

СЛАБОЕ ЗВЕНО В ЭНЕРГЕТИЧЕСКОЙ ЦЕПИ

В ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ УЖЕ МНОГОЕ СДЕЛАНО ДЛЯ ПОВЫШЕНИЯ КИБЕРБЕЗОПАСНОСТИ ЕЕ ОБЪЕКТОВ, НО ОСТАЕТСЯ ЕЩЕ РЯД НЕРЕШЕННЫХ ПРОБЛЕМ. В ТОМ ЧИСЛЕ СВЯЗАННЫХ С ПРЕСЛОВУТЫМ ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ. АНЖЕЛИКА ТИХОНОВА

В ноябре 2020 года ассоциация «Цифровая энергетика», куда входят «Росатом», «Интер РАО», «Россети» и другие представители отраслевого бизнес-сообщества, предложила создать центр кибербезопасности в энергетике. В его задачи входит обобщение опыта и компетенций как о компьютерных атаках в отрасли, так и о мерах, которые можно применять для защиты объектов, а также обучение руководителей компаний по информационной безопасности. До 2022 года центр будет частью ассоциации, а затем может обрести самостоятельность. Все это должно повысить информационную защищенность отрасли.

НЕИДЕАЛЬНАЯ СИТУАЦИЯ Пока же ситуацию с кибербезопасностью сложно назвать идеальной. С одной стороны, как замечает Алексей Парфентьев, ведущий аналитик компании «СерчИнформ», российского разработчика средств информационной безопасности и инструментов для защиты информации, многое уже сделано. Например, в 2018 году появился закон «О безопасности критической информационной инфраструктуры (КИИ) РФ», Минэнерго разработало и согласовало с Федеральной службой по техническому и экспортному контролю (ФСТЭК) методические рекомендации по определению и категорированию объектов КИИ (приказ ФСТЭК № 239). По словам Алексея Парфентьева, в отрасли есть средства на закупку оборудования, программ и наем профессиональных специалистов по информационной безопасности (ИБ). «Так как энергетические компании являются объектами критической инфраструктуры и подпадают под требования регуляторов по информационной защите, поэтому оснащенность защитными решениями тут довольно высока. Это касается и базовых программ, и специфических. Например, SIEM-, DLP-системы применяет, по нашей оценке, 31 и 47% компаний соответственно», — говорит господин Парфентьев.

С другой стороны, как отмечают в компании Group-IB, специализирующейся на предотвращении и расследовании киберпреступлений и мошенничеств с использованием высоких технологий, в отрасли есть проблемы. По мнению ее экспертов, пока затраты на кибербезопасность в энергетике малы относительно рисков. В отличие, например, от банковской сферы, где и регулятор жесткий, и инцидентов немало, и все они каждый раз анализируются, чтобы усилить защиту. «Хотя в банковской сфере и получается игра в догонялки, но отставание от атакующих групп небольшое, видно, как ИБ банков развивается», — отмечают в Group-IB. — В энергетической отрасли ситуация обстоит иначе. По нашему мнению, текущие затраты на обеспечение безопасности неотягивают до должного уровня». И речь не только о прямых финансовых затратах, но и о подготовке кадров. В Group-IB считают, что



ПОКА ЗАТРАТЫ НА КИБЕРБЕЗОПАСНОСТЬ В ЭНЕРГЕТИКЕ МАЛЫ ОТНОСИТЕЛЬНО РИСКОВ. В ОТЛИЧИЕ, НАПРИМЕР, ОТ БАНКОВСКОЙ СФЕРЫ, ГДЕ И РЕГУЛЯТОР ЖЕСТКИЙ, И ИНЦИДЕНТОВ НЕМАЛО, И ВСЕ ОНИ КАЖДЫЙ РАЗ АНАЛИЗИРУЮТСЯ, ЧТОБЫ УСИЛИТЬ ЗАЩИТУ

большинство компаний придерживается принципа «работает — не трогай», часто на местах специалисты слабо понимают, с какими киберугрозами могут столкнуться, и вообще открытых кейсов и публичных наказаний практически не встретить, а это не позволяет в полной мере оценить масштаб проблем и разработать способы их решения.

Даже рекомендации по КИИ выполняются по принципу ухода от ответственности, отмечают в Group-IB. «Регулятор обязал провести категорирование систем безопасности, но часть компаний занизила категорию. А теперь средства защиты выбираются исходя из категории. Обычным сотрудникам сложно донести до руководства, почему надо потратить больше, чем указано в категории, и получается замкнутый круг. И если по установленной категории не положены системы защиты информации, то в результате критический объект оказывается уязвим», — говорят в компании.

СПЕЦИФИЧЕСКИЕ ФАКТОРЫ Не могла не сказаться на ИБ и пандемия, а точнее последовавший из-за нее полный или частичный переход на удаленный режим работы. В принципе ее влияние, по словам Алексея Парфентьева, ощутили практически все бизнесы. Около 88% опрошенных «СерчИнформ»

компаний отметили, что в 2020 году их IT-инфраструктура потребовала больших мер защиты. «Если говорить конкретно об энергетической отрасли, тут действуют специфические факторы», — поясняет Алексей Парфентьев. — В частности, организация бизнес-процессов сложная, компании территориально распределены, с неоднородной IT-инфраструктурой (от суперсовременных компьютеров в центральных офисах до устаревшей техники где-то на периферии). В пандемию, когда приходилось по возможности вводить удаленку, ситуация стала только сложнее». Отразилось на ситуации и то, что отрасль инертная. Впрочем, это играло как в плюс, так и в минус. С одной стороны, прежние планы на закупку защитного ПО никак не страдали в связи с карантином, с другой — компании не могли оперативно отреагировать на необходимость перестраивать процессы в 2020-м, говорит Алексей Парфентьев.

При этом угрозы в отношении энергетических компаний с каждым годом усложняются. Интерес преступников представляют не только крупные, но и небольшие компании, обеспечивающие доставку электроэнергии на последней миле или оказывающие дополнительные услуги лидерам рынка. Так, по данным аналитического отчета Hi-Tech Crime Trends 2020–2021, подготовленного

Group-IB и посвященного исследованию высокотехнологичных преступлений в мире, в конце 2019 года — в первой половине 2020 года технологический сектор атаковали 13 групп, связанных со спецслужбами, семь хакеров, продающих доступ в энергетические сети, также известно об 11 случаях успешных нападений с использованием шифровальщиков.

Именно вирусы-шифровальщики в Group-IB называют главной угрозой энергетического сектора. «В некоторые такие программы преступники добавляют функции обнаружения процессов, связанных с системами управления промышленными предприятиями, чтобы обеспечить потерю данных, с которыми они работают, и повысить цену за возможность восстановления доступа. Другие распространенные киберриски сектора — эксплойты, бэкдоры и вредоносные скрипты, скрытые каналы передачи данных, бестелесные угрозы и нападения нулевого дня», — перечисляют эксперты Group-IB.

Главным уязвимым местом ИБ-инфраструктуры энергетических компаний остаются люди, которые в них работают. Аналитика реагирования на киберинциденты экспертов Лаборатории компьютерной криминалистики Group-IB показывает, что в 90% случаев атаки на сектор идут через корпоративные сети. Преступники используют методы социальной инженерии при рассылке фишинговых писем с вредоносным ПО (например, шифровальщиками), а также проникают в сеть компаний, например, через корпоративный портал или почтовый сервис.

Да, закон о критической инфраструктуре предусматривает защиту и от человеческого фактора. «К примеру, в том же приказе № 239 описывается, с помощью каких технических средств можно обезопасить компании от влияния человеческого фактора. Это системы разграничения доступа, регистрация событий информационной безопасности SIEM, удаленного доступа, контроль действий сотрудников за компьютерами DLP. А также с помощью организационных мероприятий — обеспечение безопасности процессов, обучение персонала», — говорит Алексей Парфентьев. Но все это, по его словам, лишь обязательный минимум, только совместное выполнение предписанных в отрасли мер и собственных инициатив и наработок компаний сможет действительно минимизировать человеческий фактор. Эксперты Group-IB уверены, что самое важное для отрасли — это адекватно оценивать и рассчитывать риски, избавиться от «авось» и «мы такого не видели, значит, такого не бывает», то есть готовиться к защите заблаговременно и вовлекать обслуживающий персонал в вопросы информационной безопасности. Сегодня принцип «работает — не трогай» неэффективен. В деле ИБ энергетических объектов нужно быть на шаг впереди от возможных угроз, уверены в Group-IB. ■