IT Security in der Fertigung

Das MC200/eMC200 Fernwartungsmodem

von Michael W. Folz

Zu Recht wird seit einiger Zeit die IT Security in der Fertigung verstärkt thematisiert. So zeigten einige der kürzlich bekannt gewordenen Virenattacken die Verletzbarkeit jedes vernetzten Systems. Insbesondere ist deutlich geworden, wie wehrlos ein standardisiertes System großflächig angelegten Attacken von außen gegenüber steht. Einige bekannte Opfer des „sobig.a“ Angriffs nutzten diverse Derivate der bekannten Microsoft Windows Betriebssysteme, wie z.B. Windows NT oder Windows 2000, gegen die sich die häufigsten Angriffe richten. Fatal ist hierbei, dass die Attacke in diesem Fall auf dem gleichen Mechanismus (OPC) beruhte wie auch der de facto Standard in PC-gestützter Automatisierung und Visualisierung. Dies erschwert die Abwehr aller vergleichbaren Viren massiv. Eine wirkungsvolle Defensive gibt es nicht, neue Sicherheitslücken in den Microsoft Betriebssystemen werden nahezu täglich entdeckt.

Aus der Sicht des Verantwortlichen in IT Security scheint hierbei die einzige Lösung zu sein, jeden Zugriff von außen auf vernetzte Systeme in Fertigungsanlagen grundsätzlich zu blockieren oder zumindest streng zu reglementieren. Dieser Ansatz ist auf den ersten Blick einfach und dennoch höchst effektiv. Auf der anderen Seite jedoch werden hiermit auch sinnvolle Außenverbindungen unmöglich gemacht oder zumindest massiv erschwert, wie z.B. Verbindungen zur Fernwartung von Fertigungsmaschinen. Diese Entwicklung ist in sich höchst paradox: In den vergangenen Jahren war man ständig bemüht, die Service- und Wartungskosten der Anlagen durch entsprechende Fernwartungssysteme zu minimieren und gleichzeitig die Stillstandszeiten im Störungsfall der Fertigungsanlage durch schnellstmögliche Reaktion des Herstellers über Fernverbindungen zu reduzieren. Nun wird diese in sich positive Entwicklung aus der berechtigten Sorge um die Sicherheit in der Fertigung reversiert. Ohne zusätzliche Maßnahmen im Bereich IT Security bedeutet dies einen Rückschritt auf den Stand vor einigen Jahren.

Das MC200/eMC200 Fernwartungssystem

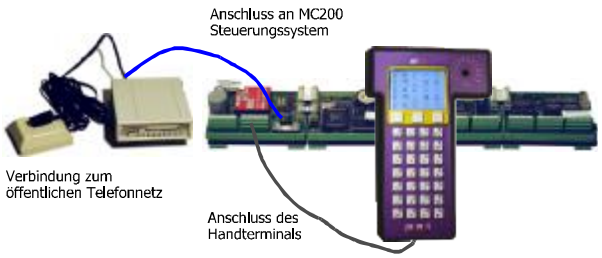

Abb. 1: MC200/eMC200 Fernwartung im autarken Betrieb

Dass es auch anders gehen kann, zeigt die Fernwartung für MC200/eMC200 Steuerungssysteme aus dem Hause MICRO DESIGN. Hier wird ein ganz anderer Ansatz verfolgt, um die Sicherheit des Systems gegen Angriffe von außen zu gewährleisten. So wird im Steuerungssystem selbst keinerlei Fremdsoftware eingesetzt. Das gesamte Betriebssystem ist genauso wie der Fernwartungskern eine Eigenentwicklung des Unternehmens. Da weder die Quellcodes öffentlich zugänglich sind noch das verwendete Prozessorsystem (Infinion SAB80C166 sowie Zilog Z180) eine marktbeherrschende Stellung einnimmt, ist ein Angriff auf dieses System höchst unwahrscheinlich, wenn nicht sogar nahezu unmöglich. Der Zugriff auf die Steuerung ist ausschließlich über eine proprietäre Zugangssoftware möglich – ebenfalls eine Eigenentwicklung aus dem Hause MICRO DESIGN. Hinzu kommt, dass das MC200/eMC200 Steuerungssystem für den autarken Betrieb ausgelegt ist: PC-Komponenten, z.B. für eine Visualisierung, greifen niemals auf den Kern des Steuerungssystems zu, sondern kommunizieren über ein serielles Protokoll mit einer abgesicherten Schicht innerhalb der Steuerung.

Die eMC200HUB Anschlussbox

Verwendet man die MC200/eMC200 zusammen mit einem eMC200HUB, erscheint dies zunächst weitaus gefährlicher: Hier sind an einer Anschlussbox PC, Modem und Steuerungen verbunden.

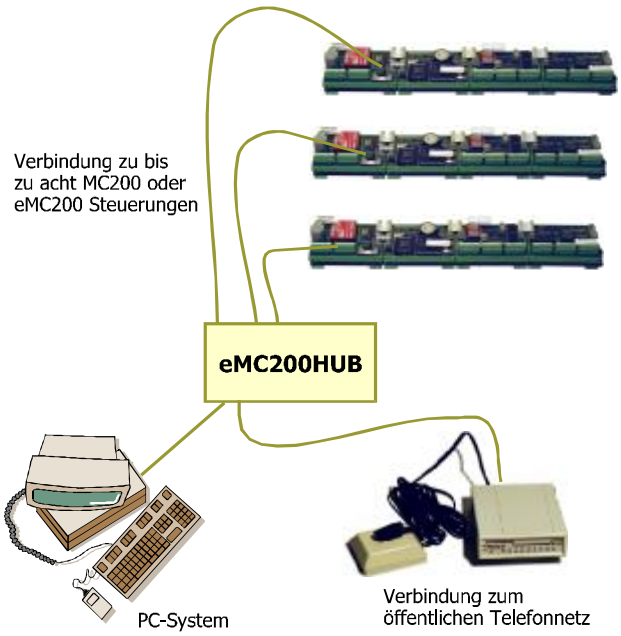

Abb. 2: MC200/eMC200 Fernwartung mit eMC200HUB

Jedoch wurden auch hier höchst effektive Maßnahmen ergriffen, um jeden Zugriff von außen auf den angeschlossenen PC zu verhindern: sobald eine Modemverbindung besteht, schaltet die eMC200HUB Anschlussbox per Hardware die Verbindung zum PC ab. Das System funktioniert hier wie ein Switch: nur einer der beiden Teilnehmer PC und Modem kann eine Verbindung zu den Steuerungen aufbauen. Eine Manipulation dieser Schaltung ist quasi unmöglich, da die Umschaltung nicht per Software oder Firmware, sondern über eine Gatterschaltung erfolgt.

Gesichertes Protokoll

Als letzte theoretische Möglichkeit bliebe einem potentiellen Angreifer der Weg, über das Modem destruktiven Code in das Steuerungssystem einzuspielen, um nach Abbruch der Modem-verbindung diesen Code an den PC weiterzuleiten und dann im Netzwerk zu verbreiten. Diese Alternative wird aber durch zwei grundsätzliche Eigenschaften des MC200/eMC200 Systems unmöglich gemacht: Zum einen arbeiten die MC200/eMC200 Steuerungen, wie bereits oben erwähnt, nicht mit Standardbetriebssystemen. Ein potentieller Angreifer müsste zunächst detaillierte Kenntnis über das verwendete Betriebssystem und den Prozessorkern erhalten, um einen Angriff überhaupt vorzubereiten. Und selbst dann wäre ein solcher Angriff alles andere als trivial, sind doch die Prozessorsysteme in der Steuerung nicht vergleichbar mit einem PC-Prozessorsystem und der Programmcode nicht kompatibel.

Des Weiteren funktioniert die Kommunikation zwischen Steuerung und PC nach dem Challange-System: Die Steuerung sendet niemals von sich aus Informationen an den PC, sondern stets nur auf Anfrage. Selbst wenn die Steuerung auf irgendeinem, wenn auch noch so unwahr–scheinlichen Weg mit schädlichem Code infiziert wurde, kann sie diesen Code nicht an den PC weitergeben, da dieser selbst entscheidet, welche Daten aus der Steuerung abgefragt werden.

Schutz vor fremdem Zugriff

Aus den vorstehenden Fakten geht eindeutig hervor, dass es praktisch unmöglich ist, über die Fernwartungsverbindung einer MC200/eMC200 Steuerung schädlichen Code auf einen angeschlossenen PC zu übertragen oder diesen Code gar in einem Netzwerk weiter zu verbreiten. Noch nicht ausgeschlossen wurde jedoch die Möglichkeit, über ebendiese Modemverbindung den Ablauf der Fertigungsanlage als solches zu stören, also ohne die Absicht, schädlichen Code auf einem PC zu installieren.

Natürlich würde ein solcher Angriff auf die Fertigungsanlage als solche zunächst einmal voraussetzen, dass der Angreifer detaillierte Kenntnis über das verwendete Steuerungssystem besitzt und in der Lage ist, sich die Entwicklungsoberfläche, das Programmiersystem und die Fernwartungssoftware „zu besorgen“ und in Betrieb zu nehmen. Unter diesen Umständen wäre ein potentieller Angreifer theoretisch in der Lage, Zugriff auf die Steuerung zu erlangen und das in der Steuerung laufende Programm zu löschen oder mit einem ungültigen Programm zu überschreiben.

Doch auch auf diesen Angriffspunkt wurde bei der Entwicklung des MC200/eMC200 Fernwartungs-systems Rücksicht genommen: Jede einzelne Steuerung kann vom Benutzer mit einem individuellen Fernwartungskennwort versehen werden. Nur mit Kenntnis dieses Kennworts kann ein potentieller Angreifer Zugriff auf das Steuerungssystem erhalten. Wird das Kennwort nicht oder fehlerhaft eingegeben, bricht die proprietäre Fernwartungssoftware die Verbindung automatisch ab.

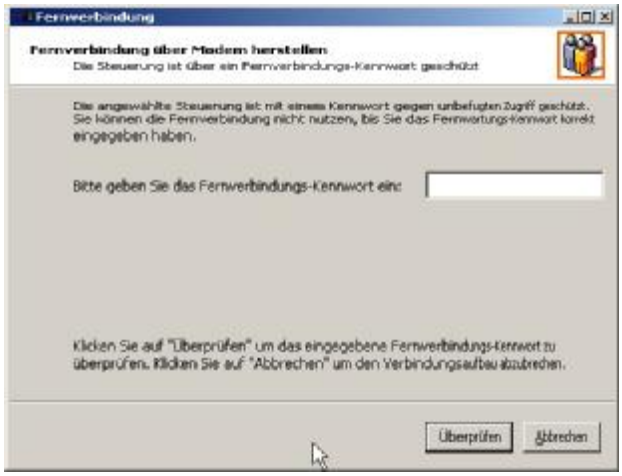

Abb. 3: Abfrage des Modemkennworts

Dem Maschinenbauer bzw. Anlagenbauer obliegt es, wie eine Änderung des Kennworts für Fernverbindungen in die SPS-Software integriert wird. Die häufigste Variante ist, das Kennwort entweder beim Einschalten der Anlage anzuzeigen (und änderbar zu machen), oder diese Abfrage in einem Konfigurationsmenü zu hinterlegen.

Fazit

Natürlich kann kein Computersystem jemals als absolut sicher bezeichnet werden. Beim Fern-wartungssystem für MC200/eMC200 Steuerungen wurden jedoch alle nur erdenklichen Vorsichts-maßnahmen getroffen, um einen Angriff von außen so schwer und damit so unwahrscheinlich wie nur möglich zu machen. Hierbei ist noch einmal hervor zu heben, dass ein solcher Angriff aufgrund des Aufbaus der Hardware niemals direkt gegen einen angeschlossenen PC gerichtet sein kann, sondern, wenn überhaupt, sich nur gegen das Ablauf-programm der Steuerung richten kann. In der Summe machen alle genannten Voraussetzungen und Maßnahmen die MC200/eMC200 Steuerungen auch bei einem Anschluss an das Telefonnetz zu einem sichern System.

Die MICRO DESIGN Industrieelektronik GmbH entwickelt und fertigt seit mehr als 20 Jahren Steuerungssysteme für den Maschinenbau. Weitere Informationen zum Unternehmen und zur Produktpalette erhalten Sie im Internet unter http://www.microdesign.de.

Über den Autor:
Michael W. Folz leitet bei MICRO DESIGN den Bereich Entwicklung und Marketing. Er war an der Konzeption des MC200/eMC200 Fernwartungssystem maßgeblich beteiligt. Bei Rückfragen erreichen Sie ihn unter der E-Mail Adresse mf@microdesign.de.