

<https://red.lnk/ugno6W>

► Der PLCnext Store setzt konsequent auf CRA-konforme Software.

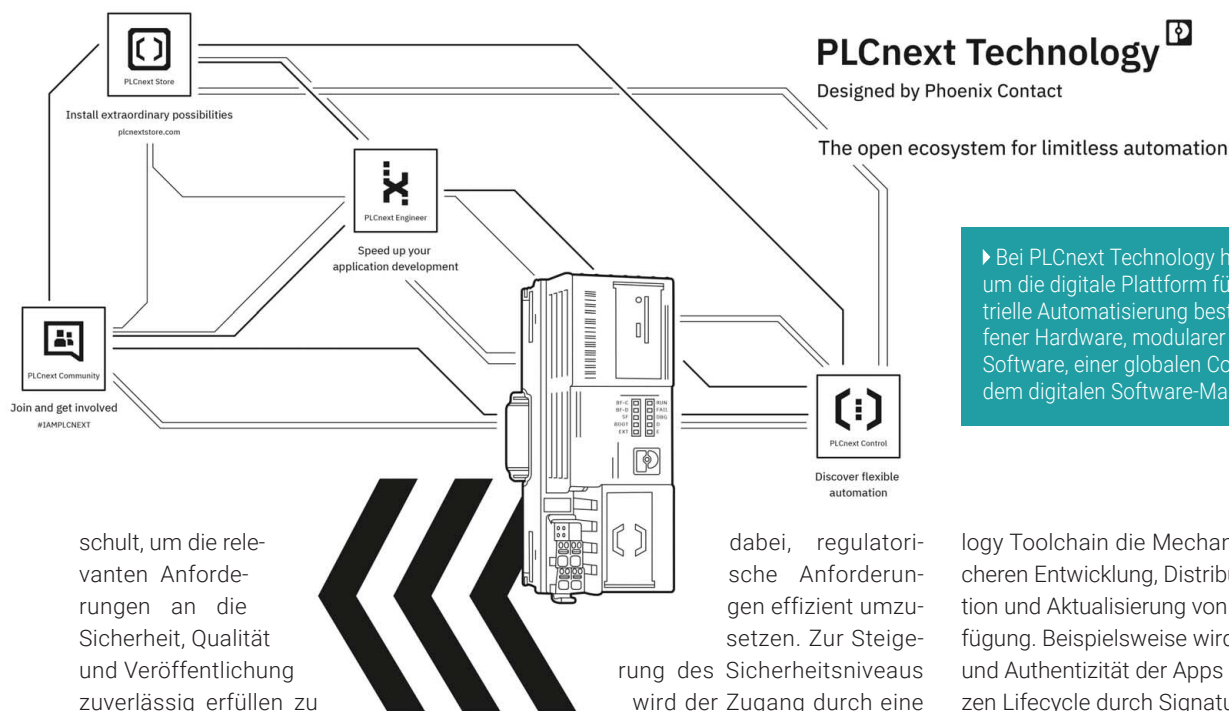
Cyber Resilience Act für industrielle Apps

SICHER DURCH DEN Software-Lifecycle

Bei PLCnext Technology von Phoenix Contact handelt es sich um ein offenes Ökosystem für die industrielle Automatisierung. Es verbindet die Bereiche Steuerungstechnik, Software, digitale Services und eine aktive Community zu einer flexiblen Plattform. Den Anwendern werden hier neue Möglichkeiten zur Umsetzung moderner Automatisierungslösungen geboten. Dabei darf das Thema Cyber Security nicht außer Acht gelassen werden.

Ein wesentlicher Erfolgsfaktor der digitalen Plattform sind starke Partnerschaften. Unternehmen wie Festo und Yaskawa nutzen PLCnext Technology als technologische Grundlage für ihre eigenen Produktfamilien Cepe bzw. iCube. Auf diese Weise entsteht ein herstellerübergreifender Ansatz, der sowohl Anwendern als auch Entwicklern im PLCnext Store verschiedene Vorteile eröffnet. Apps, die darüber bereitgestellt werden, lassen sich auf kompatiblen Systemen unterschiedlicher Hersteller einsetzen. Anwender profitieren dadurch

von einer größeren Flexibilität, vermeiden einen Vendor-Lock-in und erhalten Zugriff auf ein breites Angebot an sofort verwendbaren Applikationen. So können Entwicklungsaufwände reduziert und das Time-to-Market neuer Lösungen deutlich verkürzt werden. Gleichzeitig verschafft die herstellerübergreifende Verfügbarkeit den Entwicklern des Stores den Zugang zu einer größeren Kundengruppe. Hierbei spielt Security eine zentrale Rolle. Der Store stellt die notwendige Infrastruktur für eine sichere App-Entwicklung und -Distribution zur Verfügung. Ergänzend werden die Developer umfassend ge-



► Bei PLCnext Technology handelt es sich um die digitale Plattform für die industrielle Automatisierung bestehend aus offener Hardware, modularer Engineering-Software, einer globalen Community und dem digitalen Software-Marktplatz.

schult, um die relevanten Anforderungen an die Sicherheit, Qualität und Veröffentlichung zuverlässig erfüllen zu können.

Cyber Resilience Act als Qualitätsmerkmal

Mit dem Inkrafttreten des CRA rückt die Cyber-Sicherheit von Produkten mit digitalen Elementen stärker in den Fokus. Vor diesem Hintergrund setzt der PLCnext Store konsequent auf CRA-konforme Software. Damit wird sichergestellt, dass die Nutzer ausschließlich Anwendungen herunterladen, die den aktuellen regulatorischen Anforderungen und hohen Sicherheitsstandards entsprechen. Für die Software-Anbieter im Store bedeutet dies konkret: Sie müssen die Anforderungen des CRA erfüllen, bevor ihre Anwendungen veröffentlicht werden können. Daraus ziehen Anwender den Vorteil der erhöhten Sicherheit und Transparenz bereits bei der Auswahl von Software-Lösungen.

Der digitale Marktplatz erleichtert die CRA-konforme Veröffentlichung von Apps durch die Bereitstellung wesentlicher Funktionen für Transparenz, Sicherheit und Life-Cycle-Management. Für publizierte Apps werden die erforderlichen Nachweise wie die Security-Dokumentation, CE-Konformitätserklärung und CE-Kennzeichnung angeboten, sodass Anwender, Systemintegratoren und Maschinenbauer wichtige Informationen zum Compliance-Status direkt einsehen können. Gleichzeitig hilft der Store den Software-Anbietern

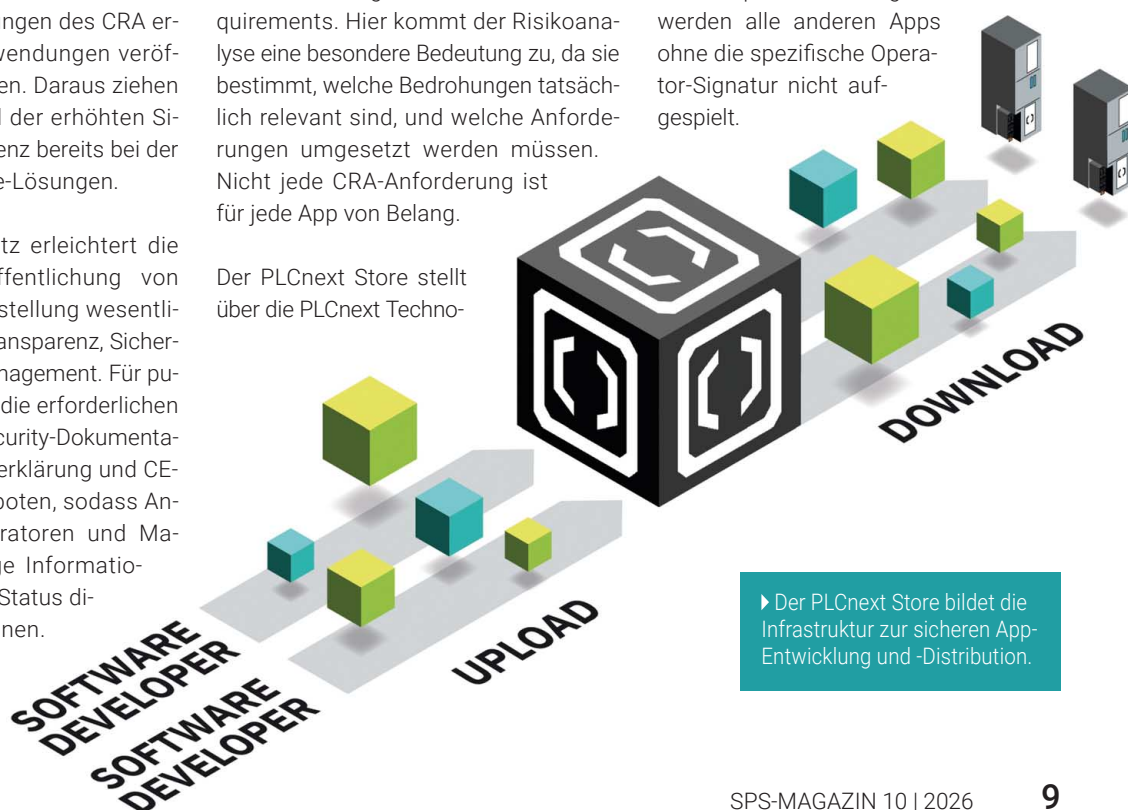
dabei, regulatorische Anforderungen effizient umzusetzen. Zur Steigerung des Sicherheitsniveaus wird der Zugang durch eine Zwei-Faktor-Authentifizierung abgesichert. Zudem unterstützt der App-Marktplatz die sichere Verteilung von Software über signierte Pakete sowie die Bereitstellung von Updates.

App-Integrität durch Signaturen

Der CRA definiert unterschiedliche Security-Anforderungen an die Software-Entwicklung. Aus Sicht einer App stehen am Anfang die Festlegung des Intended Purpose, die Beschreibung des Security-Kontexts sowie die daraus abgeleitete Risikoanalyse. Sie bildet die Grundlage für die Realisierung der CRA Essential Requirements. Hier kommt der Risikoanalyse eine besondere Bedeutung zu, da sie bestimmt, welche Bedrohungen tatsächlich relevant sind, und welche Anforderungen umgesetzt werden müssen. Nicht jede CRA-Anforderung ist für jede App von Belang.

Der PLCnext Store stellt über die PLCnext Techno-

logy Toolchain die Mechanismen zur sicheren Entwicklung, Distribution, Installation und Aktualisierung von Apps zur Verfügung. Beispielsweise wird die Integrität und Authentizität der Apps über den ganzen Lifecycle durch Signaturen sichergestellt. Ein App-Entwickler signiert die App mit seinem Zertifikat und der Store fügt seine Signatur hinzu. Beim Installieren und bestenfalls auch beim Starten werden die Signaturen kontrolliert, somit mögliche Angriffe entdeckt. Auf diese Weise wird dafür gesorgt, dass sich lediglich geprüfter Code ausführen lässt. Große Betreiber wollen ferner sicherstellen, dass auf ihren Anlagen nur von ihnen freigegebene geprüfte Apps installiert werden können. Darüber hinaus soll es keine Verbindung zum Marktplatz im Betrieb geben. Zu diesem Zweck besteht die Möglichkeit, der App eine weitere Operator-Signatur hinzuzufügen. Sind die Geräte entsprechend konfiguriert, werden alle anderen Apps ohne die spezifische Operator-Signatur nicht aufgespielt.



► Der PLCnext Store bildet die Infrastruktur zur sicheren App-Entwicklung und -Distribution.



Realisierung von Secure-by-Design Apps

App-Entwickler erhalten bei der Realisierung der CRA Essential Requirements Unterstützung durch eine Reihe von Plattformfunktionen. Als Teil des Secure-by-Design-Konzepts werden Apps in der Laufzeitumgebung ausgeführt oder lassen sich als Rootless-Podman-Container betreiben. Zusätzlich umfasst die digitale Plattform sichere Voreinstellungen und erleichtert damit die Umsetzung von Secure-by-Default. Zur Realisierung der Anforderungen im Hinblick auf die Vertraulichkeit von Daten können Entwickler auf etablierte Sicherheitsmechanismen von PLCnext zurückgreifen. Diese unterstützen die Verschlüsselung von Daten bei der Übertragung sowie von gespeicherten Daten.

Hinsichtlich der Integrität von Anwendungen und Daten lassen sich Signaturen und Integritätsprüfungen verwenden. Dadurch können Manipulationen erkannt und die Ausführung veränderter Software verhindert werden. Die Benutzer- und Rollenkonzepte ermöglichen die Authentifizierung und das Rechte-Management. Zur Absicherung der Netzwerkschnittstellen werden Funktionen wie Firewall und Netload Limiter zur Verfügung gestellt. Diese helfen die erreich-

bare Angriffsfläche zu minimieren und mögliche Angriffe über Netzwerkverbindungen zu begrenzen. Sicherheitsrelevante Ereignisse lassen sich durch Logging-, Notification- und Syslog-Funktionen erfassen und auswerten.

Vorteile für Ersteller und Anwender

PLCnext Technology sowie der PLCnext Store und die dort angebotenen Apps eignen sich für die Umsetzung der Anforderungen des CRA. Durch die Veröffentlichung CRA-konformer Software auf dem digitalen Marktplatz profitieren Anwender von hohen Sicherheitsstandards und der regulatorischen Konformität. App-Entwickler ziehen einen Nutzen aus den langjähri-

► Darstellung der fünf wichtigsten Schritte zur CRA-Konformität von Apps

gen Cyber-Security-Erfahrungen der PLCnext Technology im Umfeld der IEC62443 sowie den entsprechenden TÜV-Zertifizierungen. Die Entwicklung konformer Apps wird vereinfacht und App-Entwickler können das erworbene Knowhow auch auf weitere Software-Produkte ihres Unternehmens übertragen. ■

Boris Waldeck
Master Specialist Security

Daniel Buschatzky
Product Owner PLCnext Store

Daniel Korte
Technology Manager PLCnext Technology
Phoenix Contact GmbH & Co. KG
www.plcnext-community.net

PLCnext Store unterstützt CRA-konforme Veröffentlichung

Die EU-Verordnung Cyber Resilience Act (CRA) 2024/2847 legt verbindliche Cyber-Sicherheitsanforderungen für Produkte mit digitalen Elementen fest. Hersteller müssen Cyber Security über den gesamten Produktlebenszyklus einschließlich eines Vulnerability Managements und Security Updates sicherstellen. Distributoren und Importeure müssen verifizieren, dass die Anforderungen des CRA eingehalten worden sind. Dazu gehören die CE-Kennzeichnung, EU-Konformitätserklärung, Bereitstellung der erforderlichen Sicherheitsdokumentation und Security-Updates.

Apps werden als eigenständige Software bewertet. In der Rolle des Distributors umfasst der PLCnext Store

Apps verschiedener Hersteller für die von ihm unterstützten Steuerungen. Der digitale Marktplatz bringt die Apps CRA-konform in Verkehr. Die CRA-Konformität von Apps lässt sich in fünf wesentliche Schritte gliedern. Für jede veröffentlichte App stellt der App-Entwickler eine Software Bill of Materials (SBOM) zur Verfügung, die der Bewertung der Auswirkungen neu bekannt gewordener Schwachstellen dient. Die Verantwortung für die CRA-konforme Entwicklung und Beurteilung der App verbleibt beim Hersteller. Hierzu gehören insbesondere die Erstellung der EU-Konformitätserklärung, die CE-Kennzeichnung der App sowie der Nachweis der Essential Requirements (CRA Annex I Part I (1-2)).