Zukunft der Softwaretechnik aus Sicht der IT-Sicherheit

Markus Ullmann
Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363, D-53133 Bonn
ullmann@bsi.de

1 Die Verlässlichkeit von IT-Systemen als softwaretechnisches Thema

Vor einigen Jahren noch als Spielwiese von Militärs und Geheimdiensten abgetan, wird nunmehr selbst zunehmend in der Öffentlichkeit das Thema IT-Sicherheit wahrgenommen. Denn durch das "Online-Fieber" sind immer breitere Kreise der Bevölkerung an das Internet angeschlossen und Gefährdungen, die durch das bedenkenlose Surfen und Herunterladen von Code entstehen können ausgesetzt. Über aktuelle Viren, Trojanische Pferde, etc. wird inzwischen nicht nur in den einschlägigen Fachkreisen sondern in den allgemeinen Print-, TV und Onlinemedien berichtet. Solange man nicht selbst merkt, dass man betroffen ist, wird man versucht sein, alle Sicherheitsgefährdungen herunterzuspielen, nach dem Motto: Es wird mich schon nicht treffen. Verfügbarkeitsangriffe auf Webseiten von Big Brother in Deutschland, ebay und Amazon in den USA oder massive Virenverbreitung über eine Schwachstelle im MS-Outlook-Adressbuch zeigen, dass es reale Verletzlichkeiten gibt. Sie machen die Notwendigkeit für den Einsatz von Sicherheitsmaßnahmen deutlich. Nun stellt sich aber das Problem: Wie kann man sich von der Verlässlichkeit dieser Maßnahmen überzeugen. Dies ist selbst für Fachleute schwierig, zumal es nicht möglich ist, ohne detaillierte technische Spezifikationen "in das Innere eines Produktes zu schauen".

Inzwischen existieren unter dem Namen 'Common Criteria' weltweit standardisierte Evaluierungskriterien, die die Prüfung von Sicherheitsprodukten zum Gegenstand haben. In diesen sind Anforderungen an die Art und den Detaillierungsgrad einer Evaluierung spezifiziert. Diese Anforderungen sind in unterschiedlichen Paketen definiert und reichen bis hin zur formalen Spezifikation und dem mathematischen Nachweis von Sicherheitseigenschaften.

Aber:

a) Diese Prüfungen werden nur auf Veranlassung des Herstellers von Produkten durchgeführt und sind je nach Prüftiefe mit großen zeitlichen und finanziellen Aufwänden verbunden. Daher sind sie eher die Ausnahme, weil der Markt die Mehraufwände nicht oder nur zum Teil honoriert und

b) es ist für den Anwender schwierig zu entscheiden, welche Sicherheitsfunktionalität und Verlässlichkeit einer Sicherheitslösung seinen Sicherheitsbedürfnissen Rechnung trägt.

Denkanstoß: Was können neue Verfahren der Softwaretechnik dazu beitragen, Aussagen zur Verlässlichkeit eines Produktes/Systems leichter abzuleiten bzw. abzuschätzen?

2 Zusammenwirken des Security- und Softwareengineerings bei der Systementwicklung

Zunehmend entstehen Anforderungen an informationstechnische Systeme, die nicht rein funktionaler Art sind und die im Hinblick auf ihre Bedeutung durchaus gleichgewichtig zu funktionalen Aspekten zu betrachten sind. Ein Beispiel hierfür sind Krankenhausinformationssysteme. Hier spielen neben funktionalen Anforderungen auch Sicherheitsanforderungen eine wichtige Rolle. Für die Systementwicklung bedeutet dies, dass über die gesamte Entwicklungsphase bis hin zur Installation, mindestens zwei Sichten auf das System existieren müssen. Eine funktionale - und eine Sicherheits - Sicht. In Anlehnung an das Wasserfallmodell gedacht, beginnen die Entwicklungsarbeiten mit der Erstellung der funktionalen Anforderungen und der Durchführung der Bedrohungsanalyse. Ist dies abgeschlossen, so besteht der nächste Schritt aus der Erstellung eines funktionalen Grobkonzeptes bzw. einer geeigneten Sicherheitspolitik (Security Policy), um den definierten Bedrohungen entgegenzuwirken. Spä-

testens an dieser Stelle wird auffallen, dass bestimmte "Sicherheits-Objekte" der Security-Policy "Daten-Objekte" aus der funktionalen Betrachtung sein können, bspw. die Datei, in der die Angestellten einer Klinik gespeichert sind. D.h., es existiert mindestens in Teilen eine starke Wechselwirkung zwischen diesen beiden "System-Sichten". Diese Wechselwirkungen und Abhängigkeiten müssen im Rahmen des Entwurfsprozesses angemessen berücksichtigt werden. Hierzu zählt insbesondere auch die Sicherheitsbetrachtung von Verfeinerungsprozessen. Gehen wir auf das Bsp. mit der Angestellten-Datei zurück. Auf der Ebene der Security-Policy reicht es vielleicht aus, von einem "Sicherheits-Objekt" zu reden. Im Rahmen des Designs des Systems kann es aber vielleicht sinnvoll sein, diese auszusplitten in abteilungsbezogene Angestelltendateien, die auch noch auf verteilten Rechnersystemen liegen. Nun finden wir die Situation vor, dass das ursprüngliche "Sicherheits-Objekt" nun in 'n' verteilte Sicherheitsobjekte verfeinert wurde, die wiederum spezifischen Bedrohungen unterliegen können. Derartige Probleme müssen angemessen berücksichtigt werden.

Denkanstoß: Wie sieht eine Entwicklungsmethodologie aus, die die Entwicklung funktionaler - und sicherheitstechnischer Anforderungen unter Berücksichtigung von Wechselwirkungen unterstützt?

3 Automatische Generierung spezieller Produktspezifikationen

Eine Möglichkeit, die Verlässlichkeit eines IT-Produktes zu prüfen, ist die Evaluierung nach standardisierten Kriterien, z.B. den Common Criteria. Hierdurch entstehen beim Hersteller große Aufwände dadurch, weil er eine Fülle von Spezifikationen über das zu prüfende Produkt zur Verfügung stellen muss, die bei ihm im Rahmen des "normalen" Entwurfsprozesses nicht entstanden sind. Alles was im weitesten Sinne mit der Wirksamkeit von Sicherheitsmaßnahmen zu tun hat, kann nur das Ergebnis eines vollständigen Security-Engineering-Prozesses sein. Aber Spezifikationen, die im wesentlichen für die Korrektheits-Untersuchung notwendig sind (Grob-Design, Design, Fein-Design, ...) müssten prinzipiell aus den Spezifikationen des Entwurfsprozesses beim Hersteller generierbar sein.

Denkanstoß: Welche Möglichkeiten sind hier denkbar?

4 Sonstiges

a) Zur Ausbildung an Universitäten und Fachhochschulen:

   Abgesehen von Kryptologen, ist es im wesentlichen so, dass nur wenige Absolventen die im Bereich der IT-Sicherheit eine Anstellung finden über IT-Sicherheits-Kenntnisse verfügen. D.h. es wäre wünschenswert, das Gebiet der IT-Sicherheit innerhalb der Ausbildung der Softwaretechnik angemessen zu berücksichtigen.

b) Zur Entwicklung getypter Softwaretechniken für einzelne Anwendungsbereiche:

   Wir denken, dass heute die Situation besteht, ständig mit neuen Problemstellungen konfrontiert zu werden. Daher glauben wir, dass eine gute Grundlagenausbildung und die Technik "effizient Neues zu lernen" zielbringender ist. Dies bedeutet aber nicht, dass die Hochschulen sich nicht entwickeln müssen. Ganz im Gegenteil: Anwendungsbezogene Lehrinhalte müssen ständig dem aktuellen Stand der Entwicklung angepasst werden.

c) Zu ISO900x und den diversen Prozeßverbesserungsprogrammen:

   Die Idee, die Entwicklungs- und Herstellungsprozesse besser zu verzahnen und zu optimieren, ist natürlich immer sinnvoll. Die Frage ist nur, aus welchen Beweggründen man sich eines Prozeßverbesserungsprogramms unterzieht. Gelegentlich entsteht der Eindruck, dass nicht der Inhalt eines Prozeßverbesserungsprogramms sondern das abschliessende Zertifikat im Vordergrund stehen. In diesem Fall verkommt die gute Idee zu einem reinen Marketinginstrument.