

ИНТЕГРАЦИЯ СИСТЕМ КИБЕРБЕЗОПАСНОСТИ ПРИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРЕДПРИЯТИЯ

РУСЛАН СТЕФАНОВ
Ruslan.Stefanov@Honeywell.com

Роль цифровых технологий во всех сферах жизни и производства непрерывно растет, а вместе с этим увеличиваются и риски, связанные с киберпространством. Согласно недавнему отчету Всемирного экономического форума [1], кибератаки входят в пятерку главных опасностей, угрожающих человечеству, наряду с природными катастрофами и изменением климата.



Очевидно, что прогресс нельзя повернуть вспять. Новые технологии принесли предприятиям неоспоримые преимущества: к примеру, по нашим наблюдениям, время простоя производственного оборудования уменьшилось на 20%, расходы на техническое обслуживание — в среднем на 13%. Постоянный мониторинг данных помогает принимать эффективные управленческие решения и повышать прибыльность. Цифровизация радикально сокращает сроки и стоимость запуска новых промышленных объектов и становится условием конкурентоспособности производственных компаний.

Конечно, не может быть и речи о том, чтобы отказаться от этих достижений. Но любой проект по внедрению цифровых решений должен одновременно улучшать показатели производительности и эффективности и снижать показатели киберрисков.

Разрыв между новыми технологиями и соблюдением мер безопасности встречался в истории и раньше. К примеру, в легковых автомобилях долгое время не устанавливали ремни безопасности, хотя они были изобретены еще в 1885 г. Поначалу ремни были нужны только автогонщикам, но постепенно скорости росли, число автомобилей и аварий на дорогах увеличивалось, а средства защиты водителей и пассажиров массово так и не применялись. В СССР использование ремней безопасности узаконили только в 1979 г., когда в стране уже почти десять лет выпускались классические «Жигули».

Правила промышленной безопасности тоже развивались вслед за технологиями и нередко отставали. Так, строители первых небоскребов работали на высоте без страховки и касок — сегодня это кажется немыслимым. Чтобы уменьшить отставание в области кибербезопасности, необходимо государственное регулирование, поэтому во многих странах разрабатываются и вводятся в действие нормативные акты с требованиями о защите с порядком контроля исполнения установленных требований и ответственностью за нарушение и последствия нарушения установленных требований. Например, с 1 января 2018 г. вступил в действие Федеральный закон №187 «О безопасности критической информационной инфраструктуры Российской Федерации».

Теперь настало время цифровой эволюции. Предприятия обмени-

ваются терабайтами данных и дистанционно управляют печами, раскаленными до 1000 °C. Нужны новые стандарты, методы и технологии защиты, встроенные в сети промышленного «Интернета вещей», а при проектировании оборудования должны закладываться новые требования информационной безопасности.

Специалисты уже сейчас могут предложить готовые решения для защиты от киберугроз и программы по снижению рисков в цифровой среде. И ведущие компании активно внедряют такие системы безопасности. Но по-прежнему остается немало предприятий, реагирующих на киберинциденты, а не предупреждающих их, что напоминает ходьбу по канату без страховки.

НОВЫЕ УСЛОВИЯ — НОВЫЕ ТРЕБОВАНИЯ

Отрасли с высоким уровнем автоматизации технологических процессов вынуждены модернизировать системы кибербезопасности. С чем связаны эти изменения?

Интеграция вместо физической изоляции

Никогда прежде по сетям промышленных предприятий не передавалось такое количество данных и никогда их качество не играло такой большой роли. Если раньше данные в сети были узкоспециализированными и передавались на машинном языке, недоступном рядовому пользователю, то сегодня любая информация из АСУ ТП может стать основой для глобальных выводов. Промышленные предприятия собирают сведения о безопасности и произошедших событиях и анализируют их с помощью различных программных пакетов и сервисов.

Раньше системы управления были физически отделены от корпоративной сети и тем более Интернета — именно это гарантировало их безопасность. Но теперь предприятия постоянно извлекают данные из производственных сетей для централизованного анализа, а значит, физическое разделение АСУ ТП и систем управления предприятием больше невозможно. Обмен данными должен происходить непрерывно и автоматически, поскольку задержки и ошибки в передаче информации существенно снижают ее ценность.

Более того, закрытые внутренние сети усложняют обеспечение киберзащиты предприятия. Централизованный доступ к данным АСУ ТП помогает укрепить безопасность, в частности стандартизировать показатели рисков.

Тактика защиты предприятия зависит от того, о каких данных идет речь и как они используются. Так, например, для АСУ ТП основную проблему представляет не кража информации, как в системах розничных продаж или в системах хранения персональных данных, а нарушение целостности данных, умышленное искажение рабочих параметров, вмешательство в техпроцессы.

В стратегию защиты можно включать различные современные физические средства, повышающие безопасность обмена информацией. Защищенные каналы связи с ведением журнала действий и многоуровневой идентификацией пользователей дают возможность лишний раз убедиться в том, что доступ к важной информации предоставляется только авторизованным лицам. Подчеркнем, что речь идет о тех же каналах связи, по которым работают системы удаленного доступа, обеспечивающие рост производительности и эффективности труда.

Новый вектор угроз — поддельные USB и добыча биткоинов

На многих предприятиях сейчас нет стандартизованных показателей для оценки рисков в сфере кибербезопасности и нет единого понимания, что является «нормальной» работой.

Между тем современные угрозы обретают разные формы. Традиционные меры безопасности (например, установка исправлений), конечно, по-прежнему важны, однако предприятиям нужно искать нестандартные подходы к защите от новых опасностей в цифровую эпоху. К примеру, раньше мы боялись распространения вирусов через USB-устройства, а теперь приходится думать о том, является ли вообще то, что мы подключаем к компьютеру под видом USB-флэшки, обыкновенным устройством для хранения данных. Так, во время последних атак злоумышленникам удавалось получить контроль над АСУ ТП, подключив к разъему USB поддельное периферийное устройство, которое выглядело как провод для зарядки телефона или электронной сигареты.



Надо отметить, что многие организации до сих пор заботятся только о средствах детектирования угроз, однако уже доступны практики, сокращающие время реакции на атаки злоумышленников. Если говорить, к примеру, о программах-вымогателях, то своевременная и централизованная установка исправлений, а также оперативное восстановление систем предприятия из резервных копий могут существенно повысить шансы на благополучный исход. Поэтому так важно, чтобы развивалась дисциплина резервного копирования данных. При этом самого по себе копирования недостаточно — важно быть уверенным в том, что резервные копии действительно хранятся там, куда их положили, и правильно сработают, если нужно будет восстановить систему.

В последнее время преступники пытаются использовать инфраструктуру предприятия для несанкционированной добычи криптовалюты, а это увеличивает затраты предприятия и создает угрозы безопасности. Выявить такой незаконный майнинг можно с помощью автоматизированных средств мониторинга.

На самом деле, сегодня любая стратегия промышленной кибербезопасности должна включать элементы автоматизации, поскольку

угрозы становятся все более многосторонними и непредсказуемыми, а желание злоумышленников получить легкие деньги только растет. Технические средства контроля повышают уровень готовности. Они могут автоматически оповещать об опасных изменениях состояния систем.

Например, автоматизированная система управления рисками Honeywell Risk Manager позволяет стандартизировать отчеты о состоянии средств безопасности на разных установках и площадках предприятия. Risk Manager автоматически собирает ключевые данные и сравнивает их с пороговыми значениями, заданными компанией для определения уровня рисков. Данные выводятся на контрольную панель, по показаниям которой легко определить текущий статус. Таким образом, в критически важный момент можно быстро и просто получить сведения о состоянии средств безопасности, в то время как раньше на сбор этих данных требовалось несколько недель. Уход от ручной проверки конечных узлов позволяет существенно сократить эксплуатационные расходы. Более того, Risk Manager помогает правильно расставить приоритеты при оценке бюджета на перспективные проекты.

ПЕРВЫЕ ШАГИ ПО ДОРОГЕ К КИБЕРБЕЗОПАСНОСТИ

Многих рисков в области информационной безопасности можно избежать благодаря правильным действиям сотрудников, грамотной организации процессов и внедрению определенных технологий. Не будем забывать, что каждому предприятию важны сроки реализации проектов и окупаемость инвестиций, но это не должно мешать развертыванию средств кибербезопасности. В реальности программа модернизации предприятия и обеспечение защиты от киберугроз должны происходить параллельно.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ КИБЕРБЕЗОПАСНОСТЬЮ

Сейчас многие территориально распределенные компании, например в энергетической отрасли, стараются консолидировать функции управления в одной операторной, чтобы сократить расходы и решить кадровые проблемы, при этом внедряя технологии защищенного удаленного доступа. В результате инженеры могут подключаться к производственным объектам по защищенному каналу, удаленно проводить мониторинг и устанавливать обновления. Так, предприятие избавляется от множества незащищенных подключений, которые часто остаются без внимания. На труднодоступных объектах или в регионах с высоким уровнем киберрисков, где трудно найти опытных специалистов по кибербезопасности, подобная схема защищенных подключений заметно упрощает развертывание системы обновления ПО. Как показали недавние случаи с вредоносными программами WannaCry и Equifax, отсутствие регулярной установки исправлений часто приводит к серьезным проблемам.

Благодаря современным технологиям, таким как Honeywell ICS Shield, защищенный удаленный доступ стал реальностью для более чем 6000 промышленных площадок по всему миру. Этот инструмент уже показал себя на практике: несколько лет его применяют крупнейшие поставщики промышленных решений. Каждый раз, когда поставщики осуществляют дистанционную поддержку клиентов, они используют ICS Shield для безопасного доступа,



и это никак не мешает работе оборудования и соответствует процедурам предоставления доступа, действующим у клиентов.

Регулярная установка обновлений и исправлений обеспечивает соблюдение законодательных требований по защите критической информационной инфраструктуры. Таким образом, консолидация управления техпроцессами для повышения эффективности производства одновременно является шагом к усилению кибербезопасности.

ЗАМЕНА ОБОРУДОВАНИЯ КАК СРЕДСТВО ПОВЫШЕНИЯ БЕЗОПАСНОСТИ

Тщательный контроль цифровых подключений позволяет устраниить риск атак через USB, но только в том случае, если на заводах стоит достаточно современное оборудование, поддерживающее рекомендованные средства обеспечения безопасности. В реальности многие заводы используют устаревшую инфраструктуру, у которой просто отсутствуют необходимые функции. Не стоит забывать, что ряд важных средств защиты был создан буквально в последние несколько лет. Например, сравнительно недавно были усилены алгоритмы шифрования и оптимизированы настройки по умолчанию. Большинство старых АСУ ТП, установленных несколько десятилетий назад, не имеют этих технологий, поскольку разрабатывались без учета современных угроз. Больше всего уязвимостей, как известно, есть в системе Windows XP, и тем не менее многие компании все еще пользуются решениями, функционирующими на этой устаревшей версии операционной системы.

Чтобы решить эту проблему, компании могут внедрять средства удаленного доступа и современное оборудование поэтапно. Например, на заводе можно обеспечить удаленный доступ к наиболее современным системам, а затем, постепенно обновляя парк устройств, подключать новое оборудование к единой системе защищенного удаленного доступа.

В случае если применение современных систем защищенного доступа невозможно, предприятия могут задействовать технические средства контроля, например средства проверки

USB-устройств, такие как Secure Media Exchange от Honeywell. Дав возможность специалистам на местах безопасно проводить обновления из проверенных источников с использованием современных технологий разведки угроз на USB-накопителях, компания может защитить заводы от аварийных простоев и одновременно обеспечить безопасность. В дальнейшем, когда компания будет вкладывать средства в модернизацию оборудования или в строительство новых объектов, она сможет развертывать системы защищенного удаленного доступа там, где появится такая возможность.

СПЕЦИАЛИСТЫ ПО КИБЕРБЕЗОПАСНОСТИ

Многие промышленные предприятия сталкиваются с нехваткой квалифицированных специалистов по кибербезопасности. Иногда у компаний достаточно сотрудников для текущего управления средствами безопасности, но не хватает опыта планирования стратегий защиты. И это неудивительно, ведь в цифровую эпоху, когда новые риски возникают ежедневно и даже ежеминутно, политики в области промышленной кибербезопасности быстро устаревают, а создавать новые без соответствующего опыта совсем непросто. На других предприятиях есть специалисты, способные разработать политику безопасности, но нет возможности непрерывно отслеживать ее соблюдение и контролировать ключевые показатели.

Чтобы избавить себя от решения кадровых проблем, компании могут заключить договор с поставщиками оборудования АСУ ТП на предоставление услуг в области защиты цифровых активов. В сочетании с современными технологиями защищенного удаленного доступа это позволяет выйти на новый уровень информационной безопасности.

В случае чрезвычайного происшествия компания-эксперт на аутсорсинге сможет оперативно восстановить рабочее состояние системы, поскольку у нее есть богатый опыт, эффективный план реагирования на аварийные ситуации и четкое распределение обязанностей.

Если компании будут учиться на исторических примерах, анализировать текущие условия, брать за основу лучшие практики и методы работы, то они справятся со всеми трудностями эпохи цифровых технологий и смогут обеспечить ответственный подход к управлению предприятием. В том числе, используя системы автоматизации и опыт специалистов по кибербезопасности, они сумеют добиться большей прозрачности и взять риски под контроль. Сегодня уже нет сомнений в том, что в цифровой век побеждает тот, кто заботится об информационной безопасности. ◆

ЛИТЕРАТУРА

1. www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf.

