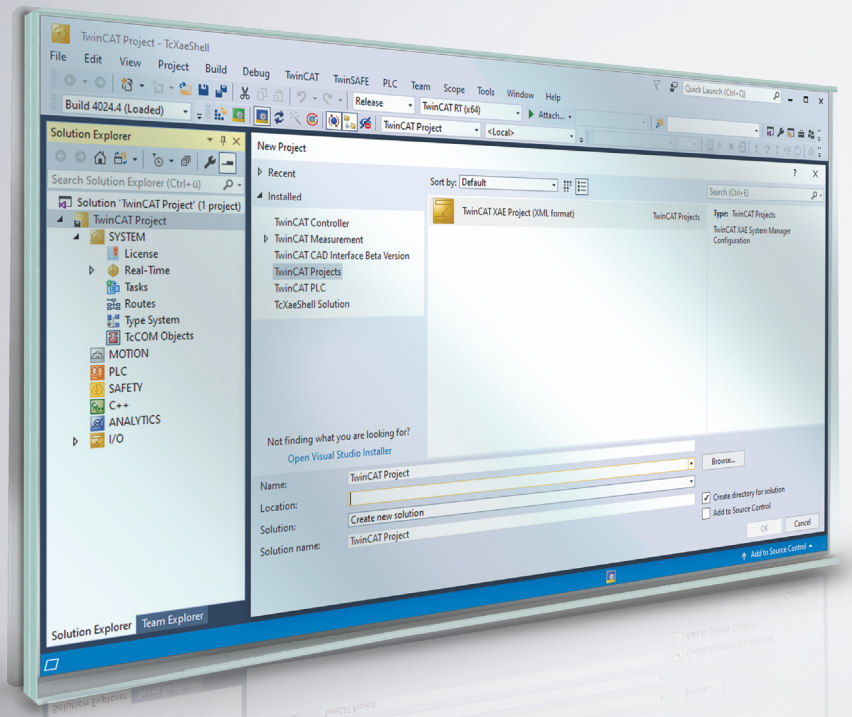
BECKHOFF New Automation Technology

Original-Handbuch | DE

IPC-Security-Leitfaden

für TwinCAT/BSD



28.03.2024 | Version: 1.1

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®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® und XPlanar® 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 Bezeichnungen führen.

Patente

Die EtherCAT-Technologie ist patentrechtlich geschützt, insbesondere durch folgende Anmeldungen und Patente:
EP1590927, EP1789857, EP1456722, EP2137893, DE102015105702
mit den entsprechenden Anmeldungen und Eintragungen in verschiedenen anderen Ländern.

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

Copyright

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 `43 7E 2F D4 C5 01 A3 76 7D C2 31 9B` und dem Fingerabdruck `EE 3C 29 C3 BA BC 4F D6 43 BE D1 B2 6B 0E 4A FD 22 CF 4E E0`

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 normaler 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® 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 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“. Beckhoff bietet die genannten Betriebssystem-Images auf dem IPC in zwei Varianten vorinstalliert an: Bei der einen Variante ist für „Administrator“ ein Zufallspasswort voreingestellt, das von einem Etikett am Gerät abgelesen werden kann. Bei der zweiten Variante ist hierfür das dokumentierte bekannte Passwort vorkonfiguriert. Bitte beachten Sie Folgendes: Letzteres ist im Hinblick auf die Anforderungen einiger Umgebungen nicht „Secure by Default“, während es für andere gut geeignet ist.

Die genannten Betriebssysteme werden nicht von Beckhoff entwickelt. Die Basis der Windows 10 Images von Beckhoff wird von der Microsoft Corporation entwickelt und gepflegt. Die Basis von TwinCAT/BSD wird von „The FreeBSD Project“ entwickelt und gepflegt. Beide 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 [▶ 35]. 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“)

Kategorie	Beschreibung
	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 [▶ 32])
- Abgeschlossener Schaltschrank [▶ 15]
- Schnittstellen im BIOS abschalten (BIOS-Einstellungen [▶ 17])
- Whitelisting für Programme [▶ 30]

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 [▶ 24]
- 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 [▶ 15]

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 [▶ 15]

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 [▶ 23])

- Whitelisting für Programme [▶ 30]

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 [▶ 23])
- Netzwerkbasierte Erkennungsmechanismen (IDS/IPS)
- Abschalten nicht benötigter Dienste
- Entfernen nicht mehr benötigter Komponenten [▶ 30]

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 [▶ 23])
- 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 [▶ 30]

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 Sichere Datenvernichtung

Bei ausrangierten oder außer Betrieb genommenen Komponenten ist es wichtig, die Daten sicher zu vernichten. Als sichere Methode eignet sich das mehrfache Überschreiben der Datenträger.

Zum sicheren Vernichten von Daten bei ausrangierten oder außer Betrieb genommenen Kom-ponenten ist das Überschreiben der Datenträger zu empfehlen. Booten Sie das Gerät dafür von dem TwinCAT/BSD Installer Stick. Falls das Gerät nicht automatisch vom Stick bootet, drücken Sie während des Boot-Vorgangs F7 um den USB-Stick auszuwählen. Im Menü des Installersticks kann nun über den Menüpunkt “Shell“ auf die TwinCAT/BSD Shell des Installer Sticks zugegriffen werden. Mit

```
ls /dev
```

lassen sich die gefundenen Device Nodes, bzw. die gefundenen Datenträger, anzeigen. Da-tenträger werden in der Regel mit ada0 oder da0 angezeigt, wobei „ada“ für Sata Datenträger und „da“ für SCSI Datenträger steht. CFast Karten werden somit als “ada” aufgeführt, USB-Sticks als „da“.

Wenn die Daten auf der CFast Karte des Geräts unwiederbringlich zerstört werden sollen, gehen Sie wie folgt vor, um den Datenträger mit Nullen zu überschreiben:

```
dd if=/dev/null of=/dev/ada0 bs=100m
```

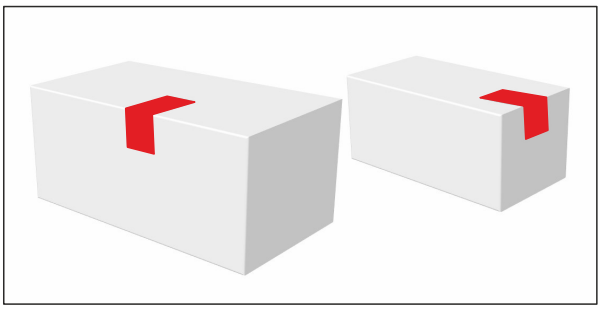
Physische Vernichtung

Wenn Sie eine Festplatte nicht überschreiben wollen oder wegen eines Defekts nicht können, so sollten Sie die Festplatte physisch beschädigen oder zerstören.

3.4 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 TwinCAT/BSD-System, um im Falle eines Datenverlustes oder bei defekten Speichermedien TwinCAT/BSD 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 werden soll.

Beckhoff bietet mit dem TwinCAT/BSD-Installer-Stick eine einfache Backup-Lösung an. Zusätzlich dazu sind mit dem Programm `restorepoint` Wiederherstellungspunkte unter TwinCAT/BSD möglich, welche den aktuellen Zustand des Systems speichern und bei Bedarf wiederherstellen. Eine Vielzahl von Implementierungen ist somit verfügbar, wobei die genaue Definition einer Backup- und Wiederherstellungsstrategie dem Anwender überlassen ist.

Folgende Szenarien sind möglich und sollen dazu dienen, die unterschiedlichen Funktionsweisen zu verstehen. Die vorgestellten Szenarien sollten jedoch nicht als der von Beckhoff empfohlene und einzige Weg betrachtet werden.

Szenario 1: Werkseinstellungen

Ein Industrie-PC mit TwinCAT/BSD soll bei einem Problem auf Werkseinstellungen zurückgesetzt werden.

- Der Anwender testet und entwickelt auf einem Industrie-PC mit TwinCAT/BSD.
- In der Test- und Entwicklungsphase gibt es ein Problem, weil beispielsweise grundlegende Einstellungen verändert wurden.
- Der Anwender löst das Problem, indem TwinCAT/BSD auf Werkseinstellungen zurückgesetzt wird (siehe: Auf Werkseinstellungen zurücksetzen [▶ 19]).

Szenario 2: Serienproduktion

Die Test- und Entwicklungsphase wurde erfolgreich abgeschlossen. Der Maschinenbauer will in die Serienproduktion gehen:

- Der Maschinenbauer erstellt einen Wiederherstellungspunkt (Auslieferungszustand OEM), um das System bei einem Fehler wiederherstellen zu können (siehe: Wiederherstellungspunkt erstellen [▶ 20]. Der Endkunde des Maschinenbauers kann diesen Wiederherstellungspunkt seinerseits bei Problemen nutzen.
- Anschließend aktiviert der Maschinenbauer den Write Filter, um TwinCAT/BSD im vorkonfigurierten Zustand zu sichern und um eine Fehlkonfiguration beim Endkunden zu verhindern (siehe: Write Filter [▶ 31]).
- Im letzten Schritt erstellt der Maschinenbauer ein Backup, welches er als Masterimage ablegt und für die Serienproduktion nutzt (siehe: Backup erstellen [▶ 22]).

Szenario 3: Inbetriebnahme beim Endkunden

Die Maschine kommt beim Endkunden an und soll nach der Inbetriebnahme abgesichert werden:

- Nach der Parametrierung der Maschine erstellt der Endkunde einen Wiederherstellungspunkt „Inbetriebnahme“ (siehe: Wiederherstellungspunkt erstellen [▶ 20]).
- Anschließend aktiviert der Endkunde den Write Filter, um eine versehentliche Fehlkonfiguration zu vermeiden (siehe: Write Filter [▶ 31]).
- Der Endkunde erstellt ein eigenes Backup (siehe: Backup erstellen [▶ 22]), um beispielsweise im Fall eines defekten Datenträgers das System wiederherstellen zu können (siehe: Backup wiederherstellen [▶ 22]).

5.1.1 Wiederherstellungspunkt

Wiederherstellungspunkte dienen dazu, einen alten Systemstand wiederherzustellen, wenn TwinCAT/BSD nach einer größeren Systemänderung oder einer Fehlkonfiguration ein unerwünschtes Verhalten aufweist und sich dieses Verhalten nicht leicht beheben lässt. Der Vorteil von Wiederherstellungspunkten ist, dass auf diese Weise Konfigurationsfehler einfach und schnell rückgängig gemacht werden, ohne TwinCAT/BSD neu zu installieren.

Den Zeitpunkt für die Erstellung eines Wiederherstellungspunktes legen Sie fest, wenn Sie beispielsweise eine größere Systemänderung vornehmen oder Programme von Drittanbietern installieren. Wiederherstellungspunkte ersetzen jedoch kein vollständiges Backup und schützen nicht vor Datenverlust. Regelmäßige Backups sind eine weitere Schutzmaßnahme, mit der Sie sich beispielsweise vor Datenverlust durch defekte Speichermedien schützen können (siehe: Backup erstellen [▶ 22]).

Die Wiederherstellungspunkte werden in der Konsole mit dem Programm `restorepoint` erstellt und verwaltet. Folgende Modi werden vom Programm unterstützt:

- `status`: Listet alle verfügbaren Wiederherstellungspunkte auf. Bei Auslieferung ist ein Wiederherstellungspunkt mit dem Namen `factoryreset`, die Beckhoff Werkseinstellungen, verfügbar.
- `create`: Erstellt einen neuen Wiederherstellungspunkt. Der Name des Wiederherstellungspunkts kann als Argument festgelegt werden. Wenn kein Name angegeben wird, wird ein automatisch generierter Name verwendet.
- `rollback`: Rückkehr zu einem bestimmten Wiederherstellungspunkt. Beachten Sie, dass alle Daten, die nach dem Wiederherstellungspunkt erstellt wurden, zerstört werden. Wenn kein Wiederherstellungspunkt als Argument angegeben wird, wird der Benutzer mit einem interaktiven Dialog gefragt.
- `destroy`: Der angegebene Wiederherstellungspunkt wird zerstört. In diesem Modus bleiben alle vorhandenen Daten erhalten, der Wiederherstellungspunkt selbst wird aber gelöscht.

Wiederherstellungspunkte unter TwinCAT/BSD basieren auf ZFS-Snapshots. Dadurch verbrauchen sie bei ihrer Erstellung kaum Speicherplatz. Jede Änderung des gespeicherten Wiederherstellungspunktes zum aktuellen Live-System, mit dem der Anwender arbeitet, spiegelt sich im verbrauchten Speicherplatz des Wiederherstellungspunktes wieder. Lassen sie sich mit `zfs list -t snap` alle Snapshots des Systems anzeigen.

Die Spalte USED zeigt den real verbrauchten Speicherplatz des Snapshots, die Spalte REFER zeigt den Speicherplatz, auf den der Snapshot verweist, der aber real in anderen Datasets gespeichert ist. Es empfiehlt sich also immer vor einer Änderung im System einen Wiederherstellungspunkt zu erstellen, da dies kaum Systemressourcen kostet. Nach einiger Zeit und vielen Änderungen zwischen Wiederherstellungspunkt und Live-System empfiehlt es sich nicht mehr benötigte Wiederherstellungspunkten zu löschen, um den anwachsenden Speicherplatz der Wiederherstellungspunkte wieder freizugeben.

5.1.1.1 Auf Werkseinstellungen zurücksetzen

Sie können TwinCAT/BSD jederzeit auf Werkseinstellungen zurücksetzen und den Auslieferungsstand wiederherstellen, wenn das System beispielsweise nach einer Fehlkonfiguration nicht mehr richtig funktioniert.

Die Wiederherstellungspunkte werden in der Konsole mit dem Programm `restorepoint` erstellt und verwaltet. In diesem Abschnitt wird gezeigt, wie Sie TwinCAT/BSD auf Werkseinstellungen zurücksetzen.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas restorepoint rollback factoryreset` in der Konsole ein.
2. Es werden alle Snapshots angezeigt, auf die das System zurückgesetzt wird.
3. Bestätigten Sie die Wiederherstellung mit **[y]**.

⇨ Das System wird auf Werkseinstellungen zurückgesetzt. Nach einem Neustart befindet sich TwinCAT/BSD wieder im Auslieferungszustand.

5.1.1.2 Wiederherstellungspunkt erstellen

Speicherplatzverbrauch durch Wiederherstellungspunkte

Ein Wiederherstellungspunkt verbraucht Speicherplatz, weil das komplette System gesichert wird, darunter auch Kernel-Dumps unter /`var/crash`. Räumen Sie das System vor der Erstellung eines Wiederherstellungspunkts auf oder löschen Sie alte Wiederherstellungspunkte.

Wiederherstellungspunkte dienen dazu, einen alten Systemstand wiederherzustellen, wenn TwinCAT/BSD nach einer größeren Systemänderung oder einer Fehlkonfiguration nicht mehr richtig funktioniert. Erstellen Sie Wiederherstellungspunkte, wenn Sie größere Systemänderungen vornehmen, Programme installieren oder Tests durchführen wollen.

Die Wiederherstellungspunkte werden in der Konsole mit dem Programm `restorepoint` erstellt und verwaltet. In diesem Abschnitt wird gezeigt, wie Sie Wiederherstellungspunkte unter TwinCAT/BSD erstellen.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas restorepoint create` in der Konsole ein.
2. Der Wiederherstellungspunkt wird mit einem automatisch generierten Namen erstellt.
3. Überprüfen Sie die Erstellung des Wiederherstellungspunktes mit dem Befehl `restorepoint status` und lassen Sie sich alle Wiederherstellungspunkte anzeigen.

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
```

4. Benutzen Sie alternativ den Befehl `doas restorepoint create your-restorepoint` um einen eigenen Namen für den Wiederherstellungspunkt festzulegen.

⇨ Der Wiederherstellungspunkt wird erstellt und kann jederzeit genutzt werden, um das System zurückzusetzen (siehe: Auf Wiederherstellungspunkt zurücksetzen [▶ 20]).

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
your-restorepoint
```

5.1.1.3 Auf Wiederherstellungspunkt zurücksetzen

HINWEIS

Datenverlust

Daten und Wiederherstellungspunkte, die nach einem bestimmten Wiederherstellungspunkt erstellt wurden, werden beim Zurücksetzen eines davor liegenden Wiederherstellungspunktes gelöscht.

Sollte TwinCAT/BSD nach einer Fehlkonfiguration nicht mehr richtig funktionieren, dann können Sie diese Konfigurationsfehler mit Hilfe von Wiederherstellungspunkten einfach und schnell rückgängig machen, ohne TwinCAT/BSD neu zu installieren.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `restorepoint status` in der Konsole ein, um sich alle verfügbaren Wiederherstellungspunkte anzuzeigen.

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
your-restorepoint
```

2. Geben Sie den Befehl `doas restorepoint rollback` in der Konsole ein, um alle vorhandenen Wiederherstellungspunkte zu sehen.
3. Wählen Sie einen Menüpunkt, um das System auf einen bestimmten Wiederherstellungspunkt zurückzusetzen.

```
Administrator@CX-4FAA38~ $ doas restorepoint rollback
Password:
    1 factoryreset
    2 2020-08-28T08:56:14Z
    3 2020-08-28T09:03:05Z
    4 your-restorepoint
```

4. Es werden alle Snapshots angezeigt, auf die das System zurückgesetzt wird.
5. Bestätigten Sie die Wiederherstellung mit **[y]**.

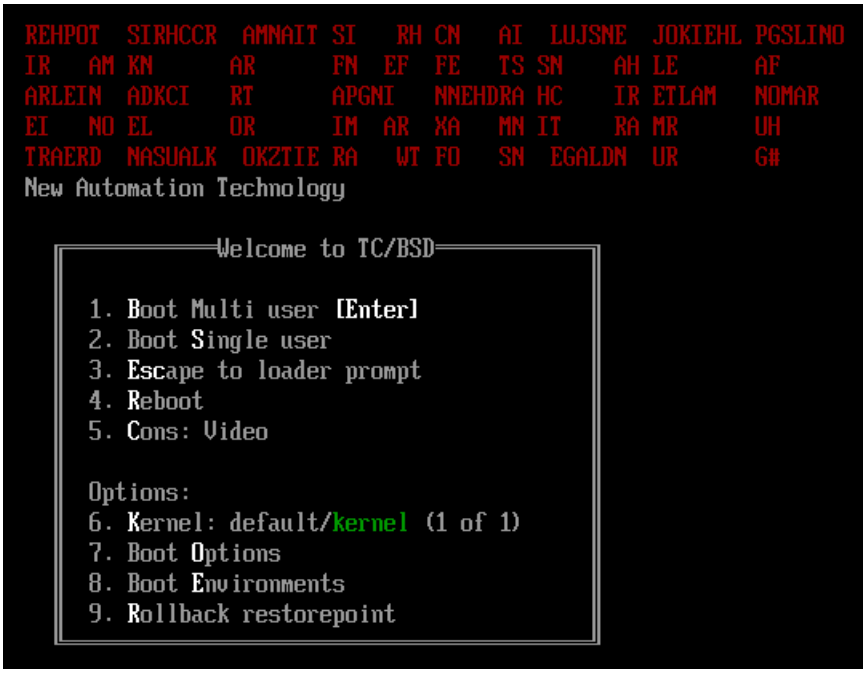
⇨ TwinCAT/BSD wird auf den Wiederherstellungspunkt zurückgesetzt und neu gestartet. Beachten Sie, dass Daten und Wiederherstellungspunkte, die nach dem gewählten Widerherstellungspunkt erstellt wurden, beim Zurücksetzen gelöscht werden.

5.1.1.4 Restore-Bootumgebung einsetzen

Sie haben die Möglichkeit einen Wiederherstellungspunkt aus der Restore-Bootumgebung wiederherzustellen, wenn TwinCAT/BSD nicht mehr bootet und dadurch die Konsole unzugänglich ist. Starten Sie dazu das Bootmenü während des Bootvorgangs, um in die Restore-Bootumgebung zu wechseln.

Gehen Sie wie folgt vor:

1. Starten Sie den Industrie-PC.
2. Halten Sie beim Booten die **[Leertaste]** gedrückt. Das Bootmenü erscheint.



3. Wählen Sie die Option **Rollback restorepoint**.

⇨ TwinCAT/BSD wird in der Restore-Bootumgebung gestartet. Jetzt können Sie die Werkseinstellungen mit dem Befehl `restorepoint rollback factoryreset` wiederherstellen oder einen eigens erstellten Wiederherstellungspunkt nutzen (siehe: Auf Wiederherstellungspunkt zurücksetzen [▶ 20]).

5.1.2 Backup und Restore

Im Gegensatz zu einem Wiederherstellungspunkt kann bei einem Backup TwinCAT/BSD als Sicherheitskopie auf einem externen Speichermedium gespeichert und verwaltet werden.

Diese Sicherheitskopie kann dazu benutzt werden, um das System im Fall eines Systemausfalls bzw. eines Datenverlustes wiederherzustellen. Erstellen Sie regelmäßig Backups von Ihrem System, um Ihren Industrie-PC wieder auf den Stand zurücksetzen zu können, den er zum Zeitpunkt des Backups hatte.

5.1.2.1 Backup erstellen

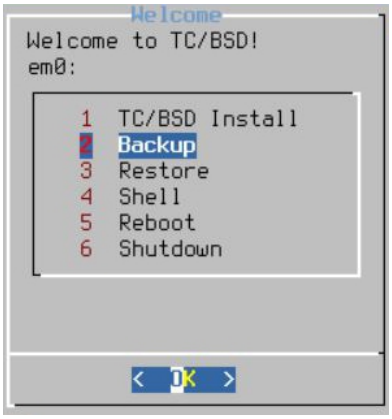
Sie können ein Backup mit Hilfe des TwinCAT/BSD-Installer-Sticks erstellen und wiederherstellen. Alle Backups werden auf einer FAT32-Partition auf dem USB-Stick gespeichert. FAT32 ist interoperabel mit Windows und FreeBSD. Dadurch können die erstellten Backups sowohl mit einem TwinCAT/BSD-System als auch mit einem Windows-System verwaltet werden.

Voraussetzungen:

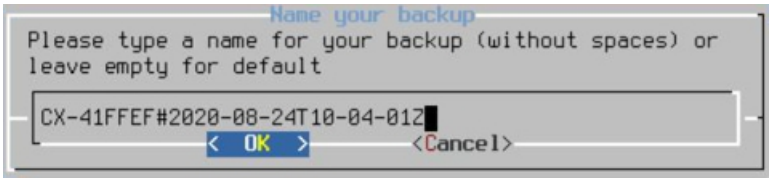
- TwinCAT/BSD-Installer-Stick (siehe: Bootfähigen USB-Stick erstellen).

Erstellen Sie ein Backup wie folgt:

1. Schließen Sie den TwinCAT/BSD-Installer-Stick an den Industrie-PC an.
2. Booten Sie den Industrie-PC vom TwinCAT/BSD-Installer-Stick.
3. Öffnen Sie das Bootmenü mit **[F7]**. wenn der Industrie-PC nicht automatisch vom USB-Stick booten sollte.
4. Wählen Sie den UEFI-Eintrag für den USB-Stick aus und bestätigen mit **[Enter]**. Der Industrie-PC bootet vom USB-Stick und der Beckhoff TwinCAT/BSD-Installer wird ausgeführt.
5. Wählen Sie die Option **Backup**.



6. Vergeben Sie einen Dateinamen für das Backup oder übernehmen Sie den Standardnamen aus Hostnamen und Zeitstempel.



7. Wählen Sie die Option **Reboot** für einen Neustart, sobald das Backup fertiggestellt wurde.

⇨ Die Backups werden mit dem jeweiligen Dateinamen auf dem USB-Stick gespeichert. Archivieren Sie die Backups auf dem USB-Stick. Sie können die Backups auch auf ein externes Speichermedium kopieren oder im Netzwerk archivieren.

5.1.2.2 Backup wiederherstellen

Geeignete Backups für die Wiederherstellung verwenden

Ein Backup darf nur auf einem Gerät innerhalb einer Serie, z.B. CX51x0, CX20x3, C6015 usw., wiederhergestellt werden, da sonst Inkompatibilitäten auftreten können, wenn das Backup auf einem Gerät einer anderen Serie wiederhergestellt wird.

Sie können ein Backup mit Hilfe des TwinCAT/BSD-Installer-Sticks wiederherstellen. Dazu muss der Industrie-PC vom TwinCAT/BSD-Installer-Stick gebootet werden.

Voraussetzungen:

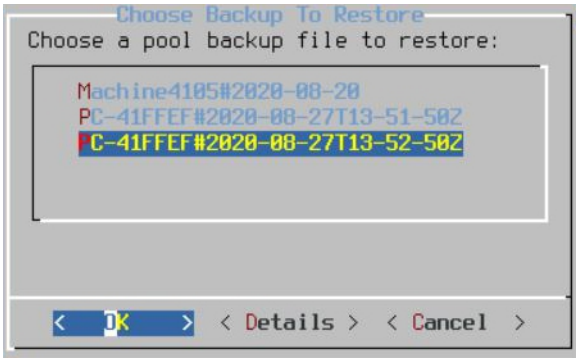
- TwinCAT/BSD-Installer-Stick (siehe: Bootfähigen USB-Stick erstellen).

Gehen Sie wie folgt vor:

1. Schließen Sie den TwinCAT/BSD-Installer-Stick an den Industrie-PC an.
2. Booten Sie den Industrie-PC vom TwinCAT/BSD-Installer-Stick.

Öffnen Sie das Bootmenü mit [F7]. wenn der Industrie-PC nicht automatisch vom USB-Stick booten sollte.

3. Wählen Sie den UEFI-Eintrag für den USB-Stick aus und bestätigen mit **[Enter]**. Der Industrie-PC bootet vom USB-Stick und der Beckhoff TwinCAT/BSD-Installer wird ausgeführt.
   Wählen Sie die Option **Restore**.
4. Wählen Sie das Backup, welches auf dem Industrie-PC wiederhergestellt werden soll.



⇨ Starten Sie den Industrie-PC nach der Wiederherstellung neu. Der Industrie-PC ist wieder auf dem Stand, den er zum Zeitpunkt des Backups hatte.

5.1.2.3 Backup aus Live-System erstellen und wiederherstellen

Wenn es ihre Applikation erfordert, können Backups auch aus dem Live-System heraus und ohne TwinCAT/BSD-Installer-Stick erstellt und wiederhergestellt werden. Benutzen Sie dazu die Skripte TcBackup und TcRestore.

Erstellen Sie ein Backup aus dem laufenden System nur dann, wenn das System zum Zeitpunkt des Backups nicht auf den Datenträger schreibt. Ein Backup kann beschädigt werden, wenn das System während des Backups schreibend auf den Datenträger zugreift. Stellen Sie also sicher, dass keine Prozesse laufen, die persistent Daten sichern und dass die Datenträger, auf der Sie ihr Backup wiederherstellen wollen, groß genug ist.

Das Ausführen von TcBackup und TcRestore sowie das Schreiben in und aus der Datei, in der das Backup gesichert wird, muss mit Root-Rechten geschehen. Führen Sie also vorher eine Shell mit Root-Rechten aus, in der Sie dann arbeiten, oder führen Sie den einzelnen Befehl als einen String mit einer Shell mit Root-Rechten aus. Letzteres wird in den nachfolgenden Beispielen gezeigt.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas sh -c "TcBackup.sh --disk /dev/ada0 > backup.tcbkp00"` ein, um ein Backup vom Datenträger ada0 in die Datei Backup.tcbkp00 zu erstellen.
2. Geben Sie den Befehl `doas sh -c "TcRestore.sh --disk /dev/ada1 < backup.tcbkp00"` ein, um ein Backup aus der Datei Backup.tcbkp00 auf dem Datenträger ada1 wiederherzustellen.

⇨ Sie können beide Befehle kombinieren. Mit dem Befehl `doas sh -c "TcBackup.sh --disk /dev/ada0 | TcRestore.sh --disk /dev/ada1"` wird ein Backup vom Datenträger ada0 erstellt und sofort auf dem Datenträger ada1 wiederhergestellt.

5.2 Updates

Regelmäßige Updates sind wichtig, da sie vor allem gefährliche Sicherheitslücken schließen. Die Open-Source-Community schließt bekannte Sicherheitslücken in der Regel sehr schnell. Dieser Vorteil sollte genutzt werden und Patches zeitnah in das System eingespielt werden. Beckhoff stellt über den öffentlichen, in jedem System voreingestellten Package Server, Updates für das Basissystem sowie für viele Programme bereit.

Für ein Systemupdate sollten Sie folgendermaßen vorgehen:

1. Wenn möglich zuerst das Update in Zusammenspiel mit eigenen Programmen auf Testhardware prüfen.
2. Ein Backup des Systems durchführen oder einen Wiederherstellungspunkt erstellen, um im Falle unvorhergesehenen Verhaltens den alten Systemzustand wiederherzustellen (Siehe: Wiederherstellungsoptionen [▶ 18]).
3. Lassen Sie sich mit `doas pkg upgrade -n` zunächst die Packages anzeigen, die aktualisiert werden können und führen Sie anschließend mit `doas pkg upgrade <packagename>` das Update aus.

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 `doas passwd`, den Befehl mit Root-Rechten ausführen 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 TwinCAT/BSD 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 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 wird der Benutzer und der Hostname des Industrie-PCs angezeigt. Zum Beispiel: CX-1D7BD4.
4. Geben Sie den Befehl `passwd` ein, um ein neues Passwort für TwinCAT/BSD festzulegen. Folgen Sie den weiteren Anweisungen.

⇨ Sie haben erfolgreich ein neues Passwort für TwinCAT/BSD festgelegt.

5.3.1.2 Passwortrichtlinien

Eine eigene Passwort-Richtlinie schützt das System vor der Nutzung schwacher Passwörter. Legen Sie Länge und Komplexität der genutzten Benutzerpasswörter fest und beachten Sie die nachfolgenden Empfehlungen:

Zum Definieren einer Passwort-Richtlinie bearbeiten Sie `/etc/pam.d/passwd` wie folgt:

```
doas ee /etc/pam.d/passwd
```

Entfernen Sie das „#“ zu Beginn der Zeile

```
password requisite pam_passwdqc.so enforce=users
```

und fügen Sie je nach Anforderung Einträge für das Modul pam_passwdqc hinzu:

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

Hinter `pam_passwdqc` können fünf Werte gesetzt werden, da für dieses Modul fünf Pass-wortkategorien vordefiniert sind. Die Kategorien umfassen Anforderungen an die Komplexität des Passworts, wie beispielsweise die Kombination von Sonderzeichen, Klein- und Großbuchstaben und Zahlen. Jede Stelle hinter `pam_passwdqc.s` kann entweder mit „disabled“ deaktiviert oder mit einer Zahl für die geforderte Passwortlänge versehen werden und steht jeweils für eine der folgenden Passwortkategorien:

- Passwörter einer Zeichenklasse sind erlaubt, d.h. Passwörter, die nur aus Zahlen oder Klein- oder. Großbuchstaben bestehen
- Passwörter bestehend aus zwei Zeichenklassen sind erlaubt, d.h. Passwörter, die bspw. aus Klein- und Großbuchstaben bestehen
- Passphrasen sind erlaubt, d.h. Aneinanderreihungen von Zeichenketten, die durch Leerzeichen voneinander getrennt sein können
- Passwörter, die aus drei Passwortkategorien bestehen, bspw. Klein- und Großbuchstaben sowie Zahlen.

- Passwörter, die aus vier Passwortkategorien bestehen, d.h. Klein- und Großbuchstaben sowie Zahlen und Zeichen.

Das dargestellte Beispiel erlaubt also nur Passwörter, die aus vier Passwortkategorien und 10 Zeichen bestehen. Das „similiar“ definiert darüber hinaus, ob ein neues Passwort dem alten Passwort ähneln darf. „retry“ beschreibt wie oft `pam_passwdqc` nach einem neuen Passwort fragt, wenn dem Benutzer die Wahl eines neuen Passworts gemäß der Passwort-Richtlinie nicht gelingt.

Weiterführende Informationen zur Konfiguration der Passwort-Richtlinien finden Sie unter https://www.freebsd.org/cgi/man.cgi?query=pam_passwdqc

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 ändern Sie die Shell des Benutzers von sh auf tcsh. Die tcsh Shell hat bereits einen Autologout implementiert, der sich anschließend definieren lässt:

```
chsh -s tcsh
ee ~/.login
```

Fügen Sie die folgende Zeile hinzu und geben Sie die gewünschte Idle-Zeit an, bis der Auto-logout ausgeführt werden soll:

```
set -r autologout=1
```

Loggen Sie sich mit `login` neu ein, damit die Änderungen aktiv werden.

5.3.3 Gruppen- und Dateiberechtigungen

TwinCAT/BSD 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:

```
doas adduser
```

Dies startet einen Assistenten, der Sie durch den Prozess der Benutzererstellung führt. Um einen Benutzer zu bearbeiten, verwenden Sie `doas chpass <Benutzer>`

Es gibt bereits einige Benutzer, die mit dem Basissystem ausgeliefert werden. Neben dem Benutzer Administrator gibt es sogenannte Systemkonten. Diese Konten sind nicht als interaktive Konten eingerichtet und dienen einzig der Verwaltung und Ausführung integrierter Programme.

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

Ändern Sie die Gruppenzugehörigkeiten und legen Sie neue Gruppen an, indem Sie `/etc/group` mit `doas ee /etc/group` entsprechend editieren.

Diese Datei zeigt alle verfügbaren Gruppen an. Die meisten angezeigten Gruppen sind Standard-Gruppen und stammen historisch von Unix. Aus Sicherheitsgründen werden diese Gruppen Systembenutzern zugewiesen, die eine bestimmte Aufgabe haben. Andernfalls würden diese Programme mit Root-Rechten ohne Einschränkungen ausgeführt werden.

Einschränkung der Systembenutzung

Mit sogenannten Anmeldeklassen können Sie Systemressourcen und Informationen definieren, die den Benutzern zur Verfügung gestellt werden.

5.3.4 File-Flags

Zusätzlich zu den grundlegenden Dateiberechtigungen bietet FreeBSD File-Flags an, die eine weitere Sicherheitsebene zur Dateikontrolle hinzufügen. Abhängig von der Sicherheitsstufe, die im Kapitel Securelevel [▶ 28] erklärt wird, haben File-Flags unterschiedliche Auswirkungen. Im Folgenden finden Sie einige gängige File-Flags, die helfen, Ihr System zu sichern. Eine vollständige Liste der File-Flags finden Sie im jeweiligen Handbuch.

sappnd: Dateien, die mit diesem Flag gekennzeichnet sind, können weder bearbeitet noch gelöscht werden, aber es ist erlaubt, den Inhalt anzuhängen. Dies ist z. B. für Protokolldateien sinnvoll, die auf diese Weise wachsen können, aber von einem Angreifer nicht gelöscht werden können, um sein Eindringen zu erschweren. Sappnd kann nur mit Root-Rechten gesetzt werden und kann nicht mit Securelevel 1 oder höher entfernt werden.

uppnd: Wie sappnd, aber neben root kann auch der Dateibesitzer dieses Flag setzen und entfernen. Nützlich, um versehentliches Löschen oder Ändern einer Datei zu verhindern.

schg: Dateien, die mit diesem Flag gekennzeichnet sind, können nicht bearbeitet, gelöscht oder an einen anderen Ort verschoben werden. Schg kann nur mit Root-Rechten gesetzt werden und kann nicht mit Sicherheitsstufe 1 oder höher entfernt werden.

uchg: Wie schg, aber neben root kann auch der Dateibesitzer dieses Flag setzen und entfernen.

Setzen Sie File-Flags mit dem Befehl `chflags`, gefolgt von dem jeweiligen File-Flag und der Datei, die Sie schützen wollen: `doas chflags sappnd /pfad/zu/datei`

File-Flags löschen, indem Sie ein "no" vor den Namen des File-Flags setzen: `doas chflags nosappnd /pfad/zu/datei`

Ein Beispiel für die Verwendung von File-Flags, um Ihr System sicherer zu machen, ist, den Kernel Ihres Dateisystems vor Änderungen zu schützen: `doas chflags schg /boot/kernel/kernel`

Beachten Sie, dass bei Systemaktualisierungen das File-Flag gelöscht werden muss.

Verwenden Sie die Option `-R`, um das File-Flag auch für Verzeichnisse und Dateien in dem von Ihnen angegebenen Ordner redundant zu setzen. Mit dem folgenden Befehl können Sie nicht alle Ihre Protokolldateien entfernen, aber Sie und das System können trotzdem Protokolle anhängen: `doas chflags -R schg /var/log`

Wenn Sie File-Flags nicht einfach entfernen können, dann befindet sich das System möglicherweise in einer höheren Sicherheitsstufe. Standardmäßig befindet sich TwinCAT/BSD in der Sicherheitsstufe -1, die keine zusätzliche Sicherheit für das System bietet und es erlaubt, File-Flags zu ändern. In höheren Sicherheitsstufen ist es nicht möglich File-Flags zu ändern.

5.3.5 Securelevel

Securelevels sind Sicherheitskonfigurationen, die im Kernel gesetzt werden. Durch das Ändern der Securelevels wird definiert, wie restriktiv das System in Bezug auf Systemänderungen sein soll.

Aktivieren Sie die Securelevels beim Booten, indem Sie die folgende Zeile in `/etc/rc.conf` einfügen:

```
kern_securelevel_enable="YES"
```

Es existieren fünf Securelevels, zwischen denen Sie wechseln können. Je höher der Securelevel Ihres Systems ist, desto mehr Sicherheitsfunktionen werden hinzugefügt. Definieren Sie den Securelevel durch Hinzufügen von `kern_securelevel=2` in `rc.conf`. Hier wurde er auf Securelevel 2 konfiguriert. Nach einem Systemneustart ist die Änderung aktiv.

Nachfolgend sind die Folgen für das System beschrieben, die der jeweilige Securelevel mit sich bringt:

-1: Standard, keine zusätzliche Kernel-Sicherheit.

0: Ein System, das auf den Securelevel "0" eingestellt ist, bootet nur mit dem Securelevel "-1" und wechselt automatisch auf den Securelevel "1", wenn es den Multi-User-Mode (Standard-Betriebsmodus) erreicht. Dies ist empfehlenswert, wenn Autostart-Skripte verwendet werden, deren Ausführung bei Securelevel 1 verboten wäre.

1: Bietet einige grundlegende Sicherheitsfunktionen:

- File-Flags können nicht einfach abgeschaltet werden (Siehe: File-Flags [▶ 27]).
- Der Benutzer kann keine Kernel-Module laden und entladen.
- Programme können nicht über Devicenodes (`/dev/mem` und `/dev/kmem`) in den Speicher schreiben.
- Devicenode `/dev/io` kann nicht angesprochen werden.
- Debuggen und Panic des Systems über das Programm `sysctl` ist deaktiviert.
- Schreiben auf Raw-Disk-Devices ist untersagt.

2: Eigenschaften von "1" mit zusätzlichen Eigenschaften:

- Benutzer kann nicht über Devicenode auf Raw-Disk-Geräte schreiben.
- Es ist verboten, die Systemzeit um mehr als eine Sekunde zu verändern

3: Beinhaltet die Funktionen der Sicherheitsstufen 1 und 2 und bietet zusätzliche Netzwerksicherheit:

- Das Editieren von Firewall-Regeln ist deaktiviert.

Passendes Securelevel auswählen

Die Wahl des Securelevels hängt von Ihren Bedürfnissen ab. Wenn Sie ständig Änderungen vornehmen und ein flexibles System benötigen, ändern Sie nichts und lassen Sie das voreingestellte Securelevel (-1) aktiv. Sollten Sie kaum noch Konfigurationen am System vornehmen müssen und soll das System in Produktivumgebung eingesetzt werden, empfiehlt es sich das Securelevel höher zu setzen. Für Systeme in Produktivumgebung, die keine weiteren Systemänderungen benötigen, ist Sicherheitsstufe 2 empfehlenswert. Wenn auch Ihr Netzwerk bereits eingestellt ist und keine weiteren Firewall-Änderungen erforderlich sind, können Sie den Securelevel auf 3 erhöhen.

5.3.6 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 Benutzereingaben können in TwinCAT/BSD protokolliert werden. Jedes Mal, wenn ein Benutzer eine bestimmte Aktion ausführt, wird das Ereignis gelogged. Diese Ereignis-Protokolle sind vor allem für die Überwachung des Systems, Erkennung unberechtigter Zugriffe und für die nach einem Sicherheitszwischenfall anschließende Analyse von Bedeutung.

Lassen Sie den Audit-Daemon nach jedem Systemstart automatisch starten:

```
doas ee /etc/rc.conf
auditd_enable="YES"
```

Starten des Audit Daemons für die aktuelle Session:

```
doas service auditd start
```

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

`/etc/security/audit_control`: Allgemeine, systemweite Audit-Einstellungen.

In den Standardeinstellungen werden die Audit-Protokolle in `/var/audit` gespeichert, bei der Belegung von 5 % des Speichers für Audit-Dateien erscheint ein Warnhinweis und nach 10 Monaten werden die Audit-Protokolle entfernt.

Mit `zroot/var/audit` besteht bereits ein eigenes ZFS-Dataset für die Audit-Protokolle. Es ist ratsam, für dieses Dataset ein Quota, d.h. ein Speicherlimit festzulegen. Auch in der Audit-Standardkonfiguration können bereits große Mengen Daten anfallen – selbst bei Berücksichtigung der automatischen Löschung der Audit-Protokolle nach 10 Monaten. Um das Speicherlimit dieses Datasets zu limitieren und auf diese Weise freien Speicher für die anderen, wichtigen Datasets zu gewährleisten, kann folgendes Kommando genutzt werden, um den Speicherplatz für Auditprotokolle auf beispielsweise 2 GB zu begrenzen:

```
doas zfs set quota=2G zroot/var/audit
```

Alternativ oder auch zusätzlich zu dieser Maßnahme kann der Zeitraum bis zum Löschen der Audit-Protokolle in /etc/security/audit_control verkürzt werden.

```
doas ee /etc/security/audit_control
```

```
expire-after:10M  expire-after:2M
```

`/etc/security/audit_user`: Audit-Einstellungen für einzelne Benutzer

Hier können für einzelne Nutzer separate Audit-Regeln definiert werden. Eine detaillierte Beschreibung der Audit-Regeln und eine Auflistung der Optionen, mit denen Auditregeln für Benutzer definiert werden können, befindet sich im FreeBSD-Handbuch: https://docs.freebsd.org/en/books/handbook/audit/

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 TwinCAT/BSD nicht. Für Unix Systeme gibt es hier verschiedene Ansätze, ein Applikationen-Whitelisting zu realisieren. Diese sind weniger populär im Vergleich zu Windows. Grund hierfür ist eine erhöhte Komplexität durch Kommandozeile und Skripte bei Unix gegenüber der zumeist grafischen Eingabe unter Windows. Stattdessen sollte genau darauf geachtet werden, aus welcher Quelle man Packages bezieht und schauen, welche Packages auf dem System installiert sind (siehe: Entfernen nicht mehr benötigter Komponenten [▶ 30]).

5.4.2 Entfernen nicht mehr benötigter Komponenten

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

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

Mit `pkg info` lassen sich alle auf dem System installierten Packages anzeigen. Bei Auslieferung sind alle hier gelisteten Packages relevant für das Basissystem oder für Beckhoff Software. Neben Packages für TwinCAT mit dem Kürzel TC, der Beckhoff IPC-Diagnose und Packages für das Basissystem, die mit „os-generic“ beginnen, liegen hier auch Abhängigkeiten, also Programme, die von anderen Programmen benötigt werden.

Löschen Sie ein Package, dass eine Abhängigkeit von einem anderen Package ist, so wird beim Löschen abgefragt, ob auch dazugehörige Packages gelöscht werden sollen. So lässt sich feststellen, ob ein Package eine Abhängigkeit von einem noch installierten Package ist. Packages, von denen Sie wissen, dass sie nicht mehr benötigt werden, können mit `doas pkg delete <pkg-name>` gelöscht werden. Danach können mit dem Befehl `doas pkg autoremove` alle nun nicht mehr benötigten Abhängigkeiten gelöscht werden. So wird sichergestellt, dass keine nicht mehr benötigten Packages auf dem System bleiben.

5.4.3 Package-Audit

Das Package Tool, das zum Installieren und Aktualisieren von Software unter TwinCAT/BSD dient, besitzt mit der Audit-Funktion eine Möglichkeit, installierte Software auf bekannte Schwachstellen zu prüfen.

```
doas pkg audit -F
```

Mit dem Kommando wird die Liste der bekannten Schwachstellen heruntergeladen und mit den lokalen Packages verglichen. Sie erhalten die CVE-Nummer (Common Vulnerabilities and Exposures) und einen Link zu weiteren Informationen zur Schwachstelle.

5.4.4 Antiviren Programme

Für TwinCAT/BSD und UNIX-Systeme im Allgemeinen erscheinen Antivirus-Programme als nicht notwendig, weil Schadsoftware für UNIX-Systeme eher selten ist. Viren für Unix-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 TwinCAT/BSD 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 Unix-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 TwinCAT/BSD 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 Write Filter

TwinCAT/BSD verfügt über einen Write Filter, der bestimmte Datasets vor Schreibzugriffen schützt. Der Vorteil eines Write Filters ist, dass der Benutzer ein System in einem vorkonfigurierten Zustand sichern kann. Nach einem Neustart wird das System automatisch in den ursprünglich definierten Zustand zurückgesetzt.

Das Dataset `zroot/ROOT/default`, dass den Großteil des Systems und TwinCAT beinhaltet, ist bei aktivem Write Filter vor Schreibzugriffen geschützt. Alle anderen Datasets werden nicht vom Write Filter erfasst. So können beispielsweise weiterhin Benutzerdateien unter `/home` oder Logdateien unter `/var/log` persistent gespeichert werden, auch wenn der Rest des Systems nach einem Neustart zurückgesetzt wird.

5.5.1 Write Filter aktivieren bzw. deaktivieren

In diesem Schritt wird gezeigt, wie Sie einen Write Filter unter TwinCAT/BSD aktiveren bzw. deaktivieren können. Beachten Sie, dass die Änderungen am Write Filter erst nach einem Neustart wirksam werden.

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas service bwf enable` in der Konsole ein, um den Write Filter zu aktivieren.
2. Bestätigen Sie den Befehl mit dem Administrator-Passwort.

```
Administrator@CX-3D6912:~ $ doas service bwf enable
Password:
bwf_enable: NO -> YES
writefilter enabled, please reboot to make your changes take effect.
```

3. Starten Sie den Industrie-PC mit `shutdown -r now` neu, damit die Einstellungen übernommen werden.

⇨ Der Write Filter ist nach dem Neustart aktiv. Mit dem Befehl `doas service bwf disable` wird der Write Filter wieder deaktiviert.

5.5.2 Ausnahmen definieren

Durch das Erstellen neuer Datasets lassen sich Ausnahmen für den Write Filter definieren, da nur das Dataset `zroot/ROOT/default` vor Schreibzugriffen geschützt wird und alle übrigen Datasets des Systems, auch die neu erstellen, vom Schutz ausgenommen sind.

In diesem Kapitel wird beispielhaft gezeigt, wie ein eigenes Dataset für das TwinCAT-Boot-Verzeichnis erstellt und dieses Verzeichnis dadurch vom Schutz des Write Filters ausgenommen werden kann.

Voraussetzungen:

- Sichern Sie im Vorfeld das TwinCAT-Boot-Verzeichnis, wenn Sie dieses Beispiel nachstellen.
- Deaktivieren Sie den Write Filter (siehe: Write Filter aktivieren bzw. deaktivieren [▶ 31]).

Gehen Sie wie folgt vor:

1. Geben Sie den Befehl `doas rm -rf /usr/local/etc/TwinCAT/3.1/Boot/*` ein.
2. Das Verzeichnis `usr/local/etc/TwinCAT/3.1/Boot` wird aus der Dateihierarchie herausgelöst.
3. Geben Sie den Befehl `doas zfs create -o mountpoint=/usr/local/etc/TwinCAT/3.1/Boot zroot/usr/TwinCAT-Boot` ein, damit das neue Dataset `zroot/usr/TwinCAT-Boot` gemountet wird.

⇨ Sie haben erfolgreich ein neues Dataset für das TwinCAT-Boot-Verzeichnis erstellt. Mit `zfs mount` werden alle gemounteten Datasets angezeigt, darunter auch das neue Dataset `zroot/usr/TwinCAT-Boot`. Alle darunterliegenden Verzeichnisse werden ab jetzt nicht mehr durch einen aktiven Write Filter vor Schreibzugriffen geschützt.

5.6 USB-Filter

Aus Sicherheitsgründen werden USB-Speichergeräte nicht automatisch gemountet. Sie müssen sie für jede Sitzung manuell einbinden oder ein automatisches Einbinden konfigurieren. Beides ist in der TwinCAT/BSD-Dokumentation beschrieben.

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 [▶ 35].

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 [▶ 34]

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 auftreten. Jede dieser Formen hat Vor- und Nachteile. Bei einer Firewall als Teil des Betriebssystems können beispielsweise im Gegensatz zu einer externen Firewall Regeln für Programme konfiguriert werden, aber sie lässt sich auch einfacher durch Malware ändern und de-/aktivieren.

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

TwinCAT/BSD nutzt Packet-Filter (PF) als Firewall. Dieser ist Bestandteil des FreeBSD Basissystems und ist ein System zum Filtern des TCP/IP-Netzwerkverkehrs. Darüber hinaus lassen sich weitere netzwerkrelevante Einstellungen wie NAT und Port-Weiterleitung vornehmen.

Standardmäßig ist das System gehärtet vorkonfiguriert und es werden nur wenige verschlüsselte Verbindungen zugelassen. So ist der ADS-Port 48898 ab Werk gesperrt und nur ADS Secure auf Port 8016 erlaubt. Weitere Ports, die von TwinCAT-Funktionen und weiteren Beckhoff Anwendungen benötigt werden, werden dynamisch in der Firewall geöffnet. Des Weiteren werden SSH, HTTPS und Ping durch die Firewall erlaubt.

Mit `cat /etc/pf.conf` werden die allgemeinen Firewall-Regeln ausgegeben.

Mit `cat /etc/pf.conf.d/bhf` erfolgt die Ausgabe der Firewall-Regeln, die für Beckhoff-Anwendungen von Bedeutung sind.

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)
IPC-Diagnose	https: 443 / tcp
Remote Desktop – RDP (nur Windows 7/10)	3389 / tcp
TwinCAT ADS	Discovery: 48899 / udp (auch ausgehend) Nicht gesichert: 48898 / tcp (auch ausgehend). Port unter TwinCAT/BSD geschlossen Secure ADS: 8016 / tcp (auch ausgehend)

Weitere Dienste

Die folgende Tabelle gibt einen Überblick von oft genutzten Diensten, die zusätzlich geöffnet werden können

Dienst	Ports (eingehend)
SMB	137-139 / tcp 445 / tcp OPC-UA: 4852 / tcp
Cerhost (Windows CE)	987 / tcp
FTP	21 / tcp

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 / tcp (lokal) 1020 / 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)

Dienst	Port (Standardeinstellung)
	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

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/english.php?content=../content/1033/tf6100_tc3_opcua/1448394251.html&id=2325029100913163478
IO Client-Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=
PLCLib Client Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=7305736008379229744
Gateway Security	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=954414165455750259

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 URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_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 auch 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 Wege, der beschrieben ist unter Coordinated Disclosure.

Nummer	Titel	Version	Sprache	Download
2023-001	Open redirect in TwinCAT/BSD package “authelia-bhf”	1.0	EN	Link
2022-001	Null Pointer Dereference vulnerability in products with OPC UA technology	1.0	EN	Link
2021-003	Relative path traversal vulnerability through TwinCAT OPC UA Server	1.0	EN	Link
2021-002	Stack Overflow and XXE vulnerability in various OPC UA products	1.0	EN	Link
2021-001	DoS-Vulnerability for TwinCAT OPC UA Server and IPC Diagnostics UA Server	1.2	EN	Link
2020-003	Privilege Escalation through TwinCAT System Tray (TcSysUI.exe)	1.1	EN	Link
2020-002	EtherLeak in TwinCAT RT network driver	1.1	EN	Link
2020-01	BK9000 couplers - Denial of service inhibits function	1.0	EN	Link
2019-07	Denial-of-Service on TwinCAT using Profinet protocol	1.1	EN	Link
2019-06	CE Remote Display behaves incorrectly with wrong credentials	1.2	EN	Link
2019-05	Remote Code Execution in Remote Desktop Service ("Dejablue")	1.0	EN	Link
2019-04	ADS Discovery	1.1	EN	Link

Nummer	Titel	Version	Sprache	Download
2019-03	Remote Code Execution in Remote Desktop Service	1.4	EN	Link
2019-02	Microarchitectural Data Sampling (MDS) vulnerabilities	1.2	EN	Link
2019-01	Spectre-V2 and impact on application performance as well as TwinCAT compatibility	1.4	EN	Link
2018-02	Updates for OPC-UA components (Several Vulnerabilities)	1.0	EN	Link
2018-01	TwinCAT 2 and 3.1 Kernel Driver Privilege Escalation	1.1	EN	Link
2017-02	Add Route using "Encrypted Password" bases on fixed key	1.3	EN	Link
2017-01	ADS is only designed for use in protected environments	1.4	EN	Link
2015-001	Potential misuse of IPC Diagnostics version < 1.8 backend	1.1	EN	Link
2014-003	Recommendation to change default passwords	1.1	EN	Link
2014-002	ADS communication port allows password bruteforce	1.1	EN	Link
2014-001	Potential misuse of several administrative services	1.1	EN	Link

8.3 Support und Service

Beckhoff und seine weltweiten Partnerfirmen bieten einen umfassenden Support und Service, der eine schnelle und kompetente Unterstützung bei allen Fragen zu Beckhoff Produkten und Systemlösungen zur Verfügung stellt.

Downloadfinder

Unser Downloadfinder beinhaltet alle Dateien, die wir Ihnen zum Herunterladen anbieten. Sie finden dort Applikationsberichte, technische Dokumentationen, technische Zeichnungen, Konfigurationsdateien und vieles mehr.

Die Downloads sind in verschiedenen Formaten erhältlich.

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 weltweiten Beckhoff Niederlassungen und Vertretungen entnehmen Sie bitte unserer Internetseite: www.beckhoff.com

Dort finden Sie auch weitere Dokumentationen zu Beckhoff Komponenten.

Beckhoff Support

Der Support bietet Ihnen einen umfangreichen technischen Support, der Sie nicht nur bei dem Einsatz einzelner Beckhoff Produkte, sondern auch bei weiteren umfassenden Dienstleistungen unterstützt:

- Support
- Planung, Programmierung und Inbetriebnahme komplexer Automatisierungssysteme
- umfangreiches Schulungsprogramm für Beckhoff Systemkomponenten

Hotline:	+49 5246 963-157
E-Mail:	support@beckhoff.com

Beckhoff Service

Das Beckhoff Service-Center unterstützt Sie rund um den After-Sales-Service:

- Vor-Ort-Service
- Reparaturservice
- Ersatzteilservice
- Hotline-Service

Hotline:	+49 5246 963-460
E-Mail:	service@beckhoff.com

Beckhoff Unternehmenszentrale

Beckhoff Automation GmbH & Co. KG

Hülshorstweg 20
33415 Verl
Deutschland

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

Tabellenverzeichnis

Abbildungsverzeichnis

Mehr Informationen:
www.beckhoff.com/TwinCAT-BSD

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