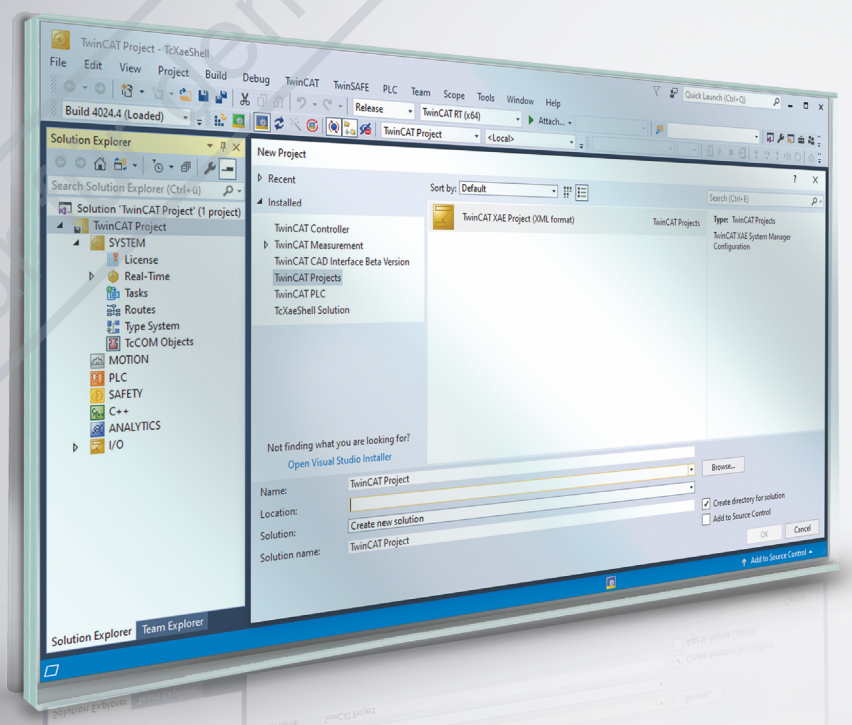
BECKHOFF New Automation Technology

Original-Handbuch | DE

IPC-Security-Leitfaden

für Windows 7



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 [▶ 52]. 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 [▶ 39])
- Whitelisting USB-Geräte (USB-Filter [▶ 47])
- Abgeschlossener Schaltschrank [▶ 15]
- Schnittstellen im BIOS abschalten (BIOS-Einstellungen [▶ 17])
- Whitelisting für Programme [▶ 33]

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 [▶ 22]
- 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:

- Dateiverschlüsselung [▶ 21]
- 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:

- Dateiverschlüsselung [▶ 21]
- 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 [▶ 33]

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 [▶ 39]

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 [▶ 39]

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.

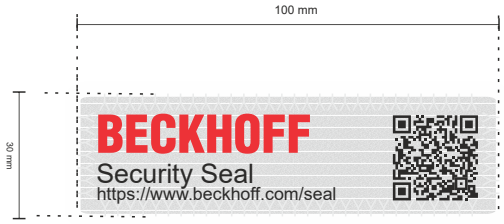
Auf dem Softwaremarkt gibt es sowohl Freeware als auch kommerzielle Produkte, die die erwähnten Überschreibmethoden ausführen. Die meisten dieser Werkzeuge bieten verschiedene Verfahren des Überschreibens an. Wir empfehlen, Programme zum Überschreiben der Festplatten zu verwenden, die von einem bootfähigen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

Physische Vernichtung

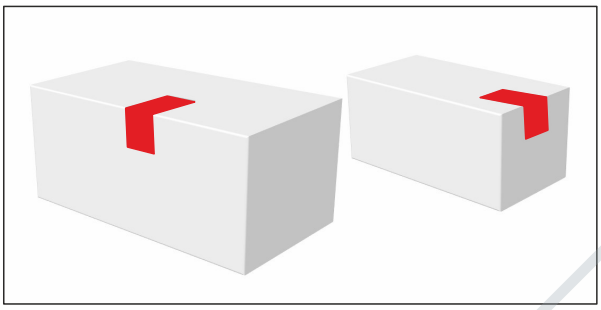
Wenn Sie eine Festplatte nicht überschreiben wollen oder wegen eines Defekts nicht können, so sollten Sie die Festplatte physisch beschädigen oder zerstören.

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

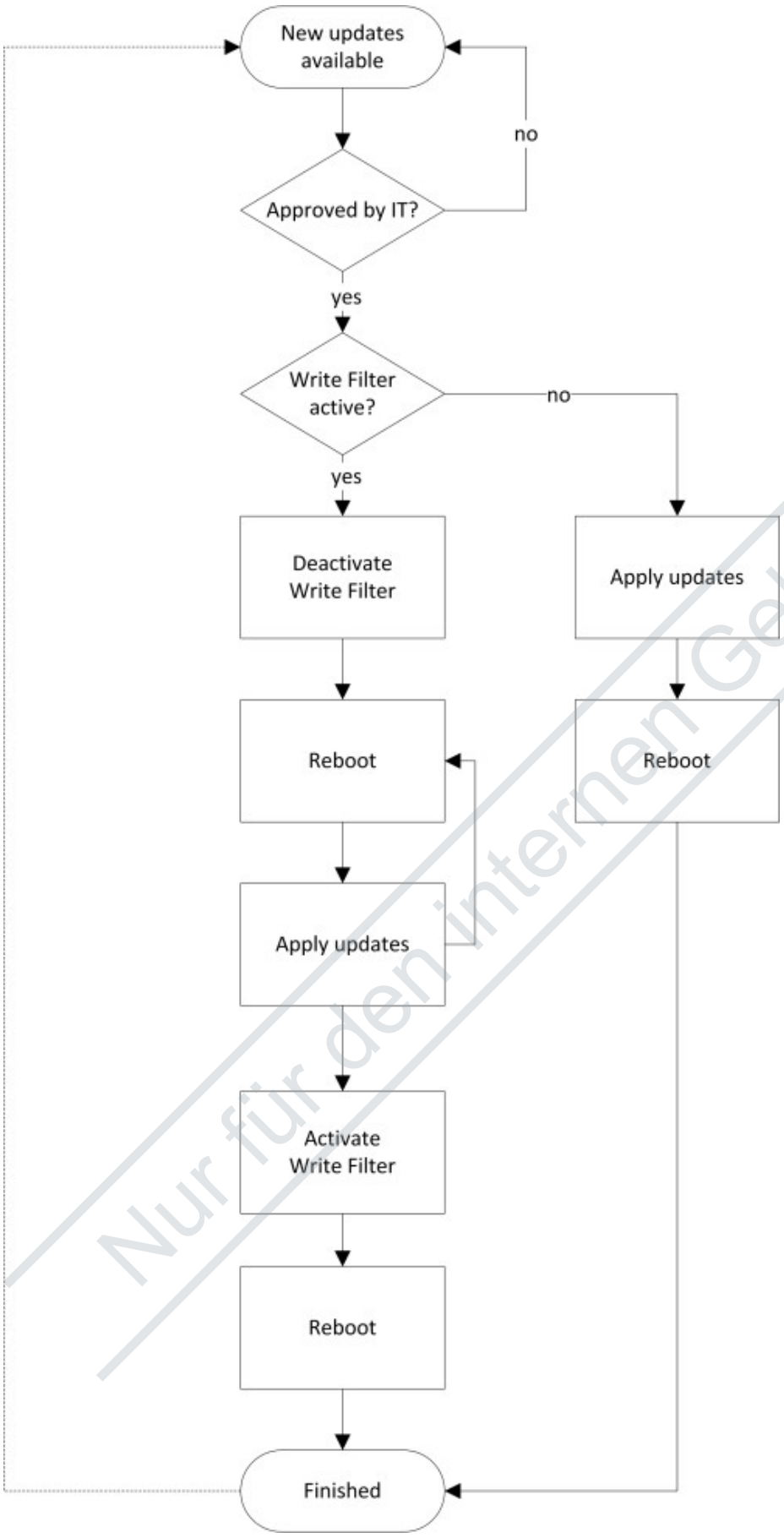
HINWEIS

Datenverlust vermeiden

Sichern Sie Ihre Daten, bevor Sie ein Update durchführen. Erstellen Sie zuerst ein Backup-Image des PCs mit Hilfe eines BST (Beckhoff Service Tool, https://www.beckhoff.de/default.asp?industrial_pc/bst.htm).

Unter Windows 7/10 gibt es einen betriebssystemeigenen Update-Mechanismus, den Windows Update Service. In den von Beckhoff bereitgestellten Images ist der Windows Update Service deaktiviert, um eine unbeabsichtigte Veränderung am System zu vermeiden. Es lassen sich weiterhin Windows Updates manuell von Microsoft herunterladen und installieren. Wenn der Windows Update Service aktiviert wird, dann werden mit den Standardeinstellungen die Updates vom Microsoft Windows Update Server bezogen. Die Kommunikation mit dem Server geschieht über eine verschlüsselte und signierte Verbindung. Die bezogenen Updates sind mit einem offiziellen Zertifikat von Microsoft signiert, um dessen Authentizität prüfen zu können.

Engineering-Rechner sollten mit Updates aktuell gehalten werden. Für die Rechner in Industrieumgebung kann das schwieriger sein. Wenn beispielsweise ein Write Filter verwendet wird, werden die ohne weitere Vorkehrung installierten Updates bei einem Neustart verworfen. Um das zu vermeiden, wird der folgende Ablauf empfohlen:



Nach diesem Vorgang müssen intensive Tests durch den Betreiber die Funktionstüchtigkeit sicherstellen. Beckhoff Geräte werden mit halbjährlich aktualisierten und getesteten Images geliefert, die kompatible Windows Updates beinhalten.

Für Windows 7 / 10 können diese Images über den Beckhoff Service angefragt werden. Hierfür wird die Seriennummer des Gerätes benötigt.

Siehe auch:

- https://www.beckhoff.de/default.asp?industrial_pc/bst.htm

5.3 Dateiverschlüsselung

HINWEIS

Fehlfunktionen

Verschlüsseln Sie nicht die gesamte System-Partition, Windows-System-Dateien oder den TwinCAT-Ordner. Dies kann zu Fehlfunktionen führen.

In der Regel reicht eine etablierte Zugriffskontrolle aus, um sensible Dateien und Verzeichnisse vor einem unberechtigten Zugriff zu schützen. Geht jedoch der Datenträger verloren, ist der Schutz dieser Daten nicht mehr gewährleistet und erfordert zusätzlichen Schutz durch Verschlüsselung einzelner Dateien und Verzeichnisse.

Windows stellt mit EFS (Encrypted File System) eine Verschlüsselungsfunktion zur Verfügung, mit der einzelne Dateien oder ganze Verzeichnisse verschlüsselt werden können. Damit wird eine zusätzliche Sicherheitsstufe und kryptografischer Schutz zur Verfügung gestellt.

Ein wichtiger Aspekt nach der Verschlüsselung ist die Schlüsselverwaltung und die Klärung folgender Fragen:

- Wer soll Zugriff erhalten?
- Welche Authentifizierungsmöglichkeiten gibt es? (USB-Token, PIN, Passwort, Benutzername + Passwort, …)
- Wie werden die Schlüssel verwaltet?

In jedem Fall sind die Daten ungeschützt, wenn sie entschlüsselt und genutzt werden.

Im Vergleich dazu unterstützt BitLocker die Verschlüsselung kompletter Datenträger. Zusätzlich bietet BitLocker maximalen Schutz, wenn es mit TPM (Trusted Platform Module) verwendet wird, wie in der TPM-Dokumentation beschrieben.

EFS aktivieren

1. Klicken Sie mit der rechten Maustaste auf einen Ordner oder eine Datei und wählen Sie in dem sich öffnenden Kontextmenü **Properties** aus.
2. Öffnen Sie die Registerkarte **General** und klicken Sie auf **Advanced**.
3. Um den Ordner oder die Datei zu verschlüsseln, aktivieren Sie das Auswahlkästchen **Encrypt contents to secure data.**

⇨ Wenn dies die ersten auf diesem Weg verschlüsselten Daten sind, erzeugt Windows automatisch ein EFS-Zertifikat im lokalen Zertifikat-Store. Das Zertifikat muss gesichert werden, da eine Wiederherstellung der Daten unmöglich ist (siehe Zertifikat sichern [▶ 21]).

Zertifikat sichern

1. Starten Sie **certmgr.msc**.
2. Klicken Sie auf **Add**, wählen Sie **My user account** und klicken Sie auf **Finish**.
3. Erweitern Sie den Ordner „Personal“ und klicken Sie auf **Certificates**

   ⇨ Sie sollten ein Zertifikat mit dem „Intended Purpose“ „Encrypting File System“ sehen.
4. Um das Zertifikat zu sichern, klicken Sie mit der rechten Maustaste auf das Zertifikat und wählen Sie **All Tasks > Export**.
5. Wählen Sie **Export Private Key**.
6. Wählen Sie **Personal Information Exchange**, **Include all certificates…** und **Enable strong protection**.

7. Geben Sie ein Passwort an, mit dem das Zertifikat geschützt werden soll. Dieses Zertifikat wird später beim Import benötigt.
8. Geben Sie den Pfad an, unter dem das Zertifikat gesichert werden soll. Sichern Sie das Zertifikat an einem anderen gesicherten Ort.

5.4 Benutzer- und Rechteverwaltung

5.4.1 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:

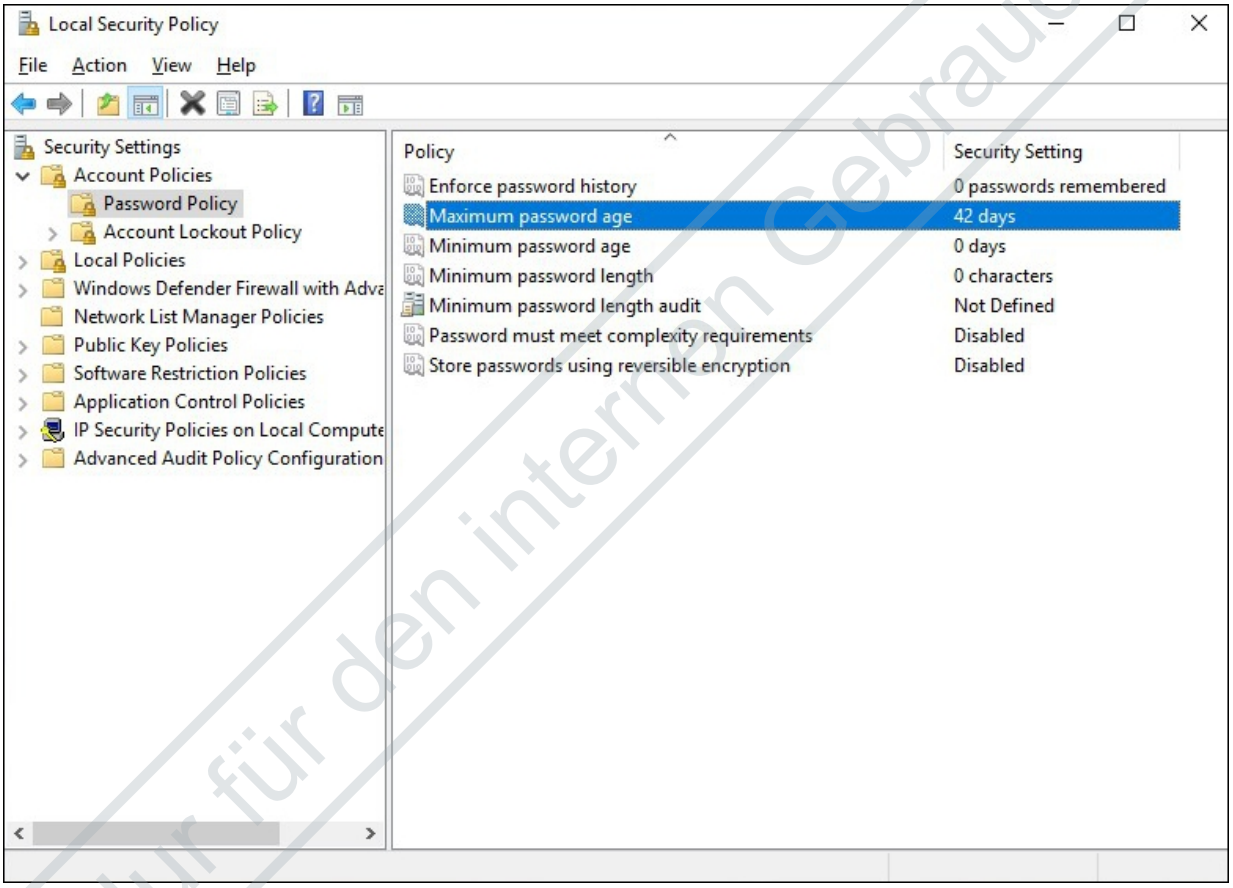
- Wörter, die in Wörterbüchern stehen
- Rückwärts geschriebene Wörter, gebräuchliche Rechtschreibfehler und Abkürzungen
- Folgen aus der Wiederholung von Zeichen, z. B. 12345678 oder abcdefgh
- Persönliche Informationen, z. B. Geburtstage, Ausweisnummern, Telefonnummern

5.4.1.1 Passwort ändern

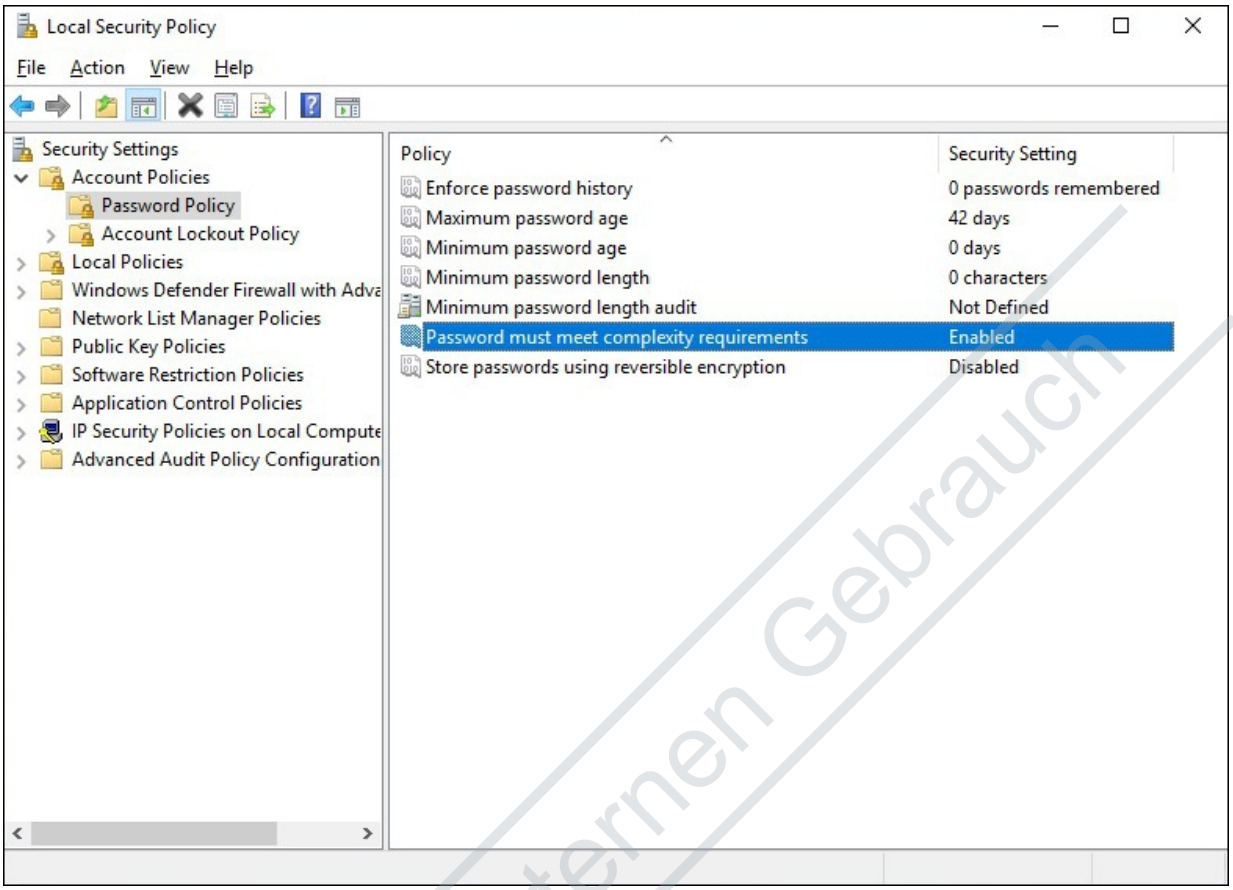
5.4.1.2 Passwortrichtlinien

Passwortrichtlinien ermöglichen es für Benutzerkonten, die wählbaren Passwörter einzuschränken, sodass Benutzer gezwungen sind, sichere Passwörter zu wählen. Eine eigene Passwort-Richtlinie schützt das System vor der Nutzung schwacher Passwörter. Legen Sie Länge und Komplexität der genutzten Benutzerpasswörter fest.

1. Öffnen Sie das **Control Panel** und wählen Sie die Einstellung **Administrative Tools > Local Security Policy**.
2. Wählen Sie im öffnenden Fenster **Account Policies > Password Policy**
3. Bestimmen Sie die Einstellungen der Passwortrichtlinie.
4. Zur Einstellung eines maximalen Alters des Passworts, kann für die Policy **Maximum password age** ein Zeitraum (in Tagen) definiert werden, bevor das System den Benutzer auffordert das Passwort zu ändern.

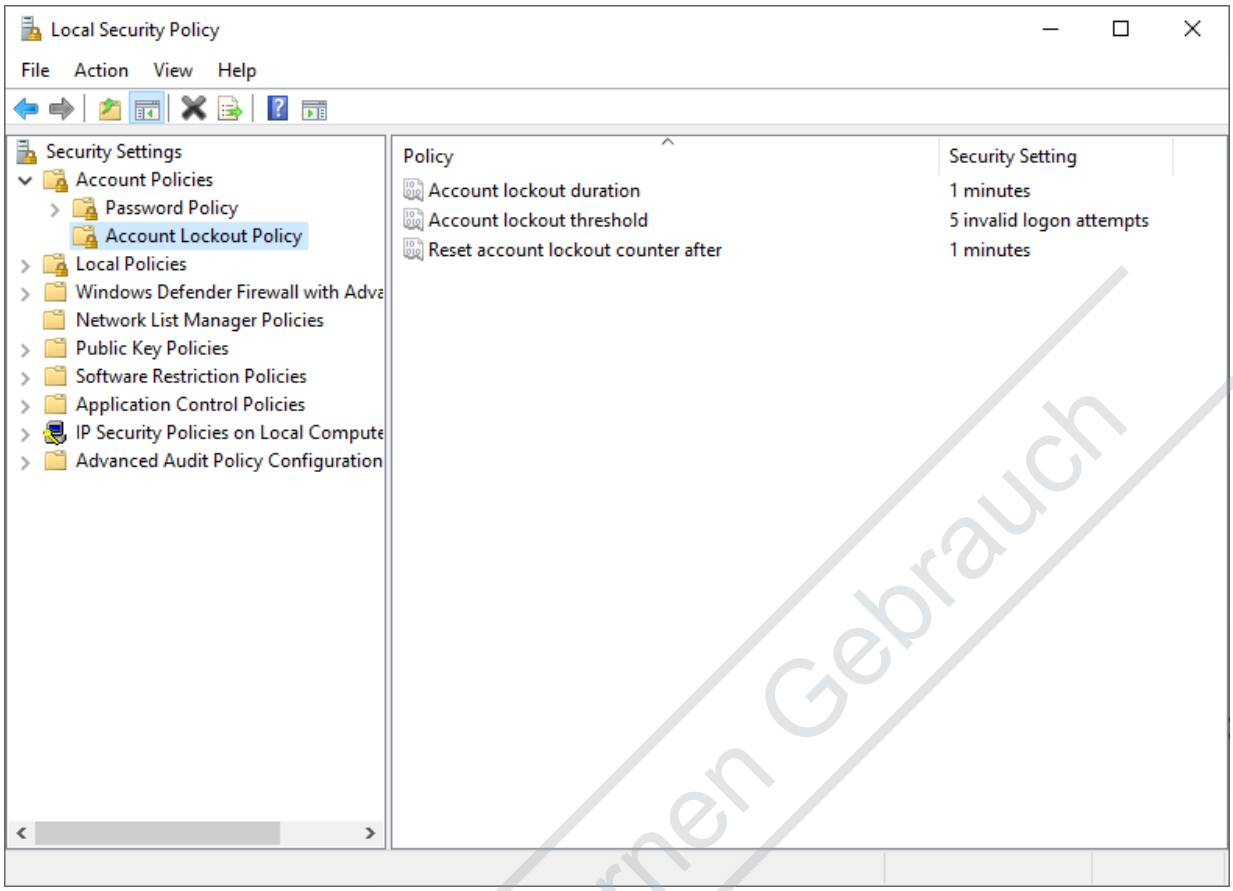


5. Um eine Komplexität von Passwörtern zu verlangen, kann die Policy **Password must meet complexity requirements** gesetzt werden. Mit dem Einschalten dieser Policy wird für zukünftig eingestellte Passwörter verlangt, dass mindestens Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen verwendet werden müssen.



6. Um Angriffe zum Erraten von Benutzerauthentifizierungsdaten zu verhindern, können die Einstellungen unter **Account Lockout Policy** gesetzt werden. Legen Sie die Anzahl der fehlgeschlagenen Anmeldeversuche fest, nach denen ein Benutzerkonto gesperrt werden soll. Mit der Richtlinie **Account**

lockout duration können Sie die Dauer in Minuten festlegen, die ein gesperrtes Konto gesperrt bleibt, bevor es automatisch entsperrt wird.



⇨ Definition der Passwortrichtlinien

5.4.1.3 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.

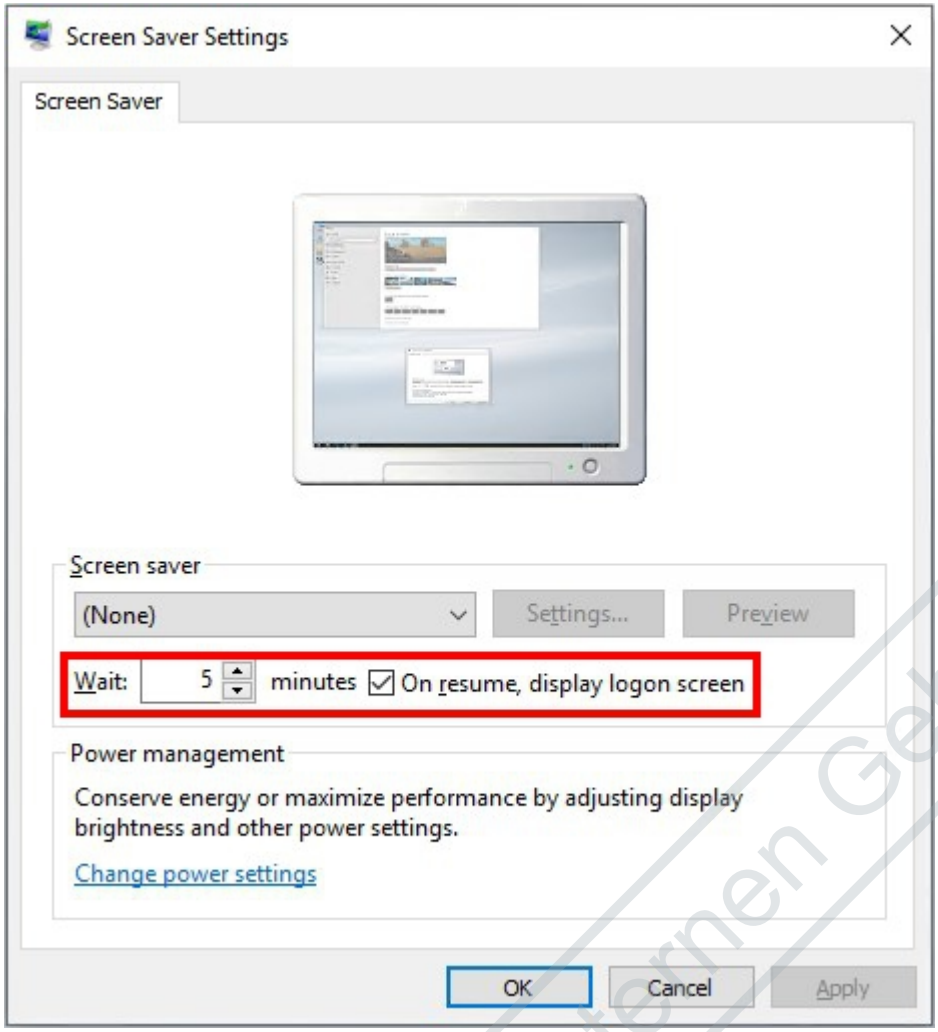
Der IPC Security Wizard leitet den Nutzer dabei an das Default-Passwort zu ändern.

Siehe auch:

- Dokumentation im Infosystem zur IPC-Diagnose

5.4.2 Automatisches Abmelden

Damit ein länger ungenutztes System nicht mit einem bereits angemeldeten Benutzer missbraucht werden kann, lässt sich ein automatisches Abmelden des Benutzers einstellen. Dazu kann in den Screen Saver Setting eine Zeit definiert werden. Nach Ablauf der Zeit wird ein ungenutztes System gesperrt und eine erneute Authentifizierung vom Benutzer verlangt.



5.4.3 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.

Microsoft hat für Windows einen Leitfaden zum Thema Sicherheitsaudits mit den entsprechenden Einstellungen und bewährten Verfahren veröffentlicht. Zu den grundlegenden Überwachungsrichtlinien gehören die folgenden Kategorien, die aktiviert werden können und standardmäßig deaktiviert sind:

- Anmeldeversuche überwachen [▶ 27]
- Datei- und Ordnerzugriffe überwachen [▶ 28]
- Anmeldeereignisse überwachen

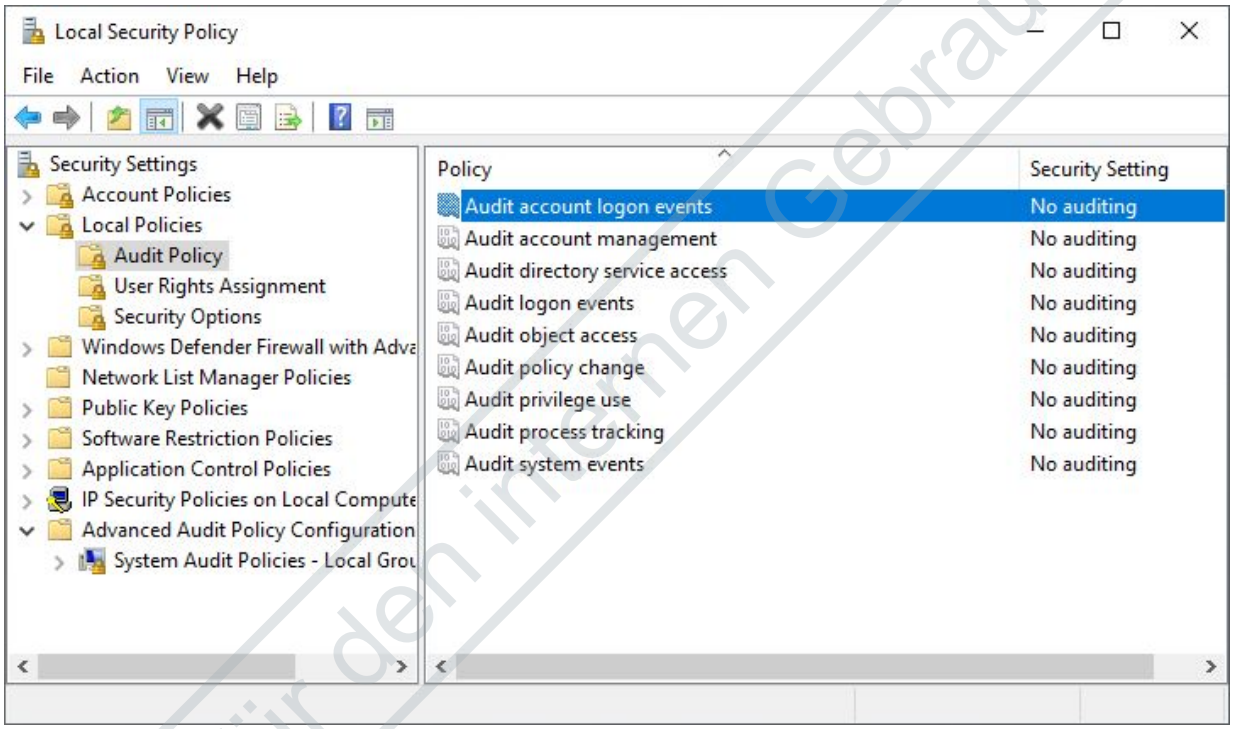
- Objektzugriffsversuche überwachen
- Richtlinienänderungen überwachen
- Rechteverwendung überwachen
- Prozessverfolgung überwachen
- Systemereignisse überwachen

5.4.3.1 Anmeldeversuche überwachen

Überwachen Sie Anmeldeversuche im Beckhoff Device Manager und aktivieren Sie die passende Richtlinie, wenn Sie feststellen wollen, wer sich beispielsweise von welcher IP-Adresse am Webinterface angemeldet hat.

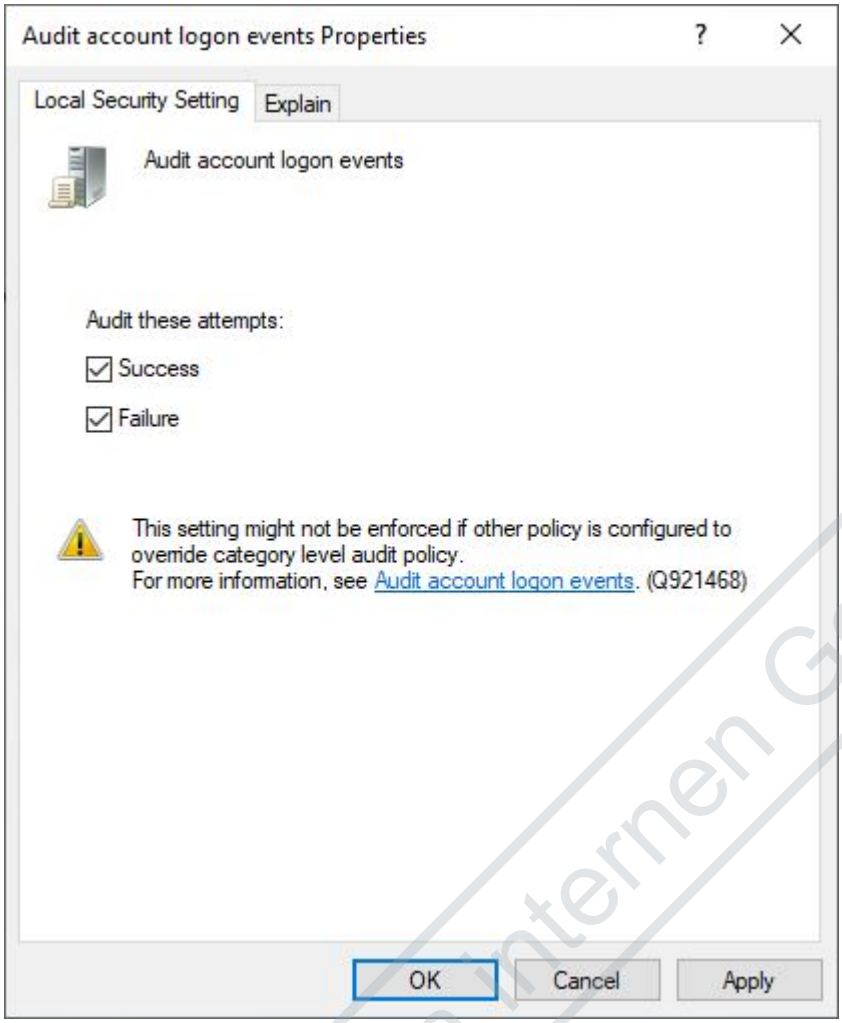
Gehen Sie wie folgt vor:

1. Rufen Sie den Ausführen-Dialog über die Tastenkombination **[Windows-Taste] + [R]** auf und geben Sie **secpol.msc** ein.
   Das Fenster **Local Security Policy** erscheint.



2. Klicken Sie links im Strukturbaum auf **Local Policies > Audit Policy** und wählen Sie die Überwachungsrichtlinie **Audit account logon events**.

3. Aktivieren Sie die Option **Failure**, wenn Sie nur erfolglose Versuche protokolieren möchten. Aktivieren Sie zusätzlich die Option **Success**, wenn Sie auch die erfolgreichen Anmeldungen protokolieren möchten.



⇨ Die protokolierten Einträge sind ab jetzt im **Event Viewer** einsehbar, den Sie mit **[Windows-Taste] + [R]** und dem Eintrag **eventvwr** aufrufen können. Die Einträge können anschließend unter **Windows Logs > Security** eingesehen werden.

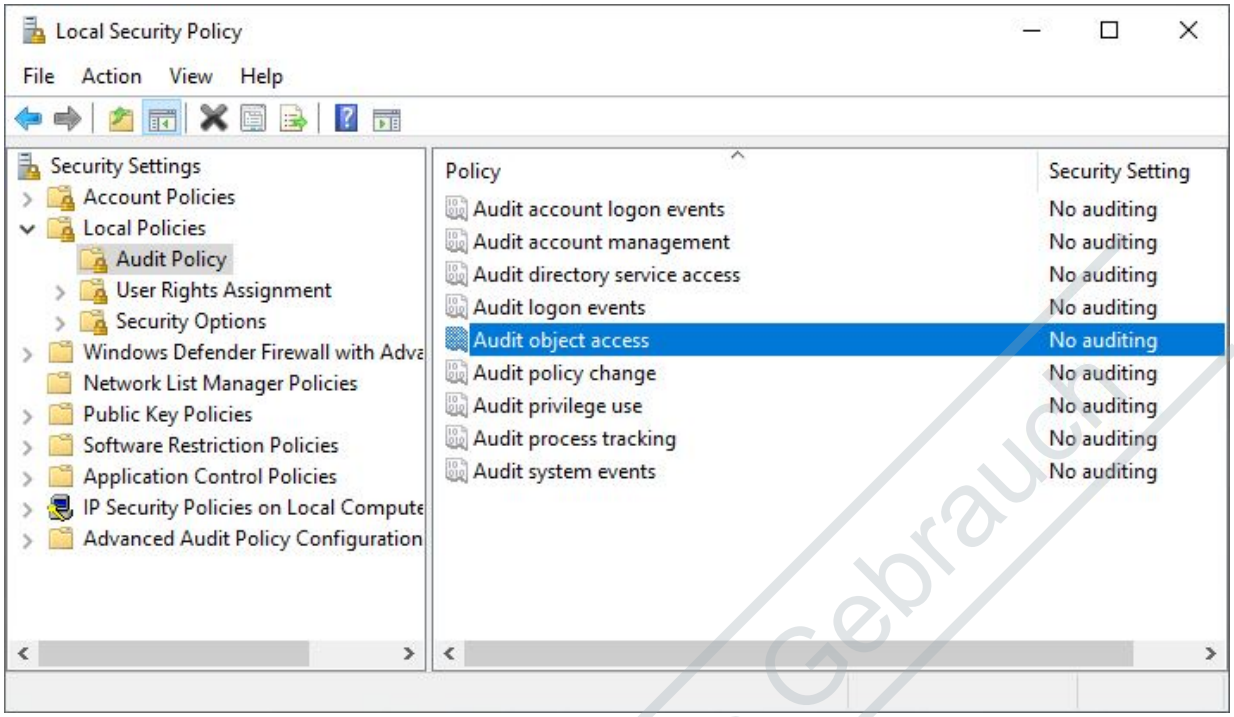
5.4.3.2 Datei- und Ordnerzugriffe überwachen

Die Größe des Windows-Protokolls wächst mit jedem Protokolleintrag an. Beachten Sie die freie Festplattenkapazität.

Datei- und Ordnerzugriffe können in Windows protokolliert werden. Jedes Mal, wenn ein Benutzer auf die ausgewählten Dateien oder Ordner zugreift, wird ein sogenanntes Überwachungsereignis in das Windows-Protokoll eingetragen.

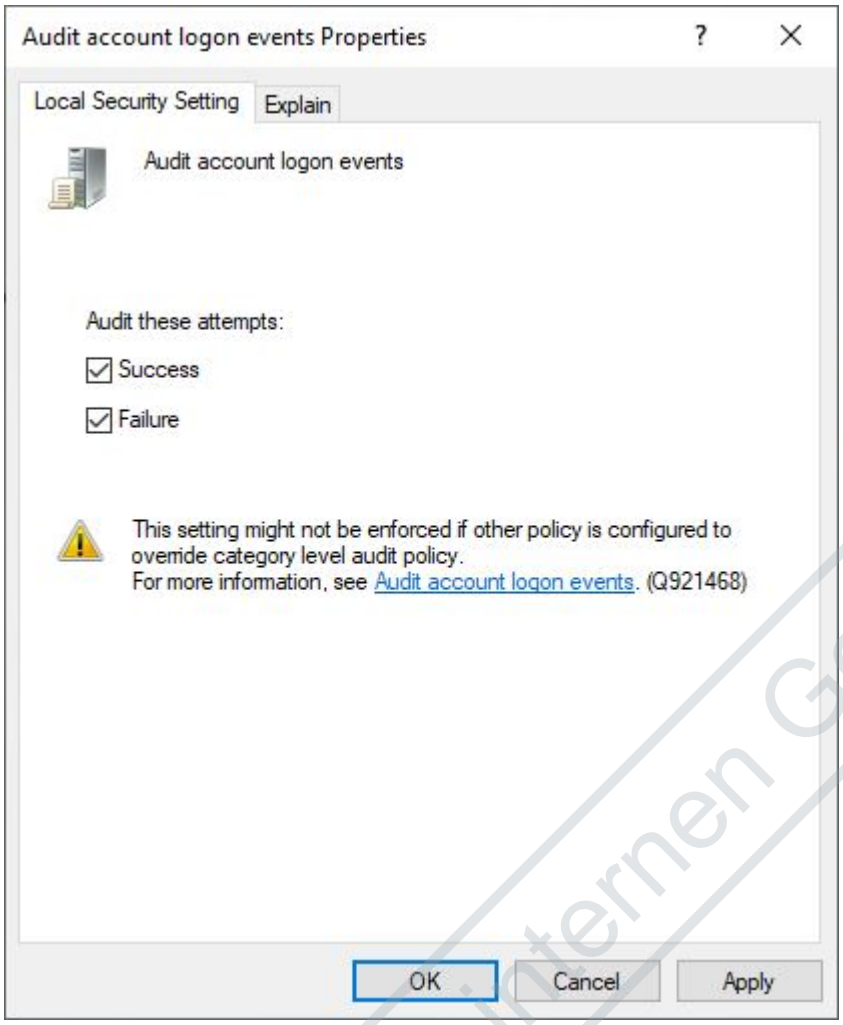
Überwachungsrichtlinie für Datei- und Ordnerzugriffe anlegen:

1. Rufen Sie den Ausführen-Dialog über die Tastenkombination **[Windows-Taste] + [R]** auf und geben Sie **secpol.msc** ein.
   Das Fenster **Local Security Policy** erscheint.



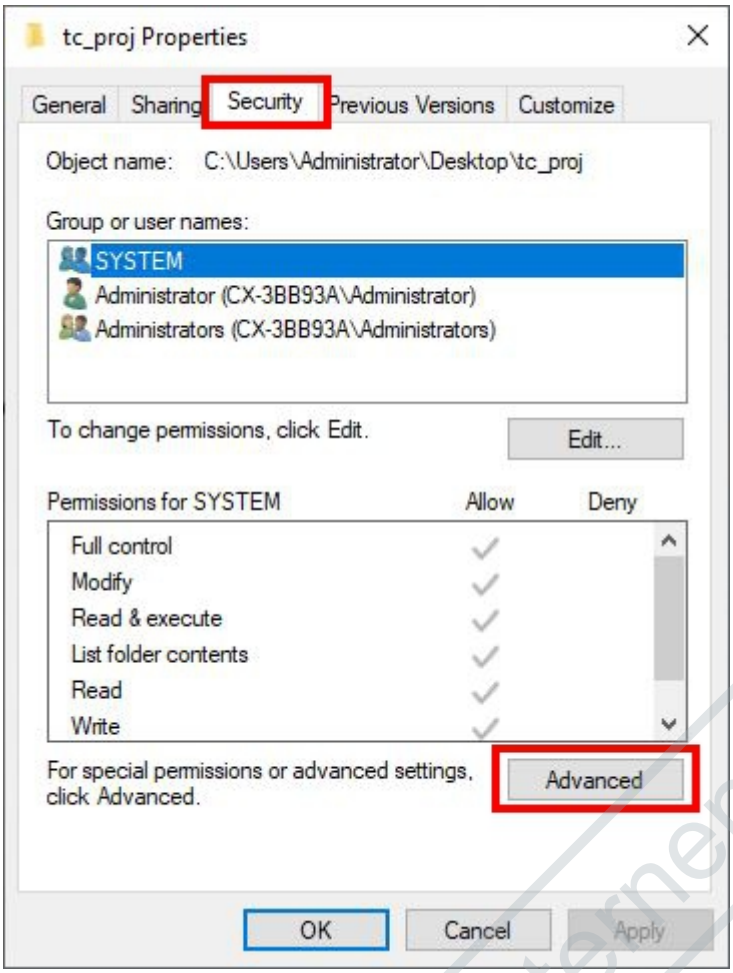
2. Klicken Sie links im Strukturbaum auf **Local Policies > Audit Policy** und wählen Sie die Überwachungsrichtlinie **Audit object access**.

3. Aktivieren Sie die Option **Failure**, wenn Sie nur erfolglose Zugriffe protokolieren möchten. Aktivieren Sie zusätzlich die Option **Success**, wenn Sie auch die erfolgreichen Zugriffe protokolieren möchten.

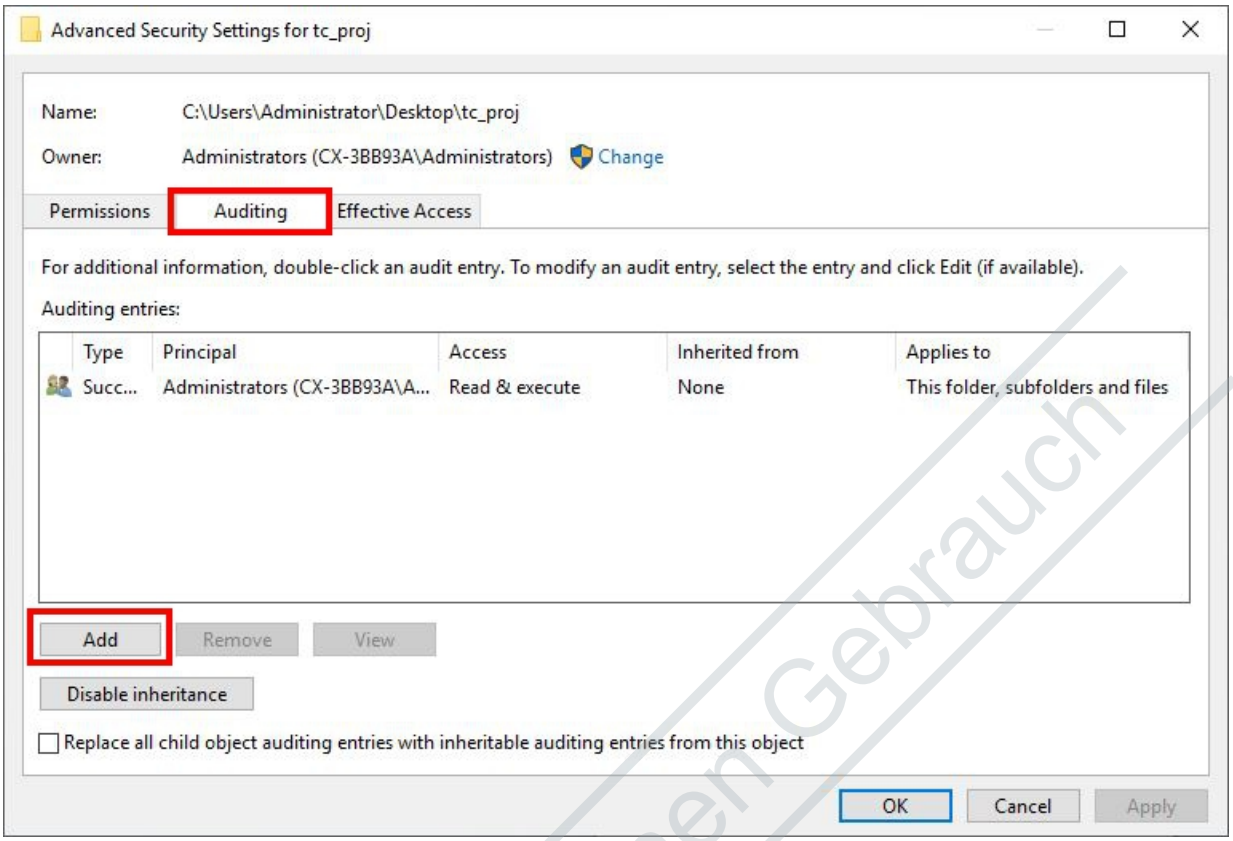


4. Klicken Sie mit der rechten Maustaste auf die entsprechende Datei oder den Ordner und anschließend auf **Properties**.

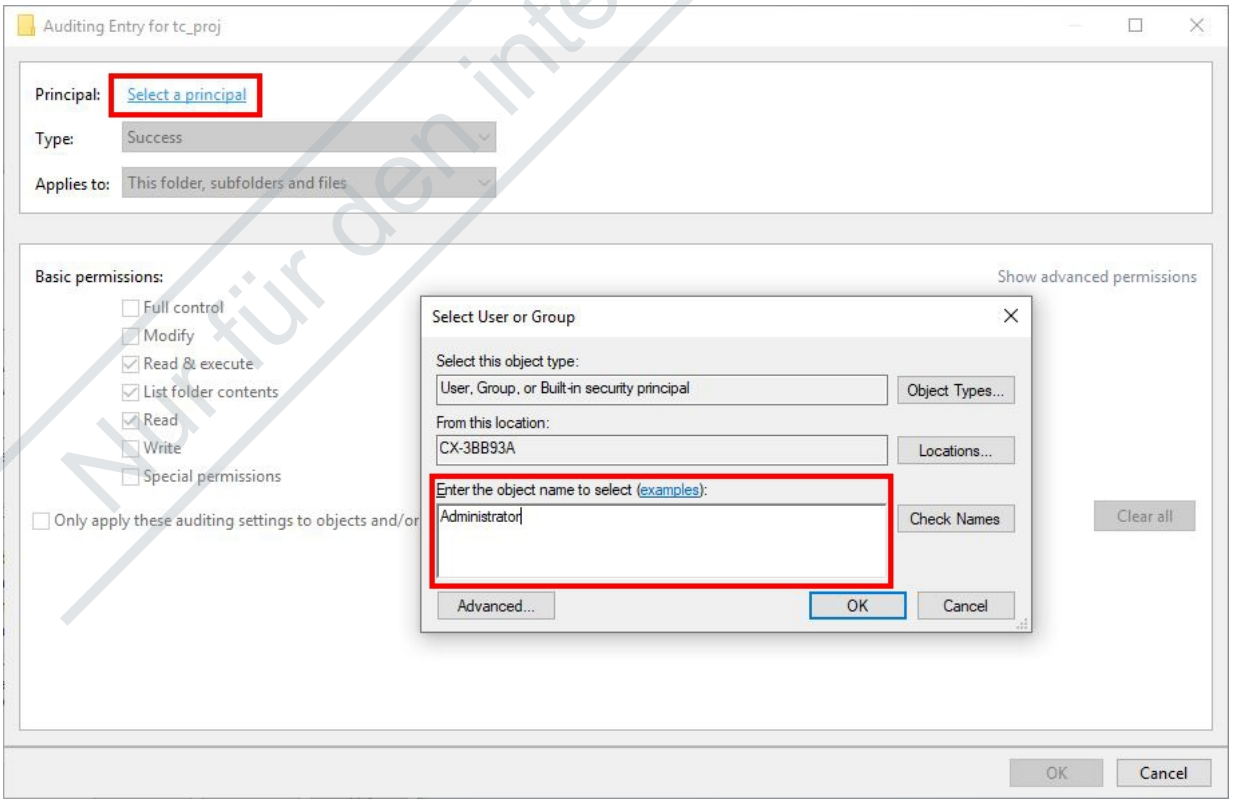
5. Klicken Sie auf die Registerkarte **Security** und anschließend auf **Advanced**.



6. Wählen Sie die Registerkarte **Auditing**, klicken Sie auf **Add**, um einen neuen Eintrag für die Überwachung anzulegen.



7. Um die Überwachung für einen Benutzer oder eine Gruppe einzurichten, geben Sie den Namen des gewünschten Benutzers oder der gewünschten Gruppe ein und wählen Sie dann **OK**.



8. Die protokolierten Einträge sind ab jetzt im **Event Viewer** einsehbar, den Sie mit **[Windows-Taste] + [R]** und dem Eintrag **eventvwr** aufrufen können. Die Einträge können anschließend unter **Windows Logs > Security** eingesehen werden.

5.5 Programme

5.5.1 Whitelisting für Programme

Das Application Whitelisting unterbindet die Ausführung aller Programme, die nicht für das System freigeben sind. Über eine Whitelist erstellt der Administrator eine Liste an genehmigten Applikationen, die das System ausführen darf. Dazu sind, anders als bei einer Antiviren-Software, keine ständigen Updates nötig, um aktuelle Sicherheitslücken zu schließen. Nur wenn neue Applikationen hinzukommen, muss die Liste erweitert werden. In der industriellen Praxis ist diese Liste häufig leichter zu warten als eine Antiviren-Software. Das Windows 10 built-in Feature heißt AppLocker.

Mit sogenannten Whitelisting-Maßnahmen kann explizit eingestellt werden, welche Programme auf dem System ausgeführt werden können. Diese Maßnahmen bieten einen Schutz vor nicht vertrauenswürdigem Code.

Windows bietet zwei verschiedene Methoden für Whitelisting:

- Richtlinien für Softwareeinschränkungen (SRP)
- AppLocker

In den „Richtlinien für Softwareeinschränkungen“ kann explizit eingestellt werden, welche Programme auf dem System ausgeführt werden können. Alle anderen Programme können dann nicht mehr ausgeführt werden. Diese Richtlinien sind über die „Lokale Sicherheitsrichtlinie“ verfügbar.

AppLocker ist in Windows ab Version 7 verfügbar und hat einen erweiterten Funktionsumfang. Unterschiede zwischen AppLocker und SRP sind hier dokumentiert.

5.5.1.1 Richtlinien für Softwareeinschränkungen (SRP)

Eine Sicherheitsstufe kann als Standard festgelegt werden. Zu den Standardstufen können Ausnahmen definiert werden.

Sicherheitsstufe	Beschreibung
Nicht erlaubt	Programme können nicht ausgeführt werden.
Standardbenutzer	Programme können mit den Berechtigungen eines Standardbenutzers ausgeführt werden.
Nicht eingeschränkt	Jeder Nutzer kann uneingeschränkt Programme ausführen.

Folgende Ausnahmeregeln können für bestimmte Programme definiert werden. Diese werden als „zusätzliche Regeln“ bezeichnet:

Typ	Beschreibung
Hashregel	Für unveränderte Programmdateien in einer bestimmten Version; der Dateiname wird ignoriert. ***Hinweis*** **Bei Updates müssen diese Hashregeln aktualisiert werden.**
Zertifikatregel	Für gültig signierte Programmdateien, deren Herausgeberzertifikat eingestellt wird.
Pfadregel	Für Programmdateien in bestimmten Pfaden. Die Pfade können auch Platzhalter und Umgebungsvariablen (wie beispielsweise %PROGRAMFILES%) enthalten.
Netzwerkzonenregel	Programme, die sich in den vom Internet Explorer definierten Netzwerkzonen befinden.

Folgende Schritte helfen Ihnen einen Kiosk Mode für Windows 10 einzurichten, in dem mehrere Anwendungen ausgeführt werden können:

https://docs.microsoft.com/en-us/windows/configuration/lock-down-windows-10-applocker

Eine allgemeine Bereitstellungsanleitung von Microsoft finden Sie hier:

https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-policies-deployment-guide

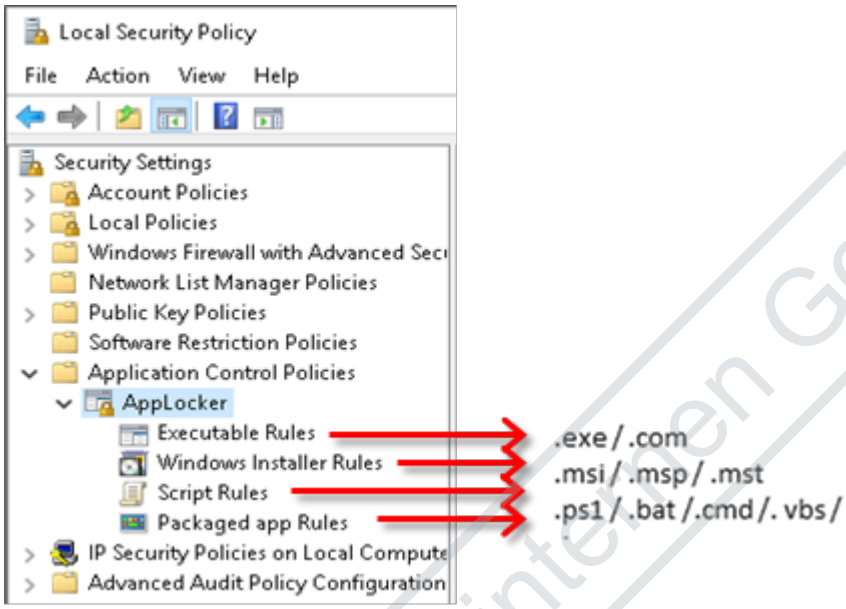
Siehe auch:

- AppLocker [▶ 34]

5.5.1.2 AppLocker

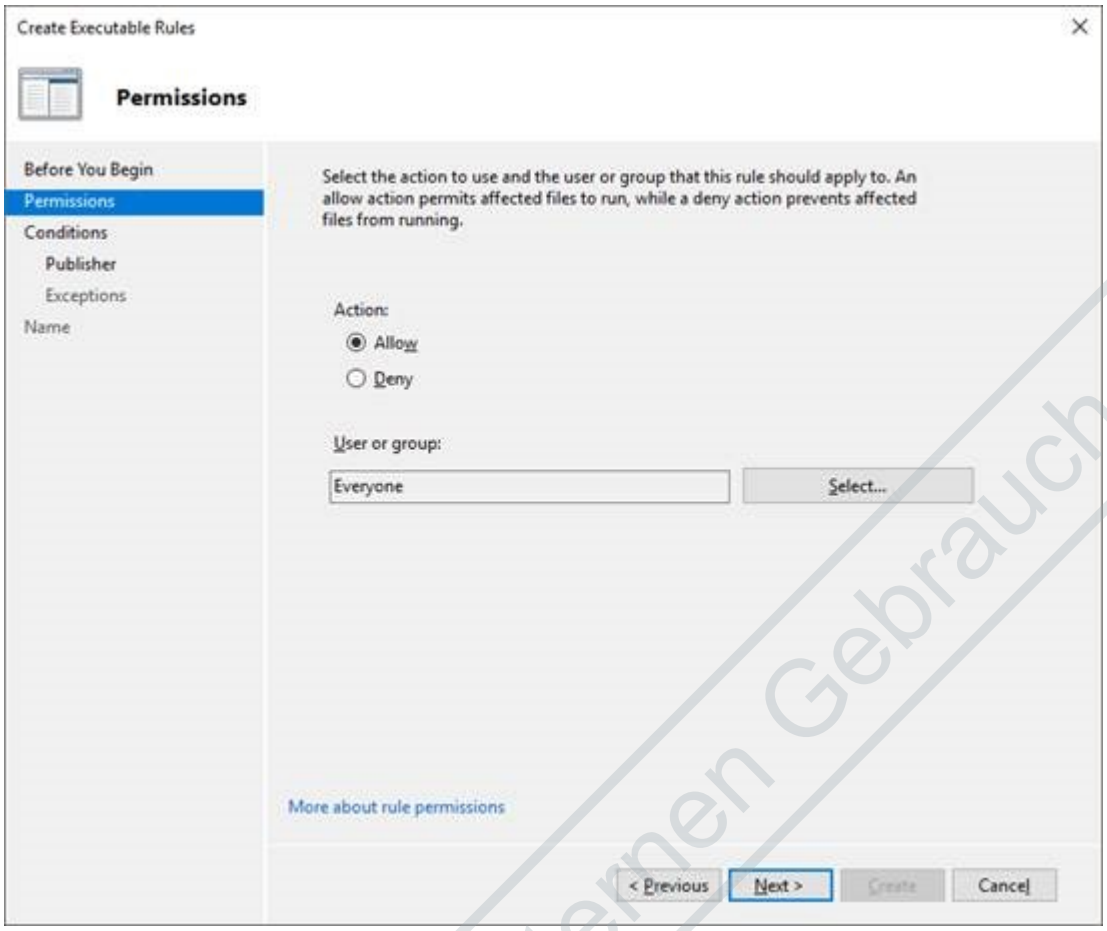
Der AppLocker bietet die Möglichkeit die Ausführung von Programmen einzuschränken.

1. Öffnen Sie die Sicherheitsrichtlinien, indem Sie **secpol.msc** ausführen. Wählen Sie **Anwendungssteuerungsrichtlinien** und darunter **AppLocker**. Durch die Regeln können verschiedene Datentypen erfasst werden:

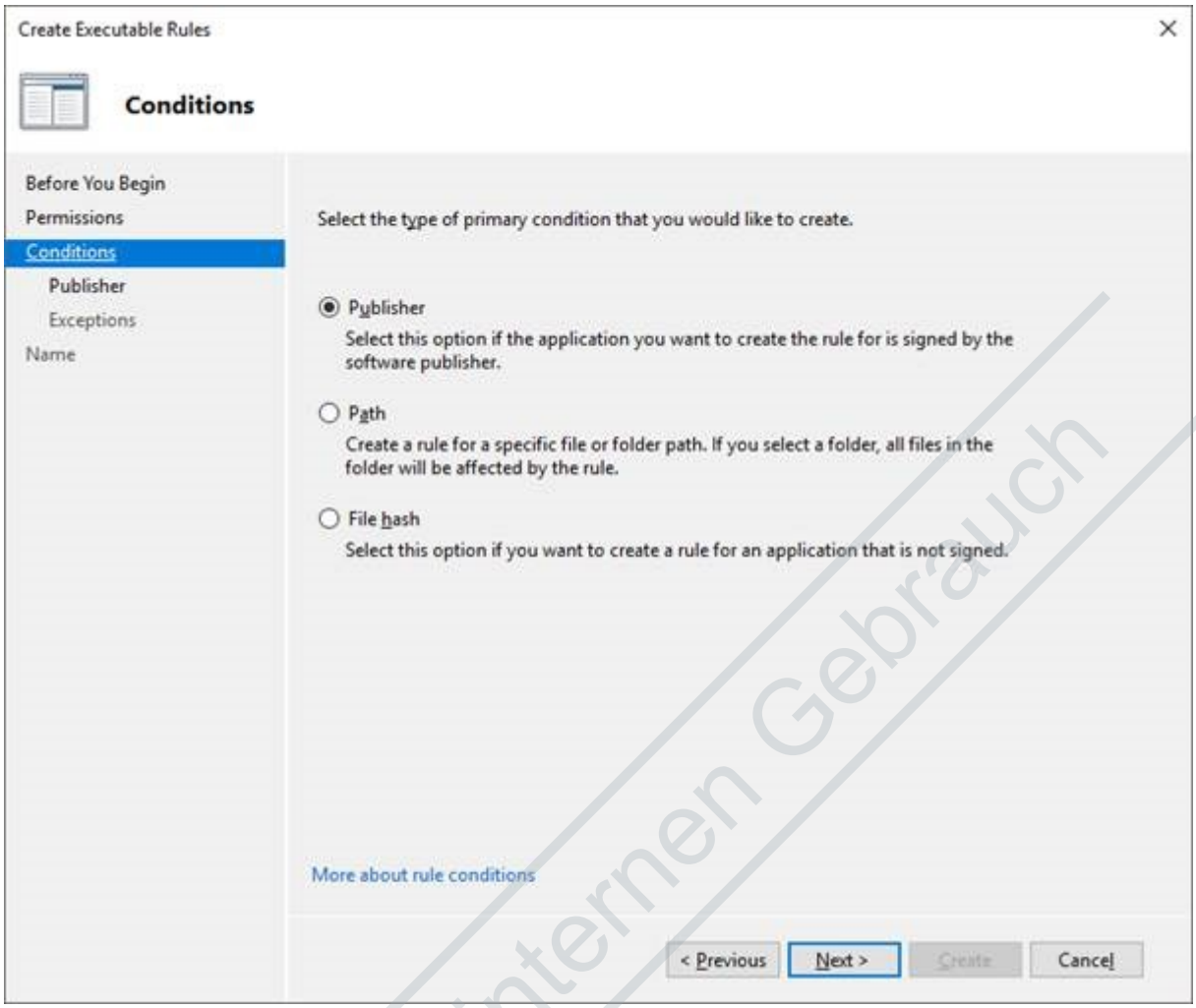


2. Über einen Rechtsklick auf eine der Regeln können Sie **Neue Regel erstellen** wählen.

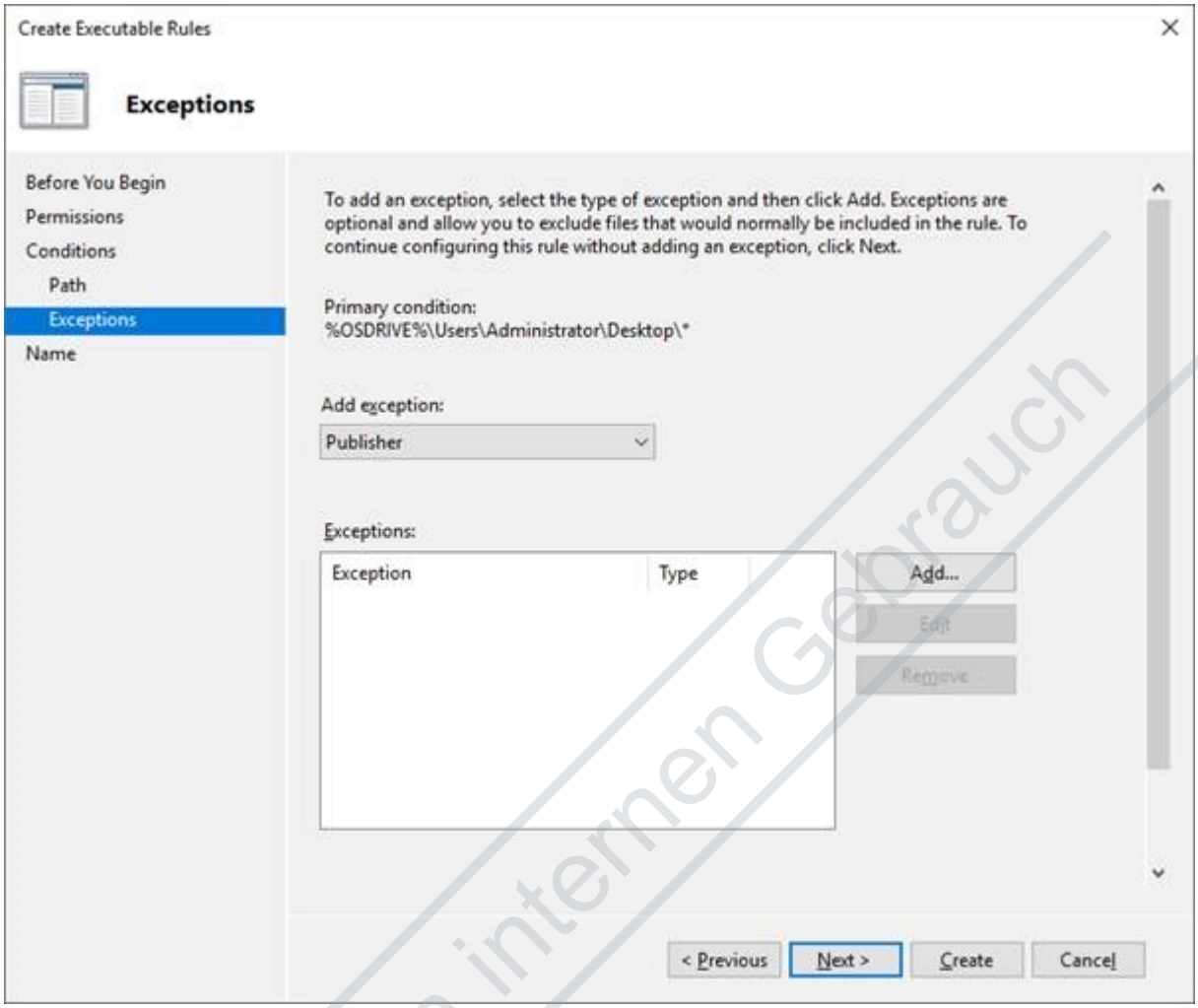
3. Wählen Sie **Zulassen** oder **Verweigern** und einen **Benutzer** oder eine **Gruppe**, für die die Regel gelten soll:



4. Wählen Sie den Typ der Primärbedingung für Ihre neue Regel aus:



5. Sie können die Regel genauer spezifizieren, indem Sie den **Herausgeber, Pfad** oder **Dateihash** angeben. Außerdem können jeweils Herausgeber, Pfade und Dateihashes von der Regel ausgeschlossen werden:



⇨ Die Konfiguration ist abgeschlossen.

Hinweise:

- AppLocker funktioniert standardmäßig als “Zulassen-Liste”.
  - AppLocker prüft zunächst, ob Regeln vorliegen, die Aktionen verweigern.
  - Regeln, die eine Aktion verweigern, werden höher priorisiert als Regeln, die eine Aktion zulassen.
- Alle Windows System-Dateien sollten erlaubt werden.
- Sogenannte “Standardregeln” (Regeln für Windows System-Dateien) können erstellt werden.
- Sie können sich über den AppLocker aus Ihrem eigenen System aussperren.

Weitere Hinweise:

- Regeln können von einer zur anderen Maschine importiert / exportiert werden.
- Unter HLKM\Software\Policies\Microsoft\Windows\SrpV2 werden die Regeln gespeichert.
- Der Anwendungsidentitäts-Service (Appidsvc) muss für die Datei-Identifikation gestartet werden.

Weitere Informationen finden Sie in der Microsoft Dokumentation:

- https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/using-software-restriction-policies-and-applocker-policies

5.5.2 Ausblenden von Programmen

Um zu verhindern, dass Benutzer Funktionalitäten nutzen, die nur für eine eingeschränkte Gruppe von Benutzern zugänglich sein sollen, können diese durch Betriebssystemfunktionen blockiert oder ausgeblendet werden.

Programme und deren Ausführung können auch über Whitelisting-Maßnahmen eingeschränkt werden.

Siehe auch:

Whitelisting für Programme [▶ 33]

Unter Windows können folgende Funktionalitäten über Änderungen in der Registry ausgeblendet werden:

Registry

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
```

Ein Eintrag mit Namen „DisableRegistryTool“ und Wert 1 verhindert, dass ein Benutzer einen Registry-Editor starten kann.

Command Prompt

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\System
```

Ein Eintrag mit Namen „DisableCMD“ hat je nach Wert eine andere Auswirkung:

- 0: Zugriff auf die Kommandozeile ist erlaubt und Batch-Dateien können ausgeführt werden.
- 1: Zugriff auf die Kommandozeile ist nicht erlaubt und Batch-Dateien dürfen nicht ausgeführt werden.
- 2: Zugriff auf die Kommandozeile ist nicht erlaubt aber Batch-Dateien können ausgeführt werden.

Network Environment

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\NonEum\
```

Ein DWORD-Eintrag mit Namen „{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}“ und Wert 1 blendet die Netzwerkumgebung aus.

Einzelne Laufwerksbuchstaben

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\
```

Mit REG_DWORD-Einträgen mit den Namen „NoViewOnDrive“ und „NoDrives“ kann konfiguriert werden, welche Laufwerksbuchstaben eingeschränkt werden sollen. „NoViewOnDrives“ schränkt den Zugriff auf Laufwerke ein. „NoDrives“ blendet die Laufwerksbuchstaben nur aus. Es kann trotzdem zugegriffen werden. Der einzutragende Wert ist jeweils die Summe der Einträge für die entsprechenden Buchstaben in der folgenden Tabelle:

A: 1	**G**: 64	**M**: 4096	**S**: 262144	**Y**: 16777216
B: 2	**H**: 128	**N**: 8192	**T**: 524288	**Z**: 33554432
C: 4	**I**: 256	**O**: 16384	**U**: 1048576	**All**: 67108863
D: 8	**J**: 512	**P**: 32768	**V**: 2097152	
E: 16	**K**: 1024	**Q**: 65536	**W**: 4194304	
F: 32	**L**: 2048	**R**: 131072	**X**: 8388608	

Um beispielsweise den Zugriff auf die Laufwerke A, B, D und P einzuschränken, muss der Wert 1 + 2 + 8 + 32768 = 32779 eingetragen werden. Nach dem Einstellen des Wertes muss das Betriebssystem neugestartet werden, damit die Einstellung wirksam wird.

Weitere Einstellungsmöglichkeiten sind hier zusammengefasst.

5.5.3 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.

Im **Control Panel** unter **Programs and Features** können nicht benötigte Programme und Windowskomponenten deinstalliert werden.

Führen Sie „control appwiz.cpl“ aus, um direkt dorthin zu gelangen.

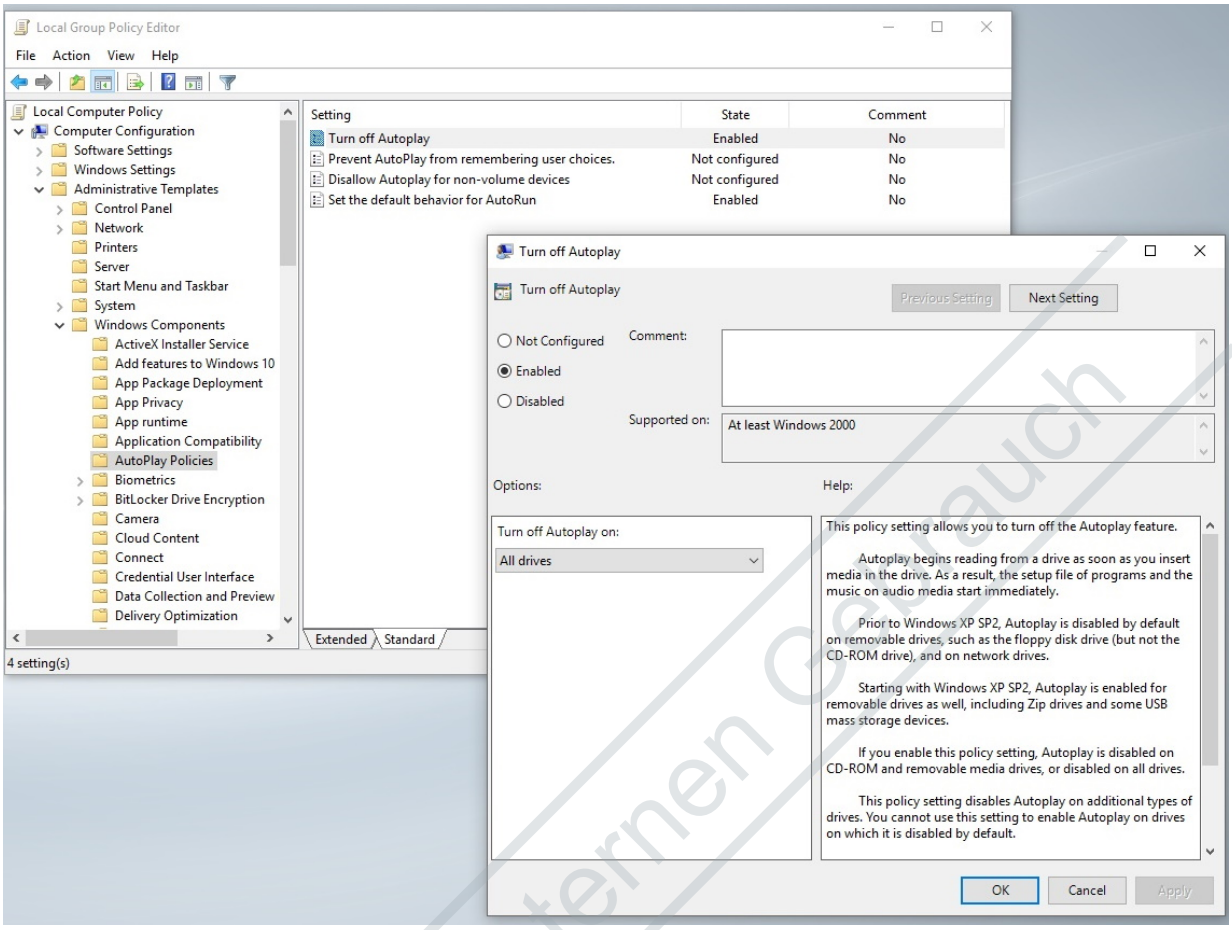
5.5.4 Autostart

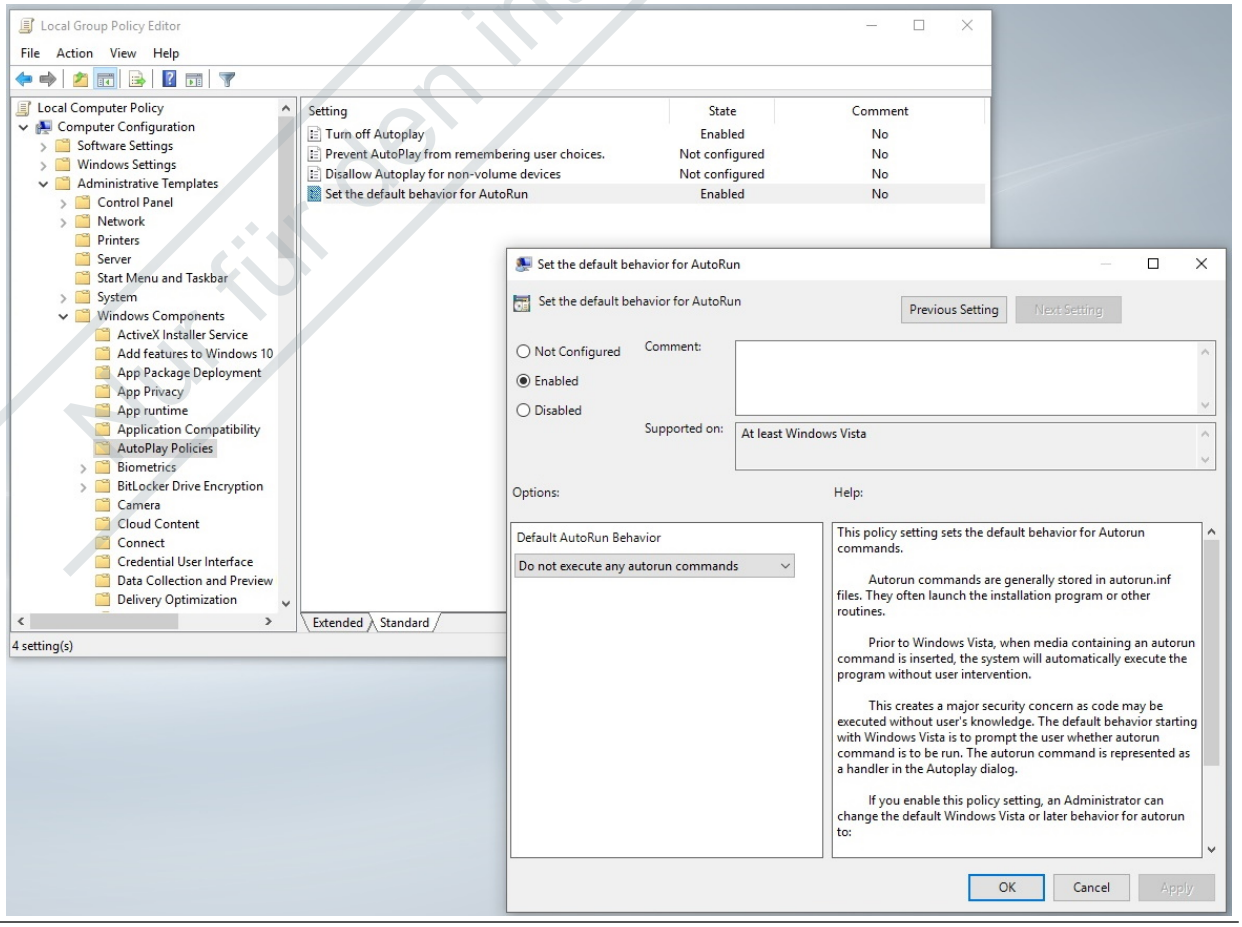
Ein Controller kann über die Mechanismen bei Anschluss externer Geräte (beispielsweise USB-Speicher oder Tastaturen) leicht infiziert werden. Dieses gilt insbesondere, wenn das Betriebssystem automatisch Aktionen ausführt, sobald ein USB Medium angesteckt wird.

Wenn diese Mechanismen nicht benötigt werden, sollten sie deaktiviert werden. Hierbei wird zwischen AutoPlay (Abspielen von Medien mit bereits installierter Software) und AutoRun (Starten von Programmen) unterschieden.

Um AutoRun und AutoPlay vollständig über die Gruppenrichtlinien auszuschalten, sollten folgende Schritte durchgeführt werden.

1. Öffnen Sie die Gruppenrichtlinien (Run „gpedit.msc“) und navigieren Sie zu Computer Configuration> Administrative Templates > Windows Components > **AutoPlay Policies**. Konfigurieren Sie dort die Richtlinien **Turn off AutoPlay** und **Set the default behavior for AutoRun** wie folgt





⇨ Nach einem Neustart sind die Einstellungen abgeschlossen.

5.5.5 Antiviren Programme

Antiviren-Software schützt ein System gegen Schadsoftware, die über Datenträger oder das Netzwerk in das System gelangt. Sie stellen ein Blacklisting von Schadsoftware dar, die bekannt ist. Antiviren-Software muss stets aktuell gehalten werden, sodass Schadsoftware erkannt werden kann. Dieses führt Nachteile mit sich.

Antiviren Programme erkennen bereits bekannte Schadsoftware („Blacklist“) und versuchen die Ausführung des Schadcodes zu verhindern.

Durch die nötigen Updates dieser Blacklists („Malware-Pattern“) erhöhen die Antiviren-Programme jedoch auch die Gefahr für ein System.

Wenn an einer Maschine immer die gleichen Programme ausgeführt werden, sollte auf das zuvor beschriebene Whitelist Verfahren zurückgegriffen werden. In jedem Fall ist abzuwägen, ob ein Blacklist-Verfahren wie bei Antiviren-Programmen insgesamt Vorteile mit sich bringt. Hierfür muss insgesamt der höheren Konfigurations-Aufwand des Whitelistings gegenüber den permanenten Updates der Antiviren-Programme gestellt werden.

Der Windows Defender hat sich in der Vergangenheit als zuverlässig und kompatibel zu TwinCAT erwiesen. Dazu muss dieser allerdings immer auf dem neusten Update-Stand sein, um auch aktuelle Sicherheitslücken zu schließen.

Insbesondere in Zusammenhang mit TwinCAT ist der Einsatz von Antiviren-Programmen genau zu evaluieren, da diese sich tief in dem Betriebssystem einrichten und somit die Echtzeitintegration von TwinCAT beeinträchtigen können.

TwinCAT hat eine eigene Beschreibung zur Kompatibilität mit Antiviren-Programmen:

Kompatibilität von Antivirenprogrammen

Weitere Informationen finden Sie in der Microsoft Dokumentation: https://support.microsoft.com/en-us/help/4013263/windows-10-stay-protected-with-windows-security

5.6 Write Filter

Windows Write Filter sind eigens von Microsoft Windows entwickelte Werkzeuge, um eine Partition vor Schreibzugriffen zu schützen. Die Schreibzugriffe werden in den RAM umgeleitet und die Partition dadurch in einem vorkonfigurierten Zustand gesichert. Nach einem Neustart wird das System automatisch in den ursprünglich definierten Zustand zurückgesetzt.

Ein Schreibschutzfilter kann je nach Anwendungsfall konfiguriert werden. So wird das System vor ungewollten Schreibzugriffen geschützt. Durch Ausnahmen („Exclusions“) wird definiert, auf welche Ordner weiterhin auch Schreibzugriffe möglich sind.

Bedeutung für IT-Security

Aus Sicht des Betreibers ist es sinnvoll, wenn die Änderungen durch Malware nach einem Neustart rückgängig gemacht werden und der Betrieb wiederaufgenommen werden kann. Jedoch können dadurch weniger Informationen über die Infektion bzw. den Angriff gesammelt werden, welcher ggf. erneut erfolgen kann.

Außerdem ist das An- und Ausschalten des Write Filters nicht gesichert. Wenn der Benutzer, in dessen Kontext der Angriff stattfindet, die Write-Filter-Einstellungen ändern kann, kann das auch ein Angreifer.

EWF

Der EWF (Enhanced Write Filter) schützt die gesamte Partition vor Schreibzugriffen ohne Ausnahmen. Wenn der EWF aktiv ist, werden alle Schreibzugriffe in den Arbeitsspeicher umgeleitet. Nach einem Neustart oder Spannungsausfall befindet sich das System wieder im ursprünglichen Zustand.

Der EWF wird mit der Software Beckhoff EWF Manger gesteuert, die bereits standardmäßig installiert ist.

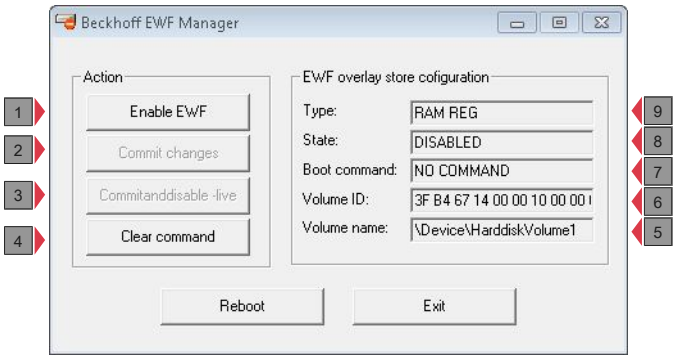


Abb. 1: Beckhoff EWF Manager, Benutzeroberfläche.

Tab. 1: Legende zum Beckhoff EWF Manager.

Nr.	Beschreibung
1	EWF einschalten, EWF ausschalten.
2	Daten können zur Laufzeit übernommen werden, wenn der EWF aktiv ist.
3	EWF ohne Neustart ausschalten.
4	Boot command zurücksetzen auf NO COMMAND.
5	Name der Partition.
6	ID der Partition, auf der der EWF ausgeführt wird (in Hexadezimal).
7	Zeigt an, welche Kommandos nach dem Neustart ausgeführt werden. Es gibt folgende Kommandos: • NO COMMAND, keine Änderungen. • ENABLE, der EWF wird nach dem Neustart eingeschaltet. • DISABLE, der EWF wird nach dem Neustart ausgeschaltet. • COMMIT, Daten werden beim Herunterfahren auf das Speichermedium geschrieben, obwohl der EWF eingeschaltet ist.
8	Zeigt den aktuellen Status an, ob der EWF eingeschaltet oder ausgeschaltet ist.
9	Zeigt den EWF Modus an. Im RAM REG Modus werden alle Zugriffe in den Arbeitsspeicher umgeleitet und die EWF Einstellungen in der Registry gespeichert.

Voraussetzungen:

- Windows Embedded Standard 2009 oder
- Windows Embedded Standard 7 P

Aktivieren Sie den EWF wie folgt:

1. Starten Sie den Industrie- oder Embedded-PC und klicken Sie unter **Start < All Programs < Beckhoff EWF Manager** auf **Beckhoff EWF Manager**.
2. Klicken Sie unter **Action** auf die Schaltfläche **Enable EWF**.
3. Bestätigen Sie die Einstellungen, damit die Änderungen wirksam werden.

⇨ Die Änderungen sind erst nach einem Neustart aktiv. Sie haben den EWF erfolgreich aktiviert.

FBWF

Im Gegensatz zum EWF arbeitet der FBWF auf Dateiebene. Dadurch ist es möglich Ausnahmen zu definieren und Schreibzugriffe auf einzelne Dateien oder Ordner zu erlauben. Alle anderen Schreibzugriffe werden in den Arbeitsspeicher umgeleitet. Nach einem Neustart befindet sich das System wieder im ursprünglichen Zustand.

Sobald der FBWF aktiviert wird, werden einige Ordner automatisch für den direkten Schreibzugriff freigegeben. So steht beispielsweise der Ordner *C:\Data* zum Schreiben von permanenten Daten zur Verfügung. Durch die Freigabe des Ordners *C:\TwinCAT\Boot* kann ein neues TwinCAT-Boot-Projekt auf den Rechner geladen werden, ohne dass der FBWF vorher deaktiviert werden muss

EWF vs. FBWF

> **EWF und FBWF nicht gleichzeitig betreiben**
>
> Wenn beide Write Filter aktiviert sind, werden die Ausnahmen des FBWF durch den EWF abgefangen und gehen nach einem Neustart des Rechners verloren.
>
> Aktivieren Sie die beiden Write Filter EWF und FBWF nicht zur selben Zeit.

In den meisten Fällen ist der FBWF die bessere Wahl, da er einfacher zu bedienen ist und direkte Schreibzugriffe erlaubt. Jedoch gibt es Szenarien in denen der EWF unverzichtbar ist, z.B. wird HORM (Hibernate Once/Resume Many) vom FBWF nicht unterstützt. Außerdem ist beim FBWF die Verwendung von komprimierten NTFS-Volumen nicht möglich.

Steuerung mit dem Beckhoff FBWF Manager

Der FBWF wird mit der Software Beckhoff FBWF Manger gesteuert, die standardmäßig installiert ist.

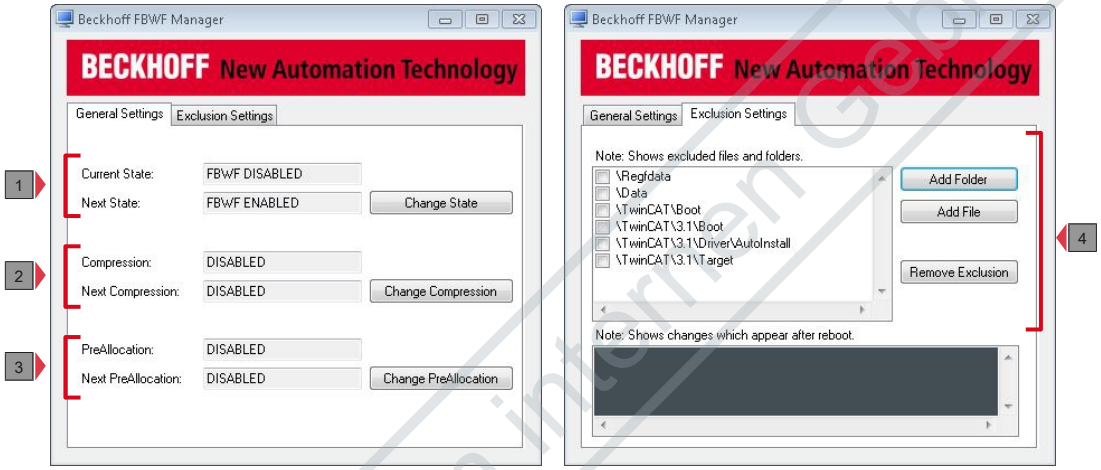


Abb. 2: Beckhoff FBWF Manager, Benutzeroberfläche.

Tab. 2: Legende zum Beckhoff FBWF Manager.

Nr.	Beschreibung
1	Über die Schaltfläche **Change State** wird der FBWF ein- oder ausgeschaltet. Der aktuelle und nächste Status wird angezeigt. Änderungen werden immer erst nach einem Neustart übernommen.
2	Die Komprimierung kann erst eingeschaltet werden, wenn der FBWF aktiv ist. Zeigt ob die Komprimierung des FBWF Overlays aktiv ist.
3	PreAllocation kann erst eingeschaltet werden, wenn der FBWF aktiv ist. Zeigt ob die PreAllocation aktiviert ist.
4	Unter der Registerkarte **Exclusion Settings** werden Ausnahmen erstellt. Bei einem aktivierten FBWF werden standardmäßig Ordner in die Ausnameliste hinzugefügt.

Voraussetzungen:

- Windows Embedded Standard 2009 oder
- Windows Embedded Standard 7 P

Aktivieren Sie den FBWF wie folgt:

1. Starten Sie den Industrie- oder Embedded-PC und klicken Sie unter **Start < All Programs < Beckhoff FBWF Manager** auf **Beckhoff FBWF Manager**.
2. Klicken Sie unter der Registerkarte **General Settings** auf die Schaltfläche **Change Settings**.
3. Die Anzeige bei **Next State** ändert sich und die Meldung FBWF ENABLED erscheint.

4. Starten Sie den Industrie- oder Embedded-PC neu.

⇨ Die Änderungen sind erst nach einem Neustart aktiv. Die Anzeige bei **Current State** wechselt nach dem Neustart auf FBWF ENABLED. Sie haben den FBWF erfolgreich aktiviert.

5.7 Keyboard Filter

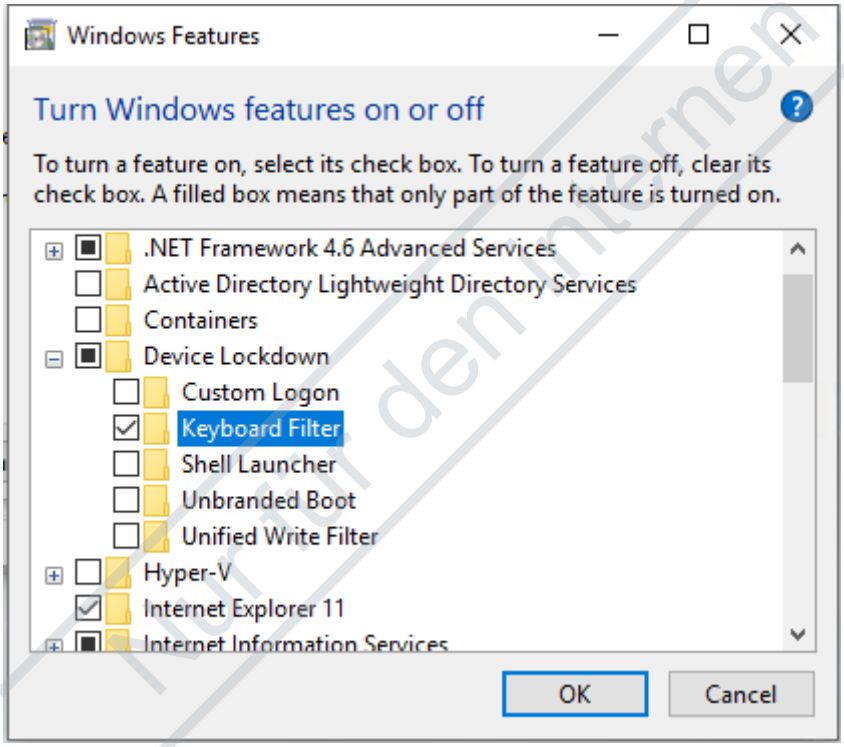
Der Keyboard Filter ist eine Möglichkeit, das System gegen ungewollte Eingriffe zu schützen. So kann z. B. eine Tastenkombination, die zum Schließen einer Applikation führt, gesperrt werden. Nur Tastatureingaben, die für die Bedienung der Anwendung benötigt werden, sind freigegeben. Außerdem können Tastenkombinationen angegeben werden, die den Keyboard Filter deaktivieren. Auch hilfreich ist die Option, die den Filter für den Administrator deaktiviert.

Keyboard Filter bieten eine weitere Möglichkeit einen Benutzer in dem Umgang mit dem Betriebssystem einzuschränken und somit Angriffsmöglichkeiten zu minimieren.

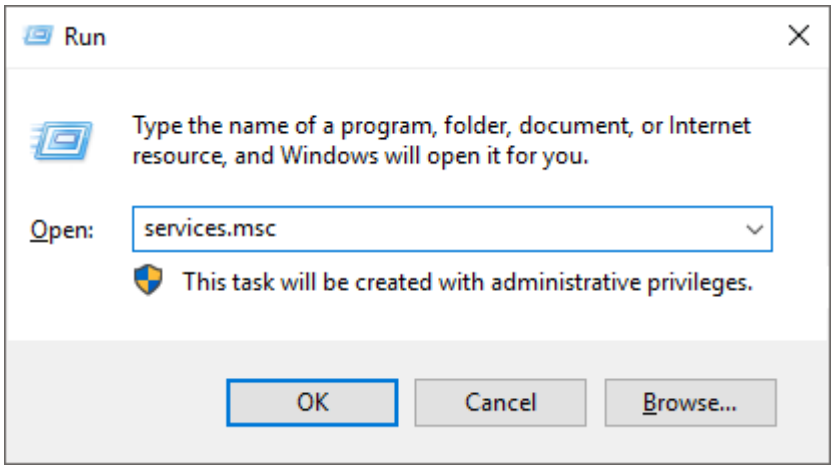
Typischerweise wird ein „Kiosk-Mode“ konfiguriert indem beispielsweise ein erfolgreich eingeloggter Nutzer nur noch eine HMI Anwendung starten kann. Der Benutzer hat keine Möglichkeit mehr, andere Programme zu starten oder auch Befehle an den IPC zu senden, wie beispielsweise das Herunterfahren.

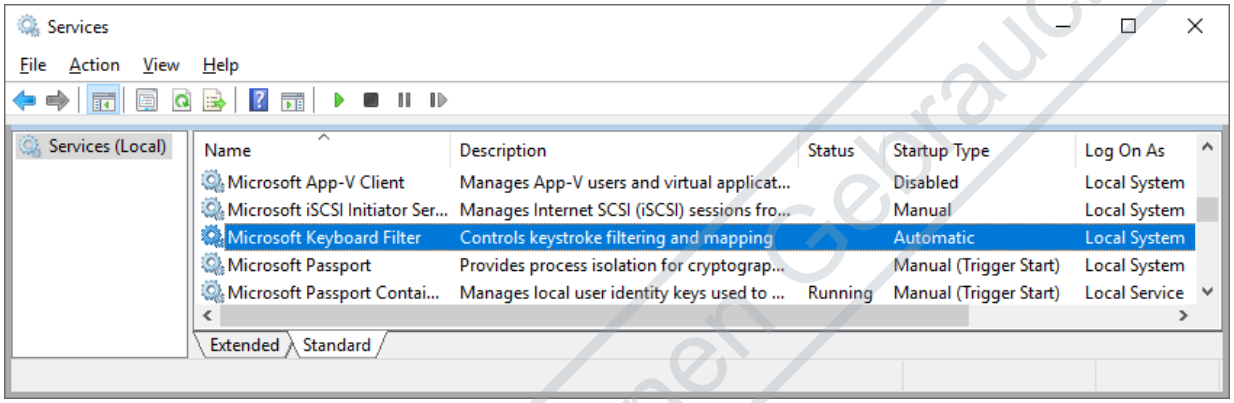
Windows 10 stellt einen Dienst für diesen Zweck bereit. Hier wird beschrieben, wie dieser aktiviert wird und konfiguriert werden kann.

Schalten Sie zunächst das Windows 10 built-in Feature ein, um den Dienst zu nutzen. Öffnen Sie dazu den Dialog **Turn Windows features on or off** und wählen Sie unter dem Menüpunkt **Device Lockdown** das Feature **Keyboard Filter** aus. Starten Sie den PC anschließend neu.

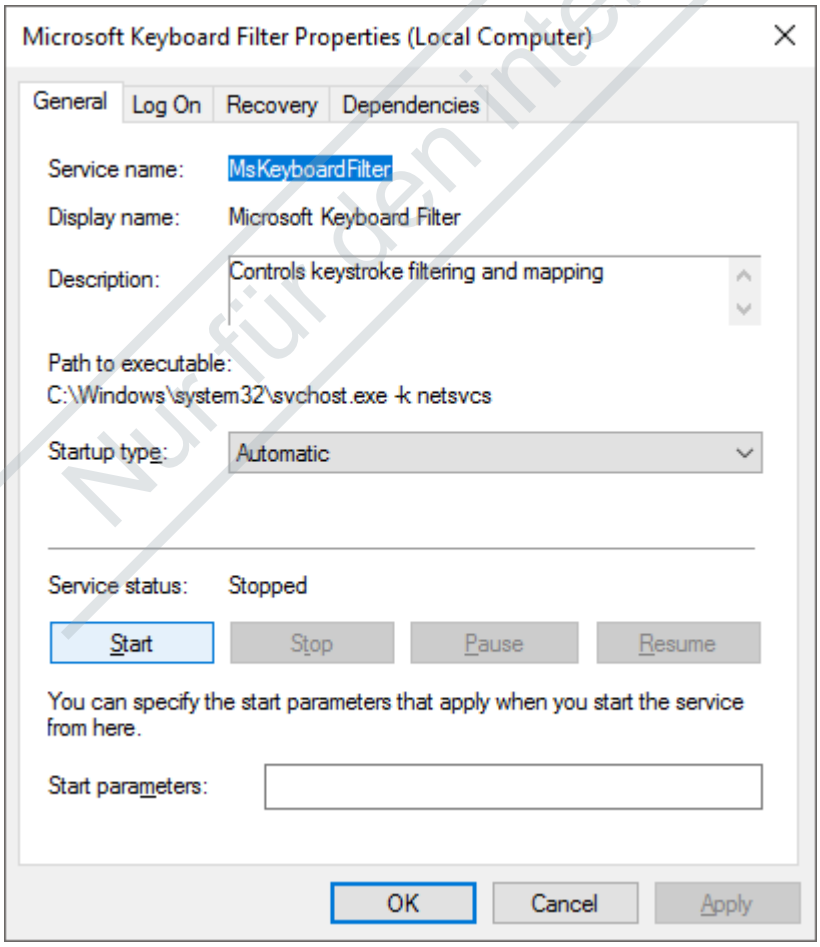


1. Starten Sie den **Microsoft Keyboard Filter**-Service.

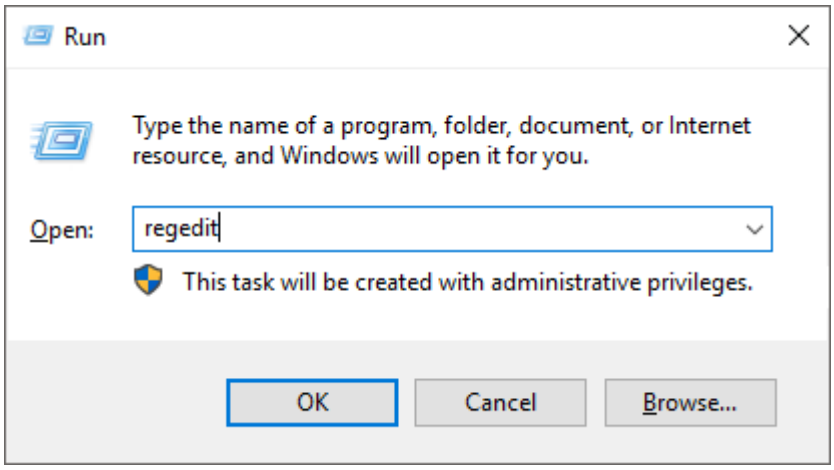




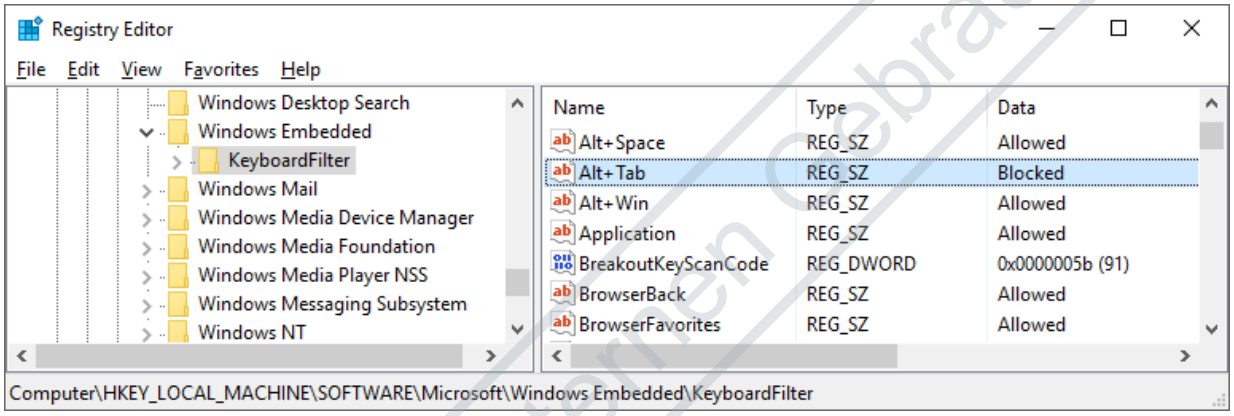
2. Setzen Sie den Startup Type auf **automatisch**:



3. Öffnen Sie den **Registry Editor**



4. Navigieren Sie zum **KeyboardFilter**: **HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows Embedded**



5. Sowohl Werte, wie auch geläufige Tastenkombinationen sind in den Tabellen unten aufgeführt.

⇨ Der Keyboard Filter ist aktiviert.

Folgende Werte stehen für die einzelnen Tasten-Kombinationen bereit:

Value	Description
„Allowed“	Tastenkombination erlauben
„Blocked“	Tastenkombinationen blockieren
DisableKeyboardFilterForAdministrator to „1“	Keyboard Filter ist für Administratoren deaktiviert
BreakoutKeyScanCode to „01“	Scancode für ESC als Breakout

Folgende Tastenkombinationen werden üblicherweise gesperrt:

Value	Description
CTRL-SHIFT-ESC	Taskmanager öffnen
CTRL-ALT-DEL	Menü mit folgenden Optionen öffnen: Lock system Open task manager Change password Shutdown system Switch user

Bitte entnehmen Sie weitere Informationen der Microsoft Dokumentation: https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/keyboardfilter

5.8 USB-Filter

Ähnlich wie bei einem Whitelisting für Applikationen können auch USB-Geräte als vertrauensvoll gelistet werden. USB-Geräte, die nicht auf der freigegebenen Liste stehen, werden vom Betriebssystem nicht akzeptiert. So können einheitliche Service-USB-Sticks für die Wartung der Geräte definiert werden, die nur freigegebene Anwendungen enthalten und regelmäßig überprüft werden. Nicht anwendungsspezifische (z. B. private) USB-Sticks können so keinen Schaden anrichten. Der USB-Filter dient dabei allen Geräten, die über USB angeschlossen werden. Dazu zählen z. B. auch HID Geräte wie Maus/Tastatur, alle Speichermedien wie USB-Sticks, Festplatten und Card-Reader.

Die USB-Filter in einem Betriebssystem beziehen sich jedoch auf Hersteller- und Produkt-ID (Vendor ID [VID] / Product ID [PID]) im USB, die keine kryptographische Absicherung haben und gefälscht werden können.

Um externe Schnittstellen wie USB zu blockieren, können diese physikalisch, z. B. durch einen Schaltschrank gesichert werden. Aber auch wenn das Gerät in einem Schaltschrank verbaut ist, gibt es Situationen, in denen ein USB-Port ausgeführt wurde bzw. werden muss. Um die dadurch vorhandene Angriffsfläche zu verkleinern, sollte die Nutzung der Schnittstelle im Betriebssystem eingestellt und beschränkt werden.

Die bei den USB Filtern verwendeten IDs sind allerdings nicht kryptographisch gesichert, sodass bösartige Angriffe mit präparierten USB Geräten die USB Filter umgehen können.

Es gibt verschiedene Wege, um USB-Device auf Betriebssystemebene einzuschränken:

- Wenn das Gerät noch nicht installiert wurde, kann die Installation verhindert werden, indem dem aktuellen Benutzer und dem Benutzer SYSTEM der Zugriff auf die folgenden Dateien entzogen wird:
  - %SystemRoot%\Inf\Usbstor.pnf
  - %SystemRoot%\Inf\Usbstor.inf
  - %SystemRoot%\System32\DriverStore\Usbstor.inf*
- Um die generelle Verwendung von USB-Massenspeichergeräten zu unterbinden, kann in der Registry unter `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSer\services\USBSTOR` der Eintrag „ImagePath“ auf einen ungültigen Pfad gesetzt werden.
- Wie die Nutzung von USB-Geräten granularer über Policy-Einstellungen (Group Policy) eingeschränkt werden kann, wird hier beschrieben.
- USB-Schnittstellen können auch im BIOS abgeschaltet werden. Beachten Sie dabei, dass über die abgeschalteten Schnittstellen auch Eingabegeräte, wie Tastatur und Maus, nicht mehr funktionieren.

Zu beachten ist, dass über die Registry eingestellte Werte NICHT automatisch mit denen in der Gruppenrichtlinie, eingestellten Werte synchronisiert werden. Es wird empfohlen, die Einstellungen ausschließlich über die Gruppenrichtlinie durchzuführen.

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 [▶ 52].

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 [▶ 51]
- RDP [▶ 51]

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.

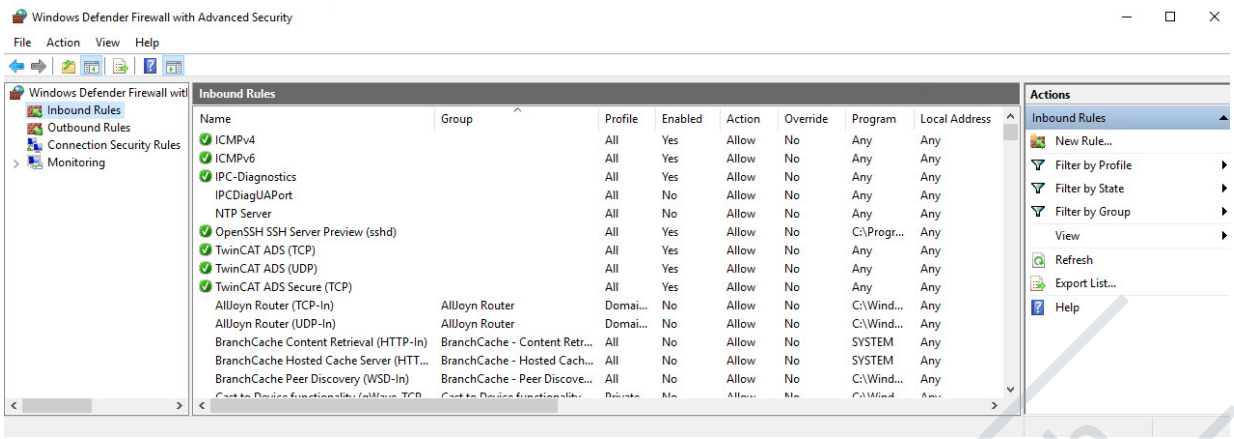
Restriktive, explizite Einstellungen für die Kommunikation über eine Firewall sind eine wichtige Maßnahme, um Netzwerkzugriffe nur im notwendigen Umfang zuzulassen.

Unter Wichtige TCP/UDP-Ports [▶ 52] befindet sich eine Liste von TCP/UDP-Ports, die typischerweise berücksichtigt werden müssen, um eine Firewall zu konfigurieren.

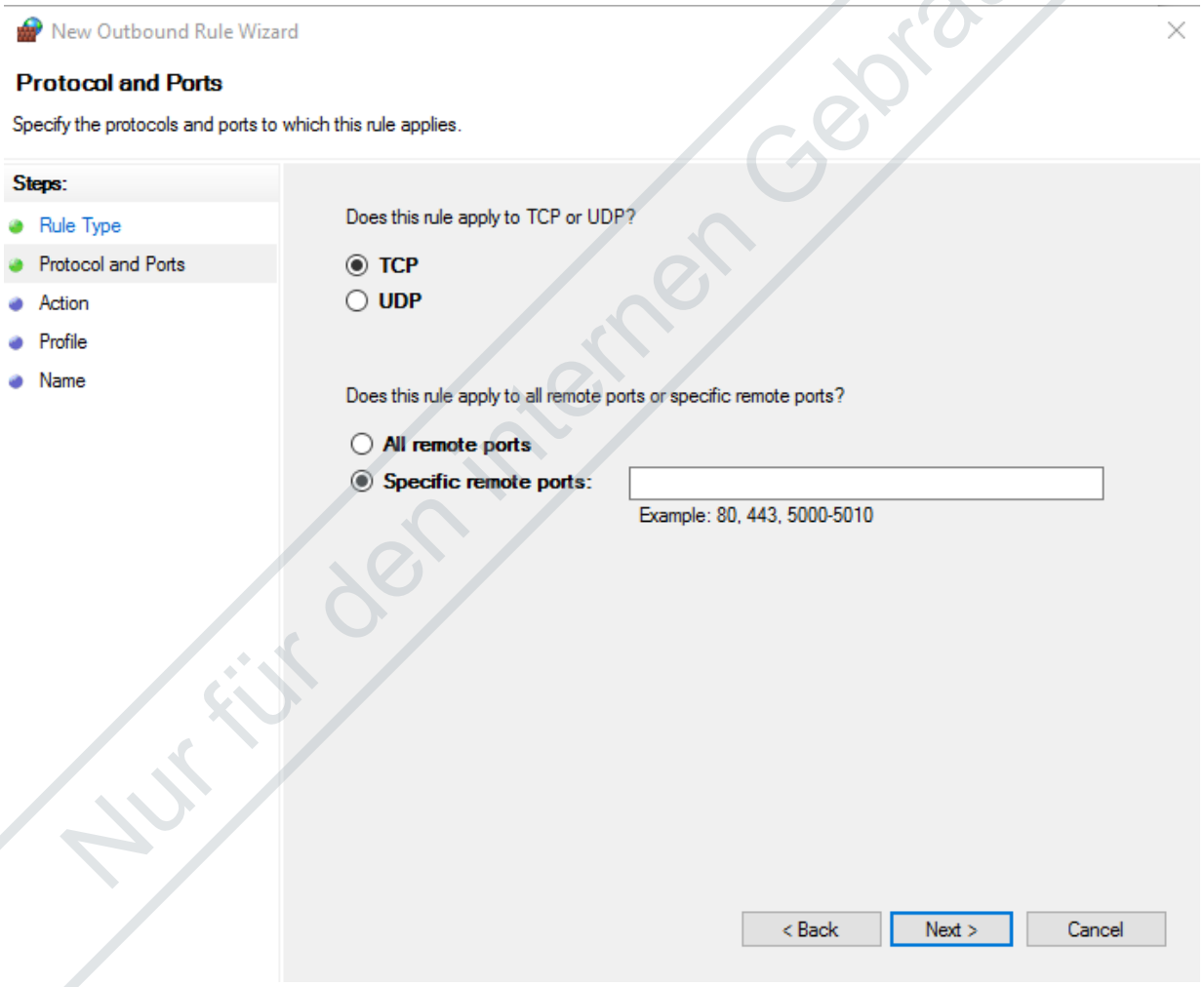
Zur Konfiguration der Firewall kann das MMC snap-in **Windows Firewall with Advanced Security** mit dem Kommandozeilenbefehl **wf.msc** geöffnet werden. Über die Schaltfläche **New Rule** können Regeln hinzugefügt werden.

Ausgewählte Regeln zum Öffnen von Ports oder Diensten können wieder geschlossen werden. Mit einem Rechtsklick auf die Regel kann mit **Disable Rule** eine Regel deaktiviert oder mit **Delete** eine Regel gelöscht werden.

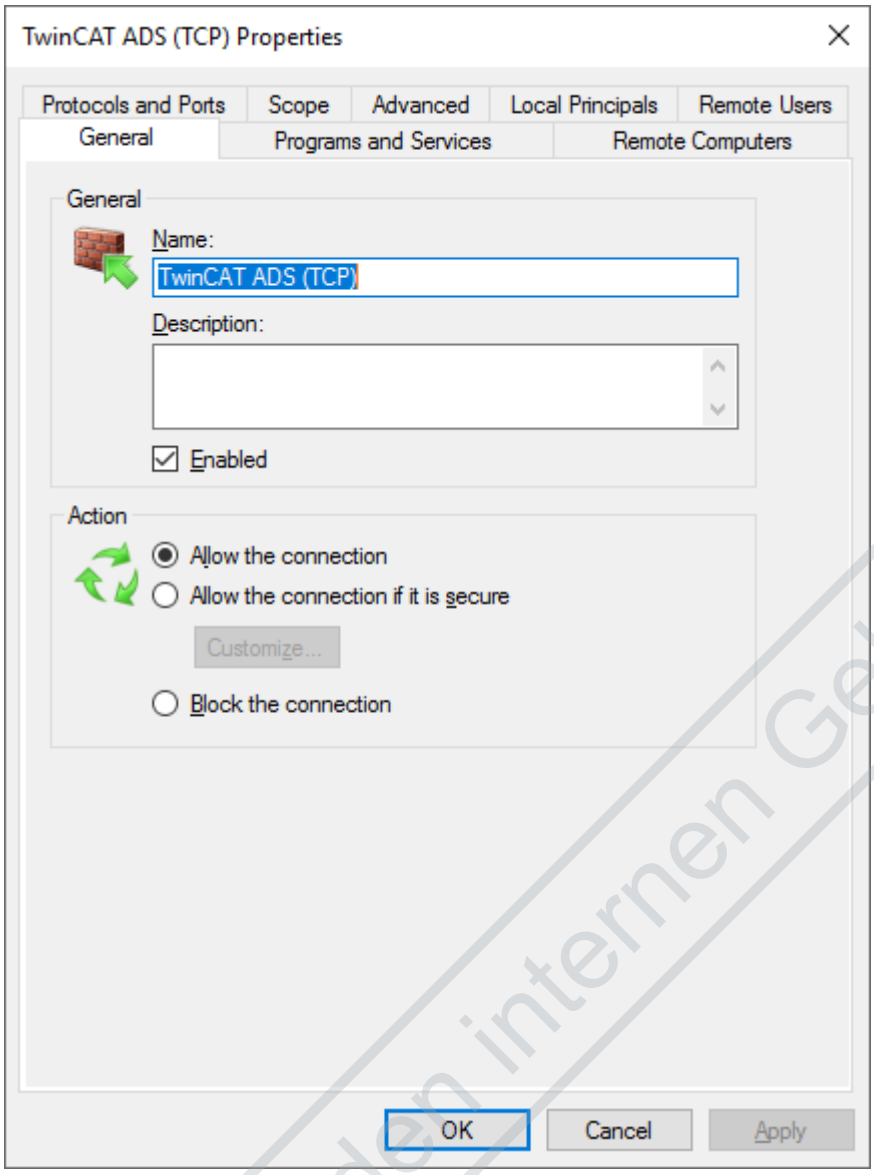
1. Öffnen Sie die Firewall Einstellungen



2. Über einen Doppelklick auf die Regel ändern Sie eine bestehende Regel, also Verbindungen erlauben oder blockieren. Über **New Rule** legen Sie eine neue Regel an.
   Es startet dabei ein Wizard, der durch die Optionen führt:



3. Die Optionen dieser Regeln können nachher auch geändert werden:



⇨ Sie haben eine neue Regel für die Firewall angelegt.

Weitere Informationen finden Sie in der Microsoft Dokumentation:

https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-integration-and-best-practices

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.

6.3.5 RDP

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

6.3.6 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).

6.4 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) Siehe auch: Dokumentation zu TF6120
TF6250 Modbus TCP	502 / tcp (eingehend), änderbar Siehe auch: Dokumentation zu TF6250
TF6310 TCP-IP	änderbar / tcp (eingehend, ausgehend)

Dienst	Port (Standardeinstellung)
	Siehe auch: Dokumentation zu TF6310
TF6311 TCP/UDP Realtime	änderbar / tcp (eingehend, ausgehend) Die Kommunikation ist nicht durch eine Betriebssystem-Firewall beeinflussbar. Siehe auch: Dokumentation zu TF6311
TF6300 FTP	20 / tcp (ausgehend) 21 / tcp (ausgehend) Siehe auch: Dokumentation zu TF6300
TF6420 Database Server	änderbar je nach Datenbank / tcp (ausgehend) Siehe auch: Dokumentation von TF6420
TF67xx IoT TF35xx Analytics	änderbar je nach Broker / tcp (ausgehend) Siehe auch: Dokumentationen der TF670x sowie TF35xx
TwinCAT EAP	34980 / udp (eingehend), falls EAP über UDP verwendet wird. Die Kommunikation ist nicht durch eine Betriebssystem-Firewall beeinflussbar. Siehe auch: Dokumentation von EAP
TwinCAT ADS-over-MQTT	änderbar je nach Broker / tcp (ausgehend) Siehe auch: Dokumentation zu ADS-over-MQTT

6.6 IIS-Webserver

Der IIS-Webserver ist unter Windows standardmäßig aktiv und wird beispielsweise für den Beckhoff Device Manager und für die PLC HMI verwendet. Um das System weiter abzuriegeln und Zugriffe über den Webserver einzuschränken, kann:

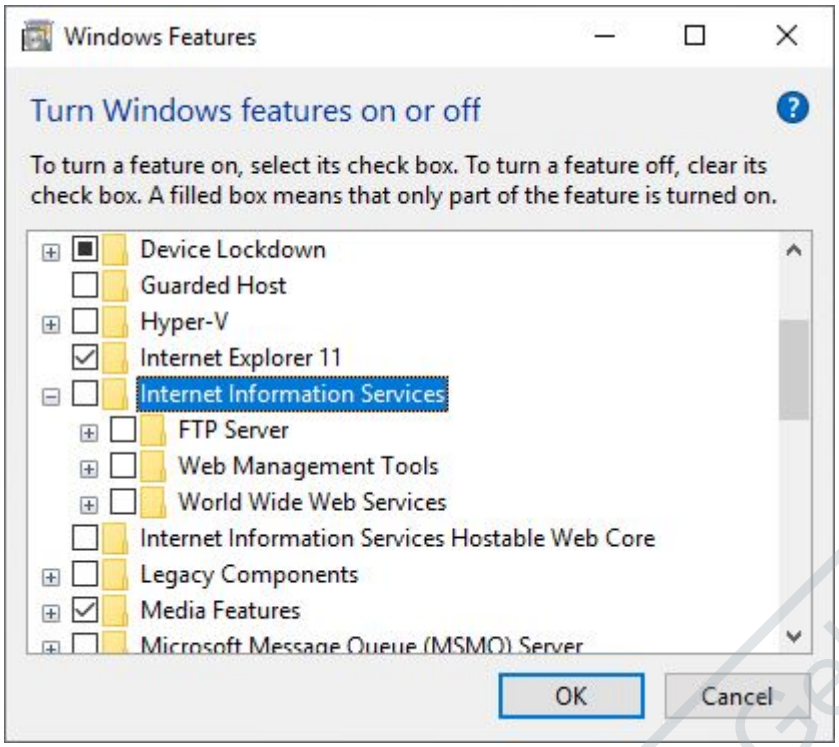
- der IIS-Webserver deaktiviert
- oder der Zugriff von außen eingeschränkt werden.

Die Entscheidung, welche der beiden Optionen die richtige für Sie ist, hängt von ihren Einsatzbedingungen ab. Beachten Sie, dass bei einer kompletten Deaktivierung alle Applikationen betroffen sind und nicht mehr funktionieren, die auf den IIS-Webserver zurückgreifen. Bei einem eingeschränkten Zugriff ist lediglich der Beckhoff Device Manager nicht mehr erreichbar. Der lokale Zugriff auf den Beckhoff Device Manager kann weiterhin genutzt werden und alle anderen Applikationen sind nicht von einer Deaktivierung betroffen.

IIS-Webserver deaktivieren:

1. Rufen Sie den Ausführen-Dialog über die Tastenkombination **[Windows-Taste] + [R]** auf und geben Sie **optionalfeatures** ein.
   Das Fenster Windows Features erscheint.

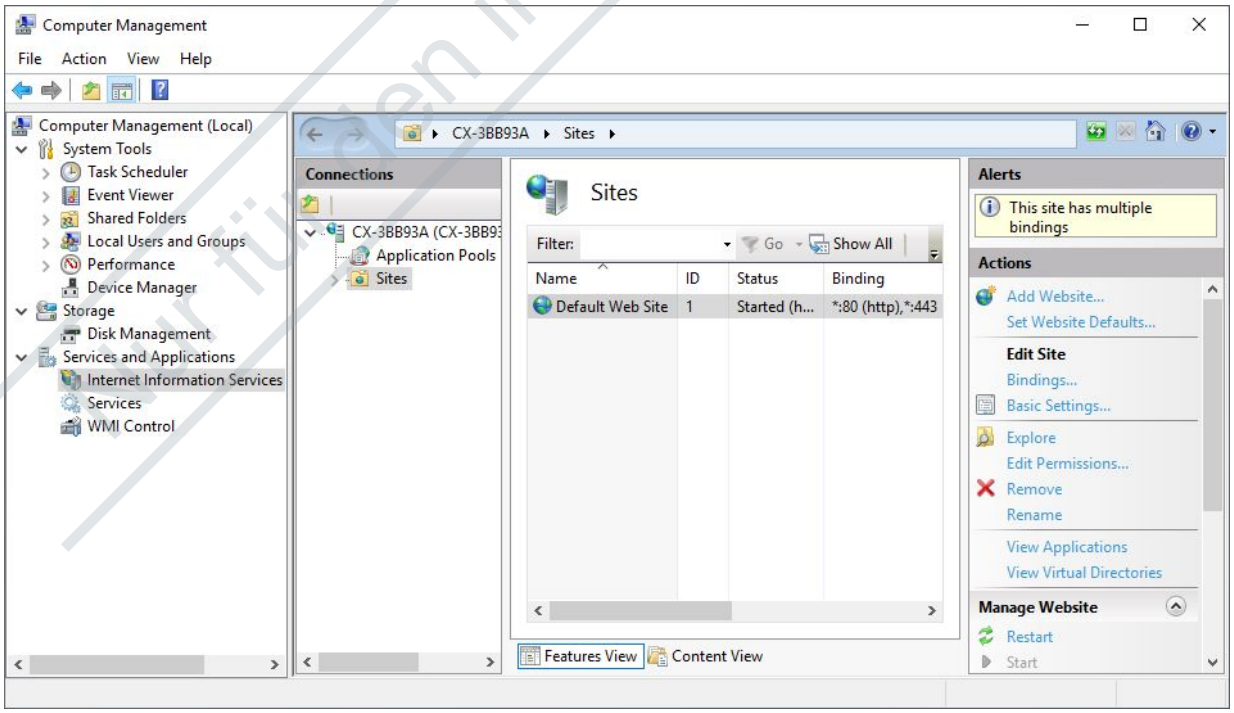
2. Deaktivieren Sie die Option unter **Internet Information Service**.



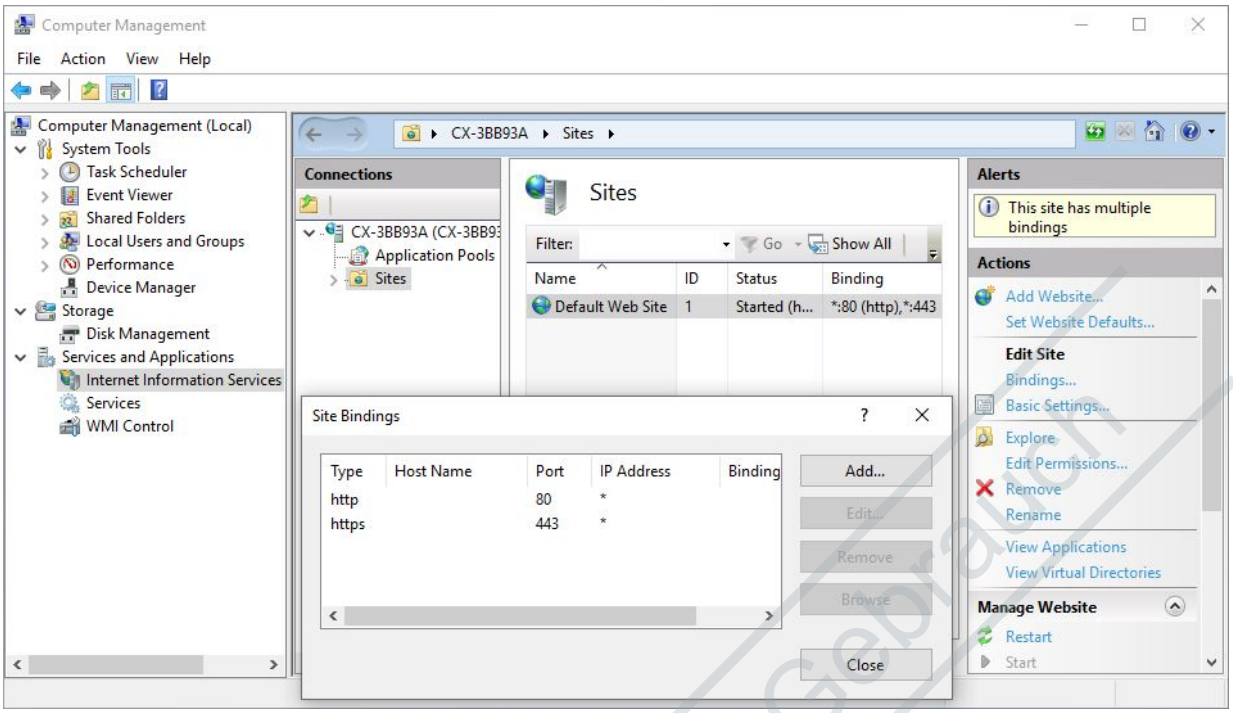
3. Damit wird der IIS-Webserver deaktiviert. Von diesen Änderungen sind alle Applikationen betroffen, die auf den IIS-Webserver zurückgreifen.

Zugriff von außen einschränken:

1. Um den Zugriff von außen zu deaktivieren, rufen Sie den Ausführen-Dialog über die Tastenkombination **[Windows-Taste] + [R]** auf und geben Sie **compmgmt.msc** ein.
2. Wählen Sie im links im Strukturbaum den Eintrag **Internet Information Services** und unter **Connections** den Ordner **Sites**.

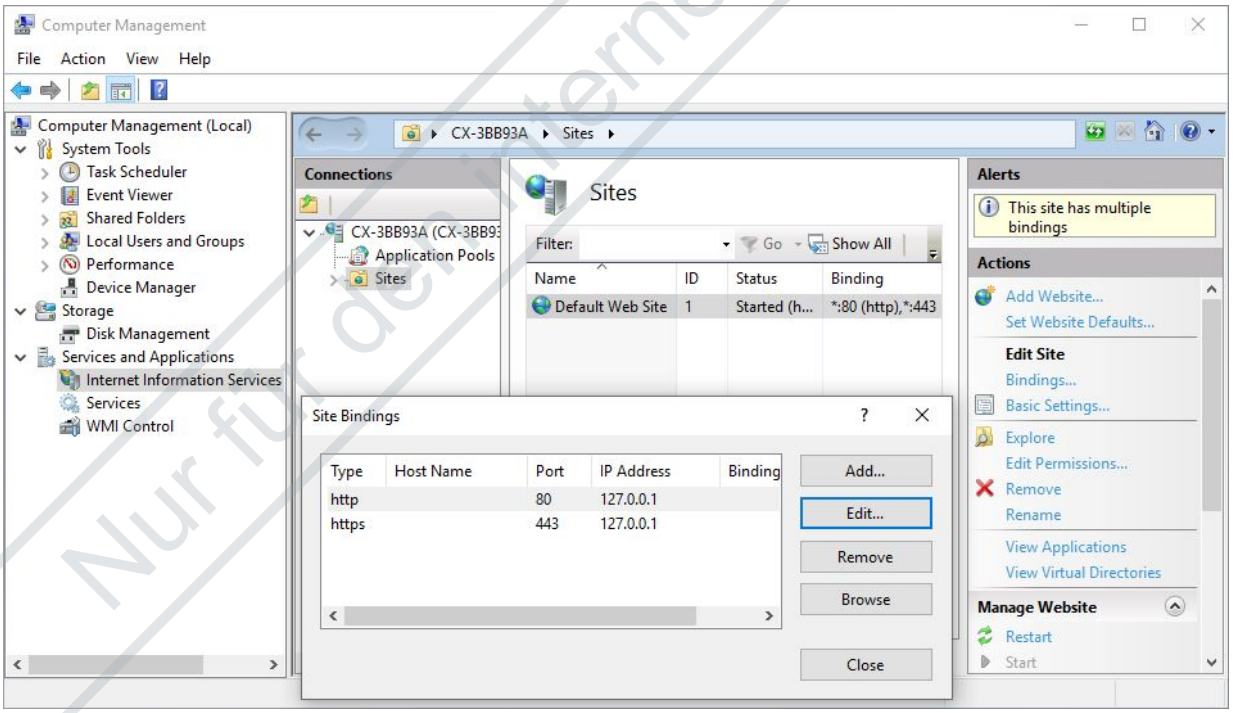


3. Klicken Sie auf der rechten Seite unter Actions auf **Bindings**. Im Fenster **Site Bindings** wird in der Spalte **IP Adress** für http und https ein Sternchen (*) angezeigt.



Damit sind alle Zugriffe von außen erlaubt.

4. Editieren Sie die Einträge für http bzw. https und erlauben Sie mit dem Eintrag **127.0.0.1** ausschließlich den lokalen Zugriff.



⇨ Der Zugriff auf den Beckhoff Device Manager ist ab jetzt von außen eingeschränkt. Der lokale Zugriff ist mit **127.0.0.1/config** weiterhin möglich und alle weiteren Applikationen von einer kompletten Deaktivierung nicht betroffen.

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. 3: 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. 4: 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. 5: 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. 6: 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

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