Общая информация

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760, Остфильдерн,
Германия
Германия
www.pilz.com

16 мая 2024 г.

Защита для компаний, оборудования и продукции

Промышленная и информационная безопасность — Комплексный подход

Остфильдерн, 16 мая 2024 г. — **Инциденты информационной безопасности больше не затрагивают только ИТ-системы, но все чаще также и производственную среду (эксплуатационные технологии). Инциденты в области информационной безопасности в промышленности включают в себя не только направленные атаки, но и непреднамеренные манипуляции. Миссия информационной безопасности на производстве — гарантировать доступность установок и оборудования, а также целостность и конфиденциальность данных и процессов на машине. В конечном счете, если компании не контролируют свои данные, то на карту поставлена безопасность как компании, так и сотрудников: без защиты данных нет промышленной безопасности, а без промышленной безопасности люди не защищены!**

Законодатель ЕС отреагировал на растущий уровень угроз: на корпоративном уровне **Директива по сетевой и информационной безопасности NIS 2** требует комплексного внедрения системы управления информационной безопасностью.

Новое Положение о машинном оборудовании 2023/1230 теперь предусматривает защиту от манипуляций для установок и оборудования и требует принятия мер безопасности для частей машины, которые влияют на функциональную безопасность.

Закон о киберустойчивости (CRA) требует принятия мер информационной безопасности для продуктов с цифровыми элементами. К ним относятся контроллеры, системы ввода-вывода и другие компоненты, используемые в машинном оборудовании.

Компании, оборудование и продукты — На каждом уровне производители машин и операторы сталкиваются с различными проблемами и правовыми рамками.

Независимо от того, что законодатель делает информационную безопасность обязательной, существует ряд веских причин заняться этим вопросом заранее и получить консультацию. Это связано с тем, что многие процедуры и факторы работы оборудования способствуют манипуляциям и требуют срочного изучения и изменения. Например, длительный срок службы оборудования часто приводит к тому, что соответствующие системы устаревают и в какой-то момент перестают соответствовать современным стандартам информационной безопасности. В этих системах есть бреши в защите данных, которые уже невозможно закрыть, поскольку поставщик прекратил предоставлять обновления информационной безопасности. Зачастую защиту от вредоносного ПО невозможно реализовать на конечных устройствах, поскольку некоторые из них слишком устарели, и в результате их производительность снизится, что потенциально может привести к простоям производства.

Комплексный пакет услуг от Pilz

Конечной целью является защита ведения бизнеса, но для этого компаниям необходимо преодолеть множество проблем: от выявления действующих законодательных требований,

обнаружения и устранения слабых мест в системах до повышения осведомленности и обучения сотрудников, а также до последующего осуществления контроля. Поскольку безопасность — это цель, которая постоянно меняется, также необходима регулярная проверка состояния оборудования с точки зрения информационной безопасности.

Компания по автоматизации Pilz подготовилась к этим требованиям и разработала пакет услуг для производителей машин и пользователей по всему миру, который комплексно включает в себя все аспекты защиты человека и машины. Услуги варьируются от базовой информации, ориентационных руководств и обучения до Консалтинговой услуги по информационной безопасности (ISCS), в рамках которой реализуются актуальные проекты.

В рамках программы «CESA — сертифицированный эксперт по информационной безопасности в автоматизации», начиная с прошлого года компания Pilz предлагает двухдневный экспертный курс, который дает слушателям конкретные знания в области информационной безопасности в соответствии с актуальным состоянием стандартов. Кроме того, обучение охватывает практические меры по снижению рисков, такие как контроль доступа, повышение безопасности сети с использованием технических средств и организационных мер для предотвращения рисков в отношении защиты данных. Когда участники сдают тест, они получают сертификат TÜV NORD «CESA — Сертифицированный эксперт в области информационной безопасности в автоматизации», который признается во всем мире.

С помощью новой консультационной услуги по информационной безопасности (ISCS) компания Pilz расширяет возможности проверки оборудования, чтобы создать целостный подход к обеспечению промышленной и информационной безопасности. Компания Pilz разработала пакет услуг, основанный на проверенной методологии обеспечения функциональной безопасности оборудования и серии стандартов безопасности IEC 62443. Воспользовавшись этой услугой, компании будут хорошо оснащены с точки зрения информационной безопасности и будут соответствовать текущим законодательным требованиям.

Четыре модуля для большей информационной безопасности

ISCS состоит из четырех модулей: «Анализ требований к защите», «Оценка рисков информационной безопасности», «Концепция информационной безопасности» и «Проверка системы информационной безопасности».

В ходе анализа требований к защите эксперты Pilz посещают компанию, чтобы определить требования к защите отдельных «активов» на заводе или оборудовании, а также цели их защиты. Второй шаг — это оценка рисков, при которой рассматриваются все риски вместе с вероятностью их возникновения для каждого подраздела на протяжении всего жизненного цикла системы. Затем эксперты Pilz встречаются с клиентом, чтобы обсудить подходы к смягчению выявленных рисков и потенциальных опасностей.

На третьем этапе эксперты Pilz создают Концепцию информационной безопасности, включающую стратегии и меры по защите и снижению рисков, возникающих в результате атак,

манипуляций и неправильного использования. Кроме того, создаются политики, правила и рекомендации для продолжения безопасной работы или структуры системы. Последний этап — проверка системы информационной безопасности — проверяет эффективность реализованных контрмер.

Обезопасьте доступность машины

Консультационная услуга по информационной безопасности помогает смягчить или предотвратить кибератаки. Количество нарушений информационной безопасности, спровоцированных непреднамеренно, также снижается. В свою очередь, это повышает эксплуатационную готовность оборудования и в конечном итоге приводит к экономии затрат и сохранению экономической эффективности.

Прежде всего, ISCS обеспечивает применение соответствующих мер безопасности для защиты людей, находящихся на машине. Потому что нарушение информационной безопасности может помешать поддержанию мер безопасности машин. Например, световая завеса перед оборудованием гарантирует, что операторы не попадут в опасную зону. Однако, если злоумышленник сможет повлиять на соответствующий контроллер и механизм, защитная функция световой завесы больше не может быть гарантирована. Защита данных обеспечивает безопасность машин!

Таким образом, производители машин и пользователи получают пакет услуг от Pilz, в котором учтены все аспекты защиты человека и машин.

Поэтому для фактического внедрения на машине имеет смысл рассматривать промышленную и информационную безопасность

вместе. Потому что: без защиты данных нет безопасности машин, а без безопасности машин люди не защищены!

Четкий контроль: кто и что может делать на машине?

Безопасность машины и ее операторов зависит от контроля доступа — будь то люди или сеть. Точки входа должны быть защищены от несанкционированного доступа, чтобы никто не находился в опасной зоне, например, во время работы машины. Если авторизованный оператор станка находится в этой опасной зоне в целях технического обслуживания, важно обеспечить, чтобы никто другой не имел доступа к установке в то же время. В противном случае даже эксплуатация или техническое обслуживание установки с благими намерениями — будь то на площадке или через сеть — может иметь фатальные последствия.

Идентификация и управление доступом (I.A.M.) является важным элементом, который четко регулирует разрешения и доступ к установкам и оборудованию в компаниях. Сюда относятся организационные меры и спецификации, а также соответствующие функции промышленной безопасности и защиты информации. Система разрешений доступа, такая как PITreader от Pilz, представляет собой соответствующий компонент продукта. Это означает, что пользователи могут удовлетворить требования в отношении защиты сотрудников, защиты ответственности, максимальной производительности и защиты данных.

Благодаря системе выбора режима работы и контроля доступа PITmode Fusion компания Pilz предлагает функционально безопасный выбор режима работы и контроль разрешений доступа к установкам и оборудованию. Каждому оператору

предоставляется транспондер с RFID-кодом, который содержит доступ к возможностям машины, соответствующим его обязанностям и квалификации. Таким образом, установка может эксплуатироваться и контролироваться только уполномоченным персоналом в определенных режимах работы. Это обеспечивает высокую степень защиты от непреднамеренных действий и манипуляций.

Добавьте компоненты модульной системы безопасности защитных ограждений к системе выбора режима работы и разрешения доступа, и в результате вы получите целостную концепцию доступа к машине — с точки зрения промышленной безопасности и защиты данных.

Лучшая защита дверей ограждений бесполезна, если данные, ноу-хау и операции недостаточно защищены от несанкционированного доступа и манипуляций, а посторонний злоумышленник может проникнуть в систему управления.

Промышленный межсетевой экран защищает от доступа извне

Задача промышленного межсетевого экрана SecurityBridge от Pilz — защитить от внешнего доступа к сетям автоматизации. Он контролирует трафик данных между ПК и контроллером и, таким образом, снижает вероятность хакерских атак и манипуляций. SecurityBridge защищает не только контроллеры Pilz, но и контроллеры сторонних производителей от несанкционированного доступа.

Компания Pilz убеждена, что только целостный подход к промышленной и информационной безопасности может гарантировать комплексную защиту человека и машины.

Компания больше не решает, хочет ли она обеспечивать информационную безопасность и в какой степени. Это теперь является юридическим требованием. В инжиниринге информационная безопасность в промышленности является не только задачей отдела информационных технологий, но и неотъемлемой частью проектирования и строительства. Ретроспективная реализация защиты данных сложна и обычно означает снижение удобства для пользователя, функциональности и производительности.

((Количество знаков: 10 173))

((Блок:))

Обзор законодательства ЕС в сфере информационной безопасности

В частности, в Европе законодатели отреагировали на уровень угрозы принятием ряда законов. В результате в Европе действуют самые строгие требования в мире. Но уже существуют договоренности с другими странами, и там такие законы тоже будут приняты. Поэтому следует ожидать глобальной гармонизации информационной безопасности.

NIS 2: Больше обязательств для компаний

NIS (сетевая и информационная безопасность) – это директива Европейского союза, направленная на укрепление кибербезопасности. Эта директива существует с 2016 года и до сих пор применялась к поставщикам критически важной инфраструктуры, включая энергетику, транспорт, банки и

финансы, здравоохранение, снабжение и распределение питьевой воды и цифровую инфраструктуру. Поставщики в этих секторах должны были внедрить «соответствующие меры информационной безопасности» и сообщать о любых серьезных инцидентах, связанных с кибербезопасностью. В будущем новая директива по сетевой и информационной безопасности 2 EU 2022/2555 (NIS 2) обязывает многие другие компании принимать меры по управлению рисками в сфере кибербезопасности. NIS 2 расширяет секторы, добавляя, например, производство / реализацию промышленных товаров и товаров производственного назначения, включая машиностроение и производителей электрооборудования.

Требования включают анализ рисков и концепции безопасности информационных систем, защиту цепочки поставок и безопасность персонала. Концепции контроля доступа и управления установками являются еще одним требованием, наряду с обязательным обучением руководителей.

Директива была принята в конце 2022 года Европейским парламентом и Советом ЕС. Как и все директивы ЕС, NIS 2 не вступает в силу немедленно и не имеет обязательной силы в государствах-членах ЕС, но должна быть включена во внутреннее законодательство стран-членов. Государства-члены ЕС должны до 18.10.2024 внедрить директиву во внутреннее законодательство. Компаниям было бы целесообразно разобраться с NIS 2 как можно скорее и провести комплексную оценку информационной безопасности компании. Например, сюда входит разработка Системы управления информационной безопасностью (ISMS). В этом контексте полезной является

сертификация по стандарту информационной безопасности ISO 27001.

NIS 2, на примере ветряных турбин: С NIS 2 производители оборудования, такие как производители электростанций (например, ветряных турбин), также должны будут соответствовать требованиям в будущем. В свою очередь производителям ветряных турбин нужны решения по автоматизации, контроллеры или датчики. Начиная с определенного размера, производители электрических компонентов также подпадают под NIS 2. А поскольку NIS 2 также предусматривает, что поставщики принимаются во внимание, такая компания, как Pilz, также должна заботиться о безопасности цепочек поставок и предъявлять требования к своим поставщикам. Таким образом, NIS 2 охватывает всю цепочку поставок.

Новый регламент в отношении машинного оборудования: нет безопасности - нет маркировки CE.

Директива по машиностроению 2006/42/EC имеет особое значение с точки зрения функциональной безопасности машин.

Для ввоза техники в Европу машиностроителям всегда приходилось проходить соответствующую процедуру оценки соответствия, завершающуюся получением маркировки CE.

Спецификации, переизданные в июне 2023 года в виде Регламента по машинному оборудованию, были обновлены в соответствии с уровнем новейших достижений науки и техники. Поскольку это регламент, его не нужно сначала преобразовывать в национальный закон. У производителей машин есть время до

20.01.2027, чтобы адаптироваться к новым требованиям и соответствовать им с ключевой даты.

Регламент по машинному оборудованию заменяет существующую Директиву по машинному оборудованию и, в отличие от нее, делает меры по кибербезопасности обязательными. Если Директива по машинному оборудованию рассматривала исключительно безопасность машин, Регламент добавляет целью обеспечение информационной безопасности в рамках «Основных требований по охране труда и технике безопасности (EHSR)», раздел «Защита от нарушений»: Функции безопасности машины не должны подвергаться риску из-за нарушений, преднамеренных или непреднамеренных.

Этот новый путь к маркировке CE поднимает ряд новых проблем для производителей и операторов машин, поскольку им придется пересмотреть существующие концепции промышленной и информационной безопасности.

Закон о киберустойчивости: Безопасность на протяжении всего жизненного цикла продукта

Помимо проверки компании и оборудования абсолютно необходимо также реализовать меры информационной безопасности непосредственно в устройствах (например, в контроллерах). В сентябре 2022 г. Европейская комиссия представила проект постановления, направленного на повышение кибербезопасности продуктов. Этот Закон об устойчивости к угрозам кибербезопасности направлен на производителей продуктов с цифровыми элементами (аппаратное и программное обеспечение), которые способны

взаимодействовать с другими продуктами. Это затрагивает продукты из сегмента B2C, такие как смартфоны или роботы-пылесосы, а также продукты из сегмента B2B, такие как контроллеры и датчики, а также чисто программные продукты, такие как операционные системы или сами машины.

Насколько велико будет влияние Закона о киберустойчивости на самом деле, зависит от критериев, которые в конечном итоге будут установлены для классификации продуктов. В соответствии с Законом о киберустойчивости на рынке могут размещаться только продукты, гарантирующие надлежащий уровень кибербезопасности — и это на протяжении всего жизненного цикла продукта. Таким образом, информационная безопасность начинается с разработки продукта. Вот почему в течение нескольких лет компания Pilz также согласовывала свои процессы разработки с IEC 62443-4-1 «Информационная безопасность систем промышленной автоматизации и управления – Часть 4-1: Требования к жизненному циклу разработки безопасной продукции», и разработала, например, SecurityBridge, что позволяет наглядным образом подтвердить безопасность разработки.

((Количество знаков: 5 826))

Рисунки

Рис. 1

Grafik_aus_Prospekt_Schulungen_mit_Pilz_3c_en_ppt

Универсальное решение для обеспечения промышленной безопасности и защиты данных: Pilz предлагает комплексный пакет решений, включающий услуги и продукты для информационной безопасности оборудования. (Фото: © Pilz GmbH & Co. KG)

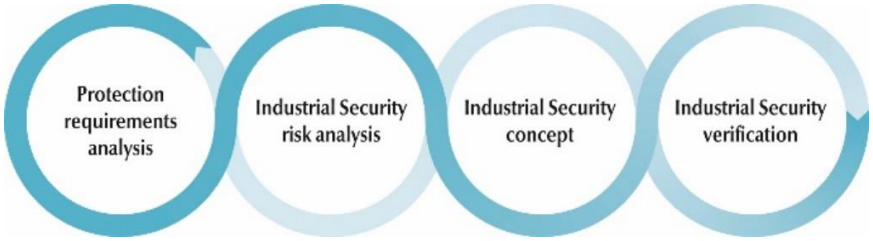
Рис. 2:

F_Services_ISCS_two_men_tablet_in_discussion_get1150297892_cold1

Pilz запускает консалтинговую услугу по информационной безопасности, помогая компаниям защитить данные своих предприятий и оборудования. (Фото: © Westend61/[westend61] via Getty Images, © Pilz GmbH & Co. KG)

Рис. 3:

G_Cycle_Industrial_Security_en



Консультационная услуга по информационной безопасности от Pilz состоит из четырех модулей: «Анализ требований к защите», «Оценка рисков информационной безопасности», «Концепция информационной безопасности» и «Проверка системы информационной безопасности». (Фото: © Pilz GmbH & Co. KG)

Рис. 4:

F_Press_IAM_Man_using_PITreader_Key_Get1169337234_Get1169337153_cold1

Комплексное управление идентификацией и доступом контролирует доступ к системе, обеспечивая тем самым целостность функций и мер безопасности — включая промышленную и информационную безопасность. (Фото: © Westend61/[Westend61] via Getty Images, © Pilz GmbH & Co. KG)

Рис. 5:

F_security_robot_man_virtual_world_Fot208731449_cold1_2019_06

Информационная безопасность в промышленности – защита производственных предприятий от намеренных или случайных сбоев. Цель состоит в том, чтобы гарантировать эксплуатационную готовность оборудования и машин, а также целостность и конфиденциальность данных и процессов на машине. (Фото: © ipopba/Fotolia.com; © Pilz GmbH & Co. KG)

Pilz — Дух безопасности

Компания Pilz является мировым поставщиком изделий, систем и услуг в области автоматизации. Будучи флагманом в области безопасной автоматизации, компания Pilz обеспечивает безопасность для человека, оборудования и окружающей среды. Основанная в 1948 году, сегодня семейная компания с головным офисом в Остфильдерне — это 2500 сотрудников в 42 дочерних компаниях и филиалах.

Компания-технологический лидер предлагает комплексные решения по автоматизации для обеспечения промышленной и информационной безопасности машинного оборудования. Сюда входят датчики, системы управления и приводная техника, а также устройства для промышленной связи, диагностики и визуализации. В международный спектр услуг также входят консалтинг, инжиниринг и обучение. Помимо машиностроения, решения Pilz используются во многих отраслях, например, во внутренней логистике, упаковочной промышленности и на железнодорожном транспорте, или в робототехнике.

www.pilz.com

Компания Pilz в социальных сетях:

На наших каналах в социальных сетях мы предоставляем справочную информацию о компании и людях, которые работают в Pilz, а также информируем о последних новостях из области автоматизации.

www.pilz.com/facebook
www.pilz.com/X
www.pilz.com/xing
www.pilz.com/youtube
www.pilz.com/linkedin

Контактные лица для прессы:

Мартин Курт

Корпоративная и техническая пресса
Тел.: +49 711 3409-158
m.kurth@pilz.de

Сабина Каррер

Техническая и корпоративная пресса
Тел.: +49 711 3409-7009
s.skaletz-karrer@pilz.de

Ева Рёсле

Техническая пресса

Тел.: +49 711 3409-7147
e.roessle@pilz.de

Хансйорг Шперлинг-Вольгемут
Руководство конференциями и презентациями
Тел.: +49 711 3409-239
h.sperling@pilz.de