Dirk Fox

Schutzprofile – Protection Profiles

Hintergrund

Für die Zertifizierung der Sicherheitseigenschaften von Produkten der Informationstechnik haben sich in einem mehrjährigen Harmonisierungsprozess die „Common Criteria" (CC) als internationaler Zertifizierungsstandard herausgebildet.[1] Er wurde am 01.12.1999 als ISO/IEC-Standard 15408 publiziert und zuletzt im Jahr 2009 aktualisiert [1].

Die Sicherheitszertifizierung eines Produkts bezieht sich dabei immer auf einen konkreten Evaluierungsgegenstand (EVG, englisch: *Target of Evaluation, TOE*). Umfang und Prüftiefe einer Evaluierung steigen mit dem gewählten Evaluierungs-Level. Sie umfassen nicht nur Sicherheitseigenschaften des Entwurfs und der Implementierung, sondern insbesondere auch Schutzmaßnahmen, die eine nicht autorisierte Modifikation des Programmcodes während des Entwicklungsprozesses verhindern sollen, wie Zugangskontrollen oder ein striktes Versionsmanagement.

Ein CC-Sicherheitszertifikat bestätigt dabei nicht, dass ein zertifiziertes IT-Produkt „sicher" ist – sondern, dass der EVG (der ggf. nur einen Teil des gesamten Produkts ausmacht) einer bestimmten Sicherheitsspezifikation, die das Produkt zu erfüllen beansprucht, genügt. Damit sind CC-Zertifikate üblicherweise sehr spezifisch – erst ein Blick in die Details des Zertifikats klärt darüber auf, welche Teile genau Gegenstand der Zertifizierung waren, für welche Betriebsmgebung die Zertifizierung gilt, welche Sicherheitseigenschaften nachgewiesen wurden und welche Prüftiefe die Evaluation besaß.

Protection Profiles

Um Sicherheitszertifikate unterschiedlicher IT-Produkte derselben Produktkategorie (wie z. B. Firewalls, Chipkartenleser oder PKIs) dennoch vergleichbar zu machen, wurde das Konzept der Schutzprofile (*Protection Profiles*) entwickelt. Ein solches Schutzprofil einer Produktkategorie beschreibt verschiedene Annahmen und Anforderungen z. B. über die Gefährdungen, die Betriebsumgebung und die Sicherheitsziele sowie – auf einer geeigneten Abstraktionsebene – eine „Musterlösung" für die Gestaltung des Produkt-Sicherheitskonzepts.

Vorteile

Protection Profiles vereinfachen den Zertifizierungsprozess – insbesondere für den Hersteller, weil er seine Sicherheitsvorgaben nicht selbst formulieren muss, sondern sich an einem (in der Regel bereits bewährten) Musterkonzept orientieren kann, und deren Eignung nicht eigens begründen muss. Gerade die Formalisierung der meist eher informellen Sicherheitsanforderungen an ein Produkt ist ein oft aufwändiger Prozess – den ein Schutzprofil einheitlich für eine ganze Produktkategorie leistet. Die *Security Functional Requirements* werden dabei in einer semi-formalen Sprache spezifiziert, die insbesondere Mehrdeutigkeiten ausschließen, testbare Anforderungen formulieren und ein durchgängiges und angemessenes Abstraktionsniveau besitzen soll. Die *Security Assurance Requirements* bieten eine standardisierte Form der Beschreibung, wie der EVG evaluiert werden soll. Je höher das gewählte Evaluierungs-Niveau (englisch: *Evaluation Assurance Level*, EAL), desto komplexer ist die Überprüfung des EVG.

Zudem kann ein Schutzprofil auch nach den Common Criteria zertifiziert werden – und schreibt dann die Prüfvorgaben für eine Evaluierung von Produkten einer bestimmten Kategorie für ein im Schutzprofil festgelegtes Evaluierungs-Niveau vor.

Wird ein Schutzprofil von der ISO registriert, wird es über das Common Criteria-Portal zugänglich gemacht [2]. Auch das BSI und das US Government publizieren von ihnen akkreditierte bzw. zertifizierte Schutzprofile auf ihren Webseiten [3, 4].

Gute Schutzprofile können zudem einen weltweit einheitlichen Sicherheitsstandard etablieren – denn auch wenn ein Hersteller sein Produkt nicht evaluieren lässt, wird er gut daran tun, sich an einem etablierten Schutzprofil zu orientieren – und möglicherweise die Konformität mit diesem Profil sogar durch eine Herstellererklärung zu bestätigen. Produkte bestimmter Kategorien werden dadurch hinsichtlich ihrer Sicherheitseigenschaften vergleichbar.

Schließlich geben Schutzprofile dem Gesetzgeber die Möglichkeit, durch die Forderung zertifizierter Produkte für bestimmte Anwendungen und Einsatzbereiche (wie z. B. Smartcards für qualifizierte digitale Signaturen oder Smart Metering Gateways im Smart Grid) auf einfache Art und Weise einen technischen Sicherheits-Mindeststandard festzulegen.

Für die Erstellung von Schutzprofilen hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen sehr instruktiven, 78-seitigen (englischen) Leitfaden publiziert [5].

Literatur

[1] Common Criteria v3.1, ISO/IEC-Standard 15408, July 2009 http://www.niap-ccevs.org/cc-scheme/cc_docs/

[2] Common Criteria Recognition Arrangement: Protection Profiles http://www.commoncriteriaportal.org/pps/

[3] U.S. Government Approved Protection Profiles http://www.niap-ccevs.org/pp/

[4] Liste der vom BSI registrierten Schutzprofile: https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/ZertifizierungnachCCundITSEC/SchutzprofileProtectionProfiles/schutzprofileprotectionprofiles_node.html

[5] BSI: The PP/ST Guide, August 2010 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/BSI_PP_ST_Guide_pdf.pdf?__blob=publicationFile

1 Zur Geschichte der IT-Sicherheitszertifizierung siehe auch Kersten/Schröder, in diesem Heft.