С чего начинается информационная безопасность АСУ ТП

Порой сложно предположить, что сбой в работе ИТ-систем или автоматизированных систем управления технологическими процессами может нанести значительный вред бизнесу/производству. В случае подобного происшествия сотрудники предприятия будут и дальше работать, выполняя свои обязанности, а системы релейной защиты предотвратят наступление чрезвычайной ситуации. Но временная остановка производства все же произойдет. Например, в случае сбоя в системе управления складом, скорее всего, остановятся или сильно затормозятся отгрузки. Товар задержится на складах, а поступающая продукция "подвиснет". Даже если систему удастся восстановить за час, то на корректировку логистики и категоризацию поступившего товара понадобится дополнительное время. Не удастся избежать и штрафов и репутационных рисков.

В отношении рисков, связанных с нарушением информационной безопасности автоматизированной системы управления складом, уместно будет привести историю, произошедшую с одной морской транспортной компанией в 2016 году. Злоумышленники проникли в систему управления складом этой компании и брали из нее информацию о грузах, транспорте и логистике, а потом продавали эти данные морским пиратам. Те в свою очередь анализировали данную информацию и прицельно выбирали свою жертву: "в нужное время в нужном месте" встречали транспортный корабль и из тысячи контейнеров грабили те, которые им были интересны. Это экономило время разбоя и повышало его эффективность. В другом случае злоумышленники, проникнув в систему управления логистикой транспортной компании и получая данные, кто, где и когда будет принимать груз, подделывали документы, после чего приезжали в место доставки и забирали товар прямо с корабля.

Рис. 1. Эволюция кибератак

Эти случаи не единственные. Вот еще примеры из других областей.

В 2012 году в Саудовской Аравии на компьютеры сотрудников нефтяной компании пришло сообщение с вирусом. В результате тридцать пять тысяч компьютеров были выведены из строя (стерта память). Это привело к остановке отгрузки нефти – 17 дней простоя. И только на восемнадцатый день компания начала отгрузки снова, но бесплатно, так как система работы с заказами и партнерами все еще не была восстановлена, но дальнейший простой привел бы к окончательной потере клиентов.

В конце 2015 года сообщение с вирусом получили сотрудники украинской электросетевой компании. И вновь большинство компьютеров предприятия оказались выведены из строя. Дополнительно были изменены прошивки рабочих станций и сенсорных панелей управления, параллельно велась DDoS-атака на call-центр. Все это привело к потере технологического управления и выходу из строя управляющего оборудования на самом объекте. Как итог, пропало напряжение на семи подстанциях 110 кВ, двадцати трех подстанциях 35 кВ и на 6 часов были обесточены 5 регионов.

Данные примеры могли бы остаться просто частными происшествиями, если бы не тот факт, что атаки все чаще переходят из частного формата в массовый и шаблонный. Набор инструментариев, используя который можно легко остановить производство в различных сферах, достаточно широк. При этом важно учитывать, что помимо инцидентов со сбоями производства злоумышленники ведут активную работу по сбору информации. В "черной" части Интернета она также продается. О том, как и кто ею воспользуется, остается только гадать. Сегодня уже можно говорить о тысячах зараженных устройств на производственных объектах и миллионах компьютеров в корпоративной сети, с помощью которых злоумышленники крадут свою "копеечку". Наглядная картина, сформированная благодаря исследованиям компании "Лаборатория Касперского", представлена на рис. 1 и 2.

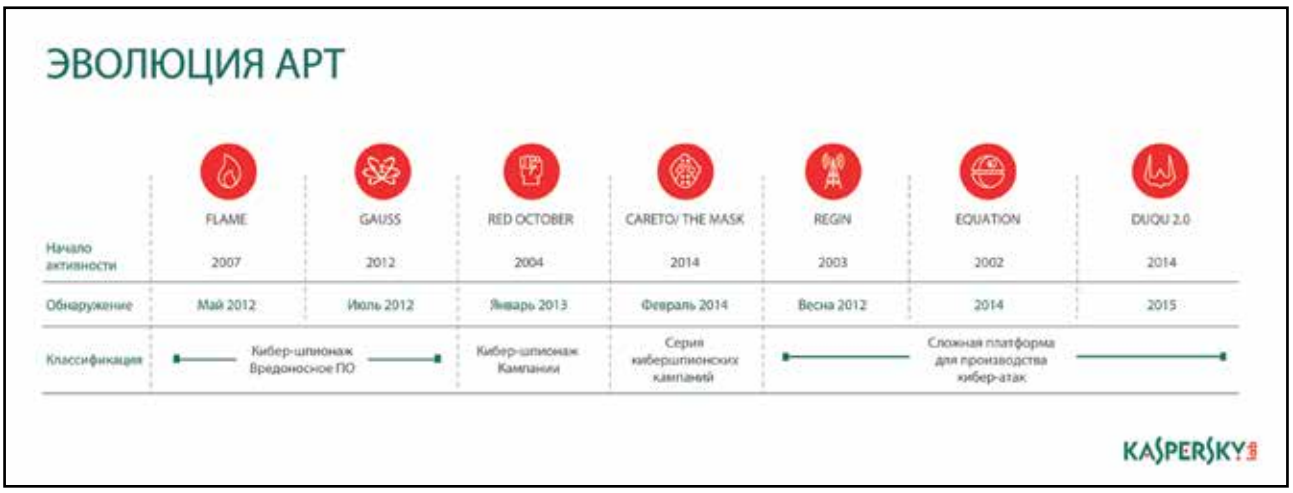

Рис. 2. Эволюция таргетированных атак

Согласно данным ICS-CERT, одной из наиболее популярных организаций, отслеживающих и консолидирующих знания по подобного рода инцидентам, в 2014 году исключительно компьютерных инцидентов с производственными компаниями Европы и Америки было зарегистрировано 245, а в 2015 уже 295, что больше почти на 20%. При этом увеличился и ущерб. 18% данных инцидентов вызывали простой более суток, а это более 50 предприятий за год. Сегодня только с помощью мышки и клавиатуры киберпреступники вагонами воруют различную продукцию. Борются ли с этим компании? Чаще всего нет. Подобные потери относят к действию человеческого фактора или неизбежным потерям. И мало кто разбирается с причиной, а уж тем более придает данные инциденты публичной огласке. Проще уволить оператора, на рабочем месте которого произошла утечка, чем озаботиться вопросами компьютерной безопасности. Хотя, когда потери становятся уж слишком значительными, приходится выбирать – разобраться в причине или прекратить бизнес.

Когда подобный крупный инцидент происходит на предприятии, владельцы бизнеса в первую очередь обсуждают случившееся с представителями службы информационной безопасности. Но так как эксплуатация информационных систем и автоматизированных систем управления технологическими процессами относится к службам информационных технологий и/или АСУ ТП, то постепенно в ситуацию вовлекаются все. Почти всегда после данных инцидентов происходят кадровые изменения во всех причастных службах предприятия. Но даже если все ограничивается выговором – приятного мало.

Чтобы неприятных моментов было меньше, лучше заблаговременно оценивать угрозы информационной безопасности и применять меры по нивелированию данных угроз в проектируемых и новых системах на производстве. А в отношении существующих АСУ ТП следует при содействии службы информационной безопасности привести инфраструктуру компании в порядок.

Со стороны государства данной проблематике уделяется внимание с 2007 года. Разработаны тематические документы: регламенты, приказы, постановления правительства и даже проекты законов. Существует, например, приказ ФСТЭК №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". Этот приказ после вступления в силу соответствующих законов по защите информации в АСУ ТП будет являться одним из ключевых нормативных документов в области борьбы с инцидентами информационной безопасности.

В целом же обеспечение надежности и стабильности работы современных систем автоматизации и снижение угроз, связанных с их информационной безопасностью, требует комплексного подхода, который должен включать в себя:

- формирование внутрикорпоративных стандартов, регламентов и требований по информационной безопасности промышленных объектов;
- создание центра управления информационной безопасностью и реагирования на инциденты;
- разработку типовых и проектных технических решений, минимизирующих риски сбоя производственного процесса по причине инцидентов информационной безопасности.

Столкнувшись с проблемой информационной безопасности, компания может пробовать решить ее самостоятельно. Дополнительные знания можно получить в том числе на специальных курсах. Но, как показывает практика, лучше обратиться за помощью к компаниям, давно занимающимся темой ИБ АСУ ТП и знающим все нюансы технических процессов и нормативного поля, регулирующихся в последнее время все жестче. Если проблемы пока нет, не стоит рассчитывать, что ваше предприятие и в будущем не коснется беда, которая уже настигла других.

Посмотрим вокруг. Мы все пользуемся электричеством, которое вырабатывается на гидроэлектростанциях или атомных электростанциях. А ведь и на объектах таких типов подобные инциденты уже были, например на Саяно-Шушинской ГЭС и АЭС в Ира-

не. Мы пьем воду из-под крана и пользуемся канализацией, но и на предприятиях, обеспечивающих нас данными ресурсами, тоже были инциденты. Например, из-за преднамеренной подмены баланса химического состава воды на очистительной установке вода фактически стала опасной для жизни. Хорошо, что данное изменение быстро заметили и отреагировали на него, и, по официальной информации, обошлось без жертв. А что, если в следующий раз так не получится? В Америке произошел инцидент, когда содержимое канализационной системы вылилось на улицы города. Причина – обиженный уволенный сотрудник после официального прекращения работы удаленно вошел в систему управления и устроил аварию.

Все это доказывает одно – в наши дни на современном предприятии перечень обязательных правил функциональной, физической, противопожарной и производственной безопасности просто необходимо дополнить регламентами по обеспечению информационной безопасности. Причем это является необходимостью бизнеса в той же степени, что и для государства.

При написании статьи автором был задан запрос "АСУ ТП" в поисковике картинок, и в первых 25 картинках по выдаче были обнаружены 2 картинки с высоким разрешением и детализацией. На каждой из них были указаны: названия объектов, явно говорящие об их местонахождении и назначении; подробные схемы технологических процессов с указанием моделей используемых средств автоматизации и сетевой инфраструктуры; краткое функциональное описание каждого блока. О чем это говорит? О том, что если вашим предприятием решит заняться злоумышленник или тренирующий свои возможности продвинутый школьник, то ему достаточно будет ввести в поисковике название предприятия или конкретного объекта, и он тут же найдет достаточное количество нужной ему информации.

Вот почему неважно, строите вы сети, систему класса MES или работаете оператором крана – знание об угрозах современности и соблюдение элементарных правил информационной безопасности позволит избежать неприятных ситуаций. А совместные усилия сотрудников отделов информационной безопасности, информационных технологий и автоматизации позволят добиться стабильности бизнеса в современных реалиях.

Алексей Петухов,
руководитель направления защиты АСУ ТП,
Центр информационной безопасности,
компания "Инфосистемы Джет"

В РАМКАХ ПЕТЕРБУРГСКОГО МЕЖДУНАРОДНОГО ГАЗОВОГО ФОРУМА

XX МЕЖДУНАРОДНАЯ
СПЕЦИАЛИЗИРОВАННАЯ ВЫСТАВКА
ГАЗОВОЙ ПРОМЫШЛЕННОСТИ
И ТЕХНИЧЕСКИХ СРЕДСТВ
ДЛЯ ГАЗОВОГО ХОЗЯЙСТВА

4-7 октября 2016

ОРГАНИЗАТОР FarEXPO IFE

ОФИЦИАЛЬНАЯ ПОДДЕРЖКА

Тел/факс: +7(812) 777-04-07; 718-35-37
st@farexpo.ru
www.farexpo.ru/gas

ДЕЛОВОЙ ПАРТНЕР EXPOFORUM

ГЕНЕРАЛЬНЫЙ ИНФОРМАЦИОННЫЙ ПАРТНЁР ТПА

МЕСТО ПРОВЕДЕНИЯ:
Санкт-Петербург, конгрессно-выставочный центр «ЭКСПОФОРУМ», павильон G, Петербургское шоссе, 64/1