Информационная безопасность промышленных предприятий Беларуси

А.С. Мохнач (ОАО «АГАТ – системы управления»)

Рассмотрены проблемные вопросы функционирования промышленных предприятий Республики Беларусь в разрезе обеспечения информационной безопасности субъектов хозяйствования, отражены наиболее актуальные киберугрозы современности, а также изложены основные рекомендации для начала работ по совершенствованию процессов информационной безопасности предприятия, приведены фактические данные в отношении тенденций роста и процентного соотношения видов киберугроз за 2018-2019 гг.

Ключевые слова: информационная безопасность, промышленные предприятия, кибербезопасность, таргетированные атаки, бот, вредоносное ПО, уязвимости.

В эпоху глобальной цифровизации экономики и ежегодного существенного развития специализированного программного обеспечения, задействованного в функционировании АСУТП промышленных и других предприятий, само понятие информации трансформируется, превращаясь в отдельный ресурс. Такой вновь формируемый ресурс обладает четкими уникальными характеристиками. В разрезе кибербезопасности одной из таких характеристик является потенциальная уязвимость.

Любая информация может быть использована легитимно и нелигитимно. Соответственно, к информации может осуществляться санкционированный либо несанкционированный доступ. В большинстве случаев несанкционированный доступ к информации влечет наступление негативных последствий для субъекта хозяйствования. Наибольшие опасения вызывает традиционно банковская сфера, где несанкционированный доступ к компьютерной информации влечет непосредственное завладение денежными средствами держателей счетов. Вместе с тем, все большее распространение начинают получать «атаки через поставщиков» (supply chain), в ходе которых атакам подвергаются не непосредственные конечные цели в виде предприятий, осуществляющих закупку тех или иных программно-аппаратных ресурсов, а вендоры самих программных и аппаратных решений. При этом в процессе сборки в код таких решений внедряются вредоносные фрагменты, которые в дальнейшем используются, как правило, для осуществления коммерческого шпионажа.

В настоящее время состояние промышленных предприятий Беларуси с позиции кибербезопасности в принципе нельзя назвать превосходным. Уровень ряда предприятий можно признать удовлетворительным (гиганты промышленности, такие как «БелАЗ» или «Беларуськалий»), состояние же материально-технической базы большинства предприятий является неудовлетворительным.

В связи с этим возникает парадоксальная ситуация, когда к обеспечению надлежащего уровня информационной безопасности (ИБ) стремятся в основном именно те предприятия, где уровень информационной безопасности и без того находится на удовлетворительном уровне. А те промышленные предприятия, где материально-техническая база не позволяет внедрить современные технические решения в сфере кибербезопасности, зачастую игнорируют вопросы ИБ. Микроэкономическое положение большого числа белорусских промышленных предприятий является уязвимым, поэтому проведение мероприятий, направленных на повышение уровня ИБ, в ряде случаев может быть осуществлено на таких предприятиях только на самом базовом техническом уровне, а также в области документального обеспечения ИБ и работы с персоналом. При этом существуют объективные препятствия, не позволяющие проводить мероприятия, направленные на достижение минимального уровня ИБ: использование давно устаревшего оборудования и операционных систем, отсутствие базовых элементов защиты, отсутствие в штате предприятия хотя бы в единственном числе специалиста в области ИБ. Работу по повышению уровня ИБ таких предприятий следует начинать в первую очередь с обновления материально-технической базы, включая приобретение современных персональных электронных вычислительных машин (ПЭВМ) с релевантными лицензионными операционными системами и прикладным программным обеспечением (ПО). Однако в силу нестабильного экономического положения многие промышленные предприятия не могут удовлетворить заявки ответственных должностных лиц, отвечающих за функционирование локальной вычислительной сети (ЛВС) на приобретение необходимого числа ПЭВМ и лицензий на ПО.

Отметим, что закупка ПЭВМ и ПО по принципу 50/50 в данном случае не работает, поскольку при обеспечении ИБ предприятия все узлы ЛВС должны быть планомерно обновлены до состояния, исключающего наличие уязвимостей хотя бы на уровне обновления основных компонентов. Для более наглядного представления можно рассматривать ИБ предприятия как обычный забор, ограждающий территорию. При этом является очевидным тот факт, что забор может выполнять свои непосредственные функции только в том случае, если он охватывает весь периметр, оборудован проходной и контрольно-пропускным пунктом. Если же сделать из четырех необходимых стен забора только две или три, при этом не закрыв весь периметр, то большого практического смысла от такого забора ожидать не следует. Аналогичным образом работают механизмы ИБ: должны быть приняты необходимые меры для того, чтобы закрыть весь периметр, все узлы ЛВС. Если же из 100 ПЭВМ поменять 50 машин и оснастить их лицензионным антивирусным ПО, при этом оставив без внимания в составе ЛВС другие 50 ПЭВМ, то такая ЛВС все равно останется уязвимой. Все сказанное выше является следствием основной проблемы белорусских промышленных предприятий: отсутствия свободных денежных средств на обновление материально-технической базы до достижения удовлетворительного состояния.

Помимо обновленной материально-технической базы необходимо также понимание сути проблемы ИБ руководством предприятия. В настоящее время такое понимание, сопряженное с активными мероприятиями по реализации комплекса мер по повышению уровня ИБ, присутствует практически исключительно у руководства тех предприятий, отдельные объекты которых отнесены к критически важным объектам информатизации, которым нормативно-правовыми актами Республики Беларусь благодаря стараниям Оперативно-аналитического Центра при Президенте Республики Беларусь прямо предписано выполнять ряд требований по обеспечению ИБ. Такие предприятия активно создают системы ИБ, занимаются проектированием и созданием систем защиты информации, привлекая для этих целей, в том числе квалифицированных сторонних исполнителей.

Отметим, что далеко не все белорусские промышленные предприятия представляют непосредственный интерес для злоумышленников по направлениям своей деятельности. Скорее, ПЭВМ из состава ЛВС данных предприятий зачастую представляют интерес только на бытовом уровне. Таким образом, вредоносное ПО, попадая в ЛВС промышленного предприятия, включает ряд незащищенных ПЭВМ в состав бот-сети[1] злоумышленника, которая использует их для достижения преступных целей, не связанных с производством самого предприятия [1]. При этом производство предприятия как таковое убытков не несет и негативному воздействию практически не подвергается (снизившаяся производительность отдельно взятой ПЭВМ из состава ЛВС в краткосрочной перспективе не может рассматриваться как серьезный неблагоприятный фактор для всего производственного процесса промышленного предприятия).

Вместе с тем не следует забывать о том, что в последние 4 года таргетированные атаки[2] окончательно вытеснили обычные атаки, преодолев в процентном отношении планку в 50%. В 2020 г. > 60% всех атак на предприятия являются именно таргетированными, совершаемыми специально подготовленными группировками атакующих для достижения определенной известной им цели [1]. В ряде случаев такие атаки являются длящимися. Такой целью может являться, например, внедрение бота слежения в ЛВС предприятия и получение непосредственных сведений о проводимых разработках, изобретениях, финансовых потоках и контрагентах предприятия-жертвы. Обладая такой информацией, группа атакующих может действовать в интересах прямых конкурентов данного предприятия и даже правительств ряда заинтересованных стран с учетом геополитической ситуации. Однако для этого продукция и производство промышленного предприятия должны представлять собой интерес для международного сообщества. Предприятие должно быть достаточно крупным и известным на международной арене, обладать потенциалом научных разработок и проводить соответствующие исследования. Если же предприятие не обладает перечисленными характеристиками, проведение таргетированных атак в отношении него представляется крайне маловероятным. Однако для любого предприятия представляют угрозу обычные примитивные атаки, совершаемые большим числом злоумышленников в отношении неопределенного круга жертв: криптеры[3], локеры[4], спам-рассылки, фишинг[5], частные ботсети, майнеры[6] и др. Разумеется, при очень низком уровне обеспечения ИБ любая ПЭВМ из состава ЛВС может быть подвергнута успешной атаке, после чего функционировать в составе бот-сети, выполняя функции, необходимые злоумышленнику, а не предприятию.

Все сказанное выше относится к базовым сторонам обеспечения ИБ промышленных предприятий Беларуси.

Если же углубляться в вопрос практического обеспечения ИБ тех промышленных предприятий страны, где материально-техническое обеспечение позволяет успешно реализовывать подобные мероприятия, следует иметь в виду не только программную, но и аппаратную часть ЛВС. В последнее 5-летие

---

[1] Бот-сети – соединенные между собой системы ПЭВМ с внедренными в них ботами. Бот – сторонний программный модуль, внедряемый в тело ОС ПЭВМ жертвы для скрытного использования ресурсов данной ПЭВМ злоумышленником в собственных целях, отличных от целей ее непосредственного владельца.

[2] Таргетированные (целевые) атаки – вид атак на ПЭВМ и ЛВС, характеризующийся наличием у атакующего прямого умысла на атаку конкретной ПЭВМ или ЛВС, имеющий своей целью достижение конкретного результата в отношении конкретного субъекта хозяйствования или отрасли. Как правило, таргетированные атаки имеют коммерческую, политическую или террористическую подоплеку.

[3] Криптер – разновидность вредоносного ПО, основной функцией которого является шифрование данных на ПЭВМ и серверах. В последнее время получают все более широкое распространение.

[4] Локер – разновидность вредоносного ПО, основной функцией которого является блокирование операционной системы ПЭВМ при ее перезагрузке. Как правило, воздействию подвергаются ПЭВМ с OC Windows.

[5] Фишинг – осуществление рассылок электронных писем с целью побуждения адресата предоставить какую-либо частную или корпоративную информацию. Как правило, рассылаются от имени контрагентов или потенциальных контрагентов, контролирующих органов и якобы финансовых учреждений.

[6] Майнер – разновидность вредоносного ПО, основной функцией которого является включение мощностей ПЭВМ-жертвы в состав бот-сети для осуществления скрытых вычислений для получения криптовалюты в интересах злоумышленника.

все большую актуальность приобретает эксплуатация непропатченных (неустраненных) уязвимостей самого оборудования. Специалисты по ИБ со всего мира уделяют самое пристальное внимание исследованию всех моделей и линеек специализированного оборудования таких вендоров, как Shneider Electric, Cisco, ABB, Moxa, Siemens и др., зачастую обнаруживая уязвимости на уровне прошивки определенных версий. Сведения о таких обнаруженных уязвимостях становятся известными вендорам, которые в большинстве случаев выпускают специальные патчи (обновления), которые необходимо применить в процессе регулярного обновления ПО. Однако такие сведения становятся известны как вендорам, так и потенциальным злоумышленникам, равно как и специализированным сообществам, занимающимся осуществлением таргетированных атак в интересах крупных корпораций и правительств [2]. Кроме того, такие отчеты можно обнаружить на закрытых ветках специализированных форумов. В дальнейшем с использованием сведений о такой уязвимости можно успешно ее проэксплуатировать удаленно. Например, на некоторые уязвимости, обнаруженные еще летом 2019 г., патчей от некоторых разработчиков средств коммуникаций пока не последовало. Помимо этого, представляется нецелесообразным оставлять настройки специального оборудования по умолчанию («по дефолту»). В данном случае необходимо вручную менять стандартные настройки, начиная с предустановленной пары «логин-пароль», а заканчивая, как минимум, указанием неспецифических портов и принудительным выставлением опции отключения («disabled») для всех незадействованных функций и служб. Аналогичные защитные меры уровня процессов могут быть осуществлены самостоятельно системными администраторами или продвинутыми пользователями ОС Windows путем выставления соответствующих флагов в отношении некоторых классов ошибок [3]. Помимо этого, при принятии решения о закупке оборудования определенной марки и модели представляется целесообразным предварительное наведение справок и поиск соответствующей информации на специализированных площадках по вопросам наличия уязвимостей в таком оборудовании. Любопытно также и то, что цепочка устранения уязвимости выглядит следующим образом: релиз от вендора — принятие в эксплуатацию — обнаружение уязвимости — опубликование сведений об уязвимости — устранение уязвимости вендором — выпуск вендором патчей по безопасности — имплементация патчей промышленными предприятиями. Срок прохождения такой цепочки составляет от 6 мес. до 2 и более лет. Некоторые уязвимости закрыть в принципе невозможно в силу специфики задействованного оборудования и протоколов. Таким образом, как минимум полгода потенциальные злоумышленники имеют возможность эксплуатации уязвимости, сведения о которой появляются на специализированных информационных ресурсах задолго до выпуска соответствующего обновления вендором.

Согласно данным, предоставленным в сборниках исследований по практической безопасности АО «Позитив Текнолоджиз», начиная с 2018 г. наметился тренд на увеличение общей доли таргетированных атак от общего числа всех атак (55% в 2018 г., 60% в 2019 г.), при этом доля атак на промышленные компании выросла до 10% в 2019 г. против 4% в 2018 г. (атаки проводились в основном с использованием вредоносного программного обеспечения (90% случаев)). Согласно исследованиям, проведенным Центром мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (ФинЦЕРТ Банка России) Департамента информационной безопасности Банка России, за 2018 г. целевые атаки с использованием вредоносного программного обеспечения, направленные на финансовые организации и клиентов финансовых организаций, составили 40,2% и 36,4% соответственно. Таким образом, доля таргетированных атак в банковской сфере только в 2018 г. составила 76,6% от общего числа.

Самым распространенным видом вредоносного программного обеспечения в 2019 г. стали шифровальщики (31% от общего числа), при этом 5% известных случаев работы программ-шифровальщиков приходится на промышленные предприятия.

В целом промышленность не является ключевой сферой интересов киберпреступников, поскольку на настоящем этапе развития общества имеются иные, гораздо более привлекательные сферы (финансово-кредитная система, личные данные людей, облачные хранилища). Однако именно с успешной реализацией атак на промышленные предприятия связан наиболее высокий риск наступления максимально негативных последствий, таких как аварии, катастрофы, которые, в том числе могут повлечь гибель работников предприятия и загрязнение окружающей среды вблизи мест расположения промышленных объектов. В связи с этим ИБ таких объектов промышленности должна быть обеспечена надлежащим образом.

Для противодействия таргетированным атакам разработаны и успешно применяются соответствующие программные решения, такие как KATA и KICS (вендор АО «Лаборатория Касперского», https://www.kaspersky.ru), ТДС (вендор АО «Групп АйБи», https://www.group-ib.ru), «Макс-патрол» (вендор АО «Позитив Текнолоджиз», https://www.ptsecurity.com/ru-ru) и др. Указанные средства обнаружения таргетированных атак с возможностью поиска фактов вторжений (intrusion detection system — IDS) и средствами активного мониторинга позволяют своевременно выявлять и подавлять большинство таргетированных атак. Основным недостатком данных решений можно считать

---

[7] APT – сложная, развитая и устойчивая атака, направленная на захват контроля над целевой инфраструктурой.

их высокую стоимость. В силу этого достаточно острым является вопрос о надлежащей оценке рисков негативных последствий. Качественно проведенная оценка рисков сможет принести понимание необходимости затрат на приобретение дорогостоящих APT[7]-решений, если риск от наступления негативных последствий исчисляется в крупных суммах или способен повлечь причинение вреда жизни или здоровью людей.

Анализируя состояние ИБ промышленных предприятий Беларуси, следует обращать внимание на состояние материально-технической базы, наличие понимания у руководства предприятий проблем ИБ и возможных негативных последствий, а также на практическую сторону обеспечения ИБ на основе лучших мировых практик.

Подводя итоги, отметим следующие основные тезисы, которые сами по себе не стоит расценивать как выводы, а всего лишь как отправную точку для дальнейших рассуждений.

1. Киберугрозы реальны.
2. Имеется устойчивая тенденция к росту числа таргетированных атак.
3. Промышленные предприятия являются одной из основных целей злоумышленников.
4. Для атак на промышленные предприятия используются различные виды вредоносного программного обеспечения, уязвимости в задействованных программных и аппаратных ресурсах, инсайдеры.
5. Успешно реализованная атака на промышленное предприятие может повлечь наступление негативных последствий вплоть до смерти человека и причинения экологического ущерба.
6. Решение о приобретении специализированных систем противодействия таргетированным атакам следует принимать после надлежащим образом проведенной процедуры оценки рисков.

Список литературы

1. *Atluri A.C., Tran V. Botnets Threat Analysis and Detection. M.: Springer. 2017. C. 15-27.*
2. *Левцов В.* Анатомия таргетированной атаки. 2016. https://www.kaspersky.ru/blog/targeted-attack-anatomy/4388/
3. *Руссинович М., Соломон Д., Ионеску А., Йосифович П.* Внутреннее устройство Windows. 7-е изд. – СПб.: Питер. 2018. С. 899-905.

Мохнач Александр Сергеевич *– начальник Центра кибербезопасности*
ОАО «АГАТ – системы управления» – управляющая компания холдинга
«Геоинформационные системы управления».
Контактный телефон (+375-17) 337-54-55.
https://soc.agat.by

От Редакции

Все проблемы, поднятые в статье, характерны не только для предприятий Беларуси, но свойственны также российским промышленным предприятиям.