Тема “Российские кибернетики – невзвзамываемая экосистема”

Группа: АДБ-20-03

Выполнил: Васильев Д.И.

Российский рынок информационной безопасности переживает очередной виток развития, импульс которому придало ослабление позиций западных вендоров. Всё чаще отечественные разработчики говорят о своём продуктовом портфеле не как о наборе разрозненных решений, но как об экосистеме, которая объединена некой идеей, миссией и концепцией. Более того, речь не всегда идёт о моновендорной конструкции: сервис-провайдеры собирают свои экосистемы из продуктов разных производителей.
Кибербезопасность как экосистема

На бытовом уровне мы уже привыкли к экосистемам продуктов и услуг. Когда есть одна точка доступа ко всем сервисам и они связаны друг с другом, это удобно. Если такими возможностями с удовольствием пользуются обычные люди, то почему бы не перенести их на решения для бизнеса? Рассмотрим на примере кибербезопасности.

Современный рынок ИБ предлагает многочисленные продукты от разных разработчиков. Большой выбор — это хорошо с точки зрения конкуренции и повышения общего уровня качества. Но на определённом этапе чрезмерное разнообразие создаёт трудности для заказчика. Например, продукты сложно интегрировать между собой, а управлять ими приходится из разных консолей, что отнимает ресурсы команд ИБ и мешает привести политики безопасности к единообразию. Как правило, компании не хотят разбираться, они просто хотят получить надёжное решение, которое защитит их от всего и прямо сейчас. Разберёмся, какие преимущества даёт компаниям экосистемный подход к кибербезопасности.

Управление временем

Поговорка «Время — деньги» крайне актуальна и в среде ИБ, особенно если речь идёт о противодействии сложным атакам. Среднее время обнаружения и реагирования (Mean Time to Detect и Mean Time to Respond) — ключевые показатели, по которым оценивается эффективность ИБ-команд. Затянувшийся киберинцидент может обойтись компании в круглую сумму. По данным «Лаборатории Касперского», в 2021 году только в 22% случаев компании реагировали на атаку в течение нескольких часов. Чаще компаниям требовались дни или даже месяцы.

Возможность централизованно управлять всей системой синхронизированных друг с другом ИБ-инструментов позволяет своевременно обнаруживать атаки и минимизировать их последствия. Важное значение имеет наличие у ИБ-сотрудников самой актуальной информации об угрозах. За это в экосистеме отвечают продукты класса Threat Intelligence. Они открывают специалистам доступ к массиву информации об актуальных угрозах со всего мира. Агрегированный опыт и знания помогают ИБ-специалистам сокращать время на обнаружение, расследование и реагирование на атаку, а значит, спасать компанию от потенциальных потерь.

С каждым годом количество и разнообразие киберугроз только растёт. Например, эксперты «Лаборатории Касперского» в 2021 году обнаруживали ежедневно более 380 тысяч новых вредоносных файлов в день. Этот показатель растёт с каждым годом. Ещё одно статистическое подтверждение: в 2021 году количество атак на корпоративные сети выросло на 50%, а в 44% всех инцидентов в 2021-м атакующая сторона использовала неизвестные ранее инструменты.

Кибербезопасность под ключ

Логика развития рынка ИБ сегодня так или иначе ведёт его к экосистемности. В России появляются продукты класса XDR (Extended Detection and Response) — расширенные системы обнаружения и реагирования на киберугрозы. Они воплощают экосистемный подход. Это моновендорная кросс-продуктовая концепция, построенная на взаимодействии комплекса защитных решений. XDR основан на расширении технологий EDR (Endpoint Detection and Response), а те, в свою очередь, базируются на классических технологиях защиты конечных точек — EPP (Endpoint Protection Platform). Этот надёжный фундамент дополняется продуктами, которые могут расширять функционал системы. О том, для каких компаний особенно актуален XDR, рассказываем здесь.

Солидный XDR сегодня — это не только EDR, но и защита почтового и веб-трафика, глубокий анализ сетевого трафика, мониторинг и корреляция событий ИБ, сильный Threat Intelligence. В состав XDR также может входить модуль для повышения цифровой грамотности сотрудников. Таким образом, зрелые и развитые отделы информационной безопасности получают всё необходимое, чтобы перекрывать возможные точки проникновения

злоумышленников в инфраструктуру компании, эффективно проводить расследования и своевременно реагировать на обнаруженные инциденты.

XDR обычно позиционируется как кибербезопасность «под ключ», поэтому в лучшем исполнении решение в том числе помогает организациям соответствовать требованиям регуляторов, чтобы даже на это не уходило драгоценное время ИБ-специалистов.

Концепция XDR появилась в процессе эволюции как продуктов информационной безопасности, так и потребностей рынка. Сегодня заказчикам необходима не просто унификация ИБ-инструментов от одного производителя, но и получение от этой унификации каких-то дополнительных преимуществ — например, в виде кросс-продуктовых сценариев, автоматизации процессов, экономии ресурсов и снижения издержек.

Спасение от выгорания

При выборе подхода к построению ИБ-системы важно учитывать собственные ресурсы компании. Хорошие специалисты всегда в дефиците. Несмотря на большой интерес к профессии, спрос на IT-шников в целом и на безопасников в частности растёт ещё стремительнее, чем предложение. По прогнозам Минтруда, до 2024 года в российских компаниях ежегодно не будет хватать около 18,5 тысяч специалистов по информационной безопасности.

Отсюда две проблемы: во-первых, качество текущей работы. Когда все сотрудники перегружены, возрастает риск ошибок и выгорания. Даже высокая квалификация не всегда может спасти от сбоев в режиме постоянного перегруза рутинными задачами по сбору, хранению и анализу данных, проведению различных действий на этапах расследования и реагирования. Во-вторых, при такой нагрузке у ИБ-отдела не остаётся времени и сил на стратегическую работу, аналитику угроз, расследования инцидентов, общее развитие и совершенствование системы безопасности. Долгосрочно это тоже чревато проблемами: система может оказаться неприспособленной к новым угрозам, и риск пропустить атаку со временем возрастает.

Например, при расследовании инцидента специалистам необходимо определить начальный вектор атаки, все вредоносные программы, техники и тактики, использованные злоумышленниками, нанесённый ущерб. Без

применения средств автоматизации этот процесс может оказаться крайне трудозатратным. Эти операции можно и нужно автоматизировать, но важно сделать это грамотно. Если использовать ряд отдельных инструментов, это увеличивает количество ручных операций и ожидаемо приводит к неэффективному использованию, перегрузке ИБ-служб и дополнительным затратам.

Современные ИБ-экосистемы предлагают готовые наборы синхронизированных продуктов, необходимых для всего цикла обработки инцидентов и позволяющих максимально автоматизировать трудоёмкие задачи. Такая продуманная автоматизация позволяет не только сэкономить дорогостоящее рабочее время аналитиков, но и снизить их загрузку, чтобы они могли сосредоточиться на противодействии действительно сложным инцидентам и совершенствовании системы безопасности.

Стабильность вендора

В этом году на сложный ландшафт угроз наложилась нестабильность самого рынка ИБ. Россию покидают западные вендоры, в результате отзыва лицензий/ подписки на их решения у бизнеса перестают работать обновления баз, в отдельных продуктах ИБ быстро теряется качество детектирования (ухудшается с каждым днём), решения начинают пропускать вредоносные объекты, разрешают подключения на нелегитимные и опасные URL-адреса, пропускают рекламный и вредоносный спам, не распознают крупные атаки.

Перед бизнесом стоят вопросы срочного и при этом безболезненного перехода на новые продукты, которые гарантированно будут работать на российском рынке, вне зависимости от любых внешних обстоятельств. Решение класса XDR с синхронизированными продуктами из единой экосистемы от отечественного поставщика — это возможность решить сразу две актуальные в 2022 году задачи: оперативно провести комплексное ИБ-замещение и повысить её эффективность перед лицом новых угроз.

При этом одна из особенностей XDR заключается в том, что несмотря на общую моновендорную концепцию в систему можно интегрировать решения от других производителей. Такой тип XDR называется гибридным. Компания может, не теряя все предыдущие инвестиции в ИБ, перестроиться

на XDR без потери накопленного опыта и имеющихся решений и спокойно развиваться под защитой нового основного поставщика.

Чёткая ответственность за результат

Экономить время компаний и их ИБ-команд поможет «режим одного окна». Если компания пользуется защитными решениями нескольких поставщиков, то, когда возникает проблема, она оказывается в ситуации корпоративного пинг-понга. Драгоценное время уходит на то, чтобы разобраться, на стороне какого вендора находится первопричина. В процессе они перекидывают друг другу заказчика, что не способствует решению проблемы. Если же компания выбирает продукты одного поставщика для всех требующих защиты элементов инфраструктуры, любой вопрос решается проще и быстрее.

Конечно, экосистемность и моновендорность — это не панацея от всех киберугроз. Споры о том, что лучше — один поставщик или несколько, ведутся уже давно. На каждый аргумент одной стороны уже существует многоуровневая аргументация — с другой. Но все они, по сути, упираются в качество исполнения. Когда каждый отдельный продукт на протяжении многих лет подтверждает своё высокое качество, безукоризненно исполняет свою роль на своём этапе защиты и бесшовно интегрируется с другими решениями, то и вся система становится гибкой и удобной в управлении, работает, как слаженный оркестр.

Российские инженеры намерены разработать вычислительную среду, "абсолютно защищенную" от взлома и потери информации. В нее будут включены линейка компьютеров, сетевое оборудование и программное обеспечение, пишут "Известия". Чтобы достичь этой цели, среда должна быть основана исключительно на отечественных программно-аппаратных разработках. Математики и инженеры бывших оборонных предприятий и институтов Москвы и Санкт-Петербурга займутся создание доверенной вычислительной среды. Разработку поддержит Национальная технологическая инициатива (НТИ), пишут "Известия" со ссылкой на руководителя рабочей группы направления SafeNet НТИ Валентина Макарова. По его мнению, независимая от зарубежных производителей аппаратно-программная платформа обеспечит надежность компьютерных систем, связанных с национальной безопасностью. НТИ поручила разработку среды математикам и инженерам бывших оборонных предприятий и

институтов Москвы и Санкт-Петербурга. Она будет работать исключительно с отечественным ПО и компонентами. Базовым процессором станет отечественный "Эльбрус". Его разработчики адаптируют к защищенным вычислениям основные системные библиотеки и прикладные программы. "Архитектура микропроцессоров "Эльбрус" — это полностью российская разработка, которая при создании намного опередила свое время, — рассказал генеральный директор АО "МЦСТ" Александр Ким "Известиям". — Мы и сейчас по некоторым направлениям идем ощутимо впереди зарубежных коллег". В частности, за один вычислительный такт "Эльбрус" способен выполнять до 25 операций, тогда как у зарубежных процессоров этот показатель не превышает 10. Значительно опережает "Эльбрус" остальные процессоры и по такому важному параметру, как аппаратный контроль за использованием машинной памяти. Если большинство современных процессоров управляет памятью блоками по 4 килобайта, то "Эльбрус" может контролировать обращения к запоминающему устройству на уровне отдельных 32-разрядных слов, то есть примерно в тысячу раз точнее. Эта так называемая технология защищенных или безопасных вычислений позволяет во много раз сократить количество ошибок, возникающих при разработке операционной системы и прикладных программ. Сейчас перед разработчиками "Эльбрусов" стоит задача адаптировать к защищенным вычислениям основные системные библиотеки и прикладные программы.

Практика выбора и использования экосистем Как выбрать экосистему Переходя к практической части онлайн-конференции, Рустэм Хайретдинов поинтересовался у спикеров: стоит ли сразу выбирать экосистему или же она должна сложиться постепенно, из совокупности отдельных продуктов? Каков типовой сценарий покупки экосистемы на отечественном рынке? Гости студии высказали мнение, что в основе экосистемы обычно лежат один или несколько продуктов, наиболее полно удовлетворяющие определённые запросы заказчика.

В дальнейшем на этом фундаменте компания может начать строить моновендорную экосистему, если другие решения того же производителя будут её устраивать, а также получать синергетический эффект, когда каждый новый элемент придаёт дополнительную ценность уже имеющимся. Можно

сказать, что развитие экосистемы внутри компании-заказчика происходит точно так же, как и внутри вендора, который строит её выпуская новые продукты. Заслужив доверие клиента одним ключевым продуктом, можно постепенно втягивать его в свою экосистему, предлагая новые возможности. Если последующие элементы экосистемы не разочаруют заказчика, то он будет всё менее и менее критично относиться к выбору каждого нового решения вендора, зная, что цены, функциональные возможности и качество сервиса этого поставщика его в целом устраивают. Заказчику важно понять преимущества, которые даёт экосистема, а также осознать, что он не переплачивает за эти преимущества. Если вендор предлагает экосистему, которая закрывает основные потребности, но дополнительные выгоды от неё кажутся незначительными, а цена превышает ожидания, то заказчик может сделать выбор в пользу отдельных продуктов. Как отметили спикеры AM Live, экосистемный подход позволяет взять те технологии, которые предлагает вендор, и начать их внедрять в том объёме, который соответствует уровню зрелости заказчика, его текущим запросам. В дальнейшем возможно поэтапное наращивание тех функций, которые нужны клиенту.

Результаты опроса, проведённого нами среди зрителей онлайн-конференции, показали, что большинство заказчиков (45 %) готовы покупать все или почти все системы информационной безопасности у одного поставщика, если те будут устраивать их по качеству. При этом 31 % опрошенных в сумме не одобряет такого подхода: 17 % считают, что это нарушает принцип эшелонированной обороны, а ещё 14 % указали на дополнительные риски от такой политики. Интересно, что стоимость экосистемы вообще не рассматривается участниками опроса как один из значимых факторов. Ни один из них не выразил готовность покупать всю информационную безопасность у одного вендора, если это окажется значительно дешевле. Затруднились с ответом 24 % респондентов.

Критерии выбора экосистемы В продолжение разговора эксперты сформулировали критерии выбора экосистемы: Полнота и способность охватывать сценарии заказчика. Уровень доверия к провайдеру экосистемы. Возможность оказания сервиса «поверх» экосистемы и наличие сильных партнёров. Зрелость корневой технологии — ядра системы. Кто является покупателями экосистем Каков портрет «типового» клиента ИБ-экосистемы? С одной стороны, логично предположить, что это крупные компании, осознавшие потребность в системном подходе и все преимущества экосистем. Но есть ли интерес к экосистемам со стороны среднего бизнеса, у

которого не хватает собственных ресурсов на интеграцию отдельных решений? Как отметили гости студии, предметно интересуются готовыми экосистемами те компании, которые имеют достаточный уровень зрелости, чтобы понимать их преимущества, с парком от 1 до 10 тысяч компьютеров. Крупные компании обычно не рассматривают возможность покупки экосистемы сразу, выращивая их постепенно. При этом крупный бизнес меньше ориентирован на сервисную модель и чаще всего строит экосистему на своей инфраструктуре. Средний и малый бизнес, напротив, чаще получает готовые и собранные в экосистему решения от MSSP. Выгоды от использования экосистемы.

Насколько выгодно пользоваться экосистемой, какие экономические стимулы есть у заказчика к тому, чтобы покупать именно её, а не набор разрозненных продуктов? Не секрет, что многие производители снижают стоимость некоторых элементов экосистемы или даже готовы предложить их бесплатно, при покупке своих корневых продуктов. Эксперты в студии подтвердили, что пользоваться экосистемой одного вендора для клиента выгоднее, поскольку разработчик может предложить таким заказчикам более выгодные условия по обслуживанию или приобретению новых продуктов. При этом надо понимать, что бесплатных ИБ-систем не бывает. Если вендор предлагает одно из своих решений со значительным дисконтом или вовсе по нулевой стоимости, то, скорее всего, недополученная прибыль включена в цену обслуживания или другого продукта. Но даже несмотря на это стоимость экосистемы в целом должна получаться ниже, чем сумма цен входящих в неё продуктов. Впрочем, важно рассматривать вопрос в комплексе, просчитывая стоимость владения с горизонтом в несколько лет. Что важно учитывать при выборе экосистемы Какие факторы важны для заказчика при выборе экосистемы кибербезопасности? Как показал наш опрос, проведённый во время эфира, ключевым показателем является широта линейки продуктов и услуг. За этот вариант проголосовали 54 % респондентов. Также важными факторами являются репутация поставщика (25 %) и планы развития экосистемы (8 %). Размер скидки и бонусов, как и в предыдущем опросе, зрители прямого эфира не посчитали важным мотивом для покупки. При этом 13 % участников опроса считают, что говорить о влияющих на выбор факторах бессмысленно, ведь в будущем нас ждёт лишь одна, государственная экосистема.

Список используемой литературы:

https://vc.ru/kaspersky/424377-kiberbezopasnost-kak-ekosistema - дата обращения 08.10.2023.

https://www.anti-malware.ru/analytics/Technology_Analysis/Cyber-Security-Ecosystems - дата обращения 08.10.2023.

https://investfuture.ru/news/id/rossiyskie-kibernetiki-sozdayut-nevzlamyvaemye-kompyutery - дата обращения 08.10.2023.