Влияние трендов безопасности на испытательное оборудование

Почему информационная безопасность заботит не только гендиректора

АННОТАЦИЯ

В то время, как организации стараются укрепить свою защиту от угроз информационной безопасности, специализированные испытательные системы создают особые проблемы. Скомпрометированная испытательная система может существенно повлиять на репутацию и доходы организации, поэтому разумно предпринять шаги для уменьшения этого риска для бизнеса. Однако вызов заключается в том, чтобы учесть различия испытательных систем и традиционных IT-систем. В этой статье исследуются тренды информационной безопасности в промышленности, имеющие отношение к испытательным системам. Приведены реальные примеры, освещающие ключевые проблемы, и практические меры, которые вы можете предпринять для решения этих проблем. Кроме того, описывается, как NI, лидер в производстве испытательного и измерительного оборудования, а также программного обеспечения, содействует решению проблем безопасности.

Тренд 1: Применение методов безопасности традиционных IT-систем к испытательным системам

Представьте сценарий, слишком хорошо знакомый работающим в обрабатывающей промышленности. Телефон звонит в 2:15 ночи, вырывая вас из сна. Вам сообщают о событии, требующем вашего срочного внимания.

Производственная линия С остановилась из-за сбоя двух программируемых логических контроллеров (ПЛК), используемых в системе финишного тестирования продукции для проверки ее качества. Центр управления производством потерял связь с контроллерами 30 минут назад и не может определить, безопасно ли включать их снова. В этом месяце уже произошло три подобных инцидента, а теперь четвертый? Однако на этот раз ваша команда была готова и переместила производство на соседний завод со свободными мощностями, в надежде, что это поможет сократить производственные потери.

Несколькими днями спустя обнаруживается, что эти сбои были результатами случая нарушения безопасности компьютера. Но не атаки извне, а «огня по своим». IT-отдел недавно реализовал ночные сканирования всех сетевых устройств для оценки их безопасности – ранее испытательное оборудование использовалось без большинства протоколов IT, но руководство изменило политику, т.к. не могло далее допускать риск информационной безопасности от неконтролируемых сетевых устройств. Поскольку примитивные программные алгоритмы в ПЛК, скорее всего, были разработаны за десятки лет до используемого программного обеспечения системы безопасности, ночные сканирование перегрузили два ПЛК большим количеством сетевых пакетов, чем они могли обработать, что привело к реакции на ошибку: отключению.

Ключевые проблемы

Тренд применения опыта информационной безопасности к испытательным системам имеет смысл по ряду причин, особенно из-за увеличившегося количества случаев нарушения безопасности, использующих уязвимость неконтролируемых сетевых устройств. Ни один гендиректор не хочет оказаться тем человеком, чья система кассовых терминалов будет скомпрометирована атакой, вызванной контроллерами обогревательной и вентиляционной системы. Аналогично, никакой руководитель не потерпит больших производственных потерь, если испытательное оборудование подвергнется нападению через корпоративную информационную систему.

Вторая причина целесообразности данного тренда в том, что методы и технологии безопасности для IT-систем общего назначения более зрелые. У специалистов по IT-безопасности есть широкий диапазон технологий для защиты систем и обнаружения опасности, от сетевых сканеров и технологий обнаружения вторжения до антивирусов и агентов мониторинга настольных компьютеров. Естественный ответ заключается в расширении областей применения этих наилучших методов и технологий обеспечения безопасности на испытательные системы и устройства особого назначения, особенно если эти методы удовлетворяют регламентированным стандартам, например, NIST SP 800-171.

Однако данный тренд категорически нецелесообразен по крайней мере по двум причинам. Главным образом, IT открытые испытательные системы менее приемлемы даже небольшие изменения конфигурации. Пользователи IT-систем могут смириться с простоями и могут даже не заметить разницы в производительности системы, но в специализированных испытательных системах (особенно, которые используются в производстве) часто такое не допускается. Даже небольшие изменения в производительности из-за обновления системы безопасности или установки нового элемента защиты могут отрицательно повлиять на результаты испытания или даже на качество собранных тестовых данных. Аналогично, даже небольшой простой применяющихся на производстве испытательных систем может оказать значительное финансовое влияние на доходы организации.

Во-вторых, к испытательным системам часто предъявляются уникальные требования к безопасности. Как правило, на них запущено специализированное тестовое программное обеспечение, не используемое на других компьютерах организации, и они оборудованы специализированными периферийными устройствами, которые не рассматриваются стандартными технологиями информационной безопасности. Например, тестовые периферийные устройства, которым необходима калибровка для поддержания точности измерений, могут снизить или даже поставить под сомнение качество испытаний, если их калибровочные данные были умышленно или случайно изменены. Слепое применение методов информационной безопасности к таким испытательным системам может привести к ложному ощущению безопасности просто потому, что в них не рассматриваются уникальные риски информационной безопасности подобных систем.

Что вы можете сделать

Предпочтительный подход к безопасности испытательного оборудования включает два основных компонента. Во-первых, используйте данные для информирования о том, какие меры IT-безопасности вы используете для вашей испытательной системы и насколько интенсивно их принимаете. Это даст вам информацию, необходимую для привлечения IT-специалистов для оценки и управления рисками. Во-вторых, добавьте к этим мерам IT-безопасности специальные элементы защиты для испытательных систем, чтобы охватить уникальные риски. Это заполнит пробелы, которые не покрывают стандартные методы IT-безопасности.

Вы можете обратиться к ежегодному отчету Verizon Data Breach Investigations Report (DBIR) в качестве источника данных. В этом отчете Verizon анализирует данные по раскрытым угрозам информационной безопасности за прошлый календарный год. Часть отчета Verizon DBIR за 2016 год содержит анализ активных кибератак, пользующихся уязвимостями в патчах, выпускаемых основными поставщиками программного обеспечения (ПО). Хакеры используют методику, которая пользуется временем задержки между выпуском производителем патча с исправлениями и инсталляцией его на компьютер. Рекомпилируя патч поставщика, хакер узнает, где находится уязвимость в нескорректированном ПО и разрабатывает вредоносный код, эксплуатирующий эту уязвимость. Хакеры активно начинают разработку в пределах от двух до семи календарных дней после выпуска патча, сосредоточившись в основном на крупных поставщиках ПО.

Вы можете использовать эти данные для принятия более точного решения о рисках установки патчей на вашу испытательную систему. Для снижения риска устанавливайте патчи безопасности в течение 7 дней после их выпуска. Это значит, что вы должны следить за уведомлениями поставщика ПО, оценивать применимость патча и быстро восстанавливать затронутые системы. Во-вторых, минимизируйте программное обеспечение ваших испытательных систем. Потраченное на это время быстро окупится снижением издержек на установку патчей и восстановление системы. Эти шаги особенно важны для испытательных систем, подверженных более высокому риску, например, используемых на производстве и в промышленности.

Второй ключевой компонент касается использования элементов безопасности, специфичных для каждого поставщика. Например, учитывая, насколько критичны данные калибровки, параметры испытаний и тестовые последовательности для поддержания качества тестов, вы можете использовать такие технологии, как контроль целостности файлов и функций целостности калибровки, специально настроенные под вашу испытательную систему и ее компоненты. Аналогично вы можете обратиться к документации о безопасности от производителей вашей испытательной системы, чтобы принимать решения о покупке, проектировании и развертывании, которые обеспечивают наилучший уровень безопасности.

Тренд 2: Компромисс канала поставок

Новости о вредоносных программах, имевших целями промышленные системы управления, оказались неожиданны в 2014 году. Это не была работа хакеров, удаленно проникших сквозь защиту конкретного завода, или тайных агентов, установивших вирус на нефтезаводе. Вирус был установлен через полученное от поставщика программное обеспечение, содержавшее троян.

Изначально кампанию назвали "Энергетический медведь", поскольку ее целью были электростанции, и считалось, что она зародилась в России. Один аспект этой кампании включал канал поставок. Они напали на трех различных поставщиков ПО, на сайтах которых было доступно для скачивания ПО для промышленных систем управления. Получив доступ к файлам на сайте, хакеры изменили легальный инсталлятор ПО, вставив в него фрагмент вирусного кода, и сохранили файл на том же месте на сайте. Это был лишь вопрос времени, когда пользователи скачают и установят зараженное ПО. Экономическое влияние на поставщиков ПО и их покупателей неизвестно.

В качестве более сложного примера в 2010 году лаборатория Касперского обнаружила компрометацию канала поставок коммерческих жестких дисков нескольких поставщиков, начавшуюся еще в 2005. То, что они обнаружили, касалось прошивки контроллеров жесткого диска, которая, на первый взгляд, работала нормально. Однако она тайно сохраняла копию конфиденциальной информации в неиспользуемых областях энергонезависимой памяти, где содержалась прошивка. Поскольку измененная прошивка не имела возможностей обмена данными, можно сделать вывод, что оперативник забрал бы жесткий диск после списания для восстановления этой важной информации. Обратите внимание, что эту информацию можно было бы восстановить, даже если бы перед списанием содержимое жесткого диска было бы стерто.

Ключевые проблемы

Компрометация сайта кампании Energetic Bear свидетельствует, что целостность испытательной (и вообще любой) системы зависит от целостности ее компонентов в течение их жизненного цикла. Каждое место, где компоненты переходят из рук в руки или где они хранятся длительный период времени, предоставляет возможность для

компрометации. Жизненно важно создать чистый канал поставок, и не менее важны меры, гарантирующие защиту и обнаружение скомпрометированного компонента на каждой стадии.

Обнаруженная лабораторией Касперского компрометация жестких дисков указывает на то, что изощренные хакеры высокого уровня готовы залезть в процесс разработки поставщика для доступа к неопубликованному исходному коду. В этом случае, украденный исходный код поставщика использовался для создания полностью готовых к установке и функциональных вариантов, которые были установлены на скомпрометированные жесткие диски значительно позже того, как эти диски были приобретены и введены в эксплуатацию.

Никакой аспект продукта не является защищенным от скомпрометированного канала поставок. Любой инсталлятор, даже кажущихся незначительными плагинов и аддонов, может быть скомпрометирован кампанией Energetic Bear. Это оказалось верно и для кажущихся незначительными прошивок контроллеров жесткого диска, позволяющими осуществлять обновления в процессе эксплуатации без строгих проверок на безопасность.

Вы должны понимать компромисс между разнообразием поставщиков и стандартизацией при анализе рисков информационной безопасности. Преимущество диверсификации поставщиков – в уменьшении риска компрометации всей системы из-за скомпрометированных компонентов одного поставщика, но часто это преимущество перевешивается затратами на обучение персонала пользованию различными типами оборудования и управление отношениями с поставщиками. Стандартизация сокращает эти затраты, но вносит больший риск компрометации всей системы.

Что вы можете сделать

У стандартизации столько финансовых преимуществ, что сложно оправдать разнообразие поставщиков, разве только в сценариях с высоким уровнем риска. Наиболее целесообразный подход предполагает стандартизацию поставщиков, когда оценка безопасности канала поставок является важной частью критерия решений.

Большинство уже определилось со стандартизацией поставщиков. В этом случае и у вас, и у поставщика имеется сильная заинтересованность в сохранении этих отношений. Самое важное, что вы можете сделать для рассмотрения вопроса безопасности канала поставок – поговорить с вашими поставщиками. Спросите их о канале поставок и о том, что они делают для защиты целостности их продуктов в процессах разработки, производства и выполнения заказов. Любые выявленные вами слабые мест в их процессах могут помочь снизить ваш риск компрометации канала поставки и помочь вашим поставщикам укрепить свою безопасность. Без такого диалога обе стороны могут принимать непродуманные решения.

Помимо предотвращения, обговорите с вашими поставщиками наличие способов обнаружения произошедшей компрометации. При наличии достаточной мотивации и ресурсов скомпрометирована может быть любая система безопасности. Убедитесь, что в системе достаточно проверок, чтобы обнаружить случившуюся компрометацию, а также имеются четкие инструкции, что делать в этом случае. В таких случаях, как компрометация сайта Energetic Bear, механизмом обнаружения "last leg" (на последней стадии) может быть проверка цифровой подписи инсталлятора, но он должен отрабатываться совместно с соответствующими процедурами и тренировкой, приводящими к прерыванию инсталляции и обращению в службу поддержки. В таких случаях, как компрометация прошивки жесткого диска, запрос поставщику обновления прошивки выявит дыру в защите, но без возможности проверить целостность инсталлированной прошивки.

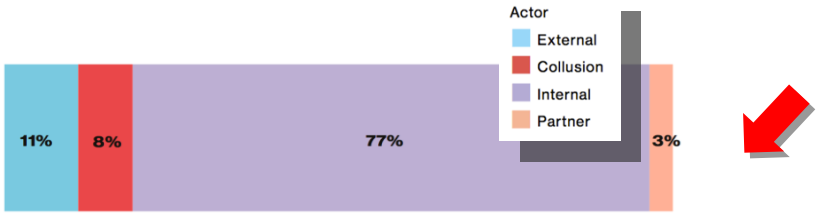
Тренд 3: Растущее внимание к угрозе изнутри

Наиболее вероятная причина усилившегося внимания к угрозе изнутри – утечка засекреченной разведывательной информации Агенства Национальной Безопасности, организованная Эдвардом Сноуденом. Экономический ущерб, понесенный от его действий индустрией высоких технологий США, оценивается от $22 до $35 миллиардов из-за возникшего недоверия к технологиям США. Но это не первый случай угрозы изнутри.

Тимоти Ллойд из компании "Omega Engineering" прославился своей деятельностью изнутри еще в 1996. На компьютерах стоял Microsoft Windows 95, и информационная безопасность редко (если вообще-когда либо) обсуждалась в средствах массовой информации. Для того времени то, чего удалось добиться Тимоти Ллойду как обладающему привилегиями сотруднику, было невероятно. Он работал системным администратором на производственном участке. Узнав, что его скоро уволят, он установил программную бомбу замедленного действия, которая систематически уничтожила все заводское ПО на контролируемых им системах. Бомба была запущена при первом входе администратора в сеть на следующий день после увольнения Ллойда. Экономический ущерб компании "Omega Engineering" составил несколько миллионов долларов и 80 рабочих мест. Компания едва не обанкротилась.

Ключевые проблемы

Ключевые проблемы в данной области многогранны и до сих пор являются серьезной темой для исследований. Проблемы включают внимание ко всем, кто имеет доступ к критическим испытательным системам, независимо от их статуса как работников или подрядчиков. Они включают четкую идентификацию наиболее критических аспектов бизнеса, людей, играющих роль в этих аспектах, и распределения полномочий между ними. Как правило, решения предполагают высокую степень контроля поведения, что может отрицательно повлиять на доверие между персоналом, необходимое для эффективной работы.



Авторами этих редких, но очень важных происшествий, как правило, были одиночки

Actor – исполнитель: External – внешний, Collusion – тайный, Internal – внутренний, Partner – партнер

% дыр по категориям опасности исполнителей, без учета неправильного применения

(Verizon DBIR, 2016)

Угрозы изнутри маловероятны, но оказывают сильное влияние, что подтверждает отчет Verizon DBIR за 2016 год. Из более 64 000 инцидентов с информационной безопасностью в 2015 году, только 172 включали злоупотребление со стороны собственных сотрудников. Более 75 процентов проникновения изнутри осуществлялись в одиночку без какой-либо внешней помощи или внутренних столкновений с другим персоналом.

Что вы можете сделать

За исключением систем с высоким уровнем критичности, лучше обдумывать угрозы изнутри после решения проблем, описанных в предыдущих трендах. В тех трендах приведены наиболее вероятные способы компрометации ваших испытательных систем.

Однако при проектировании систем с высоким уровнем критичности обдумайте угрозы изнутри как можно раньше. После определения наиболее чувствительных или критичных и ответственных аспектов системы разработайте решения по управлению привилегиями, которые разделяют обязанности между, как минимум, двумя ролями, которые не может выполнять один человек, и предотвращают любые попытки назначить обе обязанности одному человеку. Это снижает вероятность инцидента с угрозой изнутри с 77 процентов, совершаемых в одиночку, до 8 процентов, совершаемых сообща, судя по данным Verizon DBIR.

Куда двигаться дальше

Решение проблем информационной безопасности испытательной системы – сложная задача. Оно может либо завязнуть в бесконечном числе потенциальных угроз безопасности, либо никогда не начаться, потому что кажется чересчур сложной. В реальной жизни идеальная безопасность невозможна, поскольку любое решение теоретически может быть скомпрометировано при наличии достаточных ресурсов и времени. Вместо того, чтобы впадать в крайности, начните с определения приоритета проблем, основываясь на реалистичных сценариях и решайте в первую очередь наиболее важные из них, пользуясь здравым смыслом.

Начните с достижения консенсуса между вовлеченными людьми (например, вашим руководством, командой, сотрудниками отдела IT-безопасности и поставщиками) о том, что рассмотрение угроз информационной безопасности важно для всех. У такой отправной точки также есть преимущество повышения информированности всех соответствующих сотрудников о характере угроз информационной безопасности и возможных негативных последствиях случаев нарушения безопасности на их общий успех. Затем выделите время и деньги специально на проекты информационной безопасности, обучение и приобретение технологий. Поскольку угрозы информационной безопасности для испытательных систем реальны и представляют финансовый риск для вашей организации, следует выделить ресурсы организации на оценку и удовлетворение потребностей информационной безопасности. После реалистичной оценки влияния угрозы информационной безопасности на вашу деятельность, выделите пропорциональное количество ресурсов для удовлетворения этих нужд.