Informatik aktuell

W. A. Halang
H. Unger (Hrsg.)

Internet der Dinge

Echtzeit 2016

Springer Vieweg

Informatik aktuell

Herausgegeben
im Auftrag der Gesellschaft für Informatik (GI)

Wolfgang A. Halang
Herwig Unger (Hrsg.)

Internet der Dinge

Echtzeit 2016

Fachtagung des gemeinsamen Fachausschusses
Echtzeitsysteme von
Gesellschaft für Informatik e.V. (GI),
VDI/VDE-Gesellschaft für Mess- und Automatisierungstechnik (GMA) und
Informationstechnischer Gesellschaft im VDE (ITG)
Boppard, 17. und 18. November 2016

GESELLSCHAFT FÜR INFORMATIK E.V.

VDI VDE VDI/VDE-Gesellschaft Mess- und Automatisierungstechnik

ITG INFORMATIONSTECHNISCHE GESELLSCHAFT IM VDE

Springer Vieweg

CR Subject Classification (2001): C3, D.4.7

ISSN 1431-472X

ISBN 978-3-662-53442-7 e-ISBN 978-3-662-53443-4
DOI 10.1007/978-3-662-53443-4

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist Teil von Springer Nature
Die eingetragene Gesellschaft ist Springer-Verlag GmbH Germany
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Wie bereits vor zwei Jahren mit dem Leitthema „Industrie 4.0“ nimmt diese Tagungsreihe erneut einen Modebegriff auf, um ihn vor dem Hintergrund jahrzehntelanger Erfahrung auf den Gebieten Echtzeit- und eingebettete Systeme sowie Prozessautomatisierung und -leittechnik auf seine Substanz und seinen Neuheitsgehalt hin abzuklopfen. Eine Definition[1] besagt, das „Internet der Dinge bezeichne die Vernetzung von Gegenständen mit dem Internet, damit diese Gegenstände selbstständig über das Internet kommunizieren und so verschiedene Aufgaben für den Besitzer erledigen könnten. Der Anwendungsbereich erstrecke sich dabei von einer allgemeinen Informationsversorgung über automatische Bestellungen bis hin zu Warn- und Notfallfunktionen.“

Häufig wird über lange Zeit Hergebrachtes in neue Moden übernommen[2]. Als Beispiele dafür seien bzgl. des Internets der Dinge hier nur die im letzten halben Jahrhundert evolutionär entwickelten Technologien eingebetteter Systeme und zustandsabhängiger vorbeugender Anlageninstandhaltung genannt. Allein in der Verwendung von mehr Prozessoren und Sensoren, weiterer Miniaturisierung sowie erheblich gesteigertem Datenaustausch erkennt der Automatisierungstechniker jedoch genauso wie im Falle von Industrie 4.0 nichts prinzipiell Neues.

In Bezug auf den Einsatz der Radiofrequenzidentifikation 1999 von Ashton als Begriff geprägt, befindet sich das Thema Internet der Dinge nach dem 2015 veröffentlichten „New Gartner Hype Cycle for Emergent Technologies“[3] derzeit auf dem Gipfel der Euphorie, worauf in der Regel der Fall in das Tal der Enttäuschungen folgt. Dies erscheint unausweichlich, denn wie so Vieles ist das Internet der Dinge ein zweischneidiges Schwert: Einerseits soll es Effizienz und Wettbewerbsfähigkeit erhöhen, öffnet aber andererseits Werksspionage und Sabotage Tür und Tor. Gemäß der Netzseite „Sicherheit für das Internet der Dinge“[4] stellt Sicherheit die größte Herausforderung des Internets der Dinge dar.

Dabei ergibt sich mangelnde funktionale Sicherheit in vernetzten Systemen als Folge der Gefahren durch Abhören, Verfälschen oder Abfangen von Daten bei deren Übertragung sowie der Möglichkeiten des Einschleusens von Malware und der Überlastung von Knoten, die der Einsatz ungeeigneter Artefakte, nämlich im Bürobereich verbreiteter Informationstechnik und des Internets als Übertragungsmedium, mit sich bringt. Weil dieses Gefahrenpotenzial bei klassischen Technologien der Automatisierungstechnik viel geringer – oder konstruktionsbedingt überhaupt nicht vorhanden – ist, haben wir es hier bei Licht betrachtet mit einem Rückschritt hinsichtlich der technischen Qualität zu tun.

---

[1] Springer Verlag (Hg.), Gabler Wirtschaftslexikon, Stichwort: Internet der Dinge, http://wirtschaftslexikon.gabler.de/Archiv/1057741/internet-der-dinge-v4.html

[2] P. Mertens und D. Barbian: Digitalisierung und Industrie 4.0 – Trend mit modischer Überhöhung? *Informatik Spektrum* 39, 4, 301–309, 2016

[3] http://www.gartner.com/newsroom/id/3114217

[4] http://www.iot-sicherheit.ch

Aufgrund der oben umrissenen Problemlage ist die erste Sitzung der Tagung der Sicherheit im Internet der Dinge gewidmet. Sie will für das Thema Datensicherheit sensibilisieren, indem Möglichkeiten zur Absicherung von Kommunikationsnetzen diskutiert und die zur Abschirmung von Code und Daten für verschiedene Isolationskonzepte entstehenden Kosten betrachtet werden. Als konkrete Problemlösung wird ein zum Patent angemeldetes Verfahren zur sicheren anonymen Aufwertung und Belastung elektronischer Geldbörsen vorgestellt.

Das Internet der Dinge ist ohne den Einsatz von Echtzeitbetriebssystemen an den verschiedensten Stellen undenkbar. Darum beschäftigt sich eine eigene Sitzung mit den bei der Entwicklung eines dezidierten Betriebssystemkerns zusammengestellten spezifischen kombinierten Echtzeit- und Sicherheitsanforderungen, einer modular geschichteten Systemarchitektur zur Verbindung heterogener Gerätetreiber mit gängigen Übertragungsprotokollen sowie mit einem Betriebssystemkern für mit Umgebungsenergie betriebene Komponenten, das bei seinen Einplanungsentscheidungen deren schwankende Verfügbarkeit berücksichtigt.

Wegen der entscheidenden Bedeutung von Planung wird in der dritten Sitzung eine Software-Bibliothek für Ausbildungszwecke präsentiert, die die Planung des Echtzeitverhaltens unterstützt. Der Ausbildung dient auch die in Entwicklung befindliche Programmierumgebung OpenPEARL, über deren Konsistenzprüfungskomponente berichtet wird. Für die sicherheitsgerichtete Echtzeitprogrammierung wurden auf der Basis von PEARL eine Grundsprache sowie für jede der vier Sicherheitsstufen nach IEC 61508 eine inhärent sichere Teilsprache definiert, deren Syntax die Einhaltung der jeweiligen Einschränkungen erzwingt.

Im Rahmen der Tagung beschäftigt sich schon immer eine Sitzung mit aktuellen Echtzeitanwendungen. Gemäß dem Fokus Internet der Dinge werden Kontrollverfahren für die dynamische Kommunikation zwischen mobilen Hausautomatisierungsgeräten vorgestellt, eine Steuereinheit für Bewegungen mit sechs Freiheitsgraden entwickelt und in ein System virtueller Realität eingebunden sowie Methoden der erweiterten Realität zur Navigation in Gebäuden genutzt.

In der abschließenden Sitzung wird zunächst am Beispiel der Fernsteuerung von Heizungen gezeigt, dass konsequente Trennung von Anwendungsbereichen mit und ohne Echtzeitanforderungen und Verwendung jeweils geeigneter Programmiersprachen zu besseren Lösungen führt. Weiterhin werden ein Testbett für in der Raumfahrt eingesetzte und auf NAND-Flash-Speichern residierende Dateisysteme mit Redundanz sowie ein hierarchisch-asynchrones Zuteilungsverfahren für Mehrkernprozessoren vorgestellt, das die Software eingebetteter Systeme zur Laufzeit phasenabhängig rekonfiguriert.

Frau Dipl.-Ing. Jutta Düring gebührt unser herzlicher Dank dafür, dass sie zum wiederholten Male die Einreichungen mit größter Sorgfalt redigiert und den vorliegenden Band konsistent und ansprechend gestaltet hat.

Hagen, im August 2016

Wolfgang A. Halang
Herwig Unger

Inhaltsverzeichnis

Software-Entwicklung und Ablaufsteuerung

Sichere Kommunikation im Umfeld von Industrie 4.0

Linus Schleupner

Lehrstuhl für Marktorientierte Unternehmensführung
Rheinische Fachhochschule Köln
linus.schleupner@rfh-koeln.de

Zusammenfassung. Kommunikationsnetze der Automatisierungstechnik in der Produktion von Gütern erfahren aktuell im Rahmen von Industrie 4.0 ebenso eine Veränderung wie der unternehmensinterne bzw. übergreifende Datenaustausch. Bisher als Insellösungen ausgeführte Netze mit proprietären Bussystemen werden bei neuen Maschinen und Anlagen vermehrt mit Ethernet ausgestattet und, z. B. zu Fernwartungszwecken, mit dem Internet oder mit cloud-Lösungen verbunden. Solche Netze können deshalb ohne Sicherungsmaßnahmen genauso von außen angegriffen oder ausgespäht werden wie jedes Büro- oder Heimnetzwerk. Der Angriff von W32.Stuxnet im Jahr 2010 und der Angriff auf das Netz des Deutschen Bundestages im Jahr 2015 haben gezeigt, dass die Wirkung von Schadsoftware bis zur Funktionsstörung von Atomanlagen und dem Zugriff auf streng geheime Unterlagen reichen kann. Deshalb müssen Kommunikationsnetze über eine im Rahmen der gegebenen Echtzeitbedingungen sichere Kommunikation verfügen, die sie gegen schädigende Einflüsse von innen und außen unempfindlich macht. Dieser Beitrag listet verschiedene Möglichkeiten zur (organisatorischen) Absicherung von Kommunikationsnetzen auf und soll weiter dafür sensibilisieren, dass Datensicherheit ernst genommen wird.

1 Einleitung

Die ständige Verfügbarkeit von Infrastrukturen z. B. bei Verarbeitungs- und Produktionsanlagen sowie Anlagen zur Energie- oder Wasserversorgung (sogenannte KRITIS Kritische Infrastrukturen) spielt für Unternehmen, Verwaltungen und private Haushalte eine große Rolle. Dort kommen automatisierte Prozesssteuerungssysteme, IndustriePC (IPC) mit Windows-Betriebssystemen und Office-Anwendungen sowie Supervisory Control and Data Acquisition-Systeme (SCADA) zur Steuerung der verschiedenen Funktionen und Abläufe in verteilten Strukturen zum Einsatz. Zur Vernetzung ihrer Komponenten nutzen diese Systeme immer häufiger die gleiche oder ähnliche Ethernet-basierte Netzstruktur wie Standard-Computernetze.

Das führt allerdings dazu, dass Automatisierungssysteme potenziell den gleichen Gefahren durch Viren, Würmer, Trojaner und unbedachte Nutzer ausgesetzt sind wie jeder Büro- oder Heim-PC. Konzepte zur datentechnischen Einbindung aller Komponenten einer automatisierten Anlage über Ethernet-Netze

werden durch Industrie 4.0 bereits realisiert. Geschäftsmodelle zur Auslagerung von Service- und Instandhaltungsaufgaben auf externe, ggf. nicht am Standort der Anlage ansässige Unternehmen, verstärken die potenziellen Risiken zusätzlich, ebenso wie die Vernetzung verschiedener Produktionsstandorte über Enterprise Ressource Planning-Systeme (ERP). Etablierte Schutzmaßnahmen aus der Büro-Informationstechnik lassen sich aber nicht 1:1 in die Automatisierungstechnik übertragen [1, 2]. Viele Prozesse, z. B. in Kraftwerken, Stahlwerken oder der Energieerzeugung können nicht einfach angehalten werden, um notwendige Updates von Betriebssystemen oder Virenschutzprogrammen mit anschließendem Systemneustart durchzuführen. Netzmonitore, Intrusion-Detection-Systeme (System zur Erkennung von Angriffen gegen Netze) und der Einsatz von Firewalls mit sehr restriktiven Regeln können zwar einen wichtigen Beitrag zum Schutz von Netzen leisten, ihr Einsatz kann aber die Funktionsfähigkeit und die Verarbeitungsgeschwindigkeit der Prozesssteuerungssysteme erheblich beeinträchtigen.

Die Wechselwirkungen zwischen Sicherheit in der Informationstechnik (IT-Sicherheit) und der Sicherheit von Prozesssteuerungssystemen werden seit einigen Jahren intensiv diskutiert [1]. Immer mehr Hersteller, Integratoren und auch Betreiber von Prozesssteuerungssystemen erkennen die Notwendigkeit geeigneter IT-spezifischer Sicherheitsmaßnahmen. Bei der Entwicklung vieler existierender und bereits im Einsatz befindlicher SCADA-Komponenten ist der Aspekt der IT-Sicherheit allerdings noch nicht ausreichend berücksichtigt worden. Sicherheitsmechanismen, wie Authentifizierung und Verschlüsselung, wurden in der Prozesssteuerungstechnik selbst nur unvollständig oder gar nicht implementiert. Insbesondere bei der Erstellung und Fortschreibung von Sicherheitskonzepten für ältere Prozesssteuerungssysteme wird die Gefahr weiterhin unterschätzt [1].

Die Sicherheit gegen Angriffe von außen wie Sabotage oder Manipulation ist in automatisierten Anlagen in jeder Hinsicht elementarer Bestandteil zur Sicherstellung von Verfügbarkeit, Zuverlässigkeit und Authentizität. Eine Unterbrechung der Produktion aufgrund sabotierter oder manipulierter Anlagen kann schwerwiegende Folgen nach sich ziehen. Vertragsstrafen können bei falsch produzierter Menge oder verzögerter Lieferung greifen oder Rückrufaktionen können bei mangelhafter Qualität die Folge sein. Auch können Anlagen beschädigt oder unbrauchbar werden, was mit Imageschäden oder hohem Geldverlust einhergeht. Angriffe auf Kraftwerke können zudem notwendige Energie- oder Stromversorgungen ausschalten. Deshalb ist das Gefahrenpotential groß.

Die zum heutigen Stand Mitte 2016 letzte große, bekannt gewordene Attacke ist das Einschleusen eines Trojaners in das Netz des deutschen Bundestages mit der Folge des Totalzusammenbruchs der Sicherheitsmaßnahmen. Hacker konnten über Monate hinweg unbemerkt hochsensible Daten abziehen [7].

Solche Angriffe müssen künftig zuverlässig verhindert werden.

2 Bedrohungen der Maschinenautomatisierung

Bedroht wird der Netzverkehr und damit der sichere Betrieb einer Maschine oder Anlage durch

- das Abhören und Verändern von Nachrichten (Snarfing, Janus-Angriffe),
- einen unbefugten Eingriff in die Maschinensteuerung,
- den Transport von Schadsoftware (mit oder ohne Schaden am Automatisierungssystem, als gezielter Angriff oder unbewusst eingeschleust),
- das überfluten des Netzes mit unnützem Datenverkehr bzw. Angriffe auf die Verfügbarkeit des Rechners (Denial-of Service-Angriff (DoS), Distributed Denial-of-Service-Angriff (DDoS)) mit der Unterscheidung Bandbreitensättigung, Ressourcensättigung und Systemabsturz [8],
- ferngesteuerte Bot-Netze (Zusammenschaltung mehrerer fremdgesteuerter Rechner zum Versenden von Schadsoftware).

Die Vorgehensweise bei Angriffen auf fremde Kommunikationssysteme mittels Trojanern hat mittlerweile eine neue Qualität erreicht. Während der klassische Verbreitungsweg über Datenträger immer noch eine nicht zu unterschätzende Gefahr darstellt, werden Angriffe immer häufiger mit spezieller, auf das Opfer zugeschnittener Spionagesoftware durchgeführt. Zunächst wird ermittelt, welche Vorlieben, Interessen oder Hobbys die Zielperson haben könnte, um sie mit einer entsprechenden E-Mail zu konfrontieren. Beim öffnen dieser Mail wird dann unbemerkt ein Trojaner platziert. Aktuelle Trojaner bzw. ganz neu auftauchende Trojaner werden oftmals von marktgängigen Schutzprogrammen nicht erkannt [9, 10].

Der im Juni 2010 bekannt gewordene Angriff der Schadsoftware W32.Stuxnet zur Sabotage von Kraftwerken, chemischen Fabriken und industrieellen Produktionsanlagen ist nur ein Beispiel, das zeigt, dass breit angelegte Sicherheitsmaßnahmen überlegt werden müssen. Über eine vorhandene Internetverbindung wird zuerst die PC- und dann gezielt die SPS-Ebene infiziert, um Anlagen zu manipulieren oder auszuschalten [3–5].

Es ist bekannt, dass zum Schließen von Sicherheitslücken notwendige Updates von Betriebssystemen, Antiviren- oder Anwenderprogrammen durchgeführt werden müssen. Und dies gilt nicht nur für PC-Lösungen, sondern für alle eingesetzten Komponenten, die ein Betriebssystem verwenden [11]. Heutzutage müssen Antiviren-Programme stündlich und Updates der Betriebssysteme sofort bei Verfügbarkeit aktualisiert werden, weil die Gefährdung für PC und IPC, mit Viren oder anderer Schadsoftware infiziert zu werden, als sehr hoch einzustufen ist [2, 9, 10].

Einer Studie des BSI zufolge haben bereits 63% der Internetnutzer persönliche Erfahrungen mit Viren und Würmern gemacht, 35% mit Trojanern und 19% mit Spionagesoftware. Die Tendenz ist weiter steigend [1]. Im gleichen Bericht wird festgestellt, dass nur 18% befragter Unternehmen mehr als 7,5% des IT-Budgets in IT-Sicherheit investieren. Ein Grund für diese geringe Zahl ist dem Bericht zufolge, dass bei mehr als der Hälfte der befragten Unternehmen das Bedrohungsrisiko für das eigene Unternehmen als gering eingestuft wird.

Updates von Betriebssystemen und Antivirenprogrammen müssen auch bei IPC vorgenommen werden. Das Aufspielen von Updates hat jedoch oftmals einen Neustart des Gerätes zur Folge. Der Neustart eines IPC bedeutet aber auch, dass der Prozess bzw. die Produktion angehalten werden muss, wenn kein Redundanzsystem zur Verfügung steht. Ungeplante Stillstandszeiten sind für Produktionsbetriebe nicht akzeptabel. Eine Stillstandszeit ist ein Produktionsstopp, durch den hohe Kosten durch Lieferverzögerungen entstehen können. Auch können z. B. Kraftwerksprozesse, chemische Prozesse oder Produktionsanlagen der Stahl-, Aluminium oder Kunststoffindustrie nur nach einer langwierigen Vorbereitung anhalten und wieder anlaufen. Updates müssen dementsprechend bei geplanten Stillständen eingespielt werden. Der Abstand solcher geplanter Stillstände hängt von den Wartungsintervallen der Maschinen und Anlagen ab und liegt erfahrungsgemäß zwischen wenigen Wochen und mehreren Monaten. Notwendige, wichtige Sicherheitsupdates der Betriebssysteme oder von Antivirus-Lösungen werden also nicht oder nur selten durchgeführt. Es liegt also ein Konflikt zwischen hoher Sicherheit und geringer Stillstandszeit vor.

In modernen Industrieanlagen werden nicht nur zunehmend Systeme lokal miteinander vernetzt, sie werden auch mit Fernwartungs- und Ferndiagnosesystemen ausgerüstet. Damit sollen über große Entfernungen Funktionalität, Service und Kundennähe gewährleistet sein, so, als ob ein Service-Techniker lokal vor Ort wäre. Jedoch werden dabei auch sensible Informationen wie Passwörter, Messdaten, Parameter und firmeneigenes Wissen übertragen. Sicherheitsrelevante Funktionen können fernwirksam geschaltet werden. Zeichnet ein Unbefugter eine solche offene Kommunikation auf, kann er jederzeit gefährdende Funktionen auslösen oder vertrauliche Informationen sammeln.

Das Problem stellt sich in der Varianz und dem Umfang der notwendigen Abwehrmaßnahmen bei gleichzeitiger Erlaubnis des Zugriffs auf die Maschinenautomatisierung und Geheimhaltung sensibler Daten dar. Darum sollten sich die notwendigen Schutzmaßnahmen von denen der Büro-IT unterscheiden, um einen praxisgerechten, sicheren Betrieb zu gewährleisten.

Grundsätzlich sind verschiedene Szenarien denkbar:

- Der Angreifer ist ein Mitarbeiter des Produktionsbetriebes und hat direkten Zugang zum Unternehmensnetz.
- Der Angreifer ist kein Mitarbeiter des Produktionsbetriebes, hat aber direkten Zugang zu diesem Unternehmen oder zum Unternehmensnetz, z. B. als externer Service-Mitarbeiter.
- Der Angreifer ist kein Mitarbeiter des Produktionsbetriebes, hat keinen direkten Zugang zum Unternehmen, jedoch zum Unternehmensnetz, z. B. durch Abhören eines Funknetzes.

Es kann also von innen oder von außen angegriffen werden.

In diesen Szenarien helfen Strukturanalysen, Schwachstellen aufzudecken. Schwachstellen sind notwendige Bedingungen, damit eine latent vorhandene Bedrohung einen Schaden bewirken kann. Schwachstellen können beseitigt werden, Bedrohungen sind jedoch ständig vorhanden. Durch ein Risikomanagement, zu

dem auch Strukturanalysen gehören, werden technisch und organisatorisch wirksame sowie wirtschaftlich sinnvolle Schutzmaßnahmen eingeleitet und Schwachstellen geschlossen [4].

In der Prozesstechnik treten Schwachstellen beispielsweise auf bei

- Automatisierungskomponenten und IPC,
- systemnaher Middleware (z. B. OPC-Server),
- Bedienterminals und
- Zugriffspunkten zu Netzen.

Aktuell wird als wirksamste Abhilfe gegen unbefugte Zugriffe die Beschränkung der zulässigen Kommunikation mit kritischen Maschinen- oder Anlagenteilen (Zellen) auf das operativ erforderliche Maß empfohlen. Möglich ist dies durch den Einsatz dezentraler Firewalls mit geeignetem Regelwerk, das entweder aus der Systemdokumentation abgeleitet oder aus einer Lernphase direkt am Netz gewonnen werden kann. Als Regel gilt: „Was nicht explizit erlaubt ist, ist verboten!“ [11].

3 Grundprinzipien sicherer Kommunikation

Sichere Kommunikation bedarf in jedem Anwendungsfall eines ganzheitlichen Ansatzes, bei dem (a) Personen (Motivation, Wissen, Fehler), (b) Prozesse (Richtlinien, Organisation) und (c) Produkte/Technologien (Hardware, Software, Netze) dynamisch zusammenwirken. Ein Bereich alleine reicht nicht aus, um Schutzziele abschließend zu definieren.

Die folgenden Grundprinzipien verdeutlichen den Anspruch an die Sicherheit, den ein zu implementierendes System erfüllen muss. Es sind

- *Vertraulichkeit/Zugriffsschutz*: Nur dazu berechtigte Netzteilnehmer sollen in der Lage sein, auf Nachrichten im Klartext zuzugreifen und diese auszutauschen. Solche Daten können von unberechtigten Teilnehmern nicht verstanden werden, eine nicht-autorisierte Informationsgewinnung ist also nicht möglich.
- *(Daten-)Integrität/Änderungsschutz*: Der Empfänger soll in der Lage sein, festzustellen, ob eine Nachricht verändert worden ist oder nicht. Daten können also ohne Kenntnis des Empfängers von einem Dritten nicht geändert werden.
- *Authentizität/Fälschungsschutz*: Der Empfänger einer Information soll klar und eindeutig erkennen können, von welchem Absender die Information stammt. Gesendete Daten stammen auch tatsächlich vom Absender, der Absender kann sich also gegenüber dem Empfänger zweifelsfrei ausweisen.
- *Verbindlichkeit/Nichtabstreitbarkeit*: Der Absender einer Information muss jederzeit die Urheberschaft einer Nachricht nachweisen können. Die Identität des Absenders ist Dritten gegenüber nachweisbar und nicht abstreitbar.
- *Anonymität*: Die Identität des Absenders bleibt Dritten gegenüber geschützt [4, 12, 13].

Das BSI hat im Rahmen der Studie „Kommunikations- und Informationstechnik 2010 – Trends in Technologie und Markt“ neben den verwendeten Sicherheitsverfahren untersucht, welche Sicherheitseigenschaften von Systemen künftig insbesondere in eingebetteten Systemen, z. B. bei Handys oder Tablets sowie bei Informationssystemen von Bedeutung sein werden. Es zeigte sich, dass sowohl kurzfristig als auch langfristig den Merkmalen Datenintegrität und Vertraulichkeit die größte Bedeutung beigemessen wird [14]. Das bedeutet, dass eine geschützte, geheime und zuverlässige Datenübertragung gewünscht wird.

4 Normen und Richtlinien

Um Anwender bei der Abwehr von Bedrohungen gegen Netze der Informationstechnik zu unterstützen, wurden basierend auf anerkannten Regeln der Technik verschiedene Normen und Vorschläge entwickelt.

Relevant für den Schutz von informationstechnischen Netzen und Anlagen sind insbesondere:

- der Lagebericht des BSI,
- BSI-Standards wie der „Leitfaden IT-Sicherheit (IT-Grundschutz kompakt)“ des BSI,
- die DIN ISO 27000 und
- VDI-Richtlinie 2182.

5 Der Lagebericht des BSI

Im Lagebericht des BSI werden

- Bedrohungen untersucht und bewertet, welche durch technische Sicherheitslücken und ihre Nutzung entstehen,
- Chancen und Risiken beim Einsatz innovativer Technologien aufgezeigt sowie
- Trends aus den Bereichen Wirtschaft, Gesellschaft, Technik und Recht präsentiert [1].

Er gibt einen Überblick über den Umgang mit der Informationstechnik und legt dar, welche Hilfen das BSI unterschiedlichen Zielgruppen an die Hand geben kann.

Der Bericht des Jahres 2007 stellt eine Zunahme des Gefährdungspotentials im Vergleich zum Jahr 2005 fest. Mit zunehmender Verlagerung von geschäftlichen und privaten Aktivitäten in die virtuelle Welt geht auch eine Professionalisierung und Kommerzialisierung der IT-Bedrohungen einher. Daraus resultiert eine auch zukünftig anhaltend hohe Bedrohungslage der IT-Sicherheit bei Privatanwendern, Unternehmen und Verwaltungen [1].

Im Jahr 2006 schon wurden 7.247 neue Sicherheitslücken in Betriebssystemen wie Windows und Programmen wie den Office-Paketen von Microsoft entdeckt. Auch der prozentuale Anteil jener Sicherheitslücken, die von Angreifern für den Zugriff auf ein verwundbares System ausgenutzt werden können, erhöhte

sich. 52,5% der im Jahre 2006 analysierten Schwachstellen eigneten sich dafür, Benutzer- oder sogar Administratorrechte zu erlangen, mit denen dann umfangreiche Manipulationen am PC möglich werden [15]. Auch 2014 wurden 7.038 Sicherheitslücken offiziell in den Katalog der National Vulnerability Database (NVD) der US-Regierung aufgenommen [16]. Von einer darüber hinausgehenden Dunkelziffer muss ausgegangen werden, da nicht alle Sicherheitslücken an die Öffentlichkeit gelangen.

Schadprogramme (meist Trojaner und Würmer) stellen die häufigste Angriffsform gegen Informationssysteme und PCs dar. Angriffe gegen die Verfügbarkeit eines IT-Systems oder IT-Dienstes stiegen im Jahr 2006 ebenfalls an. Eine Ursache dafür ist die verstärkte Zunahme von ferngesteuerten Bot-Netzen aus mehreren Rechnern, die gerade für solche Angriffe aufgebaut oder zur Versendung von unerwünschten E-Mails (SPAM) genutzt werden.

Weiterhin stellt der Bericht fest, dass modulare Schadprogramme einen neuen Trend darstellen, um die Schäden an Computersystemen möglichst hoch zu halten. Dabei laden kleinere Schadprogramme unbemerkt ständig neue, größere Schadprogramme aus dem World Wide Web nach. Diese kleineren Schädlinge sind schwer erkennbar und nicht leicht zu bekämpfen.

Das bekannte „*actio-reactio*“ zwischen Schädlingsprogrammierer und Bekämpfer dieser Schadprogramme kann also nur beendet werden, wenn effektive und effiziente Sicherungsmaßnahmen ergriffen werden, die nicht überwunden werden können.

6 BSI-Standards und Technische Richtlinien

BSI-Standards, wie der Leitfaden IT-Sicherheit, enthalten Empfehlungen des BSI zu Methoden, Prozessen und Verfahren sowie Vorgehensweisen und Maßnahmen mit Bezug zur Informationssicherheit. Das BSI greift dabei Themenbereiche auf, die von grundsätzlicher Bedeutung für die Informationssicherheit in Behörden oder Unternehmen sind und für die sich national oder international sinnvolle und zweckmäßige Herangehensweisen etabliert haben. Zum einen dienen BSI-Standards zur fachlichen Unterstützung von Anwendern der Informationstechnik. Behörden und Unternehmen können die Empfehlungen des BSI nutzen und an ihre eigenen Anforderungen anpassen. Dies erleichtert die sichere Nutzung von Informationstechnik, da auf bewährte Methoden, Prozesse oder Verfahren zurückgegriffen werden kann. Auch Hersteller von Informationstechnik oder Dienstleister können auf die Empfehlungen des BSI zurückgreifen, um ihre Angebote sicherer zu machen. Zum anderen dienen BSI-Standards auch dazu, bewährte Herangehensweisen in ihrem Zusammenwirken darzustellen [17].

Der „Leitfaden IT-Sicherheit“ bietet nicht nur eine Vorgehensweise für den Aufbau einer Sicherheitsorganisation, sondern unterstützt auch bei der Risikobewertung, bei der Überprüfung des vorhandenen IT-Sicherheitsniveaus sowie bei der Umsetzung von Maßnahmen.

Es werden organisatorische Maßnahmen ohne technische Details vorgestellt, die einem Unternehmen sehr allgemein und grundlegend Hilfestellung geben, ein