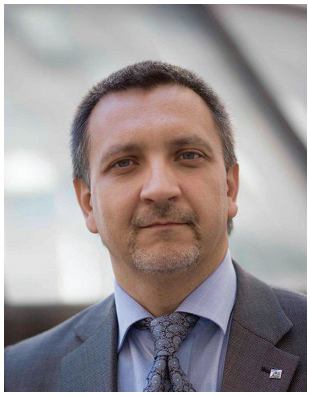
IAK устраняет "человеческий фактор"

Комментарии SN Рустэма Хайретдинова, заместителя генерального директора ГК InfoWatch, в связи с состоявшимся в сентябре 2015 г. анонсом решения InfoWatch Attack Killer (IAK).



Рустэм Хайретдинов – заместитель генерального директора ГК InfoWatch.

SN. Что представляет собой поставка IAK – ПО, унифицированный аплайнс, набор решений в стойке?

Р.Х. Клиент получает то решение, которое больше всего ему подходит: облачный сервис, лицензию на ПО, виртуальный или реальный appliance.

SN. Как организована интеграция между модулями – с использованием агентов, интерфейсов (имеющихся или дополнительных) и др.?

Р.Х. В текущей версии модули SAST-DAST-WAF-antiDDoS интегрированы через вызовы API, а anti-APT решение интегрировано с остальным комплексом через общую отчетность. В дальнейшем планируется интеграция на уровне корреляций – при определении начала атаки по одному из каналов будут меняться настройки на других каналах

SN. Сколько времени уходит на развертывание? Чьими силами это реализуется? Какова стоимость? Требуется ли предварительный аудит системы?

Р.Х. При подключении облачного сервиса после заполнения заказчиком опросника в течение нескольких минут он получает настройки приложения и перенаправляет трафик на сервисы IAK, получая полную защиту. Внедрение программного обеспечения или ПАК занимает больше времени, технологически на это отводится от одного до нескольких дней.

SN. Как организована защита к средствам управления по настройке модулей?

РХ. Защита средств управления традиционна для средств защиты: шифрование управляющего трафика, авторизация управляющих сессий и т.п.

SN. Какова масштабируемость системы в целом и ее отдельных продуктов?

Р.Х. Теоретически система не ограничена в производительности и масштабируется линейно. Фактически решение уже работает на сложных территориально распределенных системах на 200 нод и более.

SN. В условиях распространения многоэтапных атак (с использованием, в том числе, и отвлекающих атак) важна не только интеграция средств защиты, но и интеграция всей информации об угрозах и рисках с возможностью ее комплексного анализа. Реализовано ли это в рамках IAK?

Р.Х. Каждый из модулей интегрирован с соответствующим облачным сервисом, который регулярно актуализирует информацию на сервисе, обновляя информацию об активности бот-сетей, новых уязвимостях и способах атаки.

SN. В условиях все возрастающих требований к реактивности средств защиты запоминаются ли шаблоны поведения атак для ускорения их выявления? Какие продукты IAK это используют?

Р.Х. Все продукты – и анти-APT, и статический сканер, и динамический сканер, и WAF, и анти-DDoS, – обновляют соответствующие им принципы атак через облачные сервисы.

SN. Интегрированы ли в IAK средства защиты мобильной связи, развиваемые InfoWatch?

Р.Х. В текущей версии они никак не интегрированы.

SN. В условиях, когда придумываются все более хитроумные алгоритмы проникновения в системы, как можно убедить страховщиков выдавать гарантии на непроходимость атак в случае использования IAK? Проводились ли специальные исследования и тестирование IAK на устойчивость к атакам?

Р.Х. Развитие любого продукта в области информационной безопасности немыслимы без постоянных тестов на устойчивость к атакам, внутренним и внешним. Поэтому в команде есть группы, которые постоянно пытаются атаковать защищаемые ресурсы, а большинство серьезных проектов сопровождаются независимыми внешними тестами на проникновение.

SN. Всего несколько лет назад утверждалось, что невозможно противодействие DDoS на основе алгоритмов – нужны онлайновые коллективы аналитиков. В этом контексте – за счет чего в IAK удалось "избавиться" от людей? Какова пропускная способность решения?

Р.Х. При использовании IAK удалось избавиться от "человеческого фактора" на стороне клиента, поскольку именно они и есть самое "тонкое место" и большинство успешных атак связаны именно с неверной реакцией на стороне клиента. Это связано с тем, что, как бы не была совершенна система защиты от DDoS, проблема в архитектуре остается: большинство компаний пропускает трафик через центр очистки только под атакой, а без атаки пользуются неочищенным трафиком. В этой архитектуре решение о переключении трафика на центр очистки принимает оператор на стороне клиента, который, по статистике, делает это слишком поздно. В IAK же трафик постоянно проходит через распределенные центры очистки, во время атак и без них. А в центрах очистки, конечно, работают команды аналитиков, и за качество их работы и их профессиональную подготовку отвечаем мы, а не клиент. Поэтому атаки на клиентов просто не доходят, поскольку отфильтровываются еще «на дальних подступах». Пропускная способность распределенных центров очистки соответствует требованиям самых нагруженных клиентов и постоянно растет.

SN. Можно ли привести примеры новых черт интеллектуальности WAF (а также других продуктов) при использовании в составе IAK?

Р.Х. WAF в IAK настраиваются автоматически на основе двух типов алгоритмов. *Первый алгоритм* – это постоянный аудит защищаемого ресурса на наличие уязвимостей с помощью встроенных – статического и динамического – сканеров: как только обновляется инфраструктура или само приложение, они автоматически сканируются на наличие уязвимостей, проверяется эксплуатируемость найденных уязвимостей в конкретном контексте и, если они эксплуатируются на WAF, передаются настройки, закрывающие возможность такой эксплуатации, то есть выпускается "виртуальный патч".

Второй тип алгоритма – постоянное самообучение на трафике и анализ аномалий. Простейший пример: если в одно поле постоянно вводились данные, например, четыре буквы и пять цифр, а затем вдруг в это поле начинают вводиться другие символы, похожие на команды, то система динамически заблокирует такие попытки.

SN. Как реализуется интеграция IAK с SIEM-системами?

Р.Х. Система поддерживает типовые протоколы и способна выгружать события в любые SIEM, их поддерживающие. По факту у клиентов используются HP ArcSight, IBM Qradar, RUSIEM, и другие решения.

SN. Как реализуется интеграция с GRC-системами?

Р.Х. На сегодняшний день такой потребности у клиентов не выявлено, однако решение использует стандартные интерфейсы, и препятствий для интеграции не видно.

SN. Как обеспечивается защита от внутренних угроз, если отсутствует интернет (связь с облаком аналитики)?

Р.Х. При потере связи со станцией, TAD, в первую очередь, сообщает об этом оператору, чтобы он мог проверить причину потери связи. При этом агент TAD продолжает снимать «слайсы» и хранит их, чтобы при подключении передать их в облако.