https://www.elektrotechnik.vogel.de/sicheres-passwort-management-fuer-siemens-tia-portal-a-892183/

SecuritySicheres Passwort-Management für Siemens TIA Portal

02.01.2020 | Autor/ Redakteur: Stefan Bamberg* / Ines Stotz

Damit Nutzer etwa ihre Maschinensteuerungen ausreichend schützen können, hat das Karlsruher Unternehmen Wibu-Systems eine Passwortverwaltungslösung basierend auf seiner Codemeter-Technologie entwickelt und speziell für das Siemens TIA Portal erweitert.

Damit Maschinenhersteller ihre Entwicklungen vor Unbefugten ausreichend schützen können, ist der Einsatz einer starken Passwortverwaltung notwendig.
(Bild: © kras99 - stock.adobe.com)

Maschinen- und Anlagenbauer, die das Engineering-Framework Totally Integrated Automation (TIA)-Portal von Siemens nutzen, erhalten alle notwendigen Tools, um eine speicherprogrammierbare Steuerung (SPS) entwickeln zu können. Es steht in einem Software-Komplettpaket zur Verfügung – mit Funktionen zur digitalen Planung über integriertes Engineering bis zur transparenten Bedienung. Anwender profitieren durch Simulationstools von einer kürzeren Markteinführungszeit;

https://www.elektrotechnik.vogel.de/sicheres-passwort-management-fuer-siemens-tia-portal-a-892183/

Diagnose- und Energiemanagementfunktionen führen zu mehr Flexibilität und Produktivität der Fabriken. Hierbei entsteht schützenswertes Know-how, beispielsweise sensible Engineering-Daten oder Source Code zum Steuern einer Maschine oder eines Geräts. Die Programmiersprachen sind kompatibel zum Standard IEC 61131. Teil 3 umfasst die Verwendung von Leiterbahndarstellungen, Funktionspläne, strukturierte Texte, Anweisungslisten und sequentielle Funktionspläne.

Vier Grundbausteine sind im TIA-Portal enthalten: Organisationsblock (OB), Funktionsblock (FB), Funktion (FC) und Datenblock (DB). Diese Blöcke gilt es mittels Passwörter vor Unbefugten zu schützen. Um einen ausreichenden Schutz zu ge- währleisten, der sich nicht einfach umgehen lässt, hat das Karlsruher Unternehmen Wibu-Systems eine Passwortverwaltungslösung basierend auf seiner Codemeter-Technologie entwickelt und speziell für das TIA Portal erweitert. Die Passwörter sind hinreichend lang und vor den Augen der Anwender verborgen.

Siemens-Kunden erhalten ab Version 14 eine sichere und flexible Passwortverwaltung. Das TIA Portal enthält eine Passwort-API, das heißt eine Schnittstelle zur Übertragung und Nutzung von Passwörtern.

Werkzeuge zur Passwortverwaltung für die Anwender

Ergänzend zu den bekannten Tools stehen verschiedene, miteinander verknüpfte Hardware- und Software-Tools zur Verfügung:

- Schutzhardware Cm-Dongles, auch Secure Elements genannt: Hier werden die Passwörter sicher gespeichert und jeder Anwender steckt seinen Dongle auf, um mit dem TIA Portal arbeiten zu können. Die Hardware gibt es z. B. für die USB-Schnittstelle, auch USB Typ-C, als Asic oder als Speicherkarte für Schnittstellen wie SD, Micro SD oder CFast.
- Codemeter License Central: eine cloud- und datenbankbasierte Lösung zur Passwortverteilung und -verwaltung.
- Codemeter Web Depot: Ein Portal zur Passwortübertragung.
- Codemeter Keyring Password Manager: Mit Hilfe dieses Verwaltungstools konfigurieren bestimmte, mit der Passwort-Verwaltung betraute Mitarbeiter Passwörter und Rechte über die Codemeter License Central.

https://www.elektrotechnik.vogel.de/sicheres-passwort-management-fuer-siemens-tia-portal-a-892183/

- Codemeter Keyring for TIA Portal Password Provider: Dieses Add-in ermöglicht die Nutzung der Passwörter eines angeschlossenen Cm-Dongles im TIA Portal.

BUCHTIPP

Cybersicherheit ist nicht nur sinnvoll, sie ist die absolute Grundvoraussetzung für eine erfolgreiche Digitalisierung. Das Fachbuch Cybersicherheit erläutert die Relevanz von IT-Sicherheit in Industrieunternehmen und gibt die nötige Unterstützung, diese im eigenen Unternehmen umzusetzen.

Passwortgenerierung mit hohem Schutzlevel

Mit dem Codemeter Keyring for TIA Portal lassen sich Passwörter auf diese Weise sicher verwalten:

Zuerst legt das Projekt-Team des Siemens-Kunden fest, welche Mitarbeiter die Rechte eines Super-Users – sozusagen der Administrator für die Passwort-Verwaltung – erhalten. Nur diese erhalten die Berechtigung, Passwörter zu erzeugen, Einschränkungen für das Benutzen, Ändern oder Widerrufen von Passwörtern zu konfigurieren und an die Anwender zu verteilen. Mit Hilfe des Tools Codemeter Keyring Password Manager, das mit Codemeter License Central verknüpft ist, werden starke Passwörter automatisch generiert. Das Problem zu kurzer Passwörter und möglicher Passwortweitergabe wurde hierbei clever gelöst und erreicht damit einen hohen Schutzlevel. Denn selbst der Super-User kennt keines der langen Passwörter.

Jeder Anwender im Projekt-Team bekommt vom Super-User sein Passwort für das TIA Portal und die dazugehörigen Berechtigungen, sogenannte Restriktionsfunktionen, zugewiesen, was automatisch in Codemeter License Central gespeichert wird. Zusätzlich erhält jeder im ersten Schritt seinen Cm-Dongle und einen Passwort-Aktivierungs-Code (Ticket), beispielsweise per E-Mail. Im zweiten Schritt verbindet sich der Anwender über das Internet mit Codemeter Web Depot und aktiviert sein Ticket. Dies funktioniert nur, wenn zuvor der Cm-Dongle auf der passenden Schnittstelle aufgesteckt wurde. Codemeter License Central überträgt dann das Passwort und speichert es im geschützten Bereich des Dongles. Weil die Mitarbeiter oft in verschiedenen Projekten gleichzeitig arbeiten, können sie vom Super-User unterschiedliche Passwörter erhalten und alle in einem einzigen Cm-Dongle speichern.

So arbeiten die Codemeter-Tools

Wird im TIA Portal ein Passwort benötigt, wird Codemeter Keyring for TIA Portal Password Provider aktiviert, der dann die im Cm-Dongle gespeicherten Passwörter und Berechtigungen erkennt und sicher an das TIA Portal überträgt. Dort stehen dann diese Passwörter mit den dazugehörigen Berechtigungen zur Verfügung, sodass der Anwender die für ihn zuvor definierten Blöcke einsehen darf. Da sich während der Projektlaufzeit innerhalb des Projekt-Teams Veränderungen ergeben können, kann der Super-User die Passwörter zeitlich beschränken, ändern oder widerrufen.

Die Passwortverwaltung lässt sich von Maschinenherstellern ganz unterschiedlich nutzen. Beispielsweise können sie ihre Maschinen davor schützen, dass Anwender oder unbefugte Dritte unerwünschte Änderungen am Source Code vornehmen. Zusätzlich können sie damit festlegen, welche Service-Firmen mit dem Source Code überhaupt arbeiten dürfen

* Stefan Bamberg, Senior Key Account und Partner Manager, Wibu-Systems