Круглый стол

На пути к кибериммунизации промышленности

В круглом столе принимают участие

Александр ВИНЯВСКИЙ,
технологический евангелист по направлению «Кибериммунитет», «Лаборатория Касперского»

Максим ГОРИН,
руководитель ИТ-департамента, Первый Бит ЦО

Вячеслав КАСИМОВ,
директор департамента информационной безопасности, МКБ

Сергей ТУМАНОВ,
генеральный директор, ООО «СофтМолл»

Сейчас российская промышленность активно развивается: строятся новые заводы и дополнительные промышленные линии, модернизируются и автоматизируются старые. В этих условиях для новых технологических цепочек и предприятий в целом важно обеспечить эффективную защиту от кибератак. Именно поэтому новые производственные линии необходимо строить сразу на защищенных ИТ, которые получили название «кибериммунные системы», или «практическая ИБ». На круглом столе обсуждалось состояние рынка таких «защищенных по умолчанию» систем в России.

Насколько, по вашим оценкам, отечественные производители промышленных решений заботятся о встраивании тех или иных механизмов защиты? С чем связана такая ситуация?

Александр ВИНЯВСКИЙ

Риски кибербезопасности сегодня волнуют бизнес как никогда. По нашему исследованию, в 2022 г. более половины (53%) опрошенных компаний отказались от новых бизнес-проектов из-за рисков кибербезопасности. Особенно ярко эта проблема проявляется в промышленности, где киберугрозы могут выйти за пределы ИТ-контура в технологический и непосредственно повлиять на ход производственных процессов и физическую безопасность людей.

С учетом колоссального роста числа угроз (в 2022 г. обнаруживалось около 400 тыс. уникальных угроз в день) многим промышленным предприятиям становится все более очевидно, что встраивание механизмов защиты в сами системы крайне необходимо. Подход «Лаборатории Касперского» к обеспечению киберимунитета демонстрирует, как экономически эффективно создавать системы со встроенной безопасностью. Уже сейчас мы совместно с партнерами создаем коммерческие кибериммунные решения, среди которых IoT-шлюзы от компании «Апротех», IoT-контроллер от компании «ИСС». Подробнее о том, зачем нужен кибериммунитет и как он достигается на практике, мы рассказываем, например, в нашем блоге: https://os.kaspersky.ru/blog/.

Максим ГОРИН

За последние 1,5 года количество кибератак на российские компании увеличилось в несколько раз. Только в 2023 г. до 65% компаний столкнулись с угрозами кибербезопасности. Это вынуждает производителей промышленных решений уделять вопросам информационной безопасности серьезное внимание.

К сожалению, в разработке промышленных решений есть сложности, которые архитектурно либо технически не позволяют встроить те или иные механизмы защиты. Однако наметилась тенденция развития рынка продуктов, интегрирующихся в систему и обеспечивающих дополнительный уровень безопасности. К ним и проявляют интерес производители промышленных решений.

Вячеслав КАСИМОВ

Банковский опыт показывает, что есть три-четыре вендора, которые «фанатично» заботятся о защищенности своих решений, поддерживают программы SSDLC, выходят в багбаунти и проводят исследования безопасности своих продуктов. Базовые механизмы защиты есть практически везде. В промышленной сфере, на мой взгляд, ситуация хуже, так как в изолированных сегментах сети можно годами жить с уязвимостями и не догадываться о них, пока кто-нибудь не найдет лазейку из Интернета в сегменты с АСУТП. И это очевидно, поскольку пользователей систем в этой области, по понятным причинам, значительно меньше, чем в банковской сфере.

Сергей ТУМАНОВ

Тот факт, что производители промышленных решений стали заниматься вопросами информационной безопасности, сам по себе позитивный. Они, безусловно, заинтересованы в реализации такого функционала с учетом повышения конкурентных преимуществ и видимых плюсов эксплуатации. Толчком стал приказ ФСТЭК России № 31 от 14.03.2014, согласно которому предпочтения отдаются встроенным механизмам защиты. Однако нерешенным остается вопрос сертификации такого функционала, о чем производители в большинстве своем не заботятся.

Какова роль продуктов со встроенной защитой (киберимунных) в процессе импортозамещения? В каких проектах они более востребованы: при модернизации старых решений или построении новых?

Максим ГОРИН

Чем больше встроенных механизмов защиты производитель встраивает в свое решение, тем более конкурентным оно будет на рынке импортозамещения.

Сам тренд начал развиваться только 1,5 года назад. Поэтому большинство решений реализуются в новых проектах.

Вячеслав КАСИМОВ

Роль точно такая же, как и без встроенной защиты: в нее местами приходится верить, но там, где есть иные лидеры (антивирусная защита или контроль целостности, например), предпочтение всегда отдается им. Это удобнее, надежнее и «интегрируемее». «Делить» на востребованность в разрезе «модернизация – новое», на мой взгляд, некорректно, так как даже банальное замещение зарубежной ОС отечественной порождает, с одной стороны, регрессионные тестирования, с другой – доработки прикладных приложений. В конечном счете проект модернизации незначительно уступает проектам внедрения нового.

Для какого уровня промышленных систем более востребованы киберимунные продукты: для ПЛК, MES/SCADA или ERP? Почему?

Александр ВИНЯВСКИЙ

На всех упомянутых уровнях киберимунитет может обеспечить преимущества. Сейчас особую ценность представляет повышенная защита границы промышленной (OT) и ИТ-сред. Именно эту задачу решает наш киберимунный IoT-шлюз. Также существуют киберимунные тонкие клиенты, один из популярных сценариев использования которых – удаленное подключение к рабочим станциям оператора, инженера или технолога.

На всякий случай поясню, что под киберимунитетом мы

подразумеваем не абстрактную усиленную безопасность, а конкретную методологию, в соответствии с которой уже сегодня наши партнеры совместно с нами создают коммерческие решения. В сердце методологии – научные подходы и лучшие практики, сформированные на базе десятилетий мирового опыта. Технологическая основа – микроядерная операционная система KasperskyOS, которая соответствует принципам кибериммунитета «из коробки» и позволяет экономически эффективно создавать кибериммунные решения.

Максим ГОРИН

Перечисленные системы являются бизнес-критичными. Они предназначены для управления персоналом, данными и производственным оборудованием, а также сбором, обработкой, хранением и передачей информации. Это ключевые процессы в любой компании. Отказ или простой одной из систем в результате кибератаки приведет к серьезным финансовым и репутационным потерям бизнеса.

С помощью каких механизмов защиты проще реализовать требования отечественных регуляторов: встроенных или наложенных? В каком направлении изменились требования регуляторов за последний год?

Александр ВИНЯВСКИЙ

Достичь лучшего эффекта позволяет комбинация наложенных и встроенных средств защиты. При этом сам регулятор отдает предпочтение встроенным средствам защиты, об этом написано в документах регуляторов (например, приказ ФСТЭК № 239). Другое дело, что существуют сложности, связанные, в частности, с высокой стоимостью. Наша миссия – восполнить пробел, связанный со встроенной безопасностью. Сейчас мы ведем активную работу по поддержке создания российского государственного стандарта конструктивной информационной безопасности, который описывает принципы и требования к построению таких Secure by Design систем с безопасностью, встроенной на уровне архитектуры.

Максим ГОРИН

На мой взгляд, наложенных, так как архитектурно и технически проще защитить решение дополнительным механизмом, чем встраивать его в основной продукт. Сейчас появляется все больше решений для интеграции, например, системы поиска уязвимостей и их разрешений вроде BITsignal (https://bit-signal.ru/). Или различные DLP-системы, которые противодействуют утечке информации.

В связи с многочисленными взломами и утечками информации в крупном и среднем бизнесе за последние 1,5 года наблюдаем серьезный рост интереса частных и государственных компаний к решениям, которые обеспечивают информационную безопасность ИТ-инфраструктуры, данных о клиентах, информационных систем и ресурсов.

Вячеслав КАСИМОВ

Конечно же, наложенных. Невозможно встроенными решениями сделать сертифицированный файрволл и анализ трафика, передаваемого в сетевом окружении рядом с хостом.

Сергей ТУМАНОВ

Встраивая функционал ИБ в свои решения, производители тестируют его совместимость с основным функционалом оборудования. Как следствие, такие решения заведомо обеспечивают требуемые заказчиком характеристики процесса обработки информации. А вот задача тестирования на совместимость наложенных СЗИ с промышленными решениями зачастую ложится уже на плечи заказчиков. Для решений промышленности важно, чтобы система работала в режиме реального времени. Использование дополнительных наложенных механизмов защиты будет приводить к не всегда допустимым временным задержкам обработки и передачи данных. С этой точки зрения использование встроенных механизмов и выгоднее, и удобнее, кроме того, обеспечивает совместимость функционала. Но есть «обратная сторона», например, для реализации требований регуляторов по обеспечению безопасности значимых объектов КИИ СЗИ должны быть сертифицированы. Однако производители, обеспечивая встроенную защиту промышленных решений, зачастую не заботятся о сертификации, что приводит к неисполнению требований регуляторов.

Какие тенденции в создании кибериммунных решений вы бы хотели отметить? Чего не хватает для их массового использования?

Александр ВИНЯВСКИЙ

В мире сегодня наблюдается тренд на Secure by Design-системы. Компании из различных индустрий, регуляторы начинают остро осознавать неизбежность такой трансформации подходов к обеспечению безопасности киберфизических систем.

Например, в феврале текущего года Агентство по кибербезопасности и защите инфраструктуры США (CISA) сформулировало три принципа Secure by Design. У нас здесь есть преимущество, ведь в «Лаборатории Касперского» эти принципы давно сформулированы и создаются коммерческие продукты на их основе.

Особо следует отметить и экономический аспект. Хотя изначально стоимость кибериммунного

решения выше из-за дополнительных вложений на обеспечение безопасности, полная стоимость владения таким решением (TCO) оказывается ниже благодаря снижению затрат на обновления и поддержку.

Максим ГОРИН

Чаще всего производители промышленных решений прибегают к наложенным и уже существующим на рынке механизмам защиты своих решений, что позволяет быстро и без особых затрат обеспечить требуемый уровень защиты информационных систем.

В рамках нашей компании одним из уровней защиты является решение «Бит.Аутентификатор», который добавляет еще один шаг в авторизации, но значительно улучшает защищенность бизнеса. Это пример наложенного решения.

Встраивать механизмы защиты долго и дорого и в конечном результате серьезно увеличивает стоимость решений для клиента.

Вячеслав КАСИМОВ

Я бы говорил о хороших намерениях (в конце концов, систему, написанную без уязвимостей на всех ее слоях, взломать невозможно), но не самых эффективных реализациях. Для высокого качества требуется немного больше опыта, чем есть у компаний, создающих средства защиты. Тем не менее само направление правильное, способствует повышению защищенности конечных пользователей. Качество со временем придет, главное – не забрасывать эти начинания. ■

Интернет-реклама требует маркировки

1 сентября в России начнут штрафовать за интернет-рекламу без маркировки. Согласно поправкам к закону «О рекламе» организации и физические лица обязаны передавать данные о своих рекламных кампаниях в единую систему учета. Компания Kokoc Group провела опрос среди 100-тысячной базы МСП-клиентов и выяснила: несмотря на то что известно об этом законе стало давно, многие до сих пор не понимают, что им делать, чтобы избежать финансовых проблем. Поправки в закон «О рекламе» внесли год назад – всё это время действовал переходный период.

На вопрос, знают ли предприниматели, по каким из рекламных инструментов закон требует проводить маркировку и учёт, 35% опрошенных затруднились ответить. Только 55% респондентов слышали, что контекстная реклама тоже маркируется, 31% осведомлены, что маркировке подлежит медийная реклама, 29% известно про таргетированную рекламу, 21% – о том, что нужно получать токен для рекламных и PR-статей. Всего лишь 16% понимают, что нужно маркировать нативную рекламу (посевы), 8% – SEO. При этом 10% респондентов ошибочно думают, что материалы, рассылаемые по собственным базам инструментами CRM-маркетинга, требуют внешнего учета.

В реальность штрафов за рекламу не поверят 27% опрошенных, пока не увидят действие закона на практике. 26% респондентов еще даже не задумываются об этом. 47% признались, что наказания все же опасаются. Однако почти половина – 44% – не знают, с чего начать. 20% заняли выжидательную позицию. Примерно 35% респондентов находятся в активном поиске решения этих задач. Не многие компании сумели подготовиться и уже нашли специалистов: 9% пригласили партнера по вопросам маркировки рекламных форматов, 6% начали сотрудничать с экспертом по вопросам передачи отчётов, 5% будут советоваться с консультантом. И лишь 1% опрошенных пригласили в штат сотрудника, который занимается вопросами маркировки и отправляет отчёты. В рамках исследования выяснилось, что 99% опрошенных нуждаются в том или ином виде помощи. 59% достаточно короткой инструкции по этой теме. 28% хотели бы получить подробную консультацию на предмет конкретных действий, которые позволят избежать штрафов. 21% находятся в поиске партнера, который поможет обеспечить соблюдение требований закона. 11% готовы пригласить куратора, который научит сотрудников правильным действиям и будет их сопровождать еще некоторое время.