Ungeliebte IT-Sicherheit – kompliziert – aufwändig – teuer – lästig

Marcel Weinand

Sind das die Begriffe, die ihnen beim Lesen des Begriffes „Sicherheit von Informationstechnik (IT)" einfallen? Dann empfinden sie so wie viele andere IT-Benutzer. Immer noch erwarten IT-Hersteller von ihren Kunden, dass diese sich in die Geheimnisse der Administration komplexer Sicherheitsfunktionen einarbeiten. Der legitime Wunsch der normalen IT-Anwender nach einfacher und beherrschbarer, aber vor allem auch zuverlässiger IT-Sicherheit scheint ein unerfüllbarer Traum zu sein. Kann das nicht geändert werden? An diese Fragestellung hat sich mit den Datenschützern des Bundes und der Länder das Bundesamt für Sicherheit in der Informationstechnik (BSI) gewagt. Es wurde in vielen Arbeitssitzungen gemeinsam eine Sicherheitsarchitektur entwickelt, die einen großen Schritt hin zu einer anwenderfreundlichen IT-Sicherheit ermöglicht, die den oben genannten Wünschen einen großen Schritt näher kommt. Das erarbeitete Konzept wurde von DFKI[1] in die Form eines international anerkannten und vom BSI zertifizierten Schutzprofiles[1] gebracht.

3

Stellt man den beliebten Vergleich zwischen der Sicherheit eines handelsüblichen Rechners und der Sicherheit eines Autos an, dann stellt man große Unterschiede fest. Die Unterschiede betreffen dabei nicht nur die Qualität der Sicherheitsfunktionen, sondern auch deren Bedienbarkeit und Beherrschbarkeit. So kann jeder Autofahrer die Sicherheitssysteme eines PKW bedienen, denn die „Anwender-Schnittstelle" ist überall gleich: angefangen von den Bremsen oder den Sicherheitsgurten, über die Hupe, den Blinker, die Warnblinkanlage, das Licht, verschiedene Anzeigen usw. bis hin zu den angenehmen Sicherheitstechniken wie der Zentralverriegelung. Geringfügige Unterschiede zwischen den PKW-Typen sind leicht erkennbar und zu bedienen.

Daneben gibt es im Auto viele Sicherheitssysteme, die keine Aufmerksamkeit des Fahrers beanspruchen: Knautschzonen, Airbags, Antischleuder- oder Antiblockiersysteme, Zweikreisbremssysteme usw. Kein Autohersteller käme auf die Idee, ein ABS-System einzeln anzubieten und dem Autofahrer den korrekten Einbau zuzumuten.

Bezogen auf die Informationstechnik scheint ein vergleichbarer Komfort der Sicherheit unrealistisch. Der IT-Benutzer ist in der Regel gefordert, selbst zu entscheiden, welche „Sicherheitszutaten" er benötigt. Sicherheitsprodukte wie Virenscanner, Firewalls oder Verschlüsselungssoftware muss er zusätzlich kaufen. Und er muss sogar in der Lage sein, das Produkt korrekt zu installieren und zu konfigurieren, damit die Sicherheit überhaupt wirksam werden kann. Wie selbstverständlich wird vorausgesetzt, dass der Benutzer das Betriebssystem, die benutzte Datenbank, die Zugangssoftware zum Internet etc. sicherheitstechnisch beherrscht und administrieren kann.

Diese Komplexität überfordert die meisten IT-Benutzer und führt zur unsicheren Nutzung der IT. Dabei ist dem IT-Benutzer durchaus bewusst, dass IT-Sicherheit dringend notwendig ist: Insbesondere die in Zusammenhang mit dem Internet fast täglich publizierten Schwachstellen sind wesentliche Ursachen für die zögerliche Akzeptanz von E-Commerce und E-Government-Anwendungen.

Internationaler Sicherheitsstandard für Informationstechnik ISO 15408 (auch genannt CC für Common Criteria)

Die Common Criteria (CC) und das Konstrukt der Schutzprofile

Der ISO-Standard 15408 (CC) befasst sich mit dem Thema vertrauenswürdiger technischer IT-Sicherheit für IT-Produkte und IT-Systeme.
Dieser Standard bietet das Konstrukt Schutzprofil (Protection Profile, PP) zur Beschreibung von Sicherheitsanforderungen an die Informationstechnik (IT) an.
Erfolgreich evaluierte PPs erhalten vom BSI das Deutsche Sicherheitszertifikat, das international anerkannt wird. Die Zertifikate für die BISS-Schutzprofile fallen unter die internationale Anerkennung.
Die vorliegenden BISS[2]-Schutzprofile sind eine mögliche Instantiierung der auf einer regelbasierten Informationsflusssteuerung basierenden Sicherheitsarchitektur. Mit diesen Profilen wird IT-Herstellern ein Lastenheft zur Realisierung eines BISS-konformen Produktes angeboten. Die technische Implementierung wird dabei offen gelassen. Auch wird offen gelassen, welche Applikationen von BISS abzudecken sind. Das BSI bietet für Hersteller mit dem (international anerkannten) deutschen Sicherheitszertifikat eine Nachweismöglichkeit der Erfüllung aller Anforderungen des BISS-Schutzprofils an.

Autor: Marcel Weinand
Titel: Ungeliebte IT-Sicherheit – kompliziert – aufwändig – teuer – lästig
In: Jäckel (Hrsg.) Telemedizinführer Deutschland, Ober-Mörlen, Ausgabe 2004
Seite: 220-224

Eine anwenderfreundliche IT-Sicherheit ist also dringend gefragt! Das BSI hat sich gemeinsam mit den Datenschützern des Bundes und der Länder dieser Herausforderung gestellt und mit dem Projektpartner DFKI eine Sicherheitsarchitektur entwickelt, die eine gravierende Verbesserung der Anwenderfreundlichkeit realistisch werden lässt. Das Projektergebnis wurde in der Form von Schutzprofilen nach ISO 15408 (kurz CC – Common Criteria) erarbeitet.

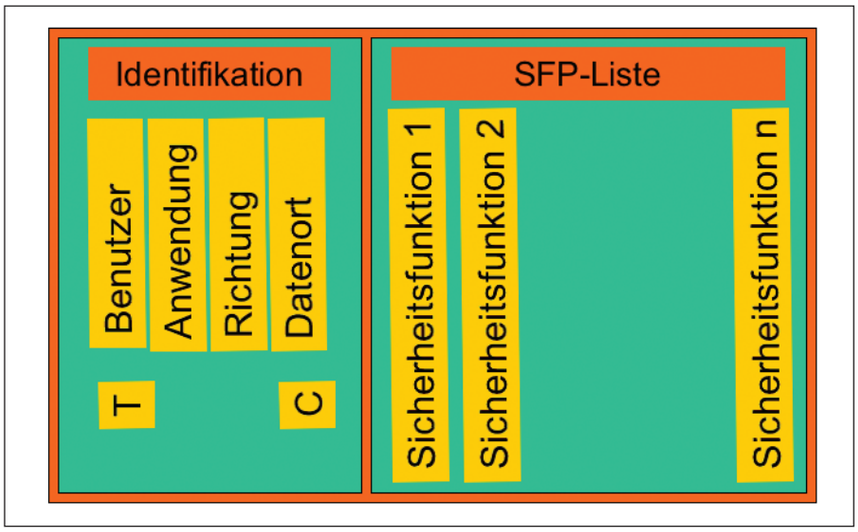

Abbildung 1: *Logischer Aufbau einer Informationsflussregel gemäß dem BISS-Schutzprofil*

IT-Sicherheit aus Anwendersicht

Als Erstes stellt sich die Frage, wie der IT-Anwender seine IT-Sicherheit umgesetzt sehen möchte. Er hat zunächst nur seine Daten im Blick. Schützenswerte Daten sollten seiner vollständigen Kontrolle unterliegen. Ein „zu kontrollieren"-Attribut der Daten sollte unabhängig von der Lokation der Daten erhalten sein.

Diese interessanten Eigenschaften wurden im vorliegenden Projektergebnis dadurch erreicht, indem man sich konsequent an der dem IT-Anwender vertrauten Mensch-Maschine-Schnittstelle ausrichtete, der Anwendung. Vom Anwendungsprogramm her initiiert der IT-Benutzer bei der täglichen Arbeit seine zu schützenden Daten- bzw. Informationsflüsse (durch Laden oder Speichern, Lese-/Schreiboperationen bzw. durch Sende-/Empfangsoperationen).

Identifikationsmerkmale eines Informationsflusses

Der IT-Benutzer initiiert einen Informationsfluss durch die Ausführung einer Applikation (Anwendungsprogramm) in Form von Lese-/Schreiboperationen zu einem Datenort. Die Identifikation eines Informationsflusses basiert auf dem Triple Datenort-Fließrichtung-Subjekt. Der Begriff „Subjekt" wird aus der Kombination der Begriffe Benutzeridentität und Anwendungsprogramm gebildet.

Die Fließrichtung bezieht sich auf die von dem Anwendungsprogramm ausgeführte Ein-/Ausgabeoperation (Lesen/Schreiben) und kann auch für eine Sende-/Empfangsoperation stehen. Der Begriff „Datenort" steht für alle Ein-/Ausgabemöglichkeiten eines IT-Systems und bezeichnet sowohl lokale Speicheradressen wie Dateinamen oder Laufwerksbezeichnungen als auch Email-Adressen, Datenbanksätze oder -felder und sonstige adressierbare Einheiten. Die Informationsflussregeln für die unterschiedlichen Datenorte unterliegen einer einheitlichen Administrationsoberfläche und können in einer einzigen Tabelle erfasst und zentral verwaltet werden.

Jedem erfassten Informationsfluss sind individuelle Sicherheitseigenschaften zuzuordnen. Einerseits muss eine Entscheidung getroffen werden, ob der Informationsfluss zulässig ist, andererseits müssen die Informationen zusätzlich zu schützen sein. Die Sicherheitsattribute aus der mit dem Datenort verknüpften Informationsflussregel werden mit dem lesenden Prozess verknüpft und bei der Ausgabe mit den Attributen der Informationsflussregel des zu beschreibenden Datenortes ausgewertet.

In der vorliegenden BISS-Version wird lediglich ein „Level-Attribut" (Low/High) gefordert. Die Anforderungen an die Übertragungssicherheit von Informationsflüssen beschränken sich auf marktübliche Kryptoalgorithmen und berücksichtigen die Sphinxspezifikation des BSI.

Aus dieser Perspektive ist jeder durch eine Applikation ausgelöste Informationsfluss auf seine Zulässigkeit zu überprüfen und – wenn er erlaubt ist – muss er schützbar sein, insbesondere wenn die Informationen über ungesicherte Netze wie das Internet laufen. Was und wie überpüft werden muss und wie geschützt werden soll, sollte in die Verantwortung des IT-Benutzers gelegt werden. Daraus entstand der Projektbegriff „benutzerbestimmbare Informationsflusssicherheit", BISS. Damit BISS in bestehende Systeme nachträglich integriert werden kann, ist es als „Middleware" spezifiziert und sitzt als solche zwischen den Anwendungen und dem Betriebssystem. Von da übernimmt es die transparente Kontrolle aller aus Sicht des IT-Benutzers zu schützenden Informationsflüsse. Die erforderliche Sicherheit für jeden Informationsfluss wird in Form von Regeln zum Ausdruck gebracht. Sobald eine Informationsflussregel einem Informationsfluss zugeordnet werden kann, wird sie ohne Eingriff des IT-Benutzers, also transparent für ihn, umgesetzt. Er wird von Einzelfallentscheidungen zur Absicherung einzelner Informationsflüsse entlastet. Lediglich in Fehlerfällen, beispielsweise bei unerlaubten Informationsflüssen oder bei qualifizierten Signaturen, erfolgt für den IT-Benutzer eine erkennbare Reaktion von BISS.

Das Schutzprofil von BISS erlaubt sogar eine Verlagerung der Sicherheits-

funktionalität in externe Komponenten, beispielsweise in Kryptomodule. Durch dieses Konzept wird eine hohe Unabhängigkeit vom Betriebssystemtyp ermöglicht. Das dem Anwender vertraute Systemverhalten bleibt erhalten.

Ein weiterer Aspekt der Anwenderfreundlichkeit von BISS ist der „Wartungsmodus". Er ermöglicht die Administration des übrigen IT-Systems durch einen externen Wartungstechniker unter Aufrechthaltung der Sicherheit von zu schützenden Informationen.

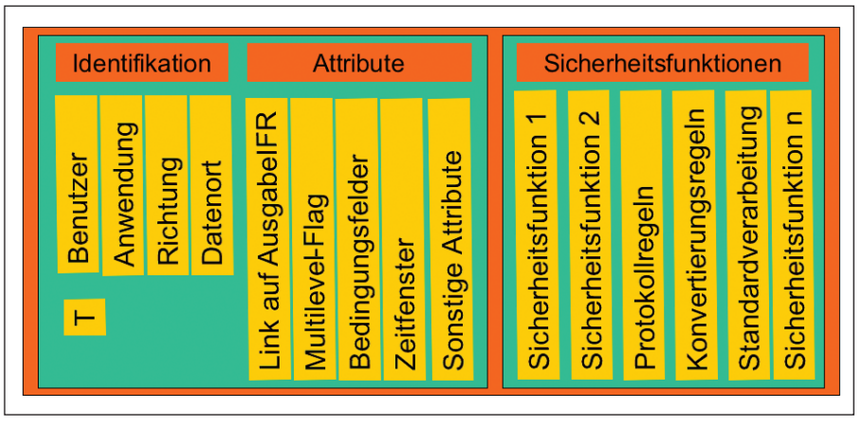

Abbildung 2: *Beispiel einer Erweiterung einer Informationsflussregel*

Logik von BISS

Die Zulässigkeitsprüfung beim Lesen

Die Zulässigkeitsprüfung eines Informationsflusses wird beim Lesen nur für die Datenorte durchgeführt, die in einer Informationsflussregel genannt und als „zu kontrollierender Datenort" gekennzeichnet sind (C=1). Der Informationsfluss ist zulässig, wenn alle Parameter übereinstimmen (Benutzeridentität, Anwendungsprogramm, Lese/Schreibrichtung und Datenort). Die Angabe von Parametermengen (etwa von Wildcards) ist möglich. Alle nicht in den Informationsflussregeln genannten Datenorte werden von BISS beim Lesevorgang ignoriert.

Die Zulässigkeitsprüfung beim Schreiben

Die Zulässigkeitsprüfung eines Informationsflusses wird beim Schreiben durchgeführt, wenn
a) gelesene Informationen aus „zu kontrollierenden Datenorten" stammen. In diesem Fall dürfen die Informationen nur auf „zu kontrollierende Datenorte" geschrieben werden. Dabei spielt es keine Rolle, ob die gelesenen Informationen aus einer Email, aus einer Datei oder einer Datenbank stammen und in welche Umgebung sie weitergeleitet werden. Der Schutz über verschiedene Schichten des OSI-Modells bleibt erhalten. Eine Ausnahme von dieser Regel wird durch die Definition des „vertrauenswürdigen Subjekts" ermöglicht. Das je Informationsflussregel vorgebbare „Trusted-Flag" (T=1) definiert das darin genannte Subjekt als „vertrauenswürdig" für diesen Informationsfluss und ermächtigt es, Informationen aus „zu kontrollierenden Datenorten" in nicht kontrollierte Datenorte zu schreiben.
b) der Datenort in der Informationsflussregelliste genannt ist. Der Informationsfluss ist zulässig, wenn alle Parameter übereinstimmen oder das C-Flag nicht gesetzt ist.

Schutz der Information

Ist die Zulässigkeitsprüfung erfolgreich, wird der Informationsfluss gemäß der zugeordneten Liste von Sicherheitsfunktionen durchgeführt.
Diese Liste kann für den betreffenden Informationsfluss sowohl leer – dann wird der Informationsfluss ohne weitere Sicherheitsfunktionalität durchgeführt – als auch beliebig komplex sein. Als Sicherheitsfunktionen sind Verschlüsselung, Signaturverfahren, Virensuche und vieles andere denkbar. In den BISS-PPs sind einige Verschlüsselungsverfahren gefordert, die dem derzeitigen technischen Stand entsprechen. Diese sind mindestens zu realisieren, können aber beliebig um andere Sicherheitsfunktionen erweitert werden. So sind Pseudonymisierungs- oder Anonymisierungsverfahren denkbar. Aber auch Funktionen, die nicht unbedingt eine Sicherheitsfunktion darstellen müssen, sind möglich.

Perspektiven der regelbasierten Informationsflusssteuerung

Die im BISS-Schutzprofil definierte Sicherheitsarchitektur dient als Basis zur Umsetzung der Sicherheitspolitiken des IT-Anwenders, etwa des Unternehmens oder der Behörde. Eine systemunabhängige Syntax erlaubt die Spezifikation der Informationsflussregeln und ermöglicht so beispielsweise die Umsetzung juristischer Vorgaben des Datenschutzes in technische Spezifikationen.

Als zusätzliche Eigenschaft können die Informationsflussregeln auch außerhalb der Sicherheit liegende Funktionen beinhalten. Damit ist beispielsweise die Unterstützung von Workfloweigenschaften möglich, etwa die Automatisierung von regelmäßigen Abläufen oder die formatgerechte Konvertierung der Informationen vor der Versendung.

Der Definition weiterer Sicherheitsattribute sind keine Grenzen gesetzt. So kann den Informationsflüssen eine Vertraulichkeitsstufe (Vertraulich, Geheim, Streng geheim) durch einen Multilevel-Securitywert zugeordnet werden.

Andere Attribute in Form von monetären Grenzwerten oder von Schlüsselbegriffen können die im Geschäfts- als auch Verwaltungsbereich üblichen Zuständigkeitsregelungen wie Unterschriftsberechtigungen berücksichtigen. Aber auch Attribute mit zeitlichem Charakter sind denkbar. Damit kann die Einhaltung von Löschfristen ebenso einfach automatisiert erzwungen werden wie die Wahrung von Bearbeitungsfristen. Als Attribut könnte sogar die Verknüpfung mit einer weiteren

Informationsflussregel vorstellbar sein. Damit würde die Weiterverarbeitung der Informationen explizit vorgegeben und die Einhaltung von Geschäftsprozessen wäre zu garantieren. Die vom Datenschutz geforderte Zweckbindung ist so durchsetzbar.

Während herkömmliche Sicherheitstechniken die Durchsetzung der Sicherheitspolitik nur innerhalb ihres Systemes (wie dem Betriebssystem oder der Datenbank) gewährleisten können, berücksichtigt die BISS-Architektur die Beachtung der Sicherheitsattribute über Systemgrenzen hinweg, etwa vom Datenbankzugriff über Transaktionsmonitore bis hin zum Email-Versand.

Vorteile der BISS-Architektur

Das bei vielen – auch modernen – IT-Systemen verwendete starre Konzept der Zugriffskontrolle (wie in Betriebssystemen, Datenbanken oder Netzwerkservern) wird in BISS durch die Kontrolle und Steuerung der Informationsflüsse abgelöst. Der Ersatz der Zugriffskontrolle durch die regelbasierte Informationsflusskontrolle gestattet eine erhebliche Verfeinerung der Granularität von Sicherheitseigenschaften und damit der individuellen Anpassung der IT-Sicherheit. Die systemweite Einhaltung von Geschäftsprozessen ist mit BISS ebenso zu erreichen wie die Entlastung der IT-Benutzer von gleichartigen, außerhalb der Sicherheit liegenden Verarbeitungsschritten. Die in vorhandenen Anwendungen existierenden Sicherheitsfunktionen können zwar noch zusätzlich genutzt werden, sind aber durch BISS prinzipiell ersetzbar.

Da die Betrachtung der Sicherheit aus der Anwendungssicht heraus geschieht und die Sicherheitsattribute dem Anwenderprozess zugeordnet werden, werden die Sicherheitseigenschaften der Informationen über Systemgrenzen hinweg berücksichtigt. Ob ein Datenort beispielsweise tatsächlich ein Dateiname oder eine Netzwerkadresse, eine Email-Adresse oder ein Datenbanksatz bzw. -feld ist, spielt für die Administration bei dieser Betrachtung keine Rolle. Generell gilt in BISS: Werden „zu kontrollierende Daten“ von irgendeinem dieser genannten Datenorte von einer Anwendung gelesen, so können sie nur an „zu kontrollierende Datenorte“ weitergeleitet werden. Die Anforderungen für eine einheitliche, robuste und verständliche Administrationsoberfläche von verschiedenen, auch herkömmlichen und bewährten Sicherheitstechniken (z.B. Verschlüsselung, Rechteverwaltung, digitale Signaturen, Virenscanner, Protokollierung, usw.) runden den Anwenderkomfort ab. Eine behutsame Integration in bestehende IT-Landschaften wird ebenfalls berücksichtigt.

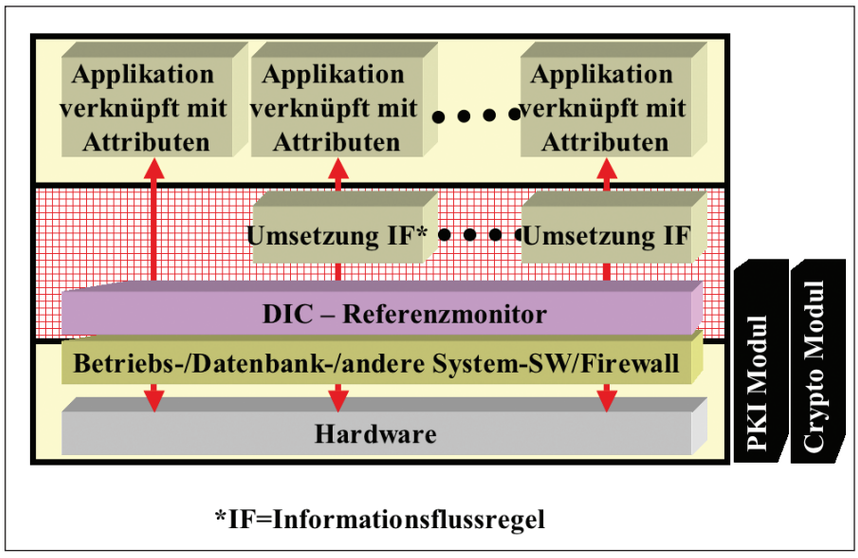

Abbildung 3: *mögliche Architektur von BISS*

Mit BISS werden moderne Forderungen an eine integrierte IT-Sicherheit umsetzbar und administrativ beherrschbar, angefangen vom Schutz einzelner Internet-PCs oder kleiner Netzwerke bis hin zu Mainframes und komplexeren IT-Ausprägungen wie VPN, der virtuellen Poststelle (VPS) oder einzelnen Bereichen von BundOnline 2005. Die Entlastung des IT-Benutzers von Auflagen zur Einhaltung der IT-Sicherheit wird durch eine transparente, regelbasierte und systemübergreifende Informationsflusssteuerung erreicht.

Das BISS-Schutzprofil – ein Lastenheft zur Realisierung eines Produktes

Die zertifizierten BISS-Schutzprofile sind eine erste Instantiierung der auf einer regelbasierten Informationsflusssteuerung basierenden Sicherheitsarchitektur. Mit diesen Profilen wird IT-Herstellern ein Pflichtenheft zur Realisierung eines BISS-konformen Produktes angeboten. Die technische Implementierung wird dabei offen gelassen. Welche Applikationen von BISS abgedeckt werden, ist ebenfalls dem Hersteller überlassen.

Das BSI bietet mit dem (international anerkannten) deutschen Sicherheitszertifikat für Hersteller den Nachweis der Erfüllung aller Anforderungen des BISS-Schutzprofils an.

Herkömmliche Softwareprodukte unterliegen einer hohen Veränderungsfrequenz. Wurde beispielsweise für ein Betriebssystem ein Sicherheitszertifikat erteilt, wird dieses bereits bei geringfügigen Veränderungen ungültig. Für Hersteller bietet das BISS-Konzept den attraktiven Vorteil, dass die gesamte Sicherheitsleistung in einem einzigen Modul konzentriert ist. Wird BISS eingeführt, so können andere Systemteile oder Anwendungen weiter entwickelt werden. Solange BISS unverändert bleibt, behält das Zertifkat seine Gültigkeit bei und ermöglicht so eine aus wirtschaftlicher Sicht befriedigend lange Gültigkeitsdauer.

Das Schutzprofil erleichtert die Zertifizierung für den Hersteller

Will ein Hersteller ein Zertifikat beim BSI erwerben, das ihm die Erfüllung des BISS-Schutzprofils bestätigt, so kann er das Schutzprofil bereits zur eigenen Dokumentation nutzen.

Es wird im Schutzprofil dem Entwickler nicht die Realisierung von BISS vorgeschrieben. Dadurch kann BISS für die unterschiedlichsten Hard- und Softwarekonstellationen entwickelt werden, was wiederum zu umgebungsbedingten zusätzlichen Schwachstellen führen wird. Das können beispielsweise temporäre Dateien oder die Nutzung von Zwischenspeichern sein. Aus der Sicht der PP-Ersteller interessieren diese erst, wenn die Realisierung vorliegt, da vorher noch keine Aussagen dazu möglich sind. Im Rahmen der Zertifizierung eines Produktes wird die Bewertung der Schwachstellen als die zentrale Aufgabe der gesamten Evaluierung verstanden. Die im Schutzprofil vorgegebene Mindestprüftiefe EAL2 fordert eine Schwachstellenbetrachtung (AVA-VLA).

Für weitere Fragen und Anregungen steht das BSI gerne zur Verfügung. Eine Weiterentwicklung der BISS-Schutzprofile wird bei Bedarf vorgenommen. Insbesondere möchte das BSI die bei der Umsetzung gemachten Erfahrungen zukünftig berücksichtigen.

Ansprechpartner für die Schutzprofile

Hr. Weinand, Tel.: 0 18 88 95 82-1 52,
Email: Marcel.Weinand@bsi.bund.de

Weitere Informationen unter

http://www.bsi.bund.de/cc/pplist/pp0008bd.pdf
http://www.bsi.bund.de/zertifiz/zert/reporte/pp0008a.pdf
http://dic.dfki.de
http://www.datenschutz.bund.de

Englischsprachige Informationen unter

http://www.commoncriteria.org
http://www.bsi.bund.de/cc/pplist/pp0008be.pdf

Allgemeine Literaturquellen

[1] Common Criteria, Version 2.1, August 1999, ISO/IEC 15408-1
[2] Common Methodology for Information Technology Security Evaluation CEM-99/045 Part 2: Evaluation Methodology, Version 1.0, August 1999

Fußnote

[1] DFKI: Deutsches Forschungszentrum für künstliche Intelligenz