ПРОМЫШЛЕННЫЙ ЩИТ ОТ КИБЕРУГРОЗ

ПОВСЕМЕСТНАЯ ЦИФРОВАЯ ТРАНСФОРМАЦИЯ СТАВИТ ПЕРЕД ПРЕДПРИЯТИЯМИ НОВЫЕ ВЫЗОВЫ, КОТОРЫЕ ПРИВОДЯТ К ПОЯВЛЕНИЮ НЕОБХОДИМОСТИ БОЛЬШЕЕ ВНИМАНИЕ УДЕЛЯТЬ СИСТЕМАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. АРИНА МАКАРОВА

По данным «Лаборатории Касперского», за последний год около 80% предприятий столкнулись хотя бы с одной попыткой атаки или киберинцидентом. И, несмотря на минимизацию взаимодействия систем и человека, все еще сохраняется большой процент угроз, которые происходят из-за халатности или неопытности персонала. Например, достаточно, чтобы сотрудник ночной смены подключил телефон или 3G-модем к рабочему месту, чтобы проверить почту.

Технический консультант по безопасности Schneider Electric Андрей Иванов убежден, что безопасность киберфизических систем должна обеспечиваться вне зависимости от размера предприятия. «Например, для предприятий, которые относятся к критической информационной инфраструктуре Российской Федерации, уже второй год действуют нормативные документы, в которых приведен достаточно объемный перечень требований по обеспечению безопасности их киберфизических систем. Эти требования относятся и к применению технических средств защиты информации, и к организационным мерам, и к организации соответствующей структуры предприятия, обеспечивающей безопасность таких систем. Кроме этого, есть набор международных стандартов и практик, описывающих подходы и способы обеспечения безопасности используемых в промышленности киберфизических систем с учетом отраслевой специфики и особенностей»,— рассказывает Андрей Иванов.

Разработкой специализированных промышленных систем защиты занимаются как зарубежные игроки (Siemens, Schneider Electric), так и отечественные компании (Kaspersky, Positive Technologies, Infowatch).

НЕ ПУСТОЙ ЗВУК По словам эксперта направления информационной безопасности IT-компании КРОК Александра Черныхова, цифровизация промышленности и автоматизированная система управления — уже не просто модная тема для разговора среди IT-специалистов, а необходимое условие для повышения эффективности и конкурентоспособности. «С их увеличением новый технологический уклад приносит новые угрозы для промышленных систем. Когда все производственные цепочки объединены в одну экосистему, то нарушение в работе одного компонента из-за вредоносного программного обеспечения может повлечь сбой во всей цепочке и остановить работу на часы и дни»,— констатирует он. Руководитель направления «Информационная безопасность» CTI Антон Афанасьев говорит, что на текущий момент большинство крупных производственных предприятий находятся в группе риска, являются объектами атак как с целью кибершантажа, так и кибершпионажа. «В недавнем прошлом мы стали свидетелями киберинцидентов, вызванных атаками шифровальщиков. Такие инциденты приводили к простою оборудования и бизнес-систем, что напрямую влияет на экономику предприятия. Поэтому эта проблематика уже не является чем-то новым для данных компаний, а производители средств защиты информации уже предлагают различные по функционалу и возможностям специализированные системы безопасности, в том числе и для АСУ ТП»,— полагает эксперт.

Руководитель направления информационной безопасности практики системной и сетевой интеграции PROF-IT GROUP Алексей Щербаков отмечает, что главными источниками атак по-прежнему остаются халатность сотрудников и конкуренты, цель которых — кража интеллектуальной собственности. «Но риски могут быть и катастрофическими, в том числе связанными с угрозами окружающей среде и даже жертвами. Забавно, что зачастую сами атакуемые не знают о рисках. При этом много атак не из-за денег, а по линии „национальной безопасности“: например, когда хакеры получили доступ к центрифугам на ядерном производстве Ирана и заразили софт вирусом, который тормозил центрифугу на 0,00001% в сутки. Заметить это нереально. Но через два года она остановилась настолько, что ядерная программа Ирана была отброшена на несколько лет назад. И таких примеров много»,— приводит пример эксперт.

Технический директор Check Point Software Technologies в России и СНГ Никита Дуров также подчеркивает, что кибербезопасность промышленных предприятий — очень актуальный сегодня вопрос: «Большинство промышленных объектов строилось в то время, когда о кибербезопасности даже не задумывались. Никто не думал, что кибератаки могут нанести существенный ущерб и что это может затронуть промышленные предприятия. Сейчас промышленные системы нуждаются в комплексных решениях для защиты инфраструктуры. Важно защищать не только офисную часть организаций, но и производственные объекты. Существуют промышленные предприятия, для которых критически важно обеспечивать безопасность. Например, это касается предприятий энергетического сектора».

Руководитель направления защиты АСУ ТП Центра информационной безопасности компании «Инфосистемы Джет» Виталий Сиянов обращает внимание на то, что, помимо исполнения требований законодательства в рамках объектов критической информационной инфраструктуры (187-ФЗ, приказы ФСТЭК России № 235, 239), предприятию необходимо определить, какие из многочисленных угроз применимы именно к нему.

ПОЙМАТЬ МОМЕНТ Специалист по оценке безопасности компьютерных систем, IT-компании «Онсек» Иван Комиссаров уверен, что полностью защититься от всех возможных уязвимостей не получится, иначе такой области, как информационная безопасность, уже бы не существовало. Но минимизировать риски, а также снизить количество потенциальных проблем все же можно.

По словам экспертов, вовремя заметить угрозы и снизить вероятность их наступления поможет комплекс мер, направленный на обеспечение безопасности всех трех китов любого производства: людей, процессов и технологий. «Большинство производственных предприятий уникальны по своему составу и архитектуре средств автоматизации. Соответственно, нет универсального решения обеспечения безопасности, которое подходило бы всем,— говорит Антон Афанасьев.— Заказчикам при обеспечении безопасности необходимо уделить внимание вопросам сегментации сетей, а также совместимости наложенных средств защиты информации с системами автоматизации. Одним из важных факторов повышения защищенности является проактивная работа служб информационной безопасности с сотрудниками технологических подразделений компаний».

Генеральный директор GPC Pharmaceuticals Алексей Филиппов считает, что повышению цифровой безопасности также способствует создание специальной операционной среды между интранетом и интернетом, через которую обеспечивается доступ к необходимым приложениям внешней сети, предотвращая прямое обращение извне к внутренней корпоративной сети. «Очень хороший результат дает внутрикорпоративное обучение персонала, направленное на то, что сотрудникам становится понятно, какие угрозы существуют для компании и как можно их предотвратить. Ведь многие нарушения происходят даже не по злому умыслу, а просто потому, что люди не думают о рисках и последствиях своих поступков»,— также полагает Алексей Филиппов. Руководитель направления информационной безопасности OTP Григорий Куликов уверен, что основными целями должны быть снижение рисков, связанных с неправомерной или несвоевременной выдачей или отзывом прав доступа пользователей, а также повышение корректности оперативности процессов управления правами. «Для обеспечения достижения этих целей существуют специализированные средства защиты класса Identity and Access Management (IAM), в последнее время активно разрабатываемые и внедряемые основными игроками рынка информационной безопасности России»,— добавляет господин Куликов. ■