Whitepaper

Schutz von Produktionsrechnern mit Windows 7 – Am 14. Januar 2020 beendet Microsoft den Support

Autor:
Andreas Fuss
Produktmarketing Security
Phoenix Contact Electronics GmbH
afuss@phoenixcontact.com

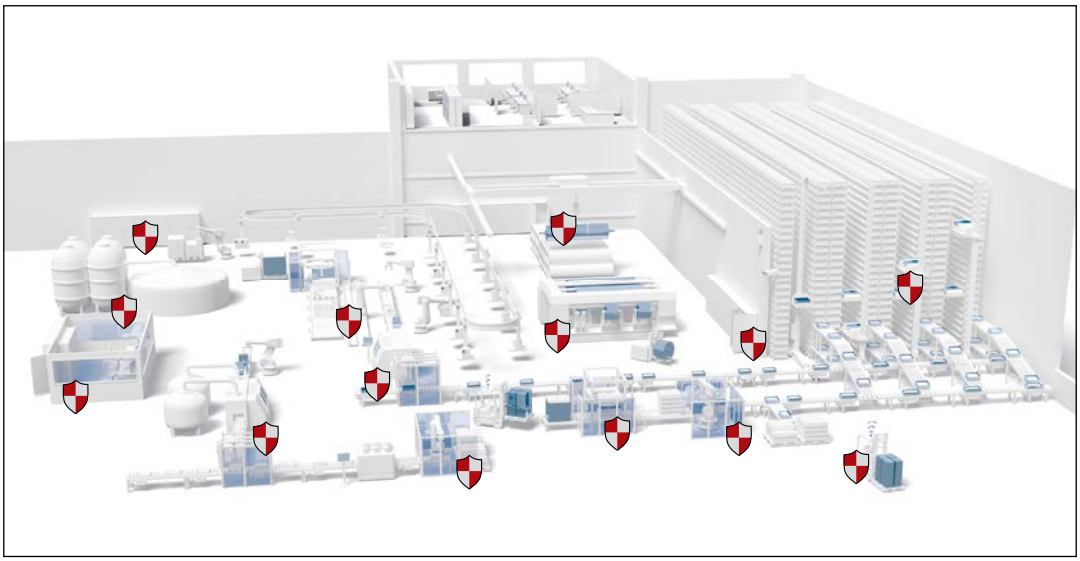
AI 05-19.000.L6

Schutz von Produktionsrechnern mit Windows 7

Anwendung

Am 14. Januar 2020 endet der erweiterte Support für Microsoft Windows 7 und am 13. Oktober 2020 endet ebenfalls der Support für Windows 7 Embedded. Nach dem Support-Ende stellt Microsoft keine Updates mehr zur Verfügung, um neue Sicherheitslücken zu schließen. Dadurch steigt täglich das Sicherheitsrisiko, dass Angreifer in Produktionsrechner mit Windows 7-Betriebssystem eindringen, oder dass diese von Viren, Trojanern oder Würmern befallen werden. Da häufig die gesamte Sicherheitsarchitektur dieser betagten Betriebssysteme nicht mehr dem aktuellen Stand der Technik entspricht, warnt Microsoft – ebenso wie Sicherheitsexperten – vor einem ungeschützten Weiterbetrieb. Aktuelle Umfragen zeigen jedoch auch, dass speziell in der Produktion auf den Einsatz von Steuerungsrechnern mit Windows 7 auch nach dem Support-Ende häufig nicht verzichtet werden kann. Es stellt sich also die Frage, wie diese Anwendungen zukünftig abgesichert werden können.

Lösung



IT-Sicherheit für Produktionsanlagen mit dem mGuard-Security-Modul

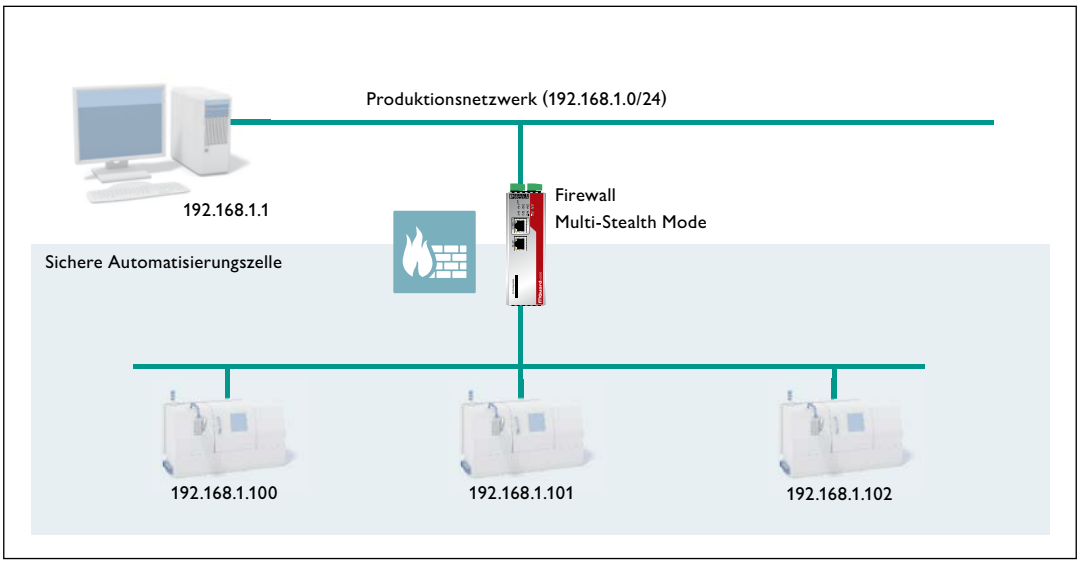
IT-Sicherheit für Produktionsanlagen

Grundsätzlich sollten natürlich ausschließlich sichere Systeme an das Produktionsnetzwerk angeschlossen werden. Die meisten Firmen verfügen bereits über entsprechende IT-Sicherheitsrichtlinien. Jedoch gilt gerade für Produktionsanlagen auch der Grundsatz „Never change a running System“. Das bedeutet, sowohl größere Änderungen an der Netzwerkinfrastruktur als auch ein Wechsel des Betriebssystems auf eine neuere Windows-Version sind in den meisten Anwendungen ausgeschlossen. Entweder erfüllen die Rechnersysteme gar nicht erst die nötigen Anforderungen für das neue Betriebssystem, oder aber notwendige Treiber sind nicht mehr verfügbar. Oft sind zudem die Auswirkungen eines entsprechenden Updates auf das Echtzeitverhalten des Rechners als kritisch einzustufen oder seitens des Maschinenherstellers sind gar keine Update-Möglichkeiten vorgesehen. In allen Fällen stehen der

potenziellen Steigerung der IT-Sicherheit hohe Kosten und Risiken bezüglich der Produktivität der Maschine gegenüber. Aus diesem Grund ist es vorteilhaft, Sicherheitsmaßnahmen durchzuführen, die ohne einen Eingriff in das zu schützende System funktionieren und einfach nachgerüstet werden können.

Schutz durch Nachrüstung von Security Appliances

Eine sichere und preiswerte Lösung ist die Nachrüstung mit einem mGuard-Security-Modul, einer industriellen Security-Appliance. Das mGuard-Security-Modul wird einfach vor dem gefährdeten Windows-PC in das Netzwerk integriert und sichert diesen PC gleich durch mehrere aufeinander abgestimmte Sicherheitsfunktionen ab. Dank einem patentierten Stealth-Modus müssen keine Änderungen am abzusichernden System durchgeführt werden: weder an der Netzwerk-infrastruktur, noch an dem eigentlichen Windows-Rechner. Das mGuard-Security-Modul kann somit auch nachträglich völlig transparent in ein bestehendes Netzwerk integriert werden. Da es dabei automatisch die MAC- und die IP-Adresse des zu schützenden Systems übernimmt, müssen nicht einmal zusätzliche Adressen für das Management der mGuard-Security-Module vergeben werden. Auch sonst bleibt die Netzwerkkonfiguration unverändert. Auf diese Weise lässt sich eine Produktionsmaschine mit Windows 7-Steuerungsrechner schnell, einfach und risikolos absichern.



Transparente Integration in bestehende Netzwerke dank patentiertem Stealth-Modus

Isolierung des Windows-Rechners durch eine Firewall

Vielen Sicherheitsrisiken ist gemeinsam, dass sie Schwachstellen von Protokollen oder Diensten ausnutzen. Schad-Software wird dann über bereits infizierte Systeme im IP-basierten Netzwerk weiter verbreitet. Um absolut sicher zu gehen, müssen also unsichere Systeme kommunikativ vollständig vom Produktionsnetzwerk abgekoppelt sein. In einer modernen Fertigung ist diese Entkopplung allerdings nicht praktikabel. Das Sicherheitsrisiko durch einen Windows 7-Rechner lässt sich aber minimieren, indem dieser Rechner so weit wie möglich vom restlichen Netzwerk isoliert wird. Die integrierte Firewall im mGuard kontrolliert und filtert die Kommunikation von und zu den zu schützenden Systemen anhand eines konfigurierbaren Regelwerks. Dadurch wird

die Kommunikation auf die Partner, Protokolle, Ports und Verbindungsrichtungen begrenzt, die für das Funktionieren der Gesamtanlage erforderlich sind. Verbindungen, die nicht vom System selbst initiiert werden, sondern von außen dort eingehen, werden größtenteils unterbunden. Auch die Kommunikation von innen nach außen lässt sich auf die notwendigen Dienste und Partner beschränken. Ein Zugriff auf das Internet sollte in jedem Fall geblockt werden.

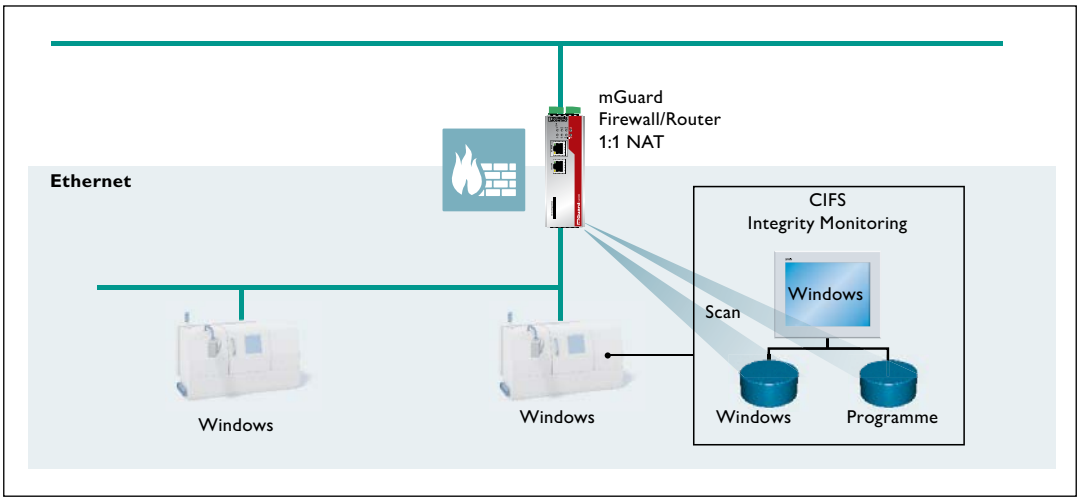
Schutz vor Viren durch CIFS-Integrity-Monitoring

Selbst die beste Firewall kann einem Windows 7-Rechner keinen 100 %-Schutz vor einer Virusinfektion bieten. Eine Schad-Software kann schließlich auch unbeabsichtigt durch einen Servicetechniker mittels Laptop oder USB-Stick direkt auf den PC gebracht werden. Daher ist eine kontinuierliche Überwachung des Windows 7-Rechners auf Befall durch Schad-Software notwendig. Jedoch stellt der Einsatz eines üblichen Viren-Scanner hohe Anforderungen an die Ressourcen des Steuerungsrechners, die die Echtzeiteigenschaften des Systems erheblich beeinträchtigen können. Zudem müssen kontinuierlich neue Virenpattern nachgeladen werden, um den Viren-Scanner auf einem aktuellen Stand zu halten.

Eine bessere Alternative ist das CIFS-Integrity-Monitoring (CIM) des mGuard.

CIFS (Common Internet File System) bezeichnet dabei das von Windows genutzte File-Sharing-Verfahren inklusive des Server Message Block-Protokolls SMB.

Bei CIFS-Integrity-Monitoring handelt es sich um einen Sensor, der das Dateisystem des Windows-Rechners auf Veränderungen überwacht und erkennt, ob dieser verändert wurde. Wird eine Veränderung festgestellt, alarmiert der mGuard den verantwortlichen Mitarbeiter sofort durch eine E-Mail oder per SNMP-Trap. CIFS-Integrity-Monitoring ist daher eine industrietaugliche Alternative zu herkömmlicher Antivirus-Software. Ihr besonderer Vorteil liegt darin, dass der Windows-Rechner kaum belastet wird und die Echtzeiteigenschaften des Systems nicht beeinflusst werden. Ein regelmäßiges Nachladen von Virenpattern ist mit dem mGuard nicht erforderlich.



Industrieller Virensensor: CIFS-Integrity-Monitoring

Unser Service – Ihr Security-Konzept

Bei Bedarf überprüfen unsere Spezialisten Ihr Netzwerk und erarbeiten auf Basis Ihrer Anforderungen ein individuelles Security-Konzept für Ihre Anlage. Darüber hinaus schulen wir Ihre Mitarbeiter im Hinblick auf industrielle Netzwerksicherheit.

Fazit

Der mGuard schützt den Produktionsrechner durch mehrere Sicherheitsfunktionen, ohne dass dessen Echtzeitfähigkeit beeinflusst wird:

1. Die integrierte Firewall isoliert den Windows 7-Rechner so weit wie möglich vom restlichen Netzwerk und lässt nur noch die benötigte Kommunikation zu.
2. Das CIFS-Integrity-Monitoring (CIM) bietet Schutz vor Viren.
3. Durch den patentierten Stealth-Modus kann das mGuard-Security-Modul einfach und ohne Änderungen an der Netzwerkkonfiguration nachgerüstet werden.

Unser Tipp

Der mGuard ist ausreichend leistungsfähig, um einen Fertigungsbereich mit mehreren Maschinen und Windows-Steuerungsrechnern zu schützen. Auf den ersten Blick erscheint dies als sehr kostengünstige Lösung. Eine Produktion muss jedoch flexibel bleiben und über die Jahre an neue Gegebenheiten oder Produkte angepasst werden, sodass Maschinen und ihre Standorte sich verändern können. Wird also über ein mGuard-Security-Modul ein ganzer Fertigungsbereich abgesichert, muss bei jeder Veränderung auch das Security-Konzept angepasst werden. Daher empfehlen wir, jede Maschine mit einem eigenen mGuard-Security-Modul abzusichern. Auf diese Weise bleibt der Schutz einzelner Maschinen auch bei Veränderungen in der Fertigung ohne zusätzlichen Aufwand erhalten.

Ihre Vorteile

- ☑ Keine Änderungen an der Netzwerkkonfiguration oder an den zu schützenden Systemen
- ☑ Schont die Ressourcen des geschützten/überwachten Systems (CPU-Leistung, Netzwerkbelastung)
- ☑ Kein Nachladen von Viren-Pattern erforderlich
- ☑ Keine Fehlalarme/False Positives bei der Integritätsprüfung
- ☑ Keine Beeinflussung des zu schützenden Systems

PHOENIX CONTACT Deutschland GmbH
Flachsmarktstraße 8
32825 Blomberg, Deutschland
Tel.: +49 5235 3-12000
Fax: +49 5235 3-12999
E-Mail: info@phoenixcontact.de
phoenixcontact.de