

Industrie PC - Härtung „Out-of-the-Box“

Erhöhung der Sicherheit von IPC-basierten Anlagen durch
Standardmechanismen



...Security **kostet Geld,**
verzögert die Inbetriebnahme
und **schränkt** bei der
Fehlersuche **ein**



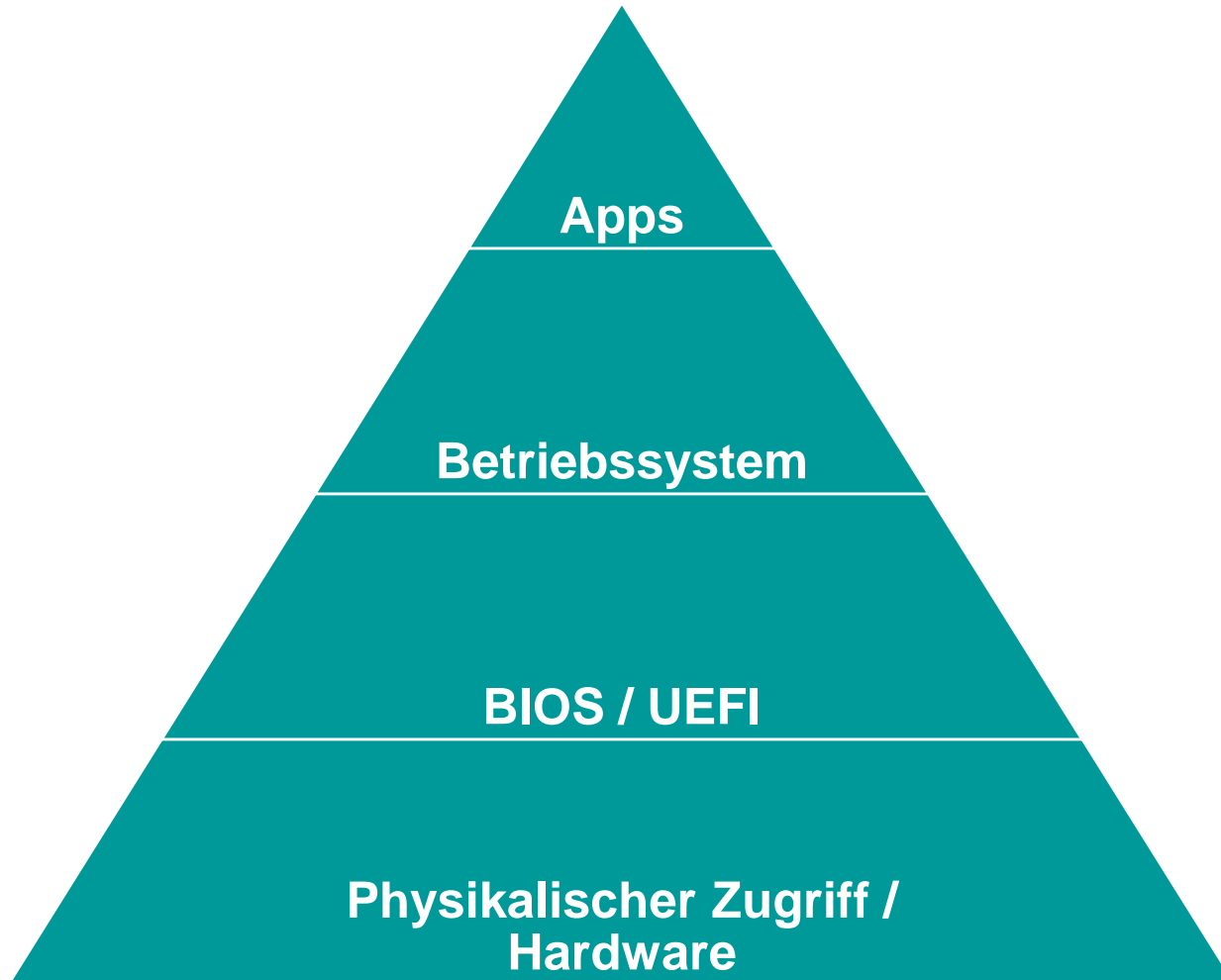
... **jetzt** stellen wir mal die
Funktion her, **dann** kümmern wir
uns um die **Security**...

Überblick und Aufteilung von Sicherheitsmaßnahmen

Die Basis ist die Hardware.

Gesamtheitliche Security Maßnahmen

Wichtig auf allen Ebenen

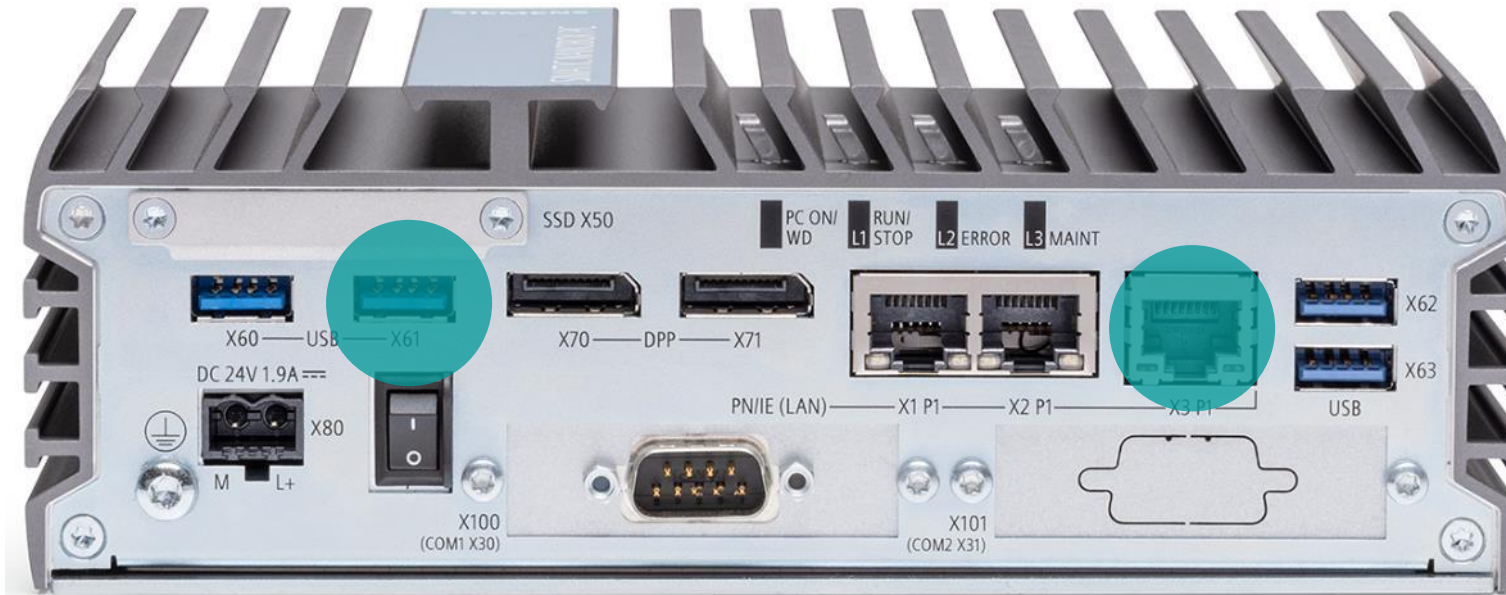


Jede Ebene stellt individuelle potentielle Angriffspfade dar und muss dadurch unabhängig abgesichert werden.

- Zugriffsberechtigung und Rechte Management
- Härtung des Betriebssystems
- Absicherung von BIOS / UEFI
- Zutrittskontrolle und Verriegelung nicht verwendeter Schnittstellen

Hardware

Schutz für Zutritt und Schnittstellen



Physikalischer Zugriffsschutz

- Versperrte Räume bzw. Schaltschränke

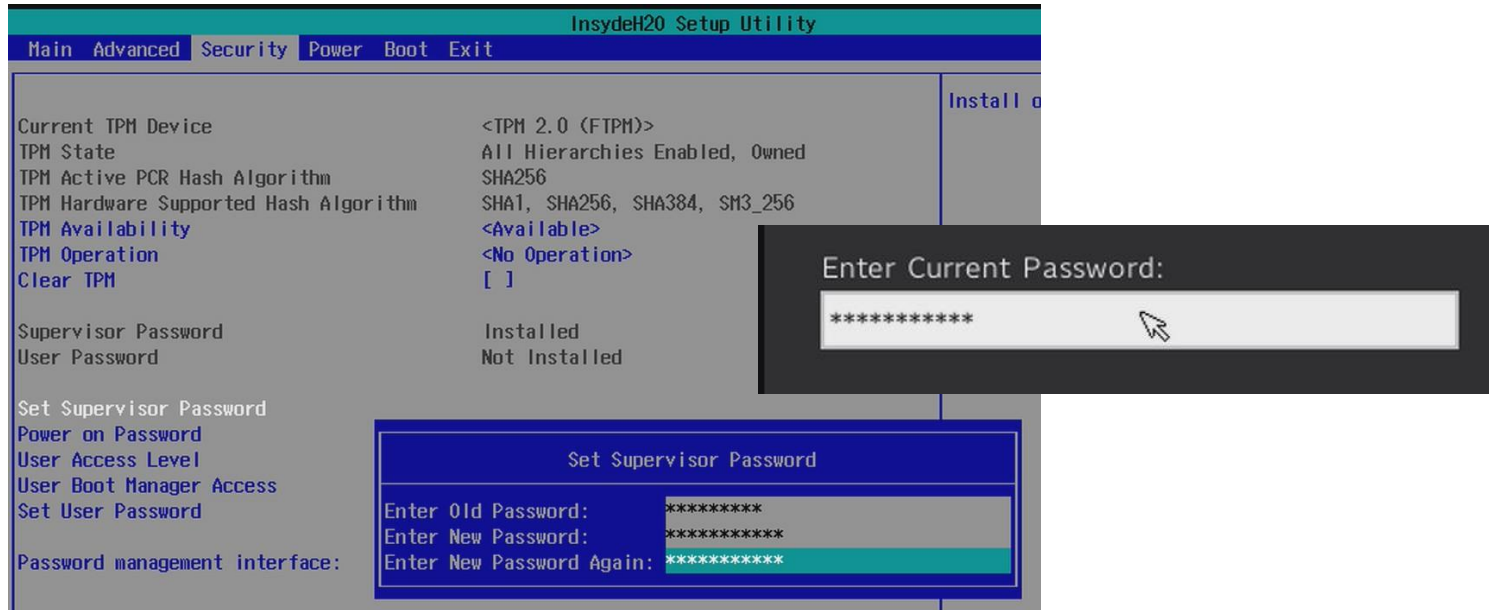
„Verplombung“ nicht verwendeter Schnittstellen

- RJ45 Lock
- USB Lock

Versperrbare Fronttüren bei Rack-IPCs zum Schutz von Front-USB Anschlüssen

UEFI / BIOS

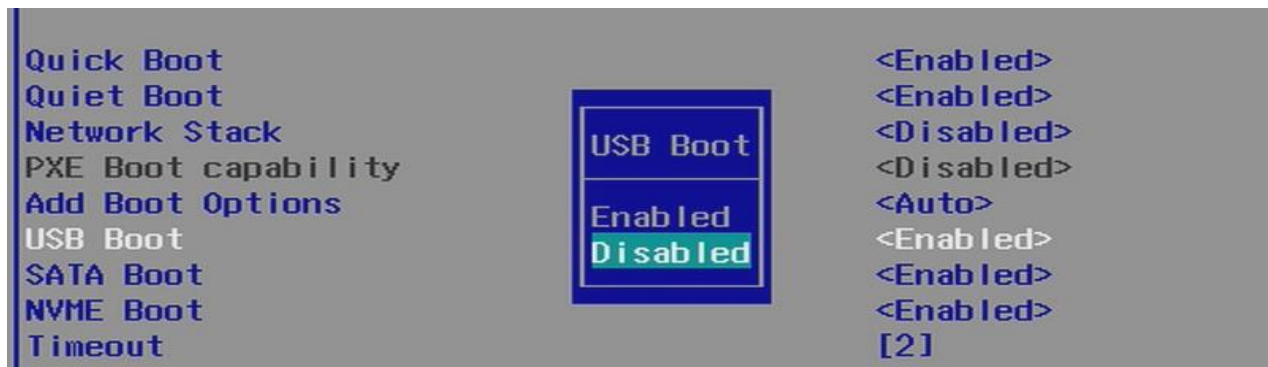
Schutz gegen das Verändern von Werten



BIOS Passwort um das Ändern von BIOS Einstellungen zu verhindern

Software basiertes Deaktivieren von Schnittstellen

- USB Ports
- Netzwerk Ports



TPM-Chip für die Ablage von **Kryptografischen Schlüssel** wie z.B. Verschlüsselung von Festplatten

5 Tipps um Betriebssysteme sicherer zu machen

Am Beispiel von Microsoft Windows® 10 Enterprise



Wie verhindere ich das Schließen
von Applikationen im Vollbildmodus?

Keyboard Filter

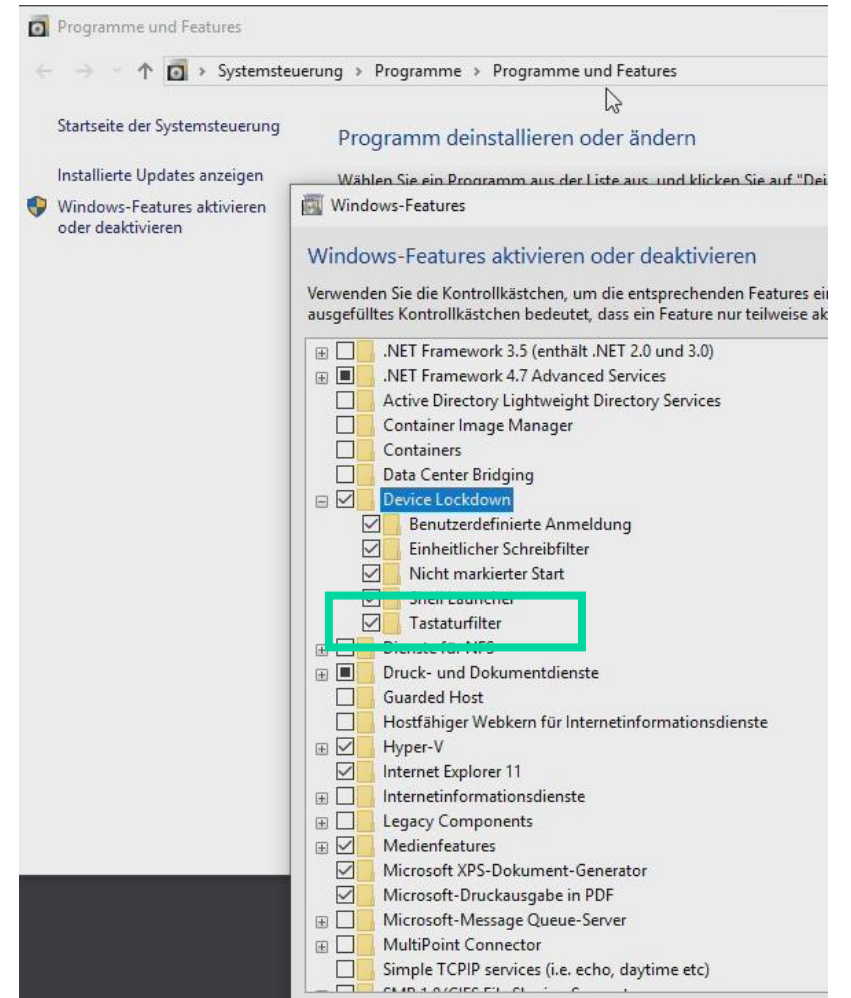
Betriebssystem (Microsoft® Windows 10 LTSC 2019)

Unterdrückt unerwünschte Eingaben oder Tastenkombinationen über die Tastatur. Der Tastaturfilter funktioniert mit physikalischen Tastaturen sowie für die Windows Bildschirmtastatur und der Touchtastatur.

Features Tastaturfilter

- Steuerung auf Benutzerkontenebene
- Deaktivierung von Tastenkombinationen für das Schließen von Programmen, Ausführen von Befehlen
z.B.: Strg + Alt + Entf oder Alt + F4

Tastaturfilter funktionieren nicht über Remote Desktop.





Welche Möglichkeiten habe ich,
ungewollte Änderungen an
Systemen zu widerrufen?

Unified Write Filter - UWF

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

Schutz von Laufwerken, indem alle Schreibvorgänge an Laufwerke (z.B. Festplatten) an einen virtuellen temporären Datenträger umgeleitet werden.

Vorteile durch UWF

- Reduzierung der Schreib-Zugriffe auf die physikalische Festplatte (Schutz von SSD Laufwerken)
- Einfache Möglichkeit zur Erstellung von „Read-Only“ Systemen
- Einbinden von Ausnahmen möglich z.B. Windows Updates, benutzerdefinierte Verzeichnisse
- Ideal für KIOSK / Visualisierungssysteme

Unterstützte Dateisysteme FAT, NTFS. Virtueller überlagerter Datenträger wächst dynamisch, abhängig der Schreibzyklen.

```
C:\Users\admin>uwfmgr get-config
UWF (Unified Write Filter)-Konfigurationshilfsprogramm, Version 10.0.17763
Copyright (c) Microsoft Corporation. Alle Rechte vorbehalten.

Einstellungen für die aktuelle Sitzung

FILTEREINSTELLUNGEN
  Filterstatus:      AUS
  Ausstehender Commit: Nicht zutreffend
  Herunterfahren steht aus: Nein

WARTUNGSEINSTELLUNGEN
  Wartungsstatus: AUS

ÜBERLAGERUNGSEINSTELLUNGEN
  Typ:              RAM
  Maximale Größe:   1024 MB
  Warnungsschwellenwert: Nicht verfügbar
  Kritischer Schwellenwert: Nicht verfügbar
  Freespace-Pass-Through: Nicht verfügbar
  Persistent:       (null)
  Zurücksetzungsmodus: Nicht zutreffend

VOLUMEINSTELLUNGEN
  *** Keine Volumes konfiguriert

REGISTRIERUNGSAUSSCHLÜSSE
  Nicht verfügbar

Einstellungen für die nächste Sitzung

FILTEREINSTELLUNGEN
  Filterstatus:      AUS
  Ausstehender Commit: Nicht zutreffend

WARTUNGSEINSTELLUNGEN
  Wartungsstatus: AUS

ÜBERLAGERUNGSEINSTELLUNGEN
  Typ:              RAM
  Maximale Größe:   1024 MB
  Warnungsschwellenwert: Nicht verfügbar
  Kritischer Schwellenwert: Nicht verfügbar
  Freespace-Pass-Through: Nicht verfügbar
  Persistent:       (null)
  Zurücksetzungsmodus: Nicht zutreffend

VOLUMEINSTELLUNGEN
  *** Keine Volumes konfiguriert
```

Unified Write Filter - UWF

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

- Schreibfilter installieren – Windows Funktionen hinzufügen oder entfernen – Device Lock-Down

- Eingabeaufforderung als Administrator starten

- zu schützendes Volume aktivieren

```
uwfmgr volume protect c:
```

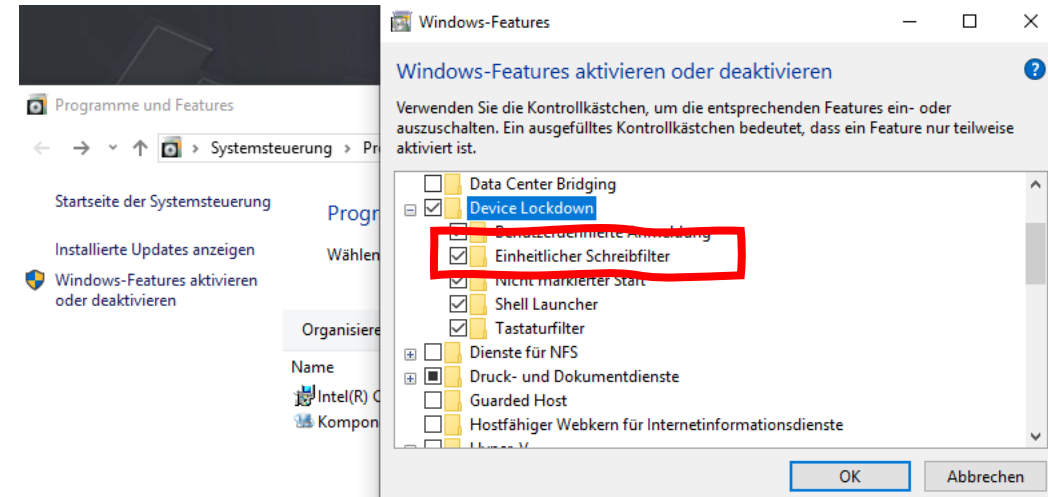
- Schreibfilter aktivieren

```
uwfmgr filter enable
```

- Neustart um Filter zu aktivieren

- Ggf. Status des Schreibfilter überprüfen / Änderungen am System vornehmen (z.B. Software Installation)

```
uwfmgr get-config
```





Kann ich definieren, welche
Applikationen und Dienste auf
ausgeführt werden?

AppLocker

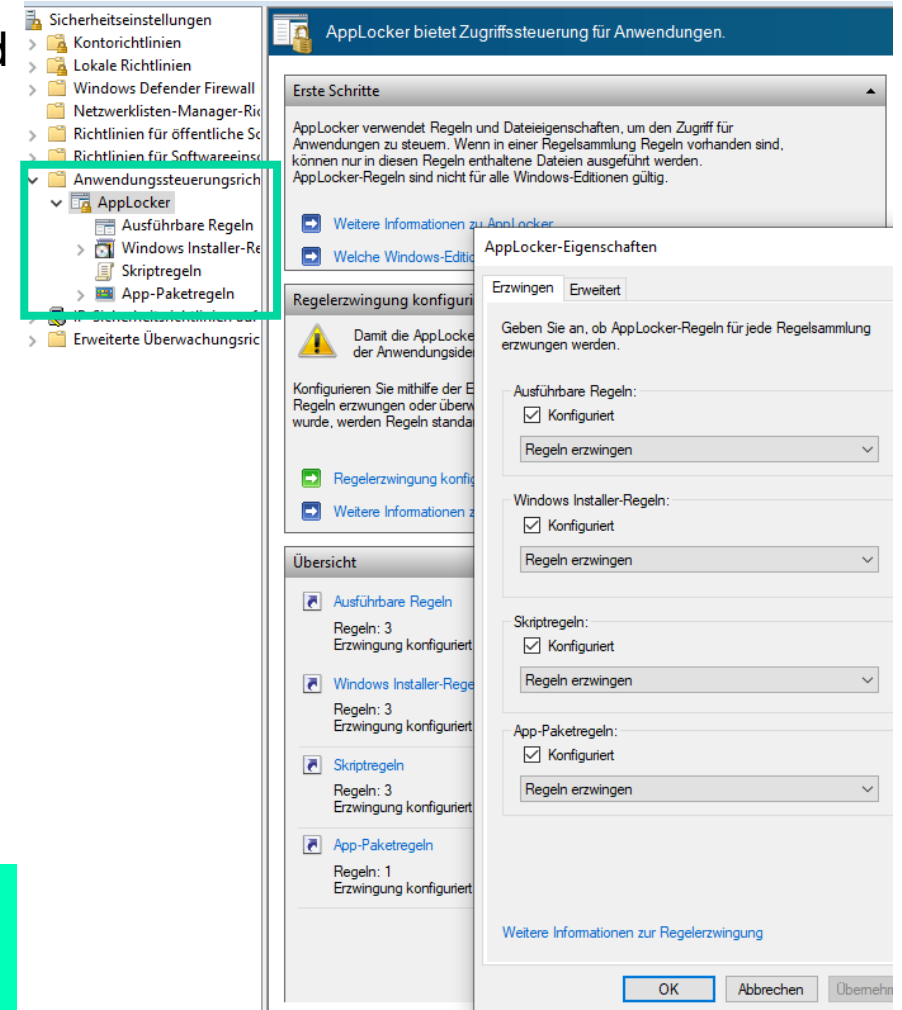
Betriebssystem (Microsoft® Windows 10 LTSC 2019)

Der AppLocker definiert den Zugriff auf gewünschte Anwendungen und Dateien. Dadurch wird eine missbräuchliche Verwendung bzw. die Installation von Schadsoftware erschwert und kann auf ausführbare Dateien, Scripts und Windows Installer Dateien angewandt werden.

Anwendungsszenarien

- Schutz vor unerwünschter Software
- Einhaltung von Lizenzen
- Softwarestandardisierung
- Verbesserungen der Verwaltbarkeit

AppLocker kann keine Prozesse steuern / überwachen, welche als Systembenutzer ausgeführt wurden.



AppLocker

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

- Systemdienst „Anwendungsidentität“ automatisch beim Systemstart starten

```
sc.exe config appidsvc start=auto
```

- Lokale Sicherheitsrichtlinie öffnen

```
secpol.msc
```

- Richtlinienerzwingung konfigurieren

The image shows a sequence of three screenshots illustrating the configuration of AppLocker. The first screenshot shows the Windows Security settings window with the 'AppLocker' folder highlighted in red. The second screenshot shows the 'AppLocker bietet Zugriffssteuerung für Anwendungen.' dialog box, with the 'Regelerzwingung konfigurieren' button highlighted in red. The third screenshot shows the 'AppLocker-Eigenschaften' dialog box, with red arrows pointing from the 'Regelerzwingung konfigurieren' button in the second screenshot to the 'Erzwingen' tab and the 'Regeln erzwingen' buttons for 'Ausführbare Regeln', 'Windows Installer-Regeln', 'Skriptregeln', and 'App-Paketregeln'.

AppLocker

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

- Standard Regeln anwenden, je nach Bedarf Regeln automatisch generieren oder Standardregeln erstellen
- Einschränkungen definieren und ggf. an Benutzer oder Benutzergruppe zuweisen.
- Test des AppLockers je nach Konfiguration z.B. Start des Internet Explorers

The screenshot displays the Windows AppLocker configuration interface. On the left, a tree view shows the navigation path: **AppLocker** > **Ausführbare Regeln**. The main area shows a list of rules:

Aktion	Benutzer	Name	Bedingung	Ausnah...
Verweigern	DESKTOP-64...	%PROGRAMFILES%\internet explorer\ie...	Pfad	
Zulassen	Jeder	(Standardregel) Alle Dateien im Ordner ...	Pfad	
Zulassen	Jeder	(Standardregel) Alle Dateien im Ordner ...	Pfad	
Zulassen	VORDEFINIE...	(Standardregel) Alle Dateien	Pfad	

The 'Eigenschaften von Verweigern' dialog box is open, showing the configuration for the selected rule:

- Name:** %PROGRAMFILES%\internet explorer\iexplore.exe
- Beschreibung:** (optional)
- Aktion:** Verweigern
- Benutzer oder Gruppe:** DESKTOP-64OKMAT\user

Buttons at the bottom of the dialog include OK, Abbrechen, and Übernehmen.



Gibt es Möglichkeiten über bestimmte Ereignisse am System informiert zu werden?

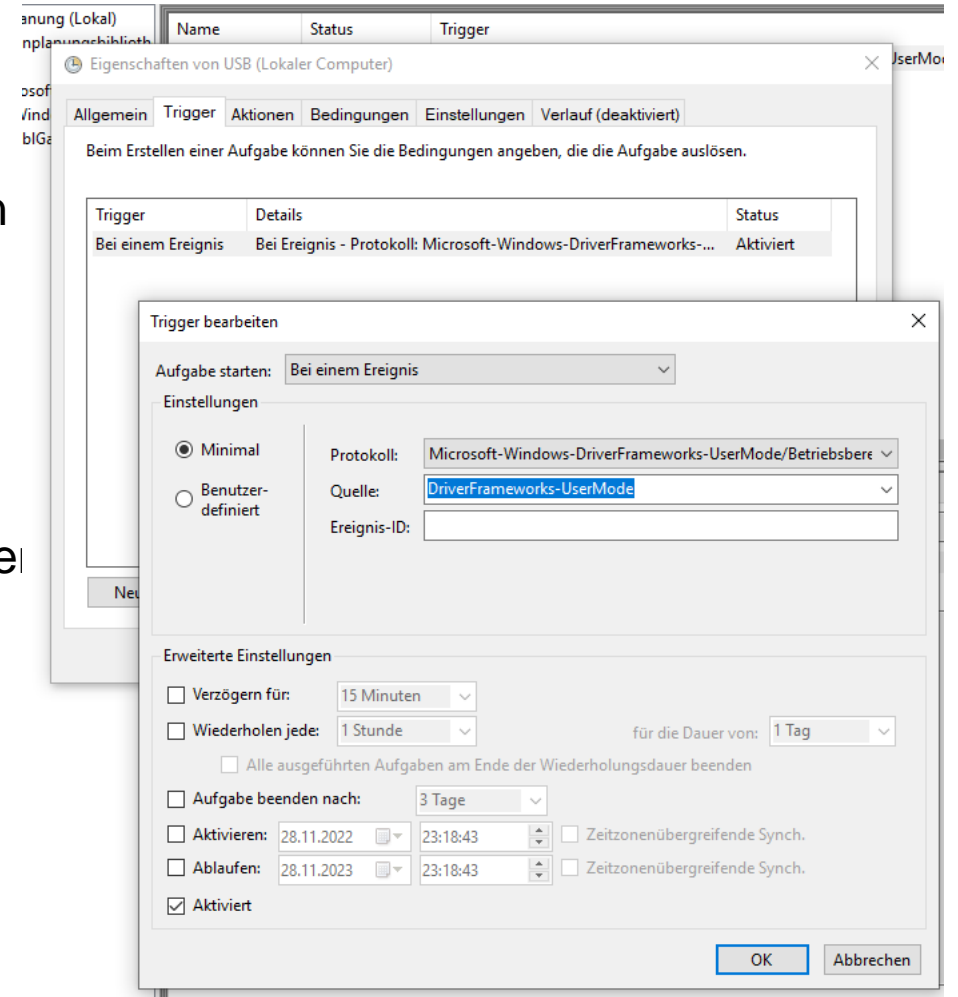
Aufgabenplanung - Überwachung von Ereignissen

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

Die Windows Aufgabenplanung ermöglicht eine benutzerdefinierte Benachrichtigung bei der Statusänderung von Programmen und Prozessen, dadurch ist es möglich einfach Überwachungsfunktionen zu realisieren und definierte Ereignisse auszuführen.

Anwendungsszenarien

- Überwachung des Status der Windows Firewall
- Erkennen, ob USB-Speichermedien gesteckt oder gezogen werden
- Erkennen, ob bestimmte Anwendungen gestartet werden



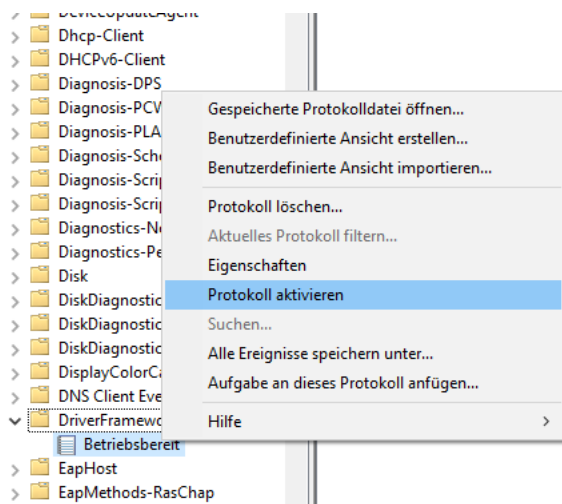
Aufgabenplanung - Überwachung von Ereignissen

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

- Protokollierung des zu überwachenden Elements aktivieren in der Ereignisanzeige definieren
z.B. Aktivieren / Deaktivieren von Volumes (USB-Sticks)

Ereignisanzeige -> Anwendungs- und Dienstprogramme ->

Microsoft -> Windows -> DriverFrameworks-UserModule -> Betriebsbereit

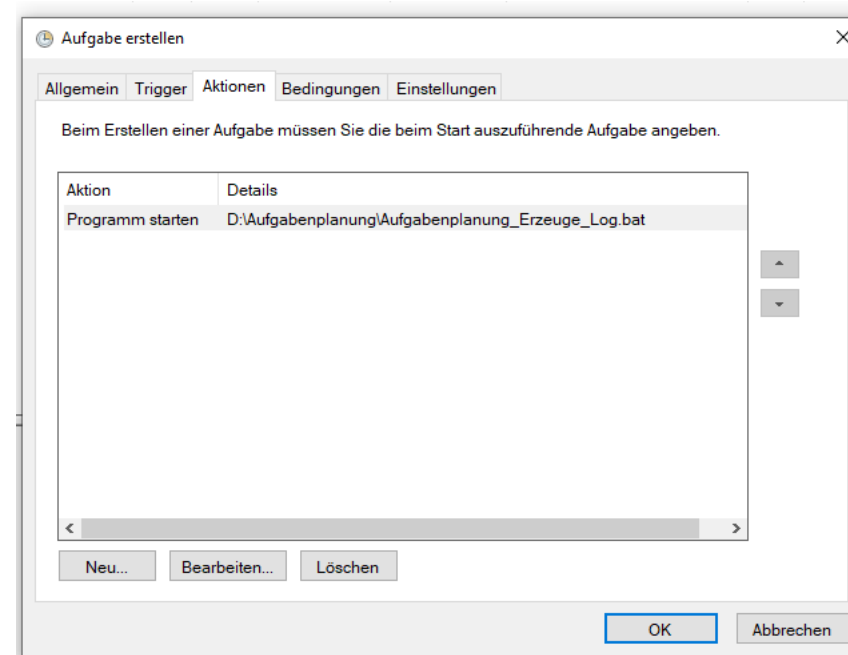
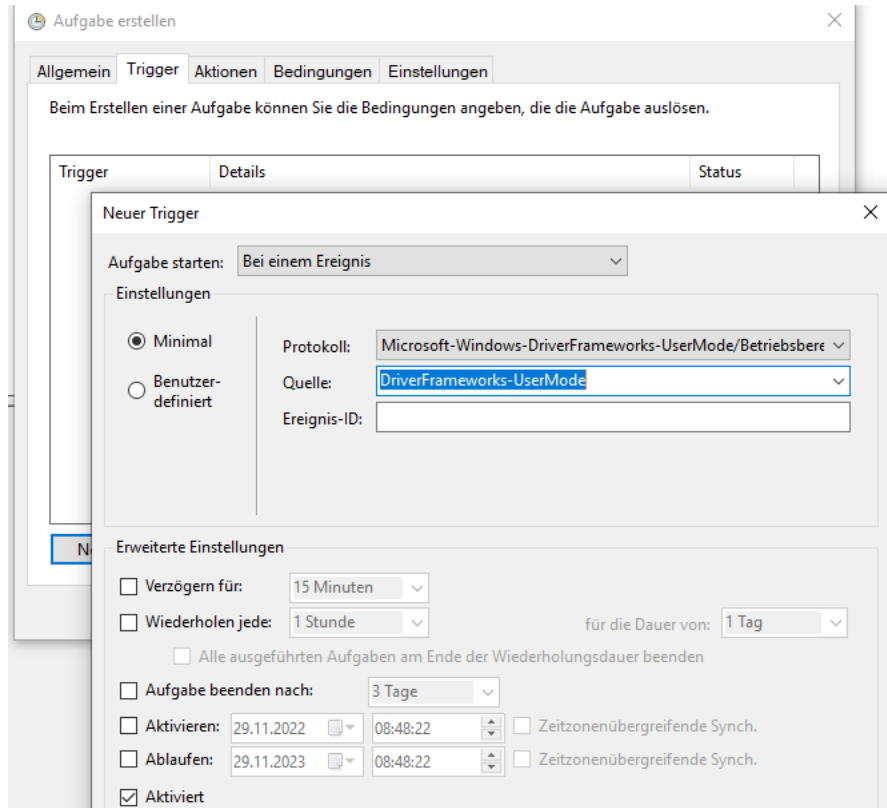


- Aufgabenplanung öffnen und neues Ereignis erstellen
taskschd.msc

Aufgabenplanung - Überwachung von Ereignissen

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

- Neues Ereignis erstellen und Trigger und Aktion festlegen



- Test der Funktion laut definierten Bedingungen, z.B. Log beim Anstecken eines USB-Sticks



Welche Möglichkeiten habe ich
einen Soll-Ist Vergleich von
Windows Einstellungen
durchzuführen?

Windows Baseline – Security Compliance Toolkit (SCT)

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

Das Security Compliance Toolkit (SCT) ist eine Sammlung von Tools, mit denen Administratoren empfohlene Sicherheitskonfigurationen für Windows und andere Microsoft Produkte auf Basis von Gruppenrichtlinien (GPOs) herunterladen, analysieren, testen und bearbeiten können.

Anwendungsbeispiele für das SCT

- Export von Richtlinien zur Dokumentation
- Konfigurationsvergleich zwischen 2 Richtlinienobjekten
- Automatisiertes setzen von GPOs

The screenshot displays the Security Compliance Toolkit (SCT) interface. The top window, 'Policy Analyzer v4.0.2004.13001', shows a list of policies with columns for Name and Date. One policy, 'MSFT-Win10-WS-v1809-FINAL', is selected. The bottom window, 'Policy Viewer - 393 items', displays a table of policy settings. The table has columns for Policy Type, Policy Group or Registry Key, Policy Setting, Baseline(s), and Effective state. Several rows are highlighted in yellow, indicating differences between the current configuration and the baseline. Below the table, the 'Policy Path' section provides details for the selected policy, including the path to the security settings and a description of the policy's function.

Policy Type	Policy Group or Registry Key	Policy Setting	Baseline(s)	Effective state
Security Template	Privilege Rights	SeProfileSingleProcessPrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeRemoteInteractiveLogonRight	*S-1-5-32-544	
Security Template	Privilege Rights	SeRemoteShutdownPrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeRestorePrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeSecurityPrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeSystemEnvironmentPrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeTakeOwnershipPrivilege	*S-1-5-32-544	
Security Template	Privilege Rights	SeTcbPrivilege		
Security Template	Privilege Rights	SeTrustedCredManAccessPrivilege		
Security Template	Service General Setting	"AppIDSvc"	2,""	2,""
Security Template	Service General Setting	"XblAuthManager"	4,""	3,""
Security Template	Service General Setting	"XblGameSave"	4,""	3,""
Security Template	Service General Setting	"XboxGipSvc"	4,""	3,""
Security Template	Service General Setting	"XboxNetApiSvc"	4,""	3,""
Security Template	System Access	ClearTextPassword	0	
Security Template	System Access	EnableAdminAccount	0	
Security Template	System Access	EnableGuestAccount	0	
Security Template	System Access	LockoutBadCount	10	
Security Template	System Access	LockoutDuration	15	
Security Template	System Access	LSAAnonymousNameLookup	0	
Security Template	System Access	MaximumPasswordAge	60	
Security Template	System Access	MinimumPasswordAge	1	

Policy Path:
Sicherheitseinstellungen
Lokale Richtlinien\Zuweisen von Benutzerrechten
Zugriff vom Netzwerk auf diesen Computer verweigern
Zugriff vom Netzwerk auf diesen Computer verweigern
Mit dieser Sicherheitseinstellung wird festgelegt, welchen Benutzern der Zugriff auf einen Computer über das Netzwerk verweigert werden soll. Wenn für ein Benutzerkonto beide Richtlinien gelten.
Standardwert: Gast

Windows Baseline – Security Compliance Toolkit (SCT)

Betriebssystem (Microsoft® Windows 10 LTSC 2019)

- Download Microsoft Security Compliance Toolkit

<https://www.microsoft.com/en-us/download/details.aspx?id=55319>

- Häufig verwendete Tools bzw. Baselines

LGPO.zip

Automatisierung des Lokalen Group Policy Editors

PolicyAnalyzer.zip

Tool zum Vergleichen von Policies

Windows 10 Update Baseline.zip

Standard Richtlinien für Windows Update

- Weitere Informationen

<https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines>

Weiterführende Informationen und Links

Siemens ProductCERT and Siemens CERT

<https://siemens.com/cert>

Netzwerkkonzepte für die Factory Automation

<https://support.industry.siemens.com/cs/at/de/view/109802750>

BIOS-Downloads für SIMATIC IPCs, SIMATIC Tablet-PCs, SIMATIC Field-PGs, SINUMERIK PCU und SIMOTION P320

<https://support.industry.siemens.com/cs/at/de/view/109763408>

Empfohlene Sicherheitseinstellungen für IPCs im Industrieumfeld

<https://support.industry.siemens.com/cs/de/de/view/109475014>

SIMATIC IPC - Security Leitfaden für Linux-Systeme

<https://support.industry.siemens.com/cs/at/de/view/109768383>

Überwachung von Aufgaben aus der Windows Aufgabenplanung mit DiagMonitor

<https://support.industry.siemens.com/cs/de/de/view/109755236>

Microsoft Windows Security baselines

<https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework/windows-security-baselines>

Disclaimer

© Siemens 2022

Änderungen und Irrtümer vorbehalten. Die Informationen in diesem Dokument enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden.

Alle Produktbezeichnungen können Marken oder sonstige Rechte der Siemens AG, ihrer verbundenen Unternehmen oder dritter Gesellschaften sein, deren Benutzung durch Dritte für ihre eigenen Zwecke die Rechte der jeweiligen Inhaber verletzen kann.

Kontakt

Herausgeber: Siemens AG Österreich

Matthias Jäger

Produktmanagement IPCs & PC-based Automation

RC-AT DI FA PR BD-P

Siemensstraße 90

1210 Wien

Österreich

Mobil +43 664 88551097

E-Mail matthias.jaeger@siemens.com