Равиль САФИУЛЛИН:

«Обнаружение угроз в реальном времени – одно из преимуществ решений IBM»

На вопросы журнала Connect отвечает Равиль САФИУЛЛИН, руководитель группы продаж департамента аппаратных средств, IBM в России и СНГ.

– Энергетика относится к одной из самых критичных сфер экономики. При этом информационная система любой энергосети/энергообъекта имеет сложную топологию, включает разнообразные сегменты, подсистемы и оконечные устройства. Какова основная проблематика обеспечения информационной безопасности энергосети?

– Информационные системы энергетических объектов сегодня зачастую построены так же и используют те же технологии, что и офисные сети: Windows, Linux, Ethernet, HTTP, XML, DCOM, .NET, SQL, SOAP и т. д. Промышленные системы вместе со всеми положительными аспектами этих технологий получили «в подарок» и все их проблемы и уязвимости, которые широко известны. Эксплуатация уязвимостей в промышленной среде хоть и имеет свою специфику, но возможна и почти не отличается от таковой в корпоративной сети.

– С какими событиями/инцидентами информационной безопасности приходится сталкиваться при обеспечении информационной безопасности энергосети/энергетического объекта? Есть ли отраслевая специфика и в чем она заключается?

– Производители и инженеры КИПиА уделяют основное внимание функционалу и производительности, а также обеспечению работоспособности часто в ущерб безопасности систем. Наиболее проблемные сегменты для энергетики обусловливаются распределенной инфраструктурой и высоким уровнем автоматизации. В зоне риска находятся дистанционные методы управления, удаленная диспетчеризация, беспроводные коммуникации, веб-технологии. Причинами возникающих инцидентов информационной безопасности часто являются последствия воздействия вирусов, «троянских программ», «червей», DoS-атак, некорректное обновление ПО, несанкционированный доступ к данным и человеческий фактор.

– Компания IBM имеет большой опыт работы в сфере энергетики во всем мире. На какие выводы наталкивает этот опыт? Что нужно/можно сделать для обеспечения безопасности энергетических объектов/сетей достаточно оперативно, что требует длительных и целенаправленных усилий?

– Опыт наших заказчиков и реализованных проектов показывает, что на многих предприятиях обеспечение технологической безопасности находится на высоком уровне, а информационной безопасности АСУ ТП должного внимания не уделяется. К примеру, применяемые контроллеры SCADA/PLC зачастую используют стандартные аутентификационные данные, прописанные явным образом в документации. Данный факт может быть не известен оператору системы, работающему на более высоком уровне АС.

Для предотвращения подобных случаев моментальный эффект достигается применением систем со встроенной экспертизой о типовых угрозах. Долговременные усилия защиты в виде анализа трафика, автоматизации мониторинга изменений и оценки воздействия изменений на конфигурации сетевой инфраструктуры позволяют динамически отслеживать ситуацию и обеспечивать высокий уровень практической защиты.

Решение IBM QRadar SIEM сочетает в себе сильные стороны обоих подходов, позволяя производить более точное обнаружение угроз в реальном времени.

– Ситуация с моральным устареванием технологий, промышленного оборудования на предприятиях российской экономики общеизвестна. В какой степени, по вашим наблюдениям, это относится к энергетической сфере? Насколько остро стоит проблема

модернизации энергосетей и как это сказывается на задачах обеспечения информационной безопасности?

– Старение основных фондов – вопрос, который для энергетической системы России с каждым годом становится все более актуальным. Но в энергетической отрасли большое значение придается современным технологиям. Постоянно внедряется эффективная, не требующая обслуживания техника, «умная» автоматика, наращиваются пропускная способность и мощность. Все чаще компании внедряют комплексные системы интеллектуального учета электроэнергии на основе технологии Smart Metering, создают центры оперативного управления сетями и производственными активами.

Если принимать в расчет сжатые сроки внедрения проектов, то на первый план при решении вопросов обеспечения информационной безопасности выходят необходимость быстрого развертывания, высокая универсальность и интегрируемость систем. Модульный принцип устройства и интегрированная экспертиза в решениях IBM позволяют оперативно настраивать сложные многофункциональные системы, обеспечивая при этом прозрачность и эффективность управления. Встроенные механизмы виртуализации обеспечивают возможность эффективного использования уже имеющихся аппаратных ресурсов как путем миграции продуктивных данных без остановки промышленных процессов, так и за счет снижения уровня необходимых первоначальных инвестиций для приобретения вычислительной инфраструктуры и ПО.

– Для каких направлений обеспечения ИБ в энергетике предназначены решения/продукты IBM? Что представляет собой программно-аппаратный комплекс PureFlex?

– Решения IBM представлены широко в корпоративной сфере, энергетическая отрасль не является исключением. Заказчики активно используют встроенную в системы IBM PureFlex экспертизу для быстрого и надежного развертывания корпоративных систем любых уровней. Поддержка вычислительных платформ на базе процессоров Intel x86, IBM Power, всех распространенных в индустрии системных сред, включая ПО с открытым кодом, широкие интегрированные коммуникационные возможности позволяют создавать на базе систем IBM PureFlex весьма надежные и экономичные решения.

о событиях/инцидентах информационной безопасности в режиме реального времени и оперативно управлять угрозами ИБ?

– IBM QRadar SIEM обладает весьма обширным перечнем источников информации о событиях/инцидентах информационной безопасности. Журналы событий, IP-репутация, отслеживаемые потоки данных, геолокационные данные, информация об активности пользователей, БД, приложений и сетевой активности поступают на вход интегрированного ителлектуального модуля

> Решение IBM Qradar SIEM сочетает в себе сильные стороны обоих подходов, позволяя производить более точное обнаружение угроз в реальном времени.

Для работы с технологиями Big Data, накопления и обработки больших массивов информации с отчетами по событиям IBM предлагает высокопроизводительные системы хранения данных со встроенными технологиями: компрессией данных «на лету» (для уменьшения объемов информации, фактически хранимой на дисковых накопителях), использованием высокопроизводительной энергонезависимой памяти Flash (для обеспечения моментального доступа к наиболее важной и востребованной информации), расширенными функциями аппаратной виртуализации (возможность использования дискового пространства существующих СХД совместно с новыми технологиями).

– Что позволяет программной платформе IBM Security QRadar SIEM отображать поступающую по сети информацию

IBM QRadar SIEM, производящего корреляцию событий и подготавливающего исключительно точные и практически применимые выводы. Модуль QRadar QFlow дополняет QRadar SIEM, обеспечивая глубокий анализ контента. Он собирает данные потоков уровня 7 (приложений) при помощи технологии deep packet inspection, предоставляя возможность обнаруживать самые современные угрозы путем анализа содержимого пакетов. QRadar VFlow обеспечивает тот же уровень видимости для виртуального сетевого трафика, предоставляя сравнимую с QRadar QFlow функциональность, но для виртуальных сред.

Таким образом, на основании широчайшего спектра данных IBM QRadar способен в режиме, близком к реальному времени, обнаруживать аномалии и производить корреляцию событий информационной безопасности с учетом контекста. ■