Vorwort

Informationstechnologie (IT) ist heute in nahezu allen Bereichen von zentraler Bedeutung: Gesundheit, Mobilität, Bildung, Unterhaltung, Produktion, Logistik, aber auch Handel, Finanzen, und öffentliche Verwaltung. IT ist eine Schlüsseltechnologie, die neue Anwendungen und auch neue Geschäftsmodelle ermöglicht. Durch die Einbettung von IT in Alltagsgegenstände und durch die zunehmende Dienste-Orientierung entsteht das Internet der Dinge (IoT) und der Dienste. Der IT-Sicherheit kommt bei dieser Entwicklung eine Schlüsselrolle zu.

Lösungen der IT-Sicherheit haben zum einen eine Wegbereiter-Funktion, da neue Anwendungen häufig nur eingesetzt und akzeptiert werden, wenn die Sicherheit der Daten gewährleistet wird. Zum anderen hat die IT-Sicherheit natürlich die bekannte Schutzfunktion. Gezielt und korrekt eingesetzte Maßnahmen der IT-Sicherheit reduzieren die Risiken wirtschaftlicher Schäden, die zum Beispiel durch eine unautorisierte Weitergabe von Daten oder durch kriminelle Aktivitäten wie Wirtschaftsspionage entstehen können. Maßnahmen der IT-Sicherheit sind aber auch notwendig, um vor Schäden an Leib und Leben zu schützen, die zum Beispiel durch manipulierte Gesundheitsdaten oder durch manipulierte Fahrzeugsensorik entstehen können.

Das vorliegende Buch hat zum Ziel, fundierte Kenntnisse über wirksame Maßnahmen zu vermitteln, die zur Erhöhung der Sicherheit heutiger Systeme beitragen können. Die Qualität eines sicheren IT-Systems hängt wesentlich davon ab, dass seine Konstruktion methodisch und systematisch erfolgt. Das Buch führt die hierfür notwendigen Techniken und Vorgehensweisen ein, wie Bedrohungsanalyse, Modellierung und Bewertung. Die zur Umsetzung der Sicherheitsanforderungen benötigten Mechanismen, Verfahren und Protokolle werden eingehend erklärt sowie anhand von Fallbeispielen erläutert. Ziel ist es, die Ursachen für Problembereiche heutiger IT-Systeme zu verdeutlichen und die grundlegenden Sicherheitskonzepte mit ihren jeweiligen Vor- und Nachteilen vorzustellen. Der Leser soll ein Verständnis für die vielschichtigen Probleme sicherer Systeme erlangen sowie ein breites und grundlegendes Wissen zu deren Behebung erwerben.

Das Buch beschäftigt sich mit Fragestellungen der Sicherheit technischer Systeme im Sinne des englischen Begriffs Security. Zur Gewährleistung

https://doi.org/10.1515/9783110985115-201

von Security-Eigenschaften setzt man Konzepte und Maßnahmen ein, um Bedrohungen abzuwehren, die im Wesentlichen durch absichtliche oder unabsichtliche Angriffe von außen auf das IT-System entstehen. Sicherheitsaspekte, die organisatorische Fragen betreffen, und solche, die durch den Begriff Safety charakterisiert werden, liegen außerhalb des behandelten Themenrahmens. Safety beschreibt die Funktionssicherheit eines Systems. Zu deren Gewährleistung benötigt man Konzepte und Verfahren, um solche Bedrohungen abzuwehren, die im Wesentlichen durch das Fehlverhalten des IT-Systems selber entstehen. Es handelt sich hierbei um Fragestellungen der Fehlervermeidung und Fehlertoleranz sowie der Steigerung der Zuverlässigkeit und Verfügbarkeit von IT-Systemen.

Seit einigen Jahren wird zunehmend der Begriff Cybersicherheit verwendet. Im vorliegenden Buch verstehen wir unter der Cybersicherheit die Ausweitung der klassischen IT-Sicherheit auf den gesamten Cyberraum. Dieser Raum umfasst die Gesamtheit der IT-Infrastrukturen in Unternehmen, Behörden oder auch in verschiedensten Anwendungsbereichen, wie in Produktionsanlagen, in Energienetzen oder im Gesundheitswesen, die über das Internet oder vergleichbare Vernetzungstechnologien zugreifbar sind. Im Cyberraum sind IT-basierte Systeme mit physischen Systemen verbunden. Moderne Fahrzeuge sind ein prägnantes Beispiel dafür, da im Fahrzeug, aber auch im Umfeld des Fahrzeugs, eine Vielzahl an IT-basierten Komponenten eingesetzt wird, um beispielsweise Fahrzeugdaten zu erfassen, auszuwerten und mit Informationen aus der Fahrzeugumgebung zu verknüpfen. Maßnahmen zur Erhöhung der IT-Sicherheit sind somit auch Maßnahmen zur Verbesserung der Sicherheit im Cyberraum, also zur Erhöhung der Cybersicherheit.

Das Buch richtet sich an Studierende der Informatik, Mathematik und Elektrotechnik sowie an interessierte Leser mit Informatik-Hintergrundwissen, die grundlegende Kenntnisse auf dem Gebiet der IT-Sicherheit erwerben bzw. bereits vorhandene Kenntnisse vertiefen wollen. Das Buch ist für die eigenständige Beschäftigung mit dem Stoff geeignet.

Vorwort zur 11. Auflage

Seit der zehnten Auflage des vorliegenden Buches hat die Bedeutung der Cybersicherheit durch das Fortschreiten der digitalen Transformation insbesondere im Zuge der Covid-19 Pandemie und durch technologische Entwicklungen noch weiter massiv zugenommen. Es ist deshalb unabdingbar, ein Lehrbuch zum Thema IT- bzw. Cybersicherheit kontinuierlich zu aktualisieren und um neue Entwicklungen zu ergänzen. Die 11. Auflage enthält neben einer Vielzahl von Aktualisierungen sowohl kleinere als auch etwas umfangreichere Erweiterungen. Zu den kleineren Ergänzungen zählen zum Beispiel Erläuterungen zu Post Quantum Kryptografie, zum SHA3-Algorithmus, oder auch zum Thema Zero Trust. Zu den umfangreicheren

Erweiterungen gehören der Messenger-Dienst Telegram, da dieser in den letzten Jahren erheblich an Bedeutung gewonnen hat, aber auch TLS 1.3 sowie WPA3. Bei diesen handelt es sich um verbesserte Protokolle zur sicheren Internetkommunikation bzw. zur Absicherung von WLAN-Verbindungen. Da das ACME Protokoll und die Let's encrypt Zertifizierungsstelle für den Bereich Web-Sicherheit eine wachsende Bedeutung erlangen, geht die 11. Auflage auch auf diese Entwicklungen ein. Mit OAuth2.0 und Shibboleth greifen wir schließlich auch noch zwei Standardprotokolle auf, die in heutigen Web- und Cloud-basierten Systemen zur Authentisierung und Autorisierung von Nutzern sehr weit verbreitet sind.

Um den Umfang des Buches durch die zusätzlich aufgenommenen Aspekte nicht zu stark vergrößern, wurden im Gegenzug viele kleinere Bereinigungen vorgenommen und einige Abschnitte gekürzt bzw. überholte Abschnitte gestrichen. So wurden die Beschreibungen des UMTS- und GPRS-Mobilfunkstandards so gekürzt, dass nur noch die für das Verständnis der Nachfolgestandards erforderlichen Konzepte eingeführt werden. Auch wurde die Fallstudie zum Network File System (NFS) entfernt und die Beschreibung des sehr alten, aber immer noch weit verbreiteten DES Verschlüsselungsstandards wurde erheblich gekürzt.

Bedanken möchte ich mich ganz herzlich bei allen Lesern, die mir Hinweise auf Fehler und Unklarheiten zukommen ließen, sowie bei dem DeGruyter-Verlag für die Unterstützung.

Für Hinweise auf Fehler und für Verbesserungsvorschläge bin ich jederzeit dankbar. Bitte senden Sie diese an claudia.eckert@aisec.fraunhofer.de.

München, im November 2022
Claudia Eckert