20.05.2025

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern
Германия
https://www.pilz.com

Сообщение для Прессы

Информационная безопасность — это вопрос управления: как компании начинают работу в этом направлении

Остфильдерн, 20.05.2025 - **Симон Нутц, консультант по информационной безопасности в промышленности**

«Информационная безопасность? Это не наша забота!» — это по-прежнему распространенный ответ производителей и операторов машин на вопрос об информационной безопасности. «Наш ИТ-отдел отвечает за безопасность», — добавляют они слегка извиняющимся тоном. Однако на практике ИТ-специалистам не хватает специальных знаний, особенно в отношении сетей автоматизации. С другой стороны, инженеры-проектировщики и даже менеджеры по охране труда и технике безопасности (ОТ и ПБ) не знают, как решать вопросы кибербезопасности. Как же подготовиться к угрозам информационной безопасности в промышленности?

Применение Регламента по машиному оборудованию (MR) является обязательным в Европейском Союзе с января 2027 года. Он распространяется на все компании, желающие импортировать или эксплуатировать машинное оборудование в ЕС. В Регламенте по машинному оборудованию прописана информационная безопасность в промышленности в виде мер защиты от злоупотреблений. Таким образом, информационная безопасность в промышленности становится критически важной для бизнеса и, следовательно, задачей для руководства. Руководство должно обеспечить прочное закрепление принципов информационной безопасности в промышленности в компании.

Соберите всех за одним столом

Чтобы добиться успеха, первым шагом является объединение всех участников. Для машиностроителей это ИТ-специалисты, специалисты по разработке/проектированию, а также, если таковые имеются, лица, отвечающие за информационную безопасность (например, Начальник управления информационной безопасности). Для пользователей это ИТ-отдел, Отдел производственных технологий, Руководство производственного отдела, менеджер по ОТ и ТБ, а также Начальник управления информационной безопасности.

Первый этап — накопление знаний и выработка общего понимания информационной безопасности: какие правовые обязательства возлагаются на отрасль промышленности, производящую установки и машинное оборудование? Как связаны безопасность машин и защита данных? Где встречаются интерфейсы IT и OT?

На втором этапе эти междисциплинарные команды разрабатывают подходящую стратегию для компании, включая концепцию ее внедрения. Речь идет о поиске позиции во внутренней структуре: где будут находиться обязанности в будущем? Как выглядит топология сети вашего оборудования? Как это согласуется с новыми требованиями законодательства?

Реализация начинается с оценки рисков

Только после этого компания может внедрить систему информационной безопасности в промышленности. Она начинается с оценки и количественного описания потенциально опасных событий и проведения анализа требований защиты. В рамках этого процесса также выявляются возможные уязвимости и потенциальные возможности для атак и манипуляций, возникающие из-за сетевых технологий, цифровизации и искусственного интеллекта. Важно: в дополнение к классическим целям защиты ИТ, таким как конфиденциальность, целостность и доступность, цели защиты информационной безопасности в промышленности также включают промышленную безопасность, т. е. функциональную безопасность машины.

Оценка рисков безопасности всегда является отправной точкой. Речь идет об анализе угроз и рисков, возникающих из-за пробелов в системе информационной безопасности. Это означает, что меры информационной безопасности должны постоянно контролироваться и адаптироваться. Зачастую это подразумевает наличие сложной ИТ-инфраструктуры и сетей, что требует дополнительных технических знаний и ресурсов.

Требуется эксперт по защите данных и безопасности машин!

Любой, кто ищет внешнюю поддержку при начале работы с информационной безопасностью в промышленности в сфере автоматизации, должен знать, что экспертиза в области ИТ-безопасности может принести лишь ограниченную пользу. Это связано с тем, что процессы снижения риска атак на оборудование (информационная безопасность в промышленности) очень похожи на процедуры снижения рисков, которые могут исходить от оборудования (безопасность машин). Любой, кто хочет внедрить систему информационной безопасности в промышленности, должен быть экспертом в области безопасности машинного оборудования и быть знакомым с соответствующими спецификациями и стандартами, прежде всего с Регламентом по машинному оборудованию.

Конкретная реализация законодательства в настоящее время находится в стадии внедрения. В некоторых моментах гармонизированные стандарты все еще находятся в стадии разработки. Будучи экспертом в области безопасности машинного оборудования, компания Pilz принимает непосредственное участие и играет активную роль в формировании соответствующих стандартов. Pilz передает этот опыт своим клиентам в форме услуг и обучения. Учебный курс «Основы информационной безопасности в промышленности» рассчитан на начинающих. Слушатели курса изучают определения терминов и требования, а также изучают кибербезопасность в контексте информационной безопасности машин и сетей. Передовой опыт способствует пониманию рисков кибербезопасности на производстве.
Учебный курс «Сетрифицированный эксперт в области информационной безопасности в автоматизации (CESA)» предоставляет инструменты, необходимые для внедрения эффективных организационных и технических мер в сетях промышленной автоматизации.

Помимо программы обучения, компания Pilz также предлагает портфолио «Идентификация и управление доступом» (I.A.M.). Продукты и индивидуальные решения для ряда задач, связанных с защитой сотрудников, защитой ответственности, максимальной производительностью и защитой данных. Варианты применения включают, например, аутентификацию пользователей, выбор безопасного режима работы, безопасность данных и сетей, а также управление доступом. Таким образом, можно объединить вопросы безопасности машин и защиты данных в одной системе.

Производители и операторы машин по всему миру должны заняться этой проблемой уже сейчас, чтобы вовремя подготовиться к вызовам информационной безопасности в промышленности. Необходимо сформировать знания, определить обязанности и интерфейсы, а также разработать индивидуальную стратегию. В идеале этот процесс инициирует руководство.

Надпись:

Тексты и изображения для скачивания вы можете найти по адресу:
https://www.pilz.com/ru-INT/company/press/messages/articles/245666

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 консультирование, инжиниринг и обучение. Помимо машиностроения, решения Pilz используются во многих отраслях, например, во внутренней логистике, упаковочной промышленности и на железнодорожном транспорте, или в робототехнике.

Компания Pilz в социальных сетях

Через наши социальные медиа-каналы мы предоставляем справочную информацию о компании Pilz и ее сотрудниках. Мы также информируем о текущих событиях в области автоматизации.

https://www.facebook.com/pilzINT

https://www.youtube.com/user/PilzINT

https://www.linkedin.com/company/pilz

Контактное лицо для журналистов

Martin Kurth
Корпоративная и Техническая пресса
+49 711 3409 - 0
publicrelations@pilz.com

Sabine Skaletz-Karrer
Техническая пресса
+49 711 3409 - 7009
s.skaletz-karrer@pilz.de