cabPROTECT

Datensicherheit beim Etikettendruck

Der verantwortungsvolle Umgang mit Daten und der manipulationsfreie Betrieb aller cab Drucksysteme sind für uns Schlüsselanliegen. Wir haben für unsere Geräte Sicherheitsstandards festgelegt. Ich stelle sie hier vor.

Mario Hiss
Strategisches Produktmanagement, cab

Industrie 4.0, mit Fokus auf Informations- und Kommunikationstechnologien, treibt intelligente Kennzeichnung voran. Bei unseren Kunden agieren Drucksysteme autark ohne Zuhilfenahme weiterer Geräte. In Netzwerken kommunizieren sie mit Anlagensteuerungen, Leitrechnern oder Systemen zur Planung und Verwaltung von Ressourcen. Prozessnetze sind inhouse, über Standorte hinweg oder transnational zusammengeschaltet. Die daraus resultierenden Vorteile sind unstrittig. Für die IT-Verantwortlichen eines Unternehmens ergeben sich daraus aber auch neue Anforderungen.

Speziell die Anbindung an eine ERP-Software und damit an Stammdaten kann bei nicht ausreichender Sicherung kritisch sein. Denken Sie bei Manipulationsmöglichkeiten zum Beispiel an Infektionen über das Internet, das Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware in ein System, Fernwartungszugänge, aber auch menschliche Fehler. Lösungen für diese Aufgabenstellung sind, heute mehr denn je, fester Bestandteil unserer Produktentwicklung.

cabPROTECT

cabPROTECT Sicherheitsstandards

Systempasswort

cab Drucksysteme werden offen, ohne Einschränkung ausgeliefert. Mithilfe eines Passworts lässt sich der Zugriff auf ein System einschränken und für Netzwerkteilnehmer ein bewertbares Sicherheitslevel erzielen. Ein Systempasswort macht insbesondere dann Sinn, wenn für geräteinterne oder Netzwerkeinstellungen Berechtigungen oder Verschlüsselungen vergeben werden. Diese könnten ohne Schutz einfach verändert oder gelöscht werden.

Zugriff von extern

cab Drucksysteme halten für die Konfiguration, Bedienbarkeit und Überwachung aus der Ferne Möglichkeiten des Zugriffs via http, SOAP WebService, FTP, VNC oder OPC UA bereit. Für jeden Dienst ist separat ein passwortgeschützter Zugang werkseitig im Gerät eingerichtet. Änderungen bedingen der Kenntnis des → **Systempasswort** (sofern ein solches für den Zugriff auf das cab Drucksystem vergeben wurde).

- **http-Service** ermöglicht das Konfigurieren, Parameter einstellen und Bedienen eines cab Drucksystems mit einem üblichen Browser von einem PC oder einem anderen mit dem Netzwerk verbundenen Endgerät aus. Der Dienst kann über die Eingabe der IP-Adresse des Drucksystems aufgerufen werden. Der Zugang erfolgt passwortgeschützt.

- **WebServices** ermöglichen Dienste und Funktionen über eine definierte Schnittstelle und Protokolle und befähigen zur Interaktion einzelner Maschinen. Die Kommunikation mit dem WebService kann aus unterschiedlichen Plattformen und mit unterschiedlichen Programmiersprachen erfolgen. Der cab WebService nutzt den Standard SOAP. Kommunikationspartner müssen sich gegenseitig über ein Passwort authentifizieren. Die http-Authentifizierungsmethoden Basic (Benutzername, Kennwort) und Digest (Benutzername, Kennwort, zufällige Zeichenfolge) werden unterstützt.

- **FTP-Service:** Die Übertragung von Daten in einem Netzwerk über das File Transfer Protocol erfolgt mehrteilig: FTPprint ermöglicht das Drucken, FTPcard den Zugriff auf einen USB-Stick, eine SD-Karte oder den internen Systemspeicher IFFS, FTPadmin die Installation von Firmware. Jeder Zugriff erfordert die Authentifizierung über ein Passwort.

- **VNC-Service:** Hiermit lässt sich das Bedienfeld eines cab Drucksystems (Server) auf den Bildschirm eines weiteren Teilnehmers im Netzwerk (Client) übertragen. Die Aktivitäten des Clients an einer Tastatur oder Maus werden auf dem Server dargestellt. VNC ist plattformunabhängig. Der Zugriff via VNC auf ein cab Drucksystem erfolgt authentifiziert über ein Passwort.

- **OPC UA** ist der Schnittstellenstandard bei Industrie 4.0. Er ist unabhängig vom Hersteller oder Systemlieferant, Betriebssystem oder Programmiersprachen und stellt die sichere Kommunikation von Feldgeräten in einem Netzwerk oder über das Internet dar. Es kommunizieren Maschinen untereinander oder mit einem PC. cab Drucksysteme haben einen OPC UA-Server und einen OPC UA-Client in die Firmware integriert. Der Server ermöglicht die Konfiguration und Überwachung des Systems. Dynamische Druckdaten lassen sich über eine definierte Programmierschnittstelle aufbereiten. Mit dem Client können Datenfelder von anderen OPC UA-fähigen Maschinen ausgelesen und auf einem Etikett platziert werden. Beim Zugriff ohne Passwort können Schreib- und Leserechte individuell vergeben werden. Der anonyme Zugriff lässt sich ausschalten und der Zugang durch ein Passwort schützen.

cabPROTECT

Import / Export von Geräteeinstellungen

Um nach erfolgter Inbetriebnahme Gerätekonfigurationen zu sichern oder auf andere Geräte zu übertragen, erlauben cab Drucksysteme den Import und Export dieser Konfiguration über → **WebDAV** in ein Netzwerk, auf einen USB-Stick, eine SD-Karte oder in den internen IFFS-Gerätespeicher. Zum Speichern und Laden kann ein Passwort definiert werden. Dessen Eingabe oder Bearbeitung bedingen der Kenntnis des → **Systempasswort** (sofern ein solches für den Zugriff auf das cab Drucksystem vergeben wurde).

WebDAV

Die Firmware der cab Drucksysteme unterstützt das Übertragungsprotoll WebDAV. Damit lassen sich virtuelle Speicher in ein cab Gerät über das Netzwerk einbinden. Der Internetspeicher wird als Laufwerk verfügbar und so überall erreichbar. Die Einrichtung des WebDAV-Clients erfolgt einmalig am cab Drucksystem. Zur Einrichtung müssen die Zugangsdaten bekannt und auf dem System ein Benutzeraccount angelegt werden. Deren Eingabe oder Bearbeitung bedingen der Kenntnis des → **Systempasswort** (sofern ein solches für den Zugriff auf das cab Drucksystem vergeben wurde).

TLS-Zertifikat

cab Drucksysteme bieten die Möglichkeit, Daten zwischen einem Teilnehmer im Netzwerk (Client) und einem Server über ein TLS-Zertifikat verschlüsselt zu übertragen. TLS ist die Weiterentwicklung des SSL-Protokolls und gegenüber diesem als noch sicherer, flexibler und effizienter anerkannt. Im Standard befindet sich auf cab Drucksystemen ein für diese Art der Datenübertragung erforderliches Zertifikat werkseitig installiert. Dieses kann jederzeit durch ein eigenes signiertes Zertifikat überschrieben werden. Das Einlesen dieses Zertifikats ist über einen USB-Stick, eine SD-Karte oder eine → **WebDAV**-Netzwerkverbindung möglich. Das Zertifikat enthält Identifizierungsinformationen, mit denen man sich zur Freigabe der Datenübertragung gegenüber einem Server oder Client ausweisen kann. Die Verwendung des Zertifikats sowie dessen Auswahl bedingt der Kenntnis des → **Systempasswort** (sofern ein solches für den Zugriff auf das cab Drucksystem vergeben wurde).
Bei aktiviertem TLS wird bei der Nutzung der Netzwerkdienste HTTP/HTTPS und FTP/FTPS automatisch auf dieses verschlüsselte Verfahren umgeschaltet.

Authentifizierung nach IEEE 802.1X

cab Drucksysteme unterstützen den Netzwerkstandard IEEE 802.1X. Damit lassen sie sich in einem Netzwerk sicher autorisieren. Anmeldungen eines Netzwerkteilnehmers werden automatisch von einem Authentifizierungsserver geprüft und freigegeben. In Abhängigkeit der gemeinsam vereinbarten Authentifizierungsinformation erfolgt, ähnlich wie beispielsweise bei einem WLAN Key, die Annahme oder Verweigerung des Datenaustauschs. Zur Authentifizierung stehen Verfahren nach den Standards EAP-PEAP, EAP-TLS und EAP-TTLS zur Verfügung.

WLAN

Insbesondere bei ausgedehnten Installationsarealen oder bei ortsunabhängigen, mobilen Anwendungen bietet die drahtlose Übertragung von Daten Vorteile. Installationskosten werden gesenkt, die Anwendung gewinnt an Flexibilität. Verschlüsselte Übertragung verhindert das unzulässige Abfangen von Daten und deren manipulierte Weitergabe. cab Drucksysteme nutzen zur Verschlüsselung des Datenaustauschs die Methoden WPA2 (überwiegend in kleineren Netzwerken), WPA2 Enterprise (größere Netzwerke) und WPA3. Die Verschlüsselung erfolgt nach allgemein als sehr sicher anerkanntem Standard AES. Teilnehmer des WLAN-Netzwerks müssen sich authentifizieren, bevor sie auf Ressourcen im Netzwerk zugreifen dürfen. Hierzu befragt der Access Point (Station, die Daten empfängt und sendet) den Authentifizierungsserver. Die Authentifizierung zwischen dem Teilnehmer und der Empfangsstation erfolgt über den WLAN Key, eine geheime Zeichenfolge. Die Änderung dieses Schlüssels bedingt der Kenntnis des → **Systempasswort** (sofern ein solches für den Zugriff auf das cab Drucksystem vergeben wurde). cab Drucksysteme mit eingerichtetem WLAN können als Hotspot verwendet und damit von mobilen Endgeräten aus konfiguriert, gesteuert und überwacht werden. Der Zugriff bedingt die unter → **Zugriff von extern** beschriebene Absicherung durch ein Passwort.

cabPROTECT

Bluetooth

Bei cab Drucksystemen ermöglicht ein Adapter, für den Austausch von Daten eine Funkschnittstelle zu einem externen Gerät einzurichten. Um eine Vertrauensbeziehung zwischen beiden Geräten sicher zu stellen, ist für beide Geräte die Eingabe einer PIN erforderlich. Diese PIN gehört nicht zum Benutzer, sondern zum jeweiligen Gerät. Das Einrichten der Bluetooth-Schnittstelle bedingt der Kenntnis des → **Systempasswort** (sofern ein solches für den Zugriff auf das cab Drucksystem vergeben wurde).

Firmwareupdate

Bei jeder Aktualisierung der Firmware wird die neue Datei zunächst auf Vollständigkeit, Schäden, die Übereinstimmung zum entsprechenden Drucksystem und korrekte Code-Sequenzen überprüft. Nur wenn das Update fehlerfrei durchlaufen wurde, wird der neue Stand dieser Firmware auf dem cab Drucksystem aktiviert. Künftig soll jedes cab Firmwarepaket einen mathematischen Algorithmus aus Buchstaben und Zahlen errechnen und veröffentlichen. Die Übereinstimmung dieser MD5-Prüfsumme mit einem beim Download der Firmware übermittelten Wert gewährleistet digitale Integrität und die Echtheit dieser Datei. Um sicher zu stellen, dass keine unerlaubten Updates am Drucksystem durchgeführt werden, wird empfohlen, den Zugriff auf externe Speichermedien sowie → **USB-Schnittstellen** abzuschalten und den FTPadmin-Bereich über ein Passwort zu schützen.

Externe Speichermedien

cab Drucksysteme unterstützen USB-Massenspeicher und SD-Karten. Diese werden in der Regel nur dann zur Datenübertragung und -speicherung verwendet, wenn das Drucksystem nicht in ein Netzwerk integriert ist.
Um sicher zu stellen, dass über diese Kanäle keine unzulässigen Daten oder Schadsoftware auf das Drucksystem übertragen werden können, lassen sich die externen Speichermedien am cab Drucksystem abschalten.
Dies verhindert zugleich das unzulässige Speichern von Daten vom Drucksystem auf externe Speichermedien.

USB-Schnittstellen

cab Drucksysteme verfügen über USB-Schnittstellen an der Geräterückseite und im Bereich des Bedienfelds.
Sie dienen der Konfiguration des Drucksystems mit Druckdaten, Layouts oder Firmware. Sie unterstützen ebenso die Eingabe von Druckdaten über eine Tastatur oder Lesegeräte, die Ansteuerung des Systems über USB oder einen Windows-Treiber. Zur 100-prozentigen Vorbeugung gegen nicht authorisierte Zugriffe, etwa eines USB-Massenspeichers oder → **cab Service Key**, lassen sich an cab Drucksystemen die USB-Schnittstellen sperren.

cab Service Key

Wurde für den Zugriff auf ein cab Drucksystem ein Passwort vergeben, dieses vom Bediener aber vergessen oder verloren, können alle Einstellungen über einen cab Service Key vorgenommen werden. cab händigt diese Schlüssel ausschließlich an autorisierte und bei cab registrierte Personen aus. Der Service Key wird am cab Drucksystem in eine der → **USB-Schnittstellen** gesteckt (Stellen Sie sicher, dass diese nicht gesperrt wurde.)
Er ist nach Beendigung der Servicearbeiten vom System zu entfernen und sicher aufzubewahren.
Sollten am Gerät die USB-Schnittstellen gesperrt und der Zugriff deshalb versagt sein, besteht die Möglichkeit, das cab Drucksystem für dessen Freischaltung ins nächstgelegene cab Werk zu schicken. Andernfalls ist im Gerät die CPU auszutauschen. Diese ist bei cab anzufordern.

cabPROTECT kompakt

www.cab.de/cabprotect

Haben Sie Fragen? info@cab.de