20.11.2024

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

Сообщение для Прессы

Юридически обязывающий — Pilz предоставляет информацию и советы по внедрению: как компании могут уже сейчас подготовиться к принятию Закона об устойчивости к угрозам кибербезопасности

Остфильдерн , 20.11.2024 - **Закон об устойчивости к угрозам кибербезопасности (CRA) был недавно опубликован в Официальном вестнике ЕС. Регламент содержит требования к кибербезопасности продукции с цифровыми элементами. У компаний затронутых Законом теперь есть 36 месяцев для выполнения требований, содержащихся в CRA. Определенные обязательства по отчетности должны быть выполнены в течение следующего 21 месяца. Кто именно несет ответственность? А что именно требует Закон об устойчивости к угрозам кибербезопасности (CRA)?**

Закон ЕС об устойчивости к угрозам кибербезопасности: Целью Закона об устойчивости к угрозам кибербезопасности является обеспечение лучшей защиты потребителей и предприятий от кибератак. Закон об устойчивости к угрозам кибербезопасности содержит ряд спецификаций для производителей, импортеров и дистрибьюторов изделий с цифровыми элементами, которые способны взаимодействовать с другими изделиями. Сюда относятся аппаратные и программные продукты. Другими словами, это касается как изделий из сегмента B2C, таких как смартфоны или роботы-пылесосы, так и продуктов из сегмента B2B, таких как контроллеры и датчики, а также чисто программных продуктов, таких как операционные системы. Закон об устойчивости к угрозам кибербезопасности (CRA) был опубликован в Официальном вестнике Европейского Союза 20.11.2024. В качестве нормативного акта данный закон вступает в силу немедленно в государствах-членах ЕС.

Основные требования к производителям машин

- Оценка рисков и гарантии: Производители должны проектировать и разрабатывать изделия таким образом, чтобы гарантировать соответствующий уровень кибербезопасности на протяжении всего жизненного цикла изделия.
- Управление уязвимостями: Производитель должен устранять известные уязвимости с помощью бесплатных обновлений системы безопасности, если иное не согласовано между производителем и коммерческим пользователем.
- Документация: Производители должны выявлять и документировать уязвимости и компоненты в своих продуктах.
- Обязательства по предоставлению информации: В течение 24 часов с момента получения информации об использованной уязвимости производитель должен сообщить об этом через платформу отчетности ENISA (Европейское агентство по кибербезопасности).

Что производители машин могут сделать сейчас

Будучи экспертом в области безопасной и надежной автоматизации, компания Pilz рекомендует всем производителям машин оперативно учитывать требования Закона об устойчивости к угрозам кибербезопасности (CRA) и работать с производителями компонентов и операторами над разработкой концепций сотрудничества. В какой сетевой зоне следует эксплуатировать машину? Как следует работать с обновлениями программного обеспечения? Если такие вопросы будут прояснены заранее, каждый хозяйствующий субъект сможет выполнить свои новые организационные и технические обязательства. На протяжении десятилетий компания Pilz оказывает поддержку производителям машин и пользователям в обеспечении безопасности их установок и оборудования — в том числе в соответствии с новыми требованиями информационной безопасности. Потому что без информационной безопасности машина со всеми ее защитными мерами остается уязвимой и незащищенной. Меры предосторожности обязательны.

2 практических совета по внедрению условий Закона об устойчивости к угрозам кибербезопасности (CRA)

1. Всегда будьте в курсе событий: Подписка на информационные бюллетени и RSS-каналы на eur-lex.europa.eu позволит вам быть в курсе изменений в законодательстве на уровне ЕС.
2. Общие принципы рекомендаций по информационной безопасности (CSAF) — это стандартизированная структура с открытым исходным кодом для передачи и автоматизированного распространения информации об уязвимостях и мерах по их устранению, которую можно обработать с помощью компьютера, так называемых рекомендаций по информационной безопасности.

- Дополнительную информацию по теме информационной безопасности можно найти здесь.

Надпись:

Тексты и изображения для скачивания вы можете найти по адресу:
https://www.pilz.com/ru-INT/company/press/messages/articles/243224

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://twitter.com/Pilz_INT

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

https://www.xing.com/companies/pilzgmbh%26co.kg

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