TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Bochum 18./19.06.2015

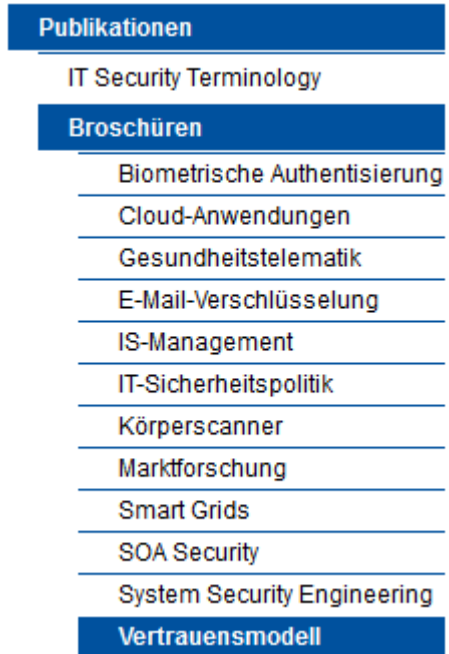
Vertrauen und IT-Sicherheit

Vertrauensmodelle für die Informationsgesellschaft

Autoren	
Einführung:	Marieke Petersohn
Kapitel 1:	Christine Ziske
Kapitel 2 und 5:	Dr. Christoph F-J Goetz
Kapitel 3:	Kerstin Mende-Stief
Kapitel 4:	Michael Barth
Kapitel 6:	Henning Arendt

Vertrauen und IT-Sicherheit
Inhaltsverzeichnis

Studien, Abhandlungen,
Links auf der TeleTrusT Website



Vertrauen und IT-Sicherheit
Zusammenfassung

Die sinnvolle Nutzung heutiger und vor allem zukünftiger IT-Anwendungen und Dienstleistungen erfordert Vertrauen in die IT-Sicherheit.
Nur punktuell lassen sich wichtige Funktionen, wie Integrität der Systeme, Sicherheit vor Missbrauch, Schutz der personenbezogenen Daten und Schutz vor digitalen Angriffen von einem Benutzer selbst überprüfen.

Ähnlich wie man im realen Leben darauf vertraut, dass das, was darauf steht, auch darin ist (die Bremsen des Autos sind vom TÜV geprüft, oder die "Bio-Äpfel" sind bio), ist es auch in der virtuellen Welt.

Dabei spielt die Psychologie des Vertrauens eine wichtige Rolle dafür, wie IT-Sicherheit persönlich wahrgenommen wird. Neben dem "Ur-Vertrauen" sind es einige Faktoren, die das Vertrauen in IT-Sicherheit beeinflussen. Dazu gehören messbare und von Unabhängigen überprüfbare Faktoren wie evaluierte Sicherheitskomponenten, unabhängige Qualitätssiegel oder Ergebnisse von automatisierten Analyseverfahren.

Weitere Faktoren sind "weiche" oder subjektive Faktoren. Das sind z. B. Empfehlungen, wie sie in Foren oder bei Anbietern zu finden sind, aber auch eigene gesammelte Erfahrungen oder die von vertrauenswürdigen Personen sowie Presseveröffentlichungen.
Ein wichtiger Faktor ist die wahrgenommene Reputation des Anbieters bzw. der Kombination von Anbietern komplexer IT-Anwendungen. Kann sich der Anbieter überhaupt Lücken in der IT-Sicherheit leisten?

Anbieter informationstechnischer Infrastrukturen sehen eine wachsende Komplexität der Herausforderungen durch immer gezieltere Angriffe, die es abzuwehren gilt. Nur durch enge internationale Kooperation kann der Professionalisierung der vorwiegend kriminellen Angreifer begegnet werden.

Die Weiterentwicklung von Sicherheitstechnologien und deren Zertifizierung durch unabhängige Experten der eingesetzten Komponenten sind eine Grundvoraussetzung. Dazu kommt die operative Sicherheit, bei der weitgehend sicherzustellen ist, dass die für Betrieb und Wartung zuständigen Personen entsprechend handeln und überprüft werden.

Vertrauen und IT-Sicherheit
Grafiken