Эра решений защиты бизнеса

В середине сентября 2015 г. ГК InfoWatch объявила о создании продукта InfoWatch Attack Killer – первого российского решения, способного обеспечить компаниям многоуровневую активную защиту web-инфраструктуры от различных видов кибератак. В дополнение, при развертывании InfoWatch Attack Killer, ГК InfoWatch планирует ввести страховую ответственность перед клиентами в случае непредотвращения атаки.

Введение

InfoWatch выделяет 3 этапа в эволюции роли ИБ и ИТ в бизнесе (рис. 1):

- *эра защиты компьютеров (1999–2007 гг.);*
- *эра защиты данных (DLP и шифрование, 2007–2012 гг.);*
- *эра защиты бизнеса (2012–2015 гг.). ИТ полностью интегрированы в бизнес-среду (2012–2015 гг.): электронные платежи и банкинг; электронное принятие решений; виртуальные совещания и рабочие группы; удаленная работа (в любом месте, в любое время, с любого устройства); мобильные устройства – основное средство взаимодействия.*

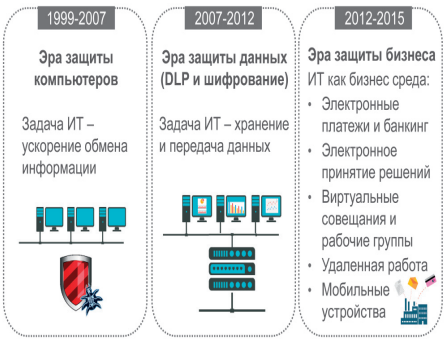

Рис. 1. Эволюция роли ИБ и ИТ в бизнесе.

В настоящее время фактически уже можно приравнять эффективность средств ИБ к эффективности бизнеса.

По данным Аналитического центра InfoWatch, в 2014 г. по сравнению с 2013 г. количество таргетированных атак увеличилось на 48%. При этом 66% инцидентов безопасности остаются незамеченными месяцами. Рост числа DDoS-атак в мире составляет 18–20%, в России эта цифра приближается к 25% в год.

Эксплуатация уязвимостей приложений и DDoS-атаки позволяют хакерам не только получить контроль над ресурсом, но и проникнуть во внутреннюю инфраструктуру компании. Хакеры используют ***комплексный подход к реализации атаки, поэтому базовые средства безопасности не способны обеспечить эффективную защиту****.*

В качестве ключевых особенностей современных таргетированных атак можно отметить следующие:

- *спланированность, наличие четкой цели, "заточенность" под конкретную инфраструктуру/организацию;*
- *многоэтапность – на каждом из этапов применяется свой тип воздействия (обхода защиты): DDoS, использование уязвимостей веб-инфраструктуры или ошибок в коде приложения, заражение компании-жертвы специализированным вредоносным ПО и др.;*
- *сложность выявления – многие атаки уже невозможно обнаружить по отдельным признакам (сигнатурам, портам, IP-адресам и др.): требуется более комплексный подход – анализ поведения, анализ с учетом факторов времени, геолокации, статуса пользователя и др.;*
- *длительность воздействия – атакующая сторона постоянно адаптирует методы атаки. Неудачная попытка не может остановить злоумышленников – они придумают более изощренный метод и повторяют атаку. Это предполагает отслеживание рисков возможных угроз в течение дней, недель, месяцев.*

Классификацию основных видов таргетированных атак можно представить следующим образом:

- *DDoS-атаки (distributed denial of services): атака на вычислительную систему с целью довести ее до отказа;*
- *атаки с использованием уязвимостей web-приложений или программного кода бизнес-приложений;*
- *таргетированные атаки с использованием специальных программ (ТАСП): подготовленные многоступенчатые ТА с использованием специально разработанного программного обеспечения;*
- *комплексные атаки: сочетание различных типов атак.*

Таргетированные атаки, в отличие от "традиционных" – вирусных, имеют свою специфику. Против них традиционная защита, как правило, бессильна и они требуют специализированных решений и привлечения дополнительной аналитики (табл. 2). И именно от них компании несут основные потери: прямые денежные потери, воровство сверхсекретной информации, потеря репутации и др.

Пример сценария многовекторной таргетированной атаки представлен на рис. 2. Сами примеры атак в эру защиты бизнеса представлены в табл. 1. Среди них: 1) заражение критически важных систем, связанных с электронными платежами и банкингом; 2) таргетированная рассылка писем; 3) кража секретных документов за счет изменения прошивки жестких дисков, интеграции вирусов в USB-носители; 4) кража денежных средств за счет заражения мобильных устройств с "привязанными" к ним банковскими картами и др.

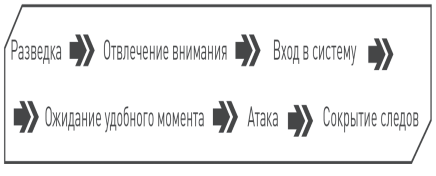

Рис. 2. Пример сценария многовекторной таргетированной атаки.

Табл. 1. Примеры современных таргетированных атак.

Тенденция	Атака	Описание	Цель	Потери
Электронные платежи и банкинг	Carbanak	•Заражение критически важных систем •Вывод средств через банкоматы, переводом через SWIFT на счет преступников, создание фальшивых счетов для обналичивания средств	Атаковано более 100 финансовых организаций преимущественно в Восточной Европе	Суммарный ущерб составляет около **1 млрд долл.** (потери 1 банка - от 2,5 до 10 млн долл.)
Электронное принятие решений	Desert Falcons	•Таргетированная рассылка писем •Использование социальной инженерии в сети Facebook	Более 3000 жертв: политические активисты и лидеры, военные и гос. ведомства, СМИ и финучреждения в Палестине, Египте,	Украли более **1 млн файлов и документов**
Виртуальные совещания и рабочие группы	Equation APT	•Изменение прошивки жестких дисков •Использование USB-червя Fanny •Присутствие вредоносных инсталляторов на CD-дисках •Использование веб-	Более 500 жертв: правительственные и дипломатические учреждения, телекоммуникации, аэрокосмическая отрасль, энергетика	Украли более **500 тыс. засекреченных файлов и документов**
Удаленная работа	Shaltay Boltay	•Взлом электронных почтовых ящиков •Взлом аккаунтов в соц. Сетях	Политические активисты и лидеры, военные и гос. ведомства	Украденные данные были проданы на «бирже» на сумму **более 1 млн долл.**
Мобильные устройства	Атака на Сбербанк	•Заражение моб. устройств вирусом, который переводит деньги с привязанных к телефонам банковских карт •Блокировка отправки SMS-уведомлений о списаниях	Пользователи приложения «Сбербанк Онлайн» на устройствах под управлением Android без антивируса	Похищено более **2 млрд руб.**

Сложившаяся экономическая ситуация усугубила ситуацию еще в бОльшей степени:

- *увеличилось число таргетированных атак;*
- *снизилась стоимость таргетированных атак;*
- *повысилась сложность проведения таргетированных атак.*

По данным Аналитического центра InfoWatch, изменение ситуации, связанной с таргетированными атаками по 2012 г. и 2014 г., представлено в табл. 3. В соответствии с ней, процент ожиданий вырос в 2,5 раза, а процент компаний, подвергшихся атакам, вырос в 7 раз.

Табл. 2. Отличительные особенности таргетированных и "традиционных" – вирусных атак.

Особенности	Вирус	Таргетированная атака
Число атакуемых объектов	Как можно больше	Один или некоторое число одинаковых
Учет особенностей конкретного объекта	Отсутствует	Обход системы безопасности
Наличие заказа	Нет	Есть
Сложность выявления	Средняя	Высокая
Ущерб	Непредсказуемый, небольшой	Заранее просчитанный, значительный
Возможность предотвращения	Достаточно антивируса	Нужны специальные средства и работа аналитиков

Табл. 3. Сравнение процентов ожидания и реализованных таргетированных атак в 2012 г. и в 2014 г.

2012 г.	2014 г.
37% компаний считают, что могут подвергнуться таргетированным атакам	**92%** компаний считают, что могут подвергнуться или подвергаются таргетированным атакам
3% компаний подвергались таргетированным атакам	**22%** компаний подвергались таргетированным атакам

Соответственно, в контексте вышесказанного, и средства ИБ стали приобретать новые особенности, прежде всего, это:

- *увеличение сложности настройки интеграции средств противодействия таргетированным атакам. Часто из-за низкой динамической адаптивности этих средств они стали недостаточными для противодействия. Для повышения реактивности противодействия необходимо запоминать историю атаки, формировать шаблон ее поведения, на основании которого можно было бы быстро выявлять подобные ей, как следствие – необходимость хранить и быстро анализировать очень большие объемы данных;*
- *необходимость группового использования корпоративных правил/политик безопасности одновременно ко всем средствам ИБ с учетом статуса пользователя;*
- *резко возросшая востребованность законченных решений ИБ – от клиентского устройства до инфраструктуры и приложений датацентра в условиях распределенной ИТ-инфраструктуры и фактически отсутствующего (размытого) защищенного периметра;*
- *особое значение стали приобретать **интегрированные автоматизированные решения ИБ**, позволяющие автоматизировать как процедуры поднастройки отдельных компонент системы защиты в случае изменения web-приложений, так и процедуры противодействия атакам (с минимальными временными задержками) и возникающим рискам ИБ;*
- *возрастает роль технологий аналитики больших данных, а также технологий, делающих утечки "безопасными" (вследствие зашифрованности информации) для минимизации рисков ИБ от внешних и внутренних угроз.*

InfoWatch Attack Killer – комплексная защита web-инфраструктуры

Текущая ситуация и цели разработки

В настоящее время для грамотного использования большинства корпоративных решений ИБ требуются профессиональные сотрудники, способные быстро анализировать многочисленные предупреждения о возникающих рисках, приоритезировать их и принимать адекватные действия. Как правило, для полноценной защиты требуется набор ИБ-решений, "закрывающих" разные уровни ИТ-инфраструктуры. При этом интеграция различных решений ИБ остается невысокой, и необходимы постоянные дополнительные усилия по их настройке в соответствии с меняющимися правилами и политиками безопасности. В результате – рост Capex и Opex и все меньшая доступность современных средств противодействия угрозам компаниям всех уровней (и это в условиях, когда эффективность средств ИБ приравнивается к эффективности бизнеса).

Вследствие отмеченного выше, при создании IAK ставились следующие цели:

- сделать защиту «из коробки», ориентированную не только на специалистов;
- разработать не конструктор для профессионалов, а решение для бизнеса;
- инициализация защиты должна происходить сразу после запроса;
- отчеты/выходные данные одного инструмента должны "пониматься" другим и использоваться им в качестве настроек при необходимости;
- сканер должен сам обучаться сразу после обновления приложения.

InfoWatch Attack Killer – синергия четырех продуктов

Продукт InfoWatch Attack Killer (IAK) был анонсирован ГК InfoWatch в сентябре 2015 г. и представляет собой первое из российских решений для активной защиты web-приложений способное обеспечить многоуровневую защиту от большинства целенаправленных атак. IAK представляет синергию четырех технологий от компаний, лидирующих в своих продуктовых нишах. Компании Cezurity и Appercut предоставляют технологии обнаружения таргетированных атак и выявления уязвимостей и недокументированных возможностей (НДВ) в коде, соответственно. За защиту веб-инфраструктуры отвечают разработки Wallarm, а защиту от DDoS-атак обеспечивает Qrator Labs. Все технологии работают вместе, непрерывно анализируя возможные угрозы и обмениваясь данными, обеспечивая защиту компании как на уровне операционной системы и серверов, так и на уровне веб-инфраструктуры.

Все четыре компании, технологии которых представлены в IAK, являются: 1) российскими, что позволяет включать разрабатываемые ими продукты и технологии в программы импортозамещения; 2) высокотехнологичными с собственными разработками, уже зарекомендовавшими себя на рынке, т.е. это не стартапы или какие-либо технологические команды; 3) заинтересованными готовыми к интеграции с другими решениями.

Таким образом, были собраны 4 решения (рис. 3):

- *InfoWatch Attack Killer Targeted Attack Detector* (TAD, Cezurity – ГК InfoWatch, борьба с таргетированными атаками);
- *InfoWatch Attack Killer Custom Code Scanner* (CCS, компания Appercut, исследование защищенности бизнес-приложений);
- *InfoWatch Attack Killer Web Application Farewall* (WAF, компания Wallarm, межсетевой экран уровня web-приложений);
- *InfoWatch Attack Killer AntiDDoS* (компания Qrator Labs., система защиты от DDoS-атак).

Модуль TAD предназначен для обнаружения таргетированных атак внутри компании. TAD основан на постоянном контекстном анализе изменений операционной системы, выявлении и анализе аномалий во времени. Сбор данных осуществляется через агентов, которые устанавливаются на каждый компьютер компании. Сам анализ выполняется самообучающейся экспертной системой, расположенной в облаке. При необходимости к анализу подключаются аналитики InfoWatch.

Модуль InfoWatch Attack Killer AntiDDoS работает на внешнем периметре сети и в непрерывном режиме защищает организацию от DDoS-атак. Распределенная сеть фильтрующих узлов, расположенная на магистралях крупнейших интернет-провайдеров, гарантирует блокировку DDOS-атак на начальном этапе.

Модуль WAF работает на уровне защиты веб-инфраструктуры. Он автоматически непрерывно изучает веб-инфраструктуру компании и отправляет на анализ в облачную экспертную систему поведенческую статистику пользователей, результаты динамического сканирования ресурсов. На основе информации об уязвимостях, найденных модулем CCS, WAF выявляет, какие из них могут стать реальными инцидентами ИБ. Благодаря самообучающимся алгоритмам система обеспечивает эффективную защиту от различных хакерских атак в автоматическом режиме. При совместном использовании модулей WAF и AntiDDoS клиент получает возможность блокировать попытки эксплуатации уязвимостей на уровне сети фильтрующих узлов, тем самым снижая нагрузку на приложение.

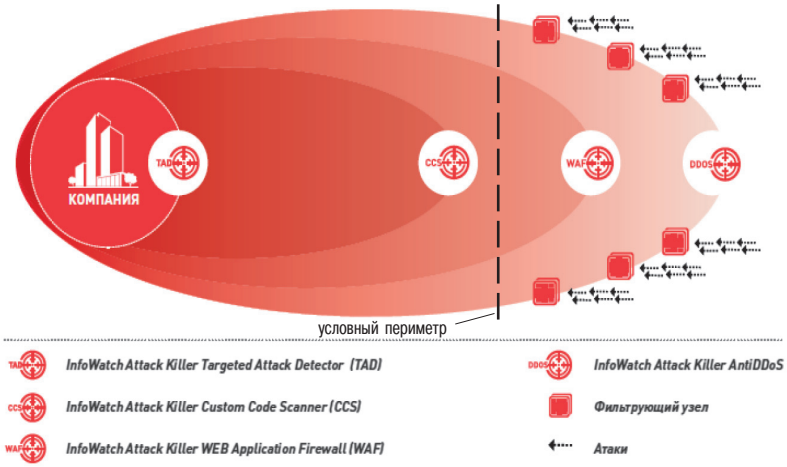

Рис. 3. Схематичное представление уровней защиты решения InfoWatch Attack Killer.

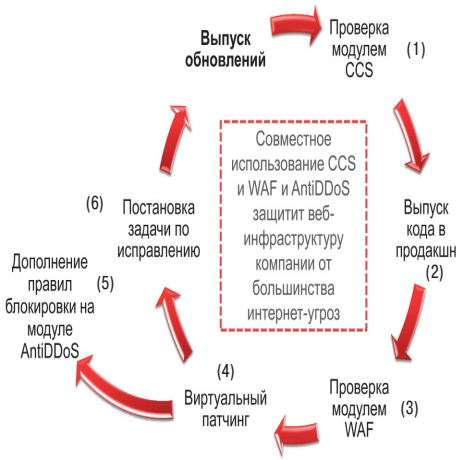

Рис. 4. Комплексная автоматизированная проверка всех изменений приложений на возможные уязвимости.

Модуль CCS детектирует уязвимости кода приложений и передает собранную информацию на модуль WAF для принятия мер по их закрытию. Интеграция модулей CCS и WAF позволяет выявить из множества событий безопасности векторы атак, которые могут стать реальными инцидентами. Обнаруженные методами статического и динамического анализа критичные уязвимости автоматически закрываются виртуальными патчами.

Два продукта – TAD и CCS – обеспечивают защиту изнутри, два других – WAF и DDoS – снаружи. Таким образом, обеспечивается циклическая и непрерывная защита (появился даже термин Continuous Security).

В результате была реализована следующая технология работы (рис. 3). После выпуска обновления приложения его защищенность проверяет CCS (1). Далее обновленное приложение проверяется сканером Wallarm (3). После чего автоматически меняются настройки Farewall и автоматически обучается решение AntiDDoS (5). Рабочие места контролирует Targeted Attack Detector. В результате формируется замкнутый цикл для поддержки постоянно меняющихся бизнес-приложений – добавление новой функции, кнопки, страницы и т.д. динамически отслеживается системой защиты. В случае нахождения уязвимостей формируются рекомендации программистам и до тех пор пока они не устраняются, закрываются виртуальные патчи.

Эти системы, постоянно обмениваясь данными друг с другом, позволяют практически полностью исключить человека из принятия решения, что положительно сказывается на реактивности системы защиты. Именно за счет больших задержек переключения трафика на центр фильтрации (или переключение происходит с большим опозданием, когда атака уже "пошла") после возникновения DDoS-атаки (из-за участия аналитиков в ее разборе), большинство подобных атак достигает цели. Аналогичная ситуация происходит при использования Web Application Farewall. Из-за того, что они очень долго обучаются и очень долго настраиваются, большинство WAF работают "сбоку". В результате атаки не предотвращают, а только фиксируются – "например, был взлом таким-то способом".

В итоге, благодаря высокой интеграции модулей и автоматическому самообучению, удалось создать процесс полностью защищенных web-приложений.

Потенциальными клиентами IAK являются компании:

- которым нужна активная защита, а не на "исследования" безопасности;
- которые имеют "кадровый голод" или которым не хватает финансовых ресурсов для построения многоуровневой системы;
- которым необходимо раскрывать SSL-трафик, т.е. компании, которые не могут пользоваться облачными сервисами для управления ключами шифрования трафика;
- которым требуются сертификаты и аттестаты, например: госструктуры, компании оборонно-промышленного комплекса, некоторые нефтяные компании и др.

В настоящее время получен сертификат только на решение CCS (компания Appercut), но в ближайшее время планируется сертификация и всех остальные продукты, а также общая – на интегрированное решение.

Более того, ГК InfoWatch в ближайшее время планирует (через страховые компании) ввести страховую ответственность за то, что если IAK пропускает атаку, то выплачивается компенсация заказчику.

Решение IAK было протестировано на больших нагруженных системах (как отдельные компоненты, так и в целом) в течение нескольких лет. И это дает основания полагать о его устойчивости и надежности.

IAK позволяет удовлетворять требования регуляторов – ФСТЭК, Банка России, PCI DSS, а также требования по безопасной разработке (приказ ФСТЭК России №21 и №17, ФЗ-№152, PCI DSS, СТО БР, НДВ4, SDL). За счет автоматизированного самообучения на отдельных применениях, например, для интернет-магазинов, IAK позволяет отказаться от выделенных сотрудников по ИБ – знаний ИТ-администратора достаточно для ее поддержания. IAK позволяет использовать каждый модуль по отдельности, в любых сочетаниях, а также быстро расширить используемый комплекс до полного комплекта.

Управление всеми компонентами InfoWatch Attack Killer осуществляется через единый веб-интерфейс. Решение создает детализированные отчеты о зафиксированных таргетированных атаках, найденных уязвимостях и попытках их эксплуатации, аномальной активности приложений и DDoS-атаках. Благодаря наглядной визуализации атак и подробным экспертным рекомендациям по устранению проблем, для интерпретации отчетов не требуется специализированных знаний.

Внедрение IAK в банке "Югра"

Банк «Югра» является одним из крупнейших российских банков, на сегодняшний день занимает 33-ю позицию по сумме чистых активов и 21-ю позицию по объему капитала в рейтинге крупнейших отечественных кредитных организаций. По всей России работает более 80 офисов банка – к концу 2015 г. планируется открытие еще около 20 филиалов.

В 2014 году Банком было принято решение разработать новый интернет-банк для розничных клиентов банка (физических лиц). В данном проекте принимались участие как ИТ- и ИБ-службы, так и основные представители со стороны бизнес-подразделений.

Так как ИБ – один из важнейших приоритетов Банка, то при реализации интернет-банка была проведена следующая подготовительная работа:

- проработаны варианты защиты от DDoS-атак;
- проанализирован код с помощью InfoWatch Appercut;
- проанализирован рынок WAF-решений;
- проработано несколько пилотных проектов по защите от таргетированных атак (anti-APT), включая InfoWatch Attack Killer.

Банк "Югра" стал первым банком, который инсталлировал полное решение IAK – все развертывание заняло 2 рабочих дня:

- установка защиты от DDoS (Qrator) – 15 минут времени на регистрацию (заполнение анкеты на сайте компании) и 15 минут на корректировку IP. Установка WAF Wallarm – 2 клика в личном кабинете. После этого весь трафик банка был перенаправлен на соответствующие сервера и очищался на стороне Qrator AntiDDoS. Одновременно сразу были получены отчеты от WAF Wallarm о потенциальных уязвимостях на нашем сайте;
- установка InfoWatch Appercut не требовалась, т.к. решение уже было реализовано в Банке;
- установка InfoWatch TAD Detector заняла 2 часа времени. Инженер Cezurity проверил политики по установке клиентов, написал соответствующие правила и политики на стороне Банка. После этого на второй рабочий день решение работало на 85% рабочих станций, а по завершении недели 100% рабочих станций было закрыто.

"В течение первых суток работы с Wallarm мы смогли найти одну неприятную уязвимость на сайте, которая возникла после последнего обновления и благодаря полученным рекомендациям закрыть ее за несколько часов. Теперь мы получаем ежедневные и еженедельные управленческие отчеты по атакам на сайт, сканированиях на уязвимости и потенциальных угрозах на серверах и рабочих станциях в периметре Банка. Пожалуй, чтение отчетов и осталось самой большой нагрузкой по данному проекту. Затраты на поддержание решения практически нулевые: один работник тратит 1 час рабочего времени. Банк доволен результатами сотрудничества по данному комплексу продуктов и будет помогать совершенствовать его в меру своих возможностей" – Кирилл Мартыненко, CISO Банка "Югра".