Матвей Войтов

КРИТИЧЕСКАЯ ИНФРАСТРУКТУРА В КОНТЕКСТЕ КИБЕРБЕЗОПАСНОСТИ

Вот уже несколько лет тема защиты критической инфраструктуры является крайне актуальной среди производителей защитных систем в сфере информационной безопасности — повышение спроса из-за участившихся кибератак на критически важные объекты рождает рост предложения, в данном случае — рынка продукции, защищающей от таких нападений[1]. Но в большинстве случаев под одной вывеской кроется множество различных направлений: сертифицированные решения для государственного сектора, использование средств информационной безопасности (ИБ) на промышленных объектах, защита национального сегмента интернета и многое другое.

В этот раз мы постараемся определить, что же, с точки зрения *Лаборатории Касперского,* представляет собой критическая инфраструктура в контексте кибербезопасности и от чего, а, главное, как ее надо защищать. Критичность объекта и, соответственно, его инфраструктуры во всем мире определяется на государственном уровне, критические для существования и функционирования государств предприятия и отрасли фиксируются в специальных перечнях. Естественно, государствообразующими являются самые различные секторы и отрасли — от финансовой и банковской системы до систем управления водо- и энергоснабжением.

Если говорить об отраслях, наиболее часто относимых к критической инфраструктуре и связанных не только с физической, но и с кибербезопасностью, то на основании усредненного мирового опыта можно составить следующий перечень, в определенной степени совпадающий у большинства государств:

- электроэнергетика (атомная энергетика часто выделяется отдельно);
- управление природными ресурсами (в частности, нефтегазовый сектор);
- управление водными ресурсами (включая водоочистку и управление сточными водами);
- транспорт;
- пищевая промышленность;

- здравоохранение;
- телекоммуникации;
- финансовая и банковская системы;
- органы государственной власти.

Данная выборка сделана на основе находящихся в открытом доступе перечней и трактовок критической инфраструктуры следующими организациями:

- министерство внутренней безопасности США[2];
- центр защиты национальной инфраструктуры Великобритании[3];
- федеральное управление по информационной безопасности Германии[4];
- правительство Австралии[5].

Естественно, каждая страна специфически трактует понятие критической инфраструктуры. Например, министерство внутренней безопасности США предоставляет более детальный перечень, включая в него в том числе военно-промышленный комплекс. Отдельного внимания заслуживают организации, открыто занимающиеся общими вопросами защиты критической инфраструктуры — от министерств и правительств до специализированных ведомств. Помимо государственных программ развиваются и международные инициативы. В качестве примера можно привести единую европейскую программу по защите критической инфраструктуры[6].

Если говорить об опыте Российской Федерации, то на данный момент единого публичного перечня элементов не существует, тем не менее имеется существенная нормативно-правовая база, состоящая из различных законов, постановлений и указов, выпущенных Правительством РФ, Советом Безопасности, ФСБ и Федеральной службой по техническому и экспортному контролю (ФСТЭК), в которых даются определения таким понятиям, как *критически важный объект* и *ключевая система информационной структуры*. Основополагающими документами в этой сфере являются *Система признаков критически важных объектов и критериев отнесения функционирующих в их составе информационно-телекоммуникационных систем к числу защищаемых от деструктивных информационных воздействий* и *Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации*[7].

Имея представление о всем многообразии элементов критической инфраструктуры, невозможно говорить о едином подходе к кибербезопасности, так называемой *серебряной пуле*, для каждой из отраслей. Тем не менее, чтобы не усложнять задачу, можно классифицировать элементы критической инфраструктуры исходя из типологии информационных систем, лежащих в основе той или иной отрасли и существующих на сегодняшний день средств их защиты.

Если функционирование некоторой части отраслей, к примеру финансовой сферы или органов госуправления, основано на *классических* информационных систе-

мах, основной целью которых является управление информацией, то другие — энергетика, транспорт, добыча природных ресурсов и т. д. — работают на основе специализированных промышленных систем, созданных для управления технологическим процессом. В подавляющем большинстве случаев инциденты, которые могут произойти на подобных промышленных объектах, потенциально могут привести к гораздо худшим последствиям, чем потеря информации или денег: к угрозе жизни людей, загрязнению окружающей среды и прочим действительно опасным результатам.

Поэтому безопасность таких объектов, в том числе кибербезопасность их инфраструктур, во множестве стран регламентируется особо. Например, в Российской Федерации требования к кибербезопасности промышленных критически важных объектов определяются приказом ФСТЭК № 31[8] от 14 марта 2014 г. Кроме того, предпринимаются усилия по развитию отраслевых стандартов безопасности, в частности давно ведется разговор о внесении детализирующих поправок в ст. 11 ФЗ 256 от 21 июля 2011 г. *О безопасности объектов топливно-энергетического комплекса*[9]. Кстати, наиболее часто атакам подвергается именно энергетическая сфера, в которой стоит отдельно выделить нефтегазовый комплекс и транспортный сектор.

Естественно, защите критических отраслей, которые функционируют на базе широко распространенных информационных систем, например телекоммуникациям или здравоохранению, также должно уделяться значительное внимание, но, с нашей точки зрения, современные средства обеспечения информационной безопасности при грамотном их использовании способны значительно снизить риски, исходящие от самых различных угроз: начиная от обычных вредоносных программ и заканчивая сложными таргетированными атаками. В промышленных информационных системах эти методы просто неприменимы в силу множества причин, о которых мы расскажем ниже.

Проигнорировать же защиту вообще и положиться на распространенную в промышленных сетях физическую изоляцию значит рано или поздно оказаться под ударом. Как показал опыт последних лет, физическая изоляция не способна остановить не только целевые атаки (последний пример — атаки на энергетические объекты и критические сектора Украины с помощью программы BlackEnergy[10]) и промышленное кибероружие (весь мир до сих пор вспоминает Stuxnet[11], а совсем недавно был обнаружен его преемник — Irongate[12]), но и стандартное вредоносное ПО, которое регулярно обнаруживают на изолированных объектах. Векторов атаки достаточно — начиная от инженера, принесшего в изолированную сеть зараженное устройство, и заканчивая подрядчиком, осуществляющим работы на объекте. Ситуация усугубляется тем, что атаки на промышленные объекты теперь не только прерогатива кибертеррористов и государственных спецслужб, но и *обычных* хакеров[13]. Можно прогнозировать, что с широким распространением промышленного интернета вещей киберпреступники активизируются еще сильнее.

Помимо заражения вредоносным ПО и целевых атак промышленные организации сталкиваются с рядом других киберугроз и рисков, направленных против всех элементов инфраструктуры: людей, процессов и технологий. Вот лишь основные риски, которые могут привести к серьезным инцидентам:

- ошибки и сбои программно-аппаратных компонентов промышленных систем;
- случайные или намеренные ошибочные действия сотрудников или подрядчиков;
- мошеннические операции в автоматизированной системе управления технологическим процессом (АСУ ТП);
- неосведомленность о правилах расследования инцидентов, особенностях сбора достоверных данных о них.

Именно поэтому защита по-настоящему критической инфраструктуры требует специального подхода и понимания. В чем же должна заключаться специфика промышленной киберзащиты? АСУ ТП требуют совершенно иного подхода к обеспечению информационной безопасности (а точнее, кибербезопасности, так как речь идет не только о защите информации) по сравнению с классической *офисной* ИТ-инфраструктурой. В корпоративных средах основное внимание уделяется сохранности конфиденциальных данных, а бесперебойная работа не настолько важна, как для АСУ ТП, где цена минуты простоя, как и любой другой ошибки, очень велика. Поэтому в обеспечении безопасности технологических процессов действует противоположный подход, при котором основной задачей является поддержание их непрерывности и оперативное устранение любых сбоев. Не говоря уже о том, что промышленная инфраструктура содержит в себе крайне специализированные элементы, не встречающиеся в корпоративной сети: системы диспетчерского управления и сбора данных, человеко-машинные интерфейсы, программируемые логические контроллеры и многое другое, что просто не поддерживается традиционными средствами обеспечения информационной безопасности. Циклы обновления программного и аппаратного обеспечения в промышленных средах гораздо более протяженные — очень часто на промышленных объектах встречается ПО, которое уже давно не поддерживается и содержит множество уязвимостей. Такие условия также не позволяют традиционным средствам обеспечения информационной безопасности эффективно работать. Кроме того, инструменты промышленной кибербезопасности должны отвечать требованиям государственных и отраслевых регуляторов и проходить сертификацию у производителей АСУ ТП.

Дополнительной сложностью является размытость зоны ответственности за обеспечение промышленной кибербезопасности: очень часто промышленный уровень является доменом инженеров АСУ ТП, которые относятся к средствам обеспечения информационной безопасности как к помехе, способной негативно повлиять на технологический процесс.

При этом инструментов обеспечения ИБ, созданных специально для защиты промышленных объектов, до сих пор крайне мало. Этот рынок активно развивается[14], и в ближайшее время таких продуктов станет больше, однако при этом крайне важно, чтобы у производителей таких средств было глубокое понимание специфики АСУ ТП и угроз безопасности этих сред. К примеру, нашей компании на создание специализированного решения в этой области потребовалось 5 лет — после обнаружения Stuxnet в 2010 г. не осталось сомнений в том, что *традиционная* защита более не эффективна.

Важной особенностью обеспечения промышленной кибербезопасности является то, что каждый проект такого рода уникален — так же, как и каждая промышленная инфраструктура, в которую просто невозможно установить некие стандартизированные продукты. Подбор оптимальной конфигурации защитных технологий и набора сервисов осуществляется после полного обследования текущей системы безопасности промышленного объекта, а имплементация выбранных мер происходит только в специально отведенное технологическое окно, чтобы не повлиять на процесс работы системы.

Несмотря на трудоемкость подобного проекта, результатом правильной интеграции специализированного решения будет действующая концепция многоуровневой защиты: через сочетание различных методов превентивной защиты, мониторинга и прочих сервисов оператор критической инфраструктуры получает средство, позволяющее реагировать на киберинциденты на всех возможных стадиях — от прогнозирования потенциальных атак и непосредственной защиты от них до обнаружения комплексных угроз и снижения ущерба. Уже можно наблюдать, как операторы постепенно осознают, что использовать этот непростой, но действенный подход к защите промышленных объектов необходимо, не дожидаясь, пока они окажутся в сводках новостей.

Примечания

1 Critical Infrastructure Protection Market Expected to Reach 144.82 Billion USD by 2021. Market Watch, 13 June 2016, http://www.marketwatch.com/story/critical-infrastructure-protection-market-expected-to-reach-14482-billion-usd-by-2021-2016-06-13-92033051 (последнее посещение: 21.06.2016).

2 Critical Infrastructure Sectors. U.S. Department of Homeland Security, https://www.dhs.gov/critical-infrastructure-sectors (последнее посещение: 21.06.2016).

3 The national infrastructure. Centre for the Protection of National Infrastructure, http://www.cpni.gov.uk/about/cni/(последнее посещение: 21.06.2016).

4 Critical Infrastructures. Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance, http://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html (последнее посещение: 21.06.2016).

5 Trusted Information Sharing Network for critical infrastructure resilience, http://www.tisn.gov.au/Pages/default.aspx (последнее посещение: 21.06.2016).

6 Communication from the Commission on a European Programme for Critical Infrastructure Protection. Commission of the European Communities, Brussels, 12 December 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786: FIN: EN: PDF (последнее посещение: 21.06.2016).

7 Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. Совет безопасности Российской Федерации, http://www.scrf.gov.ru/documents/6/113.html (последнее посещение: 21.06.2016).

8 Приказ от 14 марта 2014 г. № 31 *Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды*. Федеральная служба по техническому и экспортному контролю, http://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 (последнее посещение: 21.06.2016).

9 Федеральный закон от 21 июля 2011 г. № 256-ФЗ *О безопасности объектов топливно-энергетического комплекса*. *Российская Газета*. 2011, 26 июля, http://rg.ru/2011/07/26/tek-dok.html (последнее посещение: 21.06.2016).

10 Kaspersky Lab's Global Research & Analysis Team. При APT-атаках BlackEnergy на Украине применялся целевой фишинг с Word-документами. 28 января 2016, https://securelist.ru/blog/issledovaniya/27903/pri-apt-atakax-blackenergy-v-ukraine-primenyalsya-celevoj-fishing-s-ispolzovaniem-word-dokumentov/(последнее посещение: 21.06.2016).

11 Zero Days.The Internet Movie Database, http://www.imdb.com/title/tt5446858 (последнее посещение: 21.06.2016).

12 Spring Tom. Зловред, заточенный под АСУ ТП, украл идеи у Stuxnet. Threatpost, https://threatpost.ru/irongate-ics-malware-steals-from-stuxnet-playbook/16544 (последнее посещение: 21.06.2016).

13 Панасенко Александр. Хакеры нечаянно атаковали водоочистные сооружения. Anti-Malware, 24 марта 2016, https://www.anti-malware.ru/news/2016-03-24/18450 (последнее посещение: 21.06.2016).

14 Perkins Earl, Alaybeyi Saniye Burcu. Market Guide for Operational Technology Security. Gartner, 23 May 2016, https://www.gartner.com/doc/3327318/market-guide-operational-technology-security (последнее посещение: 21.06.2016).