«EFROS CONFIG INSPECTOR»: БЕЗОПАСНОСТЬ В ЭПОХУ ПЕРЕМЕН

В наш век постоянных изменений становится все сложнее обеспечить необходимую и достаточную безопасность. Ситуация с взаимопроникновением технологий дошла до того, что приходится думать о безопасности систем безопасности. Относительно недавно сложно было представить ситуацию, когда система охранного телевидения, состоящая из телекамер и видеорегистратора (а то и видеомагнитофона), «напала» бы на сервера (или папки с документами) бухгалтерии и «уложила» бы их. А ведь такие случаи все чаще происходят в наше время: достаточно вспомнить про ботнет Mirai, атаковавший веб-сайты и провайдеров в США. Исследования показали, что заражено было около ста тысяч устройств, а всего в Интернете на тот момент обнаруживалось более полумиллиона устройств, потенциально уязвимых для червя. В результате атаки оказался затруднен или вовсе невозможен доступ к таким сайтам, как Twitter, Github, Soundcloud и др.

Можем ли мы полностью обезопасить себя от всех угроз, возникающих в наше время? Вряд ли. Это отмечают на всех уровнях: можно привести в пример слова Президента России о том, что пока сотни человек совершенствуют законы, миллионы думают, как их обойти. Аналогичная ситуация и с безопасностью. В отношении информационной безопасности можно привести рекомендации от составителей всемирно известной библиотеки ITIL: необходимо фокусироваться не на способности отразить 100% угроз, но на возможности постоянно предоставлять минимально согласованный уровень услуг через снижение риска и планирование мероприятий по восстановлению. Иначе говоря, выживет тот, кто сумеет приспособиться.

Программный комплекс «Efros Config Inspector», разработанный ООО «Газинформсервис», является решением, которое хоть и не защищает бизнес напрямую от угроз ИБ, как, например, антивирус, но помогает оперативно реагировать на возникающие изменения. Программный комплекс подключается к устройствам, загружает конфигурационные файлы и контролируемые списки, проверяет их неизменность. Такие проверки запускаются по расписанию, по требованию, по событию. Рассмотрим три основных направления, в которых действует «Efros Config Inspector»: контроль конфигураций сетевого оборудования, контроль виртуальных сред и контроль конфигураций АСУ ТП.

Программный комплекс работает с популярными линейками сетевого оборудования, представленного на рынке в России: Cisco (IOS, PIX, ASA и др.), Korenix (JetNet), Huawei (Quidway), Фактор-ТС (Dionis LX/NX), Juniper Networks (JUNOS) и не только. Являясь разработчиком программного обеспечения, ООО «Газинформсервис» предлагает услугу по интеграции с оборудованием в интересах заказчика, что позволяет использовать «Efros Config Inspector» для контроля конфигураций сетей передачи данных, выполненных на оборудовании различных производителей.

Помимо контроля конфигураций активного сетевого оборудования «Efros Config Inspector» может осуществлять защиту информации, обрабатываемой в виртуальной среде. Учитывая возрастающую популярность решений на базе виртуальных серверов, в том числе в сфере систем физической защиты, контроль этого сегмента IT-инфраструктуры является важной составляющей комплексной безопасности объекта.

Третье, на что хочется обратить внимание читателей, – контроль целостности конфигураций АСУ ТП. И хотя обсуждение данного вопроса может вылиться в написание отдельной статьи, если не книги, следует отметить основные моменты. Требования к информационной безопасности АСУ ТП изложены в приказе № 31 ФСТЭК от 14.03.2014, а также в недавно принятом федеральном законе № 187 «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017. Программный комплекс «Efros Config Inspector» позволяет отслеживать изменения в конфигурациях оборудования АСУ ТП и оперативно реагировать на эти изменения. Встроенные в комплекс инструменты позволяют хранить в зашифрованном виде базу данных эталонных конфигураций, что может существенно облегчить работу сотрудника службы IT или ИБ по восстановлению системы в случае выявления инцидента.

Программный комплекс «Efros Config Inspector» имеет удобный интерфейс представления основной информации в системе, т. н. «Dashboard». Сотрудники получают информацию оперативно, в удобном для восприятия виде.

В заключение снова хочется обратить внимание читателей на подход к безопасности, изложенный в начале статьи. Наверняка этим «новым» мыслям примерно столько же лет, как первому потайному ходу из какой-нибудь античной крепости. Стоит ли пытаться строить непреодолимую стену или стоит задуматься: а что делать, если враг все же проникнет за нее? Будет ли у службы безопасности план на случай форс-мажорных обстоятельств? Именно с учетом этих вопросов, а также с желанием дать на них целесообразный ответ, и создавался программный комплекс «Efros Config Inspector». Приглашаем всех заинтересовавшихся ознакомиться с его функциями на сайте ООО «Газинформсервис» или на одном из мероприятий, организуемых компанией.

Рис. 1. Схема работы «Efros Config Inspector»