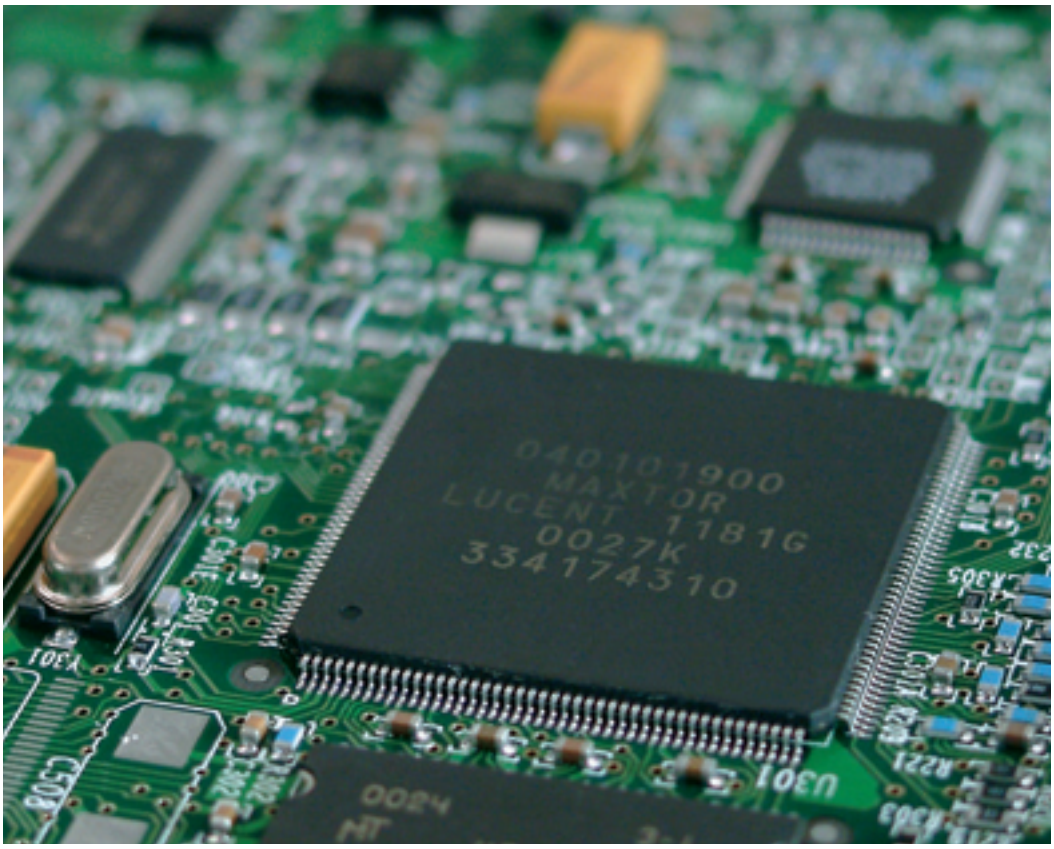
Der Hacker in der Waschmaschine

RISIKEN DER WACHSENDEN VERNETZUNG SICHERHEITSKRITISCHER SYSTEME

Steuerungen mit Internetzugang bieten nicht nur enormes Potenzial, sie bergen auch große Sicherheitsrisiken. Denn nicht nur der autorisierte Nutzer kann kilometerweit entfernt sein – auch Hacker können ihre Angriffe aus der Ferne starten. Am Fachgebiet Echtzeitsysteme werden Sicherheitsbarrieren entwickelt, die unerlaubte Zugriffe aufhalten.



Das Internet wird in fast allen Bereichen des Lebens immer gegenwärtiger.

Das Handy ruft E-Mails ab, der MP3-Player holt sich die Musik aus dem Netz und demnächst meldet die Waschmaschine eine Störung selbstständig dem Kundendienst.

Dass Geräte des Alltags in zunehmender Zahl sehr leistungsfähige Mikroprozessoren enthalten, nehmen wir kaum wahr. Ebenso wird es bald zur Selbstverständlichkeit gehören, wenn diese Kleinrechner ständig online erreichbar sind und sich zur Erfüllung ihrer Aufgaben selbständig des Internets bedienen.

Auch in der Industrie dringt die Vernetzung bis in die »letzte Ecke« vor.

So ist etwa Online-Wartung von Fertigungsanlagen bis hinunter zum einzelnen Sensor schon mit den heute verfügbaren Komponenten möglich und teilweise bereits realisiert. Dabei kann der Techniker entweder im Leitstand neben der Anlage sitzen oder auch sich über Tausende von Kilometern per Internet dazu schalten.

Ferner wird die unmittelbare Prozessdatenübermittlung der weltweit verteilten Produktionsstandorte zur Zentrale vom Management gewünscht, um auf Störungen oder andere Ereignisse rechtzeitig reagieren zu können.

Die Fusion von Automatisierungs- und Informationstechnik scheint nur noch eine Frage der Zeit zu sein.

Die ehemals sehr spezialisierten Steuerungen werden dazu mit zahlreichen neuen Funktionen versehen. So ist ein Webserver längst Standard in aktuellen Lösungen, oft auch ein FTP-Zugang oder die Möglichkeit, per E-Mail Benachrichtigungen zu versenden.

Doch welchen Einfluss hat diese Funktionsvielfalt auf die Sicherheit der Systeme?

Nur Fiktion?

Ein Waschmaschinenhersteller verkauft sein neuestes Modell mit eingebautem Web-Interface zur komfortablen Bedienung über einen Internet-Browser.

Ein Fehler in der Software ermöglicht jedoch auch eine unautorisierte Fernsteuerung der Maschine. Ein Angreifer kann bei geöffneter Tür den Wasserzulauf aktivieren und somit nicht unerheblichen Schaden anrichten.

Nachdem sich Vorfälle häufen und die Presse die Sicherheitslücke aufdeckt, ist der Hersteller zu einer Rückrufaktion gezwungen, um Soft- und Hardware mit verbesserten Sicherheitsfunktionen zu versehen.

Neben den finanziellen Verlusten erleidet das Unternehmen vor allem einen langfristigen Imageschaden.

Die Fertigungsstraße einer Fabrik basiert auf einer verteilten Steuerung, die auch mit dem Firmennetzwerk verbunden ist.

So können die Prozessdaten jederzeit bequem aus dem Büro abgerufen werden. Eine Firewall schirmt die Anlage vor unbefugten Zugriffen aus dem Internet ab. Daher war man bislang der Meinung, die Kommunikation intern ohne besondere Schutzmechanismen erlauben zu können.

Jedoch verrät ein entlassener Mitarbeiter einen Trick, wie die Firewall umgangen werden kann. Die Konkurrenz engagiert daraufhin einen Hacker, der tagelang brisante Prozessdaten aus der Steuerung abrufen kann. Anschließend legt er die gesamt Fertigung durch das Versenden sinnloser Befehle lahm.

Dies sind nur zwei fiktive Szenarien, die jedoch inzwischen der Realität sehr nahe kommen.

Neue Gefahren

Die Angreifer und ihr Vorgehen werden sich zunächst kaum von denen unterscheiden, die bereits heute Web-Server, Online-Shops oder Firmendatenbanken attackieren.

Ihre Motive sind vielfach ein falsch verstandener »sportlicher Ehrgeiz« oder auch gewöhnliche kriminelle Energie, die sich lediglich moderner Mittel bedient. Ihr Ziel besäße aber eine völlig neue Qualität: Schutzmechanismen in Anlagensteuerungen verhindern Arbeitsunfälle, zur Ferndiagnose vernetzte medizinische Geräte halten Menschen am Leben, Prozessleitrechner in der chemischen Industrie regeln die Herstellung gefährlicher Stoffe.

Das Problem ist also nicht nur der womöglich größere finanzielle Schaden, wobei schon jetzt etwa der Ausfall eines Online-Shops verheerende Auswirkungen für den Anbieter haben kann.

Steuerungssysteme tragen vielfach Verantwortung für die körperliche Unversehrtheit von Menschen, sei es direkt, wie in der Medizin, oder indirekt, wie in der Energieversorgung. Gerade unter diesem Gesichtspunkt wird oft auf einen möglichen Cyber-Terrorismus hingewiesen, der sich das hohe Schadenpotenzial zu Nutze machen könnte.

Während in Europa der Problematik bislang kaum Aufmerksamkeit gewidmet wird, existieren in den USA schon verschiedene Bestrebungen, zu übergreifenden Lösungen zu gelangen.

So hat sich das Process Control Security Requirements Forum der Aufgabe angenommen, Sicherheitsstandards für Hersteller und Anwender vernetzter Prozesssteuerungen zu erarbeiten. Ein ähnliches Ziel verfolgt das SP99-Komitee der Instrumentation, Systems, and Automation Society (ISA).

Auch politisch werden in den USA diese Bemühungen unterstützt, etwa im Rahmen der Homeland Security. So entstand ein Strategiepapier, das Gefahren aufzeigt und Vorschläge für Gegenmaßnahmen des Staates und vor allem der betroffenen Wirtschaft formuliert.

Abbildung 1 (links)
Eingebettete Systeme, wie sie in vielen elektronischen Geräten zu finden sind, werden zunehmend um Internetdienste erweitert.

Abbildung 2 (oben)
Plug and Play? Sicherheit spielt beim Anschluss von Steuerungen an das Internet bisher nur eine untergeordnete Rolle.

Bewährte Konzepte

Steuerungssysteme wurden bislang durch ein robustes Gehäuse, einen verschlossenen Raum oder auch den Werkschutz relativ zuverlässig abgeschirmt.

Mit der Vernetzung sind sie jedoch einer völlig anders gearteten Bedrohung ausgesetzt. Der Angreifer muss nicht mehr vor Ort sein. Er kann zudem sehr viele Ziele gleichzeitig ins Visier nehmen. Und oft ist er durch die computergestützte Vorgehensweise erheblich schneller, als ein menschlicher Operator reagieren kann.

Ein Blick auf die Struktur von Schutzsystemen unserer realen Alltagswelt zeigt, welche Konzepte sich dort bewährt haben.

So besteht beispielsweise der Diebstahlschutz eines Autos zunächst aus verschließbaren Türen, die den Innenraum absichern. Auf diesem Weg werden Personen mit nur begrenzter krimineller Energie davon abgehalten, Gegenstände geringeren Werts aus dem Fahrzeug zu entwenden. Den erheblich größeren Wert, das Auto selbst, sichern jedoch das Zündschloss und die Wegfahrsperre als zusätzliche Mechanismen ab.

Es wird deutlich, dass physikalischer Schutz umso mehr Stufen aufweist, je wichtiger und wertvoller das zu sichernde System ist. Ferner greifen die effektivsten Verfahren tief im Inneren an, da hier das Verhältnis Aufwand zu Nutzen günstiger ist.

Eine Bank würde niemals einen einfachen Holzschrank als Tresor verwenden und stattdessen das Gebäude mit aufwendigen Barrikaden und Zugangskontrollen umgeben.

Ein weiterer, sehr wichtiger Vorteil eines mehrstufigen Sicherheitskonzepts ist der Zeitfaktor.

Um eine realistische Chance auf Erkennung und Abwehr zu wahren, darf die Zeit zwischen Beginn und Abschluss eines erfolgreichen spurenverwischenden Angriffs nicht gegen Null gehen.

Genau das ist jedoch der Fall, wenn nur eine Barriere zu überwinden ist. Erst wenn mehrere Mechanismen nacheinander ausgeschaltet werden müssen, ist eine zeitnahe Aufdeckung möglich, und Gegenmaßnahmen können rechtzeitig eingeleitet werden.

Virtuelle Sicherheit

Betrachtet man nun die vernetzte virtuelle Welt, so findet sich dort das beschriebene Prinzip der gestaffelten, zum kritischen Kern hin stärker werdenden Mechanismen keineswegs so ausgeprägt wieder wie zu vermuten wäre.

Das Internet selbst besitzt praktisch keine Sicherheitshierarchie, diese kann erst am Zugangspunkt (das Modem des Heim-PCs, die Verbindungsleitung zum Internet-Provider, etc.) wirksam werden. Eine Firewall, die unautorisierten oder manipulierten Datenverkehr herausfiltert, stellt in der Regel die erste Stufe dar – vielfach jedoch auch die einzige. Sicherheitsmechanismen der angeschlossenen Systeme wie etwa Passwörter oder Verschlüsselungsverfahren werden nur unzureichend genutzt oder gar unter Verweis auf die Firewall ganz abgeschaltet.

Die Beschränkung der Sicherheit erfolgt aus einer Abwägung, welche die komfortable und kostengünstige Nutzung höher einstuft als das meist zu niedrig eingeschätzte Risiko eines signifikanten Schadens. Derartige Annahmen dürfen aufgrund der beschriebenen Gefahr, die Angriffe auf Steuerungssysteme darstellen, keinesfalls übernommen werden.

Doch selbst die konsequente Anwendung von Sicherheitsmechanismen der klassischen IT stieße schnell an Grenzen. Die Besonderheit von Steuerungssystemen, zu jeder Zeit Entscheidungen schnell und zuverlässig treffen zu müssen, verbietet beispielsweise den Einsatz zeitaufwendiger Autorisierungs- oder Verschlüsselungsverfahren. Eine Steuerung darf sich nicht erst lange mit der Überprüfung von Sicherheitsregeln beschäftigen, bevor sie den Befehl zur Notabschaltung einer Werkzeugmaschine ausführt.

Lösungsansätze für mehr Sicherheit

Am Fachgebiet Echtzeitsysteme wird daher nach Möglichkeiten gesucht, bewährte starke Sicherheitsmechanismen so zu modifizieren, dass sie auch den strikten Zeitanforderungen von Anwendungen der Automatisierungstechnik genügen.

Ziel ist es, Technologien und Verfahren zu entwickeln, die einen umfassenden, im Systemkern ansetzenden Entwurf von Sicherheitskonzepten für vernetzte Steuerungen erlauben.

So wurde bereits das Sicherheitsmodell Domain and Type Enforcement (DTE), das auch in einem von der National Security Agency (NSA) entwickelten Sicherheitsbetriebssystem SELinux zum Einsatz kommt, für eine Verwendung in echtzeitfähigen Systemen angepasst.

Es erlaubt eine nicht umgehbare Unterteilung des Systems in voneinander getrennte Bereiche, die unterschiedliche Prioritäten und Berechtigungen besitzen können.

Kritische Systemfunktionen, die beispielsweise direkt Aktoren in einer Fertigungsanlage ansteuern, lassen sich so zuverlässig von weniger kritischen abgrenzen, welche die Internetverbindung des Systems herstellen sollen.

Insgesamt wird der Wiederverwertung von Konzepten sowie deren Umsetzungen in Software besondere Aufmerksamkeit gewidmet.

Dafür spricht nicht nur die Zeit- und Kostenersparnis.

Auch unter Sicherheitsgesichtspunkten ist die Verwendung bewährter Komponenten vorteilhaft, da neue Software in der Regel zunächst eine Vielzahl unentdeckter Design- und Implementierungsfehler und damit potenzieller Sicherheitslücken enthält.

Eine schnelle Aufdeckung und Beseitigung dieser Fehler setzt jedoch eine eingehende Kontrolle der zugrundeliegenden Quelltexte voraus.

lösen. So stehen zur Absicherung des Datentransportes über das Internet ausgereifte Open-Source-Implementierungen von Standards wie IPSec, SSL oder SSH zur Verfügung.

Auch aus diesem Grund basieren viele Systeme, die im Rahmen der Arbeiten am Fachgebiet Echtzeitsysteme entstehen, auf Open-Source-Produkten. Umgekehrt wurden bereits eigene Entwicklungen auf dieser Basis veröffentlicht, weitere Projekte insbesondere im Rahmen der Forschungsarbeit über sichere Steuerungen sollen folgen.

Prof. Dr.-Ing. Bernardo Wagner
Jahrgang 1957, ist Geschäftsführender Leiter des Fachgebiets Echtzeitsysteme am Institut für Systems Engineering.

Dipl.-Ing. Jan Kiszka
Jahrgang 1975, ist wissenschaftlicher Mitarbeiter im Fachgebiet Echtzeitsysteme am Institut für Systems Engineering.

Abbildung 3
Hacker-Angriffe auf Steuerungssysteme von Industrieanlagen oder Kraftwerken können nicht nur zu erheblichen finanziellen Schäden führen, sondern auch Menschen gefährden.
Foto: KUKA Schweißanlagen GmbH

Literatur

- ISA – The Instrumenation, System, and Automation Society, SP99-Komitee, http://www.isa.org
- President's Critical Infrastructure Protection Board, The National Strategy to Secure Cyberspace, 2002, http://www.whitehouse.gov/pcipb/cyberstrategy-draft.html
- Rich Merrit, Is Your System Secure?, Control Magazine, Putman Media, August 2001, http://www.controlmag.com
- Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, Inc., 2000
- Morrie Gasser, Building a Secure Computer System, Van Nostrand Reinhold, 1988

Ausblick

Aufgrund der begrenzten Entwicklungsressourcen selbst großer Unternehmen bietet sich gerade für sicherheitskritische Komponenten das Open-Source-Modell an.

Es setzt nicht nur auf die Offenlegung der Quelltexte, sondern ermöglicht jedem, sie zu korrigieren oder weiterzuentwickeln. Aus diesem Software-Pool kann bereits jetzt geschöpft werden, um viele elementare Sicherheitsprobleme vernetzter Steuerungen zu

Sicherheit ist in hohem Maße ein gesellschaftliches Interesse. Sie lässt sich hingegen nach wie vor nur schlecht als wertsteigernde Produkteigenschaft verkaufen.

Eine gemeinschaftliche Entwicklung grundlegender Werkzeuge und Richtlinien durch viele Beteiligte aus Industrie und Wissenschaft kann deshalb zu einem schnelleren und nachhaltigeren Fortschritt führen als das Vertrauen auf das Verantwortungsbewusstsein der einzelnen Hersteller.

So könnte auch die Wahrnehmung dieser Problematik verbessert und der Austausch darüber angeregt werden.

Denn Sicherheit erfordert eine kontinuierliche Beschäftigung, nicht nur einzelne Maßnahmen.