SimoBIT

Gefördert durch:

Bundesministerium
für Wirtschaft
und Technologie

aufgrund eines Beschlusses
des Deutschen Bundestages

Leitfaden

Ergebnisse des SimoBIT-Arbeitsforums

IT- Sicherheit in mobilen Geschäftsprozessen

Autoren

Martin Oczko, Utimaco Safeware AG
Annette Hillebrand, WIK-Consult GmbH
Fritz Meier, Fraunhofer SCS
Stefan Faltus, ATB Bremen
Thang Tran, TU Dortmund
Michael Decker, Karlsruher Institut für Technologie (KIT)
Jochen Günther, Fraunhofer IAO
Ralf Kunoth, fun communications GmbH
Christoph Loeser, C-LAB, Siemens AG
Thilo Steckel, Claas Selbstfahrende Erntemaschinen GmbH
Günther Diederich, Hochschule Bremen
Gudrun Tschirner-Vinke, C-LAB, Siemens AG
Wolfgang Neifer, WIBU-Systems AG
Matthias Müller, RWTH Aachen
Ulli Münch, Fraunhofer SCS

Bad Honnef, Juli 2010

www.simobit.de

Inhaltsverzeichnis

Vorwort der SimoBIT-Begleitforschung V

1 SimoBIT Leitfaden IT-Sicherheit: Sichere mobile Informationstechnik in Mittelstand und Verwaltung 1

1.1 Mobile Anwendungen schaffen Flexibilität und Effizienz 1

1.2 Spezifische mobile Risiken 2

1.3 Schadprogramme 2

1.4 SimoBIT Leitfaden IT-Sicherheit 3

1.5 Rekursive Schleifen – Schritte zur Konstruktion sicherer IT-Systeme 4

1.6 Inhalte des IT-Sicherheitsleitfadens 4

2 Schritte zur strukturierten IT-Sicherheitsanalyse 6

2.1 IT-Risiken und Schutzziele 6

2.2 Kosten-Risiko-Abwägungen bei der Auswahl von Gegenmaßnahmen 7

2.3 Generische Vorgehensweise: Schritte zur strukturierten IT-Sicherheitsanalyse 8

3 Schritte zur strukturierten IT-Sicherheitsanalyse bei mobilen Anwendungen in der Öffentlichen Verwaltung 10

3.1 IT-Sicherheit im Kontext mobiler Fachprozesse 10

3.2 Anwendungsszenarien und Konzepte zur Umsetzung 12

3.3 Identifizierte Bedrohungen 14

3.4 Bewertung der Bedrohungen 16

3.5 Identifizierte Gegenmaßnahmen 17

3.6 Ausgewählte Gegenmaßnahmen 19

4 Mobile IT-Sicherheit in Handwerk und KMU: Digitale Zertifikate für sichere mobile Anwendungen 21

4.1 Spezifische Herausforderungen für Handwerk und KMU bei der Realisierung mobiler Anwendungen 21

4.2 Digitale Zertifikate für sichere mobile Anwendungen 21

4.2.1 Was sind digitale Zertifikate? 21

4.2.2 Verschlüsselung und Signatur mit digitalen Zertifikaten 23

4.2.3 Ausstellung, Lebensdauer und Kosten digitaler Zertifikate 24

4.3 Einsatz von Zertifikaten in den SimoBIT-Projekten für Handwerk und KMU 26

4.3.1 ModiFrame, M3V und MAREMBA – Die Herausforderungen 27

4.3.2 M3V 27

4.3.3 MAREMBA 28
4.3.4 Identifizierte Bedrohungen 29
4.3.5 Bewertung der Bedrohungen 30
4.3.6 Identifizierte Gegenmaßnahmen 31
4.3.7 Ausgewählte Gegenmaßnahmen 33
4.4 Digitale Zertifikate als Lösung für mobilspezifische Sicherheitsprobleme 36
5 Mobile IT-Sicherheit im Maschinenbau: Vorgehensweise zur strukturierten Reduzierung von Bedrohungen 39
5.1 Integration des Managements mobiler Maschinen in Geschäftsprozesse 39
5.2 Berücksichtigung von IT-Sicherheit bereits in der Entwicklungsphase 41
5.3 SimoBIT-Projekt R2B: Anwendungsfälle und deren Anforderungen 43
5.3.1 Anwendungsfall Grünfutterernte 43
5.3.2 Anwendungsfall IT-Wartung und Service 45
5.4 Identifizierte Bedrohungen 46
5.5 Bewertung der Bedrohungen 47
5.6 Identifizierte Gegenmaßnahmen 49
5.7 Ausgewählte Gegenmaßnahmen 51
6 Mobile IT-Sicherheit in der Gesundheitswirtschaft: Sicherheit durch Innovation - Innovation durch Sicherheit 54
6.1 Bedrohungsanalyse in der Pflege, im Rettungsdienst und bei mobilen Assets 54
6.2 Rechtliche Herausforderungen im Gesundheitswesen stellen hohe Anforderungen an die IT-Sicherheit 54
6.3 Vorgehensweise: Schritte zur strukturierten IT-Sicherheitsanalyse 56
6.4 Bedrohungen identifizieren und bewerten 57
6.5 Gegenmaßnahmen identifizieren und auswählen 58
6.5.1 Med-on-@ix 58
6.5.2 OPAL Health 61
6.5.3 VitaBIT 63
Glossar 68
SimoBIT-Förderprojekte im Überblick 73
Mitglieder des SimoBIT-Arbeitsforums IT-Sicherheit 74

Abbildungsverzeichnis

Abbildung 1-1:	Die 12 SimoBIT-Förderprojekte	3
Abbildung 2-1:	Schritte zur strukturierten IT-Sicherheitsanalyse	8
Abbildung 3-1:	IT-Infrastruktur eines mobilen Arbeitsplatzes für Forstbetriebe	11
Abbildung 3-2:	Mobis Pro: Optimierung der Prozesskette vom vorbeugenden bis zum abwehrenden Brandschutz	11
Abbildung 3-3:	simoKIM: Einführung einer zentralen Prozessausführungsumgebung innerhalb einer Kommune	12
Abbildung 3-4:	Mögliche Kommunikationsarchitektur einer mobilen Anwendung und Bedrohungspotenzial	16
Abbildung 3-5:	Mögliche Gegenmaßnahmen gegen Bedrohungen	18
Abbildung 4-1:	Privater und öffentlicher Schlüssel	22
Abbildung 4-2:	Privater Schlüssel und Zertifikat	23
Abbildung 4-3:	Dokument verschlüsseln	23
Abbildung 4-4:	Digitale Signatur eines Dokuments überprüfen	24
Abbildung 4-5:	Zertifikatsketten	25
Abbildung 5-1:	Kommunikationsszenario zwischen mobilen Einheiten und Backend im Projekt R2B	40
Abbildung 5-2:	Klassische Entwicklung im Vergleich zur Entwicklung mit IT-Sicherheitsstandard	41
Abbildung 6-1:	Funkzugangstechnologien Deutschland und Aachen am Bespiel von T-Mobile	58
Abbildung 6-2:	Übersicht der Hardwarekomponenten von Med-on-@ix	60
Abbildung 6-3:	OPAL Health Systemarchitektur	61
Abbildung 6-4:	Smartphone mit Sicherheitskomponente zur Anwendung im ambulanten Pflegedienst	64
Abbildung 6-5:	Sicherheits- und Speicherkomponente microSD	65

Vorwort der SimoBIT-Begleitforschung

Mobile Geschäftsanwendungen entwickeln sich zu einer Schlüsselapplikation in Unternehmen und öffentlichen Verwaltungen. Mit ihrer Hilfe lassen sich auf allen Ebenen betrieblicher und öffentlicher Wertschöpfungsaktivitäten Prozesse vereinfachen, flexibilisieren und effizienter gestalten. Zwar dominieren heute noch eher einfache Anwendungen wie Sprachtelefonie, SMS und mobile E-Mail die mobile Geschäftskommunikation, aber die Entwicklungen und Lösungen der zwölf SimoBIT-Projekte zeigen, dass durch den ubiquitären und jederzeitigen Zugriff beispielsweise auf Patienteninformationen, auf Geo- oder Plandaten die Qualität der ambulanten Pflege, die Effizienz landwirtschaftlicher Prozesse oder unternehmerischer Entscheidungen deutlich erhöht werden können.

Es bestehen somit hohe Erfolgsaussichten, dass sich durch mobile Geschäftsanwendungen über alle Branchen hinweg sowohl erhebliche Kosten- und Zeitersparnisse als auch beachtliche Produktivitäts- und Qualitätsgewinne bei der Reorganisation von Wertschöpfungs- und Fachprozessen realisieren lassen. Durch die Optimierung des Personaleinsatzes, Einsparungen in der Logistik und die Verbesserung der Datenqualität beim Kunden vor Ort wird nicht nur die Wettbewerbsfähigkeit von Unternehmen, sondern auch die Effizienz vieler Verwaltungsorganisationen nachhaltig gesteigert.

Mit der Übertragung immer größerer und wichtigerer Datenmengen über die Luftschnittstelle stellen sich jedoch große Herausforderungen vor allem im Bereich der IT-Sicherheit, des Datenschutzes oder etwa beim Einsatz elektronischer Signaturen. Die Mobilisierung von Anwendungen fokussiert zum einen auf IT-Sicherheitsaspekte, wie sie auch im Kontext von klassischen Festnetzen Bedeutung besitzen. Im mobilen Kontext gewinnen diese aber wegen der umfangreicheren Schnittstellen der mobilen Endgeräte, dem Technologie-Mix und der damit verbundenen größeren Angriffsfläche der mobilen Endgeräte erheblich an Bedeutung. Der zweite Fokus resultiert aus dem Einsatz mobiler Endgeräte, durch den eine weitere Herausforderung bei mobilen Geschäftsanwendungen entsteht. Ohne besondere Schutzmaßnahmen sind Angriffe im mobilen Kontext schneller und einfacher erfolgreich als im Festnetzbereich. Die sichere und robuste Integration mobiler Lösungen über alle Elemente der Mobilfunknetze und Anwendungen hinweg in bestehende IT-Backend-Architekturen bildet daher einen zentralen Schwerpunkt bei der Implementierung mobiler Geschäftsanwendungen.

Angesichts der enormen volkswirtschaftlichen Bedeutung von mobilen Geschäftsanwendungen hat das Bundesministerium für Wirtschaft und Technologie (BMWi) 2006 die Förderinitiative SimoBIT ins Leben gerufen. SimoBIT steht für „Sichere Anwendungen der mobilen Informationstechnik zur Wertschöpfungssteigerung in Mittelstand und Verwaltung“. Die Zielsetzung von SimoBIT besteht darin, durch eine nahtlose Integration von IT-Sicherheit in mobile Technologien und Anwendungen die Implementierung von mobilen Anwendungen in bestehende betriebliche und verwaltungsorganisatorische

Strukturen zu erleichtern und zu beschleunigen. Um eine möglichst effiziente Umsetzung der Förderung zu sichern und einen breiten Transfer der Ergebnisse und Lösungen in den Markt zu gewährleisten und dadurch eine Möglichkeit zur erfolgreichen Nachahmung zu eröffnen, wurde im Herbst 2008 das Arbeitsforum IT-Sicherheit ins Leben gerufen, bestehend aus den Experten der einzelnen SimoBIT-Förderprojekte. Die Ergebnisse dieses Arbeitsforums werden mit dem vorliegenden Leitfaden „IT-Sicherheit in mobilen Geschäftsprozessen“ dokumentiert. Er basiert auf den konkreten Erfahrungen der Projekte sowie der Begleitforschung. Die Gliederung der Inhalte orientiert sich an der Zuordnung der Projekte zu den Kompetenzclustern:

1. Öffentliche Verwaltung (Mobility@forest, Mobis Pro, simoKIM),

2. Handwerk und kleine Unternehmen (MAREMBA, ModiFrame, M3V),

3. Maschinenbau (SiWear, R2B – Robot to Business, MSW – Mobile Servicewelten),

4. Gesundheitswirtschaft (Med-on-@ix, VitaBIT, OPAL Health),

Der Leitfaden beinhaltet eine Übersicht über die Erfolgsfaktoren und eine Anleitung zur Beantwortung der Fragestellungen, die sich bei der Entwicklung und Implementierung von IT-Sicherheit für mobile Geschäftsanwendungen ergeben. Er soll zugleich Orientierungshilfe und Wegweiser für alle Anbieter von mobilen IKT-Lösungen sein, um diese nachhaltig gestalten zu können.

Die Verantwortung für die Inhalte des Leitfadens liegt bei den Autoren. Ihnen sei an dieser Stelle herzlich gedankt für ihr hohes Engagement.

Dr. Franz Büllingen
Leiter der SimoBIT-Begleitforschung

1 SimoBIT Leitfaden IT-Sicherheit: Sichere mobile Informationstechnik in Mittelstand und Verwaltung

1.1 Mobile Anwendungen schaffen Flexibilität und Effizienz

Mobile Geschäftsanwendungen werden immer mehr zu einem Antriebsmotor für Innovationen in Unternehmen und Verwaltungen. Zahlreiche Prozesse innerhalb einer Organisationsstruktur lassen sich mit Hilfe smarter mobiler Endgeräte vereinfachen und flexibilisieren.

Bei kleinen Betrieben beträgt der Anteil mobiler Mitarbeiter heute schon rund 50%, bei mittleren Unternehmen nahezu 75%. Ergebnisse einer aktuellen Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie[1] zeigen, dass Unternehmen ihre operativen Kosten mit Hilfe mobiler Geschäftsanwendungen um bis zu 20% reduzieren konnten.

Die Mobilität der Belegschaft ist branchenübergreifend ein integraler Erfolgsfaktor und leistet einen entscheidenden Beitrag zur Differenzierung der Unternehmen im internationalen Wettbewerb. Bei der Frage nach dem Mehrwert von mobilen Geschäftsanwendungen stehen die Erhöhung der Flexibilität, die Verbesserung der Informationsqualität und des Kundenservice sowie die Effizienzsteigerung im Vordergrund.

Gleichzeitig sehen sich KMU bei der Implementierung von mobilen Geschäftsanwendungen vor großen Herausforderungen. IT-Sicherheit, d.h. im Wesentlichen die Sicherung der Vertraulichkeit, der Integrität und der Verfügbarkeit von Daten, kommt dabei eine Schlüsselrolle zu. Das Förderprogramm SimoBIT hat zum Ziel, das Bewusstsein für die mit mobilen Geschäftsanwendungen verbundenen Herausforderungen und Chancen gerade auch im Bereich IT-Sicherheit zu erhöhen. Der vorliegende Leitfaden des SimoBIT-Arbeitsforums IT-Sicherheit will daher interessierten KMU bei der Gestaltung dieses Bereichs Unterstützung bieten.

Das Bundesministerium für Wirtschaft und Technologie (BMWi) fördert im Rahmen des Förderprogramms „SimoBIT – sichere Anwendung der mobilen Informationstechnik (IT) zur Wertschöpfungssteigerung in Mittelstand und Verwaltung“ zwölf ausgewählte Forschungs- und Entwicklungsprojekte zur beschleunigten Entwicklung und breitenwirksamen Nutzung von sicheren, mobil vernetzten Multimedia-Anwendungen in den Tätigkeitsfeldern von Unternehmen und öffentlichen Verwaltungen.

1 Vgl. Büllingen, F.; Hillebrand, A.; Schäfer, R. G.: Nachfragestrukturen und Entwicklungspotenziale von Mobile Business-Lösungen im Bereich KMU, Studie im Rahmen der SimoBIT-Begleitforschung, WIK-Consult, September 2010.

1.2 Spezifische mobile Risiken

Brisant sind die spezifischen mobilen Risiken nicht zuletzt deshalb, weil es Angreifern auch bei mobilen IKT-Systemen immer weniger darum geht, nur Hard- und Softwareschäden zu verursachen, um (irgend-)einem Unternehmen zu schaden. Vielmehr wollen Angreifer systematisch an Daten gelangen, die sich gewinnbringend weiterverwenden oder weiterverkaufen lassen.

Spezifische Risiken im Umfeld mobiler Geschäftsanwendungen sind beispielsweise das Abfangen von Informationen über die Luftschnittstelle oder das Entwenden der mobilen Endgeräte. Hardware zu zerstören, Software oder Daten zu manipulieren oder auch die Geräte-Konfiguration zu verändern ist bei mobilen Endgeräten zudem leichter möglich, weil Anwender ihre Handys, Smart Phones, Notebooks oder Tablet-PCs in den verschiedensten unsicheren Umgebungen mit sich führen und potenziellen Angreifern somit der Zugang zu den Geräten vereinfacht wird. Darüber hinaus unterstützen nicht alle Sicherheitsarchitekturen der mobilen Betriebssysteme vollständig eine Rechte- und Benutzerverwaltung.

Nach neusten Erhebungen betragen die durchschnittlichen Kosten bei Verlust eines Laptops für ein Unternehmen rund 49,246 US-Dollar.

(The Cost of a Lost Laptop, Ponemon Institute LLC, Publication: April 22, 2009)

1.3 Schadprogramme

Darüber hinaus zeichnet sich eine Zunahme von Schadprogrammen künftig auch bei mobilen Anwendungen ab. Im Zuge der Standardisierung der Betriebssysteme bei mobilen Endgeräten werden in naher Zukunft Probleme wie etwa Daten- und Identitätsdiebstahl, Zugriff auf Systeme über Hintertüren oder Manipulation von Informationen, verursacht durch Viren, Würmer, Trojaner, Spyware oder Keylogger zunehmen und sich ein kommerzieller Markt für diese Malware auch im mobilen Umfeld entwickeln.

Hinzu kommt, dass die Nutzer eines mobilen Geräts potenziell unerwünschte Anwendungen oder Schnittstellen, d.h. Features, die nicht zwangsläufig schädlich, aber für Unternehmensnetzwerke ungeeignet sind (Adware, Dialer, Bluetooth etc.) auf „ihren“ mobilen Endgeräten installieren bzw. aktivieren und damit unfreiwillig Schäden verursachen können.

BSI-Lagebericht 4. Quartal 2009: WLAN, Hotspots und Mobilfunktelefonie bilden neben Internet einen wichtigen Risikobereich: „Je mehr Kommunikationsfunktionen die mobilen Geräte bieten, desto mehr steigt auch das Risiko, dass Kriminelle an vertrauliche Daten gelangen und Software manipulieren.“

1.4 SimoBIT Leitfaden IT-Sicherheit

Ein besonderes Problem der Risikobekämpfung im Bereich „mobil“ besteht darin, dass auf allen Ebenen proprietäre Sicherheitslösungen existieren, Gesamtkonzepte für mobile IT-Sicherheit jedoch in vielen Unternehmen noch fehlen.

Das SimoBIT Arbeitsforum IT-Sicherheit wurde im Frühjahr 2009 ins Leben gerufen und entwickelte bis zum Sommer 2010 den vorliegenden Leitfaden, der einen branchenübergreifenden Transfer von Ergebnissen und Erfahrungen in die Fläche zum Ziel hat und insbesondere KMU bei der Entwicklung eines übergreifenden IT-Sicherheitskonzepts unterstützen will.

Obwohl die zwölf SimoBIT-Förderprojekte in ganz verschiedenen Branchen – Öffentliche Verwaltung, Maschinenbau, Gesundheitswirtschaft, Handwerk und KMU – umgesetzt wurden, lassen sich für das strukturierte und systematische Vorgehen zur Erhöhung der IT-Sicherheit zentrale Gemeinsamkeiten aufzeigen, die für kleine und mittlere Unternehmen nicht nur aus der jeweiligen Branche wertvolle Hinweise bieten.

Das Arbeitsforum IT-Sicherheit bietet Raum für die Erarbeitung, Analyse und Diskussion von projektübergreifendem IT-Sicherheits-Know-how. Die vier Arbeitsforen werden durch die SimoBIT-Begleitforschung koordiniert und durch einen inhaltlich-fachlich versierten Experten aus der Mitte der SimoBIT-Projekte geleitet.

Inhalte des SimoBIT-Arbeitsforums IT-Sicherheit:

- adäquate IT-Sicherheitsmaßnahmen im Kontext von Geschäfts- und Fachprozessen
- Methoden zur Analyse von Sicherheitsanforderungen unter Berücksichtigung von IT-Sicherheitsstandards
- Szenarien zur Umsetzung, Checklisten und Maßnahmen

Ziele des Arbeitsforums IT-Sicherheit:

- Grundlagen für Forscher, Entwickler und Anwender zur Einschätzung der eigenen Vorhaben schaffen
- Expertenwissen bündeln und Wissensaustausch mit Externen pflegen
- Leitfaden zur Sicherheit von mobilen IT-Systemen formulieren

Abbildung 1-1: Die 12 SimoBIT-Förderprojekte

Gesundheitswirtschaft	Maschinenbau	Öffentliche Verwaltung	Handwerk und kl. Unternehmen
▸ Med-on-@ix ▸ VitaBIT ▸ OPAL Health	▸ Mobile Servicewelten ▸ SiWear ▸ R2B	▸ Mobis Pro ▸ simoKIM ▸ Mobility@forest	▸ MAREMBA ▸ ModiFrame ▸ M3V

Quelle: WIK-Consult

1.5 Rekursive Schleifen – Schritte zur Konstruktion sicherer IT-Systeme

Basis der Empfehlungen ist ein Vorgehen auf der Grundlage eines Ablaufdiagramms, das die turnusmäßige Überprüfung der getroffenen Entscheidungen und eine Kontrolle der implementierten IT-Sicherheitsmaßnahmen vorsieht.

Die Vorteile dieses Modells der **Schritte zur strukturierten IT-Sicherheitsanalyse** liegen u.a. darin, dass

- es den Blick der Projektverantwortlichen auf die Realisierung von IT-Sicherheit für die gesamte mobile Geschäftsanwendung als Bestandteil der Unternehmens-IT lenkt,
- jeder Projektverantwortliche – je nach Projektstand - an jedem Punkt des sich wiederholenden Ablaufs starten kann und
- jeder wichtige Aspekt der systematischen Einführung von IT-Sicherheit mindestens einmal betrachtet sowie die Lösung (mindestens noch einmal) auf ihre Wirksamkeit überprüft wird.

1.6 Inhalte des IT-Sicherheitsleitfadens

In den folgenden vier Abschnitten des Leitfadens wird dargestellt, wie die jeweiligen Projekte der verschiedenen Branchen ihre IT-Sicherheitsrisiken anhand dieses Modells analysiert und welche Maßnahmen sie ergriffen haben:

- Cluster Öffentliche Verwaltung: Die Erfahrungen aus den **SimoBIT**-Projekten **Mobility@forest**, **Mobis Pro** und **simoKIM** zeigen, dass bei der Einführung mobiler Anwendungen im Umfeld der Öffentlichen Verwaltung das Thema IT-Sicherheit eine wichtige Rolle spielt. In vielen Fällen werden personenbezogene Daten sowie Informationen über kritische mobile Infrastrukturen übertragen, welche einen hohen Schutzbedarf besitzen und nur autorisierten Personen zugänglich sind. In allen drei Projekten wurde das strukturierte Vorgehen zur IT-Sicherheitsanalyse erfolgreich angewendet.
- Cluster Handwerk und kleine Unternehmen: Speziell im handwerklichen Gewerbe existieren viele Anwendungsgebiete für den Einsatz mobiler Technologien. Bei der Lösung der mobilspezifischen Sicherheitsprobleme spielen digitale Zertifikate für sichere mobile Anwendungen eine zentrale Rolle, um z. B. verbindlich Leistungen abzunehmen oder Angebote abzugeben. Die Lösungsansätze der SimoBIT-Projekte **ModiFrame**, **M3V** und **MAREMBA** werden detailliert beschrieben.

- Cluster Maschinenbau: Die automatisierte Ablauffähigkeit von Geschäftsprozessen im SimoBIT-Projekt **R2B** sowie die zeit- und ortsunabhängige Verfügbarkeit über am Körper getragene Interaktionssysteme im Projekt **SiWear** sind zentrale Ziele der Forschungsprojekte im Cluster Maschinenbau. Einblicke in das Projekt **R2B** bieten interessante Beispiele für eine strukturierte Reduzierung von Bedrohungen für Anwendungen, die auch auf andere Bereiche übertragbar sind.

- Cluster Gesundheitswirtschaft: Angelehnt an die Schritte zur strukturierten IT-Sicherheitsanalyse entschieden sich die SimoBIT-Projekte **VitaBIT**, **Med-on-@ix** und **OPAL Health** für verschiedene sicherheitsrelevante Komponenten und Prozesse, die auch die spezifischen rechtliche Anforderungen der Gesundheitswirtschaft, z. B. des Medizinproduktegesetzes, berücksichtigen.

Insgesamt zeigt sich, dass durch die Einrichtung des Arbeitsforums IT-Sicherheit unter Beteiligung der IT-Sicherheitsexperten der SimoBIT-Projekte sowie interessierter Fachleute mittels der **Schritte zur strukturierten IT-Sicherheitsanalyse** Erfolgsfaktoren für die Gestaltung von IT-Sicherheit ausgemacht werden konnten, die einen branchenübergreifenden Austausch ermöglichen und nutzbringend über die Laufzeit der Förderprojekte hinaus sind.

Die **Schritte zur strukturierten IT-Sicherheitsanalyse** werden im einführenden **Kapitel 2** dieses Leitfadens näher erläutert. Die Vorgehensweise zur Erhöhung der mobilen IT-Sicherheit wird in den nachfolgenden Kapiteln für die jeweiligen SimoBIT-Förderprojekte ausführlich beschrieben: **Öffentliche Verwaltung (Kapitel 3)**, **Handwerk und KMU (Kapitel 4)**, **Maschinenbau (Kapitel 5)** und **Gesundheitswirtschaft (Kapitel 6)**. Ein Glossar sowie eine Darstellung der SimoBIT-Förderprojekte ist im Anhang zu finden.

Ansprechpartner:

Martin Oczko
Leiter des Arbeitsforums IT-Sicherheit
Utimaco Safeware AG
Germanusstrasse 4
52080 Aachen

Tel.: 0241 1696 235
E-Mail: Martin.Oczko@aachen.utimaco.de

Annette Hillebrand
SimoBIT-Begleitforschung
Arbeitsforum IT-Sicherheit
WIK-Consult GmbH
Rhöndorfer Str.68
53604 Bad Honnef

Tel.: 02224 9225 53
E-Mail: a.hillebrand@wik-consult.com

2 Schritte zur strukturierten IT-Sicherheitsanalyse

Mobile IT-Anwendungen verändern die Aktivitäten in bestehenden Geschäftsprozessen oder bringen ganz neue Geschäftsmodelle hervor. Der Nutzen liegt u.a. darin,

- die geschäftlichen Aktivitäten zu erleichtern bzw. zu beschleunigen, z. B. durch Automatisierung von Identifikationsvorgängen,
- bestimmte Aktivitäten überflüssig zu machen, z. B. mittels automatischer Inventur,
- mehr Prozesssicherheit zu schaffen, z. B. durch mehr Transparenz,
- neue Erkenntnisse über die Aktivitäten in den Geschäftsprozessen durch geschicktes Verknüpfen verschiedenster Informationsquellen zu gewinnen sowie
- neue Zusatznutzen, z. B. durch ganz neue Geschäftsmodelle bzw. Dienstleistungen zu generieren.

Die im Rahmen der **SimoBIT**-Förderprojekte entwickelten Anwendungen, aber auch andere ähnliche Anwendungen, bieten große Nutzenpotenziale. Um diese Nutzenpotenziale realisieren zu können, müssen bestehende Aktivitäten in Geschäftsprozessen geändert werden oder Geschäftsmodelle mit ganz neuen Geschäftsprozessen entstehen. Zusätzlich kommen einerseits etablierte Technologien zum Einsatz und anderseits neue innovative Technologien. Neben Risiken, die bisher nicht ausreichend reduziert oder eliminiert wurden, kommen durch die Prozessänderungen und den Technologieeinsatz neue Risiken hinzu.

Risiken sollte man vor der Einführung der Technologie nicht ignorieren, sondern so gut wie möglich kennen, verstehen und mögliche Gegenmaßnahmen schon vor der Implementierung auswählen und mit einplanen. Identifizierte Risiken sollten nicht primär dazu führen, auf einen Einsatz der Technologie bzw. auf Prozessveränderungen zu verzichten, sondern sollten in eine ganzheitliche Betrachtung der Anforderungen und der sich ergebenden Nutzenpotenziale mit einbezogen werden.

2.1 IT-Risiken und Schutzziele

In einem Unternehmen haben ganz verschiedene Objekte einen Wert und müssen vor Risiken geschützt werden. Die spezifischen Anforderungen an den Schutz dieser Werte werden Schutzziele genannt. Zur Identifikation der Risiken, die diese Schutzziele verletzen, sollten alle Beteiligten, die von den Veränderungen durch die mobile IT-Anwendung betroffen sind, mit einbezogen werden. Dabei soll einerseits der Fokus auf der Erfassung der Sicherheitsanforderungen der Umwelt, der betroffenen Parteien und der Geschäftsprozesse selbst liegen und anderseits sollen die Kosten von IT-Sicherheitsmaßnahmen bzw. alternativ des Ignorierens der Anforderung aufgezeigt werden. Mobile IT-Anwendungen bringen von Haus aus gewisse Risiken mit, weil die

Geräte außerhalb der Firma verwendet werden, und deshalb sehr anfällig für Diebstahl, Verlieren oder „Shoulder-Sniffing“ sind; drahtlose Datenverbindungen sind auch nicht wie Kabel durch „Mauern“ u.ä. geschützt, und können daher leicht abgehört oder gar manipuliert werden.

Die meisten Risiken lassen sich einem der drei folgenden primären Schutzziele zuordnen:

- Risiken, welche die **Integrität** der Geschäftsprozesse verletzen, z. B. wenn Informationen ungewollt verändert werden,
- Risiken, welche die **Funktionsfähigkeit** der mobilen IT-Anwendung vermindern bzw. die Geschäftsprozesse stören, welche eine einwandfreie Funktionsfähigkeit der Technologie benötigen,
- Risiken welche die **Vertraulichkeit** von Informationen verletzen.

Wenn der Schutz dieser Ziele nicht gewährleistet ist und es durch technisches oder menschliches Versagen, durch höhere Gewalt oder gar durch den bewussten Angriff böswilliger Dritter zu Verletzungen der Ziele kommt, können unterschiedliche Folgen für die verschiedenen Akteure entstehen. Dabei treten nicht nur direkte monetäre Kosten auf, wie zum Beispiel durch Prozessausfälle oder Verzögerungen, sondern auch indirekte Kosten, die durch eine Beseitigung von Störfällen, durch die Verletzung von Gesetzen, Richtlinien oder Verträgen, den Verlust von Vertrauen oder durch Risiken für Leib und Leben entstehen.

Da man nicht alle Risiken gleichzeitig abstellen kann und eventuell sogar Zielkonflikte entstehen, muss man die möglichen Risiken gegeneinander abwägen, um so die wichtigsten Risiken zu identifizieren, die für den betrachteten Geschäftsprozess primär bestehen, jedoch ohne die übrigen Risiken zu ignorieren.

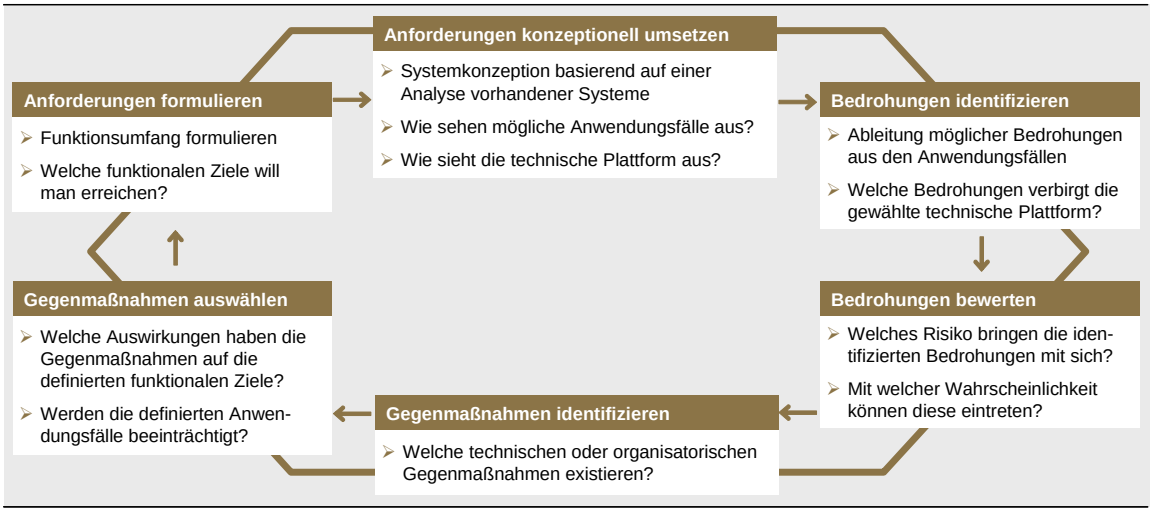
2.2 Kosten-Risiko-Abwägungen bei der Auswahl von Gegenmaßnahmen

Zur Verminderung der meisten Risiken mobiler IT existieren mehr oder weniger effiziente Gegenmaßnahmen. Um zu entscheiden, ob und in welcher Form die neue Technologie eingesetzt wird, müssen die Kosten von möglichen Gegenmaßnahmen bestimmt werden. Dabei müssen nicht nur direkte monetäre Kosten wie erhöhte Investitionskosten (z. B. die Anschaffung von sicheren mobilen Endgeräten) oder erhöhte Betriebskosten (z. B. durch ein erhöhtes Nachrichtenaufkommen oder zusätzliche manuelle Aktivitäten) betrachtet werden. Es sind auch weitere Kostenarten zu betrachten wie z. B. Opportunitätskosten, wenn etwa Risiken gegen einen Einsatz mobiler Geschäftsanwendungen sprechen oder aufgrund der Gegenmaßnahmen nicht alle Nutzenpotenziale ausgeschöpft werden können. Nach der Identifikation möglicher Gegenmaßnahmen muss unter Kostengesichtspunkten eine Auswahl getroffen werden, welche Gegenmaßnahmen umgesetzt werden sollen.

2.3 Generische Vorgehensweise: Schritte zur strukturierten IT-Sicherheitsanalyse

Um den Umgang mit Risiken und Gegenmaßnahmen verantwortungsbewusst zu gestalten, kamen in den **SimoBIT**-Projekten Ausprägungen einer generischen Vorgehensweise zum Einsatz, die sich mit dem Begriff „Schritte zur strukturierten IT-Sicherheitsanalyse“ beschreiben lässt. Je nach Art des Projektes kann dabei der Einstiegspunkt in die IT-Sicherheitsanalyse unterschiedlich sein. Zeitpunkt und Intensität der Analyse sind vom Projektumfeld abhängig.

Abbildung 2-1: Schritte zur strukturierten IT-Sicherheitsanalyse



Quelle: SimoBIT

Die einzelnen Schritte im Detail:

- **„Anforderungen formulieren“**: In diesem Schritt erfasst man die funktionalen Anforderungen an die gesamte Lösungen. Betrachtet man eine existierende Lösung, können sich durch die hinzugekommenen IT-Sicherheitsaspekte bestehende funktionale oder nicht-funktionale Anforderungen ändern. Zusätzlich können neue Anforderungen oder Randbedingungen hinzukommen. In diesem Schritt werden die Anforderungen dokumentiert, bewertet, validiert und an die verschiedenen Projektteilnehmer kommuniziert.
- **„Anforderungen konzeptionell umsetzen**“: die neuen oder veränderten Anforderungen müssen dann von den einzelnen Projektbeteiligten und deren Komponenten umgesetzt werden. dies bedeutet nicht zwangsläufig, dass das gesamte System implementiert werden muss. Oft ist es möglich, nur ein Systemmodell zu erstellen, welches im folgenden validiert und auch existierende Sicherheitsrisiken untersucht.

- **„Bedrohungen identifizieren“**: nach einer intensiven Beschäftigung mit der zu realisierenden oder bereits (in Teilen) realisierten Anwendung und der gewählten Technologien werden Risiken abgeleitet. Dabei sollten in diesem Schritt die Risiken nur zusammengetragen und strukturiert beschrieben werden.
- **„Bedrohungen bewerten“**: nicht jedes Risiko hat die gleiche Bedeutung und in den unterschiedlichen Anwendungen haben auch die Schutzziele unterschiedliches Gewicht. In diesem Schritt werden die Risiken anhand von verschiedenen Kriterien in eine Rangfolge gebracht. Die Bewertung bestimmt, mit welchem Aufwand jedem einzelnen Risiko begegnet werden muss.
- **„Gegenmaßnahmen identifizieren“**: für die meisten Risiken existieren technische oder organisatorische Gegenmaßnahmen. In diesem Schritt werden die passenden Gegenmaßnahmen den identifizierten Risiken zugeordnet. Meist gibt es mehrere ganz unterschiedliche Gegenmaßnahmen für ein konkretes Risiko.
- **„Aufwand für Einführung“**: durch die meisten Gegenmaßnahmen entstehen Kosten, welche in diesem Schritt aufgearbeitet werden. Dies dient dazu, eine Entscheidung zu treffen, welche der Gegenmaßnahmen konkret umgesetzt und als neue Anforderungen formuliert werden. Diese Anforderungen werden in der nächsten Iteration als gegeben angesehen und fließen in das Systemdesign mit ein.

Die einzelnen Schritte der Vorgehensweise sollten bewusst iterativ durchlaufen werden und die Ergebnisse der einzelnen Schritte sollten den Beteiligten in verständlicher Form kommuniziert werden. Je nach Projektstand ist es sinnvoll, mehrere Iterationen durchzulaufen, um die bestehende Lösung zu optimieren.

Die folgenden Kapitel des Leitfadens sind nach den Themenclustern Öffentliche Verwaltung, Maschinenbau, Handwerk und KMU und Gesundheitswirtschaft unterteilt.

In diesen Kapiteln wird jeweils die Anwendung der „Schritte zur strukturierten IT-Sicherheitsanalyse“ in den jeweiligen Projekten exemplarisch erläutert. Dabei wird deutlich, dass die Projekte teilweise unterschiedliche Einstiegspunkte in das Vorgehen gewählt haben und die einzelnen Schritte von unterschiedlicher Relevanz für das Projekt sind. Dies zeigt, dass das Modell einen flexiblen, generischen Ansatz eines strukturierten Vorgehens zur Reduzierung von Bedrohungen darstellt, welcher in vielen Bereichen anwendbar ist.

Ansprechpartner:

Fritz Meier
Geschäftsfeld Technologien
Zentrum für Intelligente Objekte ZIO
Fraunhofer-Arbeitsgruppe für
Supply Chain Services SCS
Dr.-Mack-Straße 81
90762 Fürth

Tel.: 0911 58061-9550
E-Mail: fritz.meier@scs.fraunhofer.de

3 Schritte zur strukturierten IT-Sicherheitsanalyse bei mobilen Anwendungen in der Öffentlichen Verwaltung

Die Erfahrungen aus den **SimoBIT**-Projekten **Mobility@forest**, **Mobis Pro** und **simoKIM** zeigen, dass bei der Einführung mobiler Anwendungen im Umfeld der Öffentlichen Verwaltung das Thema IT-Sicherheit eine wichtige Rolle spielt. In vielen Fällen werden personenbezogene Daten sowie Informationen über kritische mobile Infrastrukturen übertragen, welche einen hohen Schutzbedarf besitzen und nur autorisierten Personen zugänglich sein sollen. Mobile Anwendungen werfen zusätzliche Fragen in Bezug auf die Datensicherheit bei den mobilen Endgeräten und in der Kommunikation auf.

Zur Analyse der spezifischen Bedrohungen wurde bei allen drei Projekten das in Abbildung 2-1 beschriebene strukturierte Vorgehen zur Reduzierung von Bedrohungen angewendet, um die Risiken systematisch zu erfassen und adäquate Gegenmaßnahmen ergreifen zu können.

Während bei **Mobility@forest** die Verfügbarkeit der Daten im Vordergrund steht, liegt der Fokus bei **Mobis Pro** auf der Autorisierung der Anwender. Aufgrund der Verarbeitung von Daten sicherheitskritischer Infrastrukturen spielt bei **simoKIM** die Vertraulichkeit der Daten eine besondere Rolle.

3.1 IT-Sicherheit im Kontext mobiler Fachprozesse

Obwohl die drei Projekte in verschiedenen Bereichen der Öffentlichen Verwaltung angesiedelt sind, verfolgen alle ein ähnliches Ziel. Im Wesentlichen geht es bei allen drei Projekten um die Prozessoptimierung im kommunalen Umfeld durch den Einsatz von mobilen Endgeräten. Durch diese Optimierung wird die Effizienz gesteigert und die Kosten in den jeweiligen Organisationen werden gesenkt.

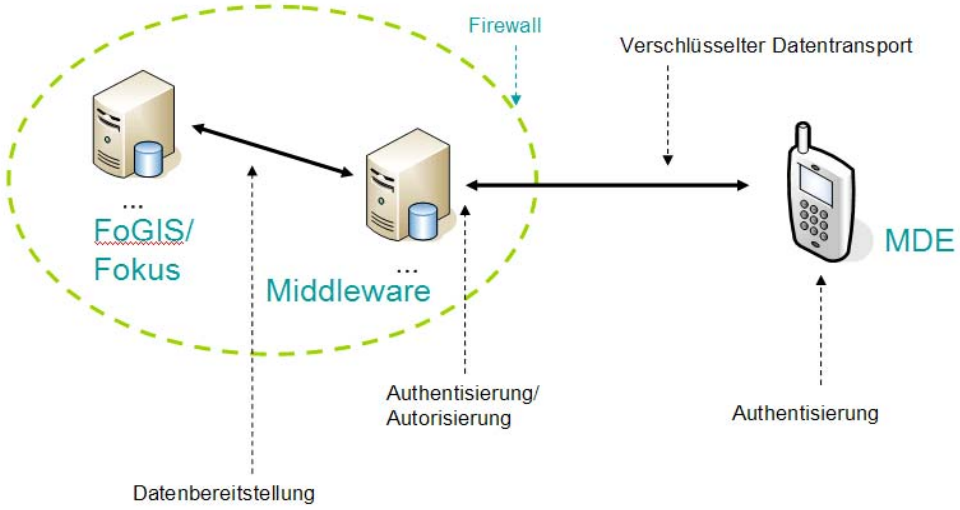
Verschiedene Ansätze der Prozessoptimierung

Im Rahmen des Forschungsprojektes **Mobility@forest** wird eine innovative und nutzerorientierte IT-Infrastruktur eines mobilen Arbeitsplatzes für Forstbetriebe entwickelt. Dabei kommt zusätzlich zum mobilen Endgerät eine Middleware[2] zum Einsatz, mit der bestehende Systeme für mobile Anwender verfügbar gemacht werden.

---

2 FoGIS: Forstwirtschaftliches Geoinformationssystem, FOKUS: Forstwirtschaftliches Datenverarbeitungssystem

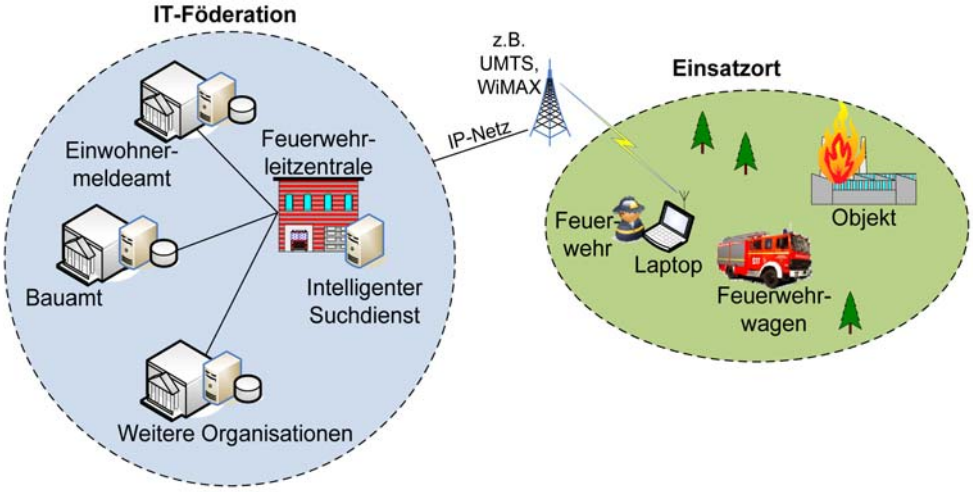
Abbildung 3-1: IT-Infrastruktur eines mobilen Arbeitsplatzes für Forstbetriebe



Quelle: Mobility@forest

Das Projekt **Mobis Pro** optimiert die gesamte Prozesskette vom vorbeugenden bis zum abwehrenden Brandschutz. Das System wird die Einsatzkräfte der Feuerwehr bei der Datenaufnahme vor Ort unterstützen, den mobilen Datenaustausch mit der Dienststelle ermöglichen und die Nachbearbeitung der erfassten Daten erleichtern. Grundlegender Ansatz ist dabei die Vereinheitlichung und Standardisierung des Zugriffs auf heterogene Daten in einem behördenübergreifenden Notfallinformationssystem. Im Einsatz unterstützt **Mobis Pro** den abwehrenden Brandschutz mit relevanten, multimedial aufbereiteten Inhalten.

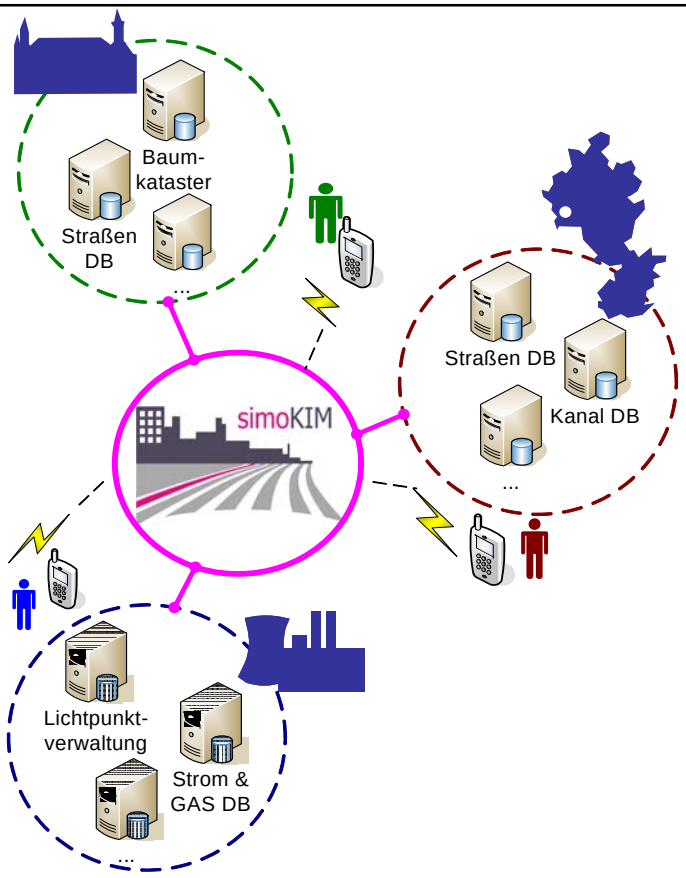
Abbildung 3-2: Mobis Pro: Optimierung der Prozesskette vom vorbeugenden bis zum abwehrenden Brandschutz



Quelle: TU Dortmund, CNI

Die Idee hinter **simoKIM** ist die Einführung einer zentralen Prozessausführungsumgebung, welche die Modellierung und Ausführung von organisationsübergreifenden Fachprozessen innerhalb einer Kommune ermöglicht. Dabei sollen über diese zentrale Ausführungsumgebung den mobilen Anwendern Daten der beteiligten Organisationen zur Verfügung gestellt werden. Darüber hinaus lassen sich organisationsübergreifende Fachprozesse einfach und unkompliziert abbilden, um deren Ausführung zu beschleunigen.

Abbildung 3-3: simoKIM: Einführung einer zentralen Prozessausführungsumgebung innerhalb einer Kommune



Quelle: simoKIM

3.2 Anwendungsszenarien und Konzepte zur Umsetzung

Das System von **Mobility@forest** basiert auf dem Einsatz einer Middleware, welche die Kommunikation zwischen den beteiligten Systemen und Organisationen regelt und die Daten gegebenenfalls zwischenspeichert. Im Wesentlichen kommunizieren hier drei verschiedene Systeme miteinander: die mobilen Datenerfassungseinheiten (MDE), die Middleware und die Bestand-Systeme. Die MDE wird vom Nutzer vor Ort im Forstbe-

trieb genutzt. Mit ihr kann der Nutzer Daten von der Middleware abrufen, aber nach der Bearbeitung auch wieder dort ablegen. Die Middleware selbst dient lediglich als Zwischenspeicher für die Bestand-Systeme und die MDE, denn die Legacy-Systeme tauschen über die Middleware die Daten mit der MDE aus. Diese Struktur macht deutlich, wie wesentlich die Verfügbarkeit aller beteiligten Systeme ist. Fällt am Ende der Kette die MDE aus, kann der Nutzer seiner Tätigkeit nicht mehr nachgehen. In Verbindung mit einem Datenverlust müssten Daten neu erfasst werden, was Kosten verursacht. Fällt die Middleware aus, entstehen Verzögerungen beim Datenaustausch mit den Bestand-Systemen. Die Verfügbarkeit der Bestand-Systeme ist zwar wesentlich, aber nicht Bestandteil des **Mobility@forest**-Projekts.

Das Projekt **Mobis Pro** hat eine Prozessoptimierung im Umfeld des Rettungswesens zum Ziel. Rettungsorganisationen wie Feuerwehr, THW, DRK oder Polizei sehen sich nach wie vor mit dem Problem einer mangelnden Verfügbarkeit von detaillierten und aktuellen Informationen über den Einsatzort konfrontiert. Der Zugriff auf Informationen, die sich auf verteilten Informationssystemen befinden, ist im konkreten Einsatzfall aktuell sehr beschränkt und muss je nach Situation erst angefordert werden. Für die effiziente Feuerwehreinsatzplanung und für den vorbeugenden Brandschutz soll im **Mobis Pro**-Projekt ein zentrales Notfallinformationssystem entwickelt werden, welches die verteilten Informationssysteme (z. B. Bauamt, Einwohnermeldeamt) sicher miteinander verknüpft und gefilterte Informationen dem Feuerwehrmann vor Ort bereitstellt. Da Informationssysteme zum Teil sensible Daten besitzen, spielen Sicherheitsanforderungen wie Vertraulichkeit, Integrität, Authentifizierung und Autorisierung eine wichtige Rolle. Eine Authentifizierung ist hier beispielsweise notwendig, um den Zugang zu diesen Daten zu schützen. Aufgrund des großen Informationspools ist weiterhin ein Berechtigungskonzept (Autorisierung) erforderlich, welches den Zugriff auf bestimmte Daten verwaltet und steuert. So hat zum Beispiel ein Einsatzleiter im abwehrenden Brandschutz ein anderes Berechtigungsprofil als ein Brandschutzgutachter beim vorbeugenden Brandschutz. Beim Austausch der Daten zwischen dem zentralen Notfallinformationssystem der Feuerwehr und den Informationssystemen der Behörden muss außerdem die Datenintegrität sichergestellt werden, damit der Empfänger sicherstellen kann, dass die Daten bei der Übertragung nicht manipuliert und die Absenderinformationen nicht gefälscht wurden.

Im Projekt **simoKIM** wird der Ansatz durch den Einsatz einer zentralen Prozessaufführungsumgebung verfolgt, um die organisationsübergreifenden Prozesse im Kontext der Verwaltung der Straßeninfrastruktur zu optimieren und zu vereinfachen. Als Beispiel können hier gemeinsame Bauvorhaben mit der Stadtverwaltung, mit Gas- und Stromanbietern sowie den Telekommunikationunternehmen genannt werden. Da dadurch im **simoKIM**-System Daten über kritische Infrastrukturen wie zum Beispiel Strom- oder Gasleitungen verarbeitet werden, ist die Sicherheit dieser Daten eine enorm wichtige Anforderung. Obwohl die klassischen Eigenschaften der IT-Sicherheit wie Integrität, Vertraulichkeit und Verfügbarkeit eine wichtige Rolle spielen und auch weitere Aspekte

wie etwa die Authentizität nicht zu vernachlässigen sind, wird im Folgenden der Fokus auf die Vertraulichkeit der Daten in **simoKIM** gelegt.

Neben vielen anderen Anwendungsfällen werden im **simoKIM**-Projekt Daten über Straßeninfrastrukturen, die bei verschiedenen kommunalen Organisationen gespeichert sind, mobilen Anwendern zur Verfügung gestellt. Dabei handelt es sich oft um Daten über so genannte kritische Infrastrukturen wie z. B. Gas-, Strom oder Wasserleitungen, die besonders schützenswert sind. Die **simoKIM**-Prozessaufführungsumgebung, auf die von mobilen Anwendern angefragt wird, greift auf die Daten dieser Organisationen zu, verschneidet gegebenenfalls mehrere Datensätze, wie z. B. Kartenmaterial, zu einem und stellt diese dem Anwender zur Verfügung. Je nach Vertraulichkeitsstufe der Daten dürfen diese nur vom entsprechend authentifizierten und autorisierten Anwender eingesehen werden und dürfen nicht im **simoKIM**-System im Klartext verarbeitet werden. Darüber hinaus müssen alle Daten sicher übertragen und abgesichert auf den mobilen Geräten abgelegt werden, damit im Falle eines Verlustes des Gerätes diese nicht eingesehen werden können.

3.3 Identifizierte Bedrohungen

Wie eingangs im Anwendungsszenario beschrieben, muss die Datenverfügbarkeit im **Mobility@forest**-Projekt bei den MDEs sowie bei der Middleware sichergestellt werden.

Da es sich bei der MDE um ein mobiles Gerät handelt, welches im Außeneinsatz genutzt wird, ist es diversen Bedrohungen ausgesetzt. Die Verfügbarkeit kann z. B. durch einen Defekt oder durch Verlust des Gerätes eingeschränkt werden. In erster Linie wäre davon der Anwender betroffen, da entweder die bereits erfassten Daten, und somit geleistete Arbeit verloren wäre, oder er der weiteren Ausführung seiner Tätigkeit nicht nachkommen könnte.

Als Verursacher kommen folgende Faktoren in Frage:

- Umwelteinflüsse – z. B. Regen oder Schmutz, können die Einsatzfähigkeit des Geräts einschränken oder es sogar komplett zerstören,
- unsachgemäße Handhabung – z. B. durch Fallenlassen, hat vergleichbare Auswirkungen wie schädigende Umwelteinflüsse. Allerdings ist gerade hier die Gefahr des Datenverlustes hoch, falls die Festplatte des Geräts in Mitleidenschaft gezogen wird.
- Diebstahl – bei mobilen Geräten ist die Gefahr des Diebstahls höher als bei stationären Geräten.

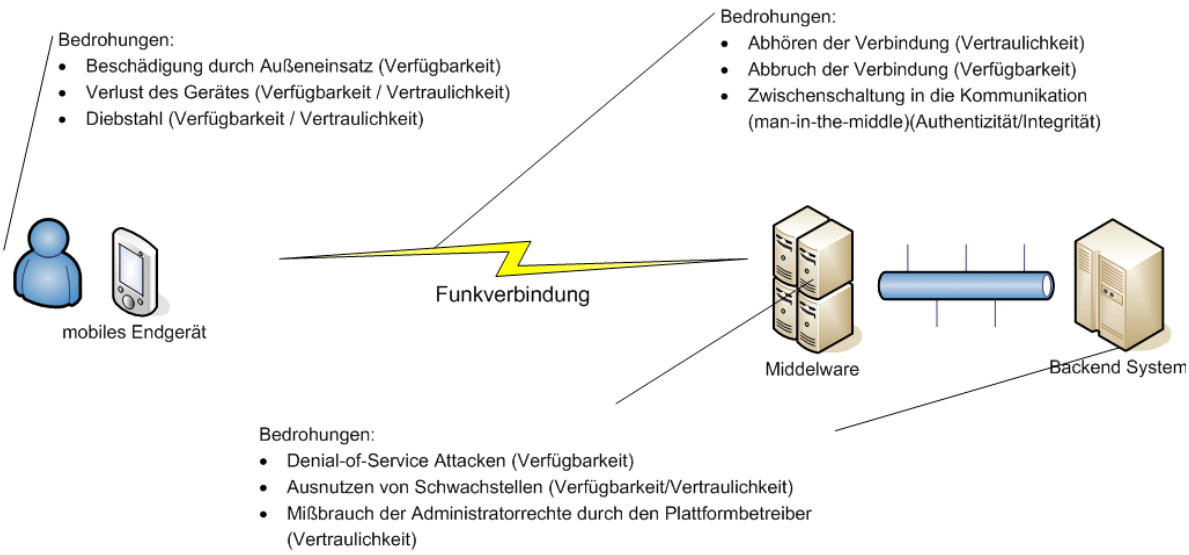
Die Middleware betreffend sind die Bedrohungen weniger vielfältig und weniger schwerwiegend, da diese nur als Zwischenspeicher dient. Fällt sie aus, ist der Datenaustausch der MDEs mit den Legacy-Systemen gestört. Da die Verarbeitung der mit einer MDE erfassten Daten aber nicht zeitkritisch ist, fällt der Ausfall der Middleware, wenn auch nur vorübergehend, nicht so sehr ins Gewicht.

Obwohl bei **Mobis Pro** die Verfügbarkeit der Daten eine wichtige Rolle spielt, wird im Folgenden die Autorisierung und Authentifizierung der Anwender in den Fokus gerückt. Würde die Authentifizierung und Autorisierung im **Mobis Pro**-System bei einem abwehrenden Brandschutz nicht existieren, könnte jede Feuerwehreinheit mittels eines mobilen Clients auf alle sensiblen Daten zugreifen und diese unter Umständen manipulieren oder sogar relevante Informationen löschen. Im Falle des Missbrauchs der vorhandenen und erteilten Berechtigungen könnte ein erheblicher wirtschaftlicher Schaden entstehen, wenn relevante Informationen während des Feuerwehreinsatzes angefordert und für illegale Zwecke eingesetzt werden.

Aus dem eingangs beschriebenen Anwendungsszenario im **simoKIM**-System ergeben sich mehrere Risiken. Zum Einen wäre es denkbar, dass die Daten auf dem Weg von der Organisation, die diese zur Verfügung stellt, zum Anwender von einem Angreifer abgehört werden. Dieses Abhören kann auf mehrere Arten erfolgen. Zum Anderen wäre das Abhören des Übertragungskanals denkbar. Dazu zählen Angriffe auf die kabelgebundene Übertragung bzw. Funkübertragung der Daten, wobei sich der Angreifer in irgendeiner Form Zugang zu der benutzten Infrastruktur verschaffen oder Funksignale abhören könnte. Da die Daten, die zwischen den angeschlossenen Organisationen und dem mobilen Anwender übertragen werden, auf jeden Fall über die zentrale **simoKIM**-Prozessausführungsumgebung weitergeleitet werden, sind auch Angriffe denkbar, bei denen sich der Angreifer Zugriff zu der Infrastruktur dieses zentralen Systems verschafft. Hier könnte er das System entsprechend manipulieren, um die Daten, die im Klartext verarbeitet werden, abzugreifen und zu einem anderen, von ihm kontrollierten, System umzuleiten.

Die folgende Grafik zeigt eine mögliche Kommunikationsarchitektur einer mobilen Anwendung und weist auf die Bedrohungen der einzelnen Komponenten hin.

Abbildung 3-4: Mögliche Kommunikationsarchitektur einer mobilen Anwendung und Bedrohungspotenzial



Quelle: simoKIM

3.4 Bewertung der Bedrohungen

Die größte Bedrohung im **Mobility@forest-**Projekt ist der Verlust der MDE, sei es durch Diebstahl oder durch einen durch äußere Einflüsse verursachten Totalschaden mit möglichem Datenverlust. Der Verlust der MDE verursacht in doppeltem Maße Kosten: Zum Einen muss das Gerät ersetzt werden und zum Anderen entstehen Kosten für die erneute Eingabe der Daten. Je nachdem, über welchen Zeitraum Daten erfasst wurden, können die daraus resultierenden Kosten erheblich sein.

Die Wahrscheinlichkeit eines geplanten Einbruchs in das Notfallinformationssystem im **Mobis Pro**-System ist eher gering. Selbst bei einem simulierten groß angelegten Terrorangriff wurde nicht versucht, die Rettungskräfte durch Fehlinformationen zu beeinträchtigen. Wahrscheinlicher sind die Bedrohungen durch zufälliges Abfangen von Informationen durch Abhören von mobilen Kommunikationsinfrastrukturen sowie ein Ausfall des Systems durch DoS-Attacken. Beides wird gerade von jugendlichen Hackern (Stichwort „Script-Kiddies“) ohne besondere Hintergrundmotivation bei der Zielauswahl als eine Art „Sport“ betrieben.

Größeres Gefahrenpotential bietet das Abfangen von sensiblen Informationen, wie z. B. der Bauplan des Tresorraumes einer Bank oder personenbezogene Daten. Das Risiko steigt analog zu der Wahrscheinlichkeit, mit der die Daten für kriminelle Handlungen

eingesetzt werden können. Da überwiegend Informationen mit geringer Sicherheitseinstufung zu erwarten sind, wird dieses Risiko als eher gering eingestuft.

Die Tatsache, dass im **simoKIM**-System Daten über kritische Infrastrukturen verarbeitet werden, stellt bei einem Verlust der Vertraulichkeit dieser Daten ein ernst zu nehmendes Sicherheitsrisiko dar. Da die Sicherheitsanforderungen an den Umgang mit diesen Daten gesetzlich geregelt sind, müssen diese zwangsläufig grundsätzlich verschlüsselt übertragen und gespeichert werden. In diesem Zusammenhang existieren mehrere Sicherheitsrichtlinien, die zum Teil die für die Verschlüsselung verwendeten Algorithmen und Schlüssellängen festlegen.

3.5 Identifizierte Gegenmaßnahmen

Die erste Sicherheitsanforderung ist die Authentifizierung, die den Zugang zu den Daten entsprechender Behörden schützt, weil es sich häufig um sensible, personenbezogene Datenbestände handelt, die nicht jedermann zugänglich gemacht werden dürfen. Beispielhafte Sicherheitsmechanismen zur Authentifizierung stellen die Verwendung langer Passwörter, 2-Faktor Authentifizierung bzw. biometrische Methoden dar, um hohem bzw. sehr hohem Schutzbedarf gerecht zu werden. Eine weitere Sicherheitsanforderung ist die Autorisierung, welche die Berechtigung für den Zugriff auf bestimmte Daten regelt (RBAC) und andere Zugriffsmethoden wie Firewalls für Portfilterung regelt, um einen hohen bzw. sehr hohen Schutzbedarf zu erzielen. Um die Nutzeraktivitäten zu identifizieren, ist es notwendig, dass die Identität des Nutzers eindeutig den entsprechenden Aktivitäten zugeordnet werden kann (Sicherheitsanforderung: Verbindlichkeiten). Hierfür können Protokollierungsdienste mit Einsatz von Zertifikaten, die von einer vertrauenswürdigen Zertifizierungsstelle signiert wurden, eingesetzt werden.

Die Sicherstellung der Vertraulichkeit der Daten muss auf zwei Ebenen erfolgen. Zum Einen müssen die Daten beim Transport zwischen den Organisationseinheiten abgesichert werden, zum Anderen müssen die Daten, die auf den mobilen Endgeräten (zwischen-) gespeichert sind, vor Fremdzugriffen abgesichert werden. Der Transport der Daten zwischen den jeweiligen Entitäten erfolgt häufig über das HTTP-Protokoll. Als Protokoll auf Applikationsebene kann SOAP zum Einsatz kommen. Der Einsatz des HTTP-Protokolls ermöglicht die Verwendung von SSL zur Absicherung der gesamten Kommunikation zwischen zwei in der Kommunikationskette direkt benachbarten Entitäten. Eine Alternative dazu stellt der Einsatz des Standards WS-Security dar. Dabei werden Technologien wie XML-Encryption und XML-Signature verwendet, welche eine kryptografische Absicherung der Daten auf Nachrichten- oder gar Informationsebene erlauben.

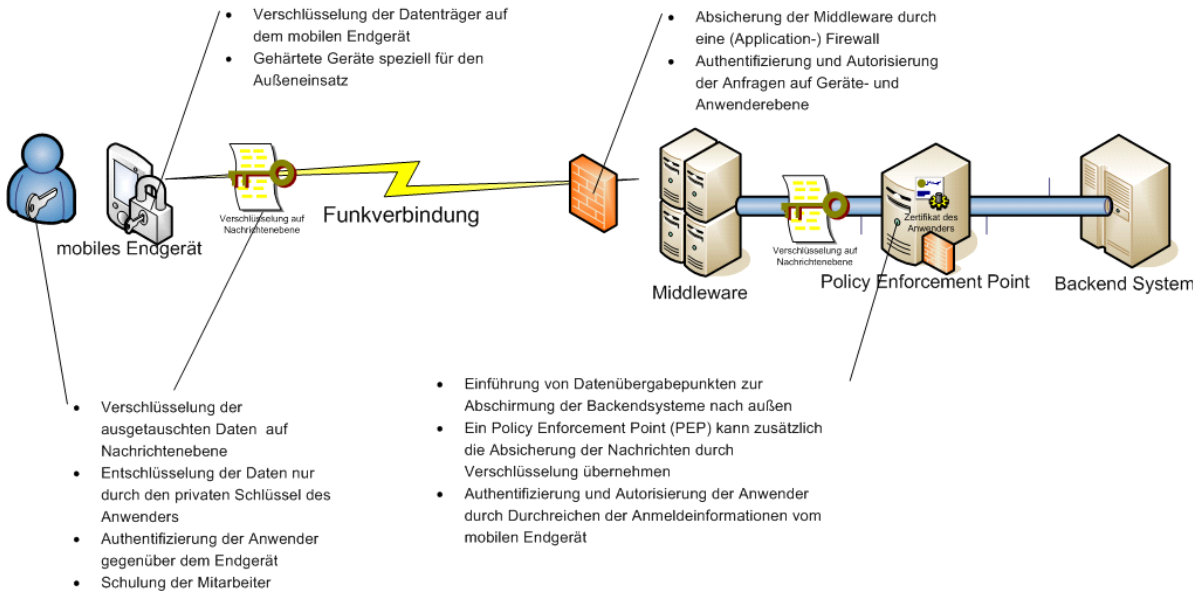
Bei der Absicherung der gespeicherten Daten auf dem Datenträger der mobilen Endgeräte kommen grundsätzlich ebenfalls zwei Optionen in Frage. Es ist möglich, den gesamten Datenträger durch Verschlüsselung auf Datenträgerebene abzusichern. Die

Alternative dazu stellt eine dateiorientierte Verschlüsselung dar, die Dateien unabhängig vom Datenträger schützt, womit auch z. B. sichergestellt wird, dass die Backupdaten ebenfalls verschlüsselt bleiben, wodurch ein durchgängiges Verschlüsselungskonzept möglich ist. Bei mobilen Anwendungen muss insbesondere die Verfügbarkeit sichergestellt werden, da sonst die entsprechenden Tätigkeiten gar nicht oder nur eingeschränkt durchgeführt werden können. In einem verteilten System ist das Ausfallrisiko, beispielsweise durch einen Angriff auf die Verfügbarkeit, als relativ hoch einzuschätzen. Die hohe Verfügbarkeit ist somit für den Erfolg des Einsatzes entscheidend. Neben der Gewährleistung der Verfügbarkeit im Backendsystem, muss bei mobilen Einsätzen auch die funkbasierte Verfügbarkeit erfüllt werden, damit das Backendsystem jederzeit erreichbar bleibt.

Bestimmte Anwendungen wie z. B. beim **Mobility@forest**- und **Mobis Pro**-Projekt erfordern auch eine sichere und robuste Hardware am Einsatzort. Bei der Brandschau im vorbeugenden Brandschutz kann es z. B. zu besonderen klimatischen Bedingungen (z. B. Tiefkühllager) sowie auch zu schmutzigen Arbeitsbereichen (z. B. Hüttenbetrieb) kommen, welche robuste mobile Endgeräte voraussetzen. Darüber hinaus müssen die erfassten Daten auf dem mobilen Endgeräten sicher verschlüsselt abgelegt werden, damit diese nicht beim Diebstahl des Gerätes gelesen werden können.

Eine nicht zu unterschätzende Sicherheitsmaßnahme stellt zudem die Schulung und Sensibilisierung der Anwender dar. Nur der bewusste Umgang mit den IT-Systemen ermöglicht das Erkennen von Bedrohungen und trägt wesentlich zum Schutz der Daten bei.

Abbildung 3-5: Mögliche Gegenmaßnahmen gegen Bedrohungen



Quelle: simoKIM

3.6 Ausgewählte Gegenmaßnahmen

Die Authentifizierung, die den Zugang zu sensiblen Daten schützt, ist elementarer Bestandteil eines jeden Sicherheitskonzeptes. Erweitert um ein Role Based Access Control Model werden Zugriffsrechte mittels Berechtigungen und Rollen definiert und zugleich administrativer Overhead reduziert. Zusätzlich können Systeme und die zugehörigen Systemkomponenten durch ein Virtual Private Network in Kombination mit Firewalls geschützt werden. Alle Nutzeraktivitäten sollten protokolliert werden, um eine gerichtliche Nachvollziehbarkeit zu ermöglichen.

Bei Einsatz einer SOA (Service orientierten Architektur) bringt der Einsatz von WS-Security wesentliche Vorteile gegenüber SSL mit sich. Im Gegensatz zu SSL, mit welchem nur eine Absicherung der Kommunikationsleitung möglich ist, kann mit WS-Security eine über mehrere Kommunikationsknoten durchgehende Absicherung der einzelnen Nachrichten empfängerorientiert umgesetzt werden. Dadurch können die Daten von einer Organisationseinheit gezielt für einen bestimmten Empfänger oder eine Empfängergruppe verschlüsselt werden. Durch die Verschlüsselung auf Nachrichten- oder Datensatzebene ist auch eine Verarbeitung der Daten im verschlüsselten Zustand möglich. Das so genannte SAML-Framework kann zur sicheren Vernetzung von Informationssystemen verwendet werden. Es nutzt Sicherheitsmechanismen wie XML-Security (XML-Encryption, XML-Signature), SSL/TLS, digitale Signaturen und PKI. Diese Sicherheitsfunktionen sollen Anforderungen wie Vertraulichkeit, Authentizität von Sender und Empfänger, Integrität und Verbindlichkeit erfüllen. Es gibt verschiedene Anforderungen für unterschiedlichen Schutzbedarf, die davon abhängen können, wie sensibel die Daten sind oder auch welche (gesetzlichen) Vorgaben existieren. Um einen hohen Schutzbedarf zu erfüllen, kann das Verschlüsselungsverfahren 3DES als Sicherheitsmechanismus genutzt werden. Sollte jedoch ein noch höherer Schutzbedarf erwünscht sein, so muss das Schlüsselverfahren AES eingesetzt werden. Um die Daten vor Manipulation zu schützen, können Sicherheitsmechanismen wie z. B. die Hash-Funktionen MD5 für den hohen Schutzbedarf oder der SHA für den sehr hohen Schutzbedarf verwendet werden.

Auch bei der Datenträgersicherheit empfiehlt sich die Verwendung von dateiorientierten Technologien. Dies hat den Vorteil, dass auf den mobilen Endgeräten, welche nur begrenzte Ressourcen zur Verfügung haben, nicht bei jedem Datenträgerzugriff kryptographische Operationen nötig sind, sondern nur bestimmte Dateien ver- und entschlüsselt werden. Dies hat allerdings den Nachteil, dass eine deutlich komplexere Technologie notwendig ist, die es ermöglicht, verschlüsselte Daten zu filtern und nach entsprechender Autorisierung gezielt zu entschlüsseln. Mit Load-Balancing und vertikalen Handover-Verfahren (nahtlose Kommunikation, z. B. Kombination von UMTS und WLAN) kann die Verfügbarkeit der Systeme erhöht werden, wenn Load-Balancing Verfahren in Kombination mit Redundanz-Systemen eingesetzt werden. Weiterhin kann die mobile Verfügbarkeit beim Einsatzort durch vertikale Handover-Verfahren erhöht werden, beispielsweise im Falle einer schwachen WLAN-Verbindung wird die Kommunikation möglichst unterbrechungsfrei über einen anderen mobilen Zugang wie UMTS oder WiMAX fortgesetzt.

Um die Gerätesicherheit und die damit verbundene Datensicherheit zu gewährleisten, empfiehlt sich der Einsatz von so genannten „Ruggedized“-Geräten, die speziell für Outdoor Mobile Computing geeignet sind und maximalen Schutz für empfindliche Komponenten, wie etwa das Display, bieten. Festplatten sollten stoß- und vibrationsgeschützt gelagert sein; hier empfiehlt sich der Einsatz von Solid State Drives (SSD), einem Speichermedium ohne bewegliche Teile, nur mit Flash-Speicher, das absolut stoßunempfindlich ist. Allgemeine Sturzunempfindlichkeit sowie Widerstandfähigkeit gegen Wasser und Schmutz müssen gewährleistet sein. Für die Klassifizierung des Schutzgrades gibt es die so genannte Schutzart. Die Schutzart gibt an, wie sehr elektrische Betriebsmittel für bestimmte Umwelt/ Umgebungsbedingungen geeignet sind und wie sehr der Nutzer gegen Gefahren bei deren Benutzung geschützt ist. Die Schutzart besteht aus zwei Ziffern. Die erste steht für Berührungs- und Fremdkörperschutz und die zweite für Wasserschutz. Für unser Anwendungsszenario benötigen wir die Schutzart IP54, welche Schutz gegen Staubablagerung (IP5x) und Schutz gegen allseitiges Spritzwasser (IPx4) sicherstellt. Damit aber auch im schlimmsten Fall keine Daten verloren gehen, werden zusätzlich regelmäßige Backups empfohlen.

Checkliste Öffentliche Verwaltung

Wichtige Hinweise für mobile IT-Sicherheit in der Öffentlichen Verwaltung

Die IT-Sicherheit wird grundsätzlich in die Disziplinen Vertraulichkeit, Verfügbarkeit oder Integrität unterteilt.

Bei prozessorientierten Ansätzen muss die Sicherheit Bestandteil der Prozesse sein.

Der Einsatz von mobilen Geräten stellt ein grundsätzliches Sicherheitsrisiko dar.

Die Sicherheitsmaßnahmen müssen den Anforderungen angemessen sein und die Benutzung des Systems nicht behindern.

Ansprechpartner:

Stefan Faltus (für Mobility@forest)
ATB Bremen
Wienerstr. 1
28359 Bremen
Tel.: 0421 22092 43
Fax: 0421 22092 10
E-Mail: faltus@atb-bremen.de

Martin Oczko (für simoKIM)
Leiter des Arbeitsforums IT-Sicherheit
Utimaco Safeware AG
Germanusstrasse 4
52080 Aachen
Tel: 0241 1696 235
Fax: 0241 1696 199
E-Mail: Martin.Oczko@aachen.utimaco.de

Thang Tran (für Mobis Pro)
Technische Universität Dortmund
Lehrstuhl für Kommunikationsnetze
Otto-Hahn-Str. 6
44227 Dortmund
Tel.: 0231 755 7815
Fax: 0231 755 6136
E-Mail: thang.tran@tu-dortmund.de

4 Mobile IT-Sicherheit in Handwerk und KMU: Digitale Zertifikate für sichere mobile Anwendungen

4.1 Spezifische Herausforderungen für Handwerk und KMU bei der Realisierung mobiler Anwendungen

Die Entwicklung sowie der Betrieb mobiler Anwendungen sollen nicht nur für große Unternehmen möglich sein, sondern auch für *kleine und mittlere Unternehmen* (KMU), wozu insbesondere auch Handwerksbetriebe zählen.

Speziell im handwerklichen Gewerbe existieren viele Anwendungsgebiete, die durch den Einsatz mobiler Technologien deutlich verbessert werden können: Ein Außendienstmitarbeiter ist beispielsweise nicht mehr auf Anleitungen oder Kundendaten auf Papier angewiesen – ein Ausgabemedium, das schnell veraltet und mit hohen Materialkosten verbunden ist.

Ebenso erfährt der umgekehrte Informationsfluss – vom Außeneinsatz zurück ins Unternehmen – eine drastische Verbesserung: Die bei einem Kunden vor Ort erfassten Bestelldaten oder Messwerte sind durch mobile Anwendungen sofort in der unternehmenseigenen Software verfügbar. Aufwändige und fehleranfällige Nacherfassungen entfallen.

Um die unstrittigen Potenziale mobiler Technologien zu realisieren, müssen im Vorfeld die zugehörigen mobilspezifischen Sicherheitsprobleme gelöst werden: Mobile Anwendungen sind beispielsweise aufgrund der Endgerätegröße sowie ihrer Einsatzszenarien besonders anfällig für Verlust und Diebstahl. Darüber hinaus ist in technischer Hinsicht eine drahtlose Kommunikation prinzipiell leichter angreifbar als eine herkömmliche drahtgebundene.

Dem entgegenwirkend stellen zertifikatsbasierte Systeme Technologien zur Verfügung, die diese Sicherheitsprobleme bewältigen.

4.2 Digitale Zertifikate für sichere mobile Anwendungen

4.2.1 Was sind digitale Zertifikate?

Ein digitales Zertifikat besteht aus strukturierten Daten. Es enthält eine digitale Signatur, die von einer autorisierten Instanz, der so genannten Zertifizierungsstelle, ausgegeben, beglaubigt und somit „zertifiziert“ wird. Darüber hinaus beinhaltet ein Zertifikat generell den Namen des Ausstellers, Angaben über die Identität des Zertifikatsinhabers sowie einen Gültigkeitszeitraum. Ein Zertifikat ist mit einem Ausweis vergleichbar.

Nachfolgende Abschnitte beleuchten die Zusammenhänge zwischen Datenverschlüsselung, einer digitalen Unterschrift, Zertifikaten und Zertifizierungsstellen.

4.2.1.1 Die Datenverschlüsselung mit Zertifikaten

Das Grundprinzip einer Verschlüsselung mit Zertifikaten ist sehr einfach. Jeder Nutzer, der durch Verschlüsselung geschützte Nachrichten empfangen möchte, erzeugt ein zusammengehöriges Schlüsselpaar: einen öffentlichen Schlüssel (engl. *public key*) sowie einen privaten (engl. *private key*) – ähnlich einem offenen Vorhängeschloss samt passendem Schlüssel. Dabei ist ein öffentlicher Schlüssel das Gegenstück zu einem privaten, der nur dem Schlüsselinhaber bekannt ist.

Private Schlüssel müssen aus diesem Grund von ihren Besitzern sicher verwahrt werden; öffentliche Schlüssel hingegen können beliebig verbreitet werden (z. B. in öffentlichen Verzeichnissen ähnlich einem Telefonbuch) und jeder kann sie verwenden, indem er einfach das Vorhängeschloss „einschnappen“ lässt.

Abbildung 4-1: Privater und öffentlicher Schlüssel

Quelle: M3V

4.2.1.2 Schlüssel und digitale Zertifikate

Bevor ein Schlüssel von einem Schlüsselinhaber veröffentlicht werden kann, erhält dieser eine eindeutige Seriennummer, die ihn von anderen öffentlichen Schlüsseln unterscheidet und seinem Besitzer eindeutig zuordnet. Das „Aufprägen“ dieser Seriennummer übernimmt eine spezielle Zertifizierungsstelle, die darüber hinaus die Identität des Besitzers gegenüber Dritten garantiert. Daraus ergibt sich ein **digitales Zertifikat**, das einen definierten öffentlichen Schlüssel beinhaltet und diesen einer bestimmten Person, einem Unternehmen usw. beglaubigt zuordnet.

Ein digitales Zertifikat enthält für Dritte kein besonderes Geheimnis: Jeder kann das Zertifikat einsehen. Durch mathematische Verfahren wird jedoch sichergestellt, dass die

Werte eines öffentlichen Schlüssels nicht veränderbar sind, ohne diese Veränderungen einfach erkennen zu können. Ein digitales Zertifikat ist darüber hinaus beliebig oft kopierbar. Es existieren öffentliche Verzeichnisdienste, vergleichbar mit einem Telefonbuch, die viele Zertifikate speichern und die schnelle Suche nach dem Zertifikat einer bestimmten Person oder Firma ermöglichen.

Abbildung 4-2: Privater Schlüssel und Zertifikat

Quelle: M3V

4.2.2 Verschlüsselung und Signatur mit digitalen Zertifikaten

Die **Verschlüsselung geheimer Daten** mit digitalen Zertifikaten kann man sich so vorstellen, dass ein Geheimnis in eine sichere Kiste gepackt und diese mit dem Zertifikat verschlossen wird. Nur der Besitzer des privaten Schlüssels kann das Schloss öffnen und das Geheimnis entnehmen. Wer der Besitzer des privaten Schlüssels ist, kann der auf dem Zertifikat aufgeprägten Identität entnommen werden.

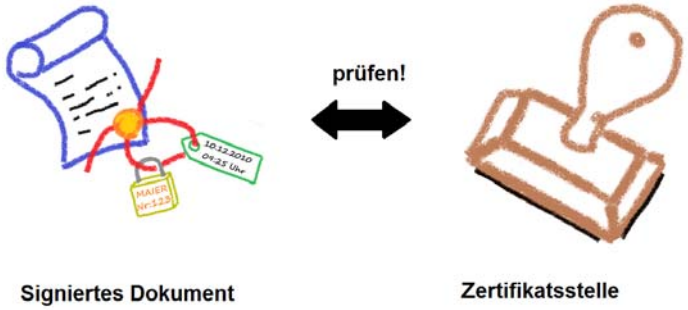
Abbildung 4-3: Dokument verschlüsseln

Quelle: M3V

Zertifikate dienen neben der Verschlüsselung geheimer Daten auch zur **digitalen Signatur für elektronische Dokumente**: An ein vorhandenes Dokument wird eine digitale Prüfsumme in Form eines Siegelbands angebracht. Hierzu wird der private Schlüssel

benötigt, d. h. nur der Besitzer des privaten Schlüssels kann das Dokument unterschreiben. An diesem Siegelband hängt das Zertifikat; das Siegel enthält die Uhrzeit der Unterschrift. Jeder kann das Dokument weiterhin lesen, da die Signatur nur eine Ergänzung darstellt.

Abbildung 4-4: Digitale Signatur eines Dokuments überprüfen



Quelle: M3V

Die Dokumentsignatur kann über die Unversehrtheit des Siegelbands (der Prüfsumme) mithilfe des Zertifikats sowie einer Zertifikatskontrolle gegenüber der Zertifizierungsstelle von jedem überprüft werden.

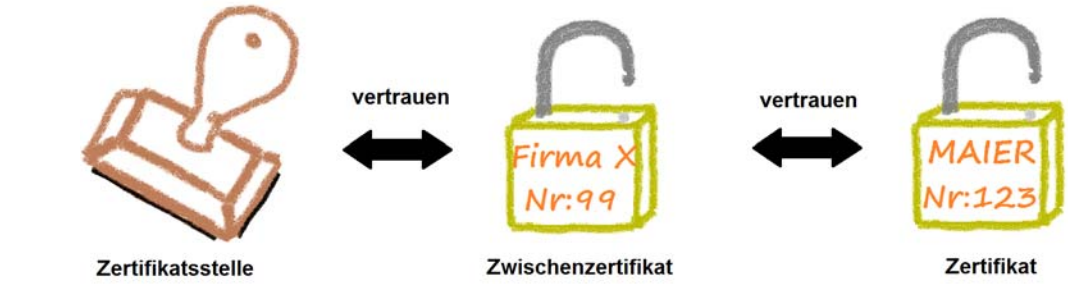
4.2.3 Ausstellung, Lebensdauer und Kosten digitaler Zertifikate

Der freie Austausch von Signaturen oder Verschlüsselungen im Internet oder unter Personen bzw. Organisationen bedarf einer Zertifikatsausstellung durch offizielle Stellen wie Firmen oder Behörden, die auf diese Ausstellung spezialisiert sind (z. B. durch VeriSign, Thawte, Deutsche Telekom). Nur bei einem Zertifikat von einer „echten“ Zertifizierungsstelle akzeptiert die Gegenseite das Zertifikat (z. B. in einem Webbrowser, der auf einen mit SSL-Verschlüsselung arbeitenden Webserver einer Firma zugreift).

Die Zertifizierungsstelle (auch „Certification Authority“, CA) stellt Zertifikate aus und legt einen oder mehrere Einsatzbereiche fest. Beispielsweise existieren Zertifikate, die ausschließlich für Verschlüsselungszwecke ausgestellt werden, und solche, die nur für Signaturen bestimmt sind oder Zertifikate, die beide Anwendungsfälle abdecken.

Ein Zertifikat wird außerdem fest mit einer Identität gekoppelt, wobei es sich bei diesen Identitäten sowohl um „natürliche“ Personen („Herr Maier“) als auch um Maschinen („Webserver der Firma X“) handeln kann. Abgesehen hiervon sind auch Zertifikatsketten nicht unüblich: Ein Zertifikat wird verwendet, um einem weiteren Zertifikat zu vertrauen.

Abbildung 4-5: Zertifikatsketten



Quelle: M3V

Zertifikate sind nur innerhalb eines bestimmten Zeitraums gültig, der von der Zertifizierungsstelle definiert wird und der sich über mehrere Jahre erstrecken kann. Ist die Gültigkeit eines Zertifikats abgelaufen, wird ein neues benötigt. Somit kann ein potenzieller Dieb eines privaten Schlüssels das Zertifikat nicht beliebig lang verwenden. Zudem könnte der technische Fortschritt künftig den Einsatz „stärkerer“ Zertifikate erfordern.

Eine Zertifikatsausstellung durch eine externe Zertifizierungsstelle ist nicht kostenlos. Der zu entrichtende Preis hängt von der Laufzeit, dem Verwendungszweck und der Qualität (Verfahren zur Identitätsfeststellung durch die Zertifizierungsstelle) ab und liegt heutzutage in einer Größenordnung von mehreren hundert Euro.

Gestohlene, verlorene oder nicht mehr benötigte private Schlüssel nebst zugehörigen Zertifikaten kommen auf die so genannte Sperrliste (*Certificate Revocation List*, CRL) der Zertifizierungsstelle.

Neben der Zertifizierungsstelle, die Zertifikate ausgibt, können diese auch selbst erstellt werden. Hierfür existieren spezielle Programme (siehe http://www.openssl.org/), die frei verfügbar sind.

4.2.3.1 Technischer Hintergrund von Verschlüsselungsverfahren

Grundsätzlich werden bei Verschlüsselungsverfahren asymmetrische (z. B. RSA, Diffie-Hellman, elliptische Kurven) und symmetrische Verfahren (z. B. AES, DES, 3DES) sowie die Berechnung von Prüfwerten (so genannte Hash-Funktionen wie MD5 oder SHA1) unterschieden.

Jedes dieser Verfahren besitzt eine individuelle Grenze, die definiert, ab welcher Schlüssellänge – ausgedrückt durch die Anzahl von Bits – das Verfahren als „sicher“ gilt. Beispielsweise wird bei dem symmetrischen Verschlüsselungsverfahren AES die

Bit-Länge *256* als sicher angenommen, während beim asymmetrischen Verfahren RSA der Schlüssel mindestens eine Länge von *1.280* Bits haben sollte.

In Abhängigkeit von dem jeweiligen Verschlüsselungsverfahren können demnach stark voneinander abweichende Schlüsselmindestlängen existieren.

4.2.3.2 Speicherung von privaten Schlüsseln

Ein privater Schlüssel muss immer sicher verwahrt werden.

Speichert man den privaten Schlüssel als Datei (d. h. als „Soft-Token“) auf einem beliebigen Datenträger, ist er im Normalfall lediglich durch ein Passwort geschützt. Die Verwendung ist nur schwer zu kontrollieren und ein Kopiervorgang der Datei wird nicht bemerkt.

Verschlüsselungs- oder Signaturzertifikate werden zusammen mit dem privaten Schlüssel oft auf speziellen Speichermedien, genannt „SmartCards“, ausgegeben. Bei SmartCards handelt es sich um kleine Computerchips, die in eine Bankkarte oder in ein Ausweisdokument integriert sind. Dadurch kann ein Benutzer den privaten Schlüssel sowie die passenden Zertifikate immer mit sich führen. Bei SmartCards erfolgt die Verwendung des privaten Schlüssels in gesicherter Umgebung auf der SmartCard selbst. Der private Schlüssel ist nicht auslesbar auf der Chipkarte hinterlegt und erst die Eingabe einer PIN (Authentifizierung) schaltet die Verwendung frei. Zahlreiche technische Maßnahmen verhindern das Auslesen des privaten Schlüssels oder das Kopieren des Inhalts einer SmartCard auf eine andere.

4.3 Einsatz von Zertifikaten in den SimoBIT-Projekten für Handwerk und KMU

In den drei **SimoBIT**-Projekten für Handwerk und KMU **ModiFrame**, **M3V** und **MAREMBA** werden so genannte Webanwendungen eingesetzt, um bestimmte Funktionen auf mobilen Engeräten zur Verfügung zu stellen.

Eine Webanwendung ist generell mit einem Computerprogramm vergleichbar, das über einen Webbrowser wie Windows Internet Explorer, Mozilla Firefox usw. bedient wird. Die eigentliche „Intelligenz“ sowie die zugehörigen Daten befinden sich auf einem speziellen Webserver. Anders als bei herkömmlichen Webseiten werden die einzelnen Seiten für jeden einzelnen Nutzer und Arbeitsschritt zur Laufzeit erzeugt. Im „normalen“ (drahtgebundenen) Internet erfreuen sich solche Anwendungen großer Beliebtheit, wie die Erfolge der Webmail- oder Online-Banking-Dienste bis hin zu ganzen Online-Office-Paketen eindrucksvoll belegen.

Allerdings muss beachtet werden, dass die Webseiten speziell auf mobile Endgeräte zugeschnitten sein müssen (siehe [Bieh]). Mobile Endgeräte unterscheiden sich sehr stark voneinander. Darüber hinaus existiert eine Vielzahl unterschiedlicher Endgeräte, sodass gegebenenfalls mehrere hundert (!) Varianten eines Computerprogramms, das direkt auf ein Endgerät installiert werden kann, erstellt werden müssten. Dieser Aufwand wäre für KMU natürlich nicht tragbar. Der große Vorteil, aufgrund dessen auch in den genannten Projekten auf Webanwendungen zurückgegriffen wurde, ist, dass Webanwendungen im Prinzip auf jedem modernen Endgerät lauffähig sind.

4.3.1 ModiFrame, M3V und MAREMBA – Die Herausforderungen

4.3.1.1 ModiFrame

Gegenstand des Projekts **ModiFrame** ist die Entwicklung eines Frameworks für mobile Dienste, das kleinen und mittleren Unternehmen den Betrieb eigener mobiler Dienste ermöglicht, ohne selbst die notwendige Infrastruktur hierfür bereitzustellen.

Ein wesentliches Ergebnis dieses Projekts ist die Erkenntnis, dass die große Vielzahl verschiedener mobiler Endgeräte und deren technische Unzulänglichkeiten das gravierendste Problemfeld für KMU darstellen – wenn es um die Realisierung mobiler Anwendungen geht. Im **ModiFrame**-Projekt wurde aus diesem Grund der Ansatz verfolgt, mobile Anwendungen in Form von Webanwendungen zu entwickeln.

Der Einsatz von Webanwendungen bietet mehrere Vorteile: Eine Anwendung muss lediglich auf einem Server installiert werden, nicht auf allen Endgeräten. Weiterhin werden alle umfangreichen Berechnungen auf dem Server ausgeführt und nicht auf dem Endgerät, das meist nur einen langsamen Prozessor besitzt. Ebenfalls müssen keine großen Datenmengen (beispielsweise eine Datenbank mit sämtlichen Kundendaten) auf dem Endgerät gespeichert werden – was unter Umständen gar nicht möglich wäre, da mobile Geräte oftmals nur einen relativ kleinen Speicher haben. Geht ein Gerät verloren (etwa durch Diebstahl), ist damit kein unwiederbringlicher Verlust sensibler Daten verbunden. Darüber hinaus ist die Schwierigkeit größer, „Raubkopien“ von einer Webanwendung zu erstellen, als von einem normalen Computerprogramm, das direkt auf einem Gerät installiert ist und auf das somit leichter zugegriffen werden kann.

4.3.2 M3V

Gegenstand des Projekts **M3V** (Mobile Multimediale Multilieferanten-Vertriebsinformationssysteme) ist, ein mobiles Vertriebssystem für Handelsvertreter mit Lieferantenanbindung sowie sicherer Informationssystematik zu schaffen – und dadurch kleinen

und mittleren Unternehmen die Möglichkeit zu bieten, internationale sowie nationale Märkte zu erschließen.

Im Speziellen nutzen **M3V**-Handelsvertreter zu Beratungs- und Verkaufsabwicklungszwecken entweder ein mobiles, multimediafähiges Endgerät mit einem Webbrowser oder eine separat installierte Anwendung auf dem mobilen Gerät. Dabei kommunizieren unterschiedliche Dienste wie PIM (*Product Information Management*), CRM (*Customer Relationship Management*) oder ERP (*Enterprise Resource Planning*) über diverse Webanwendungen miteinander. Diese Dienste befinden sich innerhalb des **M3V**-Backend-Systems oder sind extern über das Internet angebunden. Teilweise besitzen die verschiedenen Dienste eine eigene Benutzerverwaltung mit eigener Benutzeridentität.

Um den Komfort für die **M3V**-Handelsvertreter zu erhöhen, werden mehrere unterschiedliche Verfahren zum Identitätsnachweis eines Benutzers parallel eingesetzt, wie

- die Benutzername/Passwort-Methode, wobei sich ein Anwender durch Benutzername und zugehöriges Kennwort legitimiert,
- die CardSpace-Technologie, die einem Anwender oder Mitarbeiter eines Unternehmens ermöglicht, die eigene Identität gegenüber Dritten mittels unterschiedlicher, virtueller Karten (analog zu EC- oder Mitgliederkarten) zu versichern,
- dem OpenID-System, das einem Anwender die Möglichkeit bietet, sich – nach einer einmaligen Identifizierung mit Benutzername und Passwort bei einer autorisierten Stelle – mit einer OpenID, d. h. einer speziellen URL ohne Benutzername und Kennwort bei allen Webseiten anzumelden, die dieses System unterstützen.

4.3.3 MAREMBA

Ziel des Projekts **MAREMBA** (Mobile Assistenz für das Ressourcenmanagement in der Bau-Auftragsabwicklung) ist, kleinen und mittleren Handwerksunternehmen eine Beteiligung an Ausschreibungen und eine kooperative Abwicklung von Großbauprojekten zu ermöglichen.

Handwerksbetrieben fehlen oft die für das mobile Baustellen- und Wartungsmanagement erforderlichen technischen Ressourcen, wie Kräne und Hebebühnen sowie Erfahrungen mit Großbaustellen. Das Projekt **MAREMBA** bietet für Handwerksbetriebe ein ganzheitliches, prozessübergreifendes Ressourcenmanagementsystem, um den Prozess der Leistungserbringung in der Baubranche zu optimieren.

MAREMBA besteht aus einer webbasierten Kollaborationsplattform, die Daten eines zugrunde liegenden ERP-Systems integriert sowie einem mobilen, personalisierten

Ressourcenmanagementdienst. Die Komponenten von **MAREMBA** bilden damit gesamthaft den kompletten Bauprozessablauf von der Ausschreibung bis hin zur Wartung der zu erbringenden Bauleistungen ab.

Mit dem **MAREMBA**-Projekt wird die Integration von Handwerksbetrieben in mobile Projekte auf Großbaustellen erleichtert und eine verbesserte Störungsbeseitigung ermöglicht.

4.3.4 Identifizierte Bedrohungen

4.3.4.1 ModiFrame

Der von **ModiFrame** verfolgte Ansatz, auf Webanwendungen zu setzen, bringt jedoch ein Sicherheitsproblem mit sich: Bei Webanwendungen müssen häufig Daten über eine Funkverbindung übertragen werden. In Deutschland sind an fast allen Orten entsprechende Funknetze verfügbar (z. B. GPRS, EDGE, UMTS oder WLAN). Allerdings liegt es in der Natur einer drahtlosen Datenübertragung, dass diese Kommunikation abgehört werden kann („passiver Angriff“), da das verwendete Medium „Luft“ frei zugänglich ist – und nicht wie Kabel mit Mauern und Türen geschützt werden kann.

Denkbar sind ebenfalls Anwendungsfälle, bei denen der Anreiz für einen potenziellen Angreifer nicht nur im Abhören der Daten besteht, sondern auch in deren Manipulation („aktiver Angriff“) – z. B. dann, wenn mit einem PDA erfasste Bestellungen übertragen werden.

4.3.4.2 M3V

Die Aufgabe des mobilen Endgeräts besteht darin, Daten sicher von und zum **M3V**-Backend-System zu transportieren. Speichert darüber hinaus eine installierte Anwendung Daten, muss zusätzlich eine sichere Datenbewahrung bei defekten oder gestohlenen Endgeräten gewährleistet sein.

Weiterhin sollen die Dienste der Webservices vor unberechtigtem Zugriff geschützt sein. Ebenso müssen Vertraulichkeit und Integrität garantiert werden.

Eine weitere Herausforderung liegt in der notwendigen Protokollierungsmöglichkeit („Audit-Fähigkeit“) eines aufgerufenen Diensts, da die Dienste generell von unterschiedlichen Herstellern zur Verfügung gestellt werden und im Konfliktfall eine nicht abstreitbare Dokumentation über deren Verwendung vorliegen muss.

4.3.4.3 MAREMBA

Spezifische Bedrohungen im Bereich baubezogener Prozesse bestehen in der Änderung von Aufträgen und Maßangaben sowie in der Durchführung von Abnahmen und Behinderungsanzeigen durch nicht autorisierte Personen („Impersonation“). Die Übermittlung falscher Maßangaben in der Bauauftragsabwicklung beispielsweise führt zur falschen Umsetzung von Bauaufträgen.

4.3.5 Bewertung der Bedrohungen

4.3.5.1 ModiFrame

Der durch einen passiven Angriff, d. h. durch das Abhören einer drahtlosen Datenverbindung möglicherweise entstehende Schaden, hängt von der Art der mit **ModiFrame** entwickelten Geschäftsanwendung ab.

Werden etwa größere Mengen personenbezogener Daten abgehört und die Öffentlichkeit davon in Kenntnis gesetzt, kann dies einen hohen Ansehensverlust der betreffenden Firma bedeuten. Wenn Geschäftsdaten wie Preiskalkulationen abgehört werden und an Mitbewerber gelangen, kann dies zum Verlust von Aufträgen und im schlimmsten Fall zum Konkurs des Unternehmens, das den mobilen Dienst nutzt, führen.

Auch bei aktiven Angriffen, d. h. im Fall von Datenmanipulationen, ist der Schaden abhängig von der jeweiligen Geschäftsanwendung. Auftragsverluste sind denkbar, wenn ein über drahtlose Kommunikation übertragener Auftrag „gelöscht“ wird. Wird der Auftrag nur verändert, erhält der Kunde eine von seinen tatsächlichen Wünschen abweichende Lieferung – ein Umstand, der ebenfalls einen finanziellen Schaden und Vertrauensverlust verursacht.

4.3.5.2 M3V

Da in vertrieblichen Projekten sensible Geschäftsdaten wie Preise oder Kundendaten existieren, ist naturgemäß das Interesse der Konkurrenz sehr groß, diese Daten in Erfahrung zu bringen oder diese zu manipulieren. Ein bewusst herbeigeführter oder technisch bedingter Ausfall des **M3V**-Backend-Systems bedeutet für den jeweiligen Systembenutzer eine erhebliche Einschränkung seiner Arbeit – im schlimmsten Fall sogar Umsatzeinbußen. Ein Datenverlust ist für den Benutzer des **M3V**-Systems existenzgefährdend.

Die unterschiedlichen Dienste sind selbst für ihre eigene Sicherheit verantwortlich; das **M3V**-System kann ausschließlich die Kommunikation der Dienste untereinander und

zum Endgerät schützen. Darüber hinaus muss die Kommunikation nachträglich sicher nachvollziehbar sein, weswegen eine digitale Signatur der Kommunikationsdaten erforderlich ist.

4.3.5.3 MAREMBA

Eine Abänderung der Daten beim Aufmaß führt zu falschen Abrechnungen. Im schlimmsten Fall werden falsche Maß- und Mengenangaben nicht erkannt und es entsteht ein unmittelbarer finanzieller Schaden für das betroffene Unternehmen.

Auch im Fall einer Manipulationserkennung ist eine Schädigung vorhanden, da Abrechnungen storniert und neu erstellt werden müssen – eine Doppelarbeit, die indirekt zu finanziellen Verlusten führt.

Das Ausmaß einer Bedrohung, ausgelöst durch nicht autorisierte Personen, die die Anwendung nutzen, entspricht etwa dem Ausmaß einer erfolgten Datenmanipulation. Berücksichtigt werden müssen bei einer zu Unrecht erfolgten Abnahme zudem die rechtlichen Folgen hinsichtlich Leistungsansprüchen. Mögliche finanzielle Schäden sind somit deutlich höher zu bewerten.

Die Eintrittswahrscheinlichkeit der Bedrohungen durch Manipulation oder Impersonation samt zugehöriger Schadensfälle ist in der mobilen Bauauftragsabwicklung eher gering bis mäßig kritisch zu bewerten.

4.3.6 Identifizierte Gegenmaßnahmen

4.3.6.1 ModiFrame

Da drahtlose Datenübertragungen abgehört oder gar manipuliert werden können, sind einige Standards für eine Datenübertragung mit Verschlüsselungsverfahren ausgerüstet (z. B. Kasumi-Verfahren für UMTS). Ältere Datenübertragungstechniken jedoch verfügen über keine nach heutigem Kenntnisstand ausreichenden Sicherungsmechanismen, z. B. auch nicht das A5/1-Verschlüsselungsverfahren für GSM. Für WLAN existieren mittlerweile entsprechende Verschlüsselungsverfahren (WPA); diese sind allerdings oft durch die Nutzer deaktiviert.

Besteht der Grund zur Befürchtung, dass eine Internetanbindung abgehört oder manipuliert werden könnte, bieten Browser mit der SSL (*Secure Socket Layer*)-Technologie die Möglichkeit, selbst die Datenkommunikation zwischen Browser und Server zu verschlüsseln. Ist auf der Netzwerkschicht keine oder keine ausreichende Sicherung vorhanden, wird auf Anwendungsebene verschlüsselt.

Weiterhin wäre denkbar, auf die Übertragung von als sensibel eingestuften Daten ganz zu verzichten, sofern die aktuelle drahtlose Kommunikation nicht hinreichend gesichert ist.

4.3.6.2 M3V

Werden mobile Webbrowser für die Verbindung zum **M3V**-System eingesetzt, ist die Verwendung einer reinen transportorientierten Verschlüsselung mit SSL möglich. Sämtliche anderen Kommunikationen benötigen eine sichere End-to-End-Verschlüsselung (die Ver- und Entschlüsselung erfolgt in den jeweiligen Endgeräten) und eine Signatur, die letztendlich auf Zertifikaten basieren.

Innerhalb des Kommunikationsprozesses erfolgt eine Trennung zwischen Authentifizierung („Wer bin ich?“) und einer nachfolgenden Autorisierung („Was darf ich?“). Diese Trennung wird durch zwei unterschiedliche STS (*Secure Token Services*), d. h. zwei speziellen Instanzen innerhalb des Authentifizierungssystems, realisiert.

Eine digitale Signatur bei der Kommunikation zwischen den beteiligten Diensten bestätigt auch im Nachhinein die Kommunikationsdaten.

Das **M3V**-System muss hoch ausfallsicher ausgelegt und eine funktionierende Datensicherung muss vorhanden sein.

4.3.6.3 MAREMBA

Neben einer notwendigen transportorientierten Verschlüsselung erfordert vor allem die Tatsache, dass nicht autorisierte Personen die Anwendung nutzen könnten, den Einsatz von Signaturen, die eine eindeutige Identitätszuordnung erlauben.

Grundsätzlich bestehen mehrere technische Realisierungsmöglichkeiten, um eine eindeutige Identitätszuordnung im Rahmen der Bauauftragsabwicklung zu garantieren. Die Bandbreite reicht vom Einsatz einer einfachen über die fortgeschrittene bis hin zur qualifizierten Signatur.

Für formfreie Vereinbarungen ist die Verwendung einer einfachen oder fortgeschrittenen elektronischen Signatur hinreichend und kann zwischen den Vertragspartnern vereinbart werden.

Während an eine einfache elektronische Signatur keine besonderen Anforderungen gestellt werden, muss bei der fortgeschrittenen Signatur dem Ersteller der Signatur ein Signaturschlüssel zur Verfügung stehen, der unter seiner alleinigen Kontrolle steht.

Die qualifizierte Signatur besitzt zusätzlich die Merkmale, dass sie ausschließlich auf einem besonderen Medium (z. B. einer Karte) gespeichert und angewendet werden darf und die Übereinstimmung durch eine anerkannte Stelle geprüft und bestätigt werden muss. Die qualifizierte Signatur kann daher auch in Anwendungsbereichen verwendet werden, in denen per Gesetz die Schriftform vorgeschrieben ist. Eine qualifizierte Signatur kann nur bei besonders autorisierten Stellen beantragt werden.

Hinsichtlich der Rechtssicherheit sind bestimmte Anforderungen an Signaturen beachtenswert:

- Der Unterzeichner muss identifizierbar sein.
- Der Inhalt des Dokuments und das Identifizierungsmerkmal des Unterzeichners gehören zusammen.
- Nachträgliche Veränderungen am Dokument müssen erkennbar sein.
- Der Unterzeichner muss den Signaturprozess kontrollieren können.

4.3.7 Ausgewählte Gegenmaßnahmen

Die **SimoBIT**-Projekte ModiFrame, M3V und MAREMBA verwenden die SSL-Technologie. Dabei handelt es sich um ein Verfahren zur Absicherung der Datenkommunikation zwischen zwei Computern im Internet.

Die Abkürzung SSL steht für *Secure Socket Layer* und wurde ursprünglich von der Browserfirma Netscape entwickelt; inzwischen existiert mit TLS (*Transport Layer Security*) eine standardisierte Variante von SSL.

SSL und TLS sind einander derart ähnlich, dass beide Begriffe als Synonyme verwenden werden können und oft unter der Bezeichnung „SSL/TLS“ beschrieben werden. Es bestehen verschiedene Varianten von SSL, aus Sicherheitsgründen sollte heutzutage nur die aktuelle Version SSL3 eingesetzt werden.

Auch wenn es ursprünglich dafür entwickelt wurde, kann SSL nicht nur für die Absicherung von Webanwendungen verwendet werden, sondern beispielsweise auch für E-Mail- oder Dateiübertragungen. Der SSL-Einsatz bei Webverbindungen ist der bekannteste Anwendungsfall, weshalb dieser im anschließenden **ModiFrame**-Abschnitt ausführlicher beschrieben ist. Im **M3V**-Projekt wird SSL dazu verwendet, den Datenaustausch zwischen einem mobilen Endgerät und dem **M3V**-Backend-System abzusichern.

Die gebräuchlichen Browser für Desktop-Computer (Mozilla Firefox, MS Internet Explorer, Opera etc.) zeigen mit einem Schlüsselsymbol in der Statusleiste an, dass aktuell eine gesicherte SSL-Verbindung verwendet wird. Aber auch an der angezeigten Web-

adresse ist der Einsatz von SSL erkennbar: Wird SSL verwendet, beginnt diese mit „http**s**://“ statt mit „http://“.

Die Funktionsweise von SSL zur Sicherung einer Webanwendung geschieht wie folgt: Möchte ein Browser eine verschlüsselte Verbindung zu einem Server aufbauen, benötigt er das Zertifikat dieses Servers. Er fordert dies also beim Server an. Hat der Browser in der Vergangenheit bereits einmal eine verschlüsselte Verbindung zu diesem Server aufgebaut, ist das Zertifikat bereits im Browser selbst gespeichert.

Das Zertifikat enthält den offiziellen Schlüssel, den der Browser benötigt, um eine verschlüsselte Verbindung herzustellen. Der Browser überprüft zudem, ob das Zertifikat tatsächlich von dem Server (dem Unternehmen) stammt, das vorgegeben wird. Im Rahmen des **ModiFrame**-Projekts soll das Zertifikat also vom Betreiber der **ModiFrame**-Anwendung stammen, das bedeutet, von dem KMU selbst oder einer spezialisierten Betreiberfirma, dem so genannten „Hoster“.

Um das Serverzertifikat überprüfen zu können, wird immer das Zertifikat der CA benötigt, die das Serverzertifikat ausgestellt hat. Moderne Browser haben aus diesem Grund die Zertifikate der „bekanntesten“ CAs bereits integriert. Allerdings werden nicht alle Serverzertifikate von einer „bekannten“ CA ausgestellt, da diese Ausstellung gegebenenfalls mit hohen Kosten verbunden sein kann. Deshalb muss ein Browser unter Umständen das Zertifikat der ausstellenden CA nachladen. Dieses CA-Zertifikat wiederum muss auf seine Authentizität überprüft werden. Wurde dieses nachgeladene CA-Zertifikat ebenfalls von einer nicht im Browser integrierten CA ausgestellt, muss auch deren Zertifikat geladen werden. Auf diese Weise können ganze *Zertifikatsketten*, die bei dem Browser bekannten Zertifikaten beginnen und bei den eigentlichen Serverzertifikaten enden, entstehen.

4.3.7.1 ModiFrame

Die mit **ModiFrame** entwickelten mobilen Anwendungen sollen möglichst flexibel einsetzbar sein. Aus diesem Grund kann die eingesetzte Technik zur drahtlosen Datenkommunikation nicht in irgendeiner Form eingeschränkt werden (z. B. Beschränkung auf UMTS). Vielmehr ist sogar der Wechsel der Übertragungstechnologie, wie beispielsweise von WLAN auf UMTS während einer Sitzung denkbar, da der mobile Akteur unter Umständen das Firmengelände verlassen hat. Es ist also nicht möglich, sich darauf zu verlassen, dass die verwendeten drahtlosen Verfahren immer ein hinreichendes Sicherheitsniveau bieten.

Leider ist eine Webanwendung nicht in der Lage, herauszufinden, wie sicher die Internetverbindung ist, über die die Kommunikation zwischen Browser und Server abgewickelt wird. Hieran scheitert auch der Ansatz, bei unsicheren Verbindungen (z. B. ungesichertes WLAN oder GSM-Verbindung) auf die Übertragung als sensibel eingestufter Daten einfach zu verzichten. Weiterhin würde dieser Ansatz auch erfordern, alle Daten,

die potenziell von oder zu einem mobilen Endgerät übertragen werden, zu klassifizieren – ein sehr aufwändiges Vorhaben. Deshalb werden bei **ModiFrame** die Verbindungen zwischen Browser und Server mit SSL verschlüsselt; dies stellt die einzig sinnvolle Möglichkeit dar, wenn Webanwendungen eingesetzt werden.

Bei Desktop-Browsern können beliebige Zertifikate nachgeladen werden, sodass in der Regel keine Probleme mit unbekannten Zertifikaten auftreten. Bei Browsern auf mobilen Endgeräten ist dies jedoch nicht immer möglich, da insbesondere Browserprogramme auf einfachen Endgeräten das Nachladen von Zertifikaten nicht unterstützten.

Der Betreiber des **ModiFrame**-Dienstes ist in diesem Fall darauf angewiesen, das eigene Serverzertifikat von einer „bekannten“ CA ausstellen zu lassen. **ModiFrame** sieht darüber hinaus vor, den Betrieb des Dienstes zu übernehmen, sodass sich in diesem Fall der Dienstbetreiber nicht selbst um ein Zertifikat kümmern muss.

4.3.7.2 M3V

Alle Dienste im **M3V**-System kommunizieren über das XML-basierte Netzwerkprotokoll SOAP (*Simple Object Access Protocol*) und setzen die neusten Erweiterungen der WS*Technologien, einer Kombination verschiedener definierter Webservice-Standards ein.

Dabei ermöglicht WS-Security, ein Standard für Sicherheitsdaten, die Verschlüsselung und die Signierung sowie die Übertragung so genannter SAML (*Security Assertion Markup Language*)-Token. Diese Token werden von zwei unterschiedlichen STS ausgestellt, von denen ein Service für die Authentifizierung und ein anderer für die Autorisierung verantwortlich sind. Die Autorisierungs-STS (auch „Ressource-STS“) benötigt ein gültiges Token der Authentifizierungs-STS. Durch die Signierung ist eine Audit-Fähigkeit gegeben.

Eine eigene **M3V**-Zertifizierungsstelle gibt die Zertifikate aus, die für die Verschlüsselung und die Signatur benötigt werden. Für eine sichere SSL-Verbindung sind darüber hinaus ein Key- sowie ein Truststore notwendig. Jeder Dienst besitzt einen eigenen Keystore (der auch den privaten Schlüssel enthält) und einen Truststore (der ausschließlich Zertifikate beinhaltet), womit die Dienste voneinander abgegrenzt sind.

Für die Kommunikation mit den mobilen Endgeräten wird – wie bereits erwähnt – SSL eingesetzt.

4.3.7.3 MAREMBA

Da in handwerklichen Klein- und Kleinstunternehmen in der Regel nur geringe IT-Vorkenntnisse vorhanden sind, führte eine erste Evaluation zu dem Schluss, dass der

Einsatz einer qualifizierten Signatur im Bereich der Handwerksbetriebe aus organisatorischen Gründen ungeeignet erscheint. Die Beantragung und Installation einer qualifizierten Signatur stellt eine zu hohe Hürde für eine benutzergerechte, einfache Handhabung dar. Die Abgabe von Aufmaßen und Abnahmen erfolgt in **MAREMBA** aus diesem Grund mit einfacher elektronischer Signatur von Auftraggeber und Auftragnehmer. Unterschrieben wird via Touchscreen oder einem äquivalenten Ersatzgerät im Rahmen einer authentifizierten Sitzung des Aufmaßnehmers.

Die Signaturen werden über eindeutige Referenzen mit den abgegebenen Informationen (d. h. dem Protokoll der Positionsdaten sowie der erzeugten Datei mit den Maßangaben) verknüpft. Diese Informationen können anschließend nicht mehr geändert werden.

In technischer Hinsicht schließt der beschriebene Signaturprozess den Einsatz qualifizierter oder fortgeschrittener Signaturen nicht aus, sodass diese Signaturen grundsätzlich für die Abgabe von Aufmaßen oder die Abnahme von Bauleistungen verwenden werden können.

4.4 Digitale Zertifikate als Lösung für mobilspezifische Sicherheitsprobleme

Digitale Zertifikate stellen ein geeignetes Mittel dar, um verschiedene mobilspezifische Sicherheitsprobleme, auf die KMU bei der Realisierung von mobilen Anwendungen stoßen, erfolgreich zu lösen.

Ein Problem von Zertifikaten ist jedoch, dass die zugrunde liegende Technologie nicht einfach verständlich ist. Darüber hinaus kann die Ausstellung eines Zertifikats für ein Unternehmen mit hohen Kosten verbunden sein. Weiterhin muss bedacht werden, dass Zertifikate aus Sicherheitsgründen meist eine auf wenige Jahre beschränkte Laufzeit besitzen. Außerdem können verwirrende Fehlermeldungen auftreten, wenn eine Anwendung ein Zertifikat nicht verifizieren kann. All diese Probleme können aber dadurch beseitigt werden, dass die entsprechende Lösung von einem kompetenten Anbieter betrieben wird, so dass der Endnutzer sich um diese Details nicht zu kümmern braucht.

In den beschriebenen Anwendungsfällen liegen die Zertifikate als Dateien vor. Es gibt aber auch Bestrebungen, Zertifikate auf so genannten SmartCards zu speichern: Der neue elektronische Personalausweis, der in Deutschland im Jahr 2010 eingeführt wird, beinhaltet eine solche SmartCard, auf die optional ein Signatur-Zertifikat geladen werden kann. Hinter diesem Zertifikat steht eine Bundesbehörde, weshalb das Zertifikat als besonders vertrauenswürdig gilt. Da mittelfristig jeder Deutsche, der das 16. Lebensjahr vollendet hat, diesen Ausweis besitzen wird, ergeben sich hieraus interessante Möglichkeiten, mit vor allem auf den Endkundenmarkt abzielenden Anwendungen.

Checkliste Handwerk und KMU

Wichtige Hinweise für mobile IT-Sicherheit in Handwerk und KMU

Zertifikatsbasierte Systeme stellen insbesondere für Handwerk und KMU Technologien zur Verfügung, die mobile IT-Sicherheit für diese Unternehmen gewährleisten.

Mobile Webanwendungen bieten den Vorteil, dass sie mit verschiedenen Typen von mobilen Endgeräten verwendbar sind und keine große Datenmengen auf dem mobilen Client vorgehalten werden müssen.

Mehrere unterschiedliche Verfahren zum Identitätsnachweis erhöhen den Komfort für den Benutzer des mobilen Endgeräts.

Die SimoBIT-Projekte ModiFrame, M3V und MAREMBA verwenden die SSL-Technologie, um die drahtlose Datenkommunikation zwischen einem mobilen Endgerät und einem Server abzusichern.

Eine einfache elektronische Signatur von Auftraggeber und Auftragnehmer kann in vielen Anwendungen ausreichend sein. Es sollte daher im vorhinein geprüft werden, ob eine qualifizierte Signatur aus rechtlicher Sicht überhaupt erforderlich ist.

Literatur- und Linkverzeichnis

[BIEH] Bieh, Manuel: Mobiles Webdesign. Konzeption, Gestaltung, Entwicklung. Bonn: Galileo-Press, 2008.

[DECK] Decker, Michael et al.: The ModiFrame-Framework for Enabling Small and Medium-Sized Enterprises to Provide Mobile Services. In: Proceedings of the Conference on Wireless Applications and Computing (WAC07). Lissabon, 2007, Seite 131 ff.

[HOFM] Hofmann, Josephine et al.: Kollaborative Ressourcenmanagementplattform zur Steigerung der Wertschöpfung in Handwerksunternehmen. In Spath, Dieter; Hofmann, Josephine, Günther, Jochen (Hg): MAREMBA - Mobile Assistenz für das Ressourcenmanagement in der Bau-Auftragsabwicklung. Gestaltung mobiler Services im Handwerk. Stuttgart, 2010.

[SCHM] Schmeh, Klaus: Kryptografie. Verfahren, Protokolle, Vorgehensweisen. 3. Aufl. Heidelberg: dunkt-Verlag, 2007.

[SING] Singh, Simon: Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internets. München & Wien: Hanser-Verlag, 2000.

[OSSL] OpenSSL Software Foundation: *The OpenSSL Project*. URL: http://www.openssl.org/ . Stand: 23.11.2009.

Ansprechpartner:

Michael Decker (für ModiFrame)
Institut AIFB, Karlsruher Institut für Technologie (KIT)
Universität Karlsruhe
76128 Karlsruhe

Tel.: 0721 608-7467
E-Mail: decker@aifb.uni-karlsruhe.de
www.aifb.uni-karlsruhe.de

Jochen Günther (für MAREMBA)
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
70569 Stuttgart

Tel.: 0711 970-2262
E-Mail: Jochen.Guenther@iao.fraunhofer.de
http://www.iao.fraunhofer.de

Ralf Kunoth (für M3V)
fun communications GmbH
76135 Karlsruhe

Tel.: 0721 96448-0
E-Mail: ralf.kunoth@fun.de
www.fun.de

5 Mobile IT-Sicherheit im Maschinenbau: Vorgehensweise zur strukturierten Reduzierung von Bedrohungen

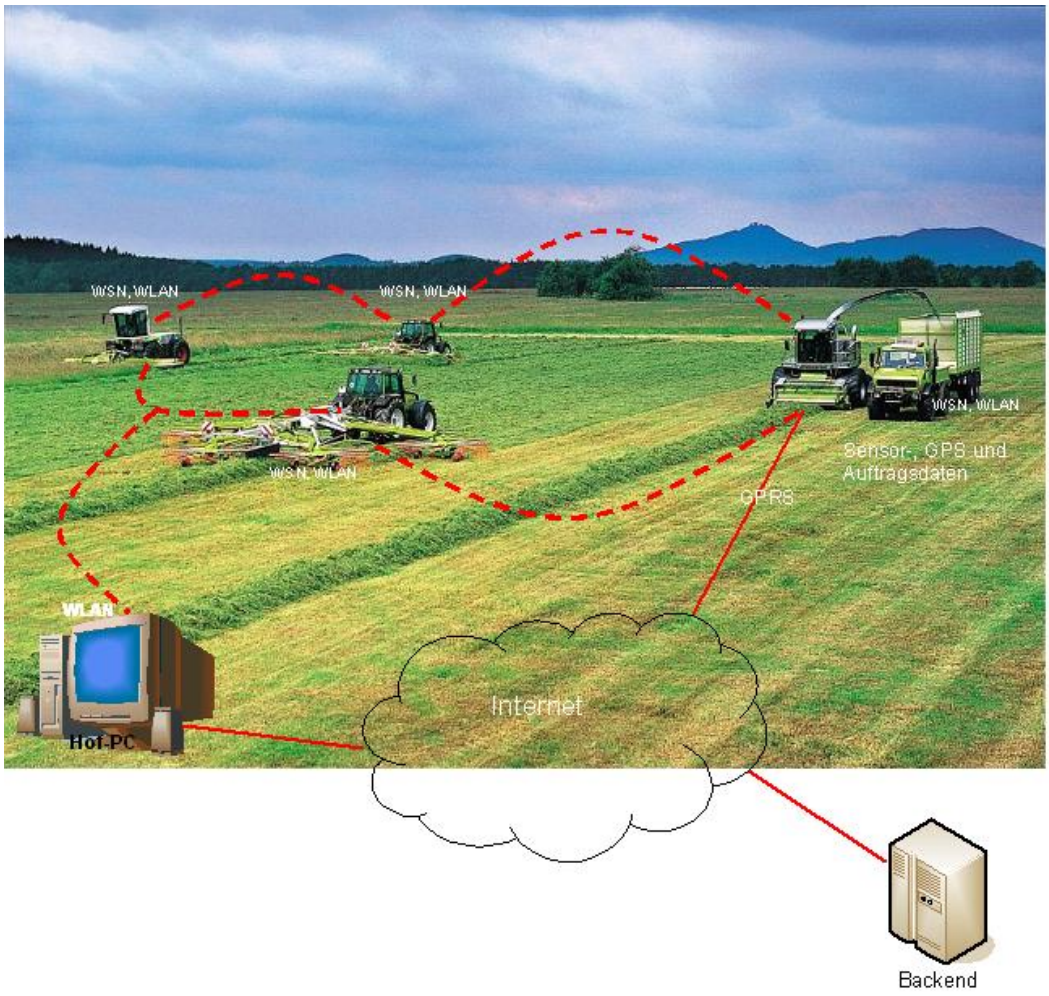
5.1 Integration des Managements mobiler Maschinen in Geschäftsprozesse

Die (teil-) automatisierte Ablauffähigkeit von Geschäftsprozessen (**R2B** – Robot to Business) sowie die zeit- und ortsunabhängige Verfügbarkeit von Informationen, ohne dass die primäre Aufmerksamkeit der Benutzer dem Computersystem gilt (**SiWear** – Sichere Wearable Systeme), sind zentrale Ziele der Forschungsprojekte im Cluster Maschinenbau. Über den Einsatz von Backend-Systemen hinaus, ist die Integration mobiler Einheiten hierbei von zentraler Bedeutung. So kommunizieren beispielsweise Maschinenmanagement-Prozesse (**R2B** Grünfutterernte-Szenario) oder Servicetechniker (**R2B** IT-Service und Wartungs-Szenario) untereinander bzw. mit dem Backend. Entwicklung und Entwurf solcher Systeme erfordern daher eine umfassende Betrachtung von der obersten Ebene der konfigurierbaren Leistung über die Ebene der ablauffähigen Prozesse bis zu der Ebene der „unteren“ embedded Geräte.

Mit zunehmender Berücksichtigung der IT-Sicherheit im Rahmen von Managementanforderungen, wächst die Forderung nach IT-Produkten, deren Funktionen einen sicheren Einsatz ermöglichen oder zumindest unterstützen. Je früher Sicherheitsanforderungen identifiziert werden können, desto geringer ist das Risiko für Verzögerungen im Entwicklungsprozess und desto höher ist die Förderung sicherheitsrelevanter Produktmerkmale. Ausgehend vom Projekt **SiWear** werden zwei Vorgehensweisen vorgestellt, die eine frühzeitige Berücksichtigung von Sicherheitsanforderungen ermöglichen. Im Projekt **R2B** wird das in der Einleitung beschriebene „strukturierte Vorgehen zur Reduzierung von Bedrohungen“ zur Analyse der Bedrohungen angewandt.

Der bisher entstandene Demonstrator des Projektes **R2B** illustriert das Szenario der „Automatischen Buchung der Arbeitserledigung“ in der Domäne der Grünfutterernte. Die aktuelle GPS-Position wird einem Polygon im Feld (Schlag) zugeordnet. Sollte die lokale Datenhaltung nicht über die nötigen Informationen verfügen, werden diese über ein Backend-System ermittelt (GPRS-Kommunikation). Während des Erntevorganges protokollieren die Maschinen verschiedene Zustände von Sensoren und Aktoren. Entsprechend vorgegebener Regeln werden diese Daten an das Backend geschickt, dort aggregiert, und die Buchung abschließend automatisiert erstellt.

Abbildung 5-1: Kommunikationsszenario zwischen mobilen Einheiten und Backend im Projekt R2B

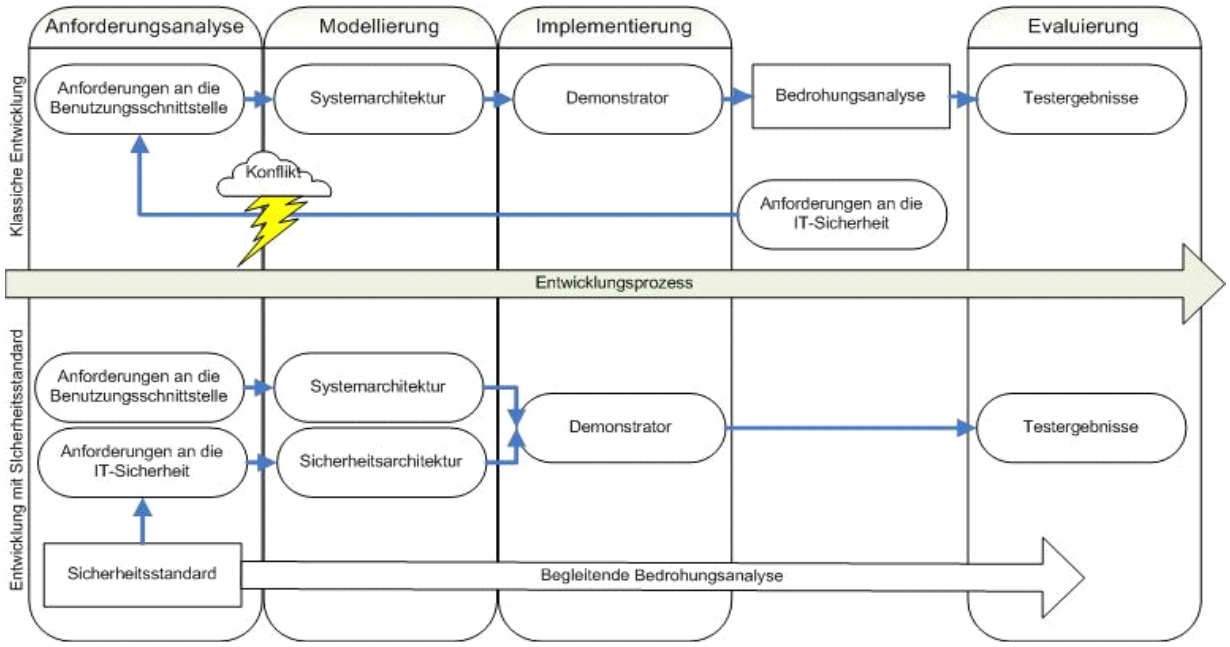


Quelle: CLAAS KGaA

5.2 Berücksichtigung von IT-Sicherheit bereits in der Entwicklungsphase

Vorschriften und Gesetze zum Risikomanagement und zur Datenverarbeitung in Unternehmen, z. B. KonTraG, Basel II, SOX, umfassen vermehrt Anforderungen an die IT-Sicherheit im Unternehmen. Um die Risiken, die mit dem Einsatz von IT-Systemen verbunden sind, zu minimieren, können Sicherheitsstandards als Basis für ein IT-Sicherheitsmanagement oder zur Prüfung und Bewertung von IT-Produkten herangezogen werden. Produktorientierte Sicherheitsstandards wie z. B. Common Criteria (CC) oder ISO/IEC 19790 (FIPS 140-2) können zur sicherheitsorientierten Weiterentwicklung von Prototypen zu Produkten herangezogen werden. Die Entwicklung von Demonstratoren und Prototypen ist mit Veränderungen an Einsatzumgebungen und Geschäftsprozessen verbunden, die von der neuen Technologie unterstützt werden. Prozessorientierte Sicherheitsstandards, die über einen Demonstrator hinaus auch Abläufe berücksichtigen, sind in solchen Projekten dementsprechend besser geeignet (z. B. ISO 27001 auf der Basis von IT-Grundschutz). Unabhängig von der Entwicklungsphase kann eine frühzeitige Berücksichtigung von Sicherheitsanforderungen helfen, zusätzliche Entwicklungszyklen zu vermeiden .

Abbildung 5-2: Klassische Entwicklung im Vergleich zur Entwicklung mit IT-Sicherheitsstandard



Quelle: G. Diederich, in: G. Diederich, R. Sethmann, S. Schäfer and Z. Ghrairi (2008)

Das SimoBIT-Projekt **SiWear** zielt auf einen Durchbruch für den Einsatz der mobilen „wearable“ IuK-Technologien in produzierenden Unternehmen und im nachgelagerten After-Sales Bereich. Der Entwicklungsgegenstand unterliegt somit fortwährenden Veränderungen in der verwendeten Technologie, den unterstützen Abläufen und der zugehörigen Einsatzumgebung. In **SiWear** werden daher unter Verwendung von ISO 27001 auf der Basis von IT-Grundschutz, allgemeine Anforderungen an den sicheren Betrieb von IT-Systemen in der designierten Einsatzumgebung des zu entwickelnden Systems ermittelt. Zusätzlich zu den Ergebnissen der Anforderungsanalyse sind hierdurch frühzeitig Anforderungen zur IT-Sicherheit verfügbar und können bereits vom ersten Entwurf an in allen folgenden Entwurfszyklen berücksichtigt werden. Mit den IT-Grundschutzkatalogen für Standardtechnologien und Abläufe stehen technische und organisatorische Vorgaben zur Verfügung, die direkt in die Entwicklung einfließen können. Im Projekt **SiWear** wurden Entscheidungen zur technologischen Infrastruktur mittels einer Modellierung nach IT-Grundschutz begleitet, so dass entwicklungsbegleitend Anforderungen für ein grundlegendes Sicherheitsniveau ermittelt werden und für die Entwicklung berücksichtigt werden konnten.

So beispielsweise im Kommissionierungs-Szenario des Projektes **SiWear**, in dem der Einsatz eines WLAN eine mögliche Verbindung der Wearable-Computer untereinander sowie des Wearable-Systems mit der IT-Infrastruktur der Einsatzumgebung darstellt. Durch Verwendung des Bausteins „B 4.6 WLAN“ des IT-Grundschutz [Bs07] können typische Gefährdungen der IT-Sicherheit beim Einsatz von WLAN an der Funkschnittstelle des Wearable-Systems bereits begleitend zu dieser Entwurfsüberlegung betrachtet werden. Gefährdungen durch höhere Gewalt (z. B. Ausfall durch Blitzeinschlag) werden hierbei ebenso berücksichtigt, wie organisatorische Mängel (z. B. fehlende Kontrolle), menschliche Fehlhandlungen (z. B. Fehlkonfiguration), technisches Versagen (z. B. unzuverlässige WLAN-Sicherheitsmechanismen) oder vorsätzliche Handlungen (z. B. Diebstahl).

Entwicklungsbedingte Änderungen an der IT-Infrastruktur, z. B. im Bereich der Server-Systeme, konnten zeitnah durch eine Anpassung der Modellierung bzgl. ihrer Auswirkungen auf die IT-Sicherheit nachvollzogen und abgeschätzt werden. Über die Möglichkeit zur Modellierung von Standardsystemen bieten die IT-Grundschutzkataloge einen Ausgangspunkt zur Bewertung neuer Technologien. So bieten Bausteine zu mobilen Systemen, z. B. die Bausteine „B 3.203 Laptop“ oder „B 3.404 Mobiltelefon“ [Bs07], klar definierte Gefährdungen als Ausgangspunkt für die weitere Untersuchung typischer Gefährdungen für Wearable-Systeme.

Mit der gleichen Zielsetzung wurde im Projekt **R2B** die in der Einleitung vorgestellte Methode zur strukturierten IT-Sicherheitsanalyse erfolgreich eingesetzt. Sie wird nachfolgend ergänzend zur Verwendung von ISO 27001 auf der Basis von IT-Grundschutz am Beispiel des Projektes **R2B** vorgestellt.

5.3 SimoBIT-Projekt R2B: Anwendungsfälle und deren Anforderungen

Im SimoBIT-Projekt **R2B** werden insgesamt zwei Szenarien betrachtet: „Grünfutterernte“ und „IT-Wartung und Service“. Da es hier um das Cluster Maschinenbau geht, wird für den Bereich „IT-Wartung und Service“ an dieser Stelle keine ausführliche Analyse der Bedrohungen erstellt. Einige Aspekte wie Authentifizierung oder die Absicherung der drahtlosen Kommunikation zwischen mobiler Einheit und Backend gelten allerdings für beide Szenarien.

5.3.1 Anwendungsfall Grünfutterernte

Ziel des Szenarios

In der Grobfutterernte geht es um das Einbringen des (Grob-/Grün-) Futters mit maximaler Qualität und Quantität. Dazu muss der optimale Zeitpunkt (maximales Qualität/Masse Verhältnis) abgepasst werden und das Erntegut (Gras/Mais) in einem auf die Tiere abgestimmten Zustand (durchschnittliche Partikellänge, angequetschte Körner etc.) aufbereitet werden. Damit das eingeholte Erntegut bis zur Verfütterung haltbar bleibt, wird es (in diesem ausgewählten Beispielszenario bei diesem Anwendungsfall) in Fahrsilos gelagert.

Prozessablauf heute

Grasernte

Das Erntegut wächst auf dem Feld und wird mechanisch abgeschnitten. Anschließend wird es aufbereitet. Im Fall von Gras geht es bei der Aufbereitung um die Erhöhung der Trockenmasse, also dem Entziehen von Wasser durch Abtrocknen (Verdunstung durch Sonne und Wind auf dem Feld) und entsprechend geeignete Maßnahmen, die diesen Vorgang unterstützen. Dazu zählt das Aufbereiten (Knicken der Halme), das breitflächige Ablegen wie auch das Wenden. Letztendlich wird das Gras in Schwaden (Haufen-Reihen) abgelegt, damit es im nachfolgenden Bearbeitungsschritt aufgenommen werden kann. Die vorletzte Etappe der Grasernte ist schließlich das Häckseln (Kurzschneiden) des abgemähten und getrockneten Grases mit dem darauffolgenden Abtransport zur Lagerstätte (Silo). Die Grasschwaden werden von einem Selbstfahrenden Feldhäcksler (SFH) aufgenommen und kleingeschnitten. Der SFH fördert das Gras auf einen nebenher fahrenden Anhänger zum Abtransport. Auf dem Silo wird das Gras in 20 bis 30 cm dicken Schichten abgeladen und verteilt, sofern die Transportfahrzeuge über keine Verteileinrichtung verfügen, und anschließend wird es mit schweren Schleppern und Walzen verdichtet, um die Luft heraus zu pressen und so die Silage haltbar zu bekommen. Finaler Schritt ist hierbei das Abdecken des gesamten Silos mit Planen, um eine Sauerstoffzufuhr zu unterbinden und das Futter wetterfest lagern zu können.

Silomaisernte

Die Silomaisernte läuft ähnlich ab. Der Silomais wird nach dem Schnitt vom SFH gehäckselt, mit der Variante, dass nun noch die Maiskörner durch einen sog. Cracker aufgebrochen werden. Der so aufbereitete Mais wird nun ebenfalls auf Anhänger überladen und zum Fahrsilo transportiert, dort abgeladen und verteilt, sofern die Transportfahrzeuge über keine Verteileinrichtung verfügen. Anschließend wird wiederum mit schweren Schleppern und Walzen verdichtet, um die Luft heraus zu pressen und so die Silage haltbar zu bekommen. Danach wird der Haufen abgedeckt.

Allgemeine Informationen

In den Gras- und Maissilos läuft nun die natürliche Milchsäuregärung ab, welche die Silage haltbar macht. Die Schnittlänge bei Gras und Mais sollte sich an der Tierphysiologie orientieren, allerdings hat die Häcksellänge einen entscheidenden Einfluss auf die Verdichtbarkeit der Fasern/Fragmente im Silo. Zudem ist die Kapazität an Walz- und Verteilmaschinen und deren Gewicht (besser: deren Radaufstandsbelastung) ausschlaggebend für die gesamte Ernteleistung der Häckselkette. Damit die Bergung des Erntegutes reibungslos ablaufen kann, ist eine gründliche Vorplanung der einzelnen Arbeitsschritte mit den jeweils benötigten (geschätzten) Ressourcen unter Berücksichtigung der Abreife und der Wetterprognose wichtig. Interessant ist dabei das so genannte Erntezeitfenster. Damit ist die Zeitspanne vom frühest möglichen bis zum (prognostizierten) spätesten Erntezeitpunkt und die erwartete Anzahl der Grasschnitte bzw. die angebaute Maissorte gemeint. Wer für den konkreten Einsatz letztendlich die Ressourcen zu Verfügung stellt, der Landwirt selber oder ein Lohnunternehmer oder Maschinenring, ist weniger entscheidend. Um eine hinreichend gute Qualität der Silage zu erhalten, sollte die so genannte Häckselkette, also der SFH mit den Transportfahrzeugen und den Walzfahrzeugen auf dem Fahrsilo harmonieren. Ausschlaggebend ist die Walzleistung auf dem Silo, um die Verdichtungsleistung entsprechend an den Trockenmassegehalt anzupassen. Entsprechend dieser „Verdichtungsleistung“ braucht man die dazu gehörige „Häckslerleistung“. Die Transportkapazität richtet sich nach der Häckslerleistung und der Feld – Silo Entfernung. Dabei spielen die Faktoren Anzahl der Transportfahrzeuge, Kapazität (Kubikmeter/Tonnen) und die erzielbare Höchstgeschwindigkeit eine Rolle.

Neben der Disposition und Logistik der Maschinen und Verbrauchsstoffe gibt es noch die Buchung und die Rechnungserstellung als Management – bzw. unterstützende Prozesse. Neben mündlichen Aufträgen (face to face, per Betriebsfunk oder Telefon kommuniziert) gibt es heute die Varianten, Arbeitsaufträge in ein Softwaresystem aufzunehmen und in gedruckter Form den Fahrern mitzugeben, oder vorgeplante Aufträge der Auftragsverwaltung der Maschinenbordrechner per Wechselmedium mitzuteilen. In umgekehrter Richtung findet das Verbuchen der erledigten Leistungen statt. Je nach Software sind die Möglichkeiten der Datenverarbeitung sehr unterschiedlich: Von der Schlagkartei-Verwaltung über die Mitarbeiterlohnkartei bis zur Maschinen(-auslastungs-)analyse reicht das heute angebotene Spektrum der Farm-Management Software (FMS).

5.3.2 Anwendungsfall IT-Wartung und Service

Ziel des Szenarios

Im Anwendungsszenario IT-Wartung und Service werden am Beispiel der CADsys GmbH typische Geschäftsfälle eines IT-Dienstleisters abgebildet. Dabei sind mehrere kundenspezifisch auftretende Fälle des Outsourcing von Dienstleistungen zu berücksichtigen: Wartung und Installation von Software-Systemen, Komplettwartung von Soft- und Hardware an Arbeitsstationen, Wartung der gesamten IT-Infrastruktur des Kunden (z. B. Serverlandschaft, Netzkomponenten, Datenbanksysteme usw.). Bei diesen Dienstleistungen sind sowohl Arbeiten vor Ort als auch mögliche Fernwartungsanteile eingeschlossen. Als wichtige Randbedingung ist eine möglichst geringe Beeinträchtigung der Arbeitsfähigkeit der Systeme des Kunden zu realisieren.

Prozessablauf heute

Software-Wartung

IT-Systeme haben sich heute für die effiziente Gestaltung aller Geschäftsprozesse in Maschinenbauunternehmen allgemein durchgesetzt. Dies gilt in besonderer Weise für die Bereiche der Produktentwicklung, Fertigungsvorbereitung bis hin zur Fertigungssteuerung und –organisation. Die den Aufgaben angepassten hochspezialisierten Software-Systeme (CAD, CAM, PLM, ERP, CRM usw.) sind in unterschiedlichem Grad durch Daten- und Prozess-Schnittstellen integriert. Wartungsprozesse an den Softwaresystemen werden einerseits durch Freigabe neuer Releases oder durch Patches und andererseits durch gestiegene Leistungsanforderungen der Nutzer, die den Austausch von Hardware-Komponenten erfordern, initiiert. Für ein Update von CAD-Software werden vorbereitend die (im Regelfall gestiegenen) Anforderungen an Hardware und System-Software überprüft, die Wartungsarbeiten so geplant, dass die Beeinträchtigung der Systemverfügbarkeit beim Kunden minimiert wird, und alle Datensicherungen aktualisiert. Nach Durchführung des Updates einschließlich der Lizenzierung wird der Arbeitsplatz wieder funktionsfähig und in die Arbeitsumgebung des Kunden integriert übergeben. Ggf. kann davor die Migration aller Entwurfsdaten oder Bibliotheken auf die neue Version erforderlich sein.

Hardware-Wartung

Bei Hardware-Wartung sind die Erneuerung/Aufrüstung im Zuge der technischen Entwicklung, Havariefälle (Rechner-Ausfälle, Garantiefälle) und geplante Erneuerung von Komponenten auf Grund von überwachten Betriebsparametern zu unterscheiden. In der Regel bedingen Arbeiten an Hardware-Komponenten auch Neu- oder Nachinstallationen von Software (z. B. bei kurzfristigen Leihstellungen zur Überbrückung von Ausfallzeiten). In Abhängigkeit von der Fehlerdiagnose werden Wartungsarbeiten vor Ort (beim Kunden) oder Inhouse (beim Dienstleister) durchgeführt.

Allgemeine Informationen

Ausgehend von der Anfrage des Kunden oder externer Initiierung erfolgt die Konfiguration der Dienstleistung nach Leistungsarten, Spezifikation und Zusatzleistungen, der ein modellierter Geschäftsprozess in der IT-Umgebung des Dienstleisters entspricht. Nach der Disposition von Technikern, ggf. erforderlichen Fahrzeugen und Ausrüstungen startet ein zweiter Prozess auf dem Mobil-Gerät des zugeordneten Service-Technikers, der eng mit den Datenbasen des Dienstleisters, dem IT-System des Kunden (Wartungsgegenstand), Kontexten und über ein User-Interface mit dem Service-Techniker selbst kommuniziert. Im Ergebnis dieses Wartungsprozesses werden alle relevanten Daten für die Abrechnung bzw. Auftragsabwicklung dem erstgenannten Prozess in der IT-Umgebung des Dienstleisters zur Verfügung gestellt.

5.4 Identifizierte Bedrohungen

Bei der Analyse der Prozesse in der Domäne der Grünfutterernte wurden folgende Bedrohungen identifiziert:

- *Vertraulichkeit*: Ein Lohnunternehmer darf nur Zugriff auf Daten des Landwirtes haben, wenn eine Geschäftsbeziehung besteht. Durch die Aggregation geeigneter Daten lassen sich Rückschlüsse auf die Ertragssituation des Kundenbetriebes erlangen. Gleiches gilt für das Verhältnis Unternehmer – Mitarbeiter im landwirtschaftlichen Betrieb und im Lohnunternehmen. Wichtig ist, dass Landwirte die Daten in ihrem Einflussbereich schützen, so dass insbesondere Abnehmer, aber auch Lieferanten nur solche Informationen erhalten, die Gegenstand der Geschäftsbeziehung sind. Die Daten auf dem Backend müssen vom Provider ebenfalls vor nicht autorisiertem Zugriff geschützt werden.
- *Integrität*: Fehlende Integrität der Daten kann zu nicht nachvollziehbaren Vorgängen in den Geschäftsprozessen führen. Anwender können im Zweifelsfall keine Nachweise führen, dass die Daten von ihnen korrekt übermittelt wurden. Ferner sind die Prozesse nicht mehr auswertbar, eine Dokumentation wird unmöglich. Eine Entscheidungsgrundlage für nachfolgende Prozesse fehlt.
- *Verfügbarkeit*: Die fehlende Verfügbarkeit von Systemen führt im weniger kritischen Fall zu einer Verlängerung von Prozessen und damit zu einer Verteuerung. Im kritischen Fall kommen Prozesse zum Erliegen. Steht das Backend nicht zur Verfügung, können die Daten von der mobilen Einheit nicht direkt übertragen werden und der Prozess verzögert sich. Können aktuelle Informationen für die Hinderniswarnung nicht zeitnah übertragen werden, kann die Landmaschine im schlimmsten Fall auf ein Hindernis auffahren und ausfallen.
- *Authentizität*: Daten müssen sicher dem Sender bzw. Urheber zugeordnet werden können.

- *Zugriffssteuerung*: Durch fehlende Zugriffssteuerung kann es zu einem Verlust der Vertraulichkeit und weiterhin zu Störungen im Prozess durch fehlerhafte Bedienung der Systeme kommen. Das betrifft die Steuerung sowohl innerhalb von Arbeitsgruppen als auch die Sicht auf das Gesamtsystem.
- *Funktionalität*: Mangelnde Funktionalität führt im Extremfall zur Ablehnung des im Projekt entwickelten Ansatzes. Prozesse werden gestört, wenn Informationen nicht im richtigen Kontext und den Bedürfnissen des Anwenders entsprechend mitgeteilt werden. Die Erfahrung zeigt, dass bei ungeeigneter Funktionalität bestimmte Prozesse (z. B. Anpassung der Maschine) das erwartete Prozessergebnis gefährden. Nicht ausreichend getestete Funktionen können in bestimmten Ausnahmesituationen falsche Ergebnisse liefern. Aufgrund fehlender Funktionalität beschäftigt sich der Fahrer mehr mit der Ausführung der Prozesse statt sich auf die Bedienung der Maschine zu konzentrieren.
- *Einhaltung betrieblicher Prozesse*: Insbesondere in der Landwirtschaft können Prozesse nur unter Unsicherheit geplant werden. Eine Einhaltung des ursprünglichen Planes ist häufig nicht möglich. Eine Nichteinhaltung kann rechtliche Konsequenzen (Förderrecht, Straf- und Zivilrecht) haben.
- *Kontinuität des Angebotes*: Ist die Kontinuität aufgrund stark abweichender Lebenszyklen einzelner Bestandteile nicht gewährleistet, können Geschäftsprozesse nicht mehr optimal, im Extremfall gar nicht mehr ablaufen. Daraus folgt ein wirtschaftlicher Schaden und eventuell Schadensersatzansprüche.
- *Geschäftsprozess-Know-how*: Sind insbesondere funktionale Bestandteile von Geschäftsprozessen nicht ausreichend vor fremden Zugriff/Einblick geschützt, können Wettbewerber Kenntnis davon erlangen.

5.5 Bewertung der Bedrohungen

Für die Bewertung der Risiken von identifizierten Bedrohungen wird folgendes Schema angewandt:

Wahrscheinlichkeit des Eintretens:	Schadenspotential:
A = hoch	1= hoch
B = mittel	2 = mittel
C = niedrig	3 = niedrig

zu *Vertraulichkeit*: Einerseits ist die Wahrscheinlichkeit eines Verlusts der Vertraulichkeit im Falle des landwirtschaftlichen Szenarios relativ gering, da die Landwirtschaft aufgrund der Regulierung ohnehin sehr transparent ist. Mittlerweile werden die EU-Förderbeträge je Betrieb im Internet aufgeführt, Nährstoffbilanzen müssen geführt und der Einsatz von Pflanzenschutzmitteln dokumentiert werden. Andererseits ist der Verlust der Vertraulichkeit bei arbeitswirtschaftlichen Daten hoch zu bewerten.
Einschätzung: B1

zu *Integrität*: Bisher in der Landwirtschaft eingesetzte Lösungen werden insbesondere auch vor dem Hintergrund der Nachvollziehbarkeit entwickelt. Bislang hat es keine größeren Probleme gegeben. Das Risiko durch falsche bzw. unvollständige Datenbestände bei nicht automatisierter Erfassung ist als größer anzusehen. Im Falle nicht integrer Daten sind jedoch die Verluste schnell bedeutsam, insbesondere wenn förderungsrelevante Sachverhalte nicht nachvollziehbar sind. Dann kann der Verlust von Fördermitteln drohen.
Einschätzung: A1

zu *Verfügbarkeit*: Die fehlende Verfügbarkeit von Systembestandteilen, insbesondere Kommunikationsstrecken führt zu einer Verzögerung im Ablauf und ggfls. zu Mehraufwand bei der Nachbearbeitung. Unter Umständen ist die Entscheidungsfähigkeit beeinträchtigt, wenn notwendige Daten nicht zur Verfügung stehen, z. B. wie viel Pflanzenschutzmittel eingesetzt werden soll. Die Wahrscheinlichkeit ist hier relativ gesehen etwas höher als bei den anderen beschriebenen Kriterien, die Verluste aber gering oder nicht vorhanden.
Einschätzung: A2

zu *Authentizität*: Die fehlende Authentizität kann insbesondere bei der Einbindung von Diensten Konsequenzen haben. So ist es beispielsweise bei Informationen zu Pflanzenschutzmitteln wichtig, dass sie von autorisierter Seite kommen und sachlich richtig und aktuell sind. Durch die bislang geringe Verbreitung/Nutzung solcher Dienste liegen noch keine Erfahrungen vor. Des weiteren ist die Authentizität der Daten bei der Übertragung von der mobilen Einheit zum Backend sehr wichtig, da sie z. B. für die Rechnungserstellung benötigt werden.
Einschätzung: C3

zu *Zugriffssteuerung*: Die Zugriffssteuerung ist vor allem auf dem Backend und den Managementsystemen von Bedeutung. Risiken sind der Verlust der Vertraulichkeit sowie Fehlbedienungen bei zu weit gehenden Rechten. Lohnunternehmen und landwirtschaftliche Betriebe sind oftmals familiär organisiert, das Risiko daher gering. Größere Gefahren gehen vom Zugriff auf Systemfunktionen (z. B. Dateimanagement, Netzwerkmanagement) aus oder von einer Mehrfachnutzung von PCs durch Familienangehörige (Spiele, fehlende Struktur der Dateiablage, fehlende Systemkenntnis). Das Risiko auf PC-Seite ist relativ hoch. Vollständiger Datenverlust ist möglich, weil unter diesen Bedingungen auch häufig keine Sicherungsstrategien verfolgt werden.
Einschätzung: A1

zu *Funktionalität*: Mangelnde Funktionalität beeinträchtigt insbesondere zu Beginn die Akzeptanz durch den Anwender. Risiko ist hier für den Anbieter der Systemwechsel, wenn Alternativen bestehen. Allerdings ist zu erkennen, dass die Kundentreue aufgrund des hohen Migrationsaufwandes hoch ist. Auf Bordrechnern führt mangelnde Funktionalität dazu, dass bestimmte informationstechnische Prozesse nicht ausgeführt werden. Vor dem Hintergrund von Aushilfs- und Saisonarbeitkräften ist dieses Risiko nicht zu unterschätzen. Schäden sind unvollständige Dokumentation der geleisteten Arbeit und damit eine schlechte Datenbasis für anschließende Prozesse. Eine mangelnde Funktionalität lenkt die Aufmerksamkeit von der Bedienung elementarer Maschinenfunktionen ab und stellt damit ein Sicherheitsrisiko für Mensch und Maschine dar. Das Schadensausmaß ist mittel (Datenverlust) bis sehr hoch (Schaden an Mensch und Maschine).
Einschätzung: B1

zu *Einhaltung betrieblicher Prozesse*: Die mangelnde Einhaltung beherrschbarer betrieblicher Prozesse beinhaltet fast alle zuvor genannten Risiken. Aufgrund der Vielzahl und Höhe der Risiken kommt diesem Punkt in **R2B** die größte Bedeutung bzgl. Sicherheit zu.
Einschätzung: A1

zu *Kontinuität des Angebotes*: Ungeeignete oder nicht vorhandene Schnittstellen werden zum Problem, wenn im Zusammenspiel zahlreicher Systembestandteile eine davon z. B. durch Abkündigung nicht mehr verfügbar ist. In der europäischen Landtechnik gibt es keine Hersteller, die sämtliche Systeme aus einer Hand anbieten. Daher ist immer mit unabgestimmten und unterschiedlichen Lebenszyklen zu rechnen. Aufgrund zunehmender Standardisierung sinkt dieses Risiko. Hersteller unterstützen ihre Kunden bei der Migration.
Einschätzung: C2

zu *Geschäftsprozess-Know-how*: Erlangen Unbefugte Detailkenntnisse zu Geschäftsprozessen, besteht die Gefahr des Kopierens und damit einer Verdrängung aus dem Marktsegment. Je höher der Nutzen aus solchen Prozessen ist, desto größer der Schaden.
Einschätzung: C2

5.6 Identifizierte Gegenmaßnahmen

zu *Vertraulichkeit*: Der Zugang zu den Systemen muss software-technisch mit geeigneten Authentifizierungsmethoden reguliert werden, sodass Daten nur von Berechtigten genutzt werden können. Der physische Zugang sowohl zum Backend-Server als auch zum Rechner der mobilen Einheiten muss beschränkt sein.

zu *Integrität*: Kritische Prozesse müssen protokolliert und versioniert werden können. Um Modifikationen während des Transfers von Daten auszuschließen, müssen geeig-

nete Techniken verwendet werden. Und um die permanente Integrität zu gewährleisten, müssen entsprechende Datensicherungsstrategien eingesetzt werden.

zu *Verfügbarkeit*: Für die Kommunikation zwischen mobilen Einheiten und dem Backend sind alternative Kommunikationsverfahren oder Pufferstrategien erforderlich. Ist z. B. eine permanente Funknetzabdeckung nicht gewährleistet, werden Daten durch eine Store-Carry-Forward-Kommunikation von einer mobilen Einheit an die nächste übertragen. Die hohe Verfügbarkeit des Backend-Servers muss mit Standardmaßnahmen, wie sie in einem Rechenzentrum eingesetzt werden (Firewall, Load-Balancing, Virtualisierung usw.), gewährleistet werden. Bei mobilen Einheiten muss durch physische Maßnahmen ein Diebstahlschutz realisiert werden.

zu *Authentizität*: Fahrer und Anwender von Backend-Applikationen müssen sich zuvor gegenüber den Systemen identifizieren, um Aktionen eindeutig einzelnen Individuen zuordnen zu können. Ferner muss sichergestellt werden, dass auch nur erfolgreich identifizierte mobile Einheiten untereinander kommunizieren können.

zu *Zugriffssteuerung*: Es muss ein einheitliches Konzept für die Steuerung der abgestuften (evtl. hierarchischen) Zugriffe vorhanden sein.

zu *Funktionalität*: Um die Aufrechterhaltung der Funktionalität zu erreichen, ergeben sich folgende Anforderungen an die Software: Trennung von Funktionalität und Oberflächen gemäß dem Model-View-Controller-Konzept und systematische Funktionstests einzelner Softwaremodule-/komponenten und des Gesamtsystems. Aus der Sicht des Endnutzers ergeben sich weitere Anforderungen an die Funktionalität: Bedürfnisse von angelernten Mitarbeitern erfassen wie z. B. Dialoge durch Automatisierung ersetzen, Dialoge und deren Elemente vereinheitlichen, Standards nutzen und auch Usability-Aspekte beachten.

zu *Einhaltung betrieblicher Prozesse*: Um das doch recht hohe Maß an Dynamik bzgl. der geplanten Ausführbarkeit beherrschen zu können, muss eine geeignete Granularität für abzulaufende (Sub-)Prozesse gefunden werden. Falls sich Randbedingungen / Kontexte ändern, kann dies Einfluss auf aktuell ablaufende Prozesse oder noch abzuarbeitende Prozesse haben.

zu *Kontinuität des Angebotes*: Es ist von essentieller Wichtigkeit, dass möglichst Standards und offene Schnittstellenbeschreibungen eingesetzt werden, sowohl bei der Wahl von Hardware- als auch bei der Wahl von Softwarearchitekturen. Dieses Paradigma zieht sich durch von der Wahl der Tool-Ketten, der Datenformate bis zu Kommunikationsschnittstellen.

zu *Geschäftsprozess Know-how*: Vertraulichkeit, Verfügbarkeit und Authentizität sind sicher zu stellen, sowie ein geeignetes Verfahren zum Schutz der eigentlichen Prozesse zu realisieren (Schutz des BPEL-Codes, Schutz der Webservices). Ein weiterer Schutz kann in der Patentierung liegen. Hierbei ist aber die aktuell unsichere Situation zur Patentierung von Dienstleistungen und Geschäftsmodellen zu berücksichtigen.

5.7 Ausgewählte Gegenmaßnahmen

zu *Vertraulichkeit*: Um die Vertraulichkeit der Daten zu gewährleisten, gibt es verschiedene Standard-Techniken für die Verschlüsselung der Kommunikation. Handelt es sich um eine Punkt-zu-Punkt-Verbindung, z. B. Zugriff vom Hof-PC auf den Konfigurator per HTTP, kann die Verbindung mit SSL/TLS verschlüsselt werden. Sollen jedoch Daten von der mobilen Einheit zum Backend (Webservice) übertragen werden, empfiehlt sich der Einsatz von WS-Security. Falls keine direkte Verbindung zum Backend möglich ist, werden die Daten mittels einer Store-Carry-Forward-Kommunikation übertragen. Mit WS-Security wird die Nachricht unabhängig von der Anzahl der Kommunikationsknoten für den Empfänger verschlüsselt. Bei der Kommunikation über GPRS zwischen mobilen Einheiten bzw. zum Backend wird ein Virtual Private Network (VPN) Tunnel aufgebaut.

zu *Integrität*: Um die Integrität der Daten sicherzustellen, werden digitale Signaturen eingesetzt. Die mobilen Einheiten haben eine eindeutige Seriennummer für die ein Zertifikat zur Verfügung steht. Dieses Zertifikat wird für die digitale Signatur benutzt. Für die Verwaltung aller Zertifikate wird eine PKI-Infrastruktur benötigt.

zu *Verfügbarkeit*: Falls keine GPRS-Kommunikation möglich ist, können die Daten von der mobilen Einheit alternativ über einen Store-Carry-Forward-Mechanismus mit entsprechenden Pufferstrategien und Bestätigungs-Nachrichten zum Backend übertragen werden. Sollten die Bestätigungen ausbleiben, können die Daten auf SD-Speicher / Memory-Stick vom Fahrer mitgenommen werden. Kann für die Hinderniswarnung nicht auf den Datenbestand des Backends zugegriffen werden, wird ein Ad-Hoc-Netzwerk mit in der Nähe vorhandenen mobilen Einheiten aufgebaut oder ggfls. auf den lokalen Datenbestand zurückgegriffen. Wie bereits erwähnt, muss das Backend besonders abgesichert werden.

zu *Authentizität*: Die Identität von Anwendern, Ressourcen und Diensten wird in den Daten mitprotokolliert. Mittel zu Verifikation der Authentizität sind X.509-Zertifikate (Kommunikation) und nicht änderbare Seriennummern (iButton, Maschine und Anbaugerät). Personen werden zur Authentifizierung iButtons zugeordnet.

zu *Zugriffssteuerung*: Abgestufte Zugriffsrechte werden durch Rollen und damit verbundenen Berechtigungen definiert. Auf Daten einer Maschine wird nur lesend zugegriffen (CAN-Gateway). Die Hardware wird vor Zugriff von Dritten entsprechend geschützt.

zu *Funktionalität*: Durchführen von Funktions- und Akzeptanztests unter Einbeziehung aller am Prozess beteiligter Personen (Landwirt, Lohnunternehmer, Fahrer, Aushilfskräfte).

zu *Einhaltung betrieblicher Prozesse*: Um die Ausführbarkeit der betrieblichen Prozesse sicherstellen zu können, werden sowohl im Backend als auch auf der Maschine standardisierte Techniken eingesetzt: BPEL-Prozesse realisieren die Ablauffähigkeit z.T. mit menschlicher Interaktion; die Kommunikation von BPEL-Prozessen und allen weiteren

Beteiligten erfolgt über Web-Service-Standards inklusive Sicherheits-Standards. Um auf Änderungen der Umgebung reagieren zu können, wird eine Context-Engine eingesetzt, welche auf einer Rules-Engine basiert. Hierdurch ist es möglich, durch eine Reihe von „wenn-dann"-Verknüpfungen zu reagieren oder auch proaktiv zu agieren.

zu *Kontinuität des Angebotes*: Um nicht von bestimmten Anbietern abhängig zu sein, werden Standards und Open Source Software wie TCP/IP, agroXML, OGC, ISO-XML, Java usw. eingesetzt. Auf Hardwarekompatibilität sowie präziser Beschreibung externer Dienste mit UDDI wird geachtet.

zu *Geschäftsprozess Know-how*: BPEL-Prozesse und Webservices dürfen nur von autorisierten Benutzern gestartet werden. Als zusätzliche Sicherheitsmaßnahme kann bei den mobilen Einheiten die Verschlüsselung des Datenträgers eingesetzt werden.

Checkliste Maschinenbau

Wichtige Hinweise für mobile IT-Sicherheit im Maschinenbau

Mobile Systeme müssen in unterschiedlichste Infrastrukturen möglichst einfach integriert werden können, um eine hohe Akzeptanz und Kontinuität im Betrieb zu erreichen. Die Verwendung von Standardtechnologien und offene Schnittstellenbeschreibungen sind hierfür von entscheidender Bedeutung.

Die Sicherheitsfunktionen mobiler Systeme müssen flexibel konfigurierbar sein, um individuelle Anforderungen verschiedenster Geschäftsprozesse an Werte wie Vertraulichkeit, Integrität und Authentizität abbilden zu können.

Für einen erfolgreichen Einsatz im Bereich Maschinenbau, insbesondere in zeitkritischen Abläufen, müssen mobile Systeme hochverfügbar sein sowie Daten rechtzeitig und korrekt zur Verfügung stellen können. Dies ist umso wichtiger, wenn es darum geht, Unfälle zu vermeiden.

Mobile Systeme müssen einfach bedient werden können. Ihre Anwendung sollte eine unterbrechungsfreie Geschäftstätigkeit sowie die kontinuierliche Wahrnehmung der Arbeitsumgebung fördern und so Arbeits- und Prozesssicherheit erhöhen.

Akzeptanz und IT-Sicherheit können erhöht werden, wenn Sicherheitsstandards und Funktionstests unter Einbeziehung aller am Prozess beteiligten Personen bereits im Entwicklungsprozess berücksichtigt werden.

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik. (2008). BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS) Version 1.5. Bonn: BSI.

G. Diederich, R. Sethmann, S. Schäfer and Z. Ghrairi, (Sept. 7, 2008) SiWear -- Sichere Wearable-Systeme: Verwendung von Sicherheitsstandards im Entwurf von Wearable-Systemen am Beispiel der Benutzungsschnittstelle; in Workshop Proceedings der Tagungen Mensch & Computer 2008, DeLFI 2008 und Cognitive Design 2008, U. Lucke, M. C. Kindsmüller, S. Fischer, M. Herczeg and S. Seehusen, Eds., Lübeck

Ansprechpartner:

Thilo Steckel (für R2B)
Claas Selbstfahrende Erntemaschinen GmbH
Münsterstr. 33
33428 Harsewinkel
Tel.: 05247 12 2074
E-Mail: thilo.steckel@claas.com

Gudrun Tschirner-Vinke (für R2B)*
Siemens AG
C-LAB
Fürstenallee 11
33102 Paderborn
Tel.: 05251 60 6091
E-Mail: gudrun.tschirner-vinke@siemens.com

Günther Diederich (für SiWear)
Institut für Informatik und Automation
Hochschule Bremen
Flughafenallee 10
28199 Bremen
Tel.: 0421 5905 5472
E-Mail: Guenther.Diederich@hs-bremen.de

* in Nachfolge für Dr. Christoph Loeser, Co-Autor.

6 Mobile IT-Sicherheit in der Gesundheitswirtschaft: Sicherheit durch Innovation - Innovation durch Sicherheit

6.1 Bedrohungsanalyse in der Pflege, im Rettungsdienst und bei mobilen Assets

Im privaten Sektor hat sich der Einsatz von neuen und mobilen Informations- und Kommunikationstechnologien stark verbreitet. Hierauf muss sich neben den Geschäftsfeldern Maschinenbau, Öffentliche Verwaltung, KMU und Handwerk auch der Bereich der Gesundheitswirtschaft einstellen und diese neuen Technologien in seinen Geschäftsprozessen etablieren. Dabei fehlt es in Deutschland jedoch an verschiedenen wissenschaftlichen Grundlagen bzw. etablierten Standards, um mobile Informations- und Kommunikationstechnologien (IKT) einzusetzen.

Im Folgenden wird auf den Einsatz von IKT im Bereich der Pflege, des Rettungsdienstes und den effizienten Einsatz von mobilen Assets bzw. die Temperaturüberwachung von Blutprodukten und deren Auswirkungen auf Informationssicherheit eingegangen. Da der Einsatz von mobilen Endgeräten, deren Datenaufkommen und der Übermittlung von patientenbezogenen Daten einen neuen Kontext darstellen, wird die Methodik der Bedrohungsanalyse speziell im Bereich der Gesundheitswirtschaft dargestellt und anhand einzelner Szenarien erörtert. Darüber hinaus wird detailliert auf das Medizinproduktegesetz eingegangen, das für den Einsatz von medizinischen Produkten zu beachten ist.

6.2 Rechtliche Herausforderungen im Gesundheitswesen stellen hohe Anforderungen an die IT-Sicherheit

Das Gesundheitswesen macht in Deutschland mit einem Volumen von über 250 Milliarden Euro jährlich einen wichtigen Ausgabenposten aus. Moderne IK-Technologien haben bisher nur teilweise Einzug in das Gesundheitswesen gehalten. Häufig sind noch papiergestützte Dokumentation und Medienbrüche die Regel. Hier könnte ein schneller, umfassender und zuverlässiger Austausch von Patientendaten zwischen behandelnden Krankenhäusern und Pflegeeinrichtungen zur Verbesserung der Qualität und Effizienz der Gesundheitsversorgung führen. Jedoch droht der immer umfangreicher werdende Informationstransfer im Gesundheitswesen, das informationelle Selbstbestimmungsrecht des Patienten zu beeinträchtigen.

Dieses Spannungsverhältnis[3] zwischen den Interessen des Einzelnen und der Gesellschaft aufzulösen, gehört zu den schwierigsten Aufgaben bei der Weiterentwicklung des Gesundheitssystems. Bei immer komplexer werdenden telemedizinischen Verfahren müssen daher die rechtlichen Voraussetzungen und Anforderungen bei der Erhebung, Verarbeitung und Nutzung personenbezogener Patientendaten mit besonderem Nachdruck betrachtet werden. Hierbei sind die verfassungsrechtlichen Grundsätze der Erforderlichkeit, Zweckbindung und Verhältnismäßigkeit sowie das Recht auf informationelle Selbstbestimmung zu beachten, unabhängig davon, auf welche Weise die Datenverarbeitung geschieht. Beim Einsatz moderner Informations- und Kommunikationstechnologien ist insbesondere die Einhaltung der Zweck- und Aufbewahrungsbestimmungen durch technische Maßnahmen zu gewährleisten. Auch die betroffenen Rechte gemäß den Datenschutzvorschriften – z. B. die Patientenansprüche auf Akteneinsicht oder die Rechte auf Auskunft, Berichtigung und Löschung der Einträge – müssen zu jeder Zeit gewahrt werden. Der Arzt darf Dritten private Informationen über den Patienten in der Regel nur dann mitteilen, wenn der Patient zugestimmt hat. Andere Erlaubnisvorschriften greifen lediglich in wenigen Ausnahmefällen und rechtfertigen nicht zwingend den Einsatz der Telemedizin.

Festzuhalten bleibt, dass ein effektiver Datenschutz die selbstverständliche Basis aller telemedizinischen Anwendungen sein muss. Der Datenschutz ist nur dann wirksam, „wenn er die Technik, die die elektronische Datenverarbeitung hervorgebracht hat, dazu einsetzt, um die Gefahren dieser Technik wieder einzugrenzen. Es bedarf aller Anstrengungen zur technischen Innovation, um die wechselseitige Abschottung der Informationssysteme mit den Zielen des Persönlichkeits- und Geheimnisschutzes auszubauen und zu sichern“[4]. Obwohl dem Bundesdatenschutzgesetz ein Schutzgedanke zu Grunde liegt, der auf den ersten Blick der Telemedizin hinderlich erscheint, nämlich die „Datenvermeidung und Datensparsamkeit“ (§ 3a BDSG), stehen die geltenden Bestimmungen dem Einsatz telemedizinischer Anwendungen im Rettungsdienst nicht entgegen. Die Ausnahmen des Datenverarbeitungsverbotes ermöglichen einen angemessenen Schutz des Patienten, ohne der fortschrittlichen Telemedizin grundsätzlich ein Hindernis zu sein. Der Sicherung der Patientenrechte kann daher auch beim Einsatz telemedizinischer Anwendungen im Rettungsdienst nachgekommen werden. Auch indem dem Telemediziner bereits bei stillschweigender Einwilligung des Patienten personenbezogene Daten übermittelt werden können, droht keine Aushöhlung des Datenschutzes, wenn vorher stets sowohl der Grundsatz der Datenvermeidung und Datensparsamkeit als auch das Erforderlichkeitskriterium beachtet wird.

---

3 Vgl. im folgenden Katzenmeier, Chr. und Slavu, St. (2009): Rechtsfragen des Einsatzes der Telemedizin im Rettungsdienst, Rechtsgutachten Med-on-@ix, Institut für Medizinrecht, Universität zu Köln, S. 182f.

4 Berg, W., Telemedizin und Datenschutz, in: MedR 2004, S. 411-414.

Das Medizinproduktegesetz (MPG)[5] setzt die europäischen Richtlinien 98/79/EG, 93/42/EWG und 90/385/EWG in deutsches Recht um. Das Gesetz bezieht sich vor allen Dingen auf Produkte, die in direktem Kontakt mit dem Patienten stehen, sei es zur Behandlung (z. B. Skalpelle) oder zur Diagnose (z. B. EKG-Monitore). Telefone in einem Krankenhaus, oder sonstige Kommunikationsinfrastruktur, die keinen direkten Kontakt mit dem Patienten hat, fallen nicht in den Geltungsbereich des MPG. Für eine gesetzeskonforme Entwicklung eines Medizinprodukts sind aufwendige Tests und Risikoanalysen notwendig. Dadurch ist der Entwicklungsaufwand deutlich größer als bei einem Produkt, das nicht in den Geltungsbereich des MPG liegt. Produkte, die eine der folgenden Eigenschaften besitzen, unterliegen diesen Regelungen:

- Erkennung, Verhütung, Überwachung, Behandlung oder Linderung von Krankheiten,
- Erkennung, Überwachung, Behandlung, Linderung oder Kompensierung von Verletzungen oder Behinderungen,
- Untersuchung, Ersetzung oder Veränderung des anatomischen Aufbaus oder eines physiologischen Vorgangs oder
- der Empfängnisregelung.[6]

Weiterhin unterliegen medizinische Sonderanfertigungen, Zubehör, Kombinationsprodukte und aktiv implantierbare medizinische Geräte dem Medizinproduktegesetz.

Relevanz für die verschiedenen Projekte ergibt sich aus der Richtlinie für Zubehör und Kombinationsprodukte. So werden Kombinationsprodukte als Erweiterung von Medizinprodukten angesehen und fallen somit ebenfalls unter das MPG. Unter Zubehör fallen alle benötigten Produkte eines Medizinprodukts (in diesem Falle auch Software). Abzuwägen ist der Einsatz des Produktes. Beispielsweise werden schon seit längerem Funkübertragungen von Vitalparametern im Bereich des Fitness-Sportes zur Selbstüberwachung eingesetzt. Der Weg in klinische Anwendungen wurde bisher aufgrund des Medizinproduktegesetzes für diese Art von Produkten vermieden.

6.3 Vorgehensweise: Schritte zur strukturierten IT-Sicherheitsanalyse

Angelehnt an die Methode „Schritte zur strukturierten IT-Sicherheitsanalyse“ entschieden sich die Projektverantwortlichen in den SimoBIT-Projekten im Bereich Gesundheitswirtschaft **VitaBIT**, **Med-on-@ix** und **OPAL Health** für verschiedene sicherheitsrelevante Komponenten bzw. Prozesse.

---

5 Medizinproduktegesetz in der Fassung der Bekanntmachung vom 7. August 2002 (BGBl. I S. 3146), geändert durch Artikel 6 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2326).

6 Vgl. Art. 1 Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte Amtsblatt Nr. L 169 vom 12/07/1993 S. 0001 – 0043.

Trotz der unterschiedlichen Ansätze ergaben sich jedoch Schnittmengen im iterativen Finden von Entscheidungen und dem iterativen Entwickeln von Komponenten und Modulen zur Unterstützung von IT-Sicherheit. Dabei war der Einstieg der Projekte bei verschiedenen Punkten der Bedrohungsanalyse, jedoch wurden Schritte durchgeführt, die sich im Einklang mit dem vorgestellten Konzept beschreiben lassen. Beispielhaft kann dies an dem Projekt **VitaBIT** verdeutlicht werden:

In **VitaBIT** stand am Anfang der Entscheidung die Frage nach der Integration einer Sicherheitskomponente für ein ideales portables Gerät zum Einsatz als digitaler Assistent für den Pflegedienst. Als Geräte waren dies anfänglich kommunikationsfähige PDAs, die als mobile Handhelds einen SD Card Slot integriert hatten. Dann wandelte sich das User-Szenario, nicht zuletzt bedingt durch den Erfolg der Smartphones. Als steckbare Sicherheitskomponente kam dann nur noch der kleinere Formfaktor der microSD in Betracht. Dies stellte jedoch eine neue Herausforderung an die Fertigungstechnologien im Halbleiterbereich dar, um auf kleinstem Raum den erforderlichen Mikrocontroller, den Sicherheitschip und den Gigabyte Flashspeicher zu integrieren. Dieser iterative Schritt zur Realisierung einer Sicherheitskarte in der kleinstmöglichen Bauform wurde vor allem durch die Anforderungen des sich äußerst dynamisch entwickelnden mobilen Endgerätemarktes ausgelöst. Aus heutiger Sicht erweist sich dieser Entwicklungsschritt als unbedingt notwendig.

6.4 Bedrohungen identifizieren und bewerten

Das künftige „Rückgrat“ für den allgemeinen und gesicherten Zugriff zu medizinischen Daten bildet künftig die Telematikinfrastruktur im Gesundheitswesen und als nicht all zu fernes Ziel sollten Informationsdienste für den Pflegedienst, wie andere geschlossene Informationssysteme im Übrigen auch, einen möglichst hohen Grad an Vernetzung mit medizinischen Instanzen ermöglichen. Übergänge von einem Sicherheitsbereich in einen anderen setzen besondere vertragliche Regelungen voraus, die den Import wie Export von sensiblen Daten regeln. Eine mögliche Kompromittierung einer Sicherheitsdomäne muss dabei unter Einbezug von technischen Maßnahmen weitestgehend ausgeschlossen werden.

Medizinische Instanzen, auch als künftige Teilnehmer an der Telematikinfrastruktur, können Daten aus **VitaBIT** sicher importieren und ebenso Daten sicher exportieren, wenn sie einen Zugang mit Sicherheitstoken zur **VitaBIT**-Plattform haben. Auf diese Weise können z. B. Hausärzte mit dem Pflegedienst auf hohem Sicherheitslevel den Datenaustausch gewährleisten. Zuvor sollte jedoch eine rechtliche Basis unter den Parteien bestehen, die die Zustimmung des Patienten im Umgang mit personenbezogenen medizinischen Daten mit einschließt.

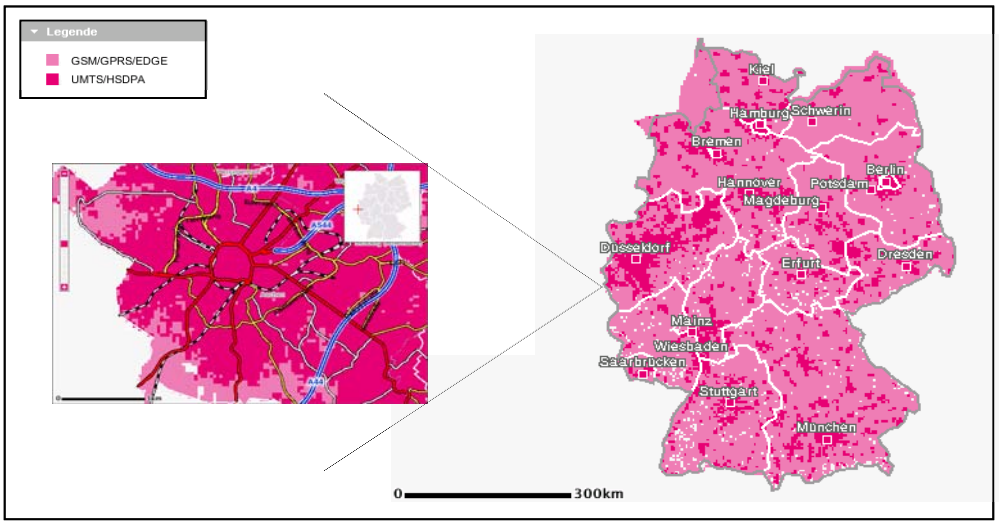
Von daher orientiert sich das Sicherheitskonzept der **VitaBIT**-Plattform an der Telematikinfrastruktur im Gesundheitswesen, um den Datenaustausch bestmöglich auf die Anwendung mobiler Smartphones im ambulanten Pflegedienst ausdehnen zu können.

6.5 Gegenmaßnahmen identifizieren und auswählen

6.5.1 Med-on-@ix

Deutschlandweit und im Besonderen in ländlichen Gebieten existieren heutzutage immer noch erhebliche Versorgungslücken, was die breitbandigen Funkzugangstechnologien der dritten Mobilfunkgeneration (UMTS/HSPA) anbelangt.

Abbildung 6-1: Funkzugangstechnologien Deutschland und Aachen am Bespiel von T-Mobile[7]



Quelle: T-Mobile

Zusätzlich kann es durch intensive Nutzung der Funkzellenkapazität einzelner Nutzer zu Qualitätsabstufungen bei den anderen Nutzern kommen. Letztendlich sind auch, wenn auch selten, Störungen im Netzbetrieb möglich, die schlimmstenfalls zu einem Gesamtausfall des Mobilfunknetzes führen. Die Hauptanforderungen aus **Med-on-@ix** an eine sichere Datenübertragung bzgl. Mobilität, hoher Verfügbarkeit und Zuverlässig-

7 Quelle: http://www.t-mobile.de/funkversorgung/inland/, Stand: 15.01.2010

keit lässt eine Standardlösung beispielsweise auf der Basis einer einzigen Funkzugangstechnologie hier nicht sinnvoll erscheinen.

Als weitere Rahmenbedingung muss sichergestellt werden, dass sensible Daten im Rahmen gesetzlicher Vorschriften geeignet gegen Zugriffe Dritter gesichert werden[8] und die Kommunikation zwischen Einsatzstelle und Kompetenzzentrum reibungslos abläuft. Da das Kommunikationssystem hauptsächlich nicht von Technikern bedient wird, müssen auch im Hinblick auf die Akzeptanz des Systems im Rettungswesen Robustheit, Zuverlässigkeit und Bedienerfreundlichkeit im Fokus liegen.

Eine Steigerung der Redundanz und damit der Ausfallsicherheit kann durch den Einsatz von mehreren, *parallel arbeitenden* Übertragungskanälen erreicht werden. Zusätzlich kann mit einer Mehr-Kanal-Mehr-Betreiber Lösung einer beschränkten Datenübertragungsrate entgegengewirkt werden. Beide Punkte führen zu einer Steigerung der Verfügbarkeit und Zuverlässigkeit von Diensten im **Med-on-@ix** System.

Frühzeitig wurden kommerzielle Mobilfunktechnologien als State-of-the-art Technologien ausgewählt. Eine mobilfunktechnische Vermessung der örtlichen, für den Evaluationsbetrieb bestimmten Region, konnte diese Auswahl bestätigen. Damit mobile Anwendungen das Potential der Mehr-Kanal-Mehr-Betreiber-Lösung nutzen können, wurde ein hybrides System entwickelt, das auf der Vermittlungsschicht (s. ISO/OSI Modell) die Anwendungsdaten so aufteilt, dass entsprechend der aktuellen Situation der Übertragungskanäle die Daten aufgeteilt werden können. Damit wird eine im Sinne der Abhörsicherheit sichere und zuverlässige bidirektionale Kommunikation zwischen mobilen und stationären Parteien ermöglicht. Für die Praxis bedeutet dies, dass ein Problem (z. B. Lastproblematik, Ausfall oder fehlende Coverage) im Mobilfunknetz eines oder mehrerer Mobilfunknetzbetreiber nicht zum Ausfall des Gesamtsystems führen muss. Anwendungen, wie beispielsweise Videostreaming, File-Transfer oder auch EKG-Live-Übertragungen können auf diese Weise trotz Problemen in der Übertragung eines Netzbetreibers oder auch mehrerer Betreiber seamless betrieben werden. Speziell in ländlichen Regionen, wo häufig nur Funkzugangstechnologien der 2. Mobilfunkgeneration verfügbar sind, kann auch eine Mindest-Datenübertragungsrate zur Verfügung gestellt werden. Für **Med-on-@ix** bedeutet dies, dass neben EKG-Daten in Echtzeit auch noch weitere Dienste wie z. B. File-Transfer zum Synchronisieren der Daten zwischen Einsatzstelle und Telenotarztzentrale dauerhaft möglich sind.

Natürlich kann das System keine Garantie für eine hundertprozentige Verfügbarkeit darstellen (beispielsweise in weit abgelegenen ländlichen Regionen, in denen Mobilfunkbetreiber aus wirtschaftlichen Gründen keine Netzabdeckung anbieten), daher müssen weitere organisatorische Maßnahmen eingeführt werden.

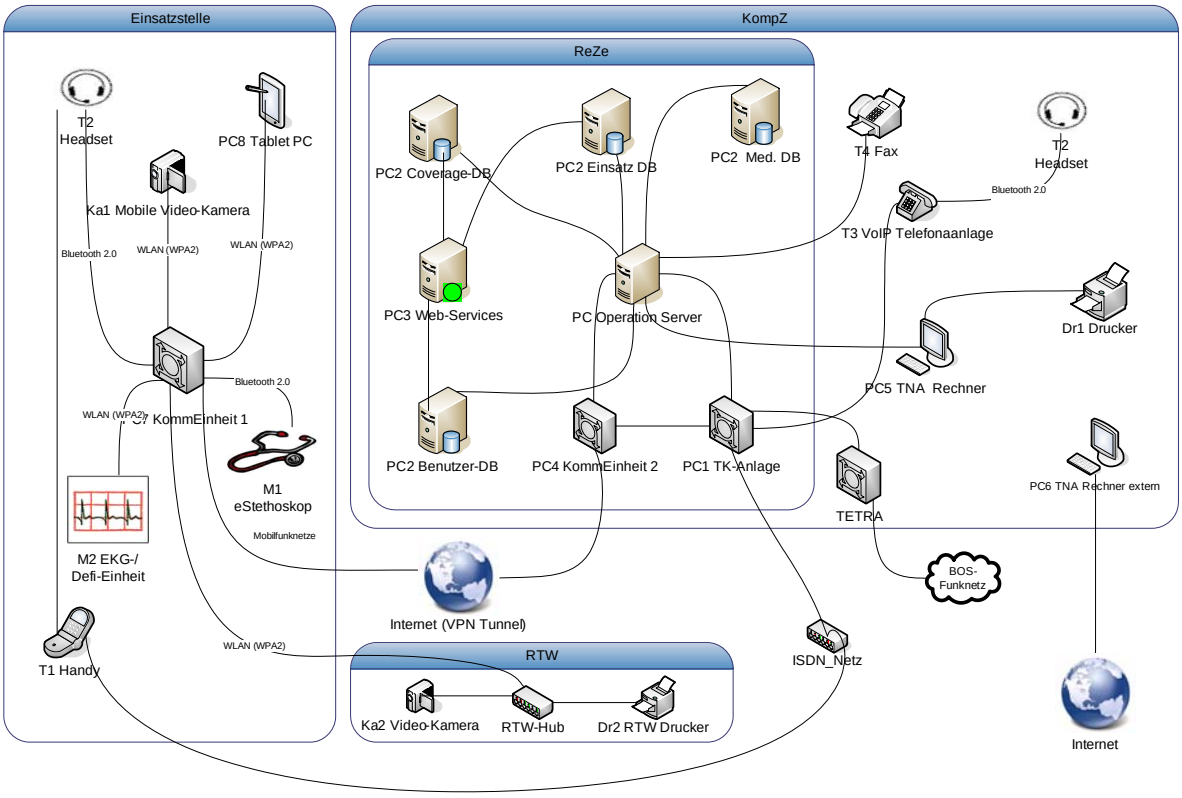
---

8 Vgl. Beispiele für entsprechende gesetzliche Vorschriften: Datenschutz-Richtlinie 95/46/EG vom 24. Oktober 1995, nationale Datenschutzgesetze (u.A. BDSG, LDSG), Ärztliche Berufsordnungen, Strafgesetzbuch (§ 203 StGB), Sozialgesetzbuch (§ 76 SGB X).

Unter den sicherheitsrelevanten organisatorischen Entscheidungen sind besonders die Abschottung vom Internet und die Handhabung der Zugriffsrechte auf die Systemdaten zu erwähnen.

Das **Med-on-@ix**-System ist vom Internet abgeschottet (Abbildung 6-2). Die Kommunikation zwischen Einsatzstelle und Telenotarzt-Zentrale ist immer über VPN verschlüsselt. Der Zugang zu wichtigen medizinischen Datenbanken im öffentlichen Internet wird durch einen separaten, vom System getrennten PC in der Telenotarzt-Zentrale ermöglicht. Dadurch wird die Angriffsfläche, die das System Angreifern aus dem Internet bietet, stark reduziert.

Abbildung 6-2: Übersicht der Hardwarekomponenten von Med-on-@ix



Quelle: Med-on-@ix

Die Zugriffsrechte des Systems werden rollenbasiert nach dem Need-to-Know-Prinzip vergeben. So hat der Administrator keinen Zugriff auf die Patientendaten und der Telenotarzt nur Zugriff auf die Daten des aktuell behandelten Notfallpatienten. Hochsensible Daten wie Videos der Patienten werden 48 Stunden aufbewahrt, bevor sie unwiederbringlich gelöscht werden. Auf der einen Seite wird so die Auswertung von kritischen

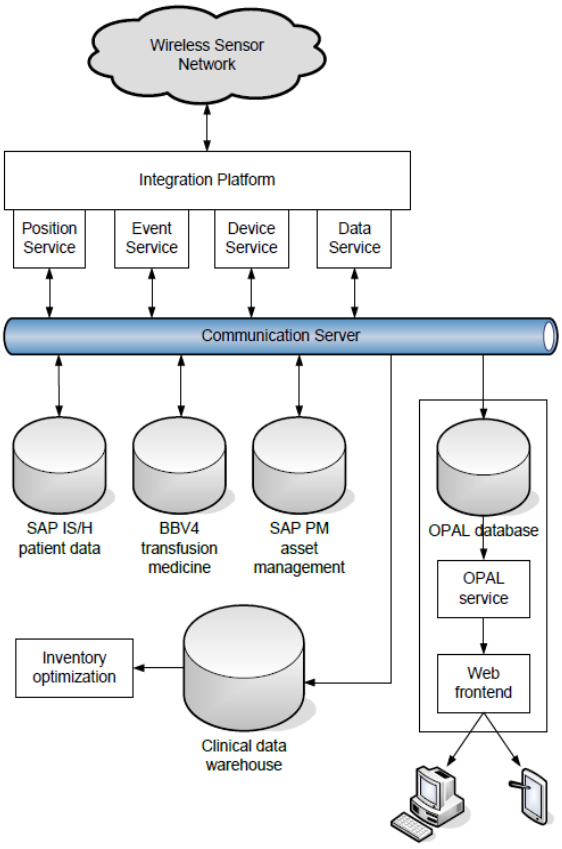
Fällen erlaubt. Auf der anderen Seite wird dadurch vermieden, dass diese schlecht anonymisierbaren, schwer elektronisch auswertbaren Daten in falsche Hände geraten und öffentlich gemacht werden.

Die erfolgreiche Kombination von technischen wie organisatorischen Maßnahmen ist der Schlüssel für die IT-Sicherheit des Systems **Med-on-@ix**.

6.5.2 OPAL Health

Im Projekt **OPAL Health** wurden nach dem iterativen Vorgehen der Bedrohungsanalysen alle identifizierten Bedrohungen im Bereich des Einsatzes von Smart Object Netzwerken herausgearbeitet und Handlungsentscheidungen getroffen, um höchste IT-Sicherheit zu garantieren. Diese Entscheidungen nahmen einen hohen Stellenwert in der weitergehenden Entwicklung des Projektes ein und mussten von den verschiedenen Projektpartnern in ihren Arbeitspaketen bedacht und in der Planung und Implementierung der verschiedenen Module realisiert werden.

Abbildung 6-3: OPAL Health Systemarchitektur



Quelle: OPAL Health

Im Falle von **OPAL Health** hat sich ein elementares Ziel herauskristallisiert, dass sowohl Prozess- als auch technologische Sicherheit garantiert. Dabei handelt es sich um die Anforderung, patientenbezogene Daten nicht auf dem Smart Object abzuspeichern, sondern über die Funkschnittstelle zu kommunizieren bzw. Prozesse und Back-End-System-Komponenten mit vertrauenswürdiger Information zu unterstützen.

Im Detail bedeutet dies, dass innerhalb von **OPAL Health** nur mit pseudonymisierten Patientenfallnummern gearbeitet wird. Eine Auflösung mit einer vermehrten Transparenz der Patientendaten kann nur in Verbindung zu dem Klinikumsinformations-System (KIS) und der Zuordnung zwischen pseudonymisierter und tatsächlicher, im KIS verwendeter, Patientenfallnummer realisiert werden. Dabei werden Sicherungssysteme, wie z. B. Authentifizierung, von den üblichen Systemen her verwendet und benötigen keine weitere Instanz von Sicherheitskomponente. Somit können die elementaren Ziele, Schutz der Vertraulichkeit, Schutz der Integrität und Verfügbarkeit, gewahrt bleiben.

Schutz der Vertraulichkeit

Im Einsatz der Smart Object-Netzwerke werden nur die pseudonymisierte Patientenfallnummer als Identifikationsgrundlage, die von einem eigenständigen Modul generiert wird und die Datenbank, die jegliche Zugriffs- und Vertraulichkeitsaspekte unterstützt, und somit eine Auflösung vollziehen kann, herangezogen. Dadurch ist das Ziel der Vertraulichkeit gewahrt.

Schutz der Integrität

Da patientenbezogene Daten in dem eingesetzten System nicht verwendet werden, sondern das Krankenhausinformationssystem weiter die Informationshoheit besitzt, werden keinerlei Schreibrechte von anderen Datenbanken oder Informationssammlungen unterstützt. Die Integrität der Daten wird durch den Einsatz der Smart Object-Technologien somit nicht verletzt.

Verfügbarkeit

Das System ist auch ohne einen Live-Zugang zu den KIS in voller Betriebsbereitschaft. Lediglich die Informationen zu patientenbezogenen Daten können nicht eingesehen werden.

Nachteile

Durch den Einsatz von pseudonymisierten Patientenfallnummern können einige Szenarien und Einsatzpotentiale der zugrunde liegenden Technologie nicht realisiert werden. So können Prozesse, die eine Abfrage von patientenbezogenen Daten benötigen bzw. die Änderungen oder einen erhöhten Informationsgehalt während gewisser Funktionen von Mitarbeitern, Ärzten bzw. Pflegepersonal brauchen, in dem Projekt **OPAL Health** nicht unterstützt werden. Damit haben sich die Einsatzpotentiale der Smart-Object

Netzwerke im Gesundheitswesen verringert, mit dem jedoch überwiegenden Vorteil, die Grundzüge der IT-Sicherheit durch einfache Mechanismen zu gewähren.

6.5.3 VitaBIT

VitaBIT bietet ein spezielles Sicherheitskonzept für mobile Anwendungen im Gesundheitswesen. In der Anwendung der Plattform für ambulante Pflegedienste beschreitet **VitaBIT** neue Wege: Der projektbegleitende Pflegedienstleister testet als Pilot-Anwender im ambulanten Pflegedienst die Bedienbarkeit der IT-gestützten Pflege-Plattform im Alltag und deren Wirtschaftlichkeit. Das Projekt setzt um, was in der Praxis bisher nur unzureichend funktioniert: Die Möglichkeit zur Kommunikation und Kooperation zwischen Hausarzt, Pflegedienstleister und mobilen Mitarbeiten – kurz: aller Beteiligten im Pflegenetzwerk rund um den Pflegenden. Die Plattform von **VitaBIT** soll die Kommunikation und den sicheren Informationsaustausch zwischen allen Beteiligten im Pflegeprozess erstmals auf der Basis eines neuen Sicherheitskonzeptes ermöglichen.

Abweichend von bisherigen Lösungen mit dedizierten und verteilten Softwareclients auf mobilen Endgeräten, die im sporadischen Kontakt mit einer zentralen Serverkomponente kommunizieren, wird in **VitaBIT** der internetbasierte Browserzugang zu zentralisierten Web- und Softwareservices favorisiert.

Dadurch ergibt sich bei Bedarf eine optimale Erweiterbarkeit und Wartungsfähigkeit des Systems an individuelle Erweiterungen und Anpassungen in Funktionen und Services. **VitaBIT** nutzt die Plugin-Fähigkeit von Browsern, mit deren Hilfe standardisierte Webservice-Schnittstellen integriert werden. Ferner werden Schnittstellen für etablierte Pflegeplanungssoftware zur Verfügung gestellt, so dass ein Pflegedienst auf bereits bekannte Software-Umgebung weiterhin zugreifen kann.

Der Zugang zu persönlichen oder gesundheitsbezogenen Daten wird dabei je nach Anwender beschränkt. Die spezielle Sicherheitskomponente der SD Card oder der microSD, je nach Verfügbarkeit des Steckplatzes, wird für die Autorisierung des mobilen Zuganges zu sensitiven Pflege- und Patientendaten in jedem Smartphone eingesetzt.

Abbildung 6-4: Smartphone mit Sicherheitskomponente zur Anwendung im ambulanten Pflegedienst

Quelle: WIBU-Systems

Eine weitere Sicherheitsanwendung während einer Pflegedienstleistung vor Ort beim Patienten sieht die Erfassung von sensiblen Messdaten vor. Life-Sensoren übertragen medizinische Daten an das mobile Smartphone im Online-Betrieb, die während einer Messung z. B. des Blutzuckers oder der Pulsfrequenz beim Patienten anfallen. Andere personenbezogene Informationen sind digitale Aufnahmen zur medizinischen Dokumentation des Verlaufes einer Wundbehandlung. Die Bildinformationen der digitalen Kamera (im Smartphone integriert) müssen ebenfalls als sensitive personenbezogene Daten behandelt werden, wenn sie übertragen und in einer digitalen Pflegeakte gespeichert werden (Abbildung 6-4).

Der Vorschlag zur Einführung eines hardwarebasierten Sicherheitstokens auf der Basis einer Flashkarte für mobile Endgeräte bestand schon ganz zu Anfang des Projekts. Die Frage nach der geeigneten Integration des Tokens in die Betriebssystem- und Kommunikationsumgebung rückte während der Entwicklung stärker in den Vordergrund und führte zu iterativen Lösungsschritten. Die weitestgehende Unabhängigkeit von Hard- und Software und die größtmögliche Interoperabilität versprach die Lösung mit Java basiertem Code zur plattformübergreifenden Unterstützung der SD Card. Die Anforderungen, die an die Sicherheitsmechanismen, wie Verschlüsselung und Generieren einer digitalen Signatur zu stellen waren, konnten über die vorhandenen Standardfunktionen des Smartcard-Chips abgedeckt werden (Abbildung 6-5).

Die Flash-Karte mit integriertem Smartcard-Chip verfügt über ein sehr leistungsfähiges Interface, das, anders als bekannte SIM-Karten, eine hohe Datenübertragungsrate besitzt. Daher eignet sich die Flash-Karte aus prinzipiellen Gründen sehr gut dazu, medi-

zinische Daten verschlüsselt zwischenzuspeichern, wenn eine Online-Übertragung einmal nicht möglich sein sollte.

Ein weiterer Vorteil der SD Card besteht darin, dass sie, wie die SIM-Karte, Zertifikate und sensible Schlüssel vor Angriffen gesichert speichert. Damit lässt sich im Smartphone unabhängig von der SIM-Karte ein weiteres Sicherheitstoken implementieren, welches unabhängig vom Netzwerkbetreiber eingesetzt werden kann.

Abbildung 6-5: Sicherheits- und Speicherkomponente microSD

Quelle: WIBU-Systems

Ein weiterer wichtiger Aspekt ist die Interoperabilität von Komponenten auf der Basis von Standards und Industriestandards. In Bezug auf die Standardisierung der SD Card ist anzumerken, dass die Leistungsfähigkeit des Standards der Marktdynamik im Consumer Electronics Bereich raschen Standardisierungsschritten folgt. Die Integration von Security-Protokollstandards im Standards-Werk ist unter anderem ein Beleg dafür.

Die IT-Sicherheit nimmt in mobilen Anwendungen einen großen Stellenwert in Bezug auf die Akzeptanz des Produktes und die damit verbundene Dienstleistung ein. Das Konzept der Bedrohungsanalyse bildet in der Gesundheitswirtschaft eine Möglichkeit, die geforderten Ziele der IT-Sicherheit zu einem frühen Zeitpunkt innerhalb von Projekten einfließen zu lassen. Hierbei ist die Evaluierung und Einschätzung der Bedrohungen und Risiken durch die Einführung mobiler Anwendungen ein Schritt hin zu einer integren Systemarchitektur und Implementierungsentscheidung, in der Sicherheitsmaßnahmen durch geeignete Methoden realisiert werden können.

Checkliste Gesundheitswirtschaft

Wichtige Hinweise für mobile IT-Sicherheit in der Gesundheitswirtschaft

Bei telemedizinischen Verfahren müssen die rechtlichen Anforderungen an die Erhebung, Verarbeitung und Nutzung personenbezogener Patientendaten mit besonderer Sorgfalt berücksichtigt werden.

Für eine gesetzeskonforme Entwicklung eines Medizinprodukts sind aufwendige Tests und Risikoanalysen notwendig

Eine insbesondere im Gesundheitswesen erforderliche Steigerung der Ausfallsicherheit kann durch den Einsatz einer Mehr-Kanal-Mehr-Betreiber-Lösung, erreicht werden.

Eine Integration von Sicherheitskomponenten in digitalen Assistenten, z. B. für den Pflegedienst, kann erfolgreich über microSD Cards realisiert werden.

Prozess- als auch technologische Sicherheit kann im Gesundheitswesen auch dadurch gewährleistet werden, dass mit pseudonymisierten Patientenfallnummern gearbeitet wird.

Literaturverzeichnis

Berg, W., Telemedizin und Datenschutz, in: MedR 2004, S. 411-414

Katzenmeier, Chr. und Slavu, St. (2009): Rechtsfragen des Einsatzes der Telemedizin im Rettungsdienst, Rechtsgutachten Med-on-@ix, Institut für Medizinrecht, Universität zu Köln

Medizinproduktegesetz in der Fassung der Bekanntmachung vom 7. August 2002 (BGBl. I S. 3146), geändert durch Artikel 6 des Gesetzes vom 29. Juli 2009 (BGBl. I S. 2326)

Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte Amtsblatt Nr. L 169 vom 12/07/1993 S. 0001 – 0043

Ansprechpartner:

Wolfgang Neifer (für VitaBIT)
WIBU-Systems AG
Rüppurrer Str. 52-54
76137 Karlsruhe
Tel.: 0721 93172 53
E-Mail: wolfgang.neifer@wibu.de

Tadeusz Brodziak (für Med-on@ix)
P3 Communications
Dennewartstr. 25-27
52068 Aachen
Tel.: 0241 9437 324
E-Mail: tadeusz.brodziak@p3-group.com

Matthias Müller (für Med-on@ix)
ZLW/IMA der RWTH Aachen
Dennewartstr. 27
52068 Aachen
Tel.: 0241 80911 34
E-Mail: mueller@zlw-ima.rwth-aachen.de

Ulli Münch (für OPAL)
Geschäftsfeld Technologien
Zentrum für Intelligente Objekte ZIO
Fraunhofer-Arbeitsgruppe für
Supply Chain Services SCS
Dr.-Mack-Straße 81
90762 Fürth
Tel.: 0911 58061-9549
E-Mail: ulli.muench@scs.fraunhofer.de

Fritz Meier (für OPAL)
Geschäftsfeld Technologien
Zentrum für Intelligente Objekte ZIO
Fraunhofer-Arbeitsgruppe für
Supply Chain Services SCS
Dr.-Mack-Straße 81
90762 Fürth
Tel.: 0911 58061-9550
E-Mail: fritz.meier@scs.fraunhofer.de

Glossar

3DES	Triple Data Encryption Standard	dreifache Anwendung eines überholten symmetrischen Kryptosystems mit je 56 Bit Schlüssellänge (effektiv 112 Bit)
A5/1		Stromchiffre (bitweise Addition eines Klartextes zum Schlüsselstrom) mit effektiver Schlüssellänge von 54 Bit (Anwendungsbereich: GSM)
AES	Advanced Encryption Standard	zeitgerechtes, symmetrisches Kryptosystem mit 128, 192 oder 256 Bit Schlüssellänge (Nachfolger des 3DES)
agroXML		auf XML basierende Datenaustauschsprache für den Agrarsektor
Aktiver Angriff		Unmittelbares Einschalten eines Dritten in computergestützte Kommunikation zwischen Sender und Empfänger beim Versuch an Informationen zu gelangen, für die man nicht befugt ist. Neben Vertraulichkeit der Daten wird auch deren Integrität und Verfügbarkeit bedroht.
Basel II		Eigenkapitalvorschriften für Kreditinstitute in der EU (Basis: EU-Richtlinien 2006/48/EG und 2006/49/EG), Name geht auf Basler Ausschuss für Bankenaufsicht zurück
DB	Datenbank	
BDSG	Bundesdatenschutzgesetz	regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten
BI	Betriebsinventur	spezieller Use-Case von Mobility@forest. Weitere Use-Cases: Forschungseinrichtung und Beratung
BPEL	Business Process Execution Language	XML-basierte Sprache zur Beschreibung von Geschäftsprozessen, deren einzelne Aktivitäten durch Webservices implementiert sind
CA	Certification Authority (Zertifizierungsstelle)	Einrichtung (z. B. Behörde oder Organisation), die digitale Zertifikate ausstellen und überprüfen kann
CAD	Computer Aided Design	Erstellen von Konstruktionsunterlagen für mechanische, elektrische oder elektronische Erzeugnisse mit Hilfe von spezieller Software
CAM	Computer Aided Manufactoring	direkte Steuerung von Produktionsanlagen sowie der unterstützenden Transport- und Lagersysteme durch Computer
CAN-Bus	Controller Area Network-Bus	asynchrones, serielles Bussystem, gehört zu echtzeitfähigen Feldbussen
CRL	Certificate Revocation List (Sperrliste)	Liste mit gesperrten Public-Key-Zertifikaten (beispielsweise weil ein zum Zertifikat gehöriger privater Schlüssel gestohlen wurde)
CRM	Customer Relation Management	Programm, das Kundenbeziehungen verwaltet und Korrespondenzen dokumentiert

DoS	Denial of Service	Ausfall eines Netzwerkdienstes infolge eines Überlastungs-Angriffs
EDGE	Enhanced Data Rates for GSM Evolution	Technik zur Erhöhung der Datenrate in GSM-Funknetzen
EKG	Elektrokardiogramm (Herzspannungskurve)	Summe der elektrischen Aktivitäten der Herzmuskelfasern
ERP	Enterprise Resource Planning	System für effizienten Einsatz vorhandener Ressourcen im Unternehmen (Kapital, Betriebsmittel, Personal)
FIPS 140-2	Federal Information Processing Standard 140-2	Sicherheitsanforderungen für kryptographische Module nach US-Standard
FMEA	Failure Mode and Effects Analysis	analytische Methoden der Zuverlässigkeitstechnik, um potentielle Schwachstellen in neuen Produkten oder Prozessen bereits in der Design- bzw. Entwicklungsphase zu finden
FMS	Farm-Management Software	Software zur strategischen Planung und ökonomischen Optimierung von landwirtschaftlichen Unternehmen
FoGIS/FOKUS	Forstwirtschaftliches Geoinformationssystem / Forstwirtschaftliches Datenverarbeitungssystem	
GPRS	General Packet Radio Service	paketorientierter Dienst zur Datenübertragung in GSM- und UMTS-Netzen
GPS	Global Positioning System	globales Navigationssatellitensystem zur Positionierung und Zeitmessung, weltweit wichtigstes Ortungsverfahren
GSM	Global System for Mobile Communications	gopulärster Standard für volldigitale Mobilfunknetze
HSPA	Highspeed Packet Access	Kombination der Mobilfunknetz-Protokolle HSDPA (Downlink) und HSUPA (Uplink); ein Datenübertragungsverfahren des UMTS, ermöglicht DSL-ähnliche Übertragungsraten
IP54		Schutzart von elektronischen Geräten, die die Tauglichkeit für bestimmte Umgebungsbedingungen angibt
ISO 27001	International Organization for Standardization/ Internationale Organisation für Normung 27001	Spezifikation für die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems
ISO/IEC19790 (FIPS 140-2)	International Organization for Standardization/ Internationale Organisation für Normung	spezifiziert die Sicherheitsanforderungen für Kryptographische Module

ISO/OSI-Modell	OSI-Schichtenmodell	Modell als Designgrundlage für Kommunikationsprotokolle, bestehend aus sieben aufeinander aufbauenden Schichten, welche getrennt voneinander betrachtet werden können. Z. B.: Anwendungsschicht, Transportschicht, physikalische Schicht
ISO-XML	International Organization for Standardization - Extensible Markup Language	XML-basierte Sprache, entwickelt zur Standardisierung des Datenaustausches auf Maschinenebene und von Maschinen zu Bürosoftware
KIS	Klinikinformationssystem	einheitliche Plattform für Telekommunikation und EDV-Anwendungen für alle Klinikprozesse
KMU	Kleine und mittlere Unternehmen	laut definierten Grenzen hinsichtlich Beschäftigtenzahl, Umsatzerlös oder Bilanzsumme
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (in Deutschland in Kraft seit 1. Mai 1998)
LDSG	Landesdatenschutzgesetz	
MD5	Message-Digest Algorithm 5	weit verbreitete kryptographische Hashfunktion, erzeugt 128 Bit Hashwert aus beliebigen Nachrichten
MDE	Mobile Datenerfassung	Konzept zur Datenerfassung im mobilen Einsatz elektronischer Hilfsmittel ohne PC-Arbeitsplatz
MedR	Schriftenreihe Medizinrecht	
MPG	Medizinproduktegesetz	Gesetz zur Einrichtung eines Meldesystems, das der Erfassung und Abwehr von Risiken aus Medizinprodukten dient
OGC	Open Geospatial Consortium	gemeinnützige Organisation mit dem Ziel, die Entwicklung raumbezogener Informationsverarbeitung auf allgemeine Standards festzulegen
Passiver Angriff		siehe *Aktiver Angriff*. Beim passiven Angriff ist jedoch nur die Vertraulichkeit bedroht, denn die Daten bleiben unverändert.
PDA	Personal Digital Assistant	kompakter, tragbarer Computer; Rechenleistung ist für Termin- und Aufgabenverwaltung ausgelegt
PIM	Product Information Management	Produktkatalog; wird durch ein Softwareprogramm angezeigt und verwaltet
PKI	Public Key Infrastructure	Gesamtheit aller notwendigen Komponenten (Hardware, Software, Personen, Policy, Maßnahmen), um digitale Zertifikate auszustellen, zu überprüfen und zu verwalten
PLM	Product Lifecycle Management	Strategisches Konzept zum Management eines Produktes über dessen gesamten Lebenszyklus
RBAC	Role Based Access Protocol	Rollenbasiertes Verfahren zur Zugriffssteuerung und –kontrolle auf Dateien und Dienste in Mehrbenutzersystemen

RSA	Rivest Shamir Adleman	asymmetrisches Kryptosystem zur Verschlüsselung und zur digitalen Signatur (entwickelt von Ronald L. Rivest, Adi Shamir und Leonard Adleman)
SAML	Security Assertion Markup Language	XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen
SD-Card	Secure Digital Card	Digitales Speichermedium bis 4 GB, arbeitet nach dem Prinzip der Flash-Speicherung
SHA	Secure Hash Algorithm	Gruppe von standardisierten kryptographischen Hashfunktionen, die zur Berechnung eines einzigartigen Hashwerts elektronischer Daten dienen
SOA	Service-Orientated Architecture	Architekturmuster, um Dienste von IT-Systemen, deren Komplexität hinter standardisierten Schnittstellen verborgen bleibt, zu strukturieren und zu nutzen
SOAP	Simple Object Access Protocol	ein Netzwerkprotokoll zum Austausch XML-basierter Nachrichten (Verwendung bei Web Services)
SOX	Sarbanes-Oxley Act of 2002	US-Bundesgesetz zur Verbesserung der Verlässlichkeit von Unternehmensbilanzierung
SSD	Solid State Drive	Speichermedium ohne beweglichte Teile (deutlich teurer und geringere Kapazitäten als bei magnetischen Festplatten)
SSL	Secure Socket Layer	Netzwerkprotokoll mit Authentifizierungsmöglichkeit zur sicheren Datenübertragung im Computernetzen (Vorgänger von TLS
STS	Secure Token Service	sind sämtliche Ausgangsbedingungen erfüllt, erstellt der STS-Dienst kryptografisch abgesicherte Token
TCP/IP	Transmission Control Protocol / Internet Protocol	Familie von wichtigsten Netzwerkprotokollen
TLS	Transport Layer Security	Netzwerkprotokoll zur sicheren Datenübertragung in Computernetzen (Nachfolger von SSL)
UDDI	Universal Description, Discovery and Integration	standardisierter, XMLbasierter Verzeichnisdienst zur Veröffentlichung und Findung von Webdiensten
UMTS	Universal Mobile Telecommunications System	Mobilfunkstandard mit deutlich höheren Übertragungsraten als bei dem Vorgänger GSM
URL	Uniform Resource Locator	identifiziert und lokalisiert eine Ressource über das verwendete Netzwerkprotokoll
VPN	Virtual Private Network	Schnittstelle in einem Netzwerk, die es ermöglicht, Endgeräte an ein anderes, darauf aufbauendes Netz zu binden, welches für das darunter liegende Netz unsichtbar sein kann
WiMAX	Worldwide Interoperability for Microwave Access	Synonym für Funksysteme für ortsfeste und mobile Geräte nach dem IEEE-Standard 802.16

WLAN	Wireless Local Area Network	lokales Funknetz, oft als Synonym für den IEEE-802.11 Standard für verschiedene Wireless-Geräte verwendet
WPA	WiFi Protected Asset	Verschlüsselungsart für Drahtlosnetzwerke, entwickelt von Wi-Fi Alliance nach Architektur von WEP, bringt jedoch zusätzlichen Schutz
WSDL	Web Services Description Language	XML-basierte Beschreibungssprache für Webdienste ; beinhaltet u.a. Informationen zu angebotenen Funktionen mit deren Parametern und Rückgabewerten
WS-Security	Webservices-Security	Kommunikationsprotokoll (als Erweiterung zu SOAP), das Sicherheitsaspekte bei Webdiensten berücksichtigt
XML	Extensible Markup Language	Auszeichnungssprache zur Darstellung hierarchisch strukturierter Datensätze in Form von Textdaten (ermöglicht Interoperabilität bei Datenaustausch zwischen unterschiedlichen Computersystemen)

SimoBIT-Förderprojekte im Überblick

Kompetenznetzwerk Gesundheitswirtschaft

- **Med-on-@ix** - E-Health in der Notfallmedizin (www.medonaix.de)
- **VitaBIT -** Offene Plattform für sichere Anwendung mobiler Informationsdienste in der Pflegelogistik **(**www.vitabit.org**)**
- **OPAL Health** - Optimierte und sichere Prozesse durch mobile und intelligente Überwachung und Lokalisierung von Betriebsmitteln und Inventar in Kliniken und Krankenhäusern (www.opal-health.de)

Kompetenznetzwerk Maschinenbau

- **Mobile Servicewelten** im Internationalen Service des Maschinen- und Anlagenbaus (www.infoman.de)
- **SiWear** - Sichere Wearable-Systeme zur Kommissionierung industrieller Güter sowie für Diagnose, Wartung und Reparatur (www.siwear.de)
- **R2B** - Robot to Business, Informationstechnische Integration teilautonomer Prozesse und mobiler Maschinen in Geschäfts- und Dienstleistungsmodellen (www.agrardienstleistungen.de/r2b/)

Kompetenznetzwerk Öffentliche Verwaltung

- **Mobis Pro** - Mobiles Informationssystem zur Prozessoptimierung in Feuerwehren und öffentlichen Verwaltungen (www.mobis-pro.de)
- **simoKIM** - Sicheres und mobiles kommunales Infrastruktur-Management (www.simokim.de)
- **Mobility@forest** - Entwicklung einer neuartigen nutzerorientierten IT-Infrastruktur eines mobilen Arbeitsplatzes für den Forstbetrieb (www.mobility-forest.de)

Kompetenznetzwerk Handwerk und kleine Unternehmen

- **MAREMBA** - Mobile Assistenz für das Ressourcenmanagement in der Bau-Auftragsabwicklung (www.maremba.de)
- **ModiFrame** - Ein Framework für mobile Dienste (www.modiframe.de)
- **M3V** - Mobile Multimediale Multilieferanten-Vertriebsinformationssysteme (www.m3v-projekt.de)

Mitglieder des SimoBIT-Arbeitsforums IT-Sicherheit

Projektverbund	Unternehmen/ Institut	Name
Leitung des Arbeitsforums	Utimaco Safeware AG	Martin Oczko
SimoBIT-Begleitforschung	WIK-Consult	Dr. Franz Büllingen
		Annette Hillebrand
Maremba	Fraunhofer-Institut für Arbeits-wirtschaft und Organisation (IAO)	Jochen Günther
Mobility@forest	ATB – Institut für angewandte Systemtechnik Bremen GmbH	Stefan Faltus
Mobis Pro	TU Dortmund, Lehrstuhl für Kommunikationsnetze	Thang Tran
R2B	Siemens AG, C-LAB	Dr. Christoph Loeser*
		Gudrun Tschirner-Vinke
OPAL Health	Fraunhofer SCS (Supply Chain Services)	Fritz Meier
		Ulli Münch
SiWear	Hochschule Bremen, Institut für Informatik und Automation	Günther Diederich
Med-on@ix	ZLW/IMA RWTH Aachen	Matthias Müller
	P3 Communications GmbH	Tadeusz Brodziak
simoKIM	Utimaco Safeware AG	Andreas Philipp
		Martin Oczko
M3V	fun communications GmbH	Ralf Kunoth
ModiFrame	AIFB - Karlsruher Institut für Technologie	Michael Decker
VitaBIT	WIBU-SYSTEMS AG	Wolfgang Neifer

* abgelöst von Gudrun Tschirner-Vinke

ISSN 2190-6467