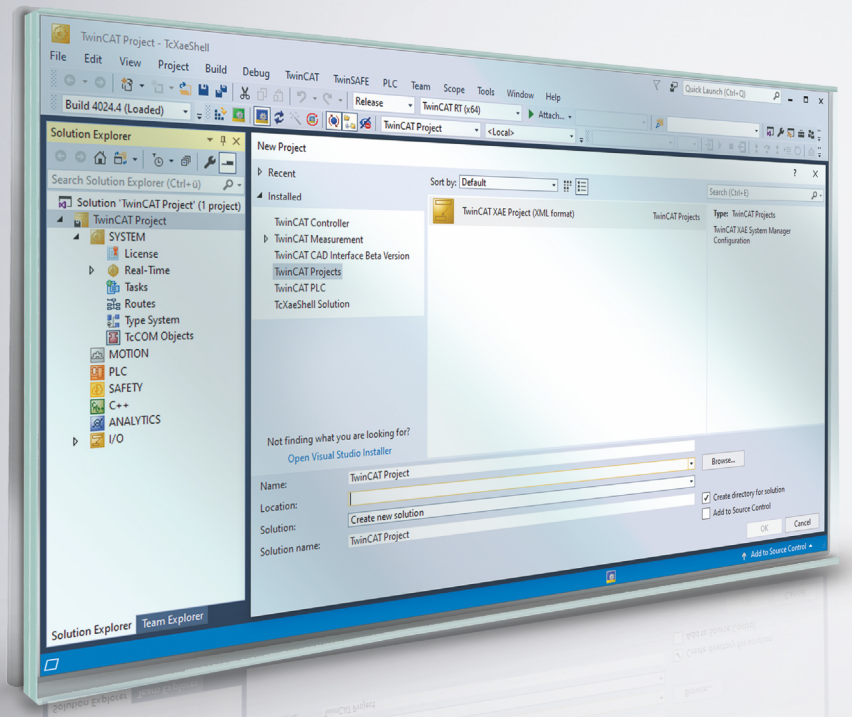
BECKHOFF New Automation Technology

Original-Handbuch | DE

IPC-Security-Leitfaden

für Beckhoff RT Linux®



12.08.2026 | Version: 1.0

Inhaltsverzeichnis

1 Hinweise zur Dokumentation

Diese Beschreibung wendet sich ausschließlich an ausgebildetes Fachpersonal der Steuerungs- und Automatisierungstechnik, das mit den geltenden nationalen Normen vertraut ist.
Zur Installation und Inbetriebnahme der Komponenten ist die Beachtung der Dokumentation und der nachfolgenden Hinweise und Erklärungen unbedingt notwendig.
Das Fachpersonal ist verpflichtet, stets die aktuell gültige Dokumentation zu verwenden.

Das Fachpersonal hat sicherzustellen, dass die Anwendung bzw. der Einsatz der beschriebenen Produkte alle Sicherheitsanforderungen, einschließlich sämtlicher anwendbaren Gesetze, Vorschriften, Bestimmungen und Normen erfüllt.

Disclaimer

Diese Dokumentation wurde sorgfältig erstellt. Die beschriebenen Produkte werden jedoch ständig weiterentwickelt.
Wir behalten uns das Recht vor, die Dokumentation jederzeit und ohne Ankündigung zu überarbeiten und zu ändern.
Aus den Angaben, Abbildungen und Beschreibungen in dieser Dokumentation können keine Ansprüche auf Änderung bereits gelieferter Produkte geltend gemacht werden.

Marken

Beckhoff®, ATRO®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, MX-System®, Safety over EtherCAT®, TC/BSD®, TwinCAT®, TwinCAT/BSD®, TwinSAFE®, XFC®, XPlanar® und XTS® sind eingetragene und lizenzierte Marken der Beckhoff Automation GmbH.
Die Verwendung anderer in dieser Dokumentation enthaltenen Marken oder Kennzeichen durch Dritte kann zu einer Verletzung von Rechten der Inhaber der entsprechenden Kennzeichnungen führen.

EtherCAT® ist eine eingetragene Marke und patentierte Technologie, lizenziert durch die Beckhoff Automation GmbH, Deutschland.

Copyright

Fremdmarken

In dieser Dokumentation können Marken Dritter verwendet werden. Die zugehörigen Markenvermerke finden Sie unter: https://www.beckhoff.com/trademarks.

1.1 Schwachstellen melden

Wir bitten die Sicherheitsanalysten darum, uns genügend Zeit für die Entwicklung einer Lösung zur Schließung einer Sicherheitslücke zu geben, bevor sie diese veröffentlichen. Die Coordinated Disclosure sorgt dafür, dass Kunden ein Update zur Schließung von Sicherheitslücken erhalten und dass sie während der Entwicklung des Updates nicht unnötig gefährdet werden. Nachdem die Kunden geschützt sind, kann die öffentliche Diskussion über die Sicherheitslücke der Industrie insgesamt helfen, ihre Produkte und Lösungen zu verbessern.

Wenn Beckhoff der Anbieter eines Produkts ist, das im Verdacht steht, verwundbar zu sein, kontaktieren Entdecker und Koordinatoren von Sicherheitslücken product-securityincident@beckhoff.com mit einem Sicherheitslückenbericht („vulnerability report“), vorzugsweise in englischer oder deutscher Sprache. Um die Wahrung von Vertraulichkeit wird gebeten. Mittel zum Senden verschlüsselter Nachrichten sind beschrieben unter Kontakt Beckhoff Incident Response Team.

Entdecker sind dazu aufgefordert, im Sicherheitslückenbericht alle erforderlichen Kontaktinformationen anzugeben, damit Rückfragen möglich sind. Nichtsdestotrotz werden auch anonyme Sicherheitslückenberichte berücksichtigt. Geben Sie bitte möglichst detaillierte Informationen an, damit die Fälle reproduziert werden können. Wenn der Entdecker die Entdeckung veröffentlichen möchte, wird Beckhoff versuchen, ein geeignetes vorläufiges Veröffentlichungsdatum innerhalb von 30 Tagen zu koordinieren. Der Entdecker wird vor dem Veröffentlichungsdatum über die Verfügbarkeit von Lösungen informiert und erhält das entsprechende Beckhoff Advisory. Beckhoff erhält die geplante Veröffentlichung des Entdeckers (gegebenenfalls einschließlich beantragter CVE). Dann wird ein endgültiges Veröffentlichungsdatum abgestimmt. An diesem Tag werden sowohl die Veröffentlichung des Entdeckers, als auch ein Beckhoff Advisory freigegeben. Wenn es der Entdecker wünscht und er sich an das vorliegende Verfahren hält, werden eine Danksagung, ein Verweis auf die Veröffentlichung des Entdeckers und, falls hilfreich, Informationen über die Veröffentlichung des Entdeckers in das Advisory hinzugefügt.

1.2 Kontakt Beckhoff Incident Response Team

Anschrift

Beckhoff Automation GmbH & Co. KG
Produktmanagement (Security)
Hülshorstweg 20
33415 Verl
Deutschland

E-Mail

<product-securityincident@beckhoff.com>

E-Mails an diese Adresse werden den zuständigen Mitarbeitern des Beckhoff Incident Response Teams zugestellt.

Öffentliche Schlüssel

Das Beckhoff Incident Response Team besitzt zwei Schlüssel zur Kontaktaufnahme:

- PGP-Schlüssel mit der ID `B4 F4 15 9A` und dem Fingerabdruck `C9 6F 56 5C 39 49 43 58 AE B5 07 93 80 95 E1 2D B4 F4 15 9A`
- S/MIME-Zertifikat mit der ID `0a 0e 85 68 56 18 0f 5c 8a 5c 4e 83` und dem Fingerabdruck `4c b4 d0 99 d4 a0 6c f0 af 69 ee 7a 8f 81 a1 c3 42 eb 17 da`

Download der Schlüssel: https://download.beckhoff.com/download/document/product-security/Keys

Arbeitszeiten

Das Incident Response Team arbeitet normalerweise zwischen 9:00 und 17:00 und nicht an Feiertagen in NRW. Zeitzone: MEZ (Europe/Berlin).

1.3 Hinweise zur Informationssicherheit

Die Produkte der Beckhoff Automation GmbH & Co. KG (Beckhoff) sind, sofern sie online zu erreichen sind, mit Security-Funktionen ausgestattet, die den sicheren Betrieb von Anlagen, Systemen, Maschinen und Netzwerken unterstützen. Trotz der Security-Funktionen sind die Erstellung, Implementierung und ständige Aktualisierung eines ganzheitlichen Security-Konzepts für den Betrieb notwendig, um die jeweilige Anlage, das System, die Maschine und die Netzwerke gegen Cyber-Bedrohungen zu schützen. Die von Beckhoff verkauften Produkte bilden dabei nur einen Teil des gesamtheitlichen Security-Konzepts. Der Kunde ist dafür verantwortlich, dass unbefugte Zugriffe durch Dritte auf seine Anlagen, Systeme, Maschinen und Netzwerke verhindert werden. Letztere sollten nur mit dem Unternehmensnetzwerk oder dem Internet verbunden werden, wenn entsprechende Schutzmaßnahmen eingerichtet wurden.

Zusätzlich sollten die Empfehlungen von Beckhoff zu entsprechenden Schutzmaßnahmen beachtet werden. Weiterführende Informationen über Informationssicherheit und Industrial Security finden Sie in unserem https://www.beckhoff.de/secguide.

Die Produkte und Lösungen von Beckhoff werden ständig weiterentwickelt. Dies betrifft auch die Security-Funktionen. Aufgrund der stetigen Weiterentwicklung empfiehlt Beckhoff ausdrücklich, die Produkte ständig auf dem aktuellen Stand zu halten und nach Bereitstellung von Updates diese auf die Produkte aufzuspielen. Die Verwendung veralteter oder nicht mehr unterstützter Produktversionen kann das Risiko von Cyber-Bedrohungen erhöhen.

Um stets über Hinweise zur Informationssicherheit zu Produkten von Beckhoff informiert zu sein, abonnieren Sie den RSS Feed unter https://www.beckhoff.de/secinfo.

1.4 Designziele für Sicherheit

Die Industrie-PC (IPC)-Hardware von Beckhoff wurde für den allgemeinen Gebrauch wie ein Consumer-PC für Büroumgebungen entwickelt, jedoch mit erheblicher zusätzlicher Robustheit für den Einsatz in industriellen Umgebungen. Das komplette Board ist für einen zuverlässigen und hoch deterministischen Betrieb in solchen Umgebungen ausgelegt. Dennoch unterstützt die Hardware universelle Betriebssysteme wie Windows® Beckhoff RT Linux® und TwinCAT/BSD, das auf FreeBSD® basiert. Folglich ist die Hardware so konzipiert, dass sie herkömmliche und Büro-IT-konforme Sicherheitsmechanismen unterstützt, wie sie von den Betriebssystemen bereitgestellt werden. Derjenige, der den IPC in eine Betriebsumgebung integriert, hat die Aufgabe, diese Sicherheitsfunktionen für die jeweilige Umgebung entsprechend zu konfigurieren. Außerdem muss diese Person dem Bediener eine Anleitung für die sichere Nutzung zur Verfügung stellen. Solche Konfigurations- und Nutzungsleitlinien sollten das Ergebnis eines ganzheitlichen Sicherheitskonzepts für die jeweilige Umgebung sein bzw. mit diesem konform sein.

Die IPCs von Beckhoff können mit und ohne Betriebssystem bestellt werden. Unter diesen Betriebssystemen sind Windows 10, Windows 11, Beckhoff RT Linux® und TwinCAT/BSD verfügbar. Diese werden, sofern nicht ausdrücklich anders bestellt, als „Secure by Default“ (standardmäßig sicher) bereitgestellt. Das bedeutet, dass in der Standardkonfiguration nur bestimmte Dienste aktiviert sind, so dass jeder Zugriff auf das Gerät authentifiziert wird, und der einzige vorkonfigurierte Benutzer administrativen Zugriff hat. Aus historischen Gründen ist der vorkonfigurierte Benutzer „Administrator“. Das dokumentierte bekannte Passwort ist für diesen Zweck vorkonfiguriert. Bitte beachten Sie Folgendes: Dies ist im Hinblick auf die Anforderungen einiger Umgebungen nicht „Secure by Default“, während es für andere gut geeignet ist.

Die genannten Betriebssysteme sind hinsichtlich ihrer Sicherheitsfunktionen seit Jahrzehnten für den Einsatz in Büro- und Serverumgebungen anerkannt. Sie enthalten und bieten modernste Sicherheitsfunktionen. Bestimmte Umgebungen und Anwendungen haben spezifische Anforderungen an die Konfiguration und Nutzung dieser Sicherheitsfunktionen. Da Beckhoff die genannten Betriebssysteme für den allgemeinen Einsatz zur Verfügung stellt und nicht einschränken will, welche Anwendungen damit implementiert werden, kann Beckhoff die spezifischen Sicherheitsanforderungen, die sich aus der jeweiligen Verwendung oder Integration ergeben, nicht vorhersehen. Eine Anleitung zur sicheren Konfiguration und Nutzung muss daher von demjenigen erstellt werden, der das Betriebssystem für eine bestimmte Verwendung in eine Umgebung integriert. Nichtsdestotrotz gibt Beckhoff im Rahmen dieses Leitfadens eine Anleitung zur sicheren Nutzung des IPC und seines Betriebssystems. Diese Anleitung ist als allgemeiner Hinweis zu verstehen und nicht als vollständige und ausreichende Referenz. Die Entwickler der Betriebssysteme stellen eine vollständige Dokumentation für die Sicherheitsfunktionen der Betriebssysteme zur Verfügung.

Beckhoff hat Erweiterungen zu diesen Betriebssystemen entwickelt, insbesondere um das deterministische Verhalten des Betriebssystems für den Einsatz mit Echtzeitanwendungen der Automatisierungsindustrie zu optimieren. Die Erweiterungen sind in die von Beckhoff vertriebenen Betriebssystem-Images integriert. Das Hauptziel bei der Entwicklung dieser Erweiterungen sind Robustheit und Determinismus für eine erhöhte Verfügbarkeit. Dennoch achtet Beckhoff darauf, dass diese Erweiterungen die grundlegenden Sicherheitsfunktionen des Betriebssystems nicht beeinträchtigen, sofern nicht anders angegeben.

Beckhoff vertreibt eine große Vielfalt an Softwareprodukten. Ein Beispiel ist das Produkt „TwinCAT 3.1 – eXtended Automation Runtime (XAR)“, kurz TwinCAT 3.1 XAR genannt. Dieses kann bei einigen IPCs als Bestandteil des Betriebssystems vorinstalliert bestellt werden. Der Hauptzweck dieser speziellen Software ist es, eine deterministische und robuste, aber hochgradig anpassbare Laufzeit für Automatisierungsanwendungen bereitzustellen. Wenn sie auf einem IPC installiert ist, macht sie dieses Gerät zu einer speicherprogrammierbaren Steuerung (SPS). Neben der Verfügbarkeit (durch Robustheit und Determinismus) wurde die Software bei ihrer Entwicklung mit Perimetersicherheit ausgestattet. Das bedeutet, dass sie so konfiguriert und verwendet werden kann, dass sie den Zugang über die von TwinCAT 3.1 XAR implementierten Protokolle sicher authentifiziert. Bei dieser Perimetersicherheit markieren die Netzwerkschnittstellen des IPCs die Grenze. Das von Beckhoff für diese Art von Sicherheit identifizierte Sicherheitsrisiko besteht darin, dass ein nicht autorisierter Benutzer über die von TwinCAT 3.1 XAR implementierten Protokolle Zugriff auf den IPC erhält. Aus historischen Gründen und wegen der Abwärtskompatibilität stellt TwinCAT 3.1 XAR nach wie vor Protokolle zur Verfügung, die vor einem solchen Zugriff keine Authentifizierung vornehmen. Einige IPCs mit vorinstalliertem TwinCAT 3.1 XAR haben eine Konfiguration für TwinCAT 3.1 XAR, die standardmäßig sicher ist. Das bedeutet, dass diese Standardkonfiguration nur sichere Protokolle von TwinCAT 3.1 XAR aktiviert. Bitte beachten Sie, dass viele IPCs, die mit vorinstalliertem TwinCAT 3.1 XAR ausgeliefert werden, aus Gründen der Abwärtskompatibilität keine standardmäßig sichere Konfiguration haben. Dieser Sicherheitsleitfaden enthält eine vollständige Liste der Protokolle, die von TwinCAT 3.1 XAR unterstützt werden, und gibt Auskunft darüber, welche Protokolle sicher sind, siehe: Wichtige TCP/UDP-Ports [▶ 30]. Für die anderen Softwareprodukte sind eigene Dokumentationen und Anleitungen vorhanden. Bitte beachten Sie Folgendes: Letzteres gilt auch für TwinCAT-Funktionen, die über einen separaten Installer zu TwinCAT 3.1 XAR hinzugefügt werden können.

2 Gefährdungen und Risikobestimmung

Dieser Abschnitt gibt einen Überblick über die Gefährdungen und die Risikobestimmung eines Automatisierungssystems. Es werden verschiedene Angreifer und Angriffstypen sowie typische Bedrohungsszenarien und Schutzprinzipien beschrieben.

2.1 Angreifer

Klassifikation nach Position eines Angreifers

Angreifer können gemäß ihrem Zugriff auf ein System in vier Klassen eingeteilt werden:

Klasse	Beschreibung
Insider Angreifer	Angreifer, die bestimmte Handlungen am Automatisierungssystem durchführen sollen. Die Angreifer versuchen jedoch schädliche Handlungen durchzuführen, zu denen sie nicht autorisiert sind. Zusätzlich verfügen diese Angreifer über private Informationen, wie beispielsweise Passwörter, die sie zur Durchführung autorisierter Handlungen brauchen.
Lokale Angreifer	Angreifer, die direkten Zugriff auf Komponenten des Automatisierungssystems haben. Die Klasse umfasst auch lokale Angreifer, die auf manche Komponenten per Hardwareschnittstellen direkt zugreifen oder die Netzwerktopologie an verschiedenen Stellen verändern können.
Angreifer im internen Netzwerk	Angreifer, die Geräte im internen Netzwerk kontrollieren. Diese Angreifer können die Netzwerktopologie im Allgemeinen nicht ändern und nur über vorhandene Dienste im Netzwerk verfügen.
Angreifer aus einem externen Netzwerk	Angreifer, die nur durch Schnittstellen, die z. B. an das Internet angebunden sind, Handlungen ausführen können. Mit erfolgreichen Angriffen auf interne Komponenten können diese Angreifer zu Angreifer im internen Netzwerk eskalieren.

Annahmen

Für alle Angreifer muss angenommen werden,

- dass sie öffentliche Informationen wie Dokumentationen aus dem Internet oder über Service-Anrufe erhalten können.
- dass sie alle Produkte am öffentlich verfügbaren Markt erwerben und durch deren Analyse Angriffe gezielt vorbereiten können.
- dass sie über große Rechenleistung verfügen, beispielsweise durch Anmietung von Rechenzeit bei einem Cloud-Anbieter.

Die manchmal propagierte Kategorisierung nach Motivation eines Angreifers ist im Allgemeinen nicht zielführend, da dort viele Abschätzungen und Spekulationen vorgenommen werden.

Die Klassifizierung hilft beim Erstellen von Security-Analysen, jedoch ist zu beachten, dass ein realer Angreifer durchaus in mehreren Kategorien verschiedene Fähigkeiten hat.

2.2 Angriffstypen

Angriffe können gemäß ihrer Durchführung kategorisiert werden. Dabei spielt der Aufwand des Angriffs eine entscheidende Rolle:

Kategorie	Beschreibung
Breite, virale Angriffe	Die Angriffe nutzen weitverbreitete Schwachstellen und verbreiten sich auf erreichbare Nachbarn. Diese ungezielten Angriffe („untargeted attacks“) zielen darauf ab, möglichst viele betroffene Systeme zu befallen, um daraus Gewinne für den Angreifer zu generieren. Die Gewinne für den Angreifer entstehen beispielsweise durch Erpressung zum Entschlüsseln von Daten („Ransomware“) oder Nutzung der Ressourcen vom Angegriffenen („Botnetz“). Oft nutzen diese Angriffe ungepatchte Schwachstellen oder verbreitete organisatorische Mängel wie die Benutzung von schwachen Passwörtern.
Hersteller- und integratorspezifische Angriffe	Die Angriffe nutzen Schwachstellen, die in bestimmten Produkten vorkommen, die eventuell einen geringeren Verbreitungsgrad haben. Diese Angriffe können sich zwar auch automatisch ausbreiten, haben aber spezielle Produkte oder Konfigurationen als Schwachstelle im Fokus (bspw. von Beckhoff oder ggf auch Konfigurationen / Erweiterungen des Integrators). Angriffsziele können auch branchenspezifisch sein, wie zum Beispiel das Ausspähen von Know-how oder ähnliches.
Betreiberspezifische Angriffe	Die Angriffe sind gegen genau eine Anlageninstallation („targeted attacks“) gerichtet. Diese Angriffe sind schwer zu entdecken und aufwändig vom Angreifer durchgeführt. Dabei werden gezielte Systemkonfigurationen ausgenutzt, um das Angriffsziel zu erreichen. Angriffsziele sind dabei vielfältig und können im Allgemeinen nicht vorhergesehen werden.

In diesem Security-Leitfaden werden nur Maßnahmen gegen breite virale und herstellerspezifische Angriffe vorgestellt. Betreiberspezifische Angriffe erfordern Analysen und Gegenmaßnahmen des Betreibers.

2.3 Typische Bedrohungsszenarien

In diesem Abschnitt werden typische Bedrohungen beschrieben. Die Liste erhebt jedoch keinen Anspruch auf Vollständigkeit.

Manipuliertes Boot-Medium

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	ausgeschlossen	ausgeschlossen	ausgeschlossen
Hersteller- und integratorspezifische Angriffe	trifft zu	trifft zu	ausgeschlossen	ausgeschlossen

Ein vorbereiteter Datenträger wird an eine Komponente angeschlossen und die Komponente von diesem gebootet. Dies ist dann möglich, wenn im UEFI/BIOS die Boot-Reihenfolge so eingestellt ist, dass von externen Datenträgern gebootet wird oder die Boot-Reihenfolge im UEFI/BIOS für den Angreifer änderbar ist.

Durch den Angriff kann ein Angreifer auf alle Daten der Komponente lesend und schreibend zugreifen, insbesondere auf Konfigurationen und Know-How. Nach einem derartigen Zugriff muss die Gesamtkomponente als unsicher angesehen werden.

Abwehrmaßnahmen:

- BIOS-Passwort (BIOS-Einstellungen [▶ 17])
- Boot-Medien festlegen (BIOS-Einstellungen [▶ 17])
- Abgeschlossener Schaltschrank [▶ 15]

Unautorisierter PXE-Boot-Server

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	ausgeschlossen	trifft zu	ausgeschlossen
Hersteller- und integratorspezifische Angriffe	ausgeschlossen	ausgeschlossen	trifft zu	ausgeschlossen

Von einem unautorisierten PXE-Boot-Server im internen Netzwerk wird gebootet. Dabei wird vom Angreifer kontrollierter Code ausgeführt.

Durch den Angriff kann ein Angreifer auf alle Daten der Komponente lesend und schreibend zugreifen, insbesondere auf Konfigurationen und Know-how. Nach einem derartigen Zugriff muss die Gesamtkomponente als unsicher angesehen werden.

Abwehrmaßnahmen:

- PXE-Boot abschalten (BIOS-Einstellungen [▶ 17])

Manipulierte USB-Geräte

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	trifft zu	ausgeschlossen	ausgeschlossen
Hersteller- und integratorspezifische Angriffe	trifft zu	trifft zu	ausgeschlossen	ausgeschlossen

Wenn manipulierte USB-Geräte angeschlossen werden, kann unter Umständen auf dem betroffenen Gerät Schadcode ausgeführt werden. Außerdem kann das betroffene USB-Gerät auch zum Diebstahl von Know-how verwendet werden. Beispielsweise kann durch einen konfigurierten Autostart beliebiger Code ausgeführt werden. Durch ein präpariertes Eingabegerät können unautorisierte Eingaben vorgenommen oder auch mitprotokolliert werden.

Durch einen solchen Angriff kann ein Angreifer auf viele Daten über das Betriebssystem lesend und schreibend zugreifen, insbesondere auf Konfigurationen und Know-how. Nach einem derartigen Zugriff muss die Gesamtkomponente als unsicher angesehen werden.

Abwehrmaßnahmen:

- Whitelisting USB-Geräte (USB-Filter [▶ 27])
- Abgeschlossener Schaltschrank [▶ 15]
- Schnittstellen im BIOS abschalten (BIOS-Einstellungen [▶ 17])
- Whitelisting für Programme [▶ 26]

Erraten schwacher Passwörter durch lokales Interface

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	ausgeschlossen	ausgeschlossen	ausgeschlossen
Hersteller- und integratorspezifische Angriffe	trifft zu	trifft zu	ausgeschlossen	ausgeschlossen

Schwache Passwörter wie Standardpasswörter oder leicht zu erratende Passwörter können durch lokale Angreifer ausgenutzt werden. Ebenso wie autorisierte lokale Nutzer können Angreifer sich mit unveränderten Standardpasswörtern anmelden.

Durch einen solchen Angriff kann ein Angreifer auf viele Daten über das Betriebssystem lesend und schreibend Zugreifen, insbesondere auf Konfigurationen und Know-how. Nach einem derartigen Zugriff muss die Gesamtkomponente als unsicher angesehen werden.

Abwehrmaßnahmen:

- Sichere Passwörter [▶ 21]
- Individuelle Benutzer einrichten, keine Sammelaccounts
- Minimale Rechte für Benutzer („Least Privilege“) insbesondere keine Administrator-Rechte, wenn nicht notwendig

Diebstahl von Datenträgern

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	ausgeschlossen	ausgeschlossen	ausgeschlossen
Hersteller- und integratorspezifische Angriffe	trifft zu	trifft zu	ausgeschlossen	ausgeschlossen

Durch unautorisiertes Entfernen von Datenträgern kann ein Angreifer mögliches Know-how über und Zugangsdaten zu Diensten im Automatisierungssystem erlangen.

Ein solcher Angriff ermöglicht es einem Angreifer, Lesezugriff auf eine große Anzahl von Daten zu erlangen, die sich auf das Betriebssystem beziehen, insbesondere auf Zugangsdaten, Konfigurationen, Know-how und andere sensible private Daten.

Ein Angreifer könnte auch versuchen, sich Zugang zu sensiblen Daten zu verschaffen, indem er die Speichermedien nach deren Entsorgung stiehlt.

Abwehrmaßnahmen:

- Abgeschlossener Schaltschrank [▶ 15]
- Sichere Datenvernichtung

Extraktion sensibler Daten aus weggeworfenem Material

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	ausgeschlossen	ausgeschlossen	ausgeschlossen
Hersteller- und integratorspezifische Angriffe	trifft zu	trifft zu	ausgeschlossen	ausgeschlossen

Ein Angreifer kann sich Zugang zu weggeworfenem Material verschaffen, das sensible Daten auf Speichermedien enthält.

Ein solcher Angriff ermöglicht es einem Angreifer, Lesezugriff auf eine große Anzahl von Daten zu erlangen, die sich auf das Betriebssystem beziehen, insbesondere auf Zugangsdaten, Konfigurationen, Know-how und andere sensible private Daten.

Abwehrmaßnahmen:

- Sichere Datenvernichtung

Behandlung nicht vertrauenswürdiger E-Mails

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	ausgeschlossen	trifft zu	trifft zu
Hersteller- und integratorspezifische Angriffe	ausgeschlossen	ausgeschlossen	trifft zu	trifft zu

Nicht vertrauenswürdige E-Mails sind typische Verbreitungswege von Malware. Vor allem das Öffnen von Hyperlinks mit veralteten Browsern und von E-Mail-Anhängen wird für Angriffe ausgenutzt. Manchmal werden E-Mails gezielt so formuliert, dass diese vertrauenswürdig erscheinen.

Ein erfolgreicher Angriff kann unautorisierte Handlungen ausführen, die mit den Berechtigungen des interagierenden Benutzers ausgeführt werden.

Abwehrmaßnahmen:

- Keine E-Mails an Steuerungsrechnern behandeln
- Regelmäßige oder automatische Software-Aktualisierungen (Updates [▶ 20])
- Whitelisting für Programme [▶ 26]

Ausnutzung bekannter Schwachstellen in veralteter Software

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	trifft zu	trifft zu	trifft zu	trifft zu
Hersteller- und integratorspezifische Angriffe	trifft zu	trifft zu	trifft zu	trifft zu

Bereits bekannte Schwachstellen werden von Herstellern in aktualisierten Versionen behoben. Falls genutzte Software nicht aktualisiert wird, können vor allem breit virale Angriffe erfolgreich durchgeführt werden.

Ein erfolgreicher Angriff kann unautorisierte Handlungen ausführen, die im Kontext der betroffenen Software Auswirkungen hat.

Abwehrmaßnahmen:

- Regelmäßige oder automatische Software-Aktualisierungen (Updates [▶ 20])
- Netzwerkbasierte Erkennungsmechanismen (IDS/IPS)
- Abschalten nicht benötigter Dienste
- Entfernen nicht mehr benötigter Komponenten [▶ 26]

Manipulierte Webseiten

Angriffstyp/Angreifer	Insider	Lokal	Internes Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	ausgeschlossen	ausgeschlossen	trifft zu
Hersteller- und integratorspezifische Angriffe	ausgeschlossen	ausgeschlossen	ausgeschlossen	trifft zu

Ein Benutzer wird dazu gebracht, eine nicht vertrauenswürdige Webseite zu besuchen. Dabei wird eine Schwachstelle im Browser ausgenutzt, um beliebigen Schadcode auszuführen, oder die Webseite ist so gestaltet, dass der Benutzer vertrauliche Information wie Login-Daten preisgibt.

Ein erfolgreicher Angriff kann unautorisierte Handlungen ausführen, die mit den Berechtigungen des interagierenden Benutzers ausgeführt werden.

Abwehrmaßnahmen:

- Regelmäßige oder automatische Software-Aktualisierungen (Updates [▶ 20])
- Organisatorische Maßnahmen zur Verhaltensweise beim Surfen im Web.

Man-in-the-Middle-Angriffe

Angriffstyp/Angreifer	Insider	Lokal	Interne Netzwerk	Remote
Breite, virale Angriffe	trifft zu	ausgeschlossen	ausgeschlossen	ausgeschlossen
Hersteller- und integratorspezifische Angriffe	trifft zu	trifft zu	trifft zu	trifft zu

Bei Nutzung eines nicht sicheren Netzwerkprotokolls kann ein Angreifer sich im Rahmen des erreichbaren Netzwerks für alle Beteiligten als die vertrauenswürdige Gegenstelle ausgeben. Dadurch kann die über dieses Protokoll versendete Information manipuliert oder abgehört werden.

Ein erfolgreicher Angriff kann zu unerwartetem Verhalten der Dienste im Automatisierungssystem führen.

Abwehrmaßnahmen:

- Netzsegmentierung
- Nutzung gesicherter Netzwerkprotokolle

Unautorisierte Nutzung von Netzwerkdiensten

Angriffstyp/Angreifer	Insider	Lokal	Interne Netzwerk	Remote
Breite, virale Angriffe	ausgeschlossen	ausgeschlossen	trifft zu	trifft zu
Hersteller- und integratorspezifische Angriffe	ausgeschlossen	ausgeschlossen	trifft zu	trifft zu

Falls Netzwerkdienste bereitgestellt werden, auf die ein Angreifer zugreifen kann, könnten dadurch unautorisierte Handlungen ausgeführt werden.

Ein erfolgreicher Angriff kann zu unerwartetem Verhalten der Dienste im Automatisierungssystem führen.

Abwehrmaßnahmen:

- Netzsegmentierung
- Nutzung von authentifizierenden Netzwerkdiensten
- Abschalten nicht benötigter Dienste
- Entfernen nicht mehr benötigter Komponenten [▶ 26]

3 Allgemeine Maßnahmen

3.1 Schulung der Mitarbeiter

Geschultes Personal ist ein wichtiger Schutz für das System. Mitarbeiter, die Zugriff auf das Gerät haben, sollten wissen wie dieses zu bedienen ist. Dazu zählen generelle Maßnahmen wie der verantwortungsbewusste Umgang mit Passwörtern und Datenträgern wie z. B. USB-Sticks. Jedem Mitarbeiter sollten beim Eingriff in das System mögliche Auswirkungen bewusst sein.

3.2 Physische Maßnahmen

Eine der leichtesten und sichersten Schutzmaßnahmen ist der physische Schutz. Stellen Sie sicher, dass nur Administratoren und Techniker Zugang zu dem Gerät haben. Angriffe über einen physischen Zugang wie beispielsweise USB-Sticks und andere Datenträger, die eine der größten Risiken darstellen, können so verringert werden. Der physische Schutz eines Gerätes wird z. B. durch einen abschließbaren Schaltschrank erreicht.

Abgeschlossener Schaltschrank

Die Standardumgebung für einen industriellen Controller sollte ein abgeschlossener Schaltschrank sein. Die Angriffsoberfläche wird stark reduziert, indem nur einzelne Schnittstellen aus dem Schaltschrank herausgeführt werden. Die dort herausgeführten Schnittstellen sollten zusätzlich geschützt werden (abschließbar). Zum Schaltschrank sollten nur Personen Zugriff haben, die diesen auch für die Erledigung ihrer Aufgaben benötigen. Es können auch elektronische Schließsysteme zum Beispiel mit Smartcards zum Einsatz kommen. Wie bei jedem Schlüsselmanagement muss beachtet werden, dass Personen der Zugang zum Schaltschrank wieder entzogen wird, wenn der Zugriff nicht mehr erforderlich ist.

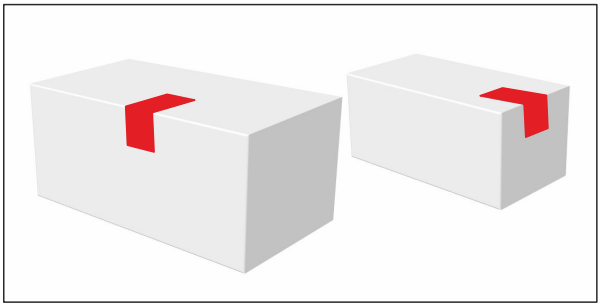
Videoüberwachung

Videoüberwachung ist für Umgebungen geeignet, in denen in Schichten gearbeitet wird und deswegen viele Personen Zugriff auf einen Controller benötigen oder in denen Anlagen geographisch weit verteilt sind. Videoüberwachung kann Angriffe jedoch nur erkennen und nicht verhindern. Diese Maßnahme ist deswegen nur in Kombination mit anderen Maßnahmen sinnvoll einsetzbar.

3.3 Security-Siegel auf Produktverpackungen

Ab Ende des Jahres 2021 werden ab Werk auf bestimmten Produktverpackungen für Industrie-PCs und Embedded-PCs Siegel mit Sicherheitsmerkmalen aufgebracht:

Die Position und Beschaffenheit des Siegels bewirken, dass das Entnehmen der Ware aus der Verpackung zu unumkehrbaren und sichtbaren Veränderungen an der Verpackung und dem Siegel führen. Durch eine Sichtprüfung kann somit die Unversehrtheit des Produktes vor dem Öffnen überprüft werden.



Das Siegel ist eine Hilfestellung, um bei der Kontrolle von verpackten Produkten effizient vorgehen zu können. Weil es keine absolute Sicherheit gibt, ist der Nutzen des Siegels auf die folgende Anwendung begrenzt: Es erlaubt eine begründete Vermutung über die Unversehrtheit, Vollständigkeit und Echtheit der Ware in der Verpackung, ohne die Verpackung öffnen zu müssen. Falls das Siegel oder die Verpackung beschädigt sind, sollte sich der Empfänger bei der Annahme oder vor der Verwendung der Ware von ihrem korrekten Zustand überzeugen. Falls die Ware für Anwendungen gedacht ist, bei denen Aspekte der IT-Security relevant sind, kann der Empfänger der Ware zum Beispiel bestimmen, dass die Ware vor Verwendung auf Manipulation überprüft wird, wenn der Zustand von Siegel oder Verpackung die Möglichkeit einer Manipulation während des Versandes vermuten lassen.

Die Gestaltung und Bestimmung sinnvoller Prozesse und Regeln bei Annahme und vor Verwendung von Produkten von Beckhoff bleibt in der Verantwortung des Empfängers.

Geöffnetes Siegel

Produkte von Beckhoff erreichen den Empfänger oft über eine mehrstufige Distributionskette. Möglicherweise wurde das Siegel in der Verarbeitung des Produkts geöffnet. Ein geöffnetes Siegel begründet keinen Gewährleistungsanspruch.

4 BIOS-Einstellungen

Es wird empfohlen, ein Passwort für das BIOS zu setzen, um sicherzustellen, dass kritische Einstellungen wie die Boot-Reihenfolge, der CPU-Takt oder die gesamten Einstellungen nicht unautorisiert geändert werden. Außerdem kann es sinnvoll sein, die Boot-Reihenfolge festzulegen und ein Starten von externen Datenträgern zu unterbinden. Einstellungen im BIOS sollten nur von versierten Personen durchgeführt werden. Das Verstellen unbekannter Parameter kann sich negativ auf die Funktion des Systems auswirken.

5 Betriebssystem

5.1 Wiederherstellungsoptionen

Definieren Sie eine Backup- und Wiederherstellungsstrategie für Ihr Beckhoff RT Linux®-System, um im Falle eines Datenverlustes oder bei defekten Speichermedien Beckhoff RT Linux® in sehr kurzer Zeit wiederherstellen zu können. Backups tragen dazu bei, Ausfallzeiten zu minimieren und auf diese Weise die Arbeit ohne große Produktionsverluste fortzusetzen. Es sollte sowohl ein Prozess für die Erstellung einer Sicherheitskopie als auch ein Prozess für deren Wiederherstellung definiert werden. Dabei sollten auch Security-Aspekte berücksichtigt werden und beispielsweise definiert werden, wo das Backup gespeichert wird. Zusätzlich sollen in Zukunft Wiederherstellungspunkte dazu dienen, den aktuellen Zustand des Systems zu speichern und bei Bedarf wiederherzustellen. Eine Vielzahl von Implementierungen wird somit verfügbar sein, wobei die genaue Definition einer Backup- und Wiederherstellungsstrategie dem Anwender überlassen ist.

5.1.1 Backup und Restore

In diesem Kapitel wird beschrieben, wie ein Backup eines Beckhoff RT Linux®-Images als Sicherheitskopie erstellt und wiederhergestellt werden kann. Das Backup kann auf einem externen Speichermedium gespeichert und verwaltet werden, um das System im Fall eines Systemausfalls bzw. eines Datenverlustes wiederherzustellen. Erstellen Sie regelmäßig Backups von Ihrem System.

5.1.1.1 Backup erstellen

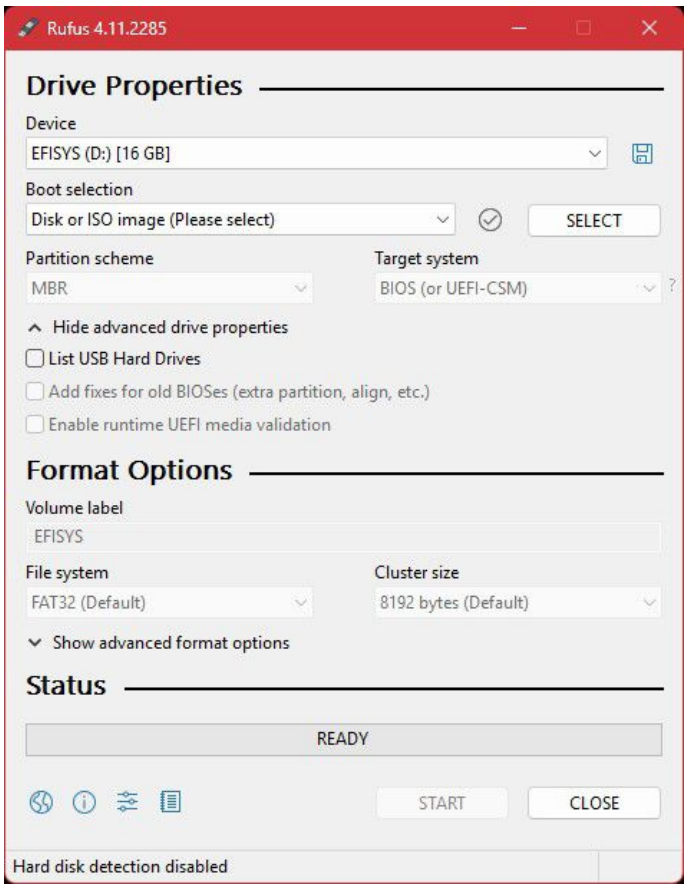
In diesem Kapitel wird beschrieben, wie Sie mithilfe des Flashtools Rufus eine Sicherheitskopie eines Beckhoff-RT-Linux®-Images erstellen können. Die Sicherheitskopie wird im VHDX-Format angelegt. Dabei ist es egal, welches Speichermedium für die Sicherung verwendet wird. Es kann sich dabei sowohl um eine MicroSD- als auch um eine CFast-Karte handeln.

Voraussetzungen:

- Speicherkartenleser
- Rufus herunterladen unter https://rufus.ie/

Gehen Sie wie folgt vor:

1. Starten Sie Rufus auf einem PC mit Windows-Betriebssystem. Das Speichermedium (MicroSD, CFast) sollte unter Windows bereits eingebunden sein.
2. Das Speichermedium, von dem eine Sicherheitskopie erstellt werden soll, erscheint unter **Device**.
3. Klicken Sie auf **Show advanced drive properties**, um erweiterte Einstellungen freizuschalten.
4. Klicken Sie auf das **Diskettensymbol**, um die Speichern-Funktion zu öffnen.



5. Der Dateityp **Compressed VHDX Image (*.vhdx)** ist bereits ausgewählt. Wählen Sie anschließend den passenden Speicherort aus und klicken Sie auf **START**, um die Sicherheitskopie zu erstellen.

⇨ Die erstellte Sicherheitskopie im VHDX-Format können Sie anschließend nach Belieben verwalten oder die Sicherheitskopie und damit das Beckhoff-RT-Linux®-Image wiederherstellen (siehe: Backup wiederherstellen [▶ 19]).

5.1.1.2 Backup wiederherstellen

Geeignetes Backup für die Wiederherstellung verwenden

Vermeiden Sie Inkompatibilitäten und verwenden Sie das passende Backup für Ihr Gerät.

Das Backup eines Beckhoff-RT-Linux®-Images kann prinzipiell auf jedem Speichermedium wiederhergestellt werden. Achten Sie jedoch darauf, dass das Backup nur auf einem Gerät derselben Serie verwendet wird, z. B. CX51x0, CX20x3, C6015 usw., da sonst Inkompatibilitäten auftreten können.

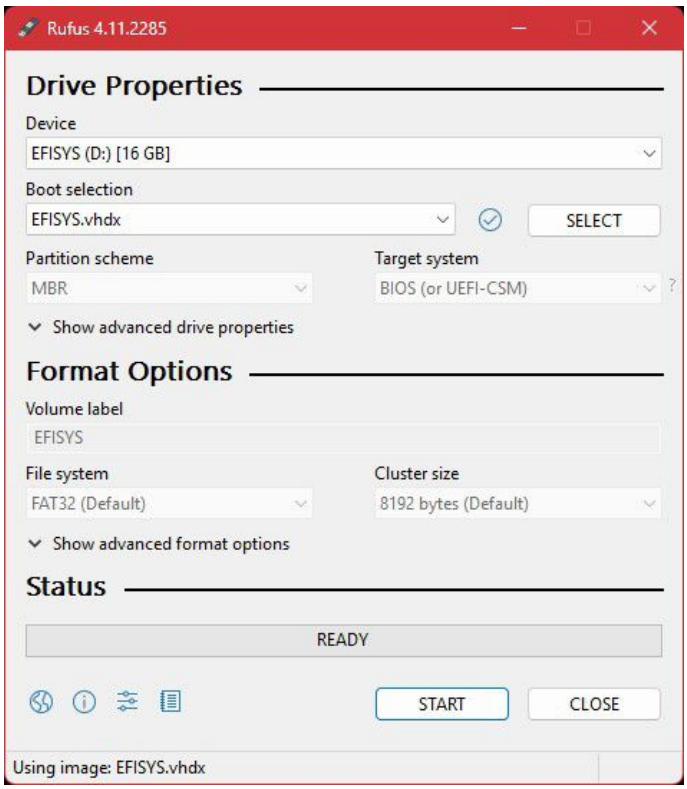
Verwenden Sie dafür ein Flashtool, beispielsweise Rufus. Das Backup wird dabei direkt auf das Speichermedium kopiert, in diesem Beispiel im VHDX-Format.

Voraussetzungen:

- Vorhandenes Backup eines Beckhoff-RT-Linux®-Images (siehe auch: Backup erstellen [▶ 18]).

Gehen Sie wie folgt vor:

1. Starten Sie Rufus auf einem PC mit Windows-Betriebssystem. Das Speichermedium (MicroSD, CFast) sollte unter Windows bereits eingebunden sein.



2. Klicken Sie auf **Select** und wählen Sie das Image aus, welches Sie auf das Speichermedium kopieren möchten.
3. Wählen Sie unter **Device** die MicroSD-Karte als Ziellaufwerk aus.
4. Klicken Sie auf **Start**, um den Kopiervorgang zu starten.

⇨ Der Vorgang kann einige Minuten dauern. Brechen Sie ihn nicht ab, bis die Meldung **Ready** erscheint. Booten Sie anschließend den Industrie-PC vom verwendeten Speichermedium und starten Sie Beckhoff RT-Linux®.

5.2 Updates

Regelmäßige Updates sind wichtig, da sie vor allem bekannte Sicherheitslücken schließen. Sie sollten Sicherheitsupdates zeitnah prüfen und nach erfolgreicher Validierung in das System einspielen. Beckhoff stellt über die öffentlichen, in jedem System voreingestellten Package Server, Updates für das Basissystem sowie alle weiteren Softwarekomponenten bereit.

Für ein Systemupdate sollten Sie folgendermaßen vorgehen:

1. Wenn möglich, zuerst das Update im Zusammenspiel mit eigenen Programmen und der eingesetzten Hardware auf Testhardware prüfen.
2. Ein Backup des Systems durchführen, um im Falle unvorhergesehenen Verhaltens den alten Systemzustand wiederherstellen zu können (siehe: Wiederherstellungsoptionen).
3. Aktualisieren Sie zunächst die Paketinformationen und lassen Sie sich anschließend die Pakete anzeigen, die aktualisiert werden können. Führen Sie danach das Update des gewünschten Pakets oder des gesamten Systems durch.

Die Paketinformationen können Sie mit folgendem Befehl aktualisieren:

```
sudo apt update
```

Die Pakete, für die ein Update verfügbar sind, können Sie mit folgendem Befehl anzeigen lassen:

```
apt list --upgradable
```

Anschließend können Sie ein einzelnes Paket mit folgendem Befehl aktualisieren:

```
sudo apt install
```

Soll das gesamte System aktualisiert werden, können Sie folgenden Befehl verwenden:

```
sudo apt upgrade
```

5.3 Benutzer- und Rechteverwaltung

5.3.1 Sichere Passwörter

Sichere Passwörter sind eine wichtige Voraussetzung für die Gewährleistung der Sicherheit einer Anlage. Beckhoff liefert die Images mit Standardbenutzernamen und Standardpasswörtern für das Betriebssystem aus. Diese müssen vom Kunden unbedingt geändert werden. Andernfalls ist Ihr Gerät über das Netzwerk und den Zugriff durch unautorisiertes Personal angreifbar.

Controller werden ohne Passwort im UEFI/BIOS ausgeliefert. Auch hier wird die Vergabe eines Passworts empfohlen.

Im System ist ein Security-Wizard integriert. Dieser wird unmittelbar nach dem Hochfahren des Gerätes bei einem lokalen Zugang gestartet. Dieser Wizard fordert den Nutzer auf, das Passwort zu ändern. Das Passwort kann jedoch auch lokal mit Mitteln des Betriebssystems geändert werden.

Es gilt:

- Passwörter sollen pro Nutzer und Dienst einzigartig sein.
- Passwortkomplexität: Das Passwort sollte große und kleine Buchstaben, Zahlen, Interpunktionszeichen und Sonderzeichen enthalten.
- Passwortlänge: Das Passwort sollte mindestens 10 Zeichen lang sein.
- Entgegen einiger älterer Empfehlungen wird empfohlen, Passwörter nicht mehr regelmäßig zu ändern, sondern nur nach einem Vorfall, in dem Passwörter unberechtigt bekannt geworden sind. Siehe auch https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/
- Es kann sinnvoll sein, eine Zwangswartezeit nach erfolgloser Authentifizierung mittels Passwort vorzusehen.

Sicheres Passwort generieren

Es gibt viele Wege, ein sicheres Passwort zu erzeugen. In der folgenden Tabelle wird eine Möglichkeit der Passwortgenerierung beschrieben. Die Vorgehensweise kann gleichzeitig dabei helfen, sich an komplexe Passwörter zu erinnern:

Vorgehensweise	Beispiel
1. Beginnen Sie mit ein bis zwei Sätzen.	Komplexe Passwörter sind sicherer
2. Entfernen Sie die Leerzeichen.	KomplexePasswörtersindsicherer
3. Kürzen Sie Wörter ab oder fügen sie Rechtschreibfehler ein.	KomplxPasswörtersinsicerer
4. Fügen Sie Zahlen und Sonderzeichen ein, um das Passwort zu verlängern.	KomplxPasswörtersinsicerer#529954#

Problematische Passwörter

Cyber-Kriminelle verwenden ausgeklügelte Werkzeuge, die performante Angriffe auf Passwörter ermöglichen. Vermeiden Sie deshalb:

- Wörter, die in Wörterbüchern stehen
- Rückwärts geschriebene Wörter, gebräuchliche Rechtschreibfehler und Abkürzungen
- Folgen aus der Wiederholung von Zeichen, z. B. 12345678 oder abcdefgh
- Persönliche Informationen, z. B. Geburtstage, Ausweisnummern, Telefonnummern

5.3.1.1 Passwort ändern

Das Passwort des jeweils eingeloggten Benutzers ändern Sie mit dem Befehl `passwd`. Beachten Sie, dass Sie mit `sudo passwd`, den Befehl mit Root-Rechten verwenden und damit das Passwort des Superusers-Accounts (`root`) ändern und nicht die des eingeloggten Benutzers. Führen Sie `passwd` nicht mit Root-Rechten aus.

Bei Auslieferung von Beckhoff RT Linux® ist standardmäßig ein Benutzer (`Administrator`) vorhanden, mit dem Sie sich in der Konsole anmelden können. Er besitzt keine klassischen Administrator-Rechte wie unter Windows-Systemen, hat jedoch die Berechtigung, sich für bestimmte Zwecke mit `sudo` Root-Rechte zu beschaffen.

Anmeldedaten:

- Login: Administrator
- Passwort: 1

Gehen Sie wie folgt vor:

1. Starten Sie den Industrie-PC.
2. Loggen Sie sich mit dem Benutzernamen `Administrator` und dem Passwort `1` ein.
3. Nach erfolgreicher Anmeldung werden der Benutzer und der Hostname des Industrie-PCs angezeigt. Zum Beispiel: CX-1D7BD4.
4. Geben Sie den Befehl `passwd` ein, um ein neues Passwort festzulegen. Folgen Sie den weiteren Anweisungen.

⇨ Sie haben erfolgreich ein neues Passwort festgelegt.

5.3.1.2 Passwortrichtlinien

Eine eigene Passwortrichtlinie schützt das System vor der Verwendung schwacher Passwörter. Legen Sie Länge und Komplexität der verwendeten Benutzerpasswörter fest und beachten Sie die nachfolgenden Empfehlungen:

Zum Definieren einer Passwortrichtlinie bearbeiten Sie die Datei `/etc/pam.d/passwd` wie folgt:

```
sudo nano /etc/pam.d/passwd
```

Fügen Sie je nach Anforderung einen Eintrag für das Modul pam_passwdqc hinzu oder passen Sie einen vorhandenen Eintrag entsprechend an. Eine mögliche Konfiguration ist beispielsweise:

```
password requisite pam_passwdqc.so min=disabled,disabled,disabled,disabled,10 similar=deny retry=3
en-force=users
```

```
@include common password
```

Ist bereits ein entsprechender Eintrag für `pam_passwdqc` vorhanden, passen Sie diesen an und fügen Sie keinen zweiten Eintrag hinzu. Bereits vorhandene PAM-Zeilen zur eigentlichen Passwortverarbeitung dürfen nicht entfernt werden.

Hinter `pam_passwdqc.so` können für den Parameter mindestens fünf Werte gesetzt werden. Diese fünf Werte stehen für vordefinierte Passwortkategorien. Jede Position kann entweder mit disabled deaktiviert oder mit einer Zahl für die geforderte Mindestlänge belegt werden. Die Positionen stehen für folgende Passwortkategorien:

- Passwörter aus einer Zeichenklasse, d. h. Passwörter, die nur aus Zahlen oder nur aus Klein- oder Großbuchstaben bestehen;
- Passwörter aus zwei Zeichenklassen, d. h. Passwörter, die beispielsweise aus Klein- und Großbuchstaben bestehen;
- Passphrasen, d. h. Aneinanderreihungen von Zeichenketten, die durch Leerzeichen voneinander getrennt sein können;
- Passwörter aus drei Zeichenklassen, beispielsweise aus Klein- und Großbuchstaben sowie Zahlen;
- Passwörter aus vier Zeichenklassen, d. h. aus Klein- und Großbuchstaben sowie Zahlen und Sonderzeichen.

Das dargestellte Beispiel erlaubt somit nur Passwörter, die aus allen vier Zeichenklassen bestehen und mindestens 10 Zeichen lang sind.

Der Parameter `similar=deny` legt fest, dass das neue Passwort dem bisherigen Passwort nicht ähneln darf. Der Parameter `retry=3` bestimmt, wie oft ein Benutzer zur Eingabe eines neuen Passworts aufgefordert wird, wenn das gewählte Passwort die Anforderungen der Passwortrichtlinie nicht erfüllt. Mit `enforce=users` wird die Richtlinie für Benutzerkonten verbindlich angewendet.

5.3.2 Automatisches Abmelden

Bei konfiguriertem Autologout wird ein Benutzer nach einer bestimmten Zeit, in der er nicht mit der Kommandozeile interagiert, automatisch ausgeloggt. Das soll vermeiden, dass Unbefugte Zugang zur Kommandozeile bekommen, wenn der IPC unbeaufsichtigt ist und ein Ausloggen durch den Benutzer versäumt wurde. Standardmäßig ist der Autologout nicht aktiv, sollte aber zur Inbetriebnahme eingeschaltet werden.

Zum Aktivieren des Autologouts bearbeiten Sie die Datei */etc/profile.d/autologout.sh* mit Root-Rechten, beispielsweise wie folgt:

```
sudo nano /etc/profile.d/autologout.sh
```

Fügen Sie die folgenden Zeilen hinzu:

```
export TMOUT=300
readonly TMOUT
```

Neu einloggen, damit der User nach 300 Sekunden (5 Minuten) automatisch ausgeloggt wird.

5.3.3 Gruppen- und Dateiberechtigungen

Beckhoff RT Linux® verwendet die Zugriffskontrollliste, die auch von anderen UNIX®-ähnlichen Systemen verwendet wird. Es gibt im Allgemeinen drei Arten von Benutzern, für die Sie die Berechtigungen definieren können: Eigentümer der Dateien, Gruppe des Eigentümers und alle anderen Benutzer (Eigentümer / Gruppe / Andere). Für jeden Benutzertyp können Sie Schreib-, Lese- und Ausführungsrechte für eine Datei festlegen.

Anzeigen der Berechtigungen von Dateien und Verzeichnissen an einem Ort mit `ls -l`

```
Administrator@CX-0C8440$ ls -l
total 10
-rw-r--r--  1 root           Administrator   5 Dec  4 12:31 file
-rw-r--r--  2 Administrator  Administrator  10 Dec  4 15:29 test
drwxr-xr-x  3 Administrator  Administrator   6 Dec  7 10:44 testdir
```

In der ersten Spalte steht das Berechtigungsschema, gefolgt von dem Eigentümer der Datei und der Gruppe des Eigentümers. Das Berechtigungsschema ist in vier Teile unterteilt. Das erste Symbol zeigt den Typ der Datei an, ob es sich um eine Datei (-) oder ein Verzeichnis (d) handelt. Die nächsten drei Symbole zeigen die Rechte des Eigentümers, die folgenden drei Symbole die Rechte der Gruppe und die letzten drei Symbole die Rechte für alle anderen Benutzer. Das erste dieser drei Symbole zeigt an, ob Leserechte erteilt wurden (r), das zweite, ob Schreibrechte erteilt wurden (w) und das dritte Symbol zeigt an, ob die Datei ausgeführt werden kann oder auf ein Verzeichnis zugegriffen werden kann (x). Das Berechtigungsschema der obigen Ausgabe von `ls -l` kann wie folgt gelesen werden:

Type	Owner	Group	Other
- file	rw- read write	r-- read	r-- read
- file	rw- read write	r-- read	r-- read
d directory	rwx read write execute	r-x read execute	r-x read execute

Standardmäßig erhält eine neue Datei die Rechte `-rw-r--r--`, d. h. neue Skripte müssen erst ausführbar gemacht werden. Mit den Standardberechtigungen kann selbst der Superuser Root das Skript nicht ausführen.

Um die Berechtigungen über ihren Entwicklungsrechner remote zu ändern, können Sie WinSCP verwenden, beschrieben in der Twin-CAT/BSD-Dokumentation im Kapitel "Dateien verwalten mit WinSCP-Client". Lokal können die Berechtigungen über das Programm `chmod` geändert werden. Geben Sie `man chmod` für das lokale Handbuch ein.

Unprivilegierte Benutzer anlegen

Es ist ratsam, verschiedene Benutzer für unterschiedliche Aufgaben zu verwenden, wie etwa einen "HMI-Benutzer" oder einen Benutzer "maintenance". Geben Sie jedem Benutzer die Rechte, die er für seine Aufgaben benötigt, und stellen Sie sicher, dass nur die verantwortlichen Benutzer Root-Rechte erhalten können. Um ein Benutzerkonto zu erstellen, verwenden Sie den folgenden Befehl:

```
sudo adduser benutzername
```

Dies startet einen Assistenten, der Sie durch den Prozess der Benutzererstellung führt. Um ein Benutzerkonto zu bearbeiten, verwenden Sie `sudo usermood [Optionen] <Benutzer>`

Gruppen

Benutzer werden in eine oder mehrere Gruppen eingeteilt. Beim Anlegen eines neuen Benutzers wird standardmäßig eine Gruppe mit demselben Namen angelegt. Zusätzlich können Benutzer mit ähnlichen Aufgaben einer gemeinsamen Gruppe zugewiesen werden, um ähnliche Berechtigungen zu erhalten. Diese Berechtigungen können der Zugriff auf bestimmte Ordner und Dateien sowie das Ausführen von Programmen sein.

Benutzern, die der Gruppe "sudo" zugewiesen sind, können Root-Rechte gewährt werden. Der vorkonfigurierte Benutzer "Administrator" ist ein "sudo"-Mitglied und erhält Root-Rechte, indem er den Befehl `sudo` vor Programme setzt und sich nochmals mit seinem Passwort authentifiziert.

Legen Sie neue Gruppen an, indem Sie `sudo addgroup <Gruppenname>` ausführen und anschließend `sudo usermod -aG <Gruppenname> <Benutzer>` um einen Benutzer zu einer Gruppe hinzuzufügen.

Darüber hinaus werden mit `sudo cat /etc/group` alle verfügbaren Gruppen angezeigt. Die meisten angezeigten Gruppen sind Standard-Gruppen und stammen aus der UNIX®-Tradition. Aus Sicherheitsgründen werden diese Gruppen Systembenutzern zugewiesen, die eine bestimmte Aufgabe haben. Andernfalls würden diese Programme mit Root-Rechten ohne Einschränkungen ausgeführt werden.

5.3.4 Überwachungsrichtlinien

Im Rahmen eines Sicherheitskonzepts für die Integration eines Geräts in ein Netzwerk sollte festgelegt werden, welche Stufe des Sicherheitsaudits geeignet ist, um potenzielle Angriffe zu erkennen. Sicherheitsaudit bedeutet, dass ein Industrie-PC Audit-Protokolle über Ereignisse erstellt, sobald mit dem Gerät interagiert wird. So können beispielsweise Datei- und Ordnerzugriffe protokolliert werden, jedes Mal, wenn ein Benutzer auf die ausgewählten Dateien oder Ordner zugreift.

Diese Protokolle sind zur Überprüfung vorgesehen, um Abweichungen von der normalen Nutzung zu erkennen, die auf einen Angriff hindeuten könnten, oder zu forensischen Zwecken, um Details über einen Angriff zu rekonstruieren. Die Überprüfung kann sofort oder in regelmäßigen Abständen durch automatisierte Mechanismen oder manuell erfolgen. Es hängt von der Umgebung und der Anwendung ab, welche Abweichungen relevant sind. Daher werden Regeln, die beschreiben, welche Aktionen protokolliert werden, üblicherweise mit Hilfe von Überwachungsrichtlinien konfiguriert.

Die Konfiguration zu vieler Regeln kann jedoch zu einer Art Blindheit führen. Die Protokolle können mit irrelevanten Einträgen überfrachtet werden, wobei die relevanten Einträge von Menschen leicht übersehen oder von automatischen Überwachungsmechanismen nicht schnell genug verarbeitet werden. Manchmal ist es eine gute Praxis, Protokolle an eine zentrale Stelle zur automatischen Überprüfung und/oder Archivierung weiterzuleiten, um unter anderem eine begrenzte Protokollkapazität nicht zu erschöpfen.

Datei- und Ordnerzugriffe sowie sicherheitsrelevante Benutzereingaben können unter Beckhoff RT Linux® protokolliert werden. Jedes Mal, wenn ein Benutzer eine definierte Aktion ausführt, wird das Ereignis geloggt. Diese Ereignisprotokolle sind vor allem für die Überwachung des Systems, die Erkennung unberechtigter Zugriffe und für die anschließende Analyse nach einem Sicherheitszwischenfall von Bedeutung.

Installieren und aktivieren Sie den Audit-Daemon:

```
sudo apt update
sudo apt install auditd audispd-plugins
sudo systemctl enable auditd
```

Starten des Audit-Daemons:

```
sudo systemctl start auditd
```

Prüfen des Status:

```
sudo systemctl status auditd
```

Soll auch der frühe Systemstart bereits auditiert werden, kann zusätzlich der Kernel-Parameter `audit=1` gesetzt werden.

In `/etc/audit` befinden sich die Konfigurationsdateien des Audit-Daemons, mit denen sich das Audit feingranular einstellen lässt. Wichtig sind hier vor allem zwei Bereiche:

`/etc/audit/auditd.conf` welche zur allgemeinen, systemweiten Audit-Einstellung dient und `/etc/audit/rules.d/*.rules` wo die eigentlichen Audit-Regeln festgelegt werden.

Für ein Beckhoff RT Linux®-System empfiehlt sich zunächst ein konservativer Satz von Regeln, der Änderungen an sicherheitsrelevanten Konfigurationsdateien, Identitätsdaten, Mount-Vorgängen, Kernelmodulen und Berechtigungen protokolliert, ohne hochfrequente Laufzeitpfade unnötig stark zu belasten.

Eine naheliegende Beispielkonfiguration ist:

```
# /etc/audit/rules.d/30-rt-security.rules

-b 8192
-f 1

# Audit-Konfiguration selbst überwachen
-w /etc/audit/ -p wa -k audit-config

# Benutzer-, Gruppen- und Authentisierungskonfiguration
-w /etc/passwd -p wa -k identity
-w /etc/shadow -p wa -k identity
-w /etc/group -p wa -k identity
-w /etc/gshadow -p wa -k identity
-w /etc/sudoers -p wa -k privilege
-w /etc/sudoers.d/ -p wa -k privilege
-w /etc/pam.d/ -p wa -k pam-config

# Zeitänderungen
-a always,exit -F arch=b64 -S adjtimex,settimeofday,clock_settime -k time-change
-w /etc/localtime -p wa -k time-change

# Host- und Netzwerkkonfiguration
-w /etc/hostname -p wa -k network-config
-w /etc/hosts -p wa -k network-config
-w /etc/resolv.conf -p wa -k network-config
-w /etc/network/ -p wa -k network-config

# Persistenzmechanismen
-w /etc/crontab -p wa -k cron
```

Bei 64-Bit-Systemen, auf denen auch 32-Bit-Anwendungen zugelassen sind, sollten die entsprechenden `arch=b32`-Regeln zusätzlich ergänzt werden.

Führen Sie `sudo augenrules –load` aus, um die Regeln zu laden und `sudo auditctl -l`, um die geladenen Regeln anzuzeigen. Anschließend können die Audit-Protokolle über Befehle wie `sudo aureport -k -i` oder `sudo ausearch -k identity -i` eingesehen werden.

Es gilt, dass Regeln vermieden werden sollten, die hochfrequente Verzeichnisse oder stark genutzte Systemaufrufe umfassend überwachen, zum Beispiel globale Regeln auf `/tmp, /run, /var/tmp` oder eine vollständige Überwachung aller `execve-`, open- oder Lesezugriffe. Solche Regeln können schnell zu großen Protokollmengen führen und die Echtzeiteigenschaften beeinträchtigen. Empfehlenswert ist stattdessen eine Fokussierung auf:

- Änderungen an Benutzer-, Gruppen- und Authentisierungsdaten
- Änderungen an Netzwerk- und Host-Konfiguration

- Änderungen an Startmechanismen und Diensten
- Mount- und Kernelmodul-Aktivitäten
- Rechte-, Eigentümer- und Attributänderungen
- optionale, gezielte Überwachung kritischer Anwendungsverzeichnisse

5.4 Programme

5.4.1 Whitelisting für Programme

Ein Applikationen-Whitelisting, wie es bei Windows mit beispielsweise AppLocker oder sogenannten Richtlinien für Softwareeinschränkungen (SRP) verfügbar ist, gibt es für Linux®-Systeme nicht in identischer Form. Es gibt jedoch verschiedene Ansätze, die Ausführung von Programmen auf definierte Anwendungen, Dateien, Dienste oder Integritätszustände zu beschränken. Diese Ansätze sind jedoch weniger einheitlich und in der Regel komplexer in Konfiguration und Betrieb als unter Windows.

Grund hierfür ist eine erhöhte Komplexität durch Kommandozeile, Skripte, Interpreter und flexible Werkzeugketten bei Linux®-Systemen gegenüber der zumeist grafischen Eingabe unter Windows. Ein strikt durchgesetztes Applikationen-Whitelisting ist daher grundsätzlich möglich, in der Praxis jedoch häufig mit erhöhtem Pflege- und Testaufwand verbunden. Insbesondere bei Beckhoff RT Linux®-Systemen muss zusätzlich berücksichtigt werden, dass sicherheitsbezogene Zusatzmechanismen je nach Ausprägung Einfluss auf Laufzeitverhalten, Wartbarkeit und Echtzeiteigenschaften haben können.

Stattdessen sollte genau darauf geachtet werden, aus welcher Quelle Pakete bezogen werden und welche Pakete auf dem System installiert sind. Es ist empfehlenswert, ausschließlich vertrauenswürdige und kontrollierte Paketquellen zu verwenden und nur die Software zu installieren, die für den bestimmungsgemäßen Betrieb tatsächlich erforderlich ist. Nicht benötigte Programme, Dienste, Interpreter, Compiler und Administrationswerkzeuge sollten entfernt oder gar nicht erst installiert werden (siehe: Entfernen nicht mehr benötigter Komponenten [▶ 26]).

Zusätzlich kann die Ausführung unerwünschter Programme durch geeignete Systemhärtungsmaßnahmen erschwert werden. Hierzu zählen beispielsweise restriktive Dienstkonfigurationen, Integritätsprüfungen, die Einschränkung schreibbarer Bereiche sowie geeignete Dateisystemoptionen. In der Praxis ist für Beckhoff RT Linux®-Systeme jedoch häufig ein reduzierter, kontrollierter und regelmäßig überprüfter Softwarebestand der naheliegendste und wartungsärmste Ansatz.

5.4.2 Entfernen nicht mehr benötigter Komponenten

Um die Angriffsoberfläche zu verkleinern, sollten nicht benötigte Programme, Dienste und Komponenten des Betriebssystems entfernt werden.

Das Entfernen von Systemkomponenten sollte nur von versierten Personen durchgeführt werden. Es können negative Seiteneffekte auftreten und Programme oder Dienste nicht mehr korrekt ausgeführt werden.

Insbesondere bei Beckhoff RT Linux®-Systemen sollten Änderungen vorab geprüft und getestet werden, da auch indirekte Abhängigkeiten Auswirkungen auf den bestimmungsgemäßen Betrieb haben können.

Mit `apt list –installed` lassen sich alle auf dem System installierten Pakete anzeigen. Bei Auslieferung sind alle hier gelisteten Pakete relevant für das Basissystem oder für Beckhoff Software. Alternativ kann auch die Paketdatenbank direkt mit `dpkg -l` abgefragt werden. Neben Paketen für die eigentliche Anwendung, Diagnose- oder Verwaltungsfunktionen werden dort auch Pakete aufgeführt, die von anderen Programmen benötigt werden.

Wird ein Paket entfernt, das von einem anderen installierten Paket benötigt wird, zeigt die Paketverwaltung an, welche weiteren Pakete davon betroffen sind oder zusätzlich entfernt werden müssten. So lässt sich feststellen, ob ein Paket noch eine Abhängigkeit anderer installierter Komponenten ist. Pakete, von denen bekannt ist, dass sie nicht mehr benötigt werden, können mit `sudo apt remove <Paketname>` entfernt werden.

Sollen zusätzlich die zugehörigen Konfigurationsdateien entfernt werden, kann stattdessen *sudo apt purge <Paketname>* verwendet werden. Danach können mit `sudo apt autoremove` automatisch installierte und nicht mehr benötigte Abhängigkeiten gelöscht werden. So wird sichergestellt, dass keine nicht mehr benötigten Pakete auf dem System verbleiben. Nicht benötigte Dienste sollten darüber hinaus deaktiviert werden, sofern sie nicht bereits durch das Entfernen der zugehörigen Pakete entfallen.

5.4.3 Package-Audit

Unter Beckhoff RT Linux® steht mit dem Werkzeug `debsecan` eine Möglichkeit zur Verfügung, installierte Software auf bekannte Schwachstellen zu prüfen. Mit dem Kommando `debsecan --suite trixie` werden die Informationen zu bekannten Schwachstellen mit den lokal installierten Paketen verglichen. Sie erhalten die CVE-Nummer (*Common Vulnerabilities and Exposures*) sowie Informationen zu den betroffenen Paketen.

5.4.4 Antiviren Programme

Für Beckhoff RT Linux® und Linux®-Systeme im Allgemeinen erscheinen Antivirus-Programme als nicht notwendig, weil Schadsoftware für Linux®-Systeme eher selten ist. Viren für Linux®-Systeme kommen noch immer sehr selten vor. Gründe hierfür sind vor allem die geringere Verbreitung der Systeme gegenüber Windows und Mac OS.

Hinzu kommt die klare Trennung der Benutzer Accounts und ihrer Rechte. Unter Beckhoff RT Linux® muss selbst der Benutzer Administrator durch eine Passworteingabe Root-Rechte zum Ändern von systemrelevanten Dateien und zum Ausführen von Programmen holen. Skripte müssen erst ausführbar gemacht werden, bevor Sie überhaupt ausgeführt werden können. Ein versehentlich heruntergeladener Virus kann zunächst nur die Dateien des eingeloggten Nutzers befallen. Eine Ausbreitung über das System ist durch die strikte Rechteverwaltung nicht einfach möglich.

Jedoch müssen Sicherheitslücken durch regelmäßige Updates geschlossen werden. Durch die große Open-Source-Community werden Sicherheitslücken für gewöhnlich schnell erkannt und behoben. Die Updates stehen dann über den in jedem System voreingestellten Beckhoff Package Server zur Verfügung.

Es gibt Antivirus-Programme für Linux®-Systeme, aber sind diese vor allem für Mail- oder Dateiserver sinnvoll, die auch von Windows-Clients genutzt werden können. Natürlich kann ein Antivirus-Programm auch genutzt werden, um dem System eine weitere Sicherheitsschicht hinzuzufügen. Für Beckhoff RT Linux® steht neben einigen proprietären Anwendungen das kostenlose Linux® Antivirus Programm Clam Antivirus zur Verfügung. Beachten Sie, dass dieses Programm unter die GPL-Lizenz fällt und an dessen Bedingungen geknüpft ist.

5.5 USB-Filter

Aus Sicherheitsgründen werden USB-Speichergeräte nicht automatisch gemountet. Sie müssen sie für jede Sitzung manuell einbinden oder ein automatisches Einbinden konfigurieren.

6 Netzwerkkommunikation

An dieser Stelle wird eine Übersicht über einige relevante Maßnahmen in Bezug auf die Kommunikation gegeben. Auf Themen, die außerhalb des eigentlichen IPCs liegen – wie beispielsweise Netzwerksegmentierung – wird nicht eingegangen.

Eine Liste der verwendeten Ports für TwinCAT-Produkte befindet sich hier: Wichtige TCP/UDP-Ports [▶ 30].

6.1 Fernwartung

Die Fernwartung spielt bei Industrieanlagen eine wichtige Rolle. Sie ermöglicht es Servicetechnikern und Programmierern im Falle einer Störung aus der Ferne Wartungsarbeiten durchzuführen.

Da Fernwartungszugänge für Wartungszwecke in der Regel immer verfügbar sind und Security-Maßnahmen oft vernachlässigt werden, um im Störungsfall schnell reagieren zu können, werden die Zugänge häufig für Angriffe genutzt.

Maßnahmen an dieser Stelle sind unbedingt notwendig, um Angriffe, durch die der Anlagenbetrieb gestört werden kann, zu verhindern.

Siehe auch:

- VPN [▶ 29]

6.2 Firewall

Firewall Einstellungen sind ein Mittel, um das System vor Netzwerkangriffen zu schützen. Eingehende Ports, die Sie nicht benötigen, sollten blockiert werden. Besser ist es jedoch, Dienste, die diese Ports öffnen, nicht zu starten. Die nötigen Einstellungen bedingen eine mit allen Beteiligten abgestimmte Übersicht der genutzten Ports.

Mit einer Firewall können die sie durchlaufenden Netzwerkpakete gefiltert werden. Je nach Firewall-Technologie lassen sich Filterregeln auf Basis von Adresse, Port, Zustand der Kommunikationsbeziehung, Inhalt des Pakets und vielem mehr formulieren. Firewalls sind damit ein Werkzeug, um die Angriffsoberfläche zu verkleinern.

Eine Firewall kann als zusätzlich installierte Software, als Teil des Betriebssystems oder als eigenständiges Gerät eingesetzt werden. Jede dieser Formen hat Vor- und Nachteile. Eine hostbasierte Firewall ermöglicht die Absicherung direkt auf dem System, während eine externe Firewall den Netzwerkverkehr zentral filtern kann.

Firewalls mit Deep-Packet-Inspection, die auch die Nutzdaten der Datenpakete auswerten, können den Inhalt von verschlüsselten Verbindungen prinzipiell nicht einsehen. Um dennoch den Inhalt verarbeiten zu können, wird beispielsweise häufig die Verschlüsselung für Webanwendungen an der Firewall terminiert und die Daten für den Client neu verschlüsselt. Hierdurch sind der Firewall die Inhalte sichtbar, aber die Ende-zu-Ende-Verschlüsselung ist unterbrochen.

Restriktive, explizite Einstellungen für die Kommunikation über eine Firewall sind eine wichtige Maßnahme, um Netzwerkzugriffe nur im notwendigen Umfang zuzulassen.

Unter Wichtige TCP/UDP-Ports [▶ 30] befindet sich eine Liste von TCP/UDP-Ports, die typischerweise berücksichtigt werden müssen, um eine Firewall zu konfigurieren.

Unter Beckhoff RT Linux® erfolgt die Paketfilterung über `netfilter` mit `nftables`. Damit lassen sich Regeln für eingehende, ausgehende und weitergeleitete Netzwerkverbindungen definieren.

Die aktuell aktive Firewall-Konfiguration kann mit `sudo nft list ruleset` angezeigt werden. Auch wenn die Standarddatei `/etc/nftables.conf` auf dem System vorhanden ist, wird sie auf diesem nicht als primäre Konfigurationsdatei verwendet. Maßgeblich ist die durch den `nftables`-Dienst geladene Datei `/etc/nftables-bhf.conf`, welche weitere Regeldateien aus `/etc/nftables.conf.d/` einbindet. Dadurch ist eine modulare und besser wartbare Struktur der Firewall-Regeln möglich.

Für die Konfiguration müssen Sie sicherstellen, dass nur die für den Betrieb tatsächlich benötigten Verbindungen freigegeben werden. Nicht benötigte Ports und Dienste sollten Sie deaktivieren oder durch entsprechende Filterregeln sperren. Falls sichere und unsichere Kommunikationsvarianten zur Verfügung stehen, sollten Sie nach Möglichkeit nur die sicheren Varianten freigeben.

Änderungen an der Firewall-Konfiguration sollten Sie nach der Inbetriebnahme und nach Software-Updates erneut prüfen, um unbeabsichtigte Freigaben oder blockierte Kommunikationsbeziehungen zu vermeiden.

6.3 Netzwerktechnologien

In diesem Abschnitt werden die Security-relevanten Besonderheiten einiger Protokolle beschrieben.

6.3.1 Modbus

Das Modbus-Protokoll wurde ursprünglich in den späten 1970ern als serielles Kommunikationsprotokoll entwickelt. Die Hauptziele waren, ein Kommunikationsprotokoll für industrielle Anwendungen bereitzustellen, das einfach einzurichten und zu warten ist und Daten überträgt, ohne dass ein Informationsmodell entwickelt werden muss. Aufgrund dieser Einfachheit war es 30 Jahre sehr beliebt. Aber diese Einfachheit macht es schwierig, Modbus in modernen Industrieanlagen einzusetzen, die komplexere Anforderungen wie beispielsweise Security und Informationsmodelle an ein Kommunikationsprotokoll stellen. Das ursprüngliche Modbus-Protokoll beinhaltet keine Security-Maßnahmen wie Verschlüsselung oder Authentifizierung.

Auch wenn Beckhoff zwei TwinCAT Functions für Modbus RTU und Modbus TCP bereitstellt, wird empfohlen, modernere Protokolle wie beispielsweise OPC UA einzusetzen, die bereits Security-Mechanismen implementieren.

6.3.2 ADS

Die Automation Device Specification (ADS) ist ein von Beckhoff entwickeltes, proprietäres Kommunikationsprotokoll. Es wurde für einen hohen Durchsatz und die Übertragbarkeit über verschiedene Transportprotokolle (z. B. TCP oder Seriell) entwickelt. ADS wurde nicht mit Security entworfen und enthält keine kryptographischen Operationen wegen ihres negativen Effekts auf Performance und Durchsatz.

Es wird empfohlen, ADS nur in gesicherten Umgebungen einzusetzen oder entsprechende gesicherte Transportkanäle zu verwenden.

Für ADS existieren aktuell zwei TCP-Transportkanäle, die eine Verschlüsselung unterstützen:

- ADS-over-MQTT
- Secure ADS

6.3.3 OPC UA

OPC Unified Architecture (IEC 62541) ist die Technologiegeneration der OPC Foundation für einen sicheren, zuverlässigen und herstellerneutralen Transport von Rohdaten und vorverarbeiteten Informationen von der Fertigungsebene bis in das Produktionsplanungs- oder ERP-System. Auf einheitliche, sichere und zuverlässige Weise steht mit OPC UA jeder berechtigten Anwendung und jeder autorisierten Person jede gewünschte Information zu jeder Zeit und an jedem Ort zur Verfügung.

Weitere Informationen finden Sie in der Dokumentation:TF6100 TC3 OPC UA

6.3.4 VPN

Virtual Private Network (VPN) ermöglicht es, ein virtuelles LAN zwischen verschiedenen Teilnehmern über öffentliche Netze zu spannen. In den meisten Fällen ist der über das öffentliche Netz geleitete Datenverkehr verschlüsselt. VPN-Lösungen können beispielsweise eingesetzt werden, um übergangsweise unsichere Protokolle zu tunneln, bis sichere Alternativen einsatzbereit sind.

6.4 Security Gateway

Eine weitere Option, um ein System vor Einflüssen aus dem Netzwerk zu schützen, ist der Einsatz eines Security-Gateways. Diese Hardwarelösung kann in einem Netzwerk vor einem IPC installiert werden. So können bestimmte Netzwerk-Segmente oder jeder einzelne PC geschützt werden.

Die Geräte bieten neben den Netzwerk-Schutzfunktionen auch die Möglichkeit, beispielsweise Antiviren-Software auszuführen und somit einen Dateitransfer, der über eine lokale Zwischenablage realisiert ist, zu überwachen – und zwar ohne dass die Echtzeitfähigkeit des eigentlichen Steuerungsrechners einzuschränken.

6.5 Wichtige TCP/UDP-Ports

Ungesicherte Protokolle müssen -je nach Anwendungsfall- abgeschaltet oder durch eine unterlagerte Schicht abgesichert werden, beispielsweise durch ein physikalisch gesichertes Netzwerk oder VPN.

Bei gesicherten Protokollen müssen entsprechend der Produkt-Dokumentation eine Inbetriebnahme der Security vorgenommen werden.

Standarddienste

Die folgende Tabelle gibt einen Überblick der im Normalfall in den ausgelieferten Images geöffneten, eingehende Ports

Dienst	Ports (eingehend)
SSH	22 / tcp
HTTPS/Device Manager	443 / tcp
ADS Secure	8016 / tcp
ADS Broadcast	48899 / udp
mDNS/lokale Namensauflösung über Ipv4 und Ipv6	5353 / udp

TwinCAT Dienste

Die Folgende Tabelle gibt eine Übersicht der typischerweise verwendeten Ports bei TwinCAT Produkten:

Dienst	Port (Standardeinstellung)
TF1810 TwinCAT PLC HMI Web	80 / tcp (eingehend) Siehe auch: Dokumentation zu TF1810
TF2000 TwinCAT HMI	1010 (Versionen ≤ 1.12), 2010 (Versionen ≥ 1.14) / tcp (lokal) 1020 (Versionen ≤ 1.12), 2020 (Versionen ≥ 1.14) / tcp (eingehend) Siehe auch: Dokumentation zu TF2000
TF6100 OPC UA	4840 / tcp (UA Server, eingehend), änderbar 48050/tcp (UA Gateway, eingehend), änderbar Siehe auch: Dokumentation zu TF6100
TF6100 OPC DA	Dynamisch (abhängig von DCOM) zwischen 1024 und 65535 (eingehend) Siehe auch: Dokumentation zu TF6120
TF6250 Modbus TCP	502 / tcp (eingehend), änderbar Siehe auch: Dokumentation zu TF6250
TF6310 TCP-IP	änderbar / tcp (eingehend, ausgehend) Siehe auch: Dokumentation zu TF6310
TF6311 TCP/UDP Realtime	änderbar / tcp (eingehend, ausgehend) Die Kommunikation ist nicht durch eine Betriebssystem-Firewall beeinflussbar. Siehe auch: Dokumentation zu TF6311
TF6300 FTP	20 / tcp (ausgehend) 21 / tcp (ausgehend) Siehe auch: Dokumentation zu TF6300
TF6420 Database Server	änderbar je nach Datenbank / tcp (ausgehend) Siehe auch: Dokumentation von TF6420
TF67xx IoT TF35xx Analytics	änderbar je nach Broker / tcp (ausgehend) Siehe auch: Dokumentationen der TF670x sowie TF35xx
TwinCAT EAP	34980 / udp (eingehend), falls EAP über UDP verwendet wird. Die Kommunikation ist nicht durch eine Betriebssystem-Firewall beeinflussbar. Siehe auch: Dokumentation von EAP
TwinCAT ADS-over-MQTT	änderbar je nach Broker / tcp (ausgehend) Siehe auch: Dokumentation zu ADS-over-MQTT

6.6 Nginx-Webserver

Der Nginx-Webserver ist unter Beckhoff RT Linux® standardmäßig aktiv und unter anderem für den Beckhoff Device Manager und verwendet.

Um das System weiter abzuriegeln und Zugriffe über den Webserver einzuschränken, können die Weiterleitungen in der Nginx-Konfiguration deaktiviert werden. Unter Beckhoff RT Linux® werden die relevanten Einträge über die Datei `mdpwebservice-bhf.conf` und die eingebundenen `location`-Dateien konfiguriert.

1. Öffnen Sie die Datei `mdpwebservice-bhf.conf` unter `/etc/nginx/sites-enabled/` und prüfen Sie die eingebundenen `location`-Dateien unter `/usr/share/mdpwebservice-bhf/locations/`. Die Dateien sollten `00-root.conf`, `10-config.conf` und `20-console.conf` heißen.
2. Kommentieren Sie die Einträge unter `location /`,`location /config/` und `location /console/` vollständig aus.

```
# location / {
# add_header ServerHostname $hostname;
# root /usr/local/www/default;
```

```
# index index.html index.htm;
# }

# location /config/ {
# include /usr/share/mdpwebservice-bhf/errorpages.conf;
# include /usr/share/mdpwebservice-bhf/auth.conf;
# include /usr/share/mdpwebservice-bhf/proxy.conf;
# proxy_pass http://unix:/var/run/mdpwebservice-bhf/web0;
# }

# location /console/ {
# include /usr/share/mdpwebservice-bhf/errorpages.conf;
# include /usr/share/mdpwebservice-bhf/auth.conf;
# include /usr/share/mdpwebservice-bhf/proxy.conf;
# proxy_set_header Upgrade $http_upgrade;
# proxy_set_header Connection "upgrade";
# proxy_pass "http://127.0.0.1:7681/";
# }
```

3. Speichern Sie die Änderungen.
4. Prüfen Sie die Konfiguration mit `sudo /usr/sbin/nginx -t`.
5. Starten Sie den Nginx-Service anschließend mit `sudo systemctl restart nginx` neu.

⇨ Sämtliche Anfragen an den Beckhoff Device Manager werden ab jetzt nicht mehr weitergeleitet.

6.7 HTTPS-Zertifikate

Dieses Kapitel beschreibt, wie Sie eigene HTTPS-Zertifikate erstellen und importieren können, falls die von Beckhoff standardmäßig für das Webinterface (Device Manager) bereitgestellten Zertifikate für Ihre Anwendung nicht geeignet sind.

In der Informationstechnologie sind Zertifikate ein Mittel, um Identitäten sicher nachzuweisen. Dadurch können Nachrichten oder Dokumente verschlüsselt werden, sodass nur der gewünschte Empfänger den Inhalt wieder entschlüsseln kann. Diese Technik wird unter anderem von jedem Webbrowser beim Abrufen einer Seite über das HTTPS-Protokoll genutzt.

Dabei erfragt ein Netzwerkteilnehmer beim Aufbau einer Kommunikationsverbindung zu einem anderen Teilnehmer dessen Zertifikat. Das Zertifikat wird geprüft und ob der andere Teilnehmer sich mit Hilfe des dazugehörigen Schlüssels authentisiert. Sobald die Identität nachgewiesen wurde, lässt sich der nachfolgende Nachrichtenaustausch über die Verbindung gegen unbefugte Manipulation und wahlweise auch gegen unbefugte Einsichtnahme schützen.

Um eigens generierte HTTPS-Zertifikate zu nutzen, muss:

- die automatische Generierung eines Zertifikats für Industrie-PCs deaktiviert,
- ein Zertifikat bei einer Zertifizierungsstelle (Certificate Authority, CA) angefordert
- und anschließend das HTTPS-Zertifikat importiert werden.

Der genaue Ablauf und die notwendigen Schritte werden in diesem Kapitel beschrieben.

6.7.1 Automatische Zertifikatserstellung deaktivieren

In manchen Anwendungsfällen ist es für den Anwender nicht sinnvoll, die automatisch generierten Zertifikate für den Webserver wiederzuverwenden. In diesem Fall können Sie die automatische Synchronisation deaktivieren und ein eigenes Zertifikat für den Webserver (nginx) verwenden.

Dafür müssen Sie zunächst die automatische Zertifikatserstellung deaktivieren, damit eigene Zertifikate installiert und nicht durch ein Standard-Beckhoff-Zertifikat überschrieben werden.

Gehen Sie wie folgt vor:

1. Deaktivieren Sie den Dienst `TcSeldSigned`, damit das Zertifikat nicht durch das Standard-Beckhoff Zertifikat überschrieben wird.
2. Geben Sie dazu den Befehl `sudo systemctl disable –now TcSelfSigned.service` in der Konsole ein.

⇨ Sie haben die automatische Generierung von Zertifikaten deaktiviert.

Sehen Sie dazu auch

- HTTPS-Zertifikat anfordern oder erstellen [▶ 33]

6.7.2 HTTPS-Zertifikat anfordern oder erstellen

Üblicherweise stellt eine Zertifizierungsstelle (Certificate Authority, CA) Installationsanweisungen zur Verfügung, wie ein von ihr ausgestelltes Zertifikat zu installieren ist. Die Zertifizierungsstelle stellt sogar Anweisungen zur Verfügung, wie das Zertifikat zu beantragen ist. Bitte befolgen Sie in erster Linie die Anweisungen der Zertifizierungsstelle.

Zunächst müssen Sie eine Zertifikatsanforderung (Certificate Signing Request, CSR) erstellen und die Zertifikatsanforderung gemäß den Anweisungen der Zertifizierungsstelle an diese weiterleiten. Die Zertifizierungsstelle wird Ihnen dann das Serverzertifikat und die Zwischenzertifikate zur Verfügung stellen, um eine Zertifikatsanforderung zu erstellen

Wenn Sie kein Zertifikat von einer offiziellen Zertifizierungsstelle (CA) haben, können Sie zu Testzwecken ein selbstsigniertes Zertifikat erstellen.

Gehen Sie wie folgt vor:

1. Generieren Sie zu Testzwecken ein selbstsigniertes Zertifikat mit dem folgenden Befehl:

```
Openssl req -new -newkey rsa:4096 -nodes -sha256 \
                -keyout IPCDiagnostics.key \
                -out IPCDiagnostics.csr \
                -subj '/CN=<hostname>' \
                -addext 'subjectAltName=DNS:<hostname>,IP:<ipaddress>'
```

2. Der Befehl erstellt einen privaten Schlüssel `IPCDiagnostics.key` und ein selbstsigniertes Zertifikat `IPCDiagnostics.crt`.

   `openssl req`: Der Befehlsteil `req` erstellt und bearbeitet Zertifikatsanfragen (CSR – Certificate Signing Request). Mit `-x509` wird stattdessen direkt ein selbstsigniertes Zertifikat erstellt.

   `-newkey rsa:4096`: Erstellt ein neues Schlüsselpaar mit dem RSA-Algorithmus und einer Schlüssellänge von 4096 Bit.

   `-nodes`: Bedeutet "no DES". Der private Schlüssel wird nicht verschlüsselt gespeichert, d. h., es wird kein Passwort benötigt, um den Schlüssel zu verwenden.

   `-sha256`: Verwendet den sicheren Hash-Algorithmus SHA-256, um die Zertifikatsignatur zu erstellen.

   `-keyout IPCDiagnostics.key`: Speichert den privaten Schlüssel in der Datei IPCDiagnostics.key.

   `-out IPCDiagnostics.crt`: Speichert das erstellte Zertifikat in der Datei IPCDiagnostics.crt.

   `-subj '/CN=<hostname>':` Gibt die Daten für das Zertifikat an, ohne eine interaktive Abfrage. `/CN=<hostname>` legt den Common-Name (CN) fest, der normalerweise der Hostname oder die Domain ist, die durch das Zertifikat geschützt wird.

   `-addext 'subjectAltName=DNS:<hostname>,IP:<ipaddress>':` Fügt eine Erweiterung (Extension) zum Zertifikat hinzu. `subjectAltName` (SAN) erlaubt zusätzliche Namen und IP-Adressen, die das Zertifikat abdecken soll.
3. Ersetzen Sie `<hostname>` durch den Hostnamen und durch die IP-Adresse Ihres Linux®-Geräts.

⇨ Im nächsten Schritt kann das Zertifikat importiert werden (siehe: Zertifikat importieren [▶ 34]).

Sehen Sie dazu auch

- Zertifikat importieren [▶ 34]

6.7.3 Zertifikat importieren

Sobald Sie ein Zertifikat von einer offiziellen Zertifizierungsstelle (CA) erhalten haben, können Sie dieses in Ihr Beckhoff RT Linux®-System importieren. Alternativ können Sie auch das selbstsignierte Zertifikat verwenden, das Sie zu Testzwecken erstellt haben.

Gehen Sie wie folgt vor:

1. Ersetzen Sie den vorhandenen privaten Schlüssel für nginx durch Ihren privaten Schlüssel:
   ```
   sudo cp IPCDiagnostics.key /etc/TwinCAT/3.1/Target/PrivateKeys/IPCDiagnostics.key
   ```
2. Ersetzen Sie das vorhandene Zertifikat für nginx durch Ihr Zertifikat:
   ```
   sudo cp IPCDiagnostics.csr /etc/TwinCAT/3.1/Target/Certificates/IPCDiagnostics.csr
   ```
3. Starten Sie den nginx-Webserver neu:
   ```
   sudo systemctl restrt nginx
   ```
4. Das Zertifikat ist nach dem Neustart des Dienstes einsatzbereit.

⇨ Wenn Sie kein Zertifikat einer offiziellen Zertifizierungsstelle (CA) verwenden, zeigt Ihr Browser eine Sicherheitswarnung an. Sie können Ihren Browser so konfigurieren, dass er das Zertifikat automatisch akzeptiert, indem Sie das Server-Zertifikat in den Zertifikatsspeicher Ihres Browsers importieren. Weitere Informationen hierzu finden Sie unter: Selbstsignierte Zertifikate für https-Verbindung

Da einige Browser (z.B. Mozilla Firefox) eigene Zertifikatsspeicher verwenden, kann es erforderlich sein, das Zertifikat direkt im Browser zu importieren.

7 TwinCAT

Was für eXtended Automation Engineering (XAE) und eXtended Automation Runtime (XAR) als Bedrohung gilt, muss aus einem Security-Konzept für die Anlage hervorgehen. Hilfestellung bei der Erstellung eines Security-Konzepts bietet die Norm IEC 62433, welche unter anderem die notwendige Bedrohungsanalyse erklärt. Zusätzlich kann der VDMA-Leitfaden herangezogen werden, der bei der Security in Betriebsprozessen und der Resilienz der Produkte gegen Cyber-Angriffe unterstützt: https://www.vdma.org/viewer/-/v2article/render/16110956

In diesem Kapitel werden einige Beispielbedrohungen bezogen auf XAE und XAR ohne Anspruch auf Vollständigkeit aufgelistet.

7.1 eXtended Automation Engineering (XAE)

Tab. 1: Unberechtigte Manipulation am Quelltext.

Gegenmaßnahmen	Beschreibung
Technisch	• Berechtigungen definieren und mit Software-Protection umsetzen • Versionskontrollsystem nutzen, um Änderungen nachvollziehbar zu machen • Individuelle Zugriffskontrolle für Versionskontrollsystem nutzen
Organisatorisch	• IT-Sicherheitsmanagementsystem nutzen (z.B. nach ISO 27001) • Versionskontrollsystem nutzen (siehe: Source-Control): • „Staging“ nutzen: ◦ Check-in zuerst in Entwicklungs-Source-Control-Repository ◦ Separates (Pre-)Release-Build-Repository nutzen, um von dort Alpha-, Beta-, RC- und Release-Versionen zu bauen ◦ Übertragung Entwicklungs-Repository -> (Pre-)Release-Build-Repository nur nach Review zum Beispiel per Project Compare Tool (siehe: Project Compare Tool)

Tab. 2: Unberechtigte Einsicht in den Quelltext.

Gegenmaßnahmen	Beschreibung
Technisch	• Quelltext mittels Software-Protection verschlüsselt ablegen (siehe: Software-Protection)
Organisatorisch	• IT-Sicherheitsmanagementsystem nutzen (z.B. Nach ISO 27001). • Zugriff auf die Speicherstellen absichern. • Verschlüsselte Ablage verwenden.

7.2 eXtended Automation Runtime (XAR)

Tab. 3: Unautorisierter Zugriff über ADS oder Secure ADS.

Gegenmaßnahmen	Beschreibung
Technisch	Secure ADS nutzen (siehe: Secure ADS): • Nur für definierte Gegenstellen öffnen • Firewall-Einschränkung • Statische Routen • Gegenstellen gegen Manipulation absichern
Organisatorisch	• Zugriffe über Secure ADS durch Zugriffe über OPC UA ersetzen.

Tab. 4: Beeinflussung der Echtzeit über ADS / Secure ADS.

Gegenmaßnahmen	Beschreibung
Technisch	Secure ADS nutzen (siehe: Secure ADS): • Nur für definierte Gegenstellen öffnen • Firewall-Einschränkung • Statische Routen • Gegenstellen gegen Manipulation absichern
Organisatorisch	• Zugriffe über Secure ADS durch Zugriffe über OPC UA ersetzen.

7.3 Weitere technische Informationen

Dieses Kapitel fasst weitere Themen in einer Linksammlung zusammen, die die Security von TwinCAT betreffen. Es wird auf weiterführende Beckhoff-Dokumentationen verlinkt, die die jeweiligen Themen ausführlich beschreiben. Die Auswahl ist eine Hilfestellung, ist als erste Anlaufstelle gedacht und erhebt keinen Anspruch auf Vollständigkeit.

TwinCAT Allgemein	Weiterführende Informationen
TwinCAT 3 Software Protection	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_security_management/index.html&id=355557539833111233
ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_intro/index.html&id=7262890787652929099
ADS deaktivieren	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/6917981195.html&id=5745105416081707706
Secure ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/index.html&id=2501949194726739202
ADS over MQTT	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_over_mqtt/index.html&id=120186874503837909

OPC UA	Weiterführende Informationen
Server-Security	https://infosys.beckhoff.com/content/1033/tf6100_tc3_opcua_server/15563113227.html?id=1035811638453978802
IO Client-Security	https://infosys.beckhoff.com/content/1033/tf6100_tc3_opcua_client/16622176779.html?id=5022570264195624057
Gateway Security	https://infosys.beckhoff.com/content/1033/tf6100_tc3_opcua_gateway/15626711307.html?id=1826922088201458894

8 Anhang

8.1 Weiterführende Literatur

IEC 62443 ist eine Reihe internationaler Standards für die Security in Automatisierungssystemen. Die Einzelteile sind teilweise noch in der Entwicklung, aber veröffentlichte gut nutzbare Teile beschreiben sowohl die organisatorischen als auch die technischen Konzepte und Maßnahmen für Anlagen und Komponenten. URL: https://webstore.iec.ch/publication/7029

NIST SP800-82 Guide to Industrial Control Systems Security beschreibt gezielt die Analyse von und Maßnahmen gegen Security-Bedrohungen für industrielle Anlagen. URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

BSI IT-Grundschutz-Kompendium bietet strukturiert Bausteine zur Analyse von Gefährdungen als auch zur Anwendung von Maßnahmen. Das Kompendium beinhaltet auch Bausteine zur industriellen IT https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html

8.2 Advisories

Unsere Securitiy Advisories sollen unseren Kunden dabei helfen, ihre Beckhoff Industrie-PCs und Embedded-PCs gegen bestimmte Effekte zu schützen. Die nachfolgende Tabelle gibt einen Überblick über alle verfügbaren Advisories zu Schwachstellen im Bereich der Security und beinhaltet eine Verknüpfung zum Download des Dokuments.

Diese Security Advisories werden auch als RSS Feed bereitgestellt. Zusätzlich veröffentlicht Beckhoff diese Advisories im Rahmen vom CERT@VDE zusammen mit anderen Herstellern: https://cert.vde.com/de/advisories/vendor/beckhoff/.

Bei vermuteten Schwachstellen bezogen auf Security in einem unserer Produkte bitten wir um Nachricht auf dem Weg, der unter Coordinated Disclosure beschrieben ist.

Nummer	Titel	Version	Sprache	Download	Externe CNA
2025-003	Vulnerabilities in Beckhoff Device Manager	1.0	EN	PDF	HTML, CSAF
2025-002	XSS Vulnerability in TwinCAT 3 HMI Server	1.0	EN	PDF	HTML, CSAF
2025-001	Deserialization of untrusted data by TwinCAT 3 Engineering	1.0	EN	PDF	HTML, CSAF
2024-005	Local command injection via TwinCAT Package Manager	1.0	EN	PDF	HTML, CSAF
2024-004	Local Denial of Service issue in TwinCAT/ BSD package “MDP”	1.0	EN	PDF	HTML, CSAF
2024-003	Local Denial of Service issue in TwinCAT/ BSD package “IPC-Diagnostics”	1.0	EN	PDF	HTML, CSAF
2024-002	Improper neutralization of input in TwinCAT/BSD package “IPC-Diagnostics-www”	1.0	EN	PDF	HTML, CSAF
2024-001	Local authentication bypass in TwinCAT/ BSD package “IPC-Diagnostics”	1.0	EN	PDF	HTML, CSAF
2023-001	Open redirect in TwinCAT/BSD package “authelia-bhf”	1.0	EN	PDF	HTML
2022-001	Null Pointer Dereference vulnerability in products with OPC UA technology	1.0	EN	PDF	HTML
2021-003	Relative path traversal vulnerability through TwinCAT OPC UA Server	1.0	EN	PDF	HTML
2021-002	Stack Overflow and XXE vulnerability in various OPC UA products	1.0	EN	PDF	HTML
2021-001	DoS-Vulnerability for TwinCAT OPC UA Server and IPC Diagnostics UA Server	1.2	EN	PDF	HTML
2020-003	Privilege Escalation through TwinCAT System Tray (TcSysUI.exe)	1.1	EN	PDF	HTML
2020-002	EtherLeak in TwinCAT RT network driver	1.1	EN	PDF	HTML
2020-01	BK9000 couplers - Denial of service inhibits function	1.0	EN	PDF	HTML
2019-07	Denial-of-Service on TwinCAT using Profinet protocol	1.1	EN	PDF	HTML
2019-06	CE Remote Display behaves incorrectly with wrong credentials	1.2	EN	PDF	
2019-05	Remote Code Execution in Remote Desktop Service ("Dejablue")	1.0	EN	PDF	
2019-04	ADS Discovery	1.1	EN	PDF	
2019-03	Remote Code Execution in Remote Desktop Service	1.4	EN	PDF	
2019-02	Microarchitectural Data Sampling (MDS) vulnerabilities	1.2	EN	PDF	
2019-01	Spectre-V2 and impact on application performance as well as TwinCAT compatibility	1.4	EN	PDF	
2018-02	Updates for OPC-UA components (Several Vulnerabilities)	1.0	EN	PDF	
2018-01	TwinCAT 2 and 3.1 Kernel Driver Privilege Escalation	1.1	EN	PDF	
2017-02	Add Route using "Encrypted Password" bases on fixed key	1.3	EN	PDF	
2017-01	ADS is only designed for use in protected environments	1.4	EN	PDF	

Nummer	Titel	Version	Sprache	Download	Externe CNA
2015-001	Potential misuse of IPC Diagnostics version < 1.8 backend	1.1	EN	PDF	
2014-003	Recommendation to change default passwords	1.1	EN	PDF	
2014-002	ADS communication port allows password bruteforce	1.1	EN	PDF	
2014-001	Potential misuse of several administrative services	1.1	EN	PDF	

8.3 Support und Service

Der Beckhoff Support und Service unterstützt bei Fragen zu Beckhoff Produkten und Systemlösungen sowie bei deren Planung, Inbetriebnahme und Betrieb.

Beckhoff Niederlassungen und Vertretungen

Wenden Sie sich bitte an Ihre Beckhoff Niederlassung oder Ihre Vertretung für den lokalen Support und Service zu Beckhoff Produkten. Die Adressen der Beckhoff Niederlassungen und Vertretungen finden Sie unter: www.beckhoff.com/worldwide.

Für Beckhoff Produkte und Technologien stehen Trainingsprogramme, Tutorials und Webinare zur Verfügung.

Beckhoff Support

Der Beckhoff Support unterstützt bei technischen Fragestellungen zur Anwendung, Planung, Programmierung und Inbetriebnahme von Beckhoff Produkten.

☎ Hotline: +49 5246 963 157
✉ E-Mail: support@beckhoff.com, Support-Formular
Webseite: www.beckhoff.com/support

Beckhoff Service

Unsere Service-Spezialisten unterstützen Sie bei allen Fragestellungen rund um die After-Sales-Service-Prozesse wie Ersatzteile, Reparaturen usw.

☎ Hotline: +49 5246 963 460
✉ E-Mail: service@beckhoff.com, Service-Formular
Webseite: www.beckhoff.com/service

Downloadfinder

Der Downloadfinder dient als zentrale Quelle für herunterladbare Dokumente und Dateien zu Beckhoff Produkten, beispielsweise Applikationsberichte, technische Dokumentationen, Zeichnungen und Konfigurationsdateien.

Beckhoff Information System

Das Beckhoff Information System ist die zentrale Online-Dokumentation für Beckhoff Produkte und enthält Dokumentationen zu Produkten und Automatisierungsthemen sowie Beispiel-Code.

Beckhoff Unternehmenszentrale

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl, Deutschland

☎ Telefon: +49 5246 963 0
✉ E-Mail: info@beckhoff.com
Webseite: www.beckhoff.com

Tabellenverzeichnis

Abbildungsverzeichnis

Trademark statements

Beckhoff®, ATRO®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, MX-System®, Safety over EtherCAT®, TC/BSD®, TwinCAT®, TwinCAT/BSD®, TwinSAFE®, XFC®, XPlanar® and XTS® are registered and licensed trademarks of Beckhoff Automation GmbH.

Third-party trademark statements

CFast is a registered trademark of CompactFlash Association.

Excel, IntelliSense, Microsoft, Microsoft Azure, Microsoft Edge, PowerShell, Visual Studio, Windows and Xbox are trademarks of the Microsoft group of companies.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Modbus is a registered trademark of Schneider Electric USA, Inc.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

OPC UA is a registered trademark of the OPC Foundation.

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Deutschland
Telefon: +49 5246 9630
info@beckhoff.com
www.beckhoff.com