ИБ своим чередом

Медиапроект «Банковское обозрение» подводит итоги первых шести месяцев 2023 года в области развития IT и ИБ в финансовой сфере на базе начатых или завершенных проектов, попавших в открытый доступ

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

Первое полугодие 2023 года в сфере банковской ИБ в целом не преподнесло существенных сюрпризов. Причина тому — пристальное внимание к этому направлению со стороны регуляторов. Детали были озвучены в ходе Уральского форума «Кибербезопасность в финансах» в феврале 2023 года **Германом Зубаревым,** заместителем председателя Банка России, в рамках ключевого доклада форума «Основные направления развития ИБ в кредитно-финансовой сфере».

В частности, на ближайшие три года ЦБ определил ключевые цели: повышение уровня доверия к цифровым технологиям, создание условий для безопасного внедрения цифровых и платежных технологий, достижение технологического суверенитета и обеспечение контроля рисков ИБ и операционной надежности. Эти задачи в целом и определили характер основной массы внедрений.

Безопасный удаленный доступ

Обращает на себя внимание значительное количество проектов в области семейства IdM-решений (Identity Management, управление учетными записями). На конференции IT IS Conf, прошедшей в июле 2023 года, компания Газинформсервис довольно емко зафиксировала происходящее в этом сегменте ИБ в названии своей презентации: «Синергия и сегрегация: NAC, SSO, PAM, IdM — новый взгляд на управление доступом».

«Финансовые организации традиционно внимательны к анализу рисков. Они же эксплуатируют сложные информационные системы, в том числе в разных режимах аутсорсинга и удаленного доступа, и логично, что угрозы такого типа они контролируют. Комплексные продукты по минимизации этих рисков позволяют защитить доступ к инфраструктуре организации и увидеть, какие действия на ней выполняют собственные сотрудники, подрядчики и аудиторы», — объяснил в интервью «Б.О» причины спроса на IdM-решения **Дмитрий Михеев,** технический директор компании «АйТи БАСТИОН».

Как пример: решение «СКДПУ НТ Шлюз доступа» этой компании было выбрано банком «Ренессанс» для защиты своей инфраструктуры при организации удаленного доступа для пользователей. Через данный шлюз к инфраструктуре организации удаленно подключаются как внутренние пользователи, так и внешние подрядчики, тем самым унифицируя решения и создавая дополнительный периметр безопасности удаленного доступа. Кроме того, удалось модернизировать процесс предоставления доступа администраторам IT-систем.

В марте 2023 года калининградский Энерготрансбанк успешно завершил внедрение комплексной системы аутентификации на основе продукта Indeed Access Manager от компании «Индид», что позволило запустить централизованную систему усиленной аутентификации при локальном и удаленном доступе к корпоративным IT-ресурсам банка. Чуть ранее крымский Генбанк при помощи «Индид» обеспечил защиту доступа к внутренним корпоративным ресурсам: к рабочим станциям с ОС Microsoft Windows и к удаленному шлюзу Microsoft RD Gateway. Для аутентификации используются одноразовые пароли, которые генерируются в мобильном приложении Indeed AirKey.

Кроме того, в январе было объявлено, что Группа СМП Банк внедрила централизованную систему управления цифровыми сертификатами Indeed CM. Проект позволил решить ряд задач в обслуживании инфраструктуры открытых ключей в банковской группе, например вопросы по управлению и инвентаризации ключевых носителей, управлению жизненным циклом сертификатов аутентификации и электронной подписи, ведению журнала учета средств криптографической защиты информации (СКЗИ).

Мониторинг всего и вся

Еще один вектор практического развития ИБ-сегмента в финансовых организациях связан с решением задач обеспечения real-time-мониторинга различных бизнес-процессов и с анализом «цифровых следов», остающихся в IT-системах. Как следствие наблюдается ряд проектов в области SOC/SIEM, антифрода и т.д.

Так, команда разработчиков Альфа-Банка создала специальную модель машинного обучения, которая следит за всеми транзакциями и моментально сообщает службе безопасности, если находит что-нибудь подозрительное. Робот оценивает каждую транзакцию по множеству показателей и решает, есть ли в ней отличие от безопасного сценария.

С помощью продвинутой аналитики за 0,03 секунды в банке оценивают каждый перевод по 3501 параметру.

Банк «Абсолют» завершил проект по замене Micro Focus ArcSight на MaxPatrol SIEM от компании Positive Technologies. Банк использует систему для обеспечения видимости IT-инфраструктуры и мониторинга инцидентов ИБ. Произошедшие обновления связаны с изменением внутреннего ландшафта, вводом в эксплуатацию новых IT-решений, а также с корректировкой значимости инцидентов. SIEM мониторит в банке около 5 тыс. узлов, что охватывает 95% инфраструктуры кредитной организации.

На момент публикации пресс-релиза категоризированы все IT-активы и подключены все источники событий: антивирусы, песочницы, сетевые устройства, рабочие станции, серверы и т.д., что делает SIEM одним из важнейших инструментов центра операционного реагирования банка. Благодаря этому удается своевременно реагировать на возникающие угрозы и предотвращать реализацию рисков.

Банк «Ренессанс» внедрил систему управления уязвимостями MaxPatrol VM. В организации уже был налажен собственный процесс работы с уязвимостями. Одно из главных требований банка состояло в том, чтобы беспрепятственно интегрировать инструмент VM в существующий процесс и автоматизировать задачи приоритизации и контроля устранения уязвимостей. Помимо этого получены дополнительные возможности, например инструментарий для поиска и выделения трендовых уязвимостей — тех, которые злоумышленники эксплуатируют прямо сейчас.

Планы дальнейшего развития

Начатые проекты подтверждают расставленные на Уральском форуме технологические приоритеты. В каких направлениях идут проекты?

- Развивается концепция «security by design», когда ИБ становится неотъемлемой частью IT-систем. Банк «Тинькофф», НСПК, Московская биржа и другие крупные игроки уже продемонстрировали свои достижения.
- Не стоит на месте криптография. В России появился первый отечественный аппаратный модуль кибербезопасности (HSM) от «КриптоПро», позиционируемый в качестве замены продукции французской компании Thales. HSM предназначен для защиты банковских транзакций от перехвата. Сейчас идет тестирование модуля в платежной инфраструктуре страны.
- Квантовые и постквантовые технологии находят применение в финансах. Например, ГПБ оптимизирует с помощью данных алгоритмов такую «тяжелую» real-time-систему, как антифрод. А ВТБ внедрил ВКС DION от холдинга Т1. Известно, что DION стал первой отечественной ВКС-системой, способной на программном уровне противостоять кибератакам с применением квантовых компьютеров. ВТБ принял участие в тестировании полностью защищенного постквантовыми алгоритмами канала связи между пользователем и сервером.
- Ожидается появление и активное внедрение новых отечественных устройств сетевой защиты уровня ядра сети: NGFW, SASE, CASB и т.д.

Что касается лучших мировых практик в области ИБ, то в России о них знают и активно обсуждают прогнозы Gartner в области Cybersecurity Mesh архитектуры: экосистемы средств безопасности и элементов управления для обеспечения безопасности современной распределенной организации. По крайней мере, об этом шла речь на IT IS Conf в презентации компании Check Point Software Technologies Russia. А это значит, что следует ожидать появления проектов по разработке и внедрению облачных сервисов типа Firewall-as-a-Service, Hybrid Mesh Firewall Platform, Cloud Firewall вплоть до выстраивания полноценной Immutable Infrastructure. Б.О