества (или так называемого банковского фрода) необходимо провести анализ банковских транзакций и выявить те из них, которые представляют угрозу для кредитной организации. Большинство банков ежедневно совершает огромное количество транзакций, поэтому обработать их в ручном режиме практически невозможно, а значит, для решения данной задачи необходимо использовать специализированные комплексы, позволяющие автоматизировать процесс анализа проводимых банком транзакций. Одним из примеров такого комплекса является продукт FraudView, разработанный компанией ArcSight.

ArcSight FraudView представляет собой специализированный программный комплекс, предназначенный для выявления фактов мошенничества со стороны злоумышленников в кредитно-финансовых организациях. FraudView позволяет легко интегрироваться со всеми основными банковскими прикладными системами, включая системы дистанционного банковского обслуживания «Банк-Клиент», «Интернет-Банк», автоматизированные банковские системы и др. При этом система позволяет в реальном масштабе времени осуществлять обработ-

ку и корреляцию данных, поступающих не только от прикладного ПО, но также и от средств защиты информации, общесистемного ПО, коммуникационного оборудования и т. д. Это позволяет выявлять сложные информационные атаки, направленные на совершение мошеннических действий.

Система включает в себя большое количество уже готовых правил корреляции, позволяющих выявлять различные виды мошенничества. При этом система предусматривает возможность добавления новых правил, что позволяет учесть специфику операционной деятельности российских банков. Помимо использования базы данных экспертных правил, система также позволяет выявлять банковский фрод посредством обнаружения отклонений от штатной работы банковских систем и их пользователей. Данные отклонения выявляются на основе статистических методов, а также нейросетевых алгоритмов.

Существует множество технологий и продуктов для выявления мошенничества, применяемых в банковском секторе. С общей точки зрения выгода от использования ArcSight FraudView заключается в том, что данное решение позволяет не просто заменить эти продукты, а связывать воедино полученные данными продуктами результаты с помощью корреляции. Помимо высокой производительности корреляции, данный программный продукт обладает тремя уникальные возможностями для обнаружения онлайн-мошенничества:

— Как оценить уровень защищенности банка от возможных угроз безопасности?

Виктор Сердюк: Одним из наиболее эффективных инструментов является проведение тестирования на проникновение (так называемый «penetration testing»). Эта услуга представляет собой имитацию последовательности действий взломщика по осуществлению несанкционированного проникновения в информационную систему банка. Этот вид аудита сегодня активно применяется зарубежными компаниями для получения независимой оценки защищенности своей корпоративной сети. Согласно стандарту PCI DSS рекомендуется проводить тест на проникновение не реже одного раза в год, а также после любого значимого изменения или обновления ИТ-инфраструктуры.

В отличие от традиционных схем проведения аудита информационной безопасности, тестирование на проникновение позволяет взглянуть на безопасность банка глазами профессионального взломщика, мотивированного на эффективное и результативное проникновение. Перед «взломщиком» ставятся задачи, максимально приближённые к реальной действительности, и непосредственно перед началом работы «взломщик» имеет самое минимальное представление об объекте проникновения. Цель, преследуемая тестированием на проникновение, заключается в получении контроля над какими-либо заранее обусловленными компонентами атакуемой системы всеми доступными взломщиком способами, и вся работа взломщика подчинена достижению этой цели. При этом политика безопасности и системы защиты, применяющиеся в атакуемой системе, рассматриваются как препятствия, которые необходимо преодолеть.

В качестве исходных данных в начале проекта банк может предоставить минимум информации в виде одного или нескольких внешних IP-адресов компании, доступных из сети Интернет. Этого будет достаточно для того, чтобы провести полноценный тест на проникновение.

— Как защититься от имитаторов взлома?

Виктор Сердюк: Перед началом проведения теста на проникновения между банком и исполнителем должно быть подписано соглашение о неразглашении (NDA), в рамках которого гарантируется сохранение в тайне всей конфиденциальной информации, которая будет получена в процессе выполнения работ. В рамках договора на выполнение работ также может отдельно определяться цель теста на проникновения. Например, в качестве такой цели может выступать получение прав администратора АБС, или демонстрация возможности получения доступа к номерам пластиковых карт клиентов банка и др.

Согласно исследованиям аналитических компаний IDC и Gartner одну из лидирующих позиций среди компаний-производителей систем мониторинга информационной безопасности на сегодняшний день занимает ArcSight (www.arcsight.ru). Флагманский продукт этой компании — ArcSight ESM — позволяет в полном объеме решить задачи, связанные с мониторингом событий информационной безопасности. Кроме этого, в отличие от других продуктов, представленных на российском рынке, система ArcSight ESM имеет сертификат соответствия ФСТЭК России.

Внедрение системы ArcSight ESM также позволяет обеспечить соответствие требованиям стандарта PCI DSS в части мониторинга:

- 10.2 — возможность реализации централизованного сбора событий с составлением отчетности о зафиксированных событиях;
- 10.5.1 — реализация разграничения доступа к просмотру журналов аудита;
- 10.5.2 — реализация защиты журналов аудита путем контроля доступа и централизации журналов на выделенном сервере;
- 10.6 и 12.9.5 — использование инструментария для сбора, анализа событий и уведомления;
- 10.7 — реализация хранения журналов.