SIEMENS

SIMATIC

Prozessleitsystem PCS 7 Konfiguration Symantec Endpoint Protection (V12.1)

Inbetriebnahmehandbuch

03/2016
A5E37491487-AA

Rechtliche Hinweise

Warnhinweiskonzept

Dieses Handbuch enthält Hinweise, die Sie zu Ihrer persönlichen Sicherheit sowie zur Vermeidung von Sachschäden beachten müssen. Die Hinweise zu Ihrer persönlichen Sicherheit sind durch ein Warndreieck hervorgehoben, Hinweise zu alleinigen Sachschäden stehen ohne Warndreieck. Je nach Gefährdungsstufe werden die Warnhinweise in abnehmender Reihenfolge wie folgt dargestellt.

⚠ GEFAHR
bedeutet, dass Tod oder schwere Körperverletzung eintreten **wird**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ WARNUNG
bedeutet, dass Tod oder schwere Körperverletzung eintreten **kann**, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

⚠ VORSICHT
bedeutet, dass eine leichte Körperverletzung eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

ACHTUNG
bedeutet, dass Sachschaden eintreten kann, wenn die entsprechenden Vorsichtsmaßnahmen nicht getroffen werden.

Beim Auftreten mehrerer Gefährdungsstufen wird immer der Warnhinweis zur jeweils höchsten Stufe verwendet. Wenn in einem Warnhinweis mit dem Warndreieck vor Personenschäden gewarnt wird, dann kann im selben Warnhinweis zusätzlich eine Warnung vor Sachschäden angefügt sein.

Qualifiziertes Personal

Das zu dieser Dokumentation zugehörige Produkt/System darf nur von für die jeweilige Aufgabenstellung **qualifiziertem Personal** gehandhabt werden unter Beachtung der für die jeweilige Aufgabenstellung zugehörigen Dokumentation, insbesondere der darin enthaltenen Sicherheits- und Warnhinweise. Qualifiziertes Personal ist auf Grund seiner Ausbildung und Erfahrung befähigt, im Umgang mit diesen Produkten/Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

Bestimmungsgemäßer Gebrauch von Siemens-Produkten

Beachten Sie Folgendes:

⚠ WARNUNG
Siemens-Produkte dürfen nur für die im Katalog und in der zugehörigen technischen Dokumentation vorgesehenen Einsatzfälle verwendet werden. Falls Fremdprodukte und -komponenten zum Einsatz kommen, müssen diese von Siemens empfohlen bzw. zugelassen sein. Der einwandfreie und sichere Betrieb der Produkte setzt sachgemäßen Transport, sachgemäße Lagerung, Aufstellung, Montage, Installation, Inbetriebnahme, Bedienung und Instandhaltung voraus. Die zulässigen Umgebungsbedingungen müssen eingehalten werden. Hinweise in den zugehörigen Dokumentationen müssen beachtet werden.

Marken

Alle mit dem Schutzrechtsvermerk ® gekennzeichneten Bezeichnungen sind eingetragene Marken der Siemens AG. Die übrigen Bezeichnungen in dieser Schrift können Marken sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Haftungsausschluss

Wir haben den Inhalt der Druckschrift auf Übereinstimmung mit der beschriebenen Hard- und Software geprüft. Dennoch können Abweichungen nicht ausgeschlossen werden, so dass wir für die vollständige Übereinstimmung keine Gewähr übernehmen. Die Angaben in dieser Druckschrift werden regelmäßig überprüft, notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

A5E37491487-AA
℗ 04/2016 Änderungen vorbehalten

Inhaltsverzeichnis

Security-Hinweise

1

Siemens bietet Produkte und Lösungen mit Industrial Security-Funktionen an, die den sicheren Betrieb von Anlagen, Lösungen, Maschinen, Geräten und/oder Netzwerken unterstützen. Sie sind wichtige Komponenten in einem ganzheitlichen Industrial Security-Konzept. Die Produkte und Lösungen von Siemens werden unter diesem Gesichtspunkt ständig weiterentwickelt. Siemens empfiehlt, sich unbedingt regelmäßig über Produkt-Updates zu informieren.

Für den sicheren Betrieb von Produkten und Lösungen von Siemens ist es erforderlich, geeignete Schutzmaßnahmen (z. B. Zellenschutzkonzept) zu ergreifen und jede Komponente in ein ganzheitliches Industrial Security-Konzept zu integrieren, das dem aktuellen Stand der Technik entspricht. Dabei sind auch eingesetzte Produkte von anderen Herstellern zu berücksichtigen. Weitergehende Informationen über Industrial Security finden Sie unter: http://www.siemens.com/industrialsecurity

Um stets über Produkt-Updates informiert zu sein, melden Sie sich für unseren produktspezifischen Newsletter an. Weitere Informationen hierzu finden Sie unter: http://support.automation.siemens.com.

Vorwort

2

Die vorliegende Dokumentation beschreibt die zu ändernden Einstellungen des Symantec Endpoint Protection V12.1 beim Einsatz in einer Industrie Anlage.

Die Konfiguration stellt einen Auszug der Einstellungen von Symantec Endpoint Protection dar, die im Verträglichkeitstest mit PCS 7 und WinCC verwendet wurden.

Wichtiger Hinweis zu diesem Whitepaper

Hinweis

Die empfohlenen Einstellungen dieser Virenscanner sind so gewählt, dass der zuverlässige Echtzeitbetrieb von PCS 7 durch die Virenscanner-Software nicht beeinträchtigt wird.

Diese Empfehlungen beschreiben den aktuell bekannten, bestmöglichen Kompromiss zwischen dem Ziel, Viren- und Schad-Software möglichst umfassend zu entdecken und unwirksam zu machen und dem Ziel, ein möglichst deterministisches Zeitverhalten des PCS 7 Leitsystems in allen Betriebsphasen zu gewährleisten.

Die Wahl anderer Einstellungen der Virenscanner kann sich unter Umständen ungünstig auf das Echtzeitverhalten auswirken.

Zweck der Dokumentation

Diese Dokumentation beschreibt die für PCS 7 und WinCC empfohlenen Anpassungen der Virenscanner-Software nach der Installation des Virenscanners.

Erforderliche Kenntnisse

Diese Dokumentation wendet sich an Personen, die in den Bereichen Projektierung, Inbetriebnahme und Service von Automatisierungssystemen mit SIMATIC PCS 7 bzw. WinCC tätig sind. Administrationskenntnisse und IT-Techniken für Microsoft Windows Betriebssysteme werden vorausgesetzt. Des Weiteren sollte das Sicherheitskonzept PCS 7 & WinCC bekannt sein.

Weitere Informationen hierzu finden Sie im Internet unter folgender Adresse:

http://support.industry.siemens.com/cs (https://support.industry.siemens.com/cs/ww/de/view/60119725)

Gültigkeitsbereich der Dokumentation

Die Dokumentation ist gültig für prozessleittechnische Anlagen, die mit der jeweiligen Produktversion von PCS 7 bzw. WinCC realisiert sind.

Hinweis

Beachten Sie, dass bestimmte Virenscanner nur für bestimmte Produktversionen freigegeben sind. Weitere Informationen hierzu finden Sie im Internet unter folgender Adresse:

http://support.industry.siemens.com/cs (https://support.industry.siemens.com/cs/ww/de/view/2334224)

Administration von Virenscannern 3

3.1 Einleitung

Der Einsatz von Virenscannern in einem Prozessleitsystem ist nur dann effektiv, wenn er Teil eines umfassenden Security-Konzeptes ist. Der alleinige Einsatz eines Virenscanners kann ein Prozessleitsystem nicht vor Security-Bedrohungen im Allgemeinen schützen.

3.2 Definitionen

Virenscanner

Ein Virenscanner ist eine Software, die bekannte schädliche Programmroutinen (Computerviren, Würmer und ähnliche Schadsoftware) aufspürt, blockiert oder beseitigt.

Scan-Engine (Scanmodul)

Die Scan-Engine ist der Teil der Virenscanner-Software, der Daten auf schädliche Software untersuchen kann.

Virensignaturdatei (Virenpatterndatei oder Virendefinitionsdatei)

Diese Datei stellt der Scan-Engine die Virensignaturen bereit, mit deren Hilfe die Suche nach schädlicher Software in den Daten durchgeführt wird.

Virenscan-Client

Der Virenscan-Client ist ein Computer, der auf Viren überprüft wird und vom Virenscan-Server verwaltet wird.

Virenscan-Server

Der Virenscan-Server ist ein Computer, der Virenscan-Clients zentral verwaltet, Virensignaturdateien lädt und auf die Virenscan-Clients verteilt.

Security Suite

Meist von ehemaligen Virenscanner-Herstellern vertriebene Programm Suites, die zusätzlich zur klassischen Virenscanfunktionalität noch weitere Sicherheitsfunktionalitäten mitbringen, wie z.B. IPS, Appilcation Control, Firewall, usw.

3.3 Einsatz von Virenscannern

Der Einsatz eines Virenscanners darf den Prozessbetrieb einer Anlage nicht beeinträchtigen. Die folgenden zwei Beispiele zeigen die Problematik, die durch den Einsatz von Virenscannern in der Automatisierung entsteht:

- Ein virenverseuchter Computer darf durch einen Virenscanner nicht abgeschaltet werden, wenn dadurch die Kontrolle über den Produktionsprozess verloren geht oder eine Anlage nicht mehr in einen sicheren Zustand gefahren werden kann.
- Auch eine virenverseuchte Projektdatei, beispielsweise ein Datenbankarchiv, darf nicht automatisch verschoben, blockiert oder gelöscht werden, wenn dadurch die Nachverfolgbarkeit von wichtigen Messwerten nicht mehr gegeben ist.

Es werden deshalb folgende Anforderungen an Virenscanner für den Einsatz in industriellen Umgebungen gestellt:

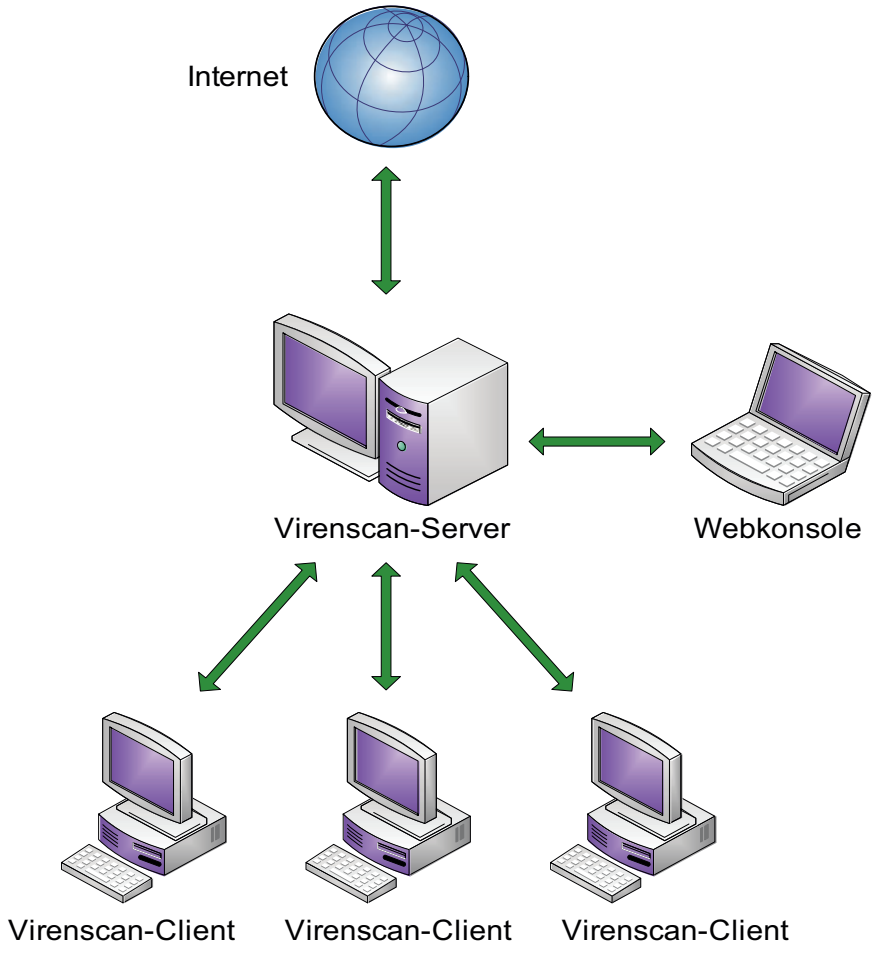
- Bei Einsatz einer Security-Suite (Virenscanner plus Optionen) müssen alle Optionen, die über die Funktionen eines klassischen Virenscanner hinausgehen, deaktivierbar sein, z.B. Firewall, E-Mail-Scan.
- Das Senden von Daten oder Berichten bei Virenfund an Virenscanner-Hersteller muss deaktivierbar sein.
- Die Virenscan-Clients in einer zentral verwalteten Virenscanner Architektur müssen in Gruppen einteilbar und konfigurierbar sein.
- Die automatische Verteilung der Virensignaturen muss deaktivierbar sein.
- Die Verteilung der Virensignaturen muss manuell und gruppenbasiert durchführbar sein.
- Ein manueller und gruppenweiser Datei- und Systemscan muss möglich sein.
- Bei Erkennung eines Virus muss immer eine Meldung generiert werden, aber nicht zwangsläufig eine Dateiaktion ausgeführt werden (z.B. löschen, blockieren, verschieben).
- Alle Meldungen müssen am Virenscan-Server protokolliert werden.
- Die Virenscan-Clients müssen so konfiguriert werden können, dass auf ihnen keine Meldung angezeigt wird, die wichtigere Prozessinformationen überdecken könnte.
- Die Virenscan-Clients sollten aus Performancegründen so konfigurierbar sein, dass ausschließlich die lokalen Laufwerke der Virenscan-Clients gescannt werden, um sich überschneidende Scans auf Netzwerklaufwerken zu verhindern.
- Die Virenscan-Clients sollten aus Performancegründen so konfigurierbar sein, dass nur der eingehende Datenverkehr geprüft wird, vorausgesetzt, dass sämtliche lokal bereits vorhandenen Daten bereits einmalig geprüft wurden.

3.4 Prinzipielle Virenscanner Architektur

Für die Realisierung der unter Kapitel "Einsatz von Virenscannern" genannten Forderungen empfiehlt sich eine Virenscanner-Architektur wie in der nachfolgenden Abbildung prinzipiell dargestellt.

Der Virenscan-Server erhält die Virensignaturen aus dem Internet vom Update-Server des jeweiligen Virenscanner-Herstellers oder von einem übergeordneten Virenscan-Server und

verwaltet seine Virenscan-Clients. Über eine Webkonsole oder ähnliches ist ein administrativer-Zugriff auf den Virenscan-Server möglich.



Je nach Hersteller ist es außerdem möglich, mehrere Virenscan-Server einzusetzen, die parallel oder in einer Hierarchie angeordnet sein können.

Konfiguration

4

4.1 Einleitung

Mit Symantec Endpoint Protection V12.1 wurden erstmals zusätzliche Funktionen über den klassischen Virenscanner hinaus freigegeben. Die nachfolgenden Konfigurationen beziehen sich auf die zentral verwaltete Variante des SEP ab V12.1, die mittels SEP Manager konfiguriert wird. Des Weiteren wird nur auf eine englische Installation eingegangen. Alle beschriebenen Konfigurationen sind Abweichungen von den Default Konfigurationen, das heißt nicht beschriebene Einstellungen werden nicht verändert.

Bitte beachten Sie

Folgende Einstellung ist unbedingt nötig für den stabilen Betrieb von PCS 7. Unter Clients->My Company->Policies->External Communication Settings:

Submission Settings	Allow Insight lookups for thread detection	Uncheck

Ist diese Option aktiv, versucht der Virenscanner bei jedem Dateiscan, direkt Symantec Server im Internet zu kontaktieren. Wenn der Virenscanner die Server nicht erreicht, kommt es zu extremen Verzögerungen. Diese machen einen stabilen Betrieb von PCS 7 unmöglich.

Alle anderen Haken unter Submission Settings sollten ebenfalls entfernt werden, um keine internen Informationen, wenn auch anonym, an Symantec zu senden. Die anderen Haken haben aber keinen negativen Einfluss auf PCS 7.

Client Restart

Clients sollten niemals automatisch neu gestartet werden. An zwei Stellen sollte ein automatischer Neustart abgeschaltet werden.

Unter “Clients->My Company->Policies->General Settings:

Restart Settings	Restart method	No restart

Unter Admin->Client Install Settings eine neue Policy erzeugen:

Restart Settings	Restart method	No restart

4.2 Überblick SEP Module und Funktionen

SEP hat folgende, über Policies konfigurierbare Module (zu finden im SEP Manager unter Policies):

- Virus and Spyware Protection
- Firewall

- Intrusion Prevention
- Application and Device Control
- LiveUpdate
- Exceptions

Des Weiteren folgende Einstellungen (zu finden im SEP Manager unter Clients > Policies > Location- independent Policies and Settings):

- Custom Intrusion Prevention
- System Lockdown
- Network Application Monitoring

Für den Einsatz im PCS 7 und WinCC Umfeld sind folgende Module und Einstellungen empfohlen und auf Verträglichkeit getestet:

- Virus and Spyware Protection
- Intrusion Prevention
- Device Control
- LiveUpdate
- Network Application Monitoring

Folgende Module und Einstellungen sind nicht empfohlen und werden im Verträglichkeitstest nicht geprüft:

- Firewall – Nur die Windows-Firewall ist für den Einsatz mit PCS 7 und WinCC freigegeben, da diese automatisch, je nach installiertem Produkt, konfiguriert wird.
- Application Control – Hierbei handelt es sich um rechnerspezifische Einstellungen, die nicht geprüft werden können.
- "Exceptions – Hierbei handelt es sich um anlagenspezifische Einstellungen, die nicht geprüft werden können.
- Custom Intrusion Prevention – Hierbei handelt es sich um anlagenspezifische Einstellungen, die nicht geprüft werden können.
- System Lockdown – Hierbei handelt es sich um rechnerspezifische Einstellungen, die nicht geprüft werden können.

Es sollten daher keine Policies für diese Module zugewiesen werden und die Einstellungen nicht "On" geschalten werden. Der Einsatz nicht empfohlener Module und Einstellungen erfolgt auf eigene Verantwortung.

4.3 SEP Module und Funktionen

4.3.1 Allgemein

In allen zu konfigurierenden Policies gibt es neben den Optionen kleine Schlösser. Es wird empfohlen alle Schlösser zu "schließen" (durch Anklicken). Dadurch wird sichergestellt, dass die Konfiguration der Virenscan-Clients nicht lokal verändert werden kann.

Aus dem gleichen Grund wird empfohlen unter Clients-> Policies-> Location-specific Settings-> Client User Interface Control Settings: Server Control und Customize anzuklicken und dort alle Hacken außer bei "Display the client" und bei "Display the notification area icon" zu entfernen.

4.3.2 Virus and Spyware Protection

Die nachfolgenden Konfigurationen beziehen sich auf eine neu erstellte Default Policy.

Windows Settings-> Scheduled Scans-> Scans->Administrator-Definded Scans	Daily Scheduled Scan	Delete

Windows Settings-> Protection Technology-> Auto-Protect-> Actions-> Actions	First action	Leave alone (log only)

Windows Settings-> Protection Technology-> Auto-Protect-> Actions-> Remediation	Terminate processes automatically	Uncheck

Windows Settings-> Protection Technology-> Auto-Protect-> Actions-> Remediation	Stop services automatically	Uncheck

Windows Settings-> Protection Technology-> Auto-Protect-> Notifications-> Notifications	Display the Auto-Protect result dialog on the infected computer	Uncheck

Windows Settings-> Protection Technology-> Download Protection-> Download Insight	Enable Download Insight to detect potential risk in downloaded files based on file reputation	Uncheck

Windows Settings-> Protection Technology-> Download Protection-> Actions-> Malicious files	First action	Leave alone (log only)

Windows Settings-> Protection Technology-> Download Protection-> Actions-> Unproven files	Specify action for unproven files	Leave alone (log only)

Windows Settings-> Protection Technology-> Download Protection-> Notifications-> Notifications	Display a notification message on the infected computer	Uncheck

Windows Settings-> Protection Technology-> SONAR-> SONAR Settings	Enable SONAR	Uncheck

Windows Settings-> Email Scans-> Internet Email Auto-Protect-> Scan Details	Enable Internet Email Auto-Protect	Uncheck

Windows Settings-> Email Scans-> Microsoft Outlook Auto-Protect-> Scan Details	Enable Microsoft Outlook Email Auto-Protect	Uncheck

Windows Settings-> Email Scans-> Lotus Notes Email Auto-Protect-> Scan Details	Enable Lotus Notes Email Auto-Protect	Uncheck

Windows Settings-> Advanced Options-> Miscellaneous-> Notifications-> Notifications	Display error messages with a URL to a solution	Uncheck

4.3.3 Intrusion Prevention

Die nachfolgenden Konfigurationen beziehen sich auf eine neu erstellte Default Policy.

Keine Änderungen nötig.

4.3.4 Application and Device Control

Die nachfolgenden Konfigurationen beziehen sich auf eine neu erstellte Default Policy.

Nur die Verwendung von Device Control, um zum Beispiel die Verwendung von USB-Geräten zu verhindern, wird empfohlen.

Unter "Application Control" sollten alle Haken entfernt werden.

4.3.5 LiveUpdate

Die nachfolgenden Konfigurationen beziehen sich auf eine neu erstellte Default Policy.

Die Einstellungen um den Symantec Update-Server im Internet zu erreichen oder einen überlagerten Update-Server, müssen der jeweiligen Netztopologie angepasst werden.

Windows Settings-> Schedule-> Live-Update Scheduling	Enable LiveUpdate Scheduling	Uncheck

Windows Settings-> Advanced Settings-> User Settings	Allow the user to manually launch LiveUpdate	Uncheck

Windows Settings-> Advanced Settings-> User Settings	Allow the user to modify HTTP, HTTPS, or FTP proxy settings for LiveUpdate	Uncheck

4.3.6 Network Application Monitoring

Diese Einstellung sollte nur von Administratoren mit guten Netzwerk- und Security-Kenntnissen benutzt werden und auf Anlagen mit einer eigenen Security-Administration.

Die Einstellung "Network Application Monitoring" befindet sich unter "Clients-> My Company-> Policies-> Location-independent Policies and Settings-> Network Application Monitoring".

Je nach Unternehmens- und Netz-Topologie muss hier die Vererbung geändert werden.

Network Application Monitoring	Enable network application monitoring	Check

Network Application Monitoring	When an application change is detected	Allow and Log