BASISWISSEN WIRTSCHAFTSINFORMATIK

Konvergenz von Sicherheit bei Business- und Car-IT

Der Markt für Software-Technologie und softwarebasierte Dienstleistungen hat sich weltweit zu einem wirtschaftlichen Schlüsselbereich entwickelt. Dies betrifft sowohl Unternehmen, die Software entwickeln bzw. vertreiben **(Primärbranche)**, als auch Unternehmen aus den Anwenderbranchen (**Sekundärbranchen** wie Fahrzeug- und Maschinenbau, Elektrotechnik, Finanzdienstleistungen, Telekommunikation). Für die Sekundärbranchen ist Software ein wichtiger Bestandteil ihrer Produkte bzw. die Grundlage ihrer Dienstleistungen. In vielen Sekundärbranchen ist der gesamte Umsatz von Software abhängig, d.h., die Produkte werden mittels Software entwickelt, produziert und vertrieben, betriebliche Abläufe werden mittels Software gesteuert und unterstützt.

Beruhen neue, eigenständige Produkte bzw. Dienstleistungen auf dieser Technologie, bezeichnet man die Software als **Business Enabler**. Ist die Software hingegen Bestandteil eines Produktes, etwa einer Fahrzeugkomponente, spricht man von **Embedded Software**. Die Entwicklung dieser eingebetteten Software findet größtenteils in den Sekundärbranchen statt (vgl. Friedewald 2001, S. 81 - 84). Die softwarebasierte Funktionalität in Produkten kann ein wichtiges Differenzierungsmerkmal im Wettbewerb sein (vgl. Schüber 2003, S. 20).

Business-IT und Car-IT Security

Die technologische Entwicklung trägt auch dazu bei, dass Autofahren komfortabler und sicherer wird. Sie erhöht allerdings auch die Komplexität des Systems „Automobil“ und macht zusätzliche Überlegungen notwendig, die weit über die Funktions- und Ausfallsicherheit hinausgehen. Diese Anstrengungen lassen sich unter dem Begriff „Car-IT Security“ zusammenfassen.

Der Einzug von **Desktop-Architekturen** in die Fahrzeuge und die sich dabei ergebenden Möglichkeiten zur **Kommunikation nach außen** bei gleichzeitiger **aktiver Beeinflussung der internen Bussysteme** zeigen (Beispiele dazu unter den Anwendungen 1 - 3), dass es hier zu Fragestellungen kommt, die auch in der klassischen, die **Geschäftsprozesse unterstützenden Informationstechnologie** (Business-IT) eine Rolle spielen. Dies gilt insbesondere für die **IT-Sicherheit**. Bedrohungen wie Denial-of-Service-Attacken oder Viren müssen künftig auch bei der Entwicklung von IT-Anwendungen für Fahrzeuge berücksichtigt werden. Die Herausforderung besteht auch darin, Sicherheit in hochspezialisierte und echtzeitfähige Systeme zu integrieren. Szenarien wie das Update eines Navigationssystems via Datenverbindung über den Server eines öffentlichen Netzes verdeutlichen dies:

- Wie kann sichergestellt werden, dass Daten und Anwendungen im Fahrzeug nicht unbefugt und unerkannt geändert werden können **(Integrität)**?
- Wie kann die **Verfügbarkeit der Software-Dienste** im Fahrzeug sichergestellt bzw. verhindert werden, dass die Kompromittierung von Software oder Daten seine Kernfunktionen beeinträchtigt?
- Wie kann sichergestellt werden, dass sensible Daten im Fahrzeug bzw. bei der Kommunikation des Fahrzeugs mit anderen Entitäten nicht von Unbefugten eingesehen werden können **(Vertraulichkeit)**?
- Wie kann verhindert werden, dass personen- bzw. ortsbezogene Daten Rückschlüsse auf den Fahrer und dessen Verhalten ermöglichen **(Anonymität)**?
- Wie kann sichergestellt werden, dass nur diejenigen auf die Daten und Anwendungen im Fahrzeug zugreifen können, die dazu berechtigt sind, und auch nur insoweit, als sie dazu berechtigt sind **(Authentizität)**?
- Wie kann verhindert werden, dass die Nutzung eines Dienstes nachträglich abgestritten wird (Nachweisbarkeit) oder urheberrechtlich geschützte Dateien missbräuchlich verwendet werden **(Digital Rights Management)**?
- Wie kann verhindert werden, dass eine missbräuchliche Anwendung IT-Systeme (Rechnernetze) gefährdet, mit denen Kommunikationsbeziehungen bestehen **(Verlässlichkeit der Kommunikation)**?

Kostspielige Sicherheitsvorfälle haben das Bewusstsein geschärft, dass eine angemessene und umfassende Sicherheit in der Business-IT ein **ganzheitliches und kontrolliertes Vorgehen** erfordert. Es entstanden Regelwerke wie das IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (Bundesamt 2004) oder der British Standard 7799 (British 1999), aus denen **allgemeine Sicherheitsgrundsätze für die Informationstechnik und konkrete Policies für einzelne Komponenten** abgeleitet werden können. Eine zusammenfassende Darstellung dieser und weiterer IT-Sicherheitsstandards enthält die Broschüre „IT-Sicherheitskriterien im Vergleich“ der Initiative D21 (Initiative 2001). Vergleichbare Grundsatzdokumente fehlen noch für das Management von IT-Sicherheit in Fahrzeugen. Allerdings gibt es bereits einige Methoden, etwa zur Sicherheitsanalyse dienstbasierter Systeme mittels Bedrohungsbäumen (vgl. Scheidemann 2004, S. 19).

Anwendung 1: Kommunikation zwischen Auto und Server

Demnächst lassen sich **Navigationssysteme** in Autos mithilfe einer bidirektionalen Datenverbindung **aktualisieren**. Das Auto sendet Informationen über eine vorangegangene Aktualisierung sowie Bezahldaten an einen Server. Im Gegenzug stellt dieser alle relevanten Daten zur Aktualisierung des Navigationssystems bereit, beispielsweise zur Verkehrsdichte, zu aktuellen Baustellen und Umleitungen oder zu neuen Straßen. Diese Server arbeiten mit **sensiblen**, da orts- und personenbezogenen **Daten**, die hohen Sicherheitsanforderungen genügen müssen. Weitere Szenarien sind Infotainment-Inhalten im Abonnement oder als Pay-Per-View sowie Flash-Software (z.B. Update der Firmware per Mobilfunk oder Bluetooth an einer Tankstelle). Schließlich ist noch der mobile Zugang ins Internet oder zu Mobilfunkdiensten zu nennen.

Die **drahtlose Kommunikation** zwischen den Beteiligten macht **Angriffe möglich**. So ist denkbar, dass ein unbefugter Dritter die übermittelten Daten abfängt und manipuliert oder den Übertragungsweg auf andere Weise stört. Dabei können sowohl Code als auch Daten manipuliert oder unbrauchbar gemacht werden. Dadurch kann beispielsweise das Navigationssystem oder auch die Motorsteuerung ausfallen. Durch diese **Behinderung des Kommunikationsablaufs** können der Betreiber oder dessen Kunden oder auch nur ausgesuchte Kunden geschädigt werden, was zum **Verlust der Integrität** übermittelter Daten führt. Da die Daten ohne unmittelbaren Kontakt zwischen Nutzer und Anbieter ausgetauscht werden, können sie unter Vortäuschung einer

STICHWORT DES MONATS

Lohndumping

In der politischen Diskussion wird häufig von Lohndumping gesprochen, wenn Tariflöhne unterboten werden. Dahinter steht die Vorstellung, dass Flächentarifverträge die Löhne eigens standardisieren, um den Lohnwettbewerb auszuschalten. Lohnunterbietung stellt einen Verstoß gegen dieses Ziel dar und wird deshalb als Dumping bezeichnet. Diese Definition kann ***ökonomisch nicht überzeugen****, weil Flächentarifverträge zwar den Lohnwettbewerb in einer geschlossenen, aber nicht in einer offenen Volkswirtschaft ausschalten können.*

Überzeugendere Definitionen bietet die ***Preistheorie*** *an. Preisdumping liegt als wichtiger Unterfall der* ***räumlichen Preisdifferenzierung*** *vor, wenn die Verkaufspreise des gleichen Gutes für Kunden des* ***Inlands- und Auslandsmarktes*** *auseinander fallen. Eine engere Definition stellt auf einen* ***Verkauf unter den Herstellungskosten*** *ab. Dieser kann strategisch motiviert sein, um eine marktbeherrschende Stellung zu erlangen. Ist dies gelungen, werden Monopolrenten abgeschöpft, die Preise eines Guts langfristig also über seine Herstellungskosten angehoben.*

Überträgt man diese Definitionen auf den Lohn, liegt Dumping vor, wenn ein Arbeitnehmer eine ***räumliche Lohndifferenzierung*** *vornimmt, sich z.B. auf dem ausländischen Arbeitsmarkt preiswerter als auf dem heimischen anbietet. Weiter ist zu prüfen, ob sich ein Arbeitnehmer unter seinen „Herstellungskosten" anbietet. Als Pendant der Herstellungskosten eines Gutes bieten sich beim Faktor Arbeit die* ***Arbeitsproduktivität*** *und die* ***Durchschnittskosten*** *an. Ein Arbeiter kann als Lohn einen Anteil der von ihm erbrachten Wertschöpfung verlangen. Liegt die Wertschöpfung in Land A höher als in Land B, kann er in Land A auch einen höheren Lohn verlangen. Legt er nur den erzielbaren Lohn in Land B zugrunde, bietet er sich* ***unterhalb seiner Produktivität*** *an, er betreibt also* ***Lohndumping****. Das Problem ist, wie man den angemessenen Wertschöpfungsanteil bestimmen soll. Denn es reicht nicht aus, den Output je Arbeitsstunde zu messen. Vielmehr muss auch der Gewinnanteil des Unternehmens bestimmt werden. Genauso schwierig ist es, die* ***Durchschnittskosten*** *zu ermitteln. Diese werden durch das* ***Existenzminimum*** *und das* ***Arbeitsleid*** *bestimmt. Von zwei Individuen mit gleicher Produktivität kann sich derjenige billiger als Arbeitskraft anbieten, der sein Minimum niedriger ansetzt und mehr Freude an der Arbeit hat. Dieser Wettbewerbsvorteil stellt aber kein Dumping dar.*

Lohndumping würde dagegen vorliegen, wenn sich eine Arbeitskraft vorübergehend ***unter ihrem Existenzminimum*** *anböte, um eine marktbeherrschende Stellung zu erlangen, die ihm langfristig einen höheren Lohn sichert. Diese Analogie zum Gütermarkt dürfte allenfalls bei hoch qualifizierten Arbeiten bestehen, die aber auch ohne strategisches Verhalten Knappheitsrenten erzielen. Bei normalen Tätigkeiten sind die Markteintrittskosten so gering, dass die marktbeherrschende Stellung bei steigenden Löhnen wieder verloren ginge. Dann wäre* ***strategisches Verhalten*** *aber* ***irrational****.*

Dr. Hagen Lesch, Köln

falschen Identität an den Nutzer gesandt werden. Damit kann die Schädigung des Anbieters (Imageverlust durch schlechte Dienstleistungsqualität) oder des Kunden (unmittelbar) oder auch eine Bereicherung mithilfe ungerechtfertigter Berechnung von Diensten beabsichtigt sein.

Als Sicherheitsanforderung ergibt sich hier, dass die **Herkunft der Daten authentisch** sein muss. Ohne Schutzmechanismen besteht die Gefahr, dass Kernfunktionen verloren gehen. Da Mediendaten starkt nachgefragt werden (z.B. Kartenmaterial), kann eine unkontrollierte und widerrechtliche Verbreitung solcher Daten zu beträchtlichen Schäden beim Betreiber führen. Das Digital Rights Managements kann dafür sorgen, dass solche Daten nachvollziehbar abgerechnet werden. Umgekehrt muss auch beachtet werden, dass die Nutzung eines Dienstes nachweisbar ist, damit sie nicht nachträglich abgestritten werden kann. Die Vertraulichkeit der Kommunikation zwischen Kunden und Betreiber ist ebenfalls ein wichtiger Aspekt. Dritte sollen keine Informationen darüber erhalten, wo sich der Kunde zu welchem Zeitpunkt aufhält oder aufgehalten hat.

Anwendung 2:
Kommunikation zwischen Automobilen

Die Kommunikation zwischen Automobilen wird dazu beitragen, **Verkehrsströme besser zu lenken**, die **Verkehrssicherheit zu verbessern** und die **Straßen effektiver zu nutzen**. So werden sich Autos **gegenseitig über die aktuelle Verkehrslage informieren** und dem Fahrer Alternativrouten vorschlagen. Dabei werden IT-Systeme aktiv und passiv in die **Fahrzeugkontrolle** eingreifen. Auf diese Weise ist das Heranführen mit angepasster Geschwindigkeit an ein Stauende oder die automatische Steuerung mehrerer Lastkraftwagen in einer Kolonne möglich. Ein weiteres Beispiel ist die Weiterleitung von Daten zu Scheibenwischerfrequenz, Fahrgeschwindigkeit oder Schleuderverhalten per WLAN an Fahrzeuge in der Umgebung. Gefahrenmeldungen über vereiste Brücken oder Ölspuren auf der Fahrbahn können ad hoc an nachfolgende Fahrzeuge weitergegeben werden.

Die Kommunikation zwischen Fahrzeugen unterliegt **ähnlichen Gefahren** wie die Kommunikation zwischen Fahrzeug und Service-Betreiber, da auch sie drahtlos vonstatten geht. Sie kann relativ **einfach gestört** werden. Auch hier spielt die Authentizität eine wichtige Rolle, um sicherzustellen, dass die Daten wie erwartet vom richtigen Partner stammen. Bei Fahrzeugflotten können Kommunikationsstörungen erhebliche Folgen wie größere Verspätungen oder auch Unfälle nach sich ziehen. Bei Angaben zu Witterung, Fahrbahnzustand oder Verkehrsaufkommen müssen die Daten mit den tatsächlichen Zuständen übereinstimmen. Hier kann **zertifizierte Software** helfen, deren Integrität zu verifizieren.

Anwendung 3:
Produktion, Tuning, Wartung, Aufrüstung und Entsorgung

Die Informationstechnik spielt im gesamten Lebenzyklus eines Fahrzeugs eine Rolle, etwa bei Produktion und Montage, bei Vertrieb, Wartung, bei der Installation zusätzlicher Services oder bei der Entsorgung. Dies führt auch zu **potenziellen Risiken** der Car-IT, etwa durch **physische und logische Manipulationen** während oder im Vorfeld dieser Aktivitäten und dementsprechend zu besonderen Anforderungen an Produzenten und Service-Anbieter, an Kommunikationsmanagement, Systembetrieb, die Zugangskontrolle sowie an Systementwicklung und Qualitätssicherung. So handelt es sich bei den **Nutzungsdaten** eines Fahrzeugs, die bei der Wartung eine Rolle spielen, mittelbar um personenbezogene Daten, die ein Mindestmaß an Vertraulichkeit oder gar Anonymität erfordern. Gefälschte Teile und damit ver-

Anforderung	Anwendung 1	Anwendung 2	Anwendung 3
Integrität	x	x	x
Authentizität	x	x	x
Nachweisbarkeit	x		x
Digital Rights Management	x		x
Verfügbarkeit von Software und Kernfunktionen des Autos (Ausfallsicherheit, Safety)	x	x	
Verlässlichkeit der Kommunikation	x	x	
Anonymität		x	x
Vertraulichkeit	x		x

Abb.: Anforderungen an die Car-IT Security bei verschiedenen Anwendungen

bundene unrechtmäßige Garantieansprüche können zu einem wirtschaftlichen Risiko für den Hersteller der Originalteile werden. Elektronisch zertifizierte Austauschteile ermöglichen die Überprüfung ihrer Authentizität bei Einbau, Update und Betrieb.

Die Abbildung fasst die Anforderungen zusammen, die sich bei Sicherheitsmaßnahmen ergeben.

Dr. Dirk Kalmring, Sankt Augustin

Literaturempfehlungen:

British Standards Institution (BSI): BS7799: A Code of Practice for Information Security Management. London 1999.

Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz: Die Basis für IT-Sicherheit. http://www.bsi.bund.de/gshb/, 2004, Abruf am 22.4.2005.

Eckert, C.: IT-Sicherheit: Konzept — Verfahren — Protokolle. 3. Aufl., München 2004.

Friedewald, M. et al.: Softwareentwicklung in Deutschland: Eine Bestandsaufnahme. In: Informatik Spektrum, Vol. 24 (2001), S. 81 - 90.

Initiative D21: IT-Sicherheitskriterien im Vergleich. http://www.initiatived21.de/druck/news/publikationen2002/doc/22_1053502380.pdf, 2001, Abruf am 22.4.2005.

Scheidemann, K. et al.: Sicherheitsaspekte nachladbarer Dienste im Automobil. escar 2004 — Embedded Security in Cars. Bonn, Vortrag am 10.11.2004.

Schüber, E.: Software: 1A-Qualität bietet nur der Profi. In: MM MaschinenMarkt — Das IndustrieMagazin, Heft 45 (2003), S. 20 - 22.

Vasek, T.: Friede den Straßen. In: Technology Review (2004), Heft 10, S. 94 - 96.

BASISWISSEN VWL

Instrumente der Geldpolitik

Die Geldpolitik hat die Aufgabe, mit den ihr zur Verfügung stehenden Instrumenten die ihr zumeist gesetzlich vorgegebenen **Ziele** wie **Preisniveaustabilität** und **Output-Stabilisierung** zu erreichen (vgl. Issing 1996, S. 71). Geldpolitik wird im Prinzip dadurch betrieben, dass eine Zentralbank Forderungen gegen sich gegen Forderungen an den Staat — typischerweise verzinsliche Schatzwechsel und Staatsanleihen — auf den Märkten für diese Finanzinstrumente eintauscht. Voraussetzung für geldpolitisches Handeln ist somit, dass ein entsprechender Bestand an staatlichen Schuldobligationen existiert. Geldpolitische Instrumente können nur deshalb wirksam werden, weil die **Kreditinstitute Forderungen gegenüber der Zentralbank halten müssen**. Die Gesamtheit dieser Forderungen wird als **„monetäre Basis"** bezeichnet. Die monetäre Basis bzw. die Menge an Zentralbankgeld setzt sich aus dem Bargeldumlauf und den so genannten Reserven zusammen, die die Kreditinstitute in Form von Sichteinlagen bei der Zentralbank halten. Die Nachfrage der Kreditinstitute nach diesen unverzinslichen Reserven variiert prozyklisch mit der wirtschaftlichen Aktivität. In Boomphasen steigt sie, bei rezessiver Entwicklung geht sie zurück. Da die Zentralbank ein monopolistischer Anbieter auf dem Geldmarkt ist, kann sie die Nachfrage der Kreditinstitute nach Reserven entweder über den Preis oder über die Menge befriedigen bzw. in ihrem Sinne beeinflussen (vgl. Friedman 2000, S. 3 ff.).

Die Wahl des geldpolitischen Instrumentes

Da sich die **Zentralbank als Monopolist** gewissermaßen einer fallenden Preis-Absatz-Funktion für Zentralbankgeld gegenübersieht, führt eine Änderung des Preises für Zentralbankgeld, des Geldmarktzinses, automatisch zu einer Änderung der Zentralbankgeldmenge. Ebenso kann sie über eine Mengensteuerung den Geldmarktzins verändern. Die **Geldpolitik** kann damit entweder **über eine Zinssteuerung oder eine Geldbasissteuerung** erfolgen. Je nach Wahl des geldpolitischen Operationsziels sind allerdings unterschiedlich ausgestaltete geldpolitische Instrumente notwendig (vgl. Bofinger et al. 1996, S. 389 f.).

Wären der Zentralbank alle Einflüsse auf die geldpolitischen Zielgrößen Preisniveau und Output bekannt, würde es keinen Unterschied machen, ob sie Geldpolitik durch Fixierung des Angebots an Reserven (bzw. — bei Berücksichtigung von Bargeld — der monetären Basis) oder durch Festlegung des Zinssatzes betreibt. Da sie jedoch nicht über diese Kenntnis verfügt, muss sie ihre