- Fahrzeug- und Verkehrstechnologien 770 Mio. €,
- Luftfahrttechnologien 270 Mio. €,
- Maritime Technologien 150 Mio. €,
- Gesundheitsforschung und Medizintechnik 800 Mio. €,
- Pflanzen 300 Mio. €,
- Sicherheitsforschung 80 Mio. €,
- Dienstleistungen 50 Mio. €

Technologieübergreifende Querschnittsmaßnahmen (Auswahl) 2.660 Mio. €

- Kräfte von Wissenschaft und Wirtschaft bündeln: Forschungsprämie, Clusterwettbewerb, Wettbewerb „Austauschprozesse zwischen Wissenschaft und Wirtschaft“, Unternehmen Region, Wettbewerb „Wissenschaft trifft Wirtschaft“ 600 Mio. €
- Bedingungen für den innovativen Mittelstand verbessern: Themenoffene Innovationsförderung für den Mittelstand (PRO INNO, IGF, INNO-WATT, Innonet, NEMO, ERP-Innovationsprogramm) 1.840 Mio. €
- Gründung neuer Technologieunternehmen unterstützen: High-Tech Gründerfonds, Existenzgründungen aus der Wissenschaft (EXIST), Best Practice-Modelle in außeruniversitären Forschungsorganisationen 220 Mio. €

Die Ausgaben für den Bereich der institutionellen Förderung sowie den Pakt für Forschung und Innovation belaufen sich auf rund 14 Mrd. €. Diese lassen sich aus statistischen Gründen nur in einigen Fällen den einzelnen Hightech-Sektoren zuordnen.

Helmut Reimer

TeleTrusT: Anwendung einer vertrauenswürdigen Trusted-Computing-Technologie

TeleTrusT *(www.teletrust.de*) wird das gebündelte Know-how seiner Mitglieder nutzen, um auf Grundlage vorliegender Forschungs- und Entwicklungsergebnisse die Anwendung des Trusted-Computing-Konzeptes in Komponenten der heterogenen IT-Infrastrukturen zu fördern. Europäische Lösungsansätze und die Kompetenz der an ihrer Entwicklung Beteiligten bieten eine passende Ergänzung internationaler Konzepte. Als unabhängige Institution greift TeleTrusT auf das Wissen und die Ressourcen seiner zahlreichen Mitglieder aus Wirtschaft, Verwaltung und Wissenschaft zurück, um die Einführung eines offenen Standards gegen die Gefahren elektronischer Geschäftsprozesse zu beschleunigen.

Die im TeleTrusT-Verein organisierten europäischen IT-Sicherheitsexperten bieten auch der Bundesregierung an, ihr fundiertes Know-how im Bereich Trusted Computing zu nutzen:

Im Rahmen der Programme „Nationaler Plan zum Schutz der Informationsinfrastrukturen“, „Aktionsplan Deutschland Online“ und „e-Government 2010“ sieht TeleTrusT viele Möglichkeiten, seine Expertise in unterschiedlichen Formen einzubringen. Wie schon bei der Spezifikation von ISIS-MTT für Anwendungen der Digitalen Signatur und der European Bridge-CA stellt TeleTrusT als neutraler Projektleiter sein Potential zur Verfügung, um die Anwendung der neuen innovativen Lösungen für die Sicherheit in immer komplexer werdenden IT-Systemen voranzutreiben.

Die Trusted-Computing-Technologie eröffnet neue Möglichkeiten, die Sicherheit vernetzter Systeme auf Infrastrukturebene zu verbessern. Die Trusted Computing Group stellt diverse Spezifikationen für unterschiedliche Anwendungen zur Verfügung. Diese basieren auf dem Trusted Platform Module (TPM) und werden von einigen Herstellern bereits in ihren Produkten implementiert. Im Sinne nationaler und europäischer Interessen stehen jedoch auch ergänzende Lösungen zur Verfügung, die es der europäischen Wirtschaft gestatten, eigene vertrauenswürdige Konzepte anzubieten. Die Anwender sind dann in dieser wichtigen Frage nicht allein von außereuropäischen Anbietern abhängig und es entsteht ein fairer Wettbewerb.

„Trusted Platform Module sind in vielen Geräten bereits eingebaut, beispielsweise in Laptops“, weiß Professor Reimer, Geschäftsführer von TeleTrusT. „Weltweit sind schon über 60 Millionen Motherboards damit ausgestattet.“ Dies sei eine gute Basis, denn die Module könnten genutzt werden, um Infrastrukturen abzusichern und unternehmensübergreifend vertrauenswürdige Umgebungen zu schaffen.

Aus dem Kompetenzpool seiner Mitglieder kann TeleTrusT umfangreiches Informationsmaterial zum Thema Trusted Computing schöpfen, um über die neuen technischen Funktionalitäten aufzuklären und deren sinnvolle Anwendung zu illustrieren. Hierbei gilt es, Vorurteile gegenüber der Trusted-Computing-Technologie abzubauen und die daraus erwachsenden Möglichkeiten aufzuzeigen. Nur wenn Trusted Computing weite Verbreitung findet, kann eine nachhaltige Verbesserung der Sicherheit von Infrastrukturen erlangt werden.

HelmutReimer

Postbank erweitert die Zusammenarbeit mit TC TrustCenter

Als Bank mit den meisten Online-Kunden in Deutschland steht die Postbank besonders im Fokus von Phishing-Attacken. Dagegen geht das Unternehmen seit längerem verstärkt vor und hat ein ganzes Maßnahmenpaket geschnürt. Ein Baustein ist die Absicherung der eMail-Kommunikation.: Ab sofort signiert das Finanzinstitut sämtliche E-Mails an ihre Kunden mit den Team Zertifikaten von TC TrustCenter.

Damit möchte die Postbank ihr Online-Banking noch umfassender absichern und ihre Kunden vor Betrügern im Internet schützen. Durch die Signaturen stellt das Unternehmen die Authentizität und Integrität seiner elektronischen Nachrichten sicher. Über die Signatur und das dafür verwendete Zertifikat ist der Kunde in der Lage, den Absender der E-Mail zu überprüfen und somit zweifelsfrei zu klären, ob sie tatsächlich von der Postbank verschickt wurde. Erhält ein Postbank-Kunde in Zukunft eine E-Mail, die nicht mit einem Postbank-Zertifikat signiert wurde, kann er sie demnach als Phishing-E-Mail identifizieren.

Die Team Zertifikate von TC TrustCenter werden auf dem Postbank-E-Mail-Gateway für bestimmte Mitarbeiterkreise eingerichtet wie beispielsweise für alle Mitarbeiter, die unter direkt@postbank.de erreichbar sind, und signieren den ausgehenden EMail-Verkehr automatisch.

Mit TC TrustCenter hat sich die Postbank für einen Anbieter entschieden, dessen Root-Zertifikate bereits in den gängigen E-Mail-Programmen vorinstalliert sind.

Mehr Informationen sind unter *www.trustcenter.de* zu erhalten.

Helmut Reimer

CrypTool in Version 1.4.00

Die kostenlose E-Learning-Applikation CrypTool (*www.cryptool.de*) für Kryptographie und Kryptoanalyse ist seit Ende Juli in der neuen Version 1.4.00 verfügbar. Mit