ДЕНИС ЗИНОВЬЕВ

ОДНА ИЗ ПРИОРИТЕТНЫХ ЗАДАЧ ТЮМЕНСКОЙ ОБЛАСТИ – ИНФОРМБЕЗОПАСНОСТЬ

Вслед за повышением плотности атак на объекты КИИ меняется профиль атак, отмечают в «Ростелеком-Solar». Так, при атаке на банк сначала идет долгое исследование периметра, получение точек присутствия, а дальше — за 2–3 часа быстрая атака, незамаскированная и лобовая, поясняет гендиректор компании Игорь Ляпунов. «В случае атак на объекты КИИ цель злоумышленника — не моментальное действие, а получение точки присутствия, возможности контроля. В большинстве случаев это очень скрытый инструментарий: бесфайловые вирусы, жизнь зловредов в оперативной памяти компьютера, практически без каких-то следов в файловых системах и почти без следов в сети»,— рассказывает Игорь Ляпунов. Это накладывает серьезные ограничения на возможность выявления таких видов атак.

При этом атаки на объекты КИИ, в отличие от простых, относительно дешевых фишинговых атак, прицельно создают коллективы по 20–30 человек. «Это очень дорого — написать такой инструментарий и реализовать такую атаку, а прямой монетизации там нет вообще»,— отмечает господин Ляпунов.

ОБЪЕКТЫ КИИ Закон №187 «О безопасности критической информационной инфраструктуры» вступил в силу 1 января 2018 года. К объектам КИИ в нем отнесены сети и информационные системы госорганов, предприятий оборонной промышленности, транспорта, кредитно-финансовой сферы, энергетики, топливной и атомной промышленности. Владельцы критической инфраструктуры должны подключить свои объекты к Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), созданной ФСБ. Также они должны составить перечень объектов КИИ и отнести их к одной из трех категорий значимости, исходя из того, какой ущерб стране и людям будет нанесен в случае атаки на нее. В результате будет создан реестр значимых объектов. Согласно ст.274.1 УК РФ, если атака нанесла вред объектам КИИ, злоумышленникам будет грозить уголовная ответственность. Сейчас КИИ находится в стадии категорирования. Оно должно завершиться в 2019 году, после чего начнется построение системы безопасности.

По данным Федеральной службы по техническому и экспортному контролю (ФСТЭК), в УрФО более 170 субъектов (владельцев) КИИ, из которых 59 — органы власти и их учреждения. Объектов (информационных систем) на Урале — порядка 1,4 тыс., однако только 15 внесены в реестр.

По данным Свердловскстата, в 2018 году объем обеспечения электрической энергией, газом и паром по УрФО превысил 700 млрд руб., на 3% увеличив показатели 2017 года. Доля УрФО в общероссийском показателе по этому виду экономической деятельности составила 12,7%. В первом квартале 2019 года объемы выросли на 5,8% по сравнению с аналогичным периодом 2017 года — до 220,3 млрд руб.

ПРОБЛЕМЫ БЕЗОПАСНОСТИ По словам Владимира Дрюкова, ключевая сложность обеспечения безопасности субъектов КИИ в том, что для них характерны разные, специфичные для каждого из рыночных сегментов вектора угроз, требующие от центров мониторинга редкой профильной экспертизы. «Необходимо обследовать и проработать модели угроз для технологических сетей и технологических процессов компании, а в этой области как у поставщиков программных продуктов, так и у интеграторов практики крайне мало»,— пояснил он.

С защитой АСУ ТП, по его словам, связана еще одна сложность: «Компании с большой неохотой подключают к мониторингу даже средний уровень инфраструктуры (уровень контроллеров)». На деле многое зависит от того, насколько каждый конкретный заказчик доверяет центру мониторинга, уверен он. «В результате сегодня мы наблюдаем картину, когда сочетание экспертизы в тематиках автоматизированных систем управления технологическими процессами (АСУ ТП) и SOC (оперативный центр безопасности) встречается буквально в 2–3 компаниях. Остальные пока продолжают ориентироваться исключительно на коммерческий рынок, корпоративные сети и нижний уровень (уровень контрольно-измерительного оборудования) сегмента АСУ ТП»,— отмечает господин Дрюков. Другим обстоятельством, осложняющим выявление атак, является малое количество разработанных средств, прошедших промышленную апробацию и способных обнаруживать атаки на ранних стадиях, считает технический директор ООО «Газинформсервис» Николай Нашивочников.

В отчете Kaspersky называют и другие проблемы безопасности промышленных предприятий, в частности — не вполне адекватную оценку уровня угрозы. К этому приводит недостаток общедоступной информации о проблемах информационной безопасности промышленных предприятий, относительная редкость целевых атак, направленных на системы автоматизации, излишняя вера в системы противоаварийной защиты и неприятие объективной реальности. Под последним, в частности, понимают отрицание факта доступа в интернет или наличия случайных заражений компонентов АСУ ТП.

Кроме того, важно понимать, что речь идет о стратегических проектах огромной ресурсоемкости, полагает эксперт. По его данным, средняя энергетическая компания — это 1 тыс. объектов по всей стране, каждый из которых требует мониторинга и команды в 30–40 человек для обслуживания. «Это при том, что сейчас даже сервис-провайдеры находятся в условиях серьезного кадрового голода. Поэтому все они трижды думают, стоит ли ввязываться в большой проект и смогут ли они “проглотить этого слона” целиком»,— констатирует эксперт. По данным ФСТЭК, в сфере информационной безопасности в России занято 22 тыс. человек. Однако более 75% этих сотрудников не имеют профессиональной квалификации в сфере информбезопасности, лишь 5–10% прошли переподготовку, остальные имеют базовое образование в сфере ИБ.

Нельзя также не отметить вопросы безопасности интернета вещей (IoT). Участники рынка признают — эта сфера еще плохо регулируется законодательством.

ГАРАНТИЯ БУДУЩЕГО Сервисы и ресурсы организаций ТЭК, как правило, редко имеют доступ в сеть интернет, поэтому при всей интенсивности атак, приходящихся на корпоративный сегмент сети компании, редкие из них заканчиваются успешно, отмечает Владимир Дрюков, тем не менее, разнородность и территориальная распределенность инфраструктуры оставляют тему безопасности по-прежнему актуальной.

По данным господина Дрюкова, существенный объем атак совершается посредством фишинга и/или вредоносного ПО, попадающего в инфраструктуру компаний с почтовыми рассылками, использующими методы социальной инженерии.

«Повсеместная цифровизация предприятия влечет за собой киберриски,— констатирует Алексей Петухов.— Информационная безопасность уже не является отдельно существующей службой. Она входит в общую систему управления рисками на предприятии, помогая автоматизировать и оптимизировать промышленные процессы и делать управление производством более эффективным».

Несмотря на обилие систем защиты, реальная безопасность технологических объектов остается низкой, признает Евгений Гнедин. «Причина во множестве факторов — от неосведомленности и незаинтересованности работников предприятий ТЭК в обеспечении ИБ до низкой эффективности ИБ компании в вопросе противостояния реальным целенаправленным атакам»,— считает он. Для эффективной защиты предприятия ТЭК, по мнению эксперта, мало просто внедрить системы для выполнения требований регуляторов, необходимо построить комплексную систему ИБ, которая гарантированно будет способна своевременно выявить кибератаку и предотвратить критические последствия.

ОЛЕГ ХАРСЕЕВ

КИБЕРАТАКИ МОГУТ ПРИВЕСТИ К АВАРИЯМ НА ПОДСТАНЦИЯХ