Fraunhofer
SIT

Testat IT-Sicherheit Fraunhofer-Institut SIT

Konzept, Kriterien, Vorgehensweise

Inhalt

Vorwort		**3**
1	**Grundgedanke**	**4**
2	**Gegenstand und Evaluationsprinzipien**	**5**
2.1	Evaluationsinstanz	5
2.2	Evaluationsgegenstand (EVG)	5
2.3	Evaluationsprinzipien	6
2.4	Evaluationstiefe	7
2.5	Ergebnisse	7
3	**Evaluationsprozess**	**8**
4	**Bedeutung im Zertifikatskontext**	**10**
5	**Grundbegriffe**	**11**

Vorwort

Mit der zunehmenden Verbreitung der Informationstechnologie (IT) und der steigenden Vernetzung der IT-Systeme wächst auch die Bedeutung der IT-Sicherheit. Bedingt ist dies zum einen durch die wachsende IT-Durchdringung aller Lebensbereiche, zum anderen durch die Zunahme allgemeiner und spezifischer Bedrohungen wie Viren oder Phishing-Attacken. Kunden und Verbraucher wollen deshalb immer häufiger wissen, wie sicher ein IT-Produkt oder eine entsprechende Dienstleistung ist.

Das Fraunhofer SIT ist nicht nur bestrebt, die allgemeine IT-Sicherheit zu verbessern und neue Sicherheitstechnologien und -anwendungen zu entwickeln, sondern untersucht im Auftrag von Partnern auch die Sicherheitseigenschaften von Software oder softwarebasierten Systemen und Diensten. Im Falle eines erfolgreichen Testverlaufs, bei dem ein Produkt ausreichende Sicherheitseigenschaften aufweist, vergibt das Institut ein qualifiziertes, produktspezifisches Testat.

Die grundlegenden Überlegungen und der Charakter der Sicherheits-überprüfungen am Fraunhofer-Institut SIT sowie die konkrete Vorgehensweise bei der Testatvergabe sind Gegenstand dieses Papiers.

1 Grundgedanke

Das Testlabor IT-Sicherheit entstand am Fraunhofer-Institut SIT aus der Überzeugung heraus, dass individuelle und anwendungsorientierte Sicherheitstests von IT-Systemen durch eine neutrale Partei die beste Grundlage bilden, um Schwachstellen effektiv aufzuspüren und verlässlich und aussagekräftig über Sicherheitseigenschaften von Produkten und Diensten zu informieren. Testat und zugehörige Dokumentation dienen dabei zur transparenten und nachvollziehbaren Darstellung der am Fraunhofer-Institut SIT erzielten Testergebnisse, wie sie Gesellschaft und Wirtschaft erfordern.

Im Unterschied zu anderen Produkten lässt sich in der Informationstechnologie die Sicherheit nicht ohne weiteres nachprüfen. Entsprechende staatliche Stellen, die Mindestanforderungen der IT-Sicherheit für alle IT-Waren durch standardisierte Pflichtkontrollen durchsetzen, um IT-Nutzer und Internet-Kunden zu schützen, gibt es nicht. Vielmehr ist es in den meisten Fällen den Herstellern überlassen, ob – und wenn ja in welchem Umfang – sie ihre Produkte und Angebote einer IT-Sicherheitsüberprüfung unterziehen. Das Testat des Fraunhofer-Instituts SIT soll Nutzer verlässlich darüber informieren, ob ein Produkt oder Dienst für einen bestimmten Einsatzzweck erforderlichen Grad an Sicherheit bietet. Demgegenüber fragen standardisierte Sicherheitsanalysen lediglich grundlegende Sicherheitseigenschaften ab; dem spezifischen Einsatzbereich und der verwendeten Technologie eines Systems tragen nationale und internationale Kriterienkataloge jedoch nur bedingt Rechnung.

Das Fraunhofer SIT versteht sein Sicherheitstestat und die ihm zugrunde liegende Analyse als anwendungsorientierte Vorstufe zu einer Zertifizierung gemäß nationalen und internationalen Kriterienkatalogen wie den Common Criteria for Information Technology Security Evaluation (CC), also den internationalen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik.

Leitidee des Testlabors IT-Sicherheit am Fraunhofer SIT ist, dass ein sicheres IT-System in seinem typischen Anwendungskontext keine relevanten Sicherheitsmängel aufweist. Als relevant werden dabei alle nach dem Stand der Kunst bekannten Sicherheitslücken betrachtet, welche die allgemeinen Schutzziele der Integrität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit gefährden. Die Bewertung der Sicherheitseigenschaften basiert auf konkreten Bedrohungsszenarien, die diesen Schutzzielen Rechnung tragen.

2 Gegenstand und Evaluationsprinzipien

Ausgehend von den allgemeinen Schutzzielen zur IT-Sicherheit (Integrität, Vertraulichkeit, Verfügbarkeit und Verbindlichkeit) orientiert sich das Testlabor IT-Sicherheit am Fraunhofer-Institut SIT bei der Entwicklung spezifischer und realistischer Bedrohungsszenarien an folgenden Leitfragen:

- Welche Sicherheitsfunktionen sind vorhanden?
- Sind diese Sicherheitsfunktionen ausreichend?
- Funktionieren die Sicherheitsfunktionen korrekt?
- Bieten die Sicherheitsfunktionen einen wirksamen Schutz?

2.1 Evaluationsinstanz

Das Fraunhofer-Institut SIT versteht sich als neutrale Instanz, die Tests mit oder ohne Kundenauftrag durchführt und bei der Ergebnisermittlung und –formulierung allein den allgemeinen Schutzzielen der IT-Sicherheit verpflichtet ist. Garantiert wird die Unabhängigkeit des Instituts durch die staatliche Grundfinanzierung der Fraunhofer-Gesellschaft, die auch die Grundlage bildet für die gesamtgesellschaftliche Verantwortung, der sich das Institut verpflichtet fühlt. Durchgeführt werden die Sicherheitsanalysen im Rahmen des Testlabors IT-Sicherheit.

Auf Kundenwunsch garantiert Fraunhofer SIT seinen Vertragspartner absolute Vertraulichkeit, die das Institut in Form von Geheimhaltungsregelungen rechtlich fixiert und durch entsprechende Sicherheitsvorkehrungen umsetzt. Sämtliche Tests und Analysen werden auf Grundlage des in Deutschland geltenden Rechts durchgeführt.

2.2 Evaluationsgegenstand (EVG)

Für Software und IT-Systeme bietet das Fraunhofer-Institut SIT die Möglichkeit einer Sicherheitsüberprüfung mit Testatsvergabe durch das Testlabor IT-Sicherheit. Möglich ist dies sowohl für geschlossene als auch für offene IT-Systeme. Hierzu zählen auch Systeme, die neben Software auch Hardware-Bestandteile aufweisen. In solchen Fällen muss jedoch gewährleistet sein, dass sämtliche IT-Sicherheitsfunktionen software-basiert sind.

Die Testatvergabe für ein Produkt oder einen Dienst kann nur für eine bestimmte Version des EVGs durchgeführt werden. Bei Änderungen am EVG muss nach Maßgabe der Verfahrensregeln für die Sicherheitsevaluationen am Fraunhofer-Institut SIT der Evaluationsprozess erneut durchlaufen werden, um ein Testat für diese geänderte Version erwerben zu können. Dies ist durch einen Re-Evaluationsprozess jederzeit möglich.

2.3 Evaluationsprinzipien

Jede Sicherheitsanalyse ist abhängig von Aufwand und Zeit, die für die Evaluierung zur Verfügung steht. Um verlässliche und ausreichend qualifizierte Aussagen über ein System zu gewährleisten, gilt bei allen Überprüfungen des Testlabors IT-Sicherheit deshalb das **Angemessenheitsprinzip**. Dementsprechend müssen der Aufwand und die Zeit einer Evaluation immer dem Sicherheitsbedarf des EVG und dessen Anwendungskontext angemessen sein. Dies verbietet insbesondere eine oberflächliche Prüfung von IT-Systemen mit hohem Sicherheitsbedarf.

Oft finden sich in einem Anwendungskontext mehrere Parteien, deren Sicherheitsinteressen sich unterscheiden. Deshalb verfolgen die Produkttests am Fraunhofer-Institut SIT das **Konzept der mehrseitigen Sicherheit**. Dies sieht eine ausgewogene Balance zwischen Schutzbedarf und Ansprüchen aller Kontextbeteiligten vor.

Ausgehend von diesen Konzepten untersucht das Fraunhofer SIT die Wirksamkeit der Schutzvorrichtungen anhand folgender Fragestellungen:

- Sind die sicherheitsspezifischen Funktionen des EVG dazu geeignet, den in den Sicherheitsvorgaben aufgezählten Bedrohungen zu widerstehen?
- Wirken die sicherheitsspezifischen Funktionen und Mechanismen synergetisch zusammen, sodass sie sich gegenseitig unterstützen und ein integriertes wirksames Ganzes bilden?
- Können die Sicherheitsmechanismen des EVG einem direkten Angriff widerstehen?
- Gibt es bekannte Schwachstellen in der Konstruktion des EVG, die in der Praxis eine Sicherheitkompromittierung des EVG erlauben?
- Schützt die Konstruktion des EVG vor Sicherheitskompromittierung durch Ausnutzung bekannter Schwachstellen?

- Erlaubt der EVG eine unsichere Konfiguration, die für Nutzer, Systemverwalter oder Betreiber nicht als unsicher zu erkennen ist?

2.4 Evaluationstiefe

Wie auch bei der formalen Zertifizierung ist die Evaluationstiefe von entscheidender Bedeutung für die zu erwartenden Aussagen über die Sicherheitseigenschaften eines Produkts oder Dienstes. Wird beispielsweise lediglich das Design einer Lösung evaluiert, so können keine Schwächen aufgedeckt werden, die in der Implementierung enthalten sind. Da aber auch die Implementierung die Gesamtsicherheit gefährden kann, wird bei Evaluationen durch das Testlabor IT-Sicherheit grundsätzlich die Implementierung in realen Einsatzumgebungen untersucht. Die Tiefe der Prüfung der Komponenten richtet sich nach den zu erwartenden Auswirkungen beim Fund von Schwachstellen sowie nach den skizzierten Bedrohungen.

Die Untersuchungen können dazu in einem Blackboxverfahren (d.h. ohne Kenntnis des internen Aufbaus des EVG) durchgeführt werden, bei dem jedoch die Spezifikationen der relevanten Schnittstellen und Sicherheitseigenschaften vorliegen müssen. Letztere dienen der effektiveren Prüfung von Angriffsvektoren aufgrund von Implementierungsfehlern. In kritischen Einsatzbereichen ist ebenso ein Whiteboxverfahren (d.h. mit Kenntnis des Quellcodes) möglich. Prüfungen in diesem Modus werden aufgrund der höheren Sicherheitsaussagen im Testat gesondert ausgewiesen.

Im Vergleich zu den Evaluationsstufen der CC muss zwischen den verschiedenen Aspekten der Evaluation unterschieden werden. Während die Prüftiefe der Implementierung mit EAL3-4 vergleichbar ist, werden andere Aspekte, wie die Prüfung des Entwicklungsprozesses und der Lebenszyklus des Produkts nicht betrachtet.

2.5 Ergebnisse

Grundsätzlich ist bei der Ergebnisveröffentlichung zu unterscheiden, ob die Geheimhaltung der Untersuchungsergebnisse nach der Testatvergabe bestehen bleibt oder nicht. Entfällt die Geheimhaltung, veröffentlicht Fraunhofer-Institut SIT die Ergebnisse vollständig. Aufgrund des detaillierten Informationsgrades der Analyse kann eine Geheimhaltung der Evaluationsergebnisse zum Beispiel aus Gründen des Innovationsschutzes notwendig sein. Bei erfolgreicher Testatvergabe erfolgt jedoch unabhängig von den direkten Untersuchungs-ergebnissen generell eine allgemeine Auskunft zu den Sicherheitseigenschaften

des EVG. Diese Auskunft umfasst die Untersuchungsmethodik, den definierten Einsatzbereich und die resultierenden Schutzziele sowie die Schutzeigenschaften des EVG gegen die realisierten Angriffsszenarien.

3 Evaluationsprozess

Die Sicherheitsanalyse eines Produkts oder Dienstes erfolgt in Kooperation und Abstimmung mit dem Auftraggeber. Zeitrahmen und Umfang der Evaluation werden vertraglich festgelegt. Zentraler Bestandteil der Sicherheitsanalyse ist die Festlegung der produkt- bzw. dienstspezifischen Sicherheitsanforderungen. Diese bilden den allgemeinen Erwartungshorizont für die nachfolgenden Untersuchungen und die abschließende Bewertung. Im Zentrum der Betrachtung steht eine Bewertung des potentiellen Ausmaßes möglicher Schäden im Hinblick auf realistische Szenarien. Das heißt, es wird bewertet, wie sicher der EVG im Hinblick auf die Bedrohungen ist, die nach aktuellem Forschungs- und Entwicklungsstand zu erwarten sind.

Ausgangspunkt jeder Sicherheitsuntersuchung am Fraunhofer-Institut SIT ist eine umfassende Bedrohungsanalyse. Diese ermittelt, unter welchen Bedingungen Gefahren entstehen können und welche Bereiche einer Software oder eines Systems diese Gefahren betreffen. Darauf folgt eine Risikoanalyse, die aus den identifizierten Gefahren mögliche Folgen ableitet. Neben zu erwartenden Schäden wird dabei auch die Wahrscheinlichkeit eines möglichen Schadensfalls erfasst. Ob ein Risiko akzeptabel ist oder nicht, spielt hierbei noch keine Rolle – die Gefahren werden zu diesem Zeitpunkt lediglich aufgenommen und priorisiert. Mit Hilfe dieser Vorüberlegungen entwickelt das Testlabor IT-Sicherheit durch struktur- und prozessorientierte Analyse der Kommunikationswege konkrete Bedrohungsszenarien. Die darin festgestellten kausalen Zusammenhänge zwischen vermeintlichen Schwachstellen und möglichen Schadenspotentialen werden dann durch prospektive Analyse überprüft.

Das Evaluationsschema gestaltet sich dementsprechend wie folgt:

Stufe 1: **IST-Analyse**

- Software-Architektur, Komponenten, Kommunikationsprotokolle, Schnittstellen
- Identifikation potentieller Schwachstellen

Stufe 2: **Bedrohungsanalyse**

- Feststellung der Sicherheitsanforderungen
- Ermittlung potentieller Bedrohungen
- Bestimmung allgemeiner und spezifischer Risiken
- Spezifikation der Angriffsszenarien

Stufe 3: **Sicherheitsanalyse**

- Realisierung der Angriffsszenarien für alle Komponenten, Kommunikationsprotokolle und Schnittstellen
- Automatischer und manueller Einsatz von Werkzeugen zum Auffinden von Schwächen
- Ergebnisdokumentation

Stufe 4: **IST/Soll-Vergleich**

- Entwicklung und Formulierung von konkreten Verbesserungsvorschlägen zur Steigerung der Sicherheit und / oder Schließung gefundener Sicherheitslücken
- Bzw. Formulierung und Publikation des Testats

Bei Nichterfüllung der Sicherheitsanforderungen kann der EVG mehrere Re-Evaluationen durchlaufen, bevor das Testat ausgestellt wird. Der für die Re-Evaluation benötigte Zeitraum und Aufwand ist in der Regel kürzer als bei der Erstevaluation.

4 Bedeutung im Zertifikatskontext

Vorgehensweise und Testkriterien des Testlabors IT-Sicherheit orientieren sich an anerkannten Verfahren, bestehenden Schutzprofilen und validierten Forschungserkenntnissen. Sicherheitsanalysen und Testat des Fraunhofer-Instituts SIT sind als eine Vorstufe zu den formalen Zertifikaten zu verstehen, wie sie im Rahmen CC-Zertifizierung vergeben werden. Die Sicherheitsanalysen des Fraunhofer SIT konzentrieren sich zwar in der Regel auf die Implementierung, berücksichtigen aber stets die Gesamtheit der Lösung. Im Vergleich zu CC werden die Prüfkriterien für jeden EVG zu Beginn der Evaluierung individuell hinsichtlich des Einsatzzwecks und eingesetzter Technologien analysiert und festgelegt. Darüber hinaus vergibt das Fraunhofer-Institut SIT keine Testate für isolierte Teilkomponenten einer Lösung.

Die Methodik zur Bestimmung von Bedrohungen, Schutzzielen und Sicherheitseigenschaften ist hingegen mit der akzeptierten CC-Vorgehensweise vergleichbar aber nicht identisch. Die Evaluierung geht über die Bewertung hinaus, da der Testbericht auch konkrete Verbesserungsvorschläge enthält, wie Schutzziele zu erfüllen und weiterführende Produktverbesserungen zu erzielen sind. Der zyklische Ansatz der Evaluation am Fraunhofer SIT erlaubt zudem eine Integration in den Entwicklungsprozess des Produkts. Das heißt, Hersteller/Anbieter können Produkte/Dienste bereits in der Entwicklungsphase testen und mit Hilfe der Ergebnisse gezielt weiterentwickeln.

Die Vorgehensweise des Testlabors IT-Sicherheit eignet sich besonders für Situationen, in denen noch kein CC-Schutzprofil für den Gesamtkontext existiert. Selbst wenn ein solches Schutzprofil vorhanden ist, kann die Evaluierung durch das Testlabor IT-Sicherheit aber unter Umständen angebracht sein, wenn das Schutzprofil dem speziellen Anwendungsfall nicht genügend Rechnung trägt. In einem solchen Fall kann das Sicherheitstestat des Fraunhofer SIT wichtige marktrelevante Sicherheitsinformationen liefern.

5 Grundbegriffe

IT-System:	Ein IT-System kann Informationen technisch speichern und verarbeiten.
Bedrohung:	Potential für die Verletzung der allgemeinen Schutzziele der IT-Sicherheit.
Zertifikat:	Im Bereich der IT-Sicherheit bestätigt ein Zertifikat die erfolgreich durchgeführte Überprüfung der Einhaltung von zurzeit geltenden Standards auf der Basis von allgemein anerkannten und verbindlichen Kriterienkatalogen durch akkredierte Zertifizierungsstellen.
Anwendungskontext:	Zusammenhang der Anwendung zu ihrer Umgebung und ihrem Einsatzzweck
Szenario:	Planung eine hypothetischen Aufeinanderfolge von Ereignissen, die zur Beachtung kausaler Zusammenhänge konstruiert wird.