Концерн «РТИ» недавно интегрировал платформу для защиты от таргетированных атак Kaspersky Anti Targeted Attack Platform (KATA) в свою корпоративную сеть. Поставку и внедрение решения осуществил партнер «Лаборатории Касперского» – компания «Инфосекьюрити». Новое решение противостоит целевым атакам на всех этапах нападения на инфраструктуру компании

От рассвета до заката охраняет сети KATA

О том, как проходило внедрение, пилотное тестирование и запуск системы в промышленную эксплуатацию, насколько эффективным оказался ИТ-проект, что получили в итоге заказчики, «БИТу» рассказывают:

Владимир Иванов,
начальник Управления информационных технологий «РТИ»

Дмитрий Григорович,
руководитель по информационной безопасности Управления безопасности и режима «РТИ»

Александр Дворянский,
коммерческий директор «Инфосекьюрити»

– Какая проблема была у концерна «РТИ» до интеграции платформы для защиты от таргетированных атак Kaspersky Anti Targeted Attack Platform (KATA) в свою корпоративную сеть? Как она отражалась на деятельности компании? Почему компания решила внедрить решение для защиты от целевых атак?

Дмитрий Григорович: Предпосылкой для выбора решения «Лаборатории Касперского» послужила не текущая проблематика, а необходимость иметь надежную превентивную систему защиты от потенциальных сложных, многоуровневых угроз, способных нанести существенный вред бизнесу

– Какие способы решения данной проблемы рассматривались компанией?

Д.Г.: На этапе выбора решения мы изучили и детально проанализировали возможности нескольких аналогичных продуктов, включая западные решения, так как хотели получить

комплексную систему дополнительно к уже имеющимся решениям безопасности. Система не должна была требовать удаления антивирусных продуктов.

Она должна была привнести большую долю детектирующих технологий сетевого уровня, а также «песочницу» к уже существующим у нас технологиям детектирования вредоносной активности (эвристический анализ, сигнатуры, IDS/IPS и так далее).

– Почему был выбран продукт «Лаборатории Касперского»? Для чего концерн приобрел также подписку на сервис Kaspersky Managed Protection?

Владимир Иванов: Решение «Лаборатории Касперского» – это качественный продукт, который имеет соответствующий сертификат ФСБ РФ и входит в Реестр отечественного ПО, что было немаловажно для концерна «РТИ».

Kaspersky Managed Protection – это экспертный сервис, который включает в себя мониторинг работы установленных в сетях заказчика продуктов Kaspersky Security для бизнеса и/или Kaspersky Anti Targeted Attack Platform (KATA), сбор и анализ полученной информации на предмет наличия следов целенаправленных атак, а также своевременное информирование клиента о возникшей угрозе.

Получаемые метаданные анализируются в автоматическом режиме, а круглосуточная служба мониторинга оперативно выявляет инциденты и собирает информацию, которая может использоваться в ходе расследования инцидентов.

К тому же сервис Kaspersky Managed Protection позволяет нам в особо трудных ситуациях получить поддержку экспертов самого высокого уровня.

– Каковы технические особенности и характеристики KATA?

Д.Г.: В основе Kaspersky Anti Targeted Attack Platform лежит целая платформа, включающая в себя множество сенсоров, собирающих различную информацию о процессах, происходящих в инфраструктуре защищаемой сети.

Анализ собранной информации, корреляция различных событий и выявление аномальных ситуаций необходимы для детектирования целевой атаки.

В состав платформы входят следующие компоненты:

- Сетевые сенсоры – модули по перехвату сетевого трафика, анализирующие обращения к веб-сайтам, почтовым и прокси-серверам. Включают в себя возможность извлечения почтовых вложений, загружаемых и передаваемых файлов для передачи их на анализ в модуль «Песочница».
- Сенсоры рабочих мест – небольшие программы, устанавливающиеся на конечные точки – рабочие станции и серверы. Выполняют перехват сетевого трафика на уровне отдельных станций, также направляя данные для анализа в другие модули.
- «Песочница» – отдельный модуль для анализа неизвестного программного обеспечения – почтовых вложений, загружаемых и передаваемых файлов. Поддерживается интеграция с облачной сетью Kaspersky Security Network для определения репутации файлов или с автономным частным облачным решением Kaspersky Private Security Network, изолированным от внешнего мира.
- «Центр анализа» – основное ядро системы, в котором проводится корреляция и анализ собранной информации, оцениваются и классифицируются угрозы по степени критичности. Кроме того, «Центр управления» обеспечивает управление всей системой защиты и предоставляет доступ администраторов к интерфейсу настройки и отчетов.

Kaspersky Managed Protection – это экспертный сервис, который включает в себя мониторинг работы установленных в сетях заказчика продуктов, сбор и анализ полученной информации на предмет наличия следов целенаправленных атак, а также своевременное информирование клиента о возникшей угрозе

– Что требовалось от ИТ-проекта? Каким должен был быть его результат? Кто исполнял требования заказчика?

В.И.: Со стороны ИТ потребовались корректировки сетевой составляющей текущей инфраструктуры для более эффективного использования возможностей решения KATA.

Реализовать требования к инфраструктурной составляющей решения в рамках настоящего проекта нам помогал наш партнер компания «Инфосекьюрити».

– Какие сроки были отведены на выполнение ИТ-проекта? Его стоимость?

В.И.: Изначально на весь проект отводилось три месяца, однако, несмотря на предновогодний период, совместными усилиями участников проекта удалось полностью завершить его за 2,5 месяца, включая внедрение, пилотное тестирование и запуск системы в промышленную эксплуатацию с по-

Kaspersky Anti Targeted Attack Platform (KATA)

Решение для защиты от целенаправленных атак. Главная опасность этих атак в том, что они тщательно прорабатываются под каждую конкретную организацию и при этом никак себя не обнаруживают. Итогом может стать утечка конфиденциальных данных, простой предприятия или удар по репутации. KATA противостоит нападениям на всех этапах и способно как обнаружить уже начавшуюся атаку и минимизировать ущерб от нее, так и защитить предприятие от потенциальных угроз, оценив риски для безопасности в текущей инфраструктуре.

ставкой необходимого оборудования и лицензий. Все участники проекта смогли уложиться в сжатые сроки, за что коллегам отдельное спасибо. Что касается стоимости ИТ-проекта, то, скажем так, он не был дешевым.

на высоком профессиональном и техническом уровне.

Это позволило нам получить действительно работающую систему, при этом не потратив месяцы на работы по ее адаптации

и масштабированию решения в нашей инфраструктуре. Со стороны «Инфосекьюрити» в ходе проекта было предложено и в итоге реализовано нами несколько дельных предложений по оптимизации работоспособности системы.

В основе Kaspersky Anti Targeted Attack Platform лежит целая платформа, включающая в себя множество сенсоров, собирающих различную информацию о процессах, происходящих в инфраструктуре защищаемой сети

– Как формировалась команда проекта? Кто вошел в нее со стороны заказчика и исполнителя? Кем проект управлялся?

В.И.: Изначально, еще на этапе опытной эксплуатации, была сформирована команда проекта, включающая инженеров и аналитиков. Безусловно, существенную поддержку оказали также эксперты «Лаборатории Касперского».

Вообще общий ход выполнения проекта – с момента старта «пилота» и до запуска системы в промышленную эксплуатацию – проходил

– Вносились ли какие-нибудь изменения в проект в ходе работ? Как они повлияли на результат?

Д.Г.: Одним из преимуществ решения является возможность изменять систему «на лету», что позволяет нам своевременно вносить корректировки в случае изменения вектора атаки.

– Как взаимодействовали во время работы над проектом заказчик и исполнитель?

Д.Г.: В целом исполнитель реализовал все наши изначально установленные требования к внедрению

– Что в итоге? Была ли достигнута цель проекта? Как внедрение KATA и сервис Kaspersky Managed Protection повлияли на бизнес концерна «РТИ»? Насколько этот проект оказался эффективным?

В.И.: В результате внедрения концерн «РТИ» получил гибкую систему противодействия целевым атакам, которая легко адаптируется под любые запросы компании.

KATA дает возможность оперативно осуществлять комплекс мероприятий по обнаружению, реагированию и прогнозированию потенциальных атак, правильно их приоритизировать и принимать меры по противодействию в соответствии с уровнем опасности.

Для нас важно быть уверенным в комплексной защищенности нашей корпоративной инфраструктуры.

Александр Дворянский: Если кратко подвести итоги запуска решения в промышленную эксплуатацию, то вывод такой: работа над проектом подобного уровня была крайне интересной и ответственной. И сейчас можно с уверенностью сказать, что мы получили достойные результаты и очень полезный опыт. БИТ

О концерне «РТИ»

Концерн «РТИ» – крупный российский отраслевой холдинг, разработчик-производитель высокотехнологичных продуктов и инфраструктурных решений с использованием собственных микроэлектронных технологий. Предприятия концерна имеют собственную R&D-инфраструктуру и реализуют уникальные по сложности и масштабу проекты в сфере радио- и космических технологий, систем безопасности, микроэлектроники и системной интеграции. Продуктовый портфель концерна представлен готовыми решениями в области национальной обороны, комплексных систем связи и безопасности, ИТ-инфраструктуры, автоматизации и оптимизации бизнес-процессов, промышленной микроэлектроники, смарт-карт и электронных носителей для паспортно-визовых документов, а также крупными оборонными проектами государственной значимости.

Об «Инфосекьюрити»

Компания «Инфосекьюрити» оказывает услуги и выполняет комплексные проекты в области информационной безопасности и системной интеграции. В штате компании более 160 высококвалифицированных специалистов, компетенции которых подтверждены международными сертификатами в области ИБ и ИТ. Среди клиентов компании финансовые, государственные и промышленные организации. Партнерами компании являются крупнейшие мировые производители телекоммуникационного оборудования, системного и прикладного программного обеспечения, а также различных систем защиты информационной безопасности. Компания является официальным аккредитованным экспертом Роскомнадзора и соучредителем ABISS. Деятельность «Инфосекьюрити» лицензирована ФСТЭК и ФСБ. Подробнее о компании можно узнать на http://gk-is.ru.

О «Лаборатории Касперского»

«Лаборатория Касперского» – международная компания, работающая в сфере информационной безопасности с 1997 года. Глубокие экспертные знания и опыт компании лежат в основе защитных решений и сервисов, обеспечивающих безопасность бизнеса, критически важной инфраструктуры, государственных органов и пользователей во всем мире. Обширное портфолио «Лаборатории Касперского» включает в себя передовые продукты для защиты конечных устройств, а также ряд специализированных решений и сервисов для борьбы со сложными и постоянно эволюционирующими киберугрозами. Технологии «Лаборатории Касперского» защищают более 400 миллионов пользователей и 270 тысяч корпоративных клиентов, помогая сохранить то, что для них важно.

Подробнее на www.kaspersky.ru.