Trusted Computing – eine Einführung

Norbert Pohlmann[1] · Helmut Reimer[2]

[1]Institut für Internet Sicherheit, FH Gelsenkirchen
pohlmann@internet-sicherheit.de

[2]TeleTrusT Deutschland e. V.
Chamissostrasse 11, 99096 Erfurt
helmut.reimer@teletrust.de

Zusammenfassung

Angesichts der Tatsache, dass sich die Vertrauenswürdigkeit des Internets trotz großer Anstrengungen der Sicherheitsexperten tendenziell nicht verbessert, verdient ein neues Konzept – wie Trusted Computing – besondere Aufmerksamkeit. Zum ersten Mal in der Geschichte der Informationstechnologie haben sich die großen IT-Systemanbieter im Rahmen der Trusted Computing Group (TCG) entschlossen, gemeinsam Verantwortung für wirksame Abhilfe zu übernehmen. Die Implementierung der Ergebnisse der TCG ist im Gange und erste Anwendungen sind nutzbar. Die Herausgeber dieser Publikation wollen mit den in diesem Buch zusammengestellten Beiträgen zeigen, dass das Trusted Computing Konzept eine neue Ära für die Gestaltung vertrauenswürdiger IT-Lösungen eröffnet. In diesem Einführungsbeitrag wird erläutert, worauf sich das innovative Potential dieser Technologie gründet. Er soll dazu anregen, die Vorteile der bereits standardisierten Hardwaremodule und offenen Schnittstellen auszuschöpfen sowie die neuen Ansätze in Anwendungsentwicklungen und Infrastrukturservices zu implementieren.

Der TeleTrusT-Verein wird sich im Bereich Trusted Computing engagieren und möchte helfen, die bestehenden Ansätze des Zusammenwirkens der Sicherheitsplattform mit den notwendigen Sicherheitsinfrastrukturen und den nützlichen Sicherheitstoken der Nutzer pragmatisch weiter zu entwickeln. Er sieht sich auch in der Rolle des Vermittlers zwischen den Technologieanbietern und –anwendern, um so die Erschließung des Potentials dieser innovativen Sicherheitstechnologie für eine vertrauenswürdige IT-Zukunft zu fördern.

1 Grundsätzliches zu IT-Sicherheitslösungen

Informations- und Kommunikationssicherheit sind Themen, die jede Diskussion über nützliche Anwendungen des Internets begleiten. Stets ist von Chancen, Risiken und Gefahren die Rede. Angesichts der über eine Milliarde PCs, die 2008 weltweit im Netz sein werden, und noch weit mehr mobiler Endgeräte ist sachlich festzustellen: **Die Chancen werden genutzt**. Einzig und allein dadurch sind die Voraussetzungen für das Erkennen bestehender Risiken und Angriffspotentiale sowie die heute mögliche Bewertung der Wirkung von Gegenmaßnahmen gegeben.

Die Nutzer des Internets auf der einen Seite verhalten sich gegenüber den bestehenden Risiken sehr differenziert. Im Allgemeinen wird das Ziel, einen deutlich erkennbaren Vorteil zu erreichen, zurzeit mit einem nutzerseitigen Vertrauensbonus, nach dem Motto: „Es wird schon nichts passieren“, verbunden. Die Sensibilität für Sicherheitslücken oder für Angriffe entsteht eher durch negative Erfahrungen als durch Wissen oder Prävention.

Auf der anderen Seite betonen die IT-Sicherheitsexperten das weit gefächerte Spektrum der potentiellen Bedrohungen. Aus dieser Bedrohungssicht ist eine große Vielfalt von hochwertigen IT-Sicherheitslö-

sungen entstanden, deren Komplexität oft über das Fassungsvermögen des durchschnittlichen Nutzers hinausgeht und die deshalb eher in geschlossenen Nutzergruppen (wie in Unternehmen oder besonders sensiblen Anwendungsbereichen z.B. im Gesundheitswesen) mit entsprechenden Infrastrukturinvestitionen Anwendung finden.

Es ist im Interesse einer kontinuierlichen Verbesserung der Sicherheitslage im gesamten Internet dringend erforderlich, Wege zu finden, mit denen die bestehende Diskrepanz zwischen dem blinden Vertrauen vieler Nutzer und den realen Schäden abgebaut werden kann.

Die Entwicklung des Internets und die Verbreitung von kompatiblen und interoperablen Endgeräten ist durch entsprechende Industriestandards entscheidend mitbestimmt worden. Nur deren pragmatische Implementierung in Hard- und Software führte zu der heute erreichten weltweiten Interoperabilität von Internetdiensten und –anwendungen. Gleichzeitig ist auf diesem Wege auch die Grundlage für den riesigen Markt mit relativ kostengünstigen Angeboten für die technische Basis entstanden.

Ähnliches gilt auch für wichtige Internet Sicherheitsstandards und –protokolle, wie SSL (TLS), S/MIME, IPSec usw., die praktisch in alle verfügbaren Betriebssysteme und viele Anwendunge implementiert sind. Auch Kryptoverfahren stehen mit quasistandardisierten Parametern allgemein zur Verfügung. Obwohl diese Werkzeuge über ein hohes Potential im Hinblick auf die Verbesserung der Informations- und Kommunikationssicherheit verfügen, ist ihreAnwendungsbreite weit hinter den Erwartungen zurückgeblieben. Drei wesentliche Gründe können – neben der oben genannten Risikobereitschaft - für die Anwendungszurückhaltung genannt werden:

- Das Handling von Anwendungen mit Sicherheitsfunktionen wird komplizierter, oft sinkt die Performance. Eine unmittelbare Wirkung von Sicherheitsmaßnahmen ist für den Nutzer häufig nicht erkennbar.
- Für den Anwender ist es – in Anbetracht der Komplexität der üblichen Internetanwendungen und der für ihn unüberschaubaren Angriffsziele – nicht möglich zu beurteilen, welches Gewicht eine von ihm implementierte Sicherheitsmaßnahme auf die Sicherheitsqualität der Anwendung besitzt.
- Kryptographieanwendungen erfordern Infrastrukturen und –dienste. Der Nutzer sieht sich hierbei vor neue Herausforderungen gestellt: Neben der Qualität der Services und den mit ihrer Inanspruchnahme verbundenen Kosten, ist häufig ungeklärt, wie die Vertrauenskette zum Diensteanbieter gerechtfertigt werden kann.

Aus Sicht der Sicherheitsexperten gibt es darüber hinaus zwei entscheidende und permanente Risikofaktoren:

- Die Einbettung der Sicherheitsfunktionalitäten als Software in eine offene System- und Netzumgebung und
- das Nutzerverhalten.

Allgemeine Bedrohungsanalysen für IT-Systeme und –anwendungen haben bereits Anfang der 1990iger Jahre zu der Erkenntnis geführt, dass in Software implementierte kryptographische IT-Sicherheitslösungen durch Hardwaremodule wirkungsvoll ergänzt und gegen Angriffe besser geschützt werden können. Für geschlossene Benutzergruppen sind dies komplexe Hardware Security Module (HSM); ein klassisches Beispiel ist der im Bankenbereich verbreitete Kryptoprozessor IBM 4758.

Für den Einzelnutzer wurde das Konzept der Kryptoprozessor SmartCard entwickelt. Inzwischen ist dieser Ansatz – durch ein umfangreiches ISO-Normenwerk begleitet – Grundlage für SmartCard basierte Token als ein entscheidendes Sicherheitsinstrument in der Hand des Nutzers. Allerdings steigen

die Infrastrukturanforderungen und –aufwendungen, bedingt durch die erforderliche Personalisierung und Verwaltung des Lebenszyklus von SmartCards, erheblich an.

Zudem hat sich herausgestellt, dass der Sicherheitsanker „personalisiertes Token“ im Hinblick auf Anwendungsumgebungen zu schwach ist. Alle Angriffe auf die übrigen IT-Systemkomponenten bleiben wirksam. Deshalb werden zusammen mit der SmartCard zahlreiche zusätzliche Sicherheitskomponenten (sichere Kartenterminals, sichere I/O-Kanäle, sicherer Viewer, virenfreie Anwendungsumgebung usw.) empfohlen, die kostenträchtig sind und welche die Anwendungsflexibilität reduzieren.

Bisher ist die Verbreitung dieser Lösung mit niedriger Performance, komplexem Handling und nur wenigen Akzeptanzstellen gering. Ihre konsequente Umsetzung als Grundlage für sichere IT-Anwendungen erfolgt zunächst nur proprietär und für geschlossene Anwendergruppen.

Das Risiko des Nutzerverhaltens zeigt sich insbesondere dadurch, dass die Nutzer auf Links in E-Mails von unbekannten Absendern und mysteriösen Webseiten klicken, und sich so Schadsoftware auf ihren Rechnersystemen laden. Dabei nutzen sie oft keine Virenscanner und Personal Firewalls und sind aus diesem Grund für Angreifer leichte Opfer. Zudem tragen sie zur Verbreitung von Schad- und Angriffsprogrammen bei.

Als ein Fazit ergibt sich: Völlige Sicherheit ist als Vertrauensgrundlage nicht erreichbar! Die Verantwortung aller Partner in der Netzwelt (Anwender, Anbieter von Lösungen oder Geschäftsprozessen, Dienstleister, Infrastrukturbetreiber usw.) für einen vertrauenswürdigen Systemzustand kann Technologie zwar unterstützt, aber nicht abgelöst werden.

2 Die Alternative zu heutigen Sicherheitslösungen

Vor dem Hintergrund der bisher zusammengefassten Erfahrungen wird deutlich, dass die bisher verfolgten Konzepte zur IT-Sicherheit ergänzungsbedürftig sind. Erfolgversprechende Bemühungen in diese Richtung sollten vor allem folgende Ziele verfolgen:

- Reduzierung der Kosten für Sicherheits-Hardwaremodule und für Infrastrukturdienste;
- Integration standardisierter Sicherheits-Hardwaremodule in Geräte und Systemkomponenten zur Verwaltung von Geräteidentitäten sowie zur Prüfung der Vertrauenswürdigkeit und Integrität ihrer Konfiguration;
- Vereinfachung des Handlings der Sicherheitslösungen und Verbesserung ihrer Performance;
- Durchsetzung einer betriebssystemunabhängigen Standardisierung der Sicherheitsfunktionen und ihrer Anwendbarkeit;
- Standardisierung von Schnittstellen für sichere Anwendungen, weitere Kryptogeräte (SmartCards, USB-Token, intelligente Speicherkarten usw.), Infrastrukturen und Management.

Letztendlich können nur auf diesem Wege hochwertige Sicherheitsfunktionen in die allgemein verfügbaren Anwendungen und Systemarchitekturen eingebracht werden.

2.1 Das Trusted Computing Konzept

Das Trusted Computing Konzept greift diese Ziele auf, indem zunächst konsequent ein Sicherheits-Hardwaremodul (Trusted Platform Module – TPM) definiert und spezifiziert worden ist, das in prozessorgestützte Geräteplattformen fest integriert werden kann. Seine standardisierten Grundfunktionen und Schnittstellen unterstützen die lokale Anwendung von Kryptoverfahren auf einem Sicherheitsniveau,

wie es auch von SmartCards geboten wird. Darüber hinaus eröffnet das Konzept zahlreiche weitere Ansätze für innovative Lösungen, mit denen die Vertrauenswürdigkeit und die Sicherheit von IT-Systemen erhöht werden können. Die Darstellung dieser Möglichkeiten ist ein Grundanliegen dieser Publikation.

Da die IT-Systeme tendenziell komplexer und heterogener werden, entscheidet die Bewertbarkeit des Sicherheitszustandes von Systemkomponenten (PCs, aber auch andere computergestützte Geräte im Netz wie Mobiltelefone, Speichergeräte, Drucker usw.) zunehmend über die Vertrauenswürdigkeit von Anwendungen. Diese Anforderung stand bei der Formulierung des Trusted Computing Konzeptes Pate. Das Trusted Platform Module (TPM) kann mittels kryptographischer Verfahren die Integrität der Soft- und Hardware-Konfiguration eines Gerätes messen und deren Hashwerte (Prüfwerte) sicher im TPM speichern. Diese Messwerte können remote überprüft werden und machen Änderungen der Soft- oder Hardware-Konfiguration erkennbar. Trusted Computing benötigt dazu als Voraussetzung und Infrastrukturkomponente eine Sicherheitsplattform (eigenständiges, sicheres kleines Betriebssystem), welche diese Integritätsüberprüfungen anstößt und auch auswertet.

Während die beteiligten Hardwaremodule und die entsprechenden Software-Schnittstellen standardisiert sind, wird die benötigte Sicherheitsplattform proprietär sowohl von der Software-Industrie als auch von Open Source Entwicklungsgruppen entwickelt.

Bedeutsam ist, dass mit dem Trusted Computing Konzept die entscheidenden Marktplayer Verantwortung für die Gestaltung und Umsetzung der genannten Ziele übernommen haben. So besteht die reale Chance, entsprechende Lösungen von unterschiedlichen Anbietern wettbewerbsneutral und – was die Hardwareergänzung betrifft – zu geringstmöglichen Zusatzkosten bereit zu stellen. Der Erfolg wird wesentlich durch die Nutzerakzeptanz bestimmt werden. Hier spielt die Transparenz der angebotenen Sicherheitsfunktionen eine entscheidende Rolle. Sie sollte für die Vertrauensbildung als ebenso bedeutend angesehen werden wie die Befolgung der Kerkhoff-Prinzipien[1] für die verwendete Kryptographie.

2.2 TPM Verbreitung

Spezifikationskonforme TPM 1.2 Module werden von mehreren führenden Chip-Produzenten angeboten und inzwischen in die Motherboards von Servern, Desktops und Laptops verbreiteter Marken integriert.

Die renommierte Marktforschungsorganisation IDC hat dazu eine Analyse und Vorschau geliefert (siehe Abbildung 1). Es wird erwartet, dass im Jahr 2010 bereits mehr als 250 Millionen TPM Module ausgeliefert werden.

1 Die Sicherheit des Kryptosystems darf nicht von der Geheimhaltung des Algorithmus abhängen. Sie darf sich nur auf die Geheimhaltung des Schlüssels gründen.

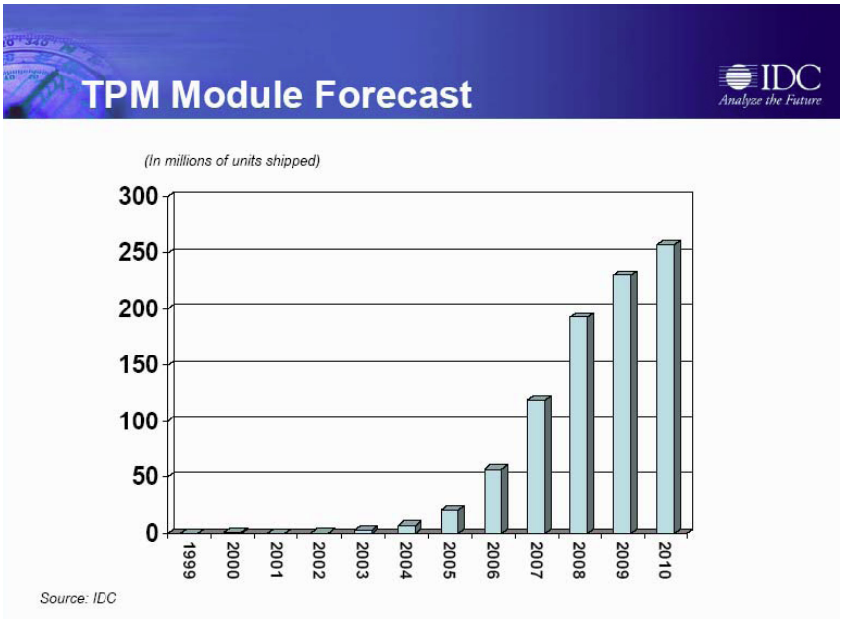

Abbildung 1: TPM Module Forecast (IDC – Oct. 2005)

In 2010 können dann nahezu 100 Prozent der ausgelieferten Laptops und ca. 90 Prozent der ausgelieferten Desktop Systeme mit einem TPM Modul ausgestattet sein (Abbildung 2).

Geht man von einer Erneuerungsrate von 10-20 Prozent pro Jahr für die PC-Ausstattung im privaten Bereich und in Unternehmen aus, könnte mehr als 80 Prozent der PC-Client-Basis des Internet mit TPM-Modulen ausgestattet sein.

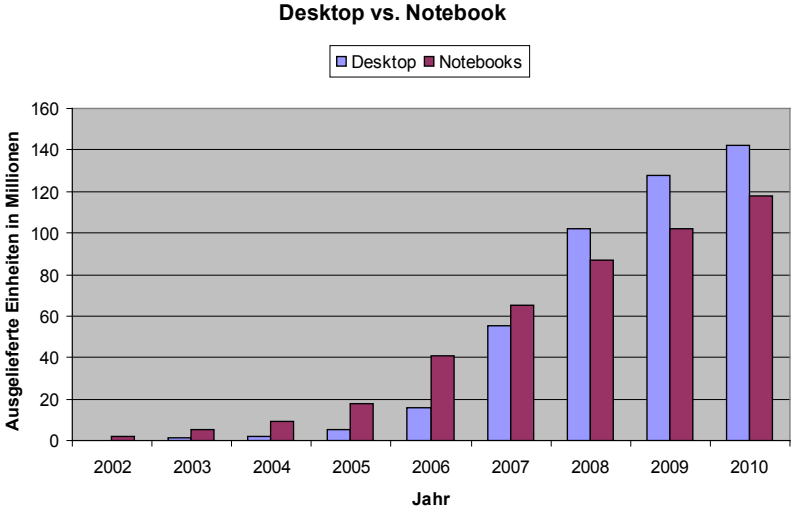

Abbildung 2: TPM Module in Desktops vs. Notebooks (Roger L. Kay, Endpoint Technologies Associates)

Diese Entwicklung ist durchaus vergleichbar mit der Einführung der USB-Schnittstelle. Vom Abschluss der ersten Spezifikation bis zur ihrer allgemeinen Verfügbarkeit sind ebenfalls etwa zehn Jahre benötigt worden.

3 Neue Vertrauensmodelle etablieren

Nun ist das Ziel von Trusted Computing Computing die Sicherheit von und das Vertrauen in die IT-Systeme zu erhöhen. Aber das Thema Vertrauen und Sicherheit ist heute in unserer vernetzten Wissens- und Informationsgesellschaft ein komplexes und vielschichtiges Thema. Das Internet ist sehr schnell zu einem äußerst großen und komplexen Kommunikations- und Informationssystem herangewachsen, das über alle geographischen, politischen und administrativen Grenzen und Kulturen hinausgeht. Es stellt somit eine ungewohnte Herausforderung für die internationale Gesellschaft dar. Dabei ist jedoch festzustellen, dass in den letzten Jahren die Auswirkungen von Sicherheitsproblemen nicht kleiner, sondern sehr viel größer geworden sind und dass das Vertrauen in die angebotenen Dienste zwangsläufig durch negative Erfahrungen immer kleiner wird.

Diesen Herausforderungen muss mit entsprechenden Lösungen angemessen begegnet werden. Aber was heißt eigentlich Vertrauen und Sicherheit für eine vernetzte Wissens- und Informationsgesellschaft?

3.1 IT-Sicherheit und deren Bedeutung

Die IT-Sicherheit hilft, die Risiken bei der Nutzung von IT-Produkten und IT-Angeboten zu minimieren. Bis heute nutzen die Angreifer jede Systemschwachstelle, um durch den Diebstahl von Identitätsdaten, das Passwort-Fishing sowie Viren, Würmer und Trojanische Pferde u.a. die IT-Anwendungen negativ zu beeinflussen und den Nutzer zu verunsichern. Es ist leider festzustellen, dass auch die von uns alltäglich genutzten Dienste, wie z. B. E-Mail-Dienste oder Online-Banking, immer wieder Schwachstellen offenbaren, die ihre Anwendbarkeit für kritische Geschäftsprozesse aus einer Risikobetrachtung heraus in Frage stellen. Die privaten Benutzer sind mit diesen Sicherheitsproblemen überfordert. Sie haben oft keine Chancen und Möglichkeiten damit umzugehen, weil sie nicht genau wissen, wie sie sich verhalten müssen und wie sie sich angemessen schützen können. Selbst Experten fällt das zuweilen schwer. Aus diesem Grund sollen passende IT-Sicherheitmaßnahmen helfen, das Risiko eines Schadens angemessen zu reduzieren. Trusted Computing ist ein Sicherheitskonzept, das helfen wird, dieses Ziel nachhaltig zu erreichen.

3.2 Was ist und wie entsteht Vertrauen?

Hundertprozentige Sicherheit kann es nicht geben. Risiken lassen sich durch geeignete Maßnahmen minimieren, Restrisiken verbleiben jedoch immer. Der konkrete Anwendungskontext bestimmt das Maß an Restrisiken, das toleriert werden kann. Wird dieses Maß regelmäßig nicht überschritten, stellt sich Vertrauen ein. Mit der stetigen Weiterentwicklung der Angriffsverfahren erhöhen sich die Risiken. Damit das zulässige Restrisiko nicht überschritten wird, ist die kontinuierliche Weiterentwicklung der Schutzmaßnahmen eine Notwendigkeit.

Vertrauen ist ein individuelles Gefühl und eine Vorbedingung für die Aufnahme von Geschäftsbeziehungen. Es ergänzt bei wenigen sachkundigen Nutzern vorhandenes und bei vielen unkundigen Nutzern fehlendes Wissen um differenzierte Sicherheitsmechanismen. Vertrauen kann bei positiven Anwendungserfahrungen wachsen und bleibt solange erhalten, bis es erschüttert wird. Zerstörtes Vertrauen ist

schwer wieder aufzubauen, gerade deshalb tragen die Anbieter von elektronischen Geschäftsprozessen, von Sicherheitslösungen und Infrastrukturdiensten eine hohe Verantwortung.

In unserer vernetzten Wissens- und Informationsgesellschaft können verschiedene Aspekte der Bildung und des Erhalts von Vertrauen betrachtet und diskutiert werden:

- Vertrauen heißt auch Zutrauen
  Zutrauen, dass die Anbieter von IT-Produkten und –Leistungen in der Lage sind, Technologie verlässlich und ausreichend sicher umzusetzen. Angebotene Produkte und Dienste müssen ordnungsgemäß und ggf. hinreichend transparent arbeiten, um Vertrauen nicht zu gefährden.
- Zuverlässigkeit erhält Vertrauen
  Mit Zuverlässigkeit ist gemeint, dass IT-Produkte und Lösungen genau die Dinge tun, die gewünscht sind – nicht weniger, aber auch nicht mehr - und das immer.
- Haftung stützt Vertrauen
  Wenn sich die Anbieter in der IT-Branche ihrer Verantwortung in dem gleichen Maß stellen, wie wir das beispielsweise aus der Automobil-Branche kennen, und Produkthaftung bieten, kann dies Vertrauen stützen.
- Vertrauen impliziert Gewissheit
  Gewissheit, dass sich jemand kompetent um die Angelegenheiten kümmert, die ausreichende Sicherheit herstellen.
- Glaubwürdigkeit trägt Vertrauen
  Glaubwürdigkeit der Aussagen, die zur Informationssicherheit gemacht werden, gemessen an den darauf folgenden Aktivitäten.

Wie entsteht Vertrauen beim Nutzer?

Die Beachtung dieser Vertrauensaspekte unterstützt die Herausbildung einer neuen Internetkultur der Nutzer, mit der sie risikoarm mit dem Internet und den angebotenen Diensten umgehen können. Erst dann sind sie in der Lage, sein Potential voll auszuschöpfen. Sie müssen mit Regeln und richtigen Verhaltensweisen vertraut gemacht werden, um Risiken und Gefahren erkennen und abschätzen zu können. Wichtig sind außerdem konkrete Hilfestellungen bei Fragen zu Anwendungen im Internet, wie Online-Banking, Internet-Telefonie, Kaufen und Bezahlen im Internet, Informationsbeschaffung und deren Bewertung, Chatten, Spiele im Internet und bezüglich Raubkopien. Um Problemen vorzubeugen oder ihnen angemessen begegnen zu können, ist es wichtig zu wissen: Was darf ich und was darf ich nicht? Ein klares, übersichtliches und verinnerlichtes Regelwerk kann beim Internet-Nutzer Vertrauen aufbauen.

Zu all den genannten Aspekten des Vertrauens kann das Trusted Computing Konzept wirkungsvolle Beiträge liefern.

IT Konzepte und Lösungen unterliegen einer schnellen Entwicklung. Es werden also Sicherheitslösungen benötigt, die flexible und passende Sicherheitsmechanismen beinhalten, welche entsprechend anpassungsfähig sein müssen, damit die Sicherheit als Basis des Vertrauens stabil bleiben kann.

4 Neue IT-Konzepte werden wirksam

Zukünftig werden die Teilnehmer im „Netz“ mit intelligenten Endgeräten, jederzeit, von überall, auf allen Wegen, mit jeder Kapazität und in der gewünschten Dienstqualität ihre geschäftlichen und ihre persönlichen Anliegen mit jeglichem Partner abwickeln.

Geschäftsmodelle und IT-Strukturen werden sich in Zukunft deutlich rascher verändern und stellen den einzelnen Teilnehmer mit seinem Equipment in den Mittelpunkt.

Von der zunehmenden Ausstattung der privaten Haushalte und der einzelnen Personen mit immer intelligenteren IT-Systemen gehen inzwischen massive Rückkoppelungen auf die Geschäftsmodelle, das Verhältnis zwischen Arbeitgeber und Arbeitnehmer und auch auf die IT-Infrastruktur der Unternehmen aus. Die größten Umwälzungen stoßen derzeit das Web 2.0, die Technologien der Consumer Electronic und die virtuellen Communities an (z.B. Xing/openBC). Die Haupttrends sind zum einen der Wandel von Produkten zu Services und zum anderen die Veränderung des Umgangs mit der IT und deren Diensten. Der Nutzer der Zukunft empfängt seine Informationen von verschiedenen multimedialen Quellen und ist in der Lage, Aufgaben parallel zu verarbeiten. Des Weiteren wird der Nutzer der Zukunft in vielen Fällen zuerst Bilder, Ton, Video und dann erst Text bearbeiten. Er interagiert gleichzeitig mit vielen anderen, dabei lernt und agiert er „Just-in-Time“.

Die im Web 2.0 vernetzte Generation organisiert sich selbst, baut Gemeinschaften außerhalb der Unternehmen auf und zwingt Unternehmen, ihre IT-Infrastruktur und Produktwelten sowie Servicestrukturen den Wünschen der Arbeitnehmer anzupassen. Es wird in Zukunft für Unternehmen immer schwieriger werden, ihre interne und externe IT-Umgebung zu kontrollieren. Ein heute übliches Business Netz mit der ‚traditionellen' Perimeter-Sicherheit und einer unflexiblen IT-Sicherheitspolicy reicht nicht mehr aus. Die neuen IT-Konzepte bedeuten, dass Informationen weltweit über fremde IT-Systeme und Netzstrukturen übertragen und verarbeitet werden müssen. Dennoch müssen diese Informationen auf fremden IT-Systemen entsprechend ihres Schutzbedarfs geschützt werden.

Es werden pragmatische sowie innovative Sicherheitsansätze und -konzepte benötigt, die in verteilten und komplexen Systemen einen notwendigen Sicherheits- und Vertrauenslevel schaffen können. Hier ist die Trusted Computing Technologie mit ihren Möglichkeiten ein richtungweisender Ansatz.

5 Vision

Das Trusted Computing Konzept definiert 25 Jahre nach der Markteinführung des PCs sehr pragmatisch eine neue Qualität von Sicherheit und Vertrauen durch die Verbindung von allgemein verfügbaren IT-Sicherheitsmechanismen. Es führt sowohl zu Innovationen bei Rechnerarchitekturen als auch zu neuen Umsetzungsstrategien bei Betriebssystemen oder Software-Sicherheitskomponenten. Das zugrunde liegende, strenge Standardisierungsprinzip, das von den marktentscheidenden Anbietern von Hard- und Software auch umgesetzt wird, ermöglicht nun eine kostengünstige und investitionssichere Vorbereitung von Anwendungen, die dann von gestiegener Sicherheitsqualität profitieren.

Die zunehmende Verbreitung von Prozessoren in Geräten für fast alle Lebensbereiche (Ubiquitous Computing) und ihre gegenseitige Vernetzung stellen dabei Sicherheits-Herausforderungen dar, denen nun auf dem beschrittenen Wege entsprochen werden kann.

Sicherheitsplattformen auf der Basis von Trusted Computing bewirken bereits einen Quantensprung in der IT-Sicherheit. Mit einem geringen Mehraufwand an Hardwarekosten und einem intelligenten Ansatz an Sicherheitstechnologien können geräteübergreifend neue Geschäftsmodelle umgesetzt werden, die ein notwendiges höheres Maß an Vertrauenswürdigkeit bieten und damit unsere Zukunft sichern.

Insbesondere in Deutschland, einer mittelstandsorientierten Softwarelandschaft mit mehr als 10.000 Softwarehäusern oder software-orientierten Unternehmen und einem Land, in dem die Werte Vertrauen und Sicherheit eine überproportionale Rolle spielen, ist die neue Sicherheitstechnologie von hohem Wert.

Die Trusted Computing Technologie kann die IT-Sicherheit der eigenen Anwendungen verbessern und wird helfen, neue und wichtige Differenzierungsmerkmale für die internationale Wettbewerbsfähigkeit aufzubauen und positiv zu nutzen.

Es muss konsequent darauf geachtet werden, dass die Spezifikationen zum Trusted Computing Konzept für alle offen und anwendbar bleiben und dass Anwendungsstandards entwickelt werden, mit denen sich die Unternehmen international sehr gut positionieren können. Gleichfalls muss die Nutzerakzeptanz ein vorrangiges Ziel bleiben. Bei allgemeiner Verfügbarkeit von Trusted Computing Lösungen, die ein Nutzer verwendet, weil er ihnen vertraut, wird er künftig auch dazu bereit sein, eigene Mitverantwortung für die allgemeine Sicherheit zu übernehmen.

6 Zu den Beiträgen in diesem Buch

Für das Trusted Computing Konzept sind durch die Trusted Computing Group (TCG) Grundlagen und Ergänzungen für wichtige Anwendungsbereiche spezifiziert worden. Die dabei entstandenen Industriestandards führen zu neuen Möglichkeiten, die Informations- und Kommunikationssicherheit in der vernetzten Wissens- und Informationsgesellschaft zu verbessern. Die Herausgeber des Buches Trusted Computing wollen mit dieser Publikation über diese Möglichkeiten aufklären und zu ihrer Anwendung ermutigen. Sie sind davon überzeugt, dass Trusted Computing in der Zukunft eine ganz besondere und wichtige Rolle spielen wird.

Die allgemeine Verfügbarkeit von standardisierten Hardwaresicherheitsmodulen ist abzusehen. Damit wird ein Wendepunkt im Bezug auf die Integration von Sicherheitslösungen in Sicherheitsarchitekturen, Betriebssystementwicklungen und Anwendungs- und Administrationswerkzeuge markiert.

Sicherheitsplattformen auf der Basis von Trusted Computing sind innovativ. Sie verbinden die Erfahrungen bei der Entwicklung und Anwendung von IT-Sicherheitslösungen und bieten die derzeit besten Voraussetzungen, um zukünftig Rechnersysteme sicherer und vertrauenswürdiger zu machen. Das Spektrum der Sicherheitsqualitäten reicht dabei vom Grundschutz für die Anwenderumgebung oder Unternehmensnetze bis zur Unterstützung von Lösungen im Hochsicherheitsbereich.

Mit dem Trusted Computing Konzept werden für einige Anwendungen auch neue Geschäftsmodelle – z.B. für ein Digital Rights Management - erschlossen, die hinsichtlich der Akzeptanz durch die potentiellen Nutzer und des erforderlichen Datenschutzes sorgfältig beobachtet werden müssen.

Im Kapitel „Grundlagen“ wird das Basiswissen über die Trusted Computing Technologie und die dazugehörigen Sicherheitsfunktionen vermittelt und es werden die Ziele und Arbeitsmethoden der Trusted Computing Group erläutert. Ausführlich werden die grundlegenden Funktionen des Sicherheitsmoduls (TPM) dargestellt. Ebenso behandelt wird die Weiterentwicklung und Anpassung von Betriebssystemen an die standardisierten Schnittstellen und Funktionalitäten des TPM, wie die Vision eines virtuellen TPM als ein flexibel in Systemumgebungen integrierbares Sicherheitskonzept.

Im Kapitel „Sicherheitsbausteine für Anwendungen“ werden weitere Sicherheitsbausteine beschrieben, die für die Einbindung der Sicherheitsfunktionen in die Anwendung wichtig sind. Es wird die Idee und Umsetzung einer Sicherheitsplattform sowie deren Sicherheitsnutzen dargestellt. Zusätzlich werden Anwendungsfelder aufgezeigt, in denen Sicherheitsplattformen auf der Basis von Trusted Computing aus heutiger Sicht eine besondere Rolle spielen. Außerdem wird das Trusted Network Connection-Konzept (TNC-Konzept) erläutert, das den Zugriff von nicht einschätzbaren Rechnersystemen auf vertrauenswürdige Netze ermöglicht. Das Kapitel endet mit der Beschreibung, wie die SmartCard in das Trusted Computing Konzept sinnvoll eingebunden werden kann.

Im Kapitel „Anwendungsszenarien“ werden unterschiedliche Anwendungsbereiche des Trusted Computing Konzeptes und die jeweiligen Anforderungen an die Sicherheitslösungen behandelt. Zuerst werden Umsetzungsideen zum Enterprise Rights Management beschrieben. Anschließend wird aufgezeigt, welche Aspekte beim Key-Management der Trusted Computing-Funktionalität berücksichtigt werden müssen. Dann wird geschildert, welche weiteren Aspekte von Trusted Computing bei Hochsicherheitsanwendungen zu berücksichtigen sind. Das breite Wirkungsspektrum des Trusted Computing Konzeptes wird anhand erreichbarer neuerer Sicherheitsqualitäten bei mobilen Anwendungen und embedded Systems im Automotiv-Bereich dargestellt.

Im Kapitel „Datenschutz und rechtliche Aspekte“ sind grundsätzliche Positionen zum Verhältnis zwischen datenschutzrechtlichen Maximen und den Ausgestaltungsmöglichkeiten der Trusted Computing Lösungen und eine Bewertung der rechtlichen Chancen und Risiken zu finden.