Денис ГАСИЛИН: «Решение SafenSoft Enterprise Suite является необходимым и достаточным для защиты корпоративной информационной среды»

Интервью с руководителем отдела маркетинга компании SafenSoft

– Как вы оцениваете существующую практику применения программных средств наблюдения за компьютером и мониторинга активности пользователей?

– В отличие от ситуации на Западе российская практика применения средств наблюдения за компьютером сотрудника и контроля активности пользователей находится в зачаточном состоянии. Несмотря на наличие на рынке готовых решений для закрытия этой «дыры» в безопасности организаций, сама идея применения подобных средств не находит отклика среди сотрудников, ответственных за ИБ. Зачастую все меры по предотвращению утечки данных сводятся к мониторингу посещаемых сотрудником веб-сайтов, авторизации с помощью USB-токенов и логирования переписки в популярных программах обмена сообщениями. При этом решения, ориентированные на запись текста в конкретных приложениях, сотрудники обычно обходят (например, путем использования веб-клиентов). Изобретательность наших соотечественников такова, что даже закрытие 95% потенциальных каналов утечки данных лишь заставит инсайдера поработать дольше. Защита должна быть комплексной, учитывающей все каналы связи – от Интернета до внешних устройств вроде принтера или съемных носителей информации.

– Каков функционал решения SafenSoft Enterprise Suite? Каковы возможности применения политик безопасности? Сохраняется ли в случае установки Enterprise Suite необходимость использования дополнительных средств защиты, таких как сетевой экран или антивирусы?

– SafenSoft Enterprise Suite – комплексное модульное решение типа «Купол». Этот термин – идея отдела маркетинга SafenSoft, которая пришлась по душе руководству компании. «Купол» в полной мере отображает принцип работы продукта: в полной конфигурации SafenSoft Enterprise Suite обеспечивает целостность программного обеспечения ПК и позволяет закрыть почти все потенциальные каналы утечки данных.

Многообразие настроек политик безопасности способно удовлетворить практически любое пожелание клиента. Одна из особенностей – возможность централизованного управления всеми подконтрольными устройствами. Наличие ролей в системе позволяет разграничить доступ пользователей к информации и внешним устройствам.

Продукт состоит из двух больших подсистем – обеспечения работоспособности компьютера и DLP. Каждая из них автономна, но весь комплекс управляется централизованно. DLP позволяет фиксировать необходимую информацию и проводить расследование инцидентов, что чрезвычайно важно в банковских системах. Наше решение является необходимым и достаточным для защиты корпоративной информационной среды. В зависимости от комплектации в продукт может входить и антивирус – клиенту предлагается несколько антивирусных решений на выбор. Для защиты серверов и каналов существуют другие решения.

Впрочем, большой необходимости в антивирусе на рабочей станции с нашим продуктом нет. Благодаря технологии проактивной защиты решение идет на шаг впереди злоумышленника, предотвращая возможность модификации приложений и процессов на компьютере. За счет совмещения работы с «белыми списками» и эвристического анализа система сохраняется в последнем заведомо рабочем состоянии, а любая подозрительная активность блокируется. Кроме того, любую программу можно запускать в изолированной среде. Такой подход позволяет не только защищать организацию от традиционных атак, с которыми борются антивирусы, но и предотвращать таргетированные атаки с использованием эксплойтов «нулевого дня».

– Каковы особенности реализации системы администрирования SafenSoft Enterprise Suite? Что выделяет это решение среди подобных продуктов ИБ?

– Администрирование осуществляется путем прописывания правил, определяющих работу с пользователями, с устройствами и с операционной системой на уровне пользователей и устройств. Это позволяет максимально расширить круг исполнения запросов. Работа с фиксированными сценариями дает возможность оперативно реагировать на изменения системы, более того, каждый сценарий может быть специально сертифицирован, что предотвращает исполнение случайных сценариев. Функционал временного контроля ключей и доступов обеспечивает очень точный контроль работы администрирующего персонала. ■