Kai Rannenberg

Zertifizierung mehrseitiger IT-Sicherheit

Kriterien und organisatorische Rahmenbedingungen

Die Deutsche Bibliothek – CIP-Einheitsaufnahme

Rannenberg, Kai:
Zertifizierung mehrseitiger IT-Sicherheit: Kriterien und organisatorische Rahmenbedingungen / Kai Rannenberg. –
Braunschweig; Wiesbaden: Vieweg, 1998
(DuD-Fachbeiträge)
ISBN 978-3-528-05666-7 ISBN 978-3-322-90281-8 (eBook)
DOI 10.1007/978-3-322-90281-8

Ursprünglich erschienen bei Friedr. Vieweg & Sohn Verlagsgesellschaft mbH,
Braunschweig/Wiesbaden 1998

Der Verlag Vieweg ist ein Unternehmen der Bertelsmann Fachinformation GmbH.

http://www.vieweg.de

Gesamtherstellung: Lengericher Handelsdruckerei, Lengerich

ISBN 978-3-528-05666-7

Inhaltsübersicht

Was wäre die Ewigkeit ohne
die Erfindung der Uhr?

Stanislaw Jerzy Lec

Vorwort

Telekommunikation wird nicht nur immer wichtiger für Arbeitswelt und Privatleben, sie basiert auch in zunehmendem Maße auf Informationstechnik (IT). Der Austausch von Bestell-, Produktions- und Konstruktionsdaten zwischen Unternehmen ist ein Beispiel dafür, ebenso die Internet-Recherche von Privatpersonen. Selbst der schon „klassisch" anmutende Telefonanruf „von Mensch zu Mensch" wird durch Rechner technisch gestützt und vermittelt. Die Gesellschaft ist, wie auf begeh- und befahrbare Straßen, auf eine funktionsfähige Telekommunikationsinfrastruktur angewiesen, und niemand kann sich ihr wirklich entziehen.

Damit ergeben sich Anforderungen an die Sicherheit dieser Telekommunikation und der ihr zugrundeliegenden Informationstechnik, die sich unter dem Begriff „Mehrseitige Sicherheit" zusammenfassen lassen. Mehrseitige Sicherheit bedeutet, daß nicht nur die Sicherheit einer der an der Kommunikation beteiligten Parteien berücksichtigt wird. Dies gilt für Diensteanbieter, Netzbetreiber, aber auch für Teilnehmer oder Nutzer. Wichtig sind insbesondere der Schutz und die Stärkung der Teilnehmer und Nutzer, damit ernsthafte – etwa kommerzielle – Anwendungen überhaupt realisierbar sind. Wer einerseits keine Kontrolle über seine via Homebanking verwalteten Finanzen oder seine elektronische Unterschrift hat und andererseits fürchten muß, daß sein Einkaufs- oder Telefonverhalten von anderen kontrolliert und ausgewertet werden kann, wird kein Vertrauen in die Technik fassen, sondern sich bei ihrer Nutzung und der damit verknüpften Übernahme von Verantwortung und Preisgabe persönlicher Informationen eher zurückhalten. Dies gilt erst recht, da elektronisch erfaßte Information als immaterielles Gut mindestens eine besondere Eigenschaft hat: Sie läßt sich zwar vergleichsweise leicht sammeln, nutzen und vervielfältigen, jedoch kann kaum eine Garantie für ihre Vernichtung oder Löschung gegeben werden, insbesondere nicht angesichts weltweiter Computernetze.

Wichtig für Vertrauen ist nicht nur, daß mehrseitige Sicherheit technisch unterstützt wird, sondern auch, daß sie als Eigenschaft der jeweiligen Kommunikations- oder Informationstechnik *erkennbar* ist. Diese Anforderung kollidiert mit der Komplexität heutiger Hardware- und Softwarekomponenten und erst recht der Komplexität zusammengesetzter Systeme, deren Sicherheitseigenschaften nicht durch einfache „Draufschau", sondern nur durch sorgfältige Prüfung zu ermitteln sind.

Ein seit den 70er Jahren beschrittener Weg, begründetes Vertrauen in Informationstechnik zu schaffen, ist die Evaluation und Zertifizierung der entsprechenden Produkte auf der Basis veröffentlichter Kriterien, sogenannter IT-Sicherheitsevaluationskriterien. Zertifikate mit Aussagen über

Sicherheitseigenschaften sollen Anwendern helfen, die angebotenen Produkte bezüglich ihrer Sicherheit zu beurteilen und auch untereinander zu vergleichen. Vergeben werden die Zertifikate von möglichst unabhängigen und fachkundigen Stellen. Als Voraussetzung muß das jeweilige Produkt eine Evaluation durch eine neutrale Instanz, im allgemeinen ein Prüflabor, erfolgreich bestehen. Entsprechende Zertifizierungssysteme existieren schon seit einiger Zeit in mehreren Staaten.

Grundlage der Evaluationen sind Kriterienkataloge wie die im Rahmen der Europäischen Gemeinschaft harmonisierten „Information Technology Security Evaluation Criteria" (ITSEC). Es ist absehbar, daß diese Kriterien erheblichen Einfluß auf die Entwicklung von IT-Systemen haben werden, da z.B. verschiedene Anwender der öffentlichen Hand Zertifikate zur Voraussetzung für die Zulassung von Produkten machen wollen. Anwenderorganisationen, wie etwa die Kassenärztliche Bundesvereinigung, haben dies bereits getan. Zusätzlich enthalten Gesetz und Verordnung zur digitalen Signatur eine entsprechende Vorschrift für wesentliche technische Komponenten, etwa zum Signieren und zum Schlüsselmanagement.

Die bisher gültigen Kriterienkataloge haben jedoch nach Ansicht vieler Kritiker erhebliche Schwächen und Lücken, gerade wenn es darum geht, im Hinblick auf mehrseitige Sicherheit zu evaluieren. Diese Schwächen wirken sich besonders bei der Anwendung auf rechnergestützte Kommunikationstechnik aus. Sie sind neben Problemen der weltweiten Harmonisierung ein Grund dafür, daß auch in der internationalen Normung (z.B. bei ISO/IEC) an Evaluationskriterien gearbeitet wird.

Ziele und Gliederung dieses Buches

In den fünf Teilen dieses Buches werden Evaluationskriterien, Zertifizierungssysteme und die relevanten Rahmenbedingungen im Hinblick auf die Anforderungen mehrseitiger Sicherheit untersucht und Verbesserungen vorgeschlagen. Drei Ziele werden dabei vorrangig verfolgt:

(1) Kriterien und Maßstäbe sollen mehrseitige Sicherheit als Qualitätsmerkmal erkennbar, prüfbar und zertifizierbar machen.

(2) Zertifizierung, Evaluation und die Information darüber sollen Anwendern und Nutzern eine realistische Möglichkeit geben, das für sie Relevante zu erfahren, den jeweiligen Zertifikaten in angemessenem Umfang zu vertrauen und um deren Grenzen zu wissen.

(3) Die Organisation der Zertifizierung und der Weiterentwicklung der Kriterien sollen auch auf neue oder heute noch unbekannte Anforderungen reagieren können.

Die zur Bearbeitung nötige Zusammenführung technischer und organisatorischer Argumente verlangt einen ständigen Spagat zwischen unterschiedlichen Gebieten. Einige Zusammenhänge zwischen Politik und technischer Entwicklung – oder Nichtentwicklung – ließen sich erst während jahrelanger Mitarbeit in der Normung ermitteln bzw. erfahren. Zudem ist Sicherheit mindestens innerhalb der Informationstechnik ein Querschnittsgebiet, was den Untersuchungsraum noch weiter aufspannt und die Lektüre nicht immer vereinfacht. Dies und die Tatsache, daß zum Thema „IT-

Sicherheitszertifizierung und -kriterien" Überblicksliteratur fehlt, machten eine recht umfangreiche Darstellung des Standes von Praxis und Entwicklung erforderlich. Deswegen führt **Teil A** zunächst allgemein in IT-Sicherheitszertifizierung und -kriterien sowie das Konzept „Mehrseitige IT-Sicherheit" ein.

In Kapitel 1 werden Zertifizierungsorganisationen und kurz die entsprechenden Kriterien vorgestellt, zum einen allgemein, zum anderen aus Sicht der beteiligten Parteien (Hersteller und Verkäufer, Anwender und Beschaffer, Evaluations- und Zertifizierungsstellen). Beschrieben wird auch das – nicht per se konfliktfreie – Verhältnis und Zusammenspiel dieser Instanzen. Der Schwerpunkt der Darstellung liegt auf der deutschen Zertifizierungslandschaft, jedoch werden auch die Zertifizierungssysteme anderer Staaten (etwa Großbritanniens und der USA) betrachtet, insbesondere wenn die Situation dort sich strukturell von der deutschen unterscheidet. Am Ende des Kapitels steht eine Übersicht der nationalen und internationalen Initiativen zur Erstellung und Harmonisierung von IT-Sicherheitskriterien, die gegenwärtig eng mit den jeweiligen Zertifizierungssystemen verknüpft sind. Traditionell spiegeln die Evaluationskriterien auch das Verständnis, das ihre Autoren von IT-Sicherheit haben, wider. Kapitel 2 beschreibt deshalb die Entwicklung im Verständnis von IT-Sicherheit und stellt „Mehrseitige IT-Sicherheit" früheren Ansätzen gegenüber.

In **Teil B** werden die wichtigsten bislang etablierten Kriterienkataloge vorgestellt und bewertet, um eine Einschätzung des Standes der Praxis, insbesondere bezüglich mehrseitiger IT-Sicherheit, zu geben. Im einzelnen werden in Kapitel 3 die US-amerikanischen „Trusted Computer System Evaluation Criteria" vorgestellt, in Kapitel 4 die europäischen ITSEC und ihre prägenden deutschen Vorläufer „IT-Sicherheitskriterien". Erfahrungen mit diesen Kriterien münden in eine zusammenfassende Bewertung der gegenwärtig etablierten Zertifizierungs- und Kriterienlandschaft (Kapitel 5) und speziell der ITSEC als der gegenwärtig in Europa gültigen Kriterien.

Die Schwächen der ITSEC sowie handelspolitische Motive veranlaßten die Entwicklung weiterer Kriterien bzw. Kriterienentwürfe. **Teil C** ist diesen „Post-ITSEC-Kriterien" und damit dem Stand der Entwicklung gewidmet. Beschrieben werden die jüngste Version der „Canadian Trusted Computer Product Evaluation Criteria" (Kapitel 6), die in der Normung bei ISO/IEC entstandenen Entwürfe (Kapitel 7) sowie die sogenannten „Common Criteria", die von Regierungsbehörden sechser Atlantikanrainerstaaten erstellt wurden (Kapitel 8). In Kapitel 9 werden diese Post-ITSEC-Kriterien der Kritik an ihren Vorgängern gegenübergestellt, um den Stand der Entwicklung zu dokumentieren.

Auch die Post-ITSEC-Kriterien weisen, gemessen an den Anforderungen mehrseitiger Sicherheit, noch erhebliche Schwächen auf. Deswegen werden in den Teilen D und E Verbesserungsvorschläge zu Kriterien und zur Zertifizierungsorganisation diskutiert.

Teil D enthält Konzepte für Kriterien mehrseitig sicherer IT-Systeme, speziell in Kapitel 10 eine neue Gliederung für Sicherheitsfunktionalität, die datensparsame Verfahren zum Nutzer- und Datenschutz berücksichtigt. Diese Gliederung wird als Beleg ihrer Tauglichkeit und ihres Verbesse-

rungspotentials auf das Beispiel einer ursprünglich an den ITSEC orientierten Funktionalitätsklasse für Telekommunikationsanlagen angewandt (Kapitel 11).

Auch neue und bessere Kriterien können jedoch allein aus sich heraus nicht alle Probleme der Zertifizierungs- und Kriterienlandschaft beseitigen. Dies gilt etwa für die vielfach als unzureichend angesehene Aussagekraft und Verwertbarkeit der Ergebnisse, für die als zu hoch beklagten Kosten sowie besonders für die als zu gering erachtete Effizienz des Evaluations- und Zertifizierungsprozesses. Um diese Probleme einer Lösung zumindest näher zu bringen, sind auch Verbesserungen der Organisation der Zertifizierung und ihrer Teilaufgaben sowie der Weiterentwicklung der fachlichen Grundlagen nötig. Vorschläge dafür enthält **Teil E**.

Zunächst werden in Kapitel 12 die Teilaufgaben der Organisation und die Anforderungen an die beteiligten Instanzen zusammengetragen und systematisiert. In den Kapiteln 13 bis 17 werden dann für jede Teilaufgabe die bestehenden Organisationsformen an den Anforderungen gemessen und mit Vorschlägen für neue Organisationsformen verglichen. Zertifizierung ist dabei Gegenstand des Kapitels 13, Evaluation des Kapitels 14. Kapitel 15 ist der Akkreditierung von Evaluationsstellen gewidmet, Kapitel 16 der Information und Beratung der Nicht-Insider. In Kapitel 17 werden Organisationsformen zur Weiterentwicklung von Evaluationskriterien und Methoden diskutiert.

Die auf den ersten Blick eher kriterienfernen Aufgaben wie Zertifizierung und Akkreditierung werden u.a. deswegen ausführlich berücksichtigt, weil die Aufgaben und die beteiligten Akteure oft so eng miteinander verflochten sind, daß die Verteilung von Kompetenz bei einer Aufgabe (etwa der Akkreditierung von Prüflabors) sich auf die Arbeiten an einer anderen Aufgabe (etwa der Weiterentwicklung der Kriterien) auswirken kann. Diese Verflechtungen und mögliche Konsequenzen daraus werden auf diese Weise mit dokumentiert und berücksichtigt.

Danksagung

Ein Text dieser Art und das zugrundeliegende Projekt waren nicht möglich ohne die Unterstützung vieler Beteiligter, auch wenn sie nicht alle namentlich erwähnt werden können. Grundlage dieses Buches ist meine Dissertation an der Albert-Ludwigs-Universität Freiburg, für die sich Prof. Dr. Günter Müller als Doktorvater und Erstgutachter zur Verfügung gestellt hat. Ihm gebührt Dank nicht nur für viele Hinweise und Hilfen, sondern auch dafür, daß er sich zu einer Zeit auf ein Thema eingelassen hat, als dessen Bedeutung nicht überall so klar war wie heute. Prof. Dr. Hans-Hermann Francke hat nicht nur das Zweitgutachten übernommen, sondern mit seinem Interesse an Arbeit und Doktorand sowie beider Fortschritt eben dazu sehr beigetragen. Der Gottlieb Daimler- und Karl Benz-Stiftung, Ladenburg verdanke ich die nicht nur materielle Unterstützung meiner Arbeit im Rahmen des Kollegs „Sicherheit in der Kommunikationstechnik".

Obwohl nicht formell beteiligt, hat Prof. Dr. Andreas Pfitzmann wesentlich bei Themenfindung und -fokussierung geholfen und neben vielem anderem geduldig frühe Versionen vieler Kapitel und Ansätze begutachtet und diskutiert. Außerdem hat er wie Rüdiger Dierstein und Prof. Dr. Fritz

Krückeberg nicht nur immer wieder inhaltlich Anteil genommen, sondern auch in bewegten Zeiten Ansatz und Idee der Arbeit im und mit dem Präsidiumsarbeitskreis „Datenschutz und IT-Sicherheit" der Gesellschaft für Informatik stark und mutig gefördert.

Dr. Klaus-Jürgen Eckardt erklärte mir nach einer sehr lebendigen Podiumsdiskussion auf der VIS'91, wenn ich zum Thema Kriterien wirklich etwas bewegen wolle, müsse ich in die Normung gehen – wohl einer der folgenreichsten Ratschläge, die ich je bekam. Manche Erkenntnisse und Einsichten wären ohne die offenen Worte vieler Aktiver bei ISO/IEC JTC1/SC27 und DIN NI-27 schwerer oder unmöglich zu erlangen gewesen. Es sind zu viele Personen, um sie hier einzeln aufzuführen, aber ich weiß auch, daß das mindestens einigen angesichts der Materie sehr recht ist. Auch manche Diskussion im nationalen Arbeitskreis „IT-Sicherheitskriterien" hat zur Schärfung des Problemverständnisses beigetragen.

Dankbar bin ich auch meinen Kollegen in der Abteilung Telematik des Instituts für Informatik und Gesellschaft der Universität Freiburg, speziell Dr. Werner Langenheder, der leider die Vollendung dieser Arbeit nicht mehr erleben konnte, obwohl er sehr dazu beigetragen hat. Dr. Ulrich Kohl, Dr. Frank Stoll und Dr. Marjan Jurecic haben mich freundlich in der „Sicherheitsgruppe" aufgenommen. Ohne die Rückendeckung und Rücksicht bei vielen Projektarbeiten, die fruchtbaren Diskussionsbeiträge sowie das geduldige Korrekturlesen von Herbert Damker, Martin Reichenbach und Sönke Gold wären wohl weder Dissertation noch Buch je fertig geworden. Uwe Jendricke hat noch kurz vor Toreschluß die (vor-)letzten Tipp- und Satzfehler sowie spezielle Gemeinheiten der Textverarbeitung aufgespürt. Vielen weiteren Kollegen, speziell Dr. Tim Bussiek und Boris Padovan, danke ich für hilfreiche Einführungen und Exkurse in die Volkswirtschaft.

Last but not least ist denen zu danken, die mit dafür sorgten, daß aus der Dissertation ein Buch wurde: den vier Herausgebern der DuD-Fachbeiträge sowie Dr. Ulrike Walter und Dr. Reinald Klockenbusch vom Verlag Vieweg, die Projekt und Autor zielorientiert und einfühlsam betreuten.

Inhaltsverzeichnis

Abbildungsverzeichnis