Актуальные аспекты ИБ в финансовом секторе

ВАЛЕРИЙ ВАСИЛЬЕВ

Снижение экономической активности в мире, обострение международной политической ситуации, принятие и расширение странами с развитой экономикой в отношении России экономических санкций, затрагивающих в том числе и финансовый сектор нашей страны, и, как следствие, декларируемая руководством страны установка на экономическую и технологическую независимость через импортозамещение дают серьезное основание для переоценки ИБ-рисков и уровня защищенности ИКТ-систем в банковских и других финансовых структурах страны.

ОБЗОР

Изменения в экономико-политических процессах не могут не влиять на приоритетность ИБ-рисков как важной части общей структуры бизнес-рисков финансовых организаций. Не стоят на месте и технологии кибератак. В частности, злоумышленники все более широко и эффективно используют целенаправленные атаки (APT-атаки), что также влияет на изменение структуры ИБ-рисков и заставляет российские предприятия искать адекватные способы и средства защиты.

В этом тематическом обзоре мы постараемся дать оценку того, как изменяющиеся в настоящее время экономические, политические и технологические условия ведения финансового бизнеса влияют на организацию его информационной безопасности.

Современные тенденции в ландшафте ИБ-рисков и угроз финансовых организаций

Напрямую изменения, происходящие в экономике и политике, не влияют на ИБ-риски и угрозы для финансового сектора, считает ведущий аналитик отдела практического анализа защищенности Центра информационной безопасности компании "Инфосистемы Джет" Артем Бычков. Тем не менее структура ИБ-рисков может изменяться вслед за корректировкой бизнес-стратегий банков, которые как раз и определяются изменениями в экономической и политической ситуациях, причем снижение активности на рынке капиталов и утрата доступа к европейским и североамериканским кредитам уже заставляют российские банки менять свои стратегии: переходить от активного кредитования к тщательному анализу заемщиков, пересматривать в кредитных портфелях доли в пользу кредитования импортозамещения в таких отраслях, как ИКТ, сельское хозяйство, оборонная промышленность.

"Как конкретно меняется ландшафт ИБ-угроз, — сказал г-н Бычков, — сейчас сказать трудно, поскольку этот процесс хотя и неотвратим, но инерционен, и результаты этих изменений проявятся позднее". Он рекомендует специалистам ИБ-служб российских финансовых учреждений сосредоточиться сегодня на постоянном мониторинге стратегии бизнеса своих компаний и адекватном подстраивании под нее корпоративных ИТ- и ИБ-стратегий.

При этом есть все основания ожидать сокращения ИТ-бюджетов, считает руководитель отдела информационной безопасности системного интегратора IBS Platformix Джабраил Матиев. Природа инвестирования в ИБ, по его словам, схожа с бюджетированием страхования, расходы на которое заметно сокращаются, когда снижается доходность и повышаются риски закрытия бизнеса, а российские финансовые организации сегодня переживают непростой период — прибыли у них существенно сокращаются. Тем не менее достигнутый к сегодняшнему дню запас прочности в корпоративной ИБ, полагает г-н Матиев, позволит российским финансовым компаниям благополучно пережить нынешнее непростое время. Во многом он видит в этом заслугу регуляторов, которые внимательно контролируют состояние ИБ в отрасли.

Менее оптимистично оценивает ситуацию заместитель генерального директора компании "Аладдин Р.Д." Алексей Сабанов. Соглашаясь с тем, что экономические проблемы, с которыми столкнулась сегодня наша страна, ведут к сокращению корпоративных ИБ-бюджетов, и будущие ИБ-проекты, скорее всего, будут сильно урезаны, он полагает, что уже в ближайшее время это сокращение негативно скажется на состоянии ИБ финансовой (и не только) отрасли.

ИБ-угрозы первого плана

Хотя наши эксперты не отмечают явного влияния перемен, происходящих в международной политике и внутренней экономической ситуации, на всю совокупность ИБ-рисков и угроз для финансового бизнеса, они указывают на изменения в возможности реализации некоторых из них, выделяя наиболее частые и угрожающие наибольшим ущербом.

Так, к наиболее вероятным эксперты относят традиционный инсайд — ущерб от непреднамеренных и злонамеренных действий собственных сотрудников. По-прежнему большой ущерб финансовым организациям приносит мошенничество, актуальны риски, связанные с утечками чувствительной информации, а вот ИБ-риски, связанные с невыполнением требований регуляторов (согласно наблюдениям г-на Матиева), временно отошли на второй план.

Ведущий аналитик отдела развития компании "Доктор Веб" Вячеслав Медведев отметил рост числа DDoS-атак на банки. Он обратил внимание также на появившиеся в 2014 г. специализированные вирусы для банкоматов, которые внедряются в них через сменные устройства. "Появление подобных узкоспециализированных вредоносов подтвердило мнение антивирусных аналитиков о недопустимости использования для ИБ-защиты банкоматов только средств контроля целостности", — констатировал он.

Сложности в экономической ситуации, как отметил г-н Бычков, стимулируют российские банки активнее использовать антикризисные меры. Для того чтобы добиваться конкурентных преимуществ, они, например, активнее развивают сервисы дистанционного банковского обслуживания и мобильного банкинга, что, в свою очередь, смещает акцент ИБ-угроз в эту сторону.

В результате экономических санкций российские финансовые учреждения (которые, как и большая часть других российских предприятий и организаций, широко используют в своей деятельности ИКТ-продукты зарубежного производства) уже столкнулись с проблемами в поддержке со стороны производителей импортных ИБ-продуктов. Эти случаи вызывают понятную озабоченность в финансовом сообществе.

Российские специалисты активно обсуждают возможные варианты противодействия санкциям на поставку зарубежного программного обеспечения, предпринимают меры по замене импортного сетевого оборудования на отечественное или оборудование из стран, не участвующих в экономических санкциях против нашей страны.

"И все-таки, — считает г-н Медведев, — российские заказчики в массе своей продолжают работать на ИКТ-оборудовании и комплектующих, разработанных иностранными компаниями, а это является источником самых серьезных ИБ-уязвимостей".

Актуальные технологические аспекты

К настоящему времени средства защиты от типовых ИБ-угроз стали универсальными, недорогими и высокоэффективными. Компаний, которые не располагают базовым набором таких инструментов, особенно в сфере финансов, в России практически не осталось. Как следствие, типовые атаки перестали представлять серьезные угрозы для финансовых структур и злоумышленники все чаще прибегают к так называемым целевым атакам.

Мы не будем пытаться в этом обзоре дать точное определение целевым атакам, поскольку специалисты пока еще не пришли к единодушному мнению на этот счет. Отметим лишь, что важнейшими их признаками являются сосредоточенность на одном объекте атаки и высокая устремленность к достижению поставленной цели, нередко связанная с привлечением больших денежных средств, широкого спектра технологий и длительным временем проведения атаки.

"Главная проблема защиты от целевых атак, — сказал г-н Матиев, — заключается в том, что они часто базируются на так называемых уязвимостях нулевого дня, к защите от которых не приспособлено ни одно классическое ИБ-средство. Однако уже существуют технологии, которые повышают вероятность оперативного обнаружения таких атак и противодействия им". Оперативность в данном случае важна, поскольку опасна не столько сама атака, сколько ее последствия, разрушительность которых при успешном развитии атаки может возрастать многократно.

Одна из технологий противодействия целевым атакам связана со сбором, анализом и корреляцией событий безопасности со всех объектов ИКТ-инфраструктуры, что позволяет улучшить видимость того, что происходит, и оперативно реагировать на аномалии. Другой пример — технология "песочниц", которая помогает детально изучать поведение различных программных приложений на предмет выявления признаков их возможной вредоносности.

В итоге же борьба с целенаправленными атаками заключается в создании комплексной системы обеспечения информационной безопасности (использующей в том числе и упомянутые технологии) и постоянном ее совершенствовании. Это под силу только тем структурам, которые отличает высокий уровень корпоративной ИБ-зрелости.

В реальной злободневности целевых атак сомневается г-н Медведев: "Прежде чем согласиться с выводом об их актуальности, нам следует внимательно ознакомиться с методиками исследований, по итогам которых они отнесены к основным современным киберугрозам, и соотнести эти результаты с рекомендациями по защите от них".

Киберпреступникам, по его мнению, пока нет надобности организовывать дорогостоящие, требующие высокой квалификации целевые атаки, поскольку сегодня, например, все еще несложно взломать и заразить часто посещаемые популярные веб-сайты (более 80% из которых по-прежнему имеют уязвимости!), а пользователи сами придут туда и перенесут заражение на свои ИКТ-ресурсы. И это только один из гораздо более действенных, чем целевые атаки, возможных сценариев атаки.

"Публикации об APT-атаках, — считает г-н Медведев, — не должны мешать ИБ-специалистам знакомиться с информацией о все еще актуальных, но более простых уловках злоумышленников, например о выпускаемых сотнями в день вредоносных программах, по-прежнему без особых проблем находящих свои жертвы".

Большой бедой для финансовых структур наши эксперты считают низкий уровень корпоративной ИБ-культуры, распространенными признаками которой являются отсутствие оценок уровней опасности ИТ-угроз, опора на технические меры защиты, слабая работа с персоналом и клиентами по направлению ИБ. Неосведомленность и безалаберность персонала в сочетании с несовершенными механизмами разграничения доступа (на всех уровнях — от физического до уровня приложений) являются залогом успеха усилий злоумышленников, согласен с мнением коллег г-н Бычков.

Пренебрежение ИБ-обучением персонала, считает г-н Медведев, снижает эффективность функционирования и технических средств защиты. Есть ли, например, смысл, заметил он, устанавливать в банкоматы защиту систем контроля целостности, если внедрение троянцев в них происходит в результате вскрытия устройств штатным ключом? Кто и откуда смог взять этот ключ? Откуда получена информация о том, что именно в том банке, которому принадлежит вскрытый банкомат, не организован контроль за вскрытием? Как злоумышленники узнали, какие системы защиты стоят в банкоматах атакуемого банка? Известно, что злоумышленники активизируются в праздники, а сколько российских финансовых организаций формируют дежурные ИТ- и ИБ-бригады на то время, когда основной персонал отсутствует на рабочих местах? Прежде чем задумываться об отражении APT-атак, банки должны иметь ответы на все эти гораздо более простые вопросы, настаивает он.

"Наиболее часто используемые злоумышленниками уязвимости, ведущие к денежным потерям, — сказал г-н Сабанов, — связаны с кражей закрытых шифроключей клиентов банков, а также подменой данных в момент подписания и отправления платежей на исполнение". В связи с этим он обратил особое внимание на организацию процесса аутентификации клиентов в банковских системах.

Наши эксперты

АРТЕМ БЫЧКОВ, *ведущий аналитик Центра информационной безопасности, "Инфосистемы Джет"*

ДЖАБРАИЛ МАТИЕВ, *руководитель отдела информационной безопасности, IBS Platformix*

ВЯЧЕСЛАВ МЕДВЕДЕВ, *ведущий аналитик отдела развития, "Доктор Веб"*

АЛЕКСЕЙ САБАНОВ, *заместитель генерального директора, "Аладдин Р.Д."*

Цель хакеров

ВЯЧЕСЛАВ МЕДВЕДЕВ

В истории войн был период, когда для завоевания территории нужно было захватить расположенные на ней города. Изобретались все новые типы осадных орудий, рылись подкопы, подкупались предатели. А потом некто умный сообразил, что города эти не так уж и нужны — можно просто оставить их в осаде и в свое удовольствие пользоваться ресурсами, расположенными вне их границы. А горожане, чувствующие себя неуязвимыми внутри красивых стен, рано или поздно сами затащат к себе троянского коня — ибо нет пределов непослушанию и любопытству.

Тенденцией нынешнего года для мира компьютеров стал возросший интерес злоумышленников к никем не защищенным местам. Установка антивируса пользователями на свои рабочие и домашние машины давно стала обязательным делом ("у всех есть, и я поставил"). Но при этом меры по защите всего того, что не является рабочими станциями да еще файловыми серверами, предпринимаются крайне редко. И у хакеров созрела вполне логичная мысль, что штурмовать априори защищенный пункт, конечно, можно — но насколько проще внедриться туда, где угрозы никто не ждёт.

Linux? Система, по мнению почти всех ее приверженцев, написанная профессионалами, неуязвимость которой обеспечивается открытостью кода — "дыру" в программе просто невозможно скрыть! Но не так давно были найдены существовавшие многие годы уязвимости Heartbleed и Shellshock (желающие сравнить количество выявленных в этом году уязвимостей хотя бы с прошлогодними показателями могут воспользоваться любой поисковой системой). Shellshock, например, позволяет злоумышленникам выполнять произвольные команды на инфицированных устройствах, операционные системы которых основаны на ядре Linux и имеют в своем составе оболочку Bash. Такими устройствами могут быть серверы, модемы, роутеры, камеры наблюдения и масса других подключенных к Интернету аппаратных средств со встроенными операционными системами, причем ПО для многих из них практически не обновляется. На что, естественно, вирусописатели отреагировали мгновенно: в самом конце сентября были выявлены бэкдоры, атакующие Linux-устройства, — Linux.BackDoor.Shellshock.1 и Linux.BackDoor.Shellshock.2.

При этом если раньше вредоносные программы портировались на Linux, то китайские вирусописатели, отметившиеся в первой половине лета распространением огромного количества троянцев для Linux, созданных с целью организации массированных DDoS-атак, пошли иным путем, выпустив Trojan.DnsAmp.1 — Windows-совместимую версию одного из троянцев Linux.DnsAmp. После запуска Trojan.DnsAmp.1 отправляет на серверы злоумышленников информацию об инфицированном компьютере и ожидает команды, когда начинать DDoS-атаку. Помимо этого троянец может загрузить и запустить на исполнение другую вредоносную программу.

Mac OS X? Продукт культовой компании, предмет желания и подражания для многих. Только за сентябрь вирусные базы Dr.Web пополнились информацией о бэкдоре Mac.BackDoor.Ventir.1, шпионе Mac.BackDoor.XSLCmd и троянце Mac.BackDoor.iWorm, позволившем хакерам создать новый ботнет из "маков".

И это примеры только новых троянцев для систем на основе Linux и Mac OS X — если раньше появление вируса для данных ОС было практически событием года, то теперь оно превратилось в обыденность.

Но если уязвимость стала известной — могут ли в Багдаде спать спокойно, используя штатные средства безопасности? Согласно отчету Synack, XProtect — решение безопасности компании Apple — "позволяет выявить лишь активный установщик вирусного ПО… Те компьютеры, которые были заражены еще до выхода новой версии XProtect, все еще остаются инфицированными".

Производители антивирусов мгновенно отреагировали на изменение интересов хакеров. Если раньше средства защиты для Linux и Mac OS X по сути ограничивались файловым монитором и антивирусным сканером для периодических проверок, то новые версии Dr.Web для Linux и Dr.Web для Mac OS X, вышедшие в этом году, включают функционал антивирусной проверки HTTP-трафика, блокирующий возможность использования вредоносными программами еще незакрытых уязвимостей, а также офисный контроль, ограничивающий доступ к потенциально вредоносным ресурсам.

Любители конспирологии только хмыкнут с пониманием, но для тех, кто знает, как на самом деле создаются сейчас вредоносные программы, совсем не секрет, что их настоящие производители давно поставили производство на поток и способны выпускать десятки и сотни новых образцов в день — и расширение систем сбора новейших вредоносных программ уже не позволяет выявлять большинство выпущенных в эти сутки инфекций. Для противодействия ураганному натиску злоумышленников антивирусные решения для всех ОС улучшили системы сканирования запущенных процессов для обезвреживания активных — ранее неизвестных — угроз. Не стали исключением и решения для "альтернативных" систем.

Но вернемся к тому, какие объекты подвергаются заражению. По счастью, инфекции для мышек, аккумуляторов и принтеров остались на уровне концептов. А вот троянец для NAS был обнаружен в "дикой природе": Trojan.Encoder.737 шифровал файлы, хранящиеся в сетевых хранилищах производства компании Synology, и, что вполне логично, требовал выкуп за расшифровку.

Год назад вызвала фурор первоапрельская шутка компании "Доктор Веб" о вирусе для бортового компьютера автомобиля, однако прошло совсем немного времени, и, похоже, шутка превращается в грустную реальность — уже зафиксированы удачные попытки перехвата управления не только автомобилями, но и кораблями. Интернет вещей, пришествие которого проповедуют сегодня, по своей идеологии беззащитен перед злоумышленниками. Его проблемы, как ни парадоксально, сходны с проблемами защиты систем управления технологическими процессами (АСУТП), банкоматов и терминалов. Как правило, все подобные устройства имеют крайне малый объем оперативной памяти, слабые процессоры и т. д. Внедрение вирусов в эти системы возможно — а вот для антивирусов ресурсов уже не хватает. Что делать?

Да очень просто — заглянуть на сайты антивирусных вендоров. Защита незащищаемого обеспечивается с помощью антивирусных шлюзов: ничто вредоносное не должно пересечь границу. Традиционно компании пренебрегали использованием шлюзовых решений — и хакеры с готовностью пользуются плодами экономии.

Как ни странно, но созданию и функционированию надежной системы защиты препятствуют две вещи: слабая информированность специалистов по информационной безопасности о современных угрозах и мерах по защите от них и пренебрежение пользователей мерами безопасности. Хотя вторую проблему можно свести к первой.

Автор — ведущий аналитик отдела развития компании "Доктор Веб".

Ссылаясь на отчеты по киберпреступности компании Verizon, г-н Бычков поддерживает мнение, что наибольший ущерб современным компаниям (в том числе и финансовым) приносят все-таки не целевые атаки, а более привычные. APT-атаки выходят на первый план лишь в том случае, если компания-жертва располагает чем-то, представляющим существенную ценность для атакующего, а проведение типовых атак не приносит результата.

Влияние импортозамещения

Очевидно, что тема импортозамещения в первую очередь актуальна для тех структур, которые уже попали в санкционные списки. Однако и остальные участники финансового рынка тоже внимательно относятся к вопросам импортозамещения, заблаговременно предполагая возможность расширения санкций.

В финансовых структурах, отметил г-н Медведев, отечественные ИБ-продукты начали использоваться (там, где это возможно, например, в антивирусной защите) и до объявления стратегии импортозамещения. Однако активно расширять список таких продуктов, по его мнению, вряд ли получится в обозримом будущем, поскольку фактически для этого требуется создать замену широкому спектру базового программного и аппаратного обеспечения ИКТ.

Осознавая возрастание рисков приостановки бизнеса вследствие экономических санкций, предприятия российского финансового сектора, считает г-н Бычков, стали активнее искать ИКТ-решения в странах Азии, прежде всего в Китае. Наметился также тренд на увеличение доли разработок с использованием ПО с открытым исходным кодом, качество которых, по его мнению, зачастую выше, чем у отечественных проприетарных аналогов, а риски, связанные с непредсказуемостью поставщиков, практически отсутствуют.

Однако г-н Медведев, говоря о рисках, связанных с отказом иностранных вендоров (в связи с экономическими санкциями) в поставке импортного ПО, полагает, что замены широко распространенным в России операционным системам, СУБД и многому другому базовому ПО нет и в ближайшее время не будет, даже если иметь в виду использование ПО с открытым исходным кодом. Он связывает это с тем, что основную работу по развитию и поддержке этого ПО выполняют крупные коммерческие организации, большая часть которых находится в США, а действуют они в соответствии с законодательством этой страны, т. е. выполняют требования наложенных на Россию санкций. К тому же нужно учитывать. что увеличение доли ПО с открытым исходным кодом в построении корпоративной ИБ обусловливает рост спроса на квалифицированные ИБ-кадры. А взять их сегодня неоткуда.

С тем, что, когда дело касается импортозамещения средств защиты информации, российским разработчикам в той или иной мере есть что предложить рынку, согласен с коллегами г-н Матиев. Однако реализация импортозамещения других компонентов корпоративной ИКТ-инфраструктуры высокозатратна, хотя бы потому, что связана она с переходом на продукцию других производителей (которым к тому же еще только предстоит появиться).

Основные проблемы стратегии импортозамещения по направлению ИБ г-н Бычков связывает с тем, что, с одной стороны, на сегодняшний день нет пригодных к промышленному использованию средств защиты информации российского производства по целому ряду направлений, в частности SIEM, DB Protection, IPS/IDS, а с другой — поиск, тестирование и замена уже внедренных средств защиты информации потребует существенных ресурсных затрат, включая привлечение все тех же квалифицированных кадров.

"В сложившейся ситуации к первоочередным задачам следует отнести организацию защиты данных финансовых учреждений и проводимых ими финансовых транзакций за счет использования российских ИБ-средств", — считает г-н Сабанов По его оценкам, в короткие сроки решить данную задачу не удастся, но возможности и предпосылки для этого имеются.

GlobalLab...

ПРОДОЛЖЕНИЕ СО С. 9

в других регионах, чем отличаются результаты. В проекте "От грохота до шепота" мы использовали для исследований мобильные телефоны и работали в режиме онлайн с другими регионами.

Это оказалось очень действенным — ученики увидели, какие источники производят больше шума, какое влияние шум оказывает на спокойствие и здоровье. В процессе работы мы с учениками поняли, что сами же и являемся источником большого шума. В результате ребята выступили с инициативой "Спокойная перемена — крепкое здоровье".

Таким образом, благодаря масштабному учебному эксперименту был получен результат, которого невозможно было добиться нравоучениями и выговорами. Но самое главное — ученики убедились, что информационные технологии — не только подготовка красивых презентаций и поиск нужных сведений в Интернете. Это прежде всего мощный инструмент в руках научных сотрудников и инженеров.

Вот что рассказала заместитель директора по ИКТ физико-математического лицея № 86 г. Ижевска Анна Кологерманская: "В исследовании "Шум вокруг нас" приняли участие мальчики 6-б класса. Перед уроком они получили задание: разбиться на пары так, чтобы у каждой пары в наличии был хотя бы один гаджет (планшет или смартфон) с установленной программой для измерения шума.

В начале урока мы провели калибровку устройств, чтобы показания были правильными, и выбрали места для измерения. Каждая группа должна была измерить шум в двух местах. Были выбраны столовая, спортзал, коридоры в старшей и начальной школах, место около расписания, кабинет психолога, урочные кабинеты в старшей и младшей школах, туалет, приемная директора.

Для проведения эксперимента был выбран "спаренный" урок, чтобы можно было экспериментировать как на уроке, так и на перемене. Результаты получились следующие: самым тихим местом оказался кабинет психолога (из чего мы сделали вывод, что в этот кабинет можно ходить не только на беседы, но и для отдыха от шума). Самыми шумными местами оказались (по гипотезе, естественно, был спортзал) коридор рядом со столовой и коридор около расписания.

Проведенное исследование не повлияло на отношение к физике и информатике, но ученики поняли, что гаджеты можно применять не только для развлечений, но и для исследований. По результатам проведенной работы один ученик выступил с докладом на научно-практической конференции".