Рост числа атак на промышленные системы

М.Л. Войтов (Компания «Лаборатория Касперского»)

Отмечено, что число кибератак на промышленные системы растет год от года. Показаны основные пути проникновения вредоносного ПО в производственные автоматизированные системы. Для решения указанных проблем необходимо использовать специализированные решения в сфере промышленной безопасности, которые основаны на реальном опыте работы. Поставщиком таких решений является «Лаборатория Касперского».

Ключевые слова: кибератака, АСУТП, информационные технологии, операционные технологии, уязвимости, промышленная безопасность.

Число кибератак на промышленные системы неуклонно растет. Если недавно эта проблема носила умозрительный характер, сейчас она приобрела реальные очертания [1]. Причем нарушение промышленной безопасности чревато последствиями, выходящими далеко за рамки финансового ущерба и потери деловой репутации. Во многих случаях защита промышленных систем от киберугроз имеет критическое значение с экологической, социальной и макроэкономической точек зрения. Немного цифр: 67% офицеров безопасности определяют уровень угроз для АСУТП как критический или высокий. По сравнению с 2015 г. этот показатель увеличился на 43% [2]. За 2015 г. фискальный год специалисты ICS-CERT отреагировали в США на 295 киберинцидентов, связанных с атаками на критическую инфраструктуру. Этот показатель также оказался выше, чем годом ранее, на 20% [3]. Таким образом, сегодня на передний план выходит риск кибератак. Особенно велика их опасность для организаций, эксплуатирующих промышленные системы или объекты критически важной инфраструктуры.

Операционные и информационные технологии: в чем разница

Автоматизированные системы управления технологическими процессами (АСУТП) — собирательный термин, описывающий автоматизированные системы, которые контролируют производственный процесс. Термин АСУТП относится к широкому спектру компьютеров, специфических устройств управления и сетевых архитектур, используемых для контроля промышленных процессов в самых разных отраслях промышленности. АСУТП обычно включает SCADA (Supervisory Control And Data Acquisition — диспетчерское управление и сбор данных), РСУ (распределенные системы управления) и ПЛК (программируемые логические контроллеры).

В терминах организационной системы все это можно разбить на две категории:

- информационные технологии (IT) — системы, необходимые для достижения бизнес-целей;
- операционные технологии (OT) — системы, необходимые для целей промышленной автоматизации.

Многие стратегии обеспечения IT-безопасности, прежде всего, ориентированы на защиту данных и базируются на модели Конфиденциальность-Целостность-Доступность. В операционных технологиях самое важное — непрерывность, поэтому защищаются не данные, а сам процесс производства. Другими словами, в промышленных сетях порядок приоритетов безопасности обратный: Доступность-Целостность-Конфиденциальность. Это определяет специфические потребности в области кибербезопасности — высочайший уровень безопасности для промышленных предприятий бесполезен, если он подвергает риску непрерывность (или целостность) процессов.

Угрозы и риски

Несмотря на то, что угрозы для АСУТП стали широко известными, многие модели обеспечения IT-безопасности основаны на устаревших предположениях, что для защиты промышленного предприятия достаточно физической изоляции систем (через так называемые «воздушные зазоры») и концепции security by obscurity (безопасность через неясность). Однако в эпоху четвертой промышленной революции большинство промышленных сетей так или иначе доступны через Internet [4].

Масштабное исследование «Лаборатории Касперского», которое опиралось на данные облачной сети Kaspersky Security Network, показало, что большинство промышленных рабочих станций подвержены тем же угрозам, что и бизнес-системы (IT), включая троянцы, компьютерные черви, потенциально нежелательные и опасные программы и эксплойты, которые используют уязвимости ОС Windows.

Червь Kido (известный также как Conficker) не предназначался специально для атак на промышленные сети, однако его неоднократно там обнаруживали. Червь Kido может полностью перегрузить сети, вызвав остановку критически важных процессов. Привычные методы обеспечения промышленной кибербезопасности не могут должным образом защитить от таких угроз.

Растет число угроз для АСУТП со стороны программ-вымогателей. С 2015 по 2016 год эта категория угроз стала гораздо масштабнее и разнообразнее. При этом программы-вымогатели, атакующие АСУТП, имеют свою специфику: вредоносное ПО нацелено не на шифрование файлов, а на прерывание технологического процесса или блокирование доступа к важнейшим активам.

Помимо угроз общего характера, промышленный сектор сталкивается с целенаправленными атаками и специализи-

рованным вредоносным ПО. Stuxnet, Citadel, Energetic Bear/Havex, Miancha, BlackEnergy, Irongate, PLC Blaster — этот список постоянно пополняется. И, как показали атаки Stuxnet и Black Energy, одного зараженного USB-накопителя или фишингового письма достаточно, чтобы злоумышленники преодолели «воздушный зазор» и проникли в изолированную сеть. Многие специализированные атаки разворачиваются и на уровне корпоративной сети, и на уровне АСУТП. Примером может служить атака BlackEnergy на украинские электростанции, которая в декабре 2015 г. привела к многочасовому отключению электричества. Для реализации этой атаки злоумышленники использовали несколько векторов. Сначала они получили доступ к учетным данным SCADA-системы с помощью таргетированной фишинговой рассылки. Обладая этими данными доступа, они начали выключать электрораспределительную сеть. После этого они внедрили вредоносный модуль KillDisk, который уничтожил или перезаписал важные системные файлы в промышленной сети. Параллельно с этим call-центр поставщика электричества подвергся DDoS-атаке, и это помешало потребителям электроэнергии вовремя сообщить об отключениях.

Помимо вредоносного ПО и целевых атак, промышленные организации сталкиваются с целым рядом угроз и рисков, направленных на людей, процессы и технологии. «Лаборатория Касперского» разработала комплексный набор технологий, решений и сервисов, чтобы помочь своим клиентам предотвратить риски, включая следующие:

- ошибки операторов или подрядчиков (третьих сторон), работающих со SCADA-системами;
- действия сотрудников (намеренные и случайные);
- несоблюдение требований регулирующих органов;
- неосведомленность о том, как расследовать инциденты и собирать о них достоверные данные;
- отсутствие отчетности по инцидентам.

Необходимость в специализированных решениях промышленной кибербезопасности

Только те поставщики защитных решений безопасности, которые понимают различия между промышленными системами и стандартными сетями коммерческих предприятий, могут предложить продукты, отвечающие уникальным потребностям систем ICS и операторов производственных инфраструктур. По мнению Forrester [5], промышленные предприятия, выбирающие поставщика решений безопасности, должны «ориентироваться на опыт специализированной работы в сфере промышленности». Аналитическая компания говорит о «Лаборатории Касперского» как об одном из немногих производителей, предлагающих специализированные решения в сфере промышленной безопасности, которые основаны на реальном опыте работы.

«Лаборатория Касперского» — признанный лидер в обеспечении кибербезопасности и защите промышленных систем. Компания постоянно разрабатывает решения, которые успешно противостоят постоянно развивающимся угрозам для критически важных инфраструктур. Компания также помогает промышленным предприятиям, регулирующим органам и государственным учреждениям прогнозировать изменения в структуре угроз и противостоять атакам.

«Лаборатория Касперского» приобрела статус доверенного партнера и поставщика решений безопасности для ведущих промышленных предприятий, которые много лет пользуются ее защитой от вредоносного ПО. Кроме того, компания сотрудничает с крупнейшими поставщиками решений для промышленной автоматизации (Emerson, Rockwell Automation, Siemens и др.), чтобы обеспечить взаимную совместимость, а также создать специализированные процедуры и платформы сотрудничества, которые позволят защитить промышленные среды от существующих и возникающих киберугроз (в том числе комплексных целенаправленных атак). «Лаборатория Касперского» развивает свой набор специализированных решений, удовлетворяющих специфические потребности промышленного сектора экономики. Эти решения обеспечивают защиту от киберугроз на всех уровнях промышленных систем (в том числе серверов SCADA, человеко-машинного интерфейса, рабочих станций, ПЛК и сетевых соединений), не влияя на непрерывность работы и стабильность технологического процесса.

Решение для защиты критической инфраструктуры Kaspersky Industrial CyberSecurity соответствует стратегии многоуровневой защиты, созданной «Лабораторией Касперского», и использует сочетание разных методов защиты. Помимо технологий и сервисов, защищающих систему на всех этапах, Kaspersky Industrial CyberSecurity обеспечивает безопасность за счет целого ряда средств, включая контроль целостности, предотвращение вторжений, а также оценку уязвимостей и защищенности от вредоносного ПО. Набор экспертных сервисов, предлагаемый «Лабораторией Касперского», составляет важную часть решения Kaspersky Industrial CyberSecurity. В него входят обучение сотрудников, анализ защищенности промышленных сетей, интеграция решения, подготовка предложений по улучшению системы безопасности и расследование инцидентов безопасности.

Список литературы

1. PwC: Global State of Information Security («Глобальное состояние информационной безопасности»), 2015. http://pwc.to/GSISS15.
2. SANS 2016 State of ICS Security Survey (Исследование о состоянии безопасности АСУТП). http://ics.sans.org/ics-library/survey/2016.
3. ICS-CERT Monitor, November-December, 2015. https://ics-cert.us-cert.gov/monitors/ICS-MM201512.
4. *Andreeva O., Gordeychik S., Gritsai G., Kochetova O., Potseluevskaya E., Sidorov S.I., Timorin A.A.* Industrial control systems and their online availability (АСУТП и их доступность через Internet). «Лаборатория Касперского». 2016. https://kasperskycontenthub.com.
5. Rick Holland, Stephanie Balaouras, Katherine Williamson. S&R Pros Can No Longer Ignore Threats to Critical Infrastructure. Forrester Research Inc. 2014.

Войтов Матвей Леонидович *– руководитель отдела продуктового маркетинга департамента защиты критических инфраструктур «Лаборатория Касперского».*
Контактный телефон (495) 797-87-00.
Http:// kaspersky.com