Заявление участников Форума по наблюдению за SWIFT
«О киберустойчивости финансовой экосистемы»

ЦЕЛЬ

В свете произошедших недавно событий в области информационной безопасности Форум по наблюдению за SWIFT (далее – Форум) разработал данный документ с целью продекларировать общее понимание важности мероприятий по обеспечению информационной безопасности, проводимых участниками SWIFT, как элемента информационной безопасности всей финансовой системы. Вследствие этого, финансовым организациям, имеющим доступ к сети SWIFT, следует руководствоваться рекомендациями, разработанными SWIFT, и активизировать изучение вопросов киберустойчивости для выявления возможностей ее повышения. Участники Форума доводят данный документ до органов, осуществляющих надзор и наблюдение за банками и инфраструктурами финансового рынка своей юрисдикции, как основу для диалога, в том числе, с их поднадзорными организациями.

Органы, осуществляющие наблюдение/надзор за SWIFT, будут следить за развитием событий и проводить оценку возможностей, которые могут быть использованы органами власти для повышения осведомленности и улучшения надзорных ожиданий.

НАБЛЮДЕНИЕ ЗА SWIFT

Цель совместного наблюдения за SWIFT состоит в получении гарантий создания в рамках SWIFT соответствующих структур управления, процедур принятия управленческих решений, процессов и процедур риск менеджмента и контроля в целях эффективного управления исходящими от SWIFT потенциальными рисками для устойчивости и надежности финансовых организаций и, в более широком смысле, для глобальной финансовой стабильности. Это достигается посредством реализации системы, ориентированной на достижение целей в отношении безопасности, операционной надежности, непрерывности деятельности и киберустойчивости инфраструктуры[1].

НЕДАВНИЕ КИБЕРАТАКИ, ПРОИЗОШЕДШИЕ В ФИНАНСОВОЙ ЭКОСИСТЕМЕ

SWIFT проинформировал участников Форума и своих клиентов, что произошедшие недавно кибератаки на участников сети передачи финансовых сообщений SWIFT не подвергли риску сеть SWIFT, сервис SWIFT по передаче финансовых сообщений или подключение к сети SWIFT. Тем не менее, данные атаки продемонстрировали, что у злоумышленников есть возможности:

- скомпрометировать платежную среду финансовых организаций, обойдя используемые средства информационной безопасности данных финансовых организаций;

[1] Приложение F к документу КПРИ-МОКЦБ «Принципы для инфраструктур финансового рынка» основано на данных принципах http://www.bis.org/cpmi/info_pfmi.htm .

- получить и использовать оригинальные ключи для создания, подтверждения и направления финансовых сообщений от имени скомпрометированных финансовых организаций;
- использовать созданное под конкретную финансовую организацию вредоносное программное обеспечение для отключения функций регистрации, информирования и иных средства контроля в целях сокрытия несанкционированных трансакций и задержки их выявления;
- в сжатые сроки перевести украденные денежные средства через множество юрисдикций с тем, чтобы исключить возможность их возврата.

Финансовые организации со слабыми средствами управления информационной безопасностью уязвимы для таких атак. Злоумышленники теперь все чаще используют передовой опыт, а также широкий спектр возможностей и функций программных продуктов, используемых финансовыми организациями. Следовательно, финансовые организации могут подвергнуться значительным денежным потерям, а также правовым, комплаенс- и репутационным рискам.

УПРАВЛЕНИЕ И РИСК-МЕНЕДЖМЕНТ

Финансовым организациям следует использовать те же самые стратегии, системы и средства в части управления и риск-менеджмента по отношению к киберугрозам, что и применяемые в отношении других видов риска. Принимая во внимание эскалацию киберугроз, важно, чтобы финансовые организации признали необходимость эффективного управления риском информационной безопасности, которое включает в себя применение как технических средств контроля и управления, так и надлежащих механизмов корпоративного управления. В частности, инфраструктура риск-менеджмента должна включать сложившуюся практику риск-менеджмента и средства управления информационными технологиями, а также сетью передачи финансовых сообщений, включая аутентификацию, авторизацию, выявление и предотвращение противоправных действий третьих лиц, системы и процессы реагирования на угрозы. Она также должна охватывать людей и процессы. Постоянная оценка способности финансовых организаций снижать риски, связанные с информационной безопасностью и поставщиками услуг в области информационной безопасности, также крайне важна для соответствующего реагирования на киберугрозы, для которых характерна технологическая сложность, рост частоты реализации и высокая способность к адаптации.

Форум определил несколько источников, содержащих руководства по обеспечению информационной безопасности.

РУКОВОДСТВА ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Финансовые организации, в конечном счете, остаются ответственными за собственную IT среду и инфраструктуру. Финансовые организации должны использовать несколько уровней обеспечения информационной безопасности, являющихся линиями защиты, и гарантировать, что их меры по управлению рисками ориентированы, в том числе на противостояние угрозам вследствие компрометации ключевой информации. Кроме того, когда это применимо, финансовые организации должны использовать руководства,

представляемые сторонними поставщиками услуг и органами регулирования деятельности финансовых организаций для получения рекомендаций по обеспечению информационной безопасности.

Утвержденное руководство по обеспечению киберустойчивости для инфраструктур финансового рынка и других финансовых организаций акцентировано на нескольких направлениях, включающих, но не ограниченных следующим:

a) проведением на постоянной основе оценки риска информационной безопасности;
b) выполнением процессов мониторинга, предотвращения и снижения риска нарушения информационной безопасности;
c) обеспечением защиты от несанкционированного доступа;
d) внедрением и тестированием на постоянной основе средств управления критически важными системами;
e) поддержанием в актуальном состоянии знаний о современных киберугрозах и программ обучения сотрудников;
f) обменом информацией о произошедших инцидентах;
g) оценкой и управлением рисками, возникающими при привлечении сторонних поставщиков услуг.

Следующие ресурсы содержат примеры, как можно поддерживать развитие и управлять инфраструктурой, обеспечивающей киберустойчивость в финансовой организации.

Руководства для инфраструктур финансового рынка:

- CPMI-IOSCO, "Guidance on cyber resilience for financial market infrastructures", June 2016, https://www.bis.org/cpmi/publ/d146.htm
- CPMI-IOSCO "Principles for financial market infrastructures," Annex F: Oversight expectations applicable to critical service providers http://www.bis.org/cpmi/publ/d101a.pdf
- CPMI paper "Cyber resilience in financial market infrastructures", November 2014 http://www.bis.org/cpmi/publ/d122.pdf

Несмотря на то, что указанные руководства по обеспечению киберустойчивости ориентированы на инфраструктуры финансового рынка, подходы, используемые в них, одинаково применимы и для банков.

Большая часть юрисдикций разработала собственные руководства, например:

- FFIEC Cybersecurity Awareness. http://www.ffiec.gov/cybersecurity.htm
- Federal Reserve Banks Operating Circular No. 5 Electronic Access, Effective June 30, 2016. https://frbservices.org/files/regulations/pdf/operating_circular_5_06302016.pdf

SWIFT подготовил единое руководство для своих пользователей по вопросам киберустойчивости. Дополнительные практические руководства SWIFT и инструкции по информационной безопасности представлены на https://www.swift.com/