УДК 004.457

Обеспечение промышленной информационной безопасности с помощью Kaspersky Industrial CyberSecurity

Солодова Екатерина Игоревна
Российский Экономический Университет им. Г.В. Плеханова
студент

Аннотация
Данная статья содержит описание программно-аппаратного комплекса Kaspersky Industrial CyberSecurity по защите автоматизированных систем управления технологическими процессами. Рассмотрена специфика защиты АСУ ТП и проанализирован российский рынок программных решений.
Ключевые слова: АСУ ТП, промышленная кибербезопасность, Лаборатория Касперского.

Industrial information security via Kaspersky Industrial CyberSecurity

Solodova Ekaterina Igorevna
Plekhanov Russian University of Economics
student

Abstract
This article discusses the Kaspersky Industrial CyberSecurity hardware and software complex for the protection of Process Automation System. Special features of protection are considered and the Russian market of software solutions is analyzed.
Keywords: PAS, industrial cybersecurity, Kaspersky Lab

Появление первых автоматизированных систем управления технологическими процессами (далее – АСУ ТП) началось примерно в 80-ых годах, когда пришло осознание того, что «безмашинной» обработки информации и управления недостаточно[1]. АСУ ТП - автоматизированная система управления технологическими процессами. Она включает в себя программный и технический комплекс по автоматизации технологических процессов и оборудования, например: DCS (Distributed Control Systems) - распределенные системы управления, PLC (Programmable Logic Controller) - программируемый логический контроллер. Все подсистемы объединяются в одну глобальную - систему операторского управления в виде SCADA-систем (с помощью промышленных сетей), пультов управления и элементов автоматики.

При появлении АСУ ТП являлись изолированными и узкопрофильными системами, что практически не представляло угрозы информационной безопасности предприятия. Они защищались физической изоляцией, но не продолжительный период оставались нетронутыми. С течением времени и развитием оборудования и технологий, автоматизированные элементы стали все больше походить на корпоративные бизнес-приложения, имеющие большую интегрированность, удаленный доступ, облачные хранилища и выход в интернет, что сделало их более уязвимыми к информационным атакам и угрозам. Свидетельством этого стал распространяемый вирус Rootkit.Win32.Stuxnet, поражающий программируемые логические контроллеры через соединения с помощью флеш-накопителя, который изменял работу центрифуг, обогащающих уран. Из-за использований внешних соединений АСУТП стала подвергаться атакам компьютерных червей и вредоносных ПО через уязвимости Windows, изначально не предназначавшихся для этих целей.

Следует разграничивать информационную безопасность для корпоративных информационных систем и для промышленных предприятий. Для операционных технологий, в отличие от информационных, в первую очередь нужно обеспечивать непрерывность и целостность процессов, чтобы обезопасить процесс производства в целом. Это является критически важной спецификой обеспечения кибербезопасности. Вместе с этим встал вопрос о информационной безопасности АСУ ТП. АСУ ТП управляют важнейшими процессами на предприятии в таких отраслях, как: энергетика, металлургия и т.д. Поэтому нарушение их безопасности может обернуться как просто финансовыми потерями, так и человеческими жизнями и техногенными катастрофами. Для киберпреступников максимальный интерес вызывают те отрасли промышленности, где ущерб будет большим: ТЭК, нефтяные компании, электроснабжение и т.д. Хорошим примером служит относительно недавнее событие на Украине, когда стало известно, что в компании «Прикарпатьеоблэнерго» осуществлялись атаки на SCADA-системы с помощью трояна «BlackEnergy», что привело к массовому отключению энергии на западе страны. Вирус доставлялся с помощью компьютеров, на которые устанавливался компонент «KillDisk». Он не только удалял файлы пользователей, но и портил системные файлы, что приводило к неработоспособности системы [2]. Алгоритмы злоумышленников в основном одинаковы. Они получают доступ к технологической сети, взламывают доступ к ПЛК и после анализа конфигурации ПЛК изменяют принцип его работы. Предупредить аварию без внедрения средств информационной защиты технологических процессов практически невозможно.

Риски, которые исключает «Лаборатория Касперского» в своих продуктах связаны с ошибками третьих сторон при работе с SCADA, несоблюдением требований регулирующих органов, отсутствием отчетности по инцидентам, неосведомленностью расследования инцидентов. Компания в

том числе предотвращает нежелательные действия сотрудников, как случайные, так и преднамеренные.

Экспертные сервисы проводят оценку перед внедрением программного решения, выявляют специфические алгоритмы, под которые нужно адаптировать систему и анализируют архитектуру предприятия. Перед установкой программного комплекса, «Лабораторией» проводится предварительный анализ и оценка защищенности от киберугроз, чтобы выявить потребности заказчика, текущий уровень безопасности, а также специфику предприятия для индивидуальной интеграции каждого решения.

Отдельным пунктом является выявление соответствия АСУ ТП требованиям Приказа ФСТЭК России от 14 марта 2014 г. №31, который утверждает требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами.

Сервисы, предлагаемые «Лабораторией Касперского», уделяют особое внимание обучению персонала. Они включают в себя тренинги по кибербезопасности и, в частности, игру «Kaspersky Industrial Protection Simulation», моделирующую возможные атаки на промышленные системы. Целью этого является повышение уровня знаний среди сотрудников, так как даже квалифицированный персонал может не знать о том, как распространяются вирусы и как реагировать при обнаружении атаки. При этом действия сотрудников в состоянии паники могут нанести еще больший ущерб при инциденте.

«KICS» (Kaspersky Industrial CyberSecurity) включает в себя три технологии, которые в едином комплексе отвечают за безопасность промышленных процессов.

«Kaspersky Industrial Cybersecurity for Nodes» (защита узлов - рабочих станций, серверов, ПЛК). Эта система предназначена в большей мере для устранения риска человеческого фактора: контролирует подключение флеш-накопителей, модемов, адаптеров, а также запуск сторонних приложений с последующей блокировкой ВПО (вредоносного программного обеспечения), обеспечивает целостность работы узлов и фильтрует сетевой трафик, предотвращая вторжения IPS/IDS. «Узлы» подвергаются периодической проверке на уязвимости для предупреждения действия эксплойтов. Для проверки целостности проектов ПЛК, программный комплекс сравнивает каждый текущий проект с заданным администратором эталонным, и в случае несовпадения контрольной суммы генерирует событие нарушения целостности.

«Kaspersky Industrial CyberSecurity for Networks» (защита сетей - мониторинг сетевого трафика в пассивном режиме). Технология работает в пассивном режиме и отслеживает появление новых сетевых устройств, сетевого трафика и появление аномальных потоков в нем, работу удаленных терминалов(RTU), контролирует команды, посылаемые ПЛК, изменения параметров техпроцесса. Эта ветка решения так же анализирует события для последующего расследования киберинцидентов, регистрирует процессы в

журнале. О всех нежелательных и потенциально опасных действиях система сразу сообщает операторам с помощью ЧМИ (человеко-машинного интерфейса), но для злоумышленников программа не обнаружима. Установка приложения производится с помощью зеркалирования трафика и подключения через SPAN-порт, позволяя не прерывать производственный процесс и никак его не изменять. Все данные об аномалиях и устройствах, приходящие с датчиков, собираются для централизованного учета в ситуационный центр.

«Kaspersky Security Center» (централизованный мониторинг и управление компонентами). Осуществляет наблюдение за всеми процессами и устройствами системы, проверяет коды и потоки на соответствие постоянно обновляемой сигнатурной базы и устраняет угрозы в случае соответствия. Как и «Kaspersky Industrial CyberSecurity for Nodes», центр мониторинга сканирует вирусы не только сигнатурным методом, но и эвристическим и поведенческим, что дает возможность распознать не только известные базе вирусы, но и выявить неизвестные ранее ВПО. «KSCenter» интегрирован с SIEM, HMI, ERP и BI, что существенно упрощает мониторинг непрерывности и контроль технических процессов.

Вся система функционирует в собственной облачной сети «Kaspersky Security Network» (KSN). Преимуществом этого является быстрое реагирование (40 секунд) на появляющиеся угрозы и снижение риска ложных срабатываний. В качестве внутренней корпоративной сети используется «Kaspersky Private Security Network».

В России нормативно закреплены обязанности и требования защиты АСУ ТП как объектов КСИИ Федеральным законом от 21.07.2011 №256-ФЗ «О безопасности объектов топливно-энергетического комплекса», требованием руководящих документов Приказа ФСТЭК России №31. Таким образом, функционирование программных продуктов по защите АСУ ТП ведется в России недавно и получить статистику использования и эффективности внедрений невозможно. «Лабораторией Касперского» KICS выпущен 21 декабря 2015 года, а версия для защиты электроэнергетической отрасли и вовсе только в этом году (20 марта 2017 года). По состоянию на 2016 год «Лаборатория Касперского», как и двумя годами ранее, занимает первую строчку в рейтинге крупнейших ИБ-компаний России[3]. Далее следуют «Softline», «Акронис», «Информзащита» и «Техносерв». Из первых 5 компаний различные проекты для защиты АСУ ТП предоставляют все, однако только «Лаборатория» предоставляет комплексный программно-аппаратный подход с собственной системой и облачным хранилищем. Компания «Softline» предоставляет самостоятельный проект однонаправленной передачи данных «дата-диод», что исключает возможность сетевых атак на сегмент системы, позволяет выгрузить данные в центр. Но исходя из статистики отзывов, «Softline» преимущественно внедряет программы своего партнера – Kaspersky. Компания «Акронис» продает свой проект решения «Acronis Backup Advanced». Физические и виртуальные системы поддаются резервному копированию и в случае

аварийной ситуации быстро восстанавливаются, в том числе и из облачного хранилища «Acronis». Такой проект решения призван обеспечивать бесперебойность работы компьютерных сред, рабочих станций, серверов и др., сохранять один из самых ценных активов предприятия – информацию, но предупреждать и выявлять риски вирусных атак он не способен. «Информзащита» внедряет свои отдельные решения, такие как SIEM, NetSec, MailSec и др. Так же поставляет решения и «Техносерв». О централизации и их управлении нет информации.

Примечательно, что конкурентами Лаборатории Касперского являются поставщики услуг с 12 (компания «УЦСБ», программное решение – «DATAPK») и 16 места (компания «InfoWatch», программное решение – «ASAP»), а третий и вовсе не вошел в топ.

В основном, все представленные на российском рынке системы очень схожи по функционалу. Развитие комплексных подходов к защите техпроцессов обязывает системы защищать не только сетевой доступ, но, в первую очередь, рабочие объекты, обеспечивая непрерывность их процессов. Характерными отличительными чертами «DATAPK» является работа без установки дополнительного ПО на компоненты АСУ ТП, а АПК «Щит» - модульная структура решения, интегрированная с ERP и MES-системами.

Несмотря на то, что «InfoWatch» уже не дочерняя компания «Лаборатории Касперского», и с 2007 года ведет самостоятельную деятельность, продукты «KICS» и «InfoWatch ASAP» практически идентичны в подходе к защите технологических процессов. «ASAP» так же осуществляет антивирусную защиту не только на верхнем уровне в виде защиты SCADA-систем, но и на исполнительном уровне, осуществляя контроль целостности работы ПЛК, контроллеров и прочих узлов. Внедрение комплекса начинается с детального анализа предприятия, его специфики и характеристик, соответствия руководящим документам ФСТЭК, после чего система внедряется в пассивном режиме и набирает статистику, исследуя параметры сети, после чего переключается в активный режим работы. Анализ атак «ASAP» проводит сигнатурным, как и Касперский, и статистическим анализом, не используя эвристическое сканирование и поведенческий анализ для обнаружения аномалий. По уровню интеграции «ASAP» уступает «KICS». Система имеет возможность передачи данных в SIEM, но отдельной компанией, с которой «InfoWatch» объединила свои усилия является только «Модульные Системы Торнадо» по автоматизации объектов промышленного производства «Tornado-N».

Подписанное соглашение с крупнейшим немецким производителем ERP-систем SAP дает «Лаборатории Касперского» существенное преимущество над другими системами. Программы взаимодействуют друг с другом, обеспечивая информационную и экономическую безопасность предприятия. Все собираемые с датчиков, контроллеров и каналов связи данные экспортируются в экономическую систему управления. Помимо прочего, «KICS» интегрирована с крупнейшими поставщиками систем промышленной автоматизации «Schneider Electric», «GE Digital», «Emerson»,

«Siemens». По расследованию компании Positive Technologies именно у этих производителей было найдено наибольшее количество уязвимостей[4]. Интеграция с этими сервисами упрощает внедрение новых технологий и унифицирует требования безопасности для поиска, предупреждения и устранения уязвимостей. Оставаясь лидером на рынке ИБ-услуг в России, «Лаборатория Касперского» предоставляет самый продуманный во всех аспектах продукт, который защищает предприятие изнутри. Конечно, нашему рынку нужно развиваться в этом плане. Защита АСУ ТП становится на повестку дня, так как последствия техногенных катастроф могут отобрать множество человеческих жизней, которые несовместимы с финансовыми потерями. Поэтому в ближайшем будущем, необходимо обеспечить предприятия большим списком альтернативных объединенных систем, а не точечными решениями.

Библиографический список

1. Моев В. Бразды управления. М: Изд. политической литературы. 1977. 92 с.
2. Исследование Лаборатории Касперского // Securelist URL: https://securelist.ru/blog/issledovaniya/27903/pri-apt-atakax-blackenergy-v-ukraine-primenyalsya-celevoj-fishing-s-ispolzovaniem-word-dokumentov/ (дата обращения: 23.05.2017).
3. Крупнейшие компании России в сфере защиты информации 2016 // CNews URL: http://www.cnews.ru/reviews/security2016/review_table/46261d569032470419476901756af8669212f786 (дата обращения: 23.05.2017).
4. Безопасность промышленных систем в цифрах v2.1 // Positive Technologies URL: https://www.ptsecurity.com/upload/corporate/ru-ru/download/SCADA_analytics_russian.pdf (дата обращения: 23.05.2017).
5. Kaspersky Industrial CyberSecurity URL: https://ics.kaspersky.com/ (дата обращения: 23.05.2017).