«Интернет вещей превратился в смертельную угрозу»

Алексей Лукацкий, бизнес-консультант по безопасности компании Cisco

20 сентября 2016 года была зафиксирована одна из крупнейших в истории распределенная DDoS-атака. Мощность воздействия на сайт журналиста Брайна Кребса составила 665 Гбит/сек и 143 Mpps, а на интернет-провайдера OVH — до 1 Тбит/сек и 93 Mpps. И в том, и в другом случае в атаке участвовало множество интернет-устройств: IP-камеры, видеорегистраторы, маршрутизаторы и т.д. В случае OVH их число достигло 150 тысяч.

Раньше подобное тоже случалось, но в атаках участвовали обычные пользовательские ПК, на которые злоумышленники, взломав их, устанавливали вредоносный код. Сбылось то, о чем специалисты по информационной безопасности (ИБ) предупреждали уже много лет назад: Интернет вещей стал их колоссальной головной болью. Со своей стороны, разработчики Интернета вещей на стенания «безопасников» не обращают внимания до сих пор, говоря, что те перестраховываются, пытаясь за счет своей «истерии» выбить деньги.

Другой пример — из области медицинского IoT. Мало кто слышал о смерти при загадочных обстоятельствах австралийского исследователя Барнаби Джека. Он изучал работу инсулиновых помп и кардиостимуляторов с точки зрения безопасности. Оказалось, что очень многие устройства, выпускаемые вполне серьезными и уважаемыми производителями, обладают очень неприятными свойствами для их обладателей. Ими можно управлять удаленно: они не только передают телеметрию о состоянии здоровья человека, но и принимают сигнал извне. Например, кардиостимулятору, представляющему собой, по сути, интернет-дефибриллятор, можно дистанционно дать команду на выпуск разряда в 800 вольт, что приведет к остановке сердца, а инсулиновая помпа может впрыснуть весь объем лекарства вместо небольшой его дозы, за чем последует анафилактический шок и смерть.

Смертельные угрозы — в промышленном IoT

Если обратиться к более приземленной области промышленного Интернета вещей, то можно обнаружить не менее серьезные угрозы. Когда они появились? Нашумевший случай произошел в 2009-2010 годах. Речь идет об атаке на атомные объекты в Иране, когда оборудование завода по обогащению урана в Натанзе было заражено вредоносным кодом. До сих пор официально не названные спецслужбы (хотя чаще всего упоминаются структуры Израиля и США) заразили полностью замкнутый объект, что повлияло на работу центрифуг. Итог — выработка обогащенного урана снизилась в два раза по сравнению с периодом до заражения. Это один из первых ставших достоянием широкой общественности пример влияния кибератаки на физический мир, хотя подобное случалось и прежде: в пищевой промышленности, медицине, транспорте. Уже в 90-годы фиксировались кибератаки на промышленные объекты, приводившие в том числе к человеческим жертвам. Считается, что абсолютно замкнутые от проникновения извне объекты — АЭС, но компьютерным атакам с большим материальным ущербом подвергались и они.

Цели таких атак различны: подготовка к возможным кибервойнам, промышленный шпионаж, конкурентная война.

Часто говорят, что системы управления ГЭС, электростанций, ЖКХ и транспорта по силам взломать только государствам в рамках спецопераций национального уровня. Но это не так. В частности, выяснилось, что за взломами систем различных энергетических компаний в конце первой декады 2000-х стоят компании вполне конкретной азиатской страны. Перед обсуждавшимися поглощениями активов в энергетике и нефтяной отрасли ими взламывались компьютерные сети, добывалась информация о данных активах, в том числе финансовая, которая затем использовалась на переговорах для выторговывания лучших условий при сделках. Промышленный шпионаж такого рода — уровень далеко не спецслужб, а отдельных компаний. По статистике американского центра реагирования на инциденты в промышленных системах ICS-CERT, в 2015 году

в США число подтвержденных инцидентов выросло на 20% — до 295. МЧС РФ в прогнозе чрезвычайной обстановки на 2016 год вполне серьезно рассматривало кибертерроризм как серьезную угрозу промышленным системам автоматизации и управления в ЖКХ, энергетике, транспорте.

Тем, кто говорит: «Внедрим классную штуку, работающую через «облако», и будет нам счастье», я могу ответить: «Счастья не будет, по крайней мере, в обозримом будущем». Перечислю несколько примеров за последний год, подтверждающих этот тезис: атака на АЭС в Японии в 2015 году, о которой стало известно только недавно; пожар на солнечной электростанции в США Ivanpah Solar Electric System в результате неправильного позиционирования зеркал, вызванного, скорее всего, киберпричинами; столкновение поездов в Казахстане и Баварии; атака на электроэнергетическую систему Украины, в которой впоследствии обвинили РФ; атака на киевский аэропорт «Борисполь». Продолжу список последними инцидентами в критической инфраструктуре: обвинение иранцев в DDoS-атаке и взломе инфосистемы плотины около Нью-Йорка; демонстрации взломов автомобилей, ставшие регулярными; атака на систему электроэнергетики Израиля; атака Dust Storm на японские объекты ТЭК; создание первого червя для PLC Siemens, распространяемого без ПК; атака на ЖКХ-компанию Lansing Board of Water & Light в США; атака на CMS управления данными о местонахождении кораблей и их грузе (результат — захват пиратами контейнеров с бриллиантами); атака на водоочистную систему Kemuri Water Company. Когда взламывают систему водоочистки или канализации, кажется, ничего страшного не происходит. Но вот еще один пример: в начале 2016 года бывший сотрудник взломал инженерную систему одного из отелей Hilton в Австралии (?), дистанционно перекрыв задвижку. В результате содержимое канализации начало выливаться на территорию пятизвездочного отеля. Говорят, запах не выветрился до сих пор.

Причины и последствия

Попробую классифицировать технологические причины, которые приводят к описанным выше инцидентам. Многие специалисты по автоматизированным системам управления (АСУ) с одобрением вспоминают изолированные от внешнего мира промышленные системы, проприетарные протоколы, лозунг «никакого Интернета», закрытые разработки, противопоставляемые открытым стандартам. Но эта эпоха в прошлом. Сегодня мы двигаемся в сторону «облачных» систем. К сожалению, из «облака» предлагается управлять тем, что не было защищено должным образом и на предшествующих этапах развития АСУ.

Системы управления АЭС в США подключены к Интернету, в РФ это запрещено. И на многих таких предприятиях с изолированными от Интернета АСУ специалисты убеждены, что они в безопасности: они мыслят категориями даже не второй и не третьей промышленной революции, а первой. Но и в их системах тоже есть уязвимости, при этом специалисты по ИБ продолжают ничего не делать для их устранения, оставаясь в ложной уверенности, что им ничего не угрожает, «пока гром не грянет».

Проблемой является и тот факт, что все объекты промышленного Интернета вещей очень разные. Одно дело — защита трубопровода со всеми его автоматизированными задвижками и компрессорами на протяжении тысяч километров, где даже и Интернета никакого нет, и совсем другое — защита движущегося автомобиля, передающего данные со своего тахографа. Если традиционная корпоративная сеть — это несколько сотен узлов, то система промышленной автоматизации — несколько десятков тысяч датчиков, каждый из которых может одномоментно отправить небольшой пакет данных о своей работоспособности. Ни одна система защиты не справляется с таким потоком данных — она просто выходит из строя.

Еще одна проблема — различия в стандартах. Коль скоро объекты очень разные, то и стандарты тоже. Современные стандарты в сфере ИБ, промышленных АСУ — это тысячи страниц, как правило, англоязычных. Для разных объектов промышленного Интернета надо прочитывать множество разных документов — их тоже тысячи. Результат — многие разработчики промышленных АСУ не читают всю эту документацию. Более того, новые стандарты выходят регулярно. Вот лишь краткий перечень недавно выпущенных документов: рекомендации FDA по ИБ медицинских устройств, рекомендации по ИБ систем управления водным транспортом, рекомендации GSMA для разработчиков IoT, новый приказ ФСТЭК по межсетевым экранам (тип «Д» — промышленные МСЭ), базовый уровень ИБ на KBO (Германия), отчеты ENISA по Smart Grid, по CIIP и по транспорту, рекомендации BSI (Германия) по безопасности OPC UA, проект приказа ФСТЭК по антивирусам.

На какие стандарты в области ИБ стоит обратить внимание в первую очередь? Если вы планируете выход на зарубежный рынок, в частности на американский, невозможно игнорировать NIST Cybersecurity Framework, де-факто используемый в США в качестве отраслевых стандартов ИБ. Это набор рекомендаций по обеспечению безопасности систем промышленной автоматизации, разработанный Американским институтом по стандартизации. Этот документ вобрал в себя лучший мировой опыт в этой области: азиатские, европейские, американские стандарты ИБ. Документ был опубликован в 2014 году, сейчас он вышел на новую стадию обновления.

Если же для вас российский рынок является первоочередным, то нельзя забывать, что система промышленной автоматизации в РФ с точки зрения ИБ регулируется очень серьезно. Один из самых важных документов здесь — приказ ФСТЭК №31 по защите АСУ ТП («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»). Все новые и модернизируемые системы должны создаваться по этому приказу, а не по документам ФСТЭК для ключевых систем информационной инфраструктуры (КСИИ) 2007 года и последующих годов. Приказ ФСТЭК очень сильно похож на NIST Cybersecurity Framework: российское ведомство ориентируется на международный опыт, так что российские нормативные документы вполне адекватны с точки зрения рекомендаций, что делать для защиты промышленных систем. Основной упор — на доступность и бесперебойность функционирования технологического процесса, поэтому в документе нет жестких требований по наличию тех или иных защитных мероприятий.

К проблемам с регулированием ИБ в сфере Интернета вещей в РФ я бы отнес то обстоятельство, что у нас до сих пор нет единого регулятора в этой области. У нас их много: Ростехнадзор, Атомнадзор, МЧС, ФСБ, ФСТЭК, Минэнерго, Совет безопасности

Поскольку геополитическая обстановка не способствует использованию зарубежных решений ИБ, в РФ активно развивается соответствующий рынок. Перечислю основные отечественные решения, всего их более десятка: Kaspersky Industrial CyberSecurity, Positive Industrial Security Incident Manager, Infowatch ASAP, DATAPK, InfoDiode, Symantron, ViPNet, Secure Diode, СТРОМ и другие. Теперь можно ожидать внесения первых решений по ИБ АСУ в реестр отечественного ПО. ■