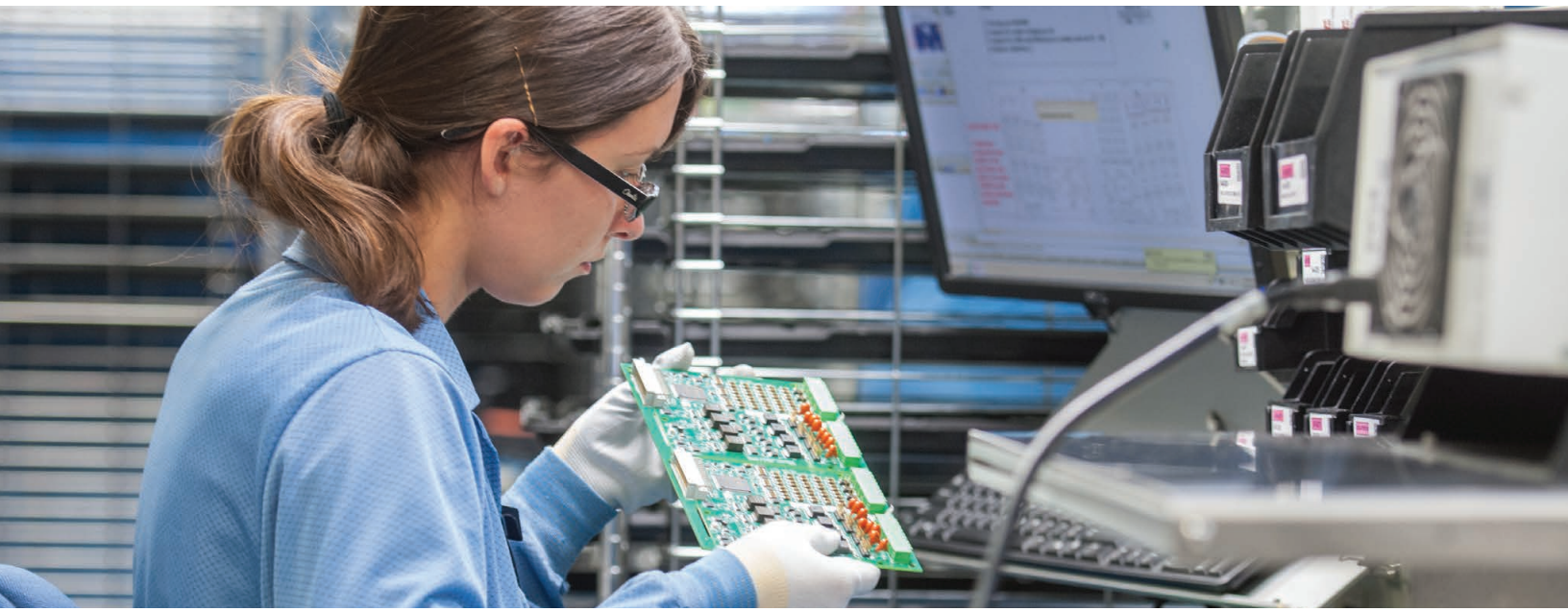
Безопасность цепочки поставок

Самые эффективные методы от SEL



Разработка планов управления рисками кибербезопасности цепочки поставок

Управление рисками цепочки поставок является важным компонентом комплексной программы обеспечения кибербезопасности. Вследствие взаимосвязанности и сложности цепочек поставок систематическая оценка рисков — необходимая, но вместе с тем трудная задача. В SEL безопасность, в том числе безопасность цепочки поставок, является главным приоритетом на протяжении более 30 лет, и мы считаем, что управление рисками цепочки поставок — основополагающий фактор для гарантии качества нашей продукции. Мы надеемся, что наши знания и опыт в этой области помогут вам в решении задач обеспечения кибербезопасности и соблюдения требований NERC CIP-013. В этом документе описаны процессы, которым следует SEL для обеспечения безопасности и надежности цепочки поставок продукции, которую мы доставляем клиентам по всему миру.

NERC CIP-013-1 «Кибербезопасность. Управление рисками цепочки поставок»

Назначение

«Снизить риски кибербезопасности для обеспечения надежной работы магистральной электрической системы (МЭС) путем внедрения мер безопасности в области управления рисками цепочки поставок в киберсистемы МЭС».

Дата вступления в силу

1 июля 2020 г.

Общие требования

- Оценка рисков, связанных с товарами или услугами поставщика (R1.1)
- Уведомление об инцидентах, идентифицированных поставщиком (R1.2.1)
- Координация реагирования на инциденты (R1.2.2)
- Уведомление от поставщика, когда удаленный доступ / посещение объекта не требуется (R1.2.3)
- Передача поставщиками информации об известных уязвимостях (R1.2.4)
- Проверка целостности и подлинности программного обеспечения (R1.2.5)
- Координация управления удаленным доступом (R1.2.6)

Меры SEL по обеспечению безопасности и надежности цепочки поставок

Цепочка поставок SEL является международной и сложной. Мы оцениваем риски нашей цепочки поставок, используя комплексный пятикомпонентный подход.

Часть 1. Создание надежных сетей поставок

Система рейтинга поставщиков

SEL использует систему рейтинга поставщиков, в которой каждый поставщик оценивается по цене, качеству, характеристикам, инновациям, условиям доставки и обслуживания. При составлении этого рейтинга мы оцениваем следующие области риска:

- Место производства
- Сроки выполнения заказов
- Финансовое состояние
- Методики пополнения запасов
- Вид технологии
- Своевременная доставка

Ежегодная конференция поставщиков

Каждый год мы проводим конференцию для компаний, которые поставляют нам комплектующие, оборудование и предоставляют услуги. В ходе этой конференции, которая проводится в нашей штаб-квартире в Пулмене, штат Вашингтон, мы делимся своими потребностями в технологической сфере и стратегическими целями на предстоящий год и определяем пути взаимовыгодного развития партнерских отношений с более чем 200 поставщиками с целью обеспечения непрерывных поставок качественных комплектующих частей.

Аудиты на объектах поставщиков

Наше взаимодействие с поставщиками предусматривает проведение регулярных аудитов на объектах поставщиков, в ходе которых мы проверяем, соответствуют ли их процессы качества и безопасности нашим требованиям.

Коллективный подход к отбору и мониторингу поставщиков

В SEL для управления рисками цепочки поставок используется межфункциональное взаимодействие. Отбор поставщиков является результатом совместной работы наших отделов разработки продукции, качества и закупок. Затем, аналогичным образом, группы специалистов из разных отделов занимаются подбором компонентов, постоянным мониторингом поставщиков и деталей, а также проведением аудитов на объектах поставщиков. При таком подходе ответственность за управление рисками делят между собой все.

Конфиденциальность

Мы не передаем наши ведомости материалов. Мы направляем прогнозные перечни с указанием номеров по каталогу, не имеющих прямой связи с устройствами. Чтобы избежать раскрытия информации о материалах, поставляемых другими поставщиками, мы никогда не рассылаем проектные схемы.

Поставщики поставщиков

Знать только наших поставщиков первого уровня для нас недостаточно. Мы просим наших поставщиков указывать своих поставщиков первого уровня, а также ключевые риски, стратегии их минимизации и методологии пополнения запасов.

Предпочтение поставщикам из США

Мы в максимально возможной степени стремимся закупать материалы в США.

Отбор транспортных компаний

Чтобы гарантировать нашим клиентам сроки доставки и целостность поставляемой продукции, мы применяем такие же процессы отбора к компаниям, занимающимся транспортировкой и отгрузкой.

Часть 2. Обеспечение целостности и доступности компонентов

Процесс проверки компонентов

Чтобы гарантировать целостность нашей продукции, мы проверяем характеристики приобретенных компонентов на соответствие спецификациям поставщика. По возможности мы закупаем компоненты напрямую у производителя или у официальных дистрибьюторов. В случае если компоненты поставляются независимыми дистрибьюторами, у нас имеется несколько методов обнаружения контрафактной продукции, которыми мы пользуемся. Среди них функциональное тестирование и микроскопия, рентгеновский контроль, рентгенофлуоресцентный анализ и проверки посредством вскрытия.

Постоянное тестирование

Мы тестируем нашу продукцию на протяжении всего производственного процесса. Если обнаруживаются отклонения в эксплуатационных характеристиках, мы ищем причины несоответствия.

Минимизация опасности прерывания цепочек поставок

Мы работаем с поставщиками, чтобы обеспечить наличие у нас и у них достаточного количества комплектующих частей специального назначения и потенциально дефицитных комплектующих частей. По возможности мы стремимся гарантировать, что критически важные компоненты могут быть получены как минимум от двух проверенных поставщиков.

Часть 3. Проверка безопасности программного обеспечения и микропрограмм

Исходный код

Мы не раскрываем исходный код или схемы. Мы разрабатываем большую часть программного обеспечения внутри компании, что дает преимущество в отношении контроля качества и возможность быстро вносить улучшения. Если мы добавляем в наши прошивки компоненты сторонних организаций, мы приобретаем исходный код. Доступ к коду имеют только инженеры отдела исследований и разработок SEL, работающие над данными проектами.

Внутреннее тестирование

У нас внедрен процесс, который включает в себя отзывы коллег-разработчиков и позитивное и негативное тестирование. Мы также используем автоматизированные инструменты проверки кода, чтобы определить потенциальные проблемы, которые разработчики могли упустить. Все тестирование выполняется внутри SEL сотрудниками SEL.

Цифровые подписи SEL и хэш-суммы

Подписывание программного обеспечения цифровой подписью позволяет гарантировать, что файлы программного обеспечения являются подлинными (созданы SEL) и не были изменены или подделаны. Пользователи Microsoft Windows могут проверять цифровые подписи программного обеспечения SEL с помощью проводника Windows (Windows Explorer). Аппаратное обеспечение SEL прозрачным образом проверяет целостность файлов микропрограмм в процессе обновления микропрограмм, используя встроенные в микропрограмму дополнительные данные. В случае несоответствия устройство SEL отклоняет файл прошивки и прерывает процесс обновления. В качестве дополнительного инструмента проверки целостности файлов прошивок SEL мы предлагаем хэши встроенного программного обеспечения.

Часть 4. Защита операций и контроль доступа

Физическая защита и информационная безопасность SEL

Наша внутренняя инфраструктура физической и информационной безопасности является многоуровневой и соответствует международно признанным стандартам. Это гарантирует, что все устройства и службы SEL работают надежным образом, а все данные, доверенные SEL, защищены. В целях повышения уровня кибербезопасности мы стремимся превосходить требования стандартов. Например, для устранения ряда распространенных сетевых уязвимостей на своем производстве мы внедрили программно-определяемые сети.

Наша система управления качеством сертифицирована по стандарту ISO 9001, а наши производственные процессы соответствуют классу 3 стандарта IPC-A-610, отвечая требованиям к высоконадежным электронным устройствам, используемых, например, в системах жизнеобеспечения и аэрокосмических системах.

Перед приемом на работу все сотрудники SEL проходят проверку биографии и проверку на наличие судимостей. Доступ к зданиям и помещениям SEL, где хранится конфиденциальная информация, защищен настраиваемыми средствами контроля доступа и контролируется видеокамерами и другими системами мониторинга. Оборудование и информационные системы SEL защищены от угроз физического характера и воздействий окружающей среды. Работа систем безопасности SEL контролируется и отлеживается в центре обеспечения безопасности, в котором круглосуточно и без выходных работают сотрудники SEL. С целью обнаружения и анализа потенциальных угроз наши сотрудники просматривают публичные и частные информационные потоки.

Принцип необходимого знания

Культура безопасности SEL основана на принципах минимальных привилегий, служебной необходимости и глубокоэшелонированной защиты. Мы ограничиваем доступ к проектам и информации внутри организации на основе служебной необходимости.

Защита информации клиентов

Мы защищаем информацию клиентов как в рамках экономических отношений, так и в рамках услуг технической поддержки. Это включает в себя защиту информации заказчика, содержащейся в устройствах, для которых оформлен возврат на ремонт. Когда мы выявляем нарушение безопасности, затрагивающее информацию клиентов, мы уведомляем клиентов и предлагаем полную поддержку при реализации мер реагирования.

Удаленный доступ

Когда для технической поддержки необходим удаленный доступ, мы используем систему мониторинга и оповещений для документирования и координации управления таким доступом.

Часть 5. Отслеживание дефектов качества и уязвимостей безопасности

Определение первопричин

Десятилетняя гарантия выступает для наших клиентов своего рода стимулом возвращать нам устройства в случае их выхода из строя. Затем мы можем проанализировать неполадки и найти причины отказа, что, в свою очередь, позволяет нам выявить недостатки в нашем процессе проектирования или процессе поставок и улучшить конструкцию наших устройств. Мы предоставляем бесплатную десятилетнюю гарантию на всю продукцию.

Отслеживание устройств на уровне компонентов

Мы ведем подробный учет всех производимых нами устройств и встроенных в них компонентов. Таким образом мы знаем, где используются устройства, и в случае чего можем уведомить клиентов о потенциальных проблемах с качеством или безопасностью.

Эксплуатационные бюллетени

При обнаружении потенциальных неполадок в работе устройства анализом проблемы занимается многопрофильная группа специалистов по проектированию. Если проблема несет в себе риск, мы информируем клиентов с помощью эксплуатационного бюллетеня.

Эксплуатационные бюллетени содержат объяснение выявленной проблемы, а также ее первопричины, последствия, наблюдаемую интенсивность отказов, устройства клиента, которых проблема может касаться, корректирующие меры и рекомендуемые действия по техническому обслуживанию. Эксплуатационные бюллетени позволяют клиенту принять обоснованное решение о том, как разрешить проблему. Мы направляем эксплуатационные бюллетени нашим клиентам как напрямую, так и через наших продавцов.

Уязвимости информационной безопасности

Эксплуатационный бюллетень, связанный с обнаруженной в устройствах уязвимостью безопасности, классифицируется как «Уязвимость безопасности». Наши специалисты разрабатывают рекомендуемые меры по исправлению уязвимости безопасности устройства и включают их в соответствующий эксплуатационный бюллетень.

Отраслевые проекты

Мы участвуем в различных государственных проектах и мероприятиях по разработке стандартов, чтобы знать о самых эффективных методиках, вносить свой вклад в развитие отрасли и владеть последней информацией о требованиях, предъявляемых к нашим клиентам. Помимо этого, мы используем руководящие документы, такие как правила по управлению кибербезопасностью NIST, для улучшения наших собственных процессов и средств контроля и формирования согласованных отраслевых практик.

Действующая политика обеспечения безопасности SEL

Политика SEL в области качества состоит в том, чтобы «постичь, создать и упростить». Она отражает нашу нацеленность на изучение возможностей, анализ проблем и создание инновационных решений, которые просты, надежны и безопасны. Управление рисками безопасности является частью повседневных обязанностей руководителей SEL. Они отслеживают новые факторы, потенциальные опасные для цепочки поставок и операций SEL, и вносят соответствующие коррективы в нашу работу.

SEL SCHWEITZER ENGINEERING LABORATORIES

Повышение безопасности, надежности и экономичности использования электроэнергии

+1.509.332.1890 | info@selinc.com | selinc.com/ru

20211130

WORLDWIDE 10 years WARRANTY