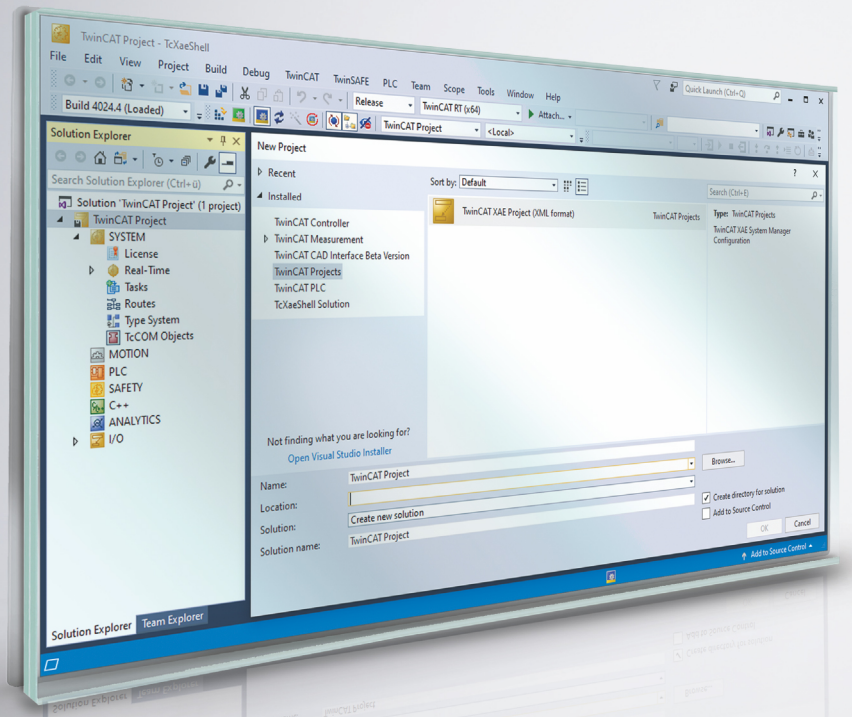
BECKHOFF New Automation Technology

Original-Handbuch | DE

IPC-Security-Leitfaden

für Windows CE



28.03.2024 | Version: 1.1

Inhaltsverzeichnis

1 Hinweise zur Dokumentation 5
1.1 Schwachstellen melden 6
1.2 Kontakt Beckhoff Incident Response Team 6
1.3 Hinweise zur Informationssicherheit 7
1.4 Designziele für Sicherheit 7
2 Gefährdungen und Risikobestimmung 9
2.1 Angreifer 9
2.2 Angriffstypen 9
2.3 Typische Bedrohungsszenarien 10
3 Allgemeine Maßnahmen 15
3.1 Schulung der Mitarbeiter 15
3.2 Physische Maßnahmen 15
3.3 Sichere Datenvernichtung 15
3.4 Security-Siegel auf Produktverpackungen 16
4 BIOS-Einstellungen 17
5 Betriebssystem 18
5.1 Backup und Recovery 18
5.2 Updates 18
5.3 Benutzer- und Rechteverwaltung 19
5.3.1 Sichere Passwörter 19
6 Netzwerkkommunikation 21
6.1 Firewall 21
6.2 Netzwerktechnologien 22
6.2.1 Modbus 22
6.2.2 ADS 22
6.2.3 OPC UA 23
6.2.4 VPN 23
6.2.5 RDP 23
6.2.6 CerHost 23
6.3 Security Gateway 23
6.4 Wichtige TCP/UDP-Ports 23
6.5 CE-Webserver 25
7 TwinCAT 26
7.1 eXtended Automation Engineering (XAE) 26
7.2 eXtended Automation Runtime (XAR) 26
7.3 Weitere technische Informationen 27
8 Anhang 28
8.1 Weiterführende Literatur 28
8.2 Advisories 28
8.3 Support und Service 29

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 [▶ 23]. 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:

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

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 [▶ 19]
- 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:

- Festplattenverschlüsselung
- 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:

- Festplattenverschlüsselung
- 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 [▶ 18])
- Whitelisting für Programme

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:

- Windows Aktualisierungen (Updates [▶ 18])
- Regelmäßige oder automatische Software-Aktualisierungen (Updates [▶ 18])
- Netzwerkbasierte Erkennungsmechanismen (IDS/IPS)
- Abschalten nicht benötigter Dienste
- Entfernen nicht mehr benötigter Komponenten

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 [▶ 18])
- 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

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.

Dabei können Daten auf intakten Festplatten mit spezieller Software durch Überschreiben vollständig und nicht wiederherstellbar gelöscht werden. Die Daten werden einmal oder mehrfach mit vorgegebenen Zeichen oder Zufallszahlen überschrieben, was in den meisten Fällen ausreichend ist.

Windows überschreibt mittlerweile beim "langsamen" Formatieren eine Partition komplett mit Nullen. Bei älteren Festplatten (< 80GB) sollten die Daten 7-fach überschrieben werden. Moderne Festplatten erlauben die Anwendung des Befehls ATA-"Enhanced Security Erase". Hierbei wird eine herstellerspezifische Routine in der Festplatte angestoßen, welche die gesamte Festplatte inklusive defekter Speicherbereiche löschen soll. Bei SSD oder SSHD wird diese Löschmethode empfohlen. Die Anwendung des Befehls sollte mit dem oben angeführten Überschreiben kombiniert werden. Die Datenträger sind nach dem Überschreiben weiterhin nutzbar.

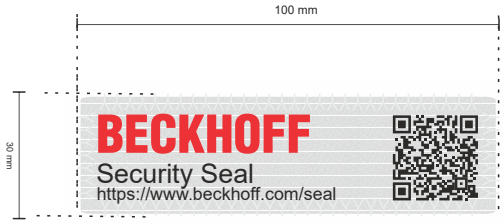
Auf dem Softwaremarkt gibt es sowohl Freeware als auch kommerzielle Produkte, die die erwähnten Überschreibmethoden ausführen. Die meisten dieser Werkzeuge bieten verschiedene Verfahren des Überschreibens an. Wir empfehlen, Programme zum Überschreiben der Festplatten zu verwenden, die von einem bootfähigen Medium (z. B. CD, USB-Stick) gestartet werden und die Festplatten im Ganzen überschreiben.

Physische Vernichtung

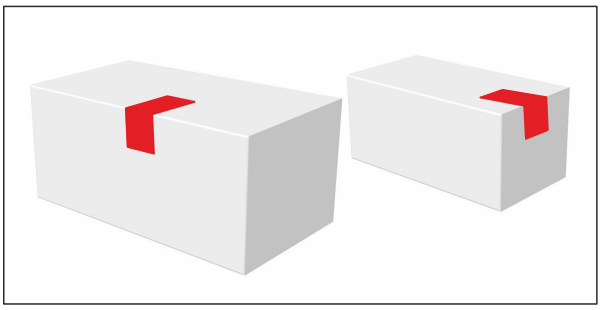
Wenn Sie eine Festplatte nicht überschreiben wollen oder wegen eines Defekts nicht können, so sollten Sie die Festplatte physisch beschädigen oder zerstören.

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 Backup und Recovery

Eine Backup- und Recovery-Strategie sollte für jedes Gerät erstellt werden und schützt vor:

- Security-Zwischenfällen,
- Datenverlust durch defekte Speichermedien,
- oder vor korrupten Daten durch unsachgemäßes Herunterfahren.

Das zuletzt erstellte Backup kann in kürzester Zeit wiederhergestellt werden und verhindert auf diese Weise große Produktionsausfälle. Wichtig ist, neben dem Anlegen von Backups auch einen Wiederherstellungsprozess festzulegen.

Backup und Recovery sind keine exklusive Security-Angelegenheit, helfen jedoch auch in Security-Vorfällen eine Ausfallzeit zu minimieren.

Ein Prozess sowohl zum Erstellen einer Sicherungskopie, aber auch ein Prozess zum Wiederherstellen sollte definiert werden. Dabei sollten auch Security-Aspekte berücksichtigt werden.

Wird eine komplett automatisierte Backup-Lösung eingesetzt, so ist das Backup-System selbst meist im Netzwerk zugreifbar und dadurch auch angreifbar; hier haben also manuelle („offline“) Backups einen Mehrwert. Offsite-Backups, also Backups, die auch örtlich getrennt gelagert werden, haben den Vorteil, dass auch bei einem lokalen Ereignis, wenn die Maschine selbst nicht betroffen ist, eine Wiederherstellung erfolgen kann.

Es sind also vielfältige Ausführungen verfügbar und denkbar.

Da die TwinCAT Boot-Projekte und alle nötigen Informationen als Dateien auf dem Dateisystem des jeweiligen Betriebssystems abgelegt sind, reicht eine dateibasierte Sicherung in diesem Fall aus.

Eine Backup- und Recovery-Lösung stellt Beckhoff mit dem „Beckhoff Service Tool“ (BST) bereit. Weitere Informationen zum BST siehe: Infosys Eintrag zum BST.

Wenn Ihr Industrie-PC mit aktivierter BitLocker-Verschlüsselung für die Systempartition ausgeliefert wird, dann ist der Schlüssel zur Entschlüsselung der Partition während eines unbeaufsichtigten Starts durch das Trusted Platform Module (TPM) auf dem Mainboard des Geräts geschützt. Das TPM-Modul stellt dem Windows-Kernel den Schlüssel zur Entschlüsselung nur dann zur Verfügung, wenn die Messung des frühen Startvorgangs zeigt, dass bisher vertrauenswürdige Software mit einer bekannten Konfiguration gestartet wurde und dass weder die Software noch die Konfiguration noch die nächste zu startende Software (d. h. der Kernel) manipuliert wurde.

Ein vollständiges Backup muss die Bootpartition und die Systempartition umfassen. Wenn Sie die komplette Boot-Disk als Raw-Device sichern, enthält Ihr Backup die verschlüsselte Systempartition. Zusätzlich zum Backup müssen Sie auch einen Wiederherstellungsschlüssel exportieren. Ein Wiederherstellungsschlüssel wird insbesondere benötigt, um das Backup auf einer anderen Hardware wiederherstellen und verwenden zu können. Bitte bewahren Sie diesen Wiederherstellungsschlüssel an einem sicheren und geschützten Ort auf. Außerdem wird dringend empfohlen, immer einen Wiederherstellungsschlüssel für den Fall bereitzuhalten, dass rechtmäßige Änderungen an der Software und der Konfiguration vorgenommen wurden, die Teil des frühen Startvorgangs sind. Dies kann beispielsweise der Fall sein, wenn die Boot-Sequenz der Firmware (BIOS) von autorisierten Personen geändert wird.

Bei aktivierter BitLocker-Verschlüsselung gibt es eine Alternative zu einer vollständigen Sicherung der Partitionen inklusive der verschlüsselten Systempartition: Sie können die Verschlüsselung der Systempartition vorübergehend deaktivieren und wie gewohnt ein Offline-Backup erstellen. Bitte vergessen Sie nicht, die Verschlüsselung anschließend wieder zu aktivieren.

5.2 Updates

Um Betriebssystem und Programme auf aktuellem Stand zu halten, gibt es verschiedene Möglichkeiten:

- Update des gesamten Images
- Update einzelner Programme

- Integrierte Betriebssystemupdates

Unter Windows CE gibt es keinen betriebssystemeigenen Update-Mechanismus. Daher gibt es nur die Möglichkeit, das gesamte Image zu aktualisieren. Um herauszufinden, welches Image aktuell installiert ist, gibt es im Ordner `\Hard Disk\` eine Datei, die den Namen (inklusive Version) des Images als Namen hat.

Für Windows CE können diese über http://download.beckhoff.com/download/software/embPC-Control bezogen werden.

Beispiel des Dateinamens-Aufbaus am CX9020 mit TwinCAT 3.1 Build 4024.7:

Name:	"CX9020_CB3011_WEC7_HPS_v608f_TC31_B4024.7"
Plattform:	CX9020 oder CB3011 Motherboard
Bestriebssystem:	WEC7 = Windows Embedded Compact 7
Typ:	HPS = HMI Protected Shell
Version:	v608f
TwinCAT Version:	TC31 = TwinCAT 3.1
TwinCAT Build:	4024.7

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

Vorgehensweise	Beispiel
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

Folgender Benutzer ist in Windows CE standardmäßig bei Auslieferung angelegt:

Benutzername	Standardpasswort
Administrator	1

Unter Windows CE können NTML Nutzer angelegt werden.

Passwort unter Windows CE setzen

✓ Die Windows-CE-Benutzeroberfläche ist gestartet.

1. Wählen Sie **Start > Control Panel > Password**.
2. Geben Sie ein Passwort ein und bestätigen Sie dieses.
3. Beenden Sie den Dialog mit **OK**.
4. Starten Sie das System neu.

⇨ Benutzer können Programme nur starten, wenn das Passwort eingegeben wird.

5.3.1.2 Passwort für RAS-Server ändern

RAS-Benutzer können den Controller aus der Ferne administrieren. Der RAS-Server ist standardmäßig deaktiviert, dennoch sollte das Passwort geändert werden, damit auf einen aktivierten RAS-Server nicht mit dem Auslieferungspasswort zugegriffen werden kann.

✓ Die Windows-CE-Benutzeroberfläche ist gestartet.

1. Wählen Sie **Start > Control Panel > CX Configuration**.
2. Wählen Sie die Registerkarte **RAS Control** aus.

⇨ Die Benutzer können auf der rechten Seite der Registerkarte verwaltet werden.

5.3.1.3 IPC Security Wizard

Über die IPC Diagnose Webseite können Nutzerpasswörter gesetzt werden. Sie ist per https auf Port 443 erreichbar.

Im Auslieferungszustand wird der IPC Security Wizard gestartet, wenn sich ein Nutzer per https verbindet oder auch lokal am Gerät arbeitet.

Der IPC Security Wizard leitet den Nutzer dabei an das Default-Passwort zu ändern.

Siehe auch:

- Dokumentation im Infosystem zur IPC-Diagnose

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 [▶ 23].

6.1 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.

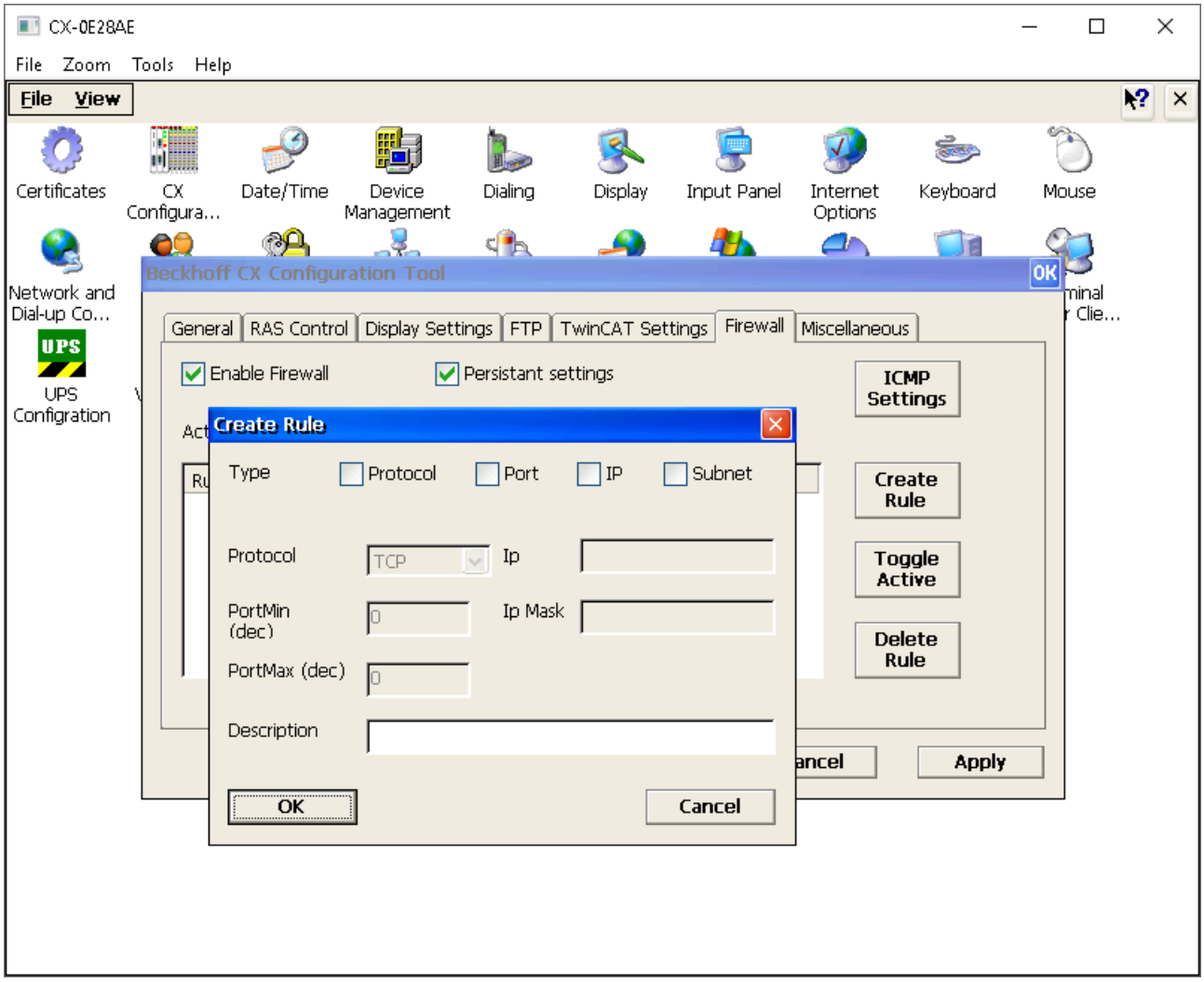
Firewalls mit Deep-Packet-Inspection, die auch die Nutzdaten der Datenpakete auswerten, können den Inhalt von verschlüsselten Verbindungen prinzipiell nicht einsehen. Um dennoch den Inhalt verarbeiten zu können, wird beispielsweise häufig die Verschlüsselung für Webanwendungen an der Firewall terminiert 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 [▶ 23] befindet sich eine Liste von TCP/UDP-Ports, die typischerweise berücksichtigt werden müssen, um eine Firewall zu konfigurieren.

Die Firewall von Windows CE wird über Einträge in der Registry konfiguriert (siehe z. B. https://msdn.microsoft.com/en-us/library/ee494503(v=winembedded.60).aspx).

Zur einfacheren Konfiguration gibt es im Beckhoff CX Configuration Tool die Registerkarte **Firewall**.



6.2 Netzwerktechnologien

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

6.2.1 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.

6.2.2 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

6.2.3 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

6.2.4 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.

6.2.5 RDP

Remote Desktop Protocol (RDP) ist ein proprietäres Protokoll von Microsoft für den graphischen Fernzugriff.

6.2.6 CerHost

CerHost ist ein proprietäres, nicht verschlüsseltes Protokoll von Microsoft für den grafischen Fernzugriff auf Windows CE basierte Betriebssysteme.

Es wird empfohlen, CerHost nur in gesicherten Umgebungen einzusetzen (beispielsweise über gesicherte Transportkanäle).

6.3 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.

6.4 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) 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)

Dienst	Port (Standardeinstellung)
	Siehe auch: Dokumentation zu TF6300
TF6420 Database Server	änderbar je nach Datenbank / tcp (ausgehend) Siehe auch: Dokumentation von TF6420
TF67xx IoT TF35xx Analytics	änderbar je nach Broker / tcp (ausgehend) Siehe auch: Dokumentationen der TF670x sowie TF35xx
TwinCAT EAP	34980 / udp (eingehend), falls EAP über UDP verwendet wird. Die Kommunikation ist nicht durch eine Betriebssystem-Firewall beeinflussbar. Siehe auch: Dokumentation von EAP
TwinCAT ADS-over-MQTT	änderbar je nach Broker / tcp (ausgehend) Siehe auch: Dokumentation zu ADS-over-MQTT

6.5 CE-Webserver

Alle Webseiten, die auf dem Webserver aufbauen, werden nicht mehr funktionieren.

Um den Windows CE-Webserver zu deaktivieren, kann der folgende Registry-Eintrag geändert werden:

`HKEY_LOCAL_MACHINE\Services\HTTPD\Flags`

Wenn dieser Eintrag auf „DWORD 4“ gesetzt wird, wird der Webserver deaktiviert.

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

Tab. 1 Unberechtigte Manipulation am Quelltext. 26
Tab. 2 Unberechtigte Einsicht in den Quelltext. 26
Tab. 3 Unautorisierter Zugriff über ADS oder Secure ADS. 26
Tab. 4 Beeinflussung der Echtzeit über ADS / Secure ADS. 27

Abbildungsverzeichnis

Mehr Informationen:
www.beckhoff.com

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