SiWear – Sichere Wearable-Systeme: Verwendung von Sicherheitsstandards im Entwurf von Wearable-Systemen am Beispiel der Benutzungsschnittstelle

Günther Diederich(+), Richard Sethmann(+), Silke Schäfer(*), Zied Ghrairi (+)

Institut für Informatik und Automation(+) / Technologie-Zentrum Informatik(*)
Mobile Research Center
Am Fallturm 1
28359 Bremen
Guenther.Diederich@hs-bremen.de
sethmann@hs-bremen.de
schaefer@tzi.de
Zied.Ghrairi@hs-bremen.de

Abstract: IT-Sicherheit und Benutzbarkeit stehen häufig im Konflikt zueinander. Dies ist verbunden mit der weitgehenden Berücksichtigung von Aspekten der Benutzbarkeit bei gleichzeitig geringer Berücksichtigung der IT-Sicherheit in den Methoden zur Anforderungsanalyse. Im Projekt SiWear[1] werden aus Einsatzszenarien die Sicherheitsanforderungen an Wearable-Systeme mit Hilfe des Sicherheitsstandards IT-Grundschutz abgeleitet. Dies ermöglicht eine frühzeitige Koordination von Anforderungen an die IT-Sicherheit sowie an die Benutzbarkeit und fördert somit die Vereinbarkeit von beiden.

1 Einleitung und Innovation

Managementanforderungen berücksichtigen zunehmend auch die IT-Sicherheit (z.B. SoX, KonTraG, Basel II), dementsprechend 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.

Derzeitige Methoden zur Anforderungsanalyse adressieren IT-Sicherheitsanforderungen nicht oder nur unzureichend (siehe [Me08]). Durch Modellierung eines Informationssicherheitsmanagementsystems (ISMS) für die Einsatzszenarien, die dem Entwurf zugrunde liegen, können Sicherheitsanforderungen aus dem ISMS in den Entwurf eingebracht und die sicherheitstechnische Entwicklung im Bereich IT-Sicherheit und Benutzbarkeit gefördert werden.

[1] Das Projekt SiWear (www.siwear.de) wird gefördert durch das Bundesministerium für Wirtschaft und Technologie (BMWi) im Förderschwerpunkt SimoBIT.

2 IT-Grundschutz im Entwurf von Wearable-Systemen

Im Projekt SiWear werden Wearable-Systeme zum Einsatz in Kommissionierung und Service in der Automobilbranche entwickelt. Entsprechend des jeweils in der aktuellen Abfolge geplanten Montageauftrags, werden die zugehörigen Bauteile anhand des jeweiligen Kommissionierauftrages auf Schubwägen zusammengestellt. Dabei durchläuft der Werker mit einem Kommissionierwagen und einem ausgedruckten Auftrag die Regalgänge eines Zwischenlagers (*Supermarkt)*. Nach vollständiger Abarbeitung des Kommissionierauftrags werden die zugehörigen Bauteile zur Übergabestelle gebracht.

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. Produktzertifizierungen z.B. nach Common Criteria (CC) oder ISO/IEC 19790 (FIPS 140-2) eignen sich aufgrund ihrer Produktorientierung nicht für eine entwicklungsbegleitende Sicherheitsbetrachtung. Prozessorientierte Sicherheits-standards, die auf Einsatzszenarien angewendet werden können, sind hier besser geeignet, z.B. ISO 27001 auf der Basis von IT-Grundschutz ([Bs07],[Bs08]).

2.1 Verwendung von IT-Grundschutz im Entwurf

Ein Wearable-System ist ein IT-System, dessen integraler Bestandteil Wearable Computer (siehe [Ma98], [Rü06]) sind, die mit anderen Wearable-Computer, mobilen oder stationären IT-Systemen interagieren. Wearable-Systeme werden als Assistenz-Systeme eingesetzt. Auf der Basis eingegebener und erfasster Informationen treffen sie, als Akteure im Prozess, ohne weitere Nutzerinteraktion prozessrelevante Entscheidungen. Dementsprechend ist ihrer Sicherheit ein hoher Stellenwert beizumessen.

Systemsicherheit ist aufgrund der derzeit verfügbaren Methoden zur Anforderungsanalyse nicht systeminhärent, dies hat zur Folge, dass der sichere Einsatz von IT-Systemen aufgrund unzureichender oder fehlender Sicherheitsfunktionen erheblich erschwert wird (siehe Abbildung 1). Schäden durch Systemausfälle oder Verletzung der Privatsphäre vermindern die Akzeptanz von IT-Systemen (siehe [Ma08], [Ro08]). Daher ist es erforderlich, Anforderungen an die IT-Sicherheit parallel zu Anforderungen an die Benutzbarkeit im Entwurf zu berücksichtigen. In SiWear werden, unter Verwendung des IT-Grundschutz, allgemeine Anforderungen an den sicheren Betrieb von IT-Systemen in der designierten Einsatzumgebung des zu entwickelnden Systems ermittelt. Zusätzlich zu den bisherigen Ergebnissen der Anforderungsanalyse sind hierdurch frühzeitig Anforderungen zur IT-Sicherheit verfügbar und können bereits vom ersten Entwurf an in allen folgenden Entwurfszyklen berücksichtigt werden.

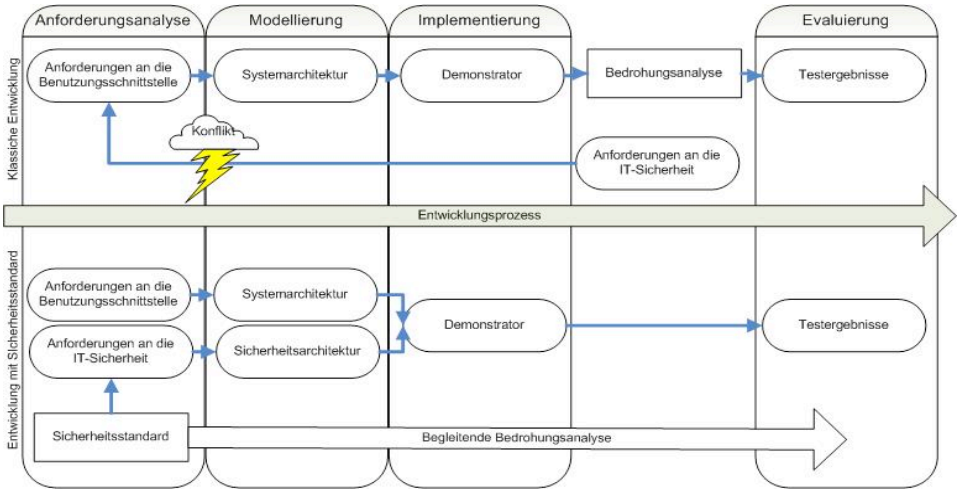

Abb. 1: Klassische Entwicklung im Vergleich zur Entwicklung mit IT-Sicherheitsstandard

2.2 Bausteine für Gefährdungen von Wearable-Systemen

Im Kommissionierungs-Szenario stellt der Einsatz eines WLAN eine mögliche Verbindung der Wearable-Computer untereinander sowie des Wearable-Systems mit der IT-Infrastruktur der Einsatzumgebung dar. 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 hier bei 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).

Ferner 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.

2.3 Sicherheitsanforderungen an die Benutzungsschnittstelle

Nachfolgend werden einige Gefährdungen aus dem Baustein „WLAN“ aufgegriffen und entsprechende Anforderungen an die Benutzungsschnittstelle formuliert.

Ausfall oder Störung eines Funknetzes

Die Benutzungsschnittstelle muss über den Ausfall oder Störung des Funknetzes informieren. Art und Weise der Information müssen geeignet sein, die Aufmerksamkeit spätestens bei der nächsten Interaktion mit der Benutzungsschnittstelle auf den Ausfall oder die Störung zu lenken.

Unzuverlässige oder fehlende WLAN-Sicherheitsmechanismen

Die Benutzungsschnittstelle muss zu jedem Zeitpunkt anzeigen, ob die WLAN-Kommunikation ungesichert oder gesichert erfolgt. Wenn WLAN-Sicherheitsmechanismen verwendet werden, müssen Informationen über die verwendeten Mechanismen abgerufen werden können.

Ungeeignete Aufstellung von sicherheitsrelevanten IT-Systemen

Das Wearable-System verfügt über eine Funktion zur Lokalisierung, außerhalb des Supermarktes wird das Wearable-System für die Nutzung gesperrt. Die Benutzungsschnittstelle muss direkt nach einer Sperrung über die erfolgte Sperrung und den Grund der Sperrung informieren.

3 Fazit und Ausblick

In der Entwicklung neuer Produkte können Bedrohungsanalysen häufig erst nach Abschluss des Produktentwurfs durchgeführt werden. Dies hat zur Folge, dass Anforderungen an die IT-Sicherheit und Benutzbarkeit nicht gleichwertig berücksichtigt werden können und daher häufig in Konflikt geraten. Im Projekt SiWear werden mit Hilfe des Standards IT-Grundschutz frühzeitig Sicherheitsanforderungen ermittelt, die in der weiteren Entwicklung des Wearable-Systems, insbesondere hinsichtlich der Benutzbarkeit, berücksichtigt werden.

Auf dieser Basis können ergänzende Sicherheitsanalysen durchgeführt werden, die insbesondere im Bereich der Wearable-Systeme auf die Identifikation typischer und von bestimmten Einsatzszenarien unabhängiger Gefährdungen zielen und somit zur Weiterentwicklung des Standards beitragen können.

Literaturverzeichnis

[Bs07] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, BSI, Bonn, 2007.

[Bs08] Bundesamt für Sicherheit in der Informationstechnik: BSI Standard 100-1 – Managementsysteme für Informationssicherheit (ISMS), BSI, Bonn, 2008.

[Ma98] Mann, S.: Keynote Address for The First International Conference on Wearable Computing, ICWC-98, May 12-13, Fairfax VA

[Ma08] Mattern, F.: Allgegenwärtige Datenverarbeitung – Trends, Visionen, Auswirkungen. In Digitale Visionen (A.R., T.S., U.W. Hrsg.), Springer, Berlin Heidelberg, 2008

[Me08] Mellado D,;Fernández-Medina E.;Piattini, M.: Security Requirements Variability for Software Product Lines. ARES 2008: S.1413-1420

[Ro08] Roßnagel, A.: Selbst- oder Fremdbestimmung – Die Zukunft des Datenschutzes. In Digitale Visionen (A.R., T.S., U.W. Hrsg.), Springer, Berlin Heidelberg, 2008

[Rü06] Ruegge, I.: Einsatzpotenziale, Nutzungsprobleme und Lösungsansätze mobil tragbarer Informations und Kommunikationstechnologien, Dissertation, Universität Bremen, 2006