cezurity

Безопасность из облака: можно ли доверить обнаружение целенаправленных атак облачному сервису?

С одной стороны, обработка данных в облаке позволяет точнее обнаруживать угрозы.
С другой, есть опасение, что важная информация будет неконтролируемо обрабатываться где-то за пределами условного периметра сети.

Облачные вычисления сегодня применяются в разных областях и подчас позволяют решить такие задачи, которые раньше казались либо очень трудными, либо неосуществимыми. Но одним из препятствий на пути использования облаков становятся вопросы безопасности. Иногда для того, чтобы избавиться от большинства опасений, достаточно внимательнее посмотреть на те или иные особенности конкретной облачной архитектуры.

Прежде всего имеет смысл разделить два совершенно разных понятия. Первое – это облачная безопасность. Под “облачной безопасностью” можно понимать очень широкий круг вещей: от конфиденциальности и целостности данных в облаке до защиты от атак облачных инфраструктур. Второе понятие – это безопасность из облака. Здесь речь идет о том, что облачные технологии используются просто как инструмент для решения задач, связанных с защитой от тех или иных угроз.

Безопасность из облака уже давно в разной степени используется в продуктах ИБ-вендоров. Хотя в корпоративных решениях иногда существует возможность отключить передачу любой информации в облако, ее довольно редко используют. Например, даже в случае с традиционным антивирусом, отключение облачных компонентов, как правило, настолько снижает уровень защиты, что делает его работу практически бесполезной.

Большинство корпоративных антивирусных решений позволяет отключить передачу каких-либо данных с компьютеров пользователей. Есть ли такая возможность в облачном решении?

Облачное решение Cezurity не позволяет полностью отключить передачу данных с компьютеров пользователей. Для обнаружения целенаправленных атак это необходимо. В основе решения лежит анализ изменений во времени критических областей систем. Такой анализ не может осуществляться локально.

Традиционные методы обнаружения предназначены для защиты от массовых атак – то есть таких атак, инструменты для осуществления которых уже использовались и, соответственно, их признаки встречались раньше. Если сравнить это, например, с медициной, то диагноз одному пациенту здесь ставится на основе наблюдаемых симптомов у другого. В случае целенаправленных атак такой метод неэффективен, потому что злоумышленники используют уникальные инструменты и методы атаки.

Некоторые данные с компьютеров сотрудников организации передаются для обработки на сервер. Не приведет ли это к тому, что будет скомпрометирована какая-либо конфиденциальная информация?

В облако Cezurity для обработки *не передаются* никакие данные, утечки которых можно опасаться.

Для обнаружения целенаправленных атак решением Cezurity COTA анализируется информация об объектах, расположенных в критических местах систем. В таких местах не хранятся ни документы, ни их содержимое, ни какие-либо другие пользовательские данные.

Для анализа в облако могут передаваться тела подозрительных исполняемых файлов. Неисполняемые файлы, например, документы и их содержимое, к таким объектам не относятся, и, соответственно, в облако не передаются. При этом оценка того, является ли каждый объект исполняемым файлом, происходит на клиенте до передачи его в облако.

Таким образом, в результате использования решения никакая конфиденциальная информация не может быть скомпрометирована – она не обрабатывается и не покидает пределов компьютера.

Не окажется ли в результате работы решения передана в облако и скомпрометирована топология корпоративной сети?

Решение Cezurity не собирает и не анализирует информацию о топологии корпоративной сети. Обнаружение атак опирается на мониторинг изменений конечных точек, без учета их взаимосвязи.

Пути к файлам в критических областях системы передаются в облако, но перед этим подвергаются анонимизации.

Если будет атаковано само решение COTA, то смогут ли злоумышленники воспользоваться установленными на каждом из компьютеров агентами для того чтобы похитить нужную им информацию?

Злоумышленники не смогут воспользоваться агентами для похищения информации.

Данные модули в автоматическом и автономном режиме выполняют следующие задачи: периодическое сканирование состояния системы, извлечение необходимого набора критических объектов и их характеристик, подготовка данных для отправки в облако (агрегация и анонимизация) и их передача. Невозможно удаленно изменить функциональность агента или получить с его помощью какую-либо другую информацию с клиентского компьютера.

Обнаружение целенаправленных атак можно реализовать только с помощью специальных решений. Обратитесь за дополнительной информацией на www.cezurity.com

Cezurity — российская компания, разрабатывающая технологии и решения для защиты от широкого круга вредоносных программ и хакерских атак. Основана в 2006 году (до 2011 года называлась «Онлайн Решения»), с момента своего появления фокусируется на разработке технологий защиты нового поколения, реализация которых стала возможна благодаря широкому применению облачных технологий и методов интеллектуального анализа больших массивов данных (Big Data). Среди ключевых технологий Cezurity — анализ событий, мониторинг изменений систем, создание защищенных сред исполнения программного обеспечения.

Россия, Санкт-Петербург
ул. Матроса Железняка, 57

+7 812 640 4143
www.cezurity.com