SIEMENS

SIMATIC

Prozessleitsystem PCS 7 Konfiguration McAfee VirusScan Enterprise 8.8 - White Paper

Applikationshandbuch

11/2014
A5E31308718-Ab

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 Digital Factory
Postfach 48 48
90026 NÜRNBERG
DEUTSCHLAND

A5E31308718-Ab
℗ 11/2014 Änderungen vorbehalten

Inhaltsverzeichnis

Vorwort

1

Wichtiger Hinweis zu diesem Whitepaper

Systemen getestet. 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.

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.automation.siemens.com (http://support.automation.siemens.com/WW/view/de/10154608)

Administration von Virenscannern 2

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.

2.1 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.

2.2 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:

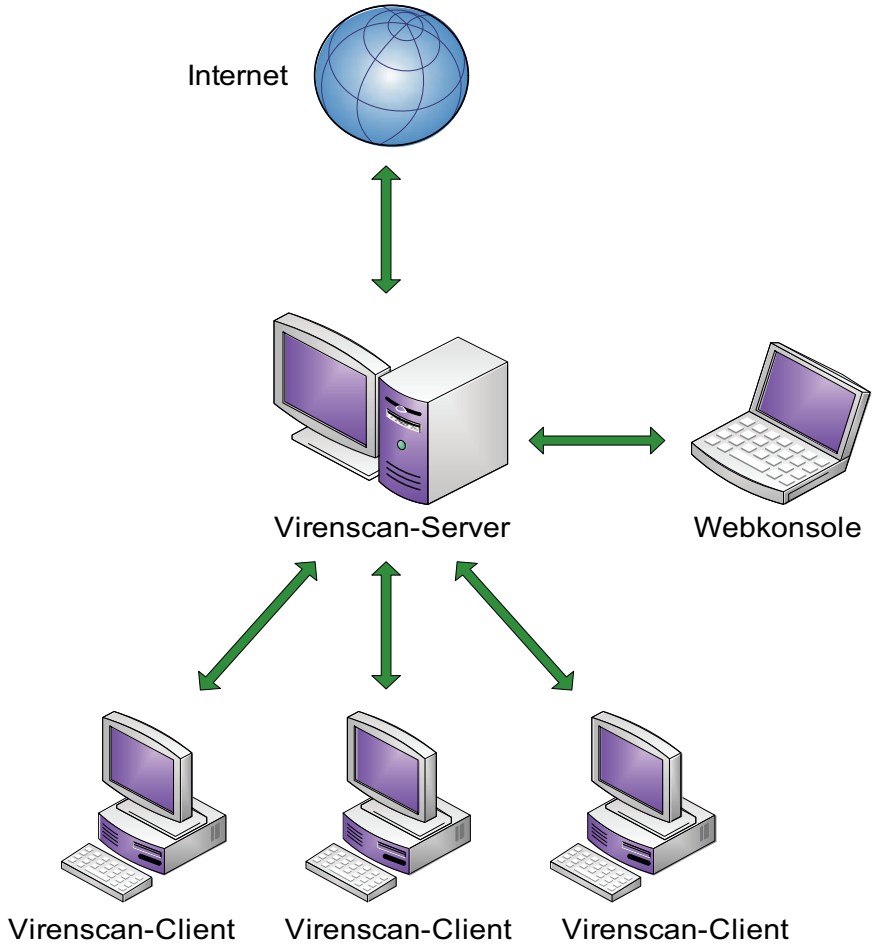
- Bei Einsatz einer Security-Suite (Virenscanner plus Optionen) müssen alle Optionen, die über die Funktionen eines klassischen Virenscanner hinausgehen, deaktivierbar sein, z.B. Firewall, E-Mail-Scan.
- Das Senden von Daten oder Berichten bei Virenfund an Virenscanner-Hersteller muss deaktivierbar sein.
- 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.

2.3 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 McAfee VirusScan Enterprise 3

3.1 Einleitung

Mit McAfee VirusScan Enterprise (VSE) 8.8 werden erstmals zusätzliche Funktionen, über den klassischen Virenscanner hinaus freigegeben. Die nachfolgenden Konfigurationen beziehen sich auf die zentral verwaltete Variante des VSE, die mittels McAfee ePolicy Orchestrator (ePO) 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.

3.2 VSE Funktionen

VSE hat folgende, über Policies konfigurierbare Funktionen (zu finden in der ePO unter "Policy Catalog"):

- "Access Protection"
- "Alert"
- "Buffer Overflow Protection"
- "General Options"
- "On Delivery Email Scan"
- "On-Access Default Processes"
- "On-Access General"
- "On-Access High-Risk Processses"
- "On-Access Low-Risk Processses"
- "Quarantine Manager"
- "Unwanted Programs"

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

- "Access Protection" (bedingt)
- "Alert"
- "Buffer Overflow Protection"
- "General Options"
- "On-Access Default Processes"
- "On-Access General"
- "Quarantine Manager"
- "Unwanted Programs"

Folgende Funktionen sind nicht empfohlen und werden im Verträglichkeitstest nicht geprüft:

- "On Delivery Email Scan" – Der Einsatz von Email-Programmen ist auf PCS 7 und WinCC Rechnern nicht empfohlen.
- "On-Access High-Risk Processses" – Diese Funktion ist eine Verfeinerung der "On-Access General" Funktion. Es wird aber empfohlen alle PCS 7 und WinCC Rechner gleich zu konfigurieren und alle Daten gleich zu behandeln.
- "On-Access Low-Risk Processses" – Diese Funktion ist eine Verfeinerung der "On-Access General" Funktion. Es wird aber empfohlen alle PCS 7 und WinCC Rechner gleich zu konfigurieren und alle Daten gleich zu behandeln.

Es sollten daher keine Policies für diese Funktionen zugewiesen werden. Der Einsatz nicht empfohlener Funktionen und Einstellungen erfolgt auf eigene Verantwortung.

3.2.1 Allgemein

Es wird empfohlen für alle PCS 7 und WinCC Rechner die gleichen Policies zu verwenden und für Workstation und Sever die gleichen Einstellungen vorzunehmen.

3.2.2 Access Protection

Die nachfolgenden Konfigurationen beziehen sich auf eine neue Policy, abgeleitet von der McAfee Default Policy.

Es werden nur die McAffe Default Einstellungen auf Verträglichkeit untersucht. Jede Änderung ist anlagenspezifisch und kann daher nicht untersucht werden.

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

3.2.3 Alert

Die nachfolgenden Konfigurationen beziehen sich auf eine neue Policy, abgeleitet von der McAfee Default Policy.

Keine Änderungen nötig.

3.2.4 Buffer Overflow Protection

Die nachfolgenden Konfigurationen beziehen sich auf eine neue Policy, abgeleitet von der McAfee Default Policy.

Buffer Overflow Protection

Buffer overflow settings-> Enable buffer overflow protection	Warning mode	Select

Client system warning	Show the messages dialog box when a buffer overflow is detected	Uncheck

3.2.5 General Options

Die nachfolgenden Konfigurationen beziehen sich auf eine neue Policy, abgeleitet von der McAfee Default Policy.

Display Options

System tray icon	Show the system tray icon with minimal menu options	Select

Console options	Allow this system to make remote console connections to other systems	Uncheck

Console options	Disable default AutoUpdate task schedule	Select

Console options	Enable splash screen	Uncheck

Password Options

User interface password	Password protection for all items listed	Select; choose a password

3.2.6 On-Access Default Processes

Die nachfolgenden Konfigurationen beziehen sich auf eine neue Policy, abgeleitet von der McAfee Default Policy.

Scan Items

Scan files	When reading from disk	Uncheck

Scan files	Opened for backup	Uncheck

Compressed files	Scan inside archives (e.g. .ZIP)	Check

Compressed files	Decode MINE encoded files	Check

Actions

When a thread is found	If the first action fails, then perform this action	Deny access to files

When an unwanted program is found	If the first action fails, then perform this action	Deny access to files

3.2.7 On-Access General

Die nachfolgenden Konfigurationen beziehen sich auf eine neue Policy, abgeleitet von der McAfee Default Policy.

General

Artemis (Heuristic network check for suspicious files	Sensitivity level	Disabled

ScriptScan

ScriptScan-Exeptions	Processes	Add bfmappersrvx.exe

Blocking

Block the connection	Block the connection when a threatened file is detected in a shard folder	Uncheck

Messages

User messages	Show the messages dialog box when a threat is detected and display the specified text in the message	Uncheck

Actions available to user	Remove message from the list	Uncheck

Actions available to user	Clean files	Uncheck

3.2.8 Quarantine Manager

Die nachfolgenden Konfigurationen beziehen sich auf eine neue Policy, abgeleitet von der McAfee Default Policy.

Keine Änderungen nötig.

3.2.9 Unwanted Programs

Die nachfolgenden Konfigurationen beziehen sich auf eine neue Policy, abgeleitet von der McAfee Default Policy.

Keine Änderungen nötig.

3.2.10 Pattern Updates

Das Verteilen von Pattern- und anderen Updates wird nicht über die McAfee VirusScan Policies konfiguriert, sondern über "Produkt Update" Client Tasks des McAfee Agents. Es wird empfohlen Pattern zeitversetzt zu aktualisieren. Nähere Informationen dazu im Sicherheitskonzept "Detaildokument Administration von Virenscannern".