РБК +

Иван Мелехин

«Бизнес заинтересован в автоматизации реагирования на киберугрозы»

Издание: plus.rbc.ru

Директор по развитию НИП «Информзащита» Иван Мелехин — о том, как комплексные облачные сервисы укрепят информационную безопасность российских компаний.

Фокус киберпреступников с организаций финансового сектора и вывода денежных средств смещается на хищения персональных данных, использование шифровальщиков с целью шантажа и нарушение функционирования критичных объектов. Традиционно наиболее подвержены атакам организации государственного сектора, финансовой отрасли, промышленность. В последнее время растет число кибератак в ретейле и здравоохранении.

Согласно отчетам Банка России, объем несанкционированных операций с использованием банковских счетов ежегодно снижается. Например, в 2018 году ущерб составил около $22 млн. При этом статистика по количеству общих атак говорит о ежегодном их росте примерно на 10–11%.
Часто исходными точками проникновения в инфраструктуру становятся подразделения, активно общающиеся с внешним миром и клиентами. Именно на них направлены, например, попытки атак с использованием социальной инженерии: рассылки фишинговых писем и вредоносного программного обеспечения.

Растущие риски, а также усиливающееся регуляторное давление — усиление требований в области информационной безопасности, особенно в части защиты критической инфраструктуры и требований к организациям финансового сектора — вынуждают бизнес инвестировать в кибербезопасность.

Рынок информационной безопасности (ИБ) по совокупной выручке его лидеров стабильно растет на протяжении последних нескольких лет. При этом в ряде

отраслей мы наблюдаем тенденцию к экономии бюджетов со стороны потребителей, в том числе за счет отказа от капитальных вложений и перехода на сервисную модель.

Растет интерес к переносу инфраструктуры ИБ в облака: повышается спрос на решения киберзащиты по модели SaaS и, соответственно, предложение подобных услуг. Мы видим большой интерес к средствам выявления и предотвращения кибератак, таргетированных атак, к средствам такого класса, которые позволяют осуществлять максимально точный мониторинг ИТ-инфраструктуры и обнаруживать вредоносные действия на ранней стадии, — например, EDR (endpoint detection and response) и NTA (network traffic analysis). Бизнес заинтересован в автоматизации реагирования на инциденты и ищет средства защиты для промышленной автоматики.

Сегодня все игроки пытаются занять долю рынка сервисных услуг: вендоры начинают активно развивать сервисы на базе своих продуктов, а интеграторы — продукты на базе своих сервисов. Растущая конкуренция будет способствовать улучшению качества обслуживания. Тем более что сегодня на рынок ИБ активно выходят новые крупные игроки, поддерживаемые Сбербанком, «Ростелекомом» и другими естественными монополиями. С одной стороны, небольшим игрокам будет сложно соревноваться с подобного рода инвестпроектами, поэтому можно ожидать слияний и поглощений, а с другой — сотрудничество дает преимущества, что будет способствовать альянсам.

Мы, в частности, в сотрудничестве с Microsoft предложили клиентам комплексные решения защиты на основе управления системой ИБ предприятия из облачной среды. Первым продуктом в рамках нашей совместной работы стал виртуальный центр оперативного реагирования на киберугрозы (Security Operation Center, SOC) на базе Microsoft Azure Sentinel.

Чем известна ГК «Информзащита»

Группа компаний «Информзащита» — российский системный интегратор в области информационной безопасности специализируется на оказании услуг в области консалтинга, аудита и анализа защищенности, проектировании, поставке и внедрению решений по обеспечению информационной безопасности

современных автоматизированных систем различного назначения и любого уровня сложности. Компания реализовала свыше 300 проектов для государственных, финансовых, страховых, промышленных организаций, а также транспортных и других компаний.
По итогам 2018 года «Информзащита» вошла в топ-1000 успешных российских поставщиков по версии торговой площадки B2B-Center. Исследование проводилось среди 406 тыс. компаний.

Используя технологическую платформу и набор инструментов Microsoft Azure, наши специалисты обнаруживают и предотвращают даже самые изощренные атаки на ранних стадиях: у Microsoft достаточно богатый набор облачных сервисов, в том числе системы для сбора и обработки событий информбезопасности (SIEM) и противодействия таргетированным атакам (APT).

Принципиальное отличие виртуального SOC от традиционного — простота подключения и масштабирования сервиса, в рамках облака Azure это происходит совершенно прозрачно.
При этом мы ориентированы на заказчиков, которые хотят получать сервис как для традиционной инфраструктуры на площадке или в облаке, так и для критической инфраструктуры, к которой предъявляются регуляторные требования. Наш центр мониторинга — IZ: SOC является единым окном, в котором клиенты получают комплексный сервис, покрывающий все требования как к функционалу инфраструктуры ИБ, так и к соответствию законодательству.

Кроме того, не стоит забывать, что практически 90% успеха отражения киберугроз зависит от квалификации аналитика. Несмотря на то, что автоматизация и роботизация рутинных операций со временем облегчат работу на первой линии SOC, рынок пока еще довольно далек от появления полноценных «беспилотных» средств защиты.
Квалифицированных специалистов сильно не хватает. Подготовка в вузах не всегда позволяет выпускникам сразу приступать к практической работе: зачастую у них недостаточно развиты навыки для работы в рамках DevOps — взаимодействия специалистов разработки и информационно-технологического обслуживания, умения писать скрипты автоматизации. Остро востребована сегодня способность работать с большими данными.

Мы в СМИ

РБК +

В нашей команде работают профессионалы отрасли, хорошо знакомые в том числе со спецификой регулирования и требования российского законодательства в сфере ИБ. Совместно с Microsoft мы запустили образовательную программу для специалистов российских компаний в области ИБ, она позволяет отработать самые сложные сценарии киберинцидентов. А также планируем серию совместных мероприятий, на которых готовы делиться опытом обнаружения и предотвращения кибератак.