Новое — это компромисс со старым

В мире ИБ рождается новая область знаний, фокусом которой станет понимание того, что безопасность — это качество бизнеса. Процесс оценки защищенности станет непрерывным, что позволит сразу же устранять возникшие проблемы

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



Immutable, Offensive и Resistance — это не просто новые термины из области ИБ, это целостные подходы со своими идеологиями и своим инструментарием для борьбы с киберпреступностью и обеспечения безопасности банков и других финансовых компаний.

На отечественном рынке данные подходы только начинают применяться и активно изучаются профильными специалистами. Не последнюю роль в этом играют открытые обсуждения со всеми признанными экспертами в сфере ИБ. Некоторые наиболее интересные мнения, безусловно, представляют огромный интерес для практикующих специалистов.

Mesh и Immutable Infrastructure

Подводя итоги первых шести месяцев 2023 года в области развития IT и ИБ в финансовой сфере, медиапроект «Банковское обозрение» обратил внимание на проникновение в нашу страну концепции архитектуры Gartner Cybersecurity Mesh: экосистемы средств безопасности и элементов управления для обеспечения ИБ современной распределенной организации. Эксперты с довольно большой долей осторожности говорили тогда, что подобный подход просто обречен на выстраивание полноценной Immutable Infrastructure. Не прошло и нескольких месяцев, как мир ИБ перешел от слов к делу.

Наверняка одним из драйверов принятия сообществом Mesh-архитектуры безопасности стали планы Банка России по легализации IT-аутсорсинга и облачных вычислений. Многие банки уже сегодня представляют собой сложные экосистемные проекты с элементами компонентов Cloud Native, а также многочисленными взаимосвязями как с внутренними элементами, так и с внешними поставщиками сервисов.

По мнению представителей компании Check Point Software Russia, Mesh предполагает комплексный и масштабируемый подход к расширению средств контроля безопасности даже для широко распределенных IT-активов. В его рамках инструменты безопасности взаимодействуют через несколько вспомогательных

уровней, таких как консолидированное управление политиками, аналитика безопасности и фабрика идентификации. Все вместе эти инструменты способны контролировать данные, хранящиеся в различных местах и форматах, а также отлично решают задачи, характерные для мира, где информация существует далеко не только в физических офисах и ЦОД.

Иммутабельность (Immutable) — отсутствие возможности у IT-объекта изменить его состояние в облаке, а значит, появляется возможность вынести состояние системы, размещенной в инфраструктуре, в отдельные хранилища. Например, если что-то необходимо обновить, исправить или изменить, создаются новые виртуальные серверы с соответствующими изменениями, которые заменяют старые.

Не углубляясь в детали, подчеркнем, что Immutable Infrastructure в рамках Mesh-архитектуры открывает широкие возможности для создания новых, более эффективных форм управления, которые обеспечивают больший контроль и безопасность обновления ПО и структуры его поддержки. Однако есть одно «но»: необходимо изменить образ мышления и производственную культуру команд DevSecOps.

Offensive security

Аналитики Gartner выяснили, что в 2021-2022 годах общемировым трендом стало повышение риск-аппетита топ-менеджеров компаний из самых разных сфер бизнеса, включая финансовый сектор. Для руководителей служб ИБ (CISO) это означает, что в складывающихся условиях нестабильности им может пригодиться наступательный подход к обеспечению ИБ, который получил название Offensive Security (OffSec).

Вадим Шелест, ведущий эксперт отдела анализа защищенности МТС RED, в ходе прямого эфира AM Live «Как оценить степень защищенности компании в 2023 году» дал такое определение: «OffSec — это оценка уровня ИБ-зрелости компании. Все методы, которые мы используем в Offensive Security, необходимы именно для оценки степени безопасности бизнеса. Начинается этот процесс с анализа защищенности, тестов на проникновении и т.д. Наша цель — собрать максимум уязвимостей во внешнем и внутреннем периметрах компании, чтобы оптимизировать ее защиту».

Понятно, что OffSec невозможен без реальной оценки преимуществ и недостатков тестирования на проникновение (пентестов), командной имитации атак (Red Teaming и Purple Teaming), программ выплат за уязвимости (Bug Bounty), а также без ответа на вопрос, как на практике сочетать эти методы между собой.

По словам **Дмитрия Шмойлова,** руководителя отдела безопасности программного обеспечения «Лаборатории Касперского», одним из главных выводов из дискуссии стало понимание того, что Offensive Security действительно способствует повышению уровня интеграции тех команд, которые занимаются защитой и нападением. В результате будет рождаться новая область знаний, фокусом которой станет понимание того, что безопасность — это качество бизнеса.

Возможно, это самое качество будет определяться достигнутым банком уровнем интеграции с искусственным интеллектом. Процесс оценки защищенности станет непрерывным, что позволит сразу же устранять возникшие проблемы.

Однако внедрение OffSec в финансовой сфере в настоящее время может стать непростой задачей; например, сложная IT-инфраструктура, а также наличие Legacy-систем являются преградой для проведения качественного тестирования на проникновение. Кроме того, отечественные реалии изобилуют проблемами юридического характера, которые объясняются довольно медленной процедурой декриминализации хакерских действий, связанных с пентестами.

Attack Resistance

Не самая простая судьба у довольно оригинального ИБ-подхода — «сопротивляемость атакам» (Attack Resistance). На сайте известного эксперта **Алексея Лукацкого** «Бизнес без опасности» можно узнать подробности громких претензий некоторых вендоров к Attack Surface Management (ASM), которые, однако, не меняют его суть.

Attack Resistance в терминах ИБ является базовым концептом в защите IT-инфраструктур и чувствительных данных от вредоносных или несанкционированных действий, который включает в себя использование различных мер и приемов для предотвращения и обнаружения атак, а также для минимизации их последствий.

Сопротивляемость атакам основывается на следующих основных принципах:

- защита в глубину (defense in depth) — использование нескольких слоев защиты для создания барьеров для злоумышленников. Каждый слой обеспечивает отдельную линию обороны, и в случае преодоления одного слоя следующий сможет предотвратить дальнейшую атаку;
- принцип наименьших привилегий (principle of least privilege) — каждый пользователь или процесс должен иметь только необходимые привилегии и роли. Это уменьшает риск несанкционированного доступа и возможность злоумышленников получить контроль над системой;
- аутентификация и авторизация — необходимо гарантировать подлинность пользователей и устройств, а также контролировать их права доступа к ресурсам системы;
- регулярное обновление и патчи;
- обучение и осведомленность пользователей.

Несмотря на все усилия, невозможно достичь абсолютной сопротивляемости атакам из-за так называемого разрыва, который появляется вследствие излишней веры в действенность средства класса ASM. Тем не менее использование базовых принципов и последовательная реализация мер безопасности значительно повышают уровень защиты системы и снижают риск успеха атаки. Поэтому иногда необходим компромисс со старым стеком.

«Интересно, что в России, даже несмотря на уход многих зарубежных вендоров, есть почти все нужные компоненты для обеспечения Attack Resistance. Дело за малым — выстроить целостную программу, которая объединяла бы все нужные компоненты. Правда, с этим как раз и возникают проблемы», — подвел итог Алексей Лукацкий. Б.О