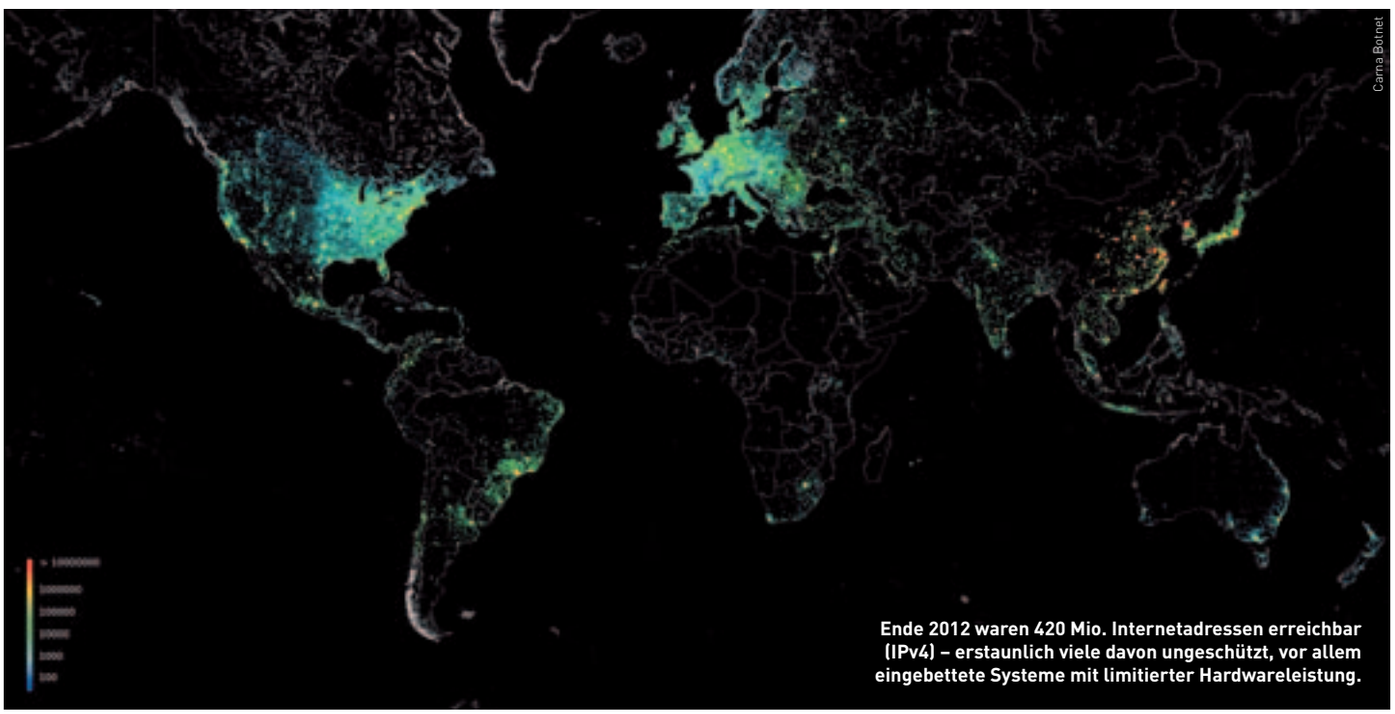
Business Software

Statt spezielle Hardware zu entwickeln, werden Funktionen immer häufiger mit Software realisiert, die auf einem eingebetteten Rechner läuft. Das bietet neue Möglichkeiten wie die Anbindung an das Internet, aber zugleich auch Sicherheitsrisiken, die beachtet werden müssen. Wer noch einen Schritt weiter geht, kann mit der Software sogar Hardware simulieren, um mechanische Risiken auszuschliessen.



Ende 2012 waren 420 Mio. Internetadressen erreichbar (IPv4) – erstaunlich viele davon ungeschützt, vor allem eingebettete Systeme mit limitierter Hardwareleistung.

Angriffe auf eingebettete Systeme

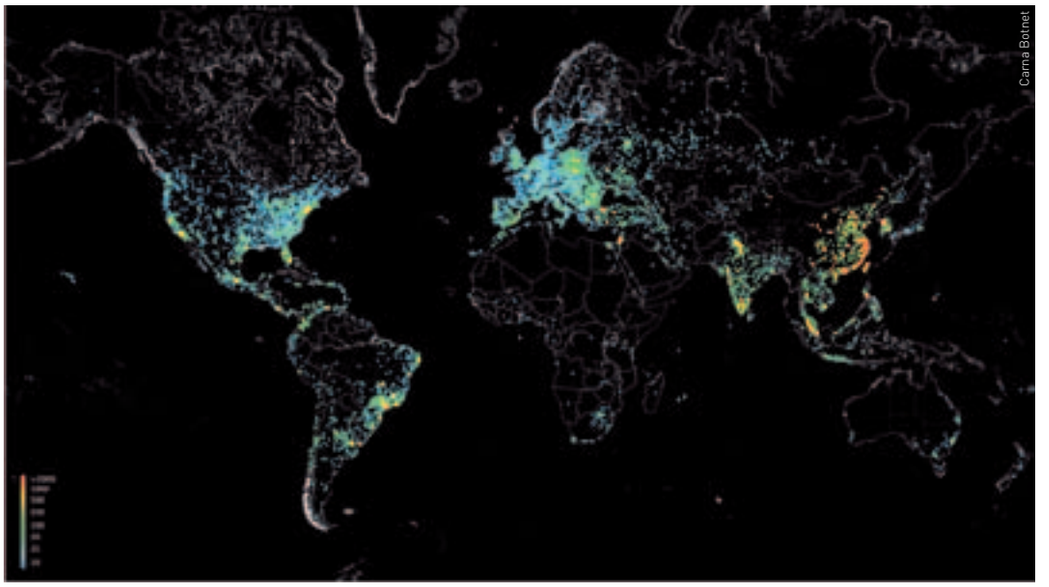
Die eingebettete Elektronik ist heute so leistungsfähig, dass viele Produkte über das Internet kommunizieren könnten. Die Security ist aber oft der Spielverderber: Die Vernetzung führt auch zu Angriffen. Einige konkrete Fälle wurden in der letzten Zeit publik. Die Systeme müssen deshalb geschützt werden, wie es bei PCs und Servern schon lange üblich ist.

«Hunderttausende von privaten Netzwerkkomponenten gekapert», «Echte Bedrohung durch digitale Terrorangriffe auf kritische Infrastrukturen» – solche Schlagzeilen machten in den letzten Monaten auf die Risiken aufmerksam, die die Vernetzung von Steuerungen und Maschinen sowie kleinen und kleinsten Geräten über das öffentliche Internet mit sich bringt. Dass diesen Risiken ein Nutzen gegenübersteht, ist unbestritten. Doch müssen die Sicherheit gewährleistet und so die Risiken begrenzt werden.

Seit einiger Zeit sind nicht mehr nur Arbeitsplatzrechner und Server vernetzt mit dem Internet, sondern auch vielerlei eingebettete Systeme, in denen der Laie teilweise gar keinen Computer im herkömmlichen Sinn erkennt. Die Bandbreite der vernetzten Systeme reicht von privaten Endgeräten wie Druckern, Webcams, VoIP-Telefonen, Spiegelreflex-Digitalkameras, netzwerkfähigen Bilderrahmen und NAS über eingebettete Systeme im professionellen Umfeld wie in der Gebäudeautomation und in industriellen Steuerungen bis hin zu Industrieanlagen und kritischen Infrastrukturen in der Strom- und Wasserversorgung.

Erfolgreiche Angriffe

Vor einigen Monaten wurde ein Experiment bekannt, bei dem innert kürzester Zeit 420 000 komplett ungeschützte und mit dem Internet verbundene Geräte wie Firewalls, Router, Drucker oder Kameras unter Kontrolle gebracht wurden (internetcensus2012.bitbucket.org). Der Angriff war möglich, da selbst die rudimentärsten Schutzmassnahmen vernachlässigt wurden: Die Geräte hatten kein Passwort oder das im Werk voreingestellte Standardkennwort.
Der Autor setzte den Angriffscode nach eigenen Angaben nicht für negative Zwecke ein, es wäre aber leicht gewesen, die entsprechenden Netzwerke auszuspionieren oder einen gross angelegten, verteilten Angriff auf ein anderes Ziel zu starten.
Auch die Sicherheitslücke in der Steuereinheit einer Heizanlage für kleine Wohnhäuser erregte vor Kurzem Aufsehen: Laut Heise.de sollen unberechtigte Zugriffe möglich sein, wenn die



Die Internetadressen wurden von dem hier abgebildeten Botnet gezählt, das aus rund 420 000 Embedded-Systemen bestand, die nicht passwortgeschützt waren oder «root» resp. «admin» als Passwort akzeptierten.

Heizanlage mit dem Internet verbunden ist. Der Hersteller forderte darauf die Kunden auf, die Geräte vom Internet zu trennen, bis ein Servicetechniker ein Softwareupdate installiert hat.

Kamera gekapert

Dass moderne Spiegelreflexkameras netzwerktauglich und angreifbar sind, wurde im Februar bekannt: Wird eine solche Kamera mit dem Internet verbunden – auch über ein öffentliches WLAN im Hotelzimmer oder am Flughafen – ist das Gerät Angriffen ausgeliefert, die den Zugriff auf die Kamerafunktionen und die gespeicherten Bilder ermöglichen.
Potenzielle Angreifer sind bereits auf der Suche nach weiteren Zielen, wie eine Studie der Sicherheitsfirma Trend Micro zeigt: Dazu verbanden die Forscher simulierte Industriecomputer mit dem Internet, sogenannte «Honeypots», die sich als industrielle Steuerungsanlagen mit vermeintlichen Schwachstellen ausgaben. Bereits kurze Zeit später konnten Angriffe aus einer Vielzahl von Ländern auf diese Systeme beobachtet werden, darunter auch bislang unbekannte Angriffsarten.
Der 2010/11 öffentlich gewordene Fall des Computerwurms Stuxnet weicht bezüglich des Angriffswegs von den obigen Beispielen ab, da die betroffenen Systeme nicht direkt mit dem Internet verbunden waren. Dennoch erlaubt die Attacke zwei Erkenntnisse: Für einen Angriff muss das Zielsystem nicht direkt erreichbar sein. Es reicht, auf irgendeinem Weg ein System zu kompromittieren, von dem aus wiederum ein direkter oder indirekter Zugriff auf das Ziel möglich ist. Ausserdem hat Stuxnet gezeigt, dass auch dauerhafte Ausfälle durch physische Zerstörung möglich sind – im Iran wurden Zentrifugen zerstört, indem Stuxnet die Drehzahl veränderte.

Kombination von Ursachen

Die Gründe, weshalb die geschilderten Angriffe möglich sind und in der Anzahl zunehmen, haben damit zu tun, dass die Anzahl der mit dem Internet verbundenen Geräte stark zunimmt. Privatanwender schliessen die Geräte – oft unbedacht – ungeschützt ans Internet an, um bequem von irgendwo auf der Welt darauf zugreifen zu können. Offenbar sind sich aber auch Anwender aus dem industriellen Umfeld der hohen Risiken einer direkten Internet-Anbindung von eingebetteten Systemen wenig bewusst, wie das bayerische Fernsehen in der Sendung Kontrovers vom 6. März zeigte. Vielfach wird schlicht nicht wahrgenommen, dass es sich bei den Geräten genauso um potenziell anfällige Computer handelt wie bei Desktop-PCs oder Servern. Verschärft wird das Problem durch technische Faktoren: Eingebettete Systeme sind häufig nicht sehr leistungsfähig, weshalb Schutzmassnahmen oft minimal ausfallen. Zudem ist die Aktualisierung der Software/Firmware vielfach nur mit hohem Aufwand möglich, weshalb sie von den Betreibern vernachlässigt wird. Sicherheitslücken bleiben somit unnötig lange bestehen. Wenn dazu noch Dienste aktiviert sind, für die kein Bedarf besteht, steigt das Risiko weiter.

Identische Passwörter

Die Authentisierung zeigt häufig ebenfalls Schwachpunkte: Entweder wird von zugreifenden Personen und Systemen gar keine oder nur eine mangelhafte Authentisierung verlangt. Oft sind die Passwörter bei allen Geräten identisch und weithin bekannt. Damit auch technisch weniger versierte Personen die Geräte in Betrieb nehmen können, ist die Standardkonfiguration häufig unsicher – damit alle angepriesenen Eigenschaften möglichst problemlos genutzt werden können. Dazu kommen Protokolle, mit denen Geräte sich und ihre Fähigkeiten öffentlich bekannt machen, um möglichst bequem vernetzt werden zu können, sowie verschiedene Massnahmen, die allfällige Sicherheitseinrichtungen wie Firewalls teilweise umgehen.
Letztlich gilt auch hier: Die hohe Sicherheit hat ihren Preis. Das sind höhere Entwicklungskosten, erschwerte Integration in die Zielumgebung und höhere Ansprüche an das Sicherheitsbewusstsein und die Fähigkeiten der Abnehmer, die nur durch Erfahrung und Schulung erreicht werden können. Doch während bei Sicherheitsanforderungen in der realen Welt (z.B. den Bremsen eines Autos) nur selten aus Kostengründen zu hohe Risiken in Kauf genommen werden, scheint dies in der Informatik bei eingebetteten Systemen anders zu sein.

Massnahmen

Verschiedene Massnahmen steigern die Sicherheit eingebetteter Systeme bis zu einem angemessenen Grad. Dringend nötig ist eine Bewusstseinsänderung bei den Abnehmern. Auch wenn die Hersteller es manchmal glauben machen wollen, können Planung und Inbetriebnahme keineswegs ad-hoc und ohne weitere Kenntnisse sicher vorgenommen werden. Das gilt gleichermassen für industrielle Nutzer wie Privatkunden, wobei naturgemäss Letztere schwer zu sensibilisieren sind. Hierzu kann eine Kombination aus Information über Angriffe und verschärfte Haftungsvorschriften dienen. Gerade im privaten Bereich stellt ein System, in das Angreifer eingedrungen sind, oft eine Bedrohung für andere dar, beispielsweise durch Teilnahme an verteilten Dienstblockaden-Angriffen. Im kommerziellen Umfeld, wo die Schäden oft im Unternehmen selbst anfallen (Ausfälle, dauerhafte Infrastrukturschäden, Reputation etc.), sollte ein Umdenken sowieso selbstverständlich sein. Dabei ist auch die Politik gefragt: An Betreiber kritischer Infrastrukturen müssen erhöhte Sicherheitsanforderungen gestellt werden – die auch nach-

Dieses Heizungssystem bot in seiner ursprünglichen Version offenen Zugriff, wenn es mit dem Internet verbunden war.

gewiesen werden sollen, ähnlich wie beim öffentlichen Transport oder den Betreibern potenziell umweltgefährdender Anlagen.

Technische Schranken

Auf technischer Ebene gibt es eine Vielzahl von Massnahmen: Gefährdete Systeme dürfen niemals direkt mit dem Internet verbunden werden, sondern über entsprechende Firewalls. Zudem braucht es eine Segmentierung der Netzwerkbereiche in Zonen unterschiedlicher Sicherheitsniveaus, damit erfolgreiche Angriffe auf die Büro-IT eines Unternehmens keinen Zugriff auf kritische Industrieanlagen ermöglichen. Beim Design eingebetteter Systeme sollen nur essenzielle Kernfunktionen eingebaut werden. Jeder Dienst, der nicht angeboten wird, erhöht die Sicherheit. Querschnittsfunktionalität wie zentrale Authentisierung, Logging, Aufbereitung von Benutzerinterfaces oder Netzwerkfilterung kann von dedizierten und auf diesen Zweck optimierten Komponenten bereitgestellt werden, auf denen Softwareupdates leichter vorgenommen werden können. Authentisierungsinformationen wie Passwörter und Schlüssel müssen unbedingt von ihren Standardwerten geändert werden. Hierzu kann der Systemlieferant einen Beitrag leisten, beispielsweise indem seine Software bei der Initialkonfiguration dies vom Benutzer verlangt. Falls Zugriffe von aussen nötig sind, z.B. für Wartungsarbeiten, sind geeignete Sicherheitsmassnahmen wie verschlüsselte Verbindungen vorzusehen. Unsichere Protokolle müssen deaktiviert werden. Schliesslich können auch die Medien ihren Teil beitragen: Testberichte sollten nicht nur Funktionalität und Usability bewerten, sondern auch die Sicherheit.

Spielregeln einhalten

Die Angriffe auf eingebettete Systeme sind heute real – betroffen sind sowohl Privatanwender als auch professionelle Nutzer bis hin zu Betreibern kritischer Infrastruktur. Das Bewusstsein, dass die Systeme geschützt werden müssen, muss geschärft werden. Wenn sich alle Nutzer an die Spielregeln halten, wird nicht der Hacker zum Spielverderber, sondern die Internet-Community verdirbt den Hackern das Spiel.

Peter K. Brandt ist Informatik-Ingenieur und bei Ergon Informatik AG im Bereich eingebetteter und mobiler Softwarelösungen tätig.
www.ergon.ch