Антон СВИНЦИЦКИЙ
директор по консалтингу
АО «ДиалогНаука»

SWIFT В СТРАНЕ БЕЗОПАСНОСТИ

ТРЕБОВАНИЯ SWIFT CSCF КАК ИНСТРУМЕНТ ДОВЕРИЯ

Международная система обмена платежными поручениями SWIFT существует давно. Она обеспечивает обмен платежными поручениями между банками в разных странах, реализуя разветвленные международные транзакции. Объемы транзакций между участниками системы SWIFT огромны, что и привлекает к ней внимание компьютерных мошенников.

ПРОБЛЕМЫ SWIFT

Большое количество участников и существенные объемы транзакций делают систему очень привлекательной для хакеров, которые уже давно изучают возможности манипуляции платежными поручениями на уровне клиентов системы SWIFT (банков) — такие махинации очень прибыльны даже в единичных случаях. При этом для подготовки и проведения атаки, направленной на отправку нелегитимного платежного поручения, используется не только инфраструктура SWIFT, размещенная в корпоративной сети банка, но и ее окружение.

Наиболее известный пример атаки на SWIFT — «цифровое» ограбление национального банка Бангладеш на общую сумму 81 млн долл., которое было совершено в феврале 2016 года. Злоумышленниками было организовано около 40 фиктивных запросов на общую сумму 951 млн долл., из которых четыре транша было пропущено, и в результате со счетов ЦБ Бангладеш в ФРС Нью-Йорка было переведено в филиппинские казино 81 млн долл. Атака была совершена с помощью троянской программы, которая обеспечила удаленный контроль узла доступа к инфраструктуре SWIFT в банке.

Аналогичная атака была совершена и на один российский банк в середине декабре 2017 года, хотя ни имя банка, ни ущерб не озвучивается. Сообщается только, что украденные средства были переведены за рубеж, а при проверке системы безопасности банка со стороны Банка России, проведенной после данного инцидента, были обнаружены серьезные проблемы. Эксперты Group-IB посчитали, что к преступлению может иметь отношение группировка Cobalt.

С УЧЕТОМ ЭТОЙ ТЕНДЕНЦИИ МОЖНО С УВЕРЕННОСТЬЮ ПРЕДПОЛОЖИТЬ, ЧТО АТАКИ НА БАНКИ И ИНФРАСТРУКТУРУ SWIFT БУДУТ ПРОДОЛЖАТЬСЯ

Последняя же крупная зафиксированная атака на SWIFT относится уже к апрелю этого года, когда неизвестные злоумышленники вывели около 20 млн долл. из национального банка Мексики. С учетом этой тенденции можно с уверенностью предположить, что атаки на банки и инфраструктуру SWIFT, направленные на несанкционированный перевод денежных средств, будут продолжаться.

Следует отметить, что не всегда проблемы возникают на стороне SWIFT — во многих случаях банки, из которых выводятся деньги, сами виноваты в проблемах, поскольку не уделяли достаточного внимания вопросам обеспечения информационной безопасности корпоративной информационной системы и организации безопасного информационного взаимодействия в рамках реализации процесса перевода денежных средств через систему SWIFT.

ТРЕБОВАНИЯ SWIFT CSCF

Понимая важность обеспечения защиты не только внутри самой сети, но и клиентов, SWIFT в мае 2016 года инициировала процесс реализации единого подхода к формированию требований по обеспечению информационной безопасности инфраструктуры SWIFT, размещенной у банков, а также проведения самооценки участков обмена на предмет наличия у них необходимых контролей. Сами требования формализованы в документе SWIFT Customer Security Controls Framework (CSCF) и состоят из 27 контролей, 11 из которых пока являются рекомендуемыми к реализации.

Требования SWIFT CSCF скорее технические и больше похожи на стандарт PCI DSS, чем на обобщенные требования, описанные в международном стандарте ISO/IEC 27002:2013. Впрочем, в самом документе есть таблица соответствия между контролями SWIFT CSCF и следующим набором стандартов: PCI DSS 3.2, ISO/IEC 27002:2013 и NIST Cybersecurity Framework v1.0. Это упрощает задачи специалистов, которые ранее использовали в своей работе перечисленные стандарты, и позволяет им быстрее разобраться в требованиях SWIFT. Набор требований, необходимых к реализации, зависит от типа подключения к сети SWIFT: выделено четыре типа подключения клиента в зависимости от расположенных в корпоративной сети клиента компонент. Но даже в случае подключения к сети SWIFT через поставщика услуг, необходимо реализовывать 11 обязательных контролей, направленных на защиту процесса перевода и ИТ-инфраструктуры.

Стандарт безопасности формулирует требования для основных компонентов и объектов среды их обработки: приложений (ПО, реализующее интерфейсы взаимодействия, SWIFTNet Link, коннекторы), сетевых сегментов размещения инфраструктуры SWIFT, сетевого оборудования, съемных носителей, оборудования (серверы, рабочие станции, HSM), рабочих мест операторов, а также иных систем и компонентов, обеспечивающих формирование и передачу сообщений SWIFT.

МЯГКАЯ СИЛА SWIFT CSCF

До 31 декабря 2017 года банки должны были провести самооценку и отчитаться о ее результатах в SWIFT. Однако никаких штрафов и наказаний за отсутствие результатов самооценки не будет, кроме возможного предупреждения со стороны регулятора, в случае России — Центробанка РФ. Списки банков, не заявивших о завершении процедуры самооценки, уже должны быть переданы российскому регулятору в начале 2018 года.

РИСК НЕСОБЛЮДЕНИЯ ТРЕБОВАНИЙ НА ДАННОМ ЭТАПЕ ИСКЛЮЧИТЕЛЬНО РЕПУТАЦИОННЫЙ, ЧТО ДЛЯ МЕЖДУНАРОДНОЙ БАНКОВСКОЙ СРЕДЫ МОЖЕТ ОКАЗАТЬСЯ ПРИНЦИПИАЛЬНЫМ

В рамках самооценки банки должны либо заявить о реализации контроля, либо указать срок, в течение которого контроли будут реализованы. Однако этот срок ограничен 4 кварталом 2018 года.

То есть до конца этого года все организации, имеющие собственный BIC, должны реализовать все требуемые контроли, если они не хотят привлекать внимание основного регулятора. В дальнейшем предполагается раз в год также проводить переоценку ситуации, чтобы не упустить происходящих изменений.

Следует отметить, что SWIFT не создает собственной системы проведения аудита — компания полностью доверяет в этом вопросе регуляторам и партнерам. Так, например, компания ДиалогНаука входит в список Directory of CyberSecurity Service Providers, опубликованный на сайте SWIFT, где указаны компании, готовые предоставлять услуги по кибербезопасности для клиентов SWIFT, в том числе услуги по проведению оценки соответствия требованиям стандарта CSCF.

Риск несоблюдения требований на данном этапе исключительно репутационный, что для международной банковской среды может оказаться принципиальным. Предполагается, что если банк не выполнил требования безопасности SWIFT, об этом должны узнать его партнеры, которые самостоятельно принимают решения о том, доверять ли сообщениям от данного контрагента или нет. От самой SWIFT штрафов за несоблюдение требований не предполагается, но международную репутацию может быть очень трудно исправить.

САМООЦЕНКА И ПРИВЕДЕНИЕ В СООТВЕТСТВИЕ

Сама процедура самооценки предполагает следующие этапы:

- определение области действия стандарта и типа подключения к инфраструктуре SWIFT;
- составление плана и программы аудита, что может быть выполнено в том числе и сторонней организацией;
- проведение оценки соответствия, во время которой клиенты должны заполнить специальную анкету, где перечислены все обязательные и рекомендательные контроли и их реализация;
- регистрация отчета на портале The KYC Registry, где и нужно указать напротив каждого контроля его статус. Варианты могут быть следующие: «соответствие рекомендациям Implementation Guidelines», «соответствие с применением альтернативных мер», «планируемое соответствие» с указанием срока, «несоответствие» и «не применимо»;
- формирование плана устранения несоответствий, в результате которого поля, отмеченные как «несоответствие», должны быть заменены на «планируемое соответствие» с указанием даты.

Предполагается, что к концу этого года нужно запланировать и привести в соответствие все контроли SWIFT.

* * *

На текущий момент гибкий подход SWIFT к возможности заменить любой контроль, описанный в SWIFT CSCF, на аналогичный контроль, направленный на снижение таких же рисков информационной безопасности, позволяет учитывать особенности ИТ-инфраструктуры и технологических процессов, но не позволяет сравнивать результаты оценки соответствия разных организаций. Скорее всего, дальнейшее развитие стандарта будет зависеть от практики внедрения и успешности/неуспеха хакерских атак на систему.