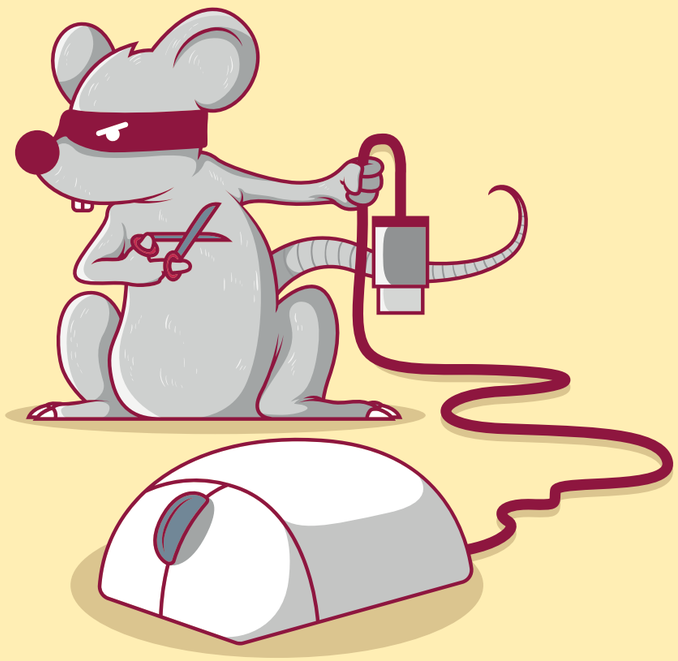
Новое технологическое мы́шление

Одним из основных итогов первого полугодия 2024 года в области кибербезопасности в финансовой сфере стало понимание реальной роли менеджмента в управлении ИБ. Но не только это



Текст
ВАДИМ ФЕРЕНЕЦ,
ОБОЗРЕВАТЕЛЬ **«Б.О»**



Продолжение роста активности социальных инженеров и сохранение на ИБ-радарах иных видов комбинированных атак, обычно начинающихся с фишинга или спама и заканчивающихся кражей персональных данных и закреплением злоумышленников в IT-инфраструктуре организаций, было предсказуемо и никого особенно не удивило.

Начало новых интриг, похоже, находится в области импортозамещения и переоценки роли менеджмента в обеспечении безопасности. Что касается обретения технологического суверенитета на фоне заявлений известных представителей мира ИБ о закрытии отечественными вендорами более 80% потребностей сектора, то явно что-то пошло не так.

И дело здесь не только в дефиците квалифицированных кадров, незрелости многих отечественных решений и менталитете некоторых «забронзовевших» ИБ-офицеров. На фоне лавинообразного роста количества кибератак банкам приходится непрерывно на ходу перестраивать свои ИБ-системы вслед за изменяющимися бизнес-моделями. Буквально на глазах множится «зоопарк» мало совместимых между собой IT- и ИБ-систем, большая часть которых уже переходит в разряд legacy, так и не успев стать лучшими в своем классе. А бизнес мчится в это время вперед…

О ситуации от первых лиц

Александр Бабкин, вице-президент — начальник департамента мониторинга ИБ ГПБ, признался в интервью CNews: «Сейчас ИБ-решения в Газпромбанке замещены только на 65%. Однако при подобных оценках учитывается только прикладной слой, т.е. непосредственно сами средства защиты информации (СЗИ) без учета системного слоя, включающего ОС и СУБД, которые необходимы для функционирования этих СЗИ. Переход на отечественные ОС и СУБД требуют от производителей защитных решений существенных трудозатрат, при этом ресурсы будут потрачены не на развитие функционала продукта, а на обеспечение совместимости с новым российским системным софтом, который также непрерывно меняется и дорабатывается».

К сожалению, по словам эксперта, при сравнениях в реальных условиях современной сетевой инфраструктуры финансового учреждения большинство отечественных решений (в том числе многострадальные межсетевые экраны нового поколения, NGFW) пока проигрывают зарубежным конкурентам по пропускной способности и функционалу, что особенно обидно с учетом высокой стоимости российских устройств, в несколько раз превосходящей импортные аналоги.

Вице-президент по кибербезопасности СберБанка **Сергей Лебедь** в июне 2024 года отметил: «Нам необходимо не только успевать за критическими изменениями ИБ-ландшафта, но и предугадывать их, быть впереди, заранее готовить механизмы реагирования. Стремительный рост технологической сложности работы банка на фоне развития цифровых угроз делает использование технологий ИИ жизненно необходимым для обеспечения кибербезопасности».

В данном контексте речь идет не столько об ИИ, сколько об острой необходимости в механизмах, интегрирующих существующие средства защиты для комплексной работы с рисками кибербезопасности и принятии управленческих решений топ-менеджерами всех уровней.

Изначально развитие систем кибербезопасности в Сбербанке шло по пути закупки и развертывания коробочных решений. Подобный подход обеспечивал надежную защиту от типовых угроз и возможность внедрения нового решения в кратчайшие сроки, но не позволял увидеть полноценную картину происходящего в IT-ландшафте, оценить риски и обеспечить их минимизацию.

Таким образом, хоть и не явно, но признается конфликт интересов IT-подразделений и бизнеса, с одной стороны, и ИБ и служб комплаенса, с другой. И это касается множества самых разнообразных участников финансового рынка, о чем не раз говорил в своих публичных выступлениях **Сергей Демидов,** директор департамента операционных рисков, информационной безопасности и непрерывности бизнеса Группы «Московская биржа». По его мнению, в рамках классических процессов ИБ волей-неволей эта служба становится тормозящим элементом в бизнес-схеме «фабрики» по производству цифровых продуктов, поскольку финансируется большей частью по остаточному принципу и не имеет достаточных ресурсов для ускорения. Мало того, противоречивость многочисленных регуляторных норм дала основания Сергею Демидову заявить: «Мы живем в эпоху невыполнимых требований».

Глазами хакеров

«Почему так важно изучать и оценивать результаты киберучений, работу киберполигонов и тестов на проникновение в IT-инфраструктуру “белыми“ хакерами? Потому что мы, “ИБ-шники”, часто живем в плену иллюзий о том, как будет действовать “живой“ хакер. И исходя из наших мыслей мы создаем модель угроз, а потом по ней строим систему ИБ. А у хакера могут быть совсем иной майндсет, как модно говорить на Западе, иное мышление и совсем иные способы реализации угроз, отличные от того, что напридумывал себе “ИБ-шник”», — прокомментировал итоги анализа проведения пентестов в 2023 году компанией Positive Technologies **Алексей Лукацкий,** бизнес-консультант по безопасности этой организации.

Важнейшим выводом этого документа, по мнению эксперта, является то, что офицеры ИБ постоянно сталкиваются с так называемой дилеммой защитника, когда им надо найти и закрыть все дыры в своей инфраструктуре, а хакеру нужно найти всего одну единственную. И чтобы эта дилемма решалась, нужно думать, как он, и действовать, как он. Тогда, вы сможете приблизиться к пониманию того, как вас будут реально ломать и что можно этому противопоставить.

Но это не тот путь, по которому предпочитают идти множество специалистов: зачем изучать чужой опыт, прекрасно зная, что написанные на бумаге и согласованные с регуляторами модели киберугроз являются той самой соломкой, которую не грех заранее подстелить. Одно дело — согласовать с ФСТЭК модель прошлых угроз и совсем другое — попробовать по ней защитить виртуальный город (банк, страховую компанию или завод) на киберполигоне. И уж третье дело — защищаться от реальных «плохих парней».

Какие проекты сейчас актуальны?

Как бы там ни было с трендами, здесь и сейчас банкиры пытаются с разной степенью успешности решать текущие проблемы. Кейсов довольно много, но есть те, о которых необходимо сказать отдельно.

Например, в феврале Т-Банк протестировал и запустил специальные мобильные команды из сотрудников «Тинькофф Защиты» для спасения жертв мошенников в тот момент, когда они планируют перевести злоумышленникам деньги. Незадолго до этого в 2023 году Тинькофф Банк объявил о запуске сервиса «Защитим или вернем деньги». Это сервис, который с помощью ИИ-технологий определяет мошенничество во время звонка с вероятностью более 99% и защищает клиентов от телефонных аферистов. А уже в апреле 2024 года Т-Банк запустил для всех своих сотрудников комплексную программу поиска уязвимостей, связанных с защитой данных, Data Guard. Кроме того, банк научился в автоматическом режиме выявлять дропов.

Невзирая на международную обстановку, ОТП Банк провел миграцию платформы противодействия мошенничеству на базе «СмартВиста» в рамках политики импортозамещения при активном участии компании БПС. Антифрод-платформа от БПС работает на PostgreSQL и осуществляет мониторинг всех транзакций, проводимых по каналам ДБО и банковским картам. Основным требованием команды ОТП Банка являлось сохранение всех исторических данных и базы прецедентов и расследований.

Как видно, комплексная защита клиентов от мошенничества становится причиной старта комплексных и сложных проектов. Однако в ближайшем будущем стоит ожидать не менее сложных интеграционных проектов банков как между собой, так и с элементами ИБ-инфраструктуры регуляторов. И они уже пошли! **Б.О**