Что такое встраиваемые системы, и какая кибербезопасность им нужна

Как защищать встраиваемые системы

kaspersky активируй будущее

Почему это актуально?

Встраиваемые системы оперируют ценными данными (например, финансовыми или персональными) и поэтому представляют собой весьма привлекательную цель для киберпреступников.

Встраиваемые системы вокруг нас

Мы пользуемся встраиваемыми системами каждый день. Банкоматы, кассовые терминалы в магазинах, вендинговые автоматы, билетные киоски, медицинские компьютерные томографы, даже автоматические заправочные станции — все это специализированные машины на базе встраиваемых систем Windows или Linux.

Эти устройства оперируют ценными данными (например, финансовыми или персональными) и поэтому представляют весьма привлекательную цель для киберпреступников. Именно поэтому надежная защита таких устройств является жизненно необходимой для любой компании, имеющей их в своем арсенале.

В то же время о безопасности встраиваемых систем, в отличие от обычных офисных, компании задумываются не всегда или же этот вопрос отходит на второй план. Между тем, это очень важная и при этом очень нетривиальная задача, поскольку эти системы имеют свою специфику, которую необходимо принимать во внимание.

Встраиваемые системы: отрасли и типы устройств

Отрасли	Устройства
Финансовый сектор	Банкоматы
Транспорт и туризм (продажа билетов)	Билетные автоматы
Розничная торговля	Бензоколонки
Ресторанный и гостиничный бизнес	Кассы POS-терминалы
Здравоохранение	Медицинское оборудование
Государственный и некоммерческий сектор	Устаревшие компьютеры
Развлечения	Игровые автоматы

Особенности встраиваемых систем

Несмотря на значительное, на первый взгляд, сходство с обычными компьютерами, встраиваемые системы обладают рядом существенных отличий, которые необходимо учитывать при разработке защитной стратегии.

Модель использования

По этому аспекту типичная встраиваемая система кардинально отличается от обычного рабочего компьютера. Компьютер используется одним пользователем для широкого набора задач. Типичная встраиваемая система используется, чаще всего, неограниченным количеством пользователей, исполняя при этом очень небольшой спектр задач.

Есть и другие отличия. Например, взаимодействие с такими системами часто осуществляется с помощью специфических органов ввода (цифровая клавиатура, чувствительный экран с узкоспециализированным интерфейсом пользователя). Таким образом, введение произвольных данных и команд оказывается невозможным.

Порты обмена, позволяющие подключение внешней периферии, у таких устройств, как правило, доступны только для технических специалистов. Общение с внешним миром осуществляется через интернет, локальную сеть, а также с использованием таких функционально ограниченных хранилищ информации, как банковские карты.

При этом банкомат, очевидно, не будет использоваться для чтения электронной почты или посещения веб-сайтов — а значит, эти каналы не могут быть использованы для заражения. Однако возрастает значимость сетевого соединения. Этот канал — один из основных, используемых для атак на встраиваемые системы, ведь почти все типы встраиваемых систем имеют соединение с локальной сетью компании — а значит, проникнув туда, злоумышленник может через сеть «дотянуться» и до этих специализированных машин. Что касается портов, хакеру может помочь специфика физического расположения подобных устройств.

Физическое расположение

Подавляющее большинство программно-аппаратных комплексов (ПАК) на базе встраиваемых систем располагается в общественном пространстве, в полном согласии с моделью использования. От получения незапланированного доступа к элементам ПАК призваны защищать прочный стальной корпус и ограничения в способе взаимодействия с устройством.

Однако, поскольку никакое устройство невозможно сделать полностью необслуживаемым, любой самый прочный корпус открывается с помощью ключа — а значит, его может открыть и злоумышленник. Получив доступ к компьютерной части ПАК, он может подключить стандартные мышь и клавиатуру, накопитель с нужным ему зловредным ПО или даже с операционной системой, позволяющей загрузить ПАК в обход его собственной ОС. В некоторых случаях это может быть даже одноплатный компьютер, с помощью которого можно взламывать саму систему — или, например, анализировать команды, заставляющие диспенсер выдавать пользователю купюры.

Остальное — дело техники; нужно только внедрить в систему нужные хакеру инструменты и с их помощью заставить встроенный компьютер делать то, что ему угодно — от выдачи денег или осуществления теневых транзакций до похищения данных пользователя. Что угодно — если только встраиваемая система должным образом не защищена.

Вызовы с точки зрения защиты

Высокий риск непосредственного вмешательства в работу ПО, включая ОС, специализированного программного обеспечения и самого защитного решения.

Длительный срок использования и ограниченные системные ресурсы

Будучи построенными вокруг конкретной задачи, встраиваемые системы чаще имеют не более чем «необходимый и достаточный» уровень производительности процессора. А поскольку программно-аппаратные комплексы, использующие встраиваемые компьютерные системы, как правило, имеют долгий срок службы, встретить, например, работающий банкомат с не просто слабым, но и давно устаревшим «железом» отнюдь не является редкостью.

Вызовы для организации защиты

Устаревшее, слабое «железо» защищаемых устройств может представлять существенную проблему: для многих современных решений безопасности такая конфигурация будет явно недостаточной.

Устаревшее, уязвимое программное обеспечение

Долгая жизнь дорогостоящих ПАК на базе встроенных систем имеет еще один побочный эффект: устаревшее ПО. Скромная системная конфигурация часто просто не позволяет использовать более новую операционную систему, да и специализированное прикладное ПО новых версий на старой «операционке» неработает (или же его может просто не существовать). Следствием этого являются активно используемые системы, для которых обновлений безопасности просто больше не выпускается, а значит, любая уязвимость при отсутствии специальной защиты может эксплуатироваться злоумышленником.

Вызовы с точки зрения защиты

Повышенный риск атаки через уязвимости в ПО в сочетании с крайне ограниченным выбором защитных решений; найти современный продукт, который «согласится» работать на старой ОС, такой как Windows XP, крайне сложно.

Слабое интернет-соединение

Некоторые устройства, такие как банкоматы, билетные терминалы, автоматические топливные заправки, могут находиться в удаленных локациях, где нет проводного интернета, а беспроводной может работать медленно и со сбоями. Прикладное ПО рассчитано на подобный сценарий — поэтому, например, транзакции могут обслуживаться банком асинхронно, «когда связь позволит». А вот современные защитные решения зависят от хорошей связи гораздо сильнее. В стремлении уменьшить время установки и размер установленного ПО, они уменьшают объем локальных компонентов, взамен сильно опираясь на облачную инфраструктуру.

Вызовы с точки зрения защиты

Отсутствие постоянной надежной высокоскоростной связи предоставляет преступникам дополнительные сценарии компрометации транзакций. При этом эффективность многих современных решений, чрезмерно зависящих от связи с облачной инфраструктурой вендора, может быть значительно снижена.

Требования регуляторов

Большинство встраиваемых систем оперируют ценными финансовыми и персональными данными, поэтому работа с ними регулируется законодательно. Регулирующие органы требуют обязательного присутствия надежной защиты, чтобы максимально снизить риск инцидента и обеспечить наличие подробных данных для расследования, если инцидент все же произошел. При этом в списке рекомендуемых могут значиться некоторые специфические технологии, такие, как контроль целостности системы.

Вызовы с точки зрения защиты

Повышенные запросы к защите данных требуют высокой эффективности защиты, рекомендуя при этом технологии, которые в типичных решения класса EPP попросту недоступны или предоставляются только в решениях для серверов.

В поисках компромисса

Суммируя вышесказанное, можно заключить, что встроенные системы — многопользовательские, однозадачные, маломощные, имеют специфические векторы атак (сеть, прямой доступ к устройству). При этом они оперируют крайне ценными данными (помимо финансовых, это могут быть очень чувствительные персональные данные, как, например, в случае медоборудования), для которых важна не только конфиденциальность, но и неизменность.

Проблематика популярного подхода

Одновременно их традиционная защита может быть связана с целым рядом проблем, поскольку типичное решение класса EPP будет испытывать проблемы с работой на слабом «железе» и в принципе не заработает на устаревших ОС, которые до сих пор в ходу. Там, где такое решение все же запустится, возможны проблемы с производительностью и совместимостью.

Один из подходов, которые выбрали для себя многие производители защитных решений:

Основан на полном запрете всего, что не нужно для выполнения основной задачи устройств. Технология контроля приложений в режиме «запрет по умолчанию» просто блокирует любые программы, не занесенные изначально в так называемый «белый список».

В теории позволяет отказаться от механизмов детектирования угроз, ведь вредоносная программа просто не должна запуститься, а ресурсов такая схема требует совсем немного.

На практике может оказаться бессильным против некоторых типов атак. Например, против инъекции кода в легальный, уже запущенный процесс в памяти (в этом злоумышленникам могут помочь уязвимости в устаревшем ПО).

Да, в целом, хакерам на слабой системе доступно меньше возможностей, но бизнес, использующий встроенные системы, такой как банк или ретейлер, вряд ли будет использовать технику только одного поколения.

Что делать?

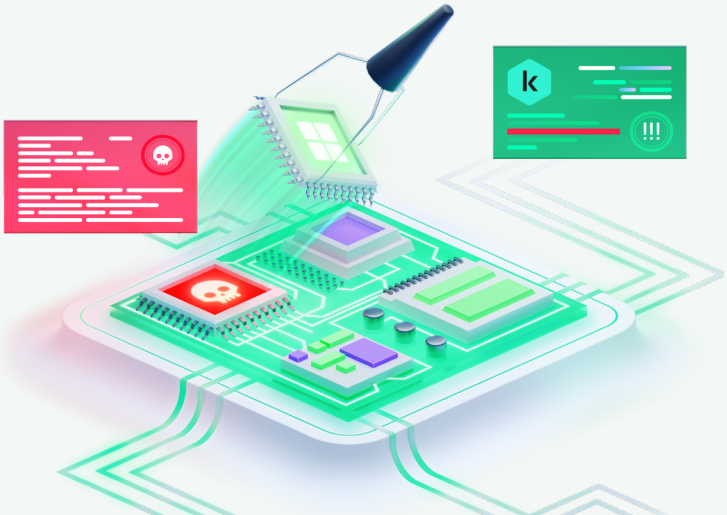
1

Использовать разные решения для слабых и более мощных систем?

Для слабых использовать решение на базе «запрета по умолчанию», а на более мощные пытаться внедрить обычный антивирус для рабочих станций, надеясь, что проблем с совместимостью удастся избежать.

2

Или попробовать найти действительно универсальную систему?



Особая защита для особых устройств

Если взглянуть на текущие предложения защиты для встраиваемых систем на рынке, большинство вендоров предлагают два варианта.

Вариант 1. «Экономное», ресурсоэффективное решение

Способно работать, в том числе, и на устаревших системах — но обеспечивает лишь простейшую однослойную защиту на основе технологии контроля приложений и режима «запрет по умолчанию» (Default Deny).

Помимо отсутствия инструментов для противостояния ряду типичных для встраиваемых систем атак, такое специализированное решение чаще всего стоит особняком и управляется отдельно от других продуктов экосистемы ИБ.

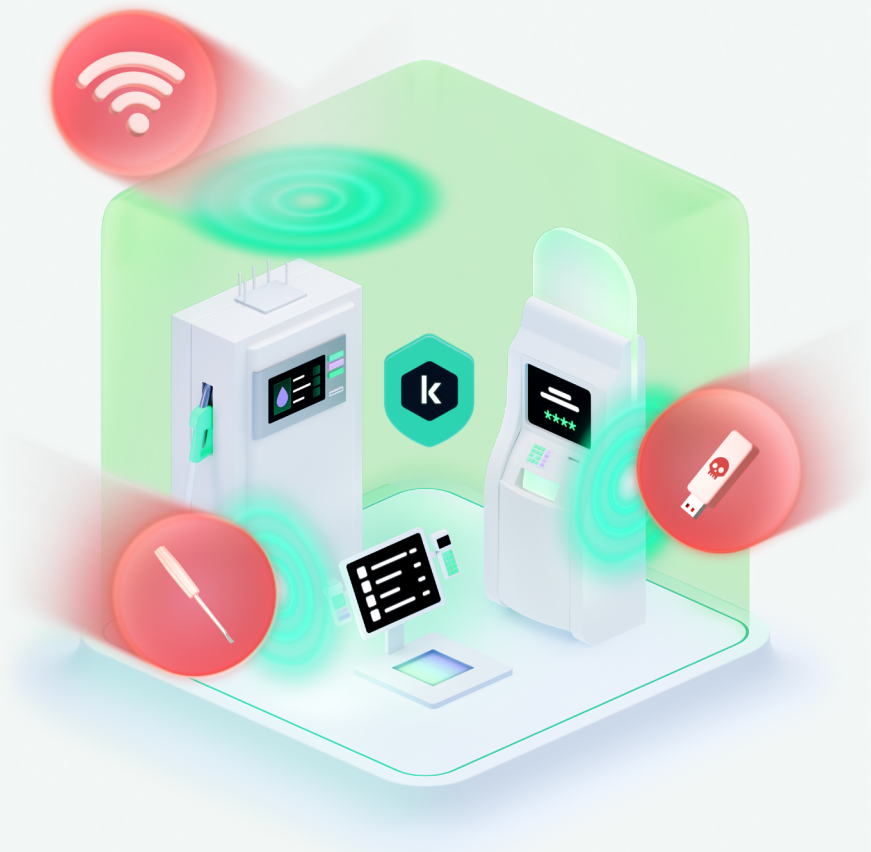
Вариант 2. Обычное решение класса Endpoint Security

Для встраиваемых систем большинство производителей предлагает использовать то же самое решение, что защищает обычные рабочие станции. Такое решение, несомненно, обладает современным стеком защитных технологий и может быть встроено в экосистему вендора, но, как правило, не учитывает указанную выше специфику встраиваемых систем.

Кроме того, такие решения эффективно работают только на самых современных и мощных ПАК, оставляя за бортом все еще работающие, но устаревшие устройства.

Вывод

Даже если использовать оба варианта одновременно, это не решит все проблемы. Кроме того, разнородные подходы к управлению (особенно если это решения от разных производителей) способны сильно осложнить работу администраторов ИТ и ИБ.



Каким должно быть идеальное решение?

Из чего же складывается образ идеального защитного решения, которое бы подошло для широкого спектра встраиваемых систем и сценариев их использования?

Решение должно:

Обеспечивать максимально возможный уровень защиты

В современных условиях, это означает наличие стека различных технологий для защиты от релевантного (то есть характерного для встроенных систем всех типов) набора векторов атак и используемых техник.

Обеспечивать максимально возможную защиту на системах любого уровня

Как старых и маломощных, так и современных, обладающих достаточным запасом производительности и памяти.

Однако, поскольку на слабом железе попросту невозможно физически запустить одновременно все, что есть в технологическом стеке, необходима возможность масштабирования.

Другими словами, решение должно позволять раздельное управление слоями защиты, отключая или задействуя тот набор, который дает максимальную защиту для конкретного набора «железа» и сценария использования системы.

Поддерживать наиболее популярные ОС

Популярные ОС, использующиеся для создания встраиваемых систем. Как минимум, это Windows и Linux.

Поддерживать устаревшие версии ОС

Устаревшие версии ОС, использующихся во все еще работающих встраиваемых системах.

Отвечать требованиям регуляторов

Иметь в своем защитном стеке рекомендуемые ими технологии и возможность подробного логирования событий в централизованной системе мониторинга событий безопасности (SIEM).

Быть тщательно проверено на совместимость

Как минимум, с типовыми конфигурациями встраиваемых систем разных типов.

В идеале — поставляться в составе программного-аппаратного комплекса (ПАК), все компоненты которого протестированы производителем (сборщиком) данного ПАК на беспроблемную совместную работу.

Иметь централизованное управление

В идеале — унифицированное с другими продуктами экосистемы вендора для создания единой системы безопасности, обеспечивающей наблюдение и защиту всех уровней ИТ-инфраструктуры компании через единую консоль.

Kaspersky Embedded System Security

Kaspersky Embedded Systems Security

Много лет назад, прежде чем прийти к пониманию, как должно выглядеть специализированное решение для защиты встраиваемых систем, «Лаборатория Касперского» начала с попыток использования для этой задачи приложений из состава линейки продуктов Kaspersky Security для бизнеса. Но скоро стало ясно, что использовать обычное приложение для полного спектра встраиваемых систем просто невозможно. Поэтому было принято решение разработать специализированное решение.

Результатом стало появление продукта Kaspersky Embedded Systems Security, с поддержкой сперва ОС Windows, а затем и ОС Linux.

Основные преимущества решения

Исключительно редкое сочетание

на мировом рынке многослойного технологического стека для разных платформ

Скромные требования

к системным ресурсам

Поддержка устаревших версий ОС

вплоть до Windows XP SP2

Часть богатой экосистемы

безопасности «Лаборатории Касперского»

Управление из той же консоли управления,

что и другие защитные продукты «Лаборатории Касперского»

Простая интеграция в существующие процессы

обеспечения информационной безопасности (как часть общей защитной стратегии компании)

Основные преимущества и возможности продукта

Подробнее

Технические подробности продукта для Windows

Подробнее

Технические подробности продукта для Linux

Подробнее

Kaspersky Embedded System Security

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее