# IT-Sicherheit im Lauf der Zeit

**Prof. Dr. Norbert Pohlmann**

Institut für Internet-Sicherheit, FH-Gelsenkirchen
pohlmann [at] internet-sicherheit [dot] de

## Kurzfassung

Wir leben in einer vernetzten Wissens- und Informationsgesellschaft in der die IT-Sicherheit eine immer bedeutendere Rolle bekommt. Die Werte, die als Bit und Bytes zur Verfügung stehen und die Abhängigkeit der angebotenen IT-Dienstleistungen werden immer größer. Die Angriffsflächen werden durch die komplexere Software und komplizierteren Zusammenhänge zwischen Protokollen, Diensten und Infrastrukturen immer vielfältiger. Die Angriffe werden immer verteilter, raffinierter und professioneller ausgeführt und die IT-Kriminalität erfährt eine zunehmende Industrialisierung und damit eine nicht zu unterschätzende und nie dagewesen Nachhaltigkeit.

Dieser Beitrag beschreibt die Veränderung der Angriffsmodelle und der IT-Sicherheitssysteme im Lauf der Zeit und zeigt auf, welche IT-Sicherheitsanforderungen wir in der Zukunft bewältigen müssen.

***Stichwörter:*** Angriffsmodelle, IT-Sicherheitsmechanismen, Internet, zukünftige Herausforderungen

## 1 IT-Sicherheit eine sich verändernde Herausforderung

Mit der Entwicklung der Informationstechnologie (IT) hat sich auch die IT-Sicherheit weiterentwickelt. Die Informationstechnologie begann mit Rechnern, die typischerweise im Rechnerzentrum standen und das Sammeln von Daten sowie die Automatisierung und Rationalisierung von lokalen Prozessen in Organisationen einfach ermöglicht. Zu dieser Zeit hatte die IT-Sicherheit eine lokale Bedeutung. Mit der Einführung von Kommunikationsnetzen wurde der Austausch von Daten über große Entfernungen möglich und die IT-Sicherheit hat sich als neue Herausforderung mit der Kommunikationssichereit beschäftigt. Das Thema IT-Sicherheit ist heute 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 neue und ungewohnte Herausforderung für die internationale Gesellschaft dar. Dabei müssen wir jedoch feststellen, dass in den letzten Jahren die Bedeutung von IT-Sicherheitsproblemen nicht kleiner, sondern sehr viel größer geworden ist.

**Was sind die besonderen Herausforderungen in der IT-Sicherheit im Lauf der Zeit?**

Die Werte, die über IT-Technologie zur Verfügung gestellt werden, sind immer höher. Werte, die sich als Bits und Bytes darstellen, sind z.B. Entwicklungsunterlagen, Geld-Konten, Strategiepapiere, Kundendatenbank, e-Filme, e-Musik, e-Bücher etc. Aber auch die Abhängigkeit

der IT-Technologie und IT-Dienste wird immer größer und damit auch der Anspruch an die Verfügbarkeit der IT. Durch die immer komplexer werdenden IT-Systeme werden insbesondere die Software-Sicherheitslücken immer mehr und die Verbreitung über diese Software-Sicherheitslücken geht immer schneller, d.h. das Angriffspotential und damit das Risiko wird immer größer. Wir können eine zunehmende Industrialisierung der Internet-Kriminalität erkennen, die sehr professionell die Schwachstellen ausnutzt, um damit Geld zu machen. Angriffe werden zunehmend verteilt und international ausgeführt. Jedes Land hat besondere rechtliche Vorteile und die Grenzen übergreifende Strafverfolgung funktioniert nicht flächendeckend. Sehr viele moderne IT-Sicherheitsmaßnahmen arbeiten reaktiv, d.h. sie laufen den Angriffen hinterher. Die vernetzte Wissens- und Informationsgesellschaft als Ganzes und die Internet-Benutzer im speziellen sind nicht richtig auf die Anforderungen des neuen Mediums Internet vorbereitet.

**Analogie mit dem Straßenverkehr**

Der Straßenverkehr ist eine geordnete Infrastruktur, die mit Hilfe von Ampeln, Verkehrsschildern, Radarsystemen und Kontrollen international für mehr Vertrauen und Sicherheit im Verkehrswesen sorgt. Ausstattungen wie Airbags, Sicherheitsgurte, ABS und Fahrgastzellen erzielen mehr Vertrauen und Sicherheit für das Auto und damit für uns, die mit dem Auto Mobilität nutzen.

Mit dem Auto wollen wir schnell ein Ziel erreichen, dabei nehmen wir die Gefahr, einen Unfall zu erleiden, bewusst in Kauf. Zu bequem ist einfach die Mobilität und zu gering die Wahrscheinlichkeit, dass tatsächlich im Straßenverkehr etwas passiert. Dennoch müssen wir uns an die Verkehrsordnung und -regeln halten. Diese gesetzlichen Regelungen, dazu das Bestreben der Automobilhersteller sichere Fahrzeuge zu entwickeln sowie eine Eigenverantwortlichkeit, wie wir uns im Straßenverkehr verhalten sollen, helfen zusammen dabei, uns als Verkehrsteilnehmer zu schützen. Eine ausnahmslose Sicherheit kann hier trotz allem niemandem garantiert werden. Eine ähnliche Situation müssen wir gemeinsam im Internet erreichen.

**Angemessene IT-Sicherheit**

Ähnlich wie im Straßenverkehr, wo sich die Anzahl der Verkehrstoten jedes Jahr reduziert, müssen wir eine angemessene IT-Sicherheit etablieren, damit wir als vernetzte Wissens- und Informationsgesellschaft die Möglichkeiten der modernen IT risikoarm nutzen können.

## 2 Kommunikationsnetze

In den 80er entwickelte sich mit dem PC eine Individualisierung und Dezentralisierung der IT. Gleichzeitig kam zunehmend der Wunsch auf, diese dezentralen IT-Systeme über Kommunikationsnetze miteinander zu verbinden.

Mit den Kommunikationsnetzen entstand die Herausforderung an die IT-Sicherheit, die ausgetauschten Daten während der Übertragung zu sichern. Hintergrund ist das Angriffsmodell, das Angreifer in der Lage sind, Zugriff auf die Kommunikationsleitungen zu bekommen und somit die übertragenden Daten mitzulesen und für sich zu verwenden oder zu manipulieren.

IT-Sicherheitsmechanismen, die in dieser Zeit entwickelt wurden, sind z.B. Verschlüsselungsgeräte auf der Schicht 1, die einfach in der Lage sind, die ausgetauschten Bits zu verschlüsseln. Beispiele sind Leitungsverschlüsselungsgeräte für Modems, 2- oder 34 MBit/s, usw.

Eine andere Variante ist die IT-Sicherheit von Daten-Netzen, wie das X.25 Netz. Hier kann mit Hilfe von X.25-Verschlüsselungsgeräten, die neben der Verschlüsselung und Integrität der Anwendungsdaten auch für eine Authentikation der Verschlüsselungsgeräte sorgen und damit auch den Kommunikationsendpunkt des gewünschten Kommunikationspartners verifizierbar machte [1].

Durch das einfache Angriffsmodell, konnten zu dieser Zeit die Risiken mit passenden Verschlüsselungsgeräten auch überschaubar klein gehalten werden.

# 3 Internet

In den 90er begann sich das Internet zu entwickeln. Dadurch wurde eine globale Kommunikation und die Integration weitere Medien ermöglicht. Das Internet ist ein Verbundnetz und besteht aus einer sehr großen Anzahl voneinander unabhängiger Netze, den so genannten Autonomen Systemen. Diese Autonomen Systeme sind nach bestimmten Strategien der einzelnen Betreiber miteinander verbunden.

**Aufbau des Internets**

Ein Autonomes System ist ein Netz aus Routern und Teilnetzen und untersteht einer einzigen administrativen Instanz. Diese Netze, die sich in Größe und räumlicher Ausdehnung immens unterscheiden, handeln absolut autonom, d.h. sie werden unterschiedlich und vollkommen unabhängig voneinander verwaltet. Das bedeutet z.B., dass sie eine unabhängige Strategie haben, wie sie mit Hilfe von Routing-Protokollen die Kommunikation der IP-Pakete in ihrem Netz organisieren. Die physikalischen Leitungen, die das Netz mit Hilfe von Routern bilden sind meistens so ausgelegt, dass die reale Bandbreite nicht mehr als 50% der theoretischen Bandbreite ausmacht. Damit nun ein Autonomes System vollständig und redundant in das Verbundnetz Internet integriert ist, sorgt der Betreiber für möglichst viele unterschiedliche Verbindungen zu anderen Autonomen Systemen, um aktiv am Verbund Internet teilhaben zu können. Dabei verfolgt jeder Provider unterschiedliche Strategien, abhängig vom Kerngeschäft des Unternehmens und der Größe und Ausdehnung des Autonomen Systems. Unterschieden wird dabei zwischen zwei grundlegenden Verbindungs-Typen: Transit und Peering. Regional begrenzte AS sind auf Verbindungen zu großen nationalen und globalen AS angewiesen. In diesem Fall schließt ein regionaler Provider ein Transit-Abkommen mit einem Provider nationaler, europäischer oder globaler Ausdehnung ab. Dabei zahlt er für sein aufkommendes Datenvolumen. Anders ist dies bei einer Peering-Vereinbarung. Dabei treffen zwei Provider ein Abkommen, kostenneutral Daten zwischen ihren Netzen auszutauschen. Hierbei handelt es sich um ein so genanntes Private-Peering. Beim Peering wird nur der Verkehr der Autonomen Systeme selbst und der Kunden des AS ausgetauscht. Ein Autonomes System erlaubt im Regelfall z.B. keinen Durchgangsverkehr von einem Peering-Partner zu seinem Transit-Provider. Diese Einstellungen können die Provider vorab durch Richtlinien (Policies) beim Routing festlegen. Das Zustandekommen einer Peering-Vereinbarung ist abhängig von vielen Faktoren und die Provider gehen mit unterschiedlichsten Standpunkten in die Verhandlungen. Dabei versuchen sie ihre eigene Größe und Stärke zu nutzen. Die entscheidende Frage ist immer „Wer zahlt an wen?“. Die Provider möchten für möglichst geringe Kosten eine qualitativ hochwertige Dienstleistung für ihre Kunden erbringen. Das Peering ist dabei meist eine Vereinbarung von Partnern auf Augenhöhe Andererseits ist es auch möglich, dass große Provider mit kleineren Providern peeren, da sie sich einen wirtschaftlichen Vorteil durch dieses Abkommen erhoffen. Zur Absicherung existieren in den Peering-Verträgen meist Vereinbarungen über maximale Datenvolumen, welche in die jeweilige Richtung geschickt werden. Eine andere Möglichkeit ist ein Peering an einem Internet Exchange Point (IXP), wie dem DE-CIX oder anderen regionalen und europäischen Internetaustauschpunkten. Hier spricht man dann von einem Public-Peering. Beim Public-Peering können mehrere Peering-Vereinbarungen über eine physikalische Anbindung erstellt werden.

**Das Internet**

Zurzeit gibt es mehr als 27.000 Autonome Systeme, die über mehr als 60.000 Verbindungen das Internet bilden. Statistisch gesehen bleiben ca. 20 % der Kommunikation im eigenen AS, 20 % wird über Public- und 33 % über Private-Peering abgewickelt. 27 % der Kommunikation ist Transit

(Upstream), für das bezahlt werden muss. Für eine genauere Betrachtung und eine richtige Einschätzung der Bedeutung von einzelnen Autonomen Systemen ist es wichtig zu sehen, welche Rolle das jeweilige Autonome System im Zusammenspiel des Internet-Verbunds einnimmt. Im Folgenden werden fünf unterschiedliche Typen von Autonomen Systemen dargestellt [2]:

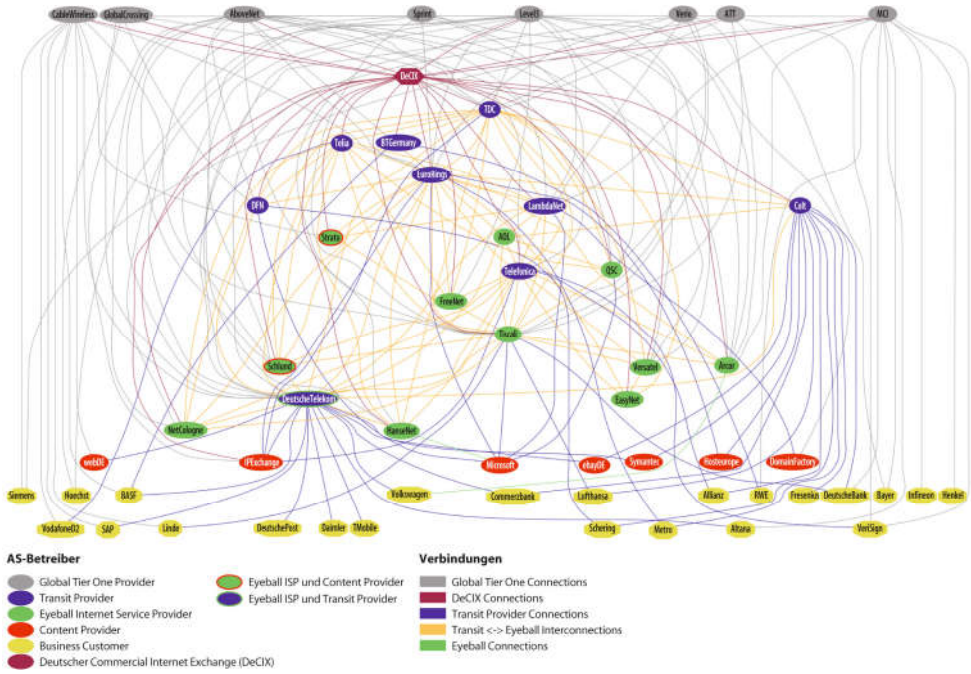


Abb. 1: Internet-Deutschland

**Global Tier One Provider** sind die größten weltweiten IP-Carrier. Dies sind z.B. Verizon (MCI), AT&T, Sprint, Level3, Qwest, Cogent, Global Crossing, C&W. **Transit Provider** sind Provider, die wenig bis keine privaten Internet-Kunden haben. Sie bieten Upstream für Eyeball ISPs und Business Customer und betreiben zumeist Peerings mit anderen Transit Providern und haben einen Upstream zu den großen Global Tier One Providern. Transit Provider, die für Deutschland eine besondere Rolle spielen, sind z.B. Telekom (D), LambdaNet (D), KPN-Eurorings (NL), Telia (Schweden), TDC (Dänemark), Colt (NL), Telefonica (ES**). Eyeball ISPs** sind die größten Internet-Access-Provider. Millionen von Internet-Benutzer sorgen hier für riesige Datenmengen. Eyeball ISPs sind z.B., T-Online (Telekom), 1&1 (United Internet), AOL, Freenet (Mobilcom), Arcor, HanseNet (Telecom Italia), NetCologne, GelsenNET. **Content Provider** stellen Webinhalte bereit, sei es durch das Hosten von vielen privaten Webseiten oder durch das Betreiben eines stark frequentierten Online-Portals. Content Provider sind z.B., Microsoft, Google, T-Online (Telekom), ebay, United Internet, Hosteurope, IP-Exchange. **Business Customer** sind große Unternehmen, die ein eigenes Autonomes System betreiben. Hier geht es mehr um die ökonomische Bedeutung der Verbindungen als um das Datenvolumen. Business Customer sind z.B. Deutsche Bank, Lufthansa, Allianz, BASF, Siemens, DATEV, Volkswagen, Metro, RWE. Eine weitere Rolle spielen bei dieser Betrachtung die so genannten **Internet Exchange Points (IXP).** Sie dienen als Austauschknoten für den Datenverkehr zwischen den Autonomen Systemen. Sie werden typischerweise genutzt, um die Abhängigkeit von Upstream-Providern zu reduzieren sowie die Effizienz und Fehlertoleranz zu steigern. Größter deutscher CIX (Commercial Internet Exchange) ist der DECIX (Deutscher CIX) in Frankfurt am Main.

**Philosophie des Internets**

Ein wichtiger Grund für die schnelle Entwicklung des Internet ist, dass reichlich Raum für individuelle Ideen und Freiheiten vorhanden waren. Dieses Prinzip war sehr wichtig und besonders erfolgreich für die schnelle Schaffung und Bedeutung des Internets. Aber die Situation hat sich entscheidend verändert. Die vernetzte Wissens- und Informationsgesellschaft ist heute sehr stark abhängig vom Internet. Die Bedrohungen, welche wir heute sehen, scheinen aus der Kontrolle zu laufen. An dem erfolgreichen Prinzip der grenzenlosen Freiheit festzuhalten, verursacht ein Risiko, welches wir nicht kalkulieren können. Aus diesem Grund müssen wir überlegen, welche Strukturen und Regeln wir wie einfügen können, um eine höhere Verlässlichkeit des Internets zu erlangen.

**Entwicklung der Internet-Dienste**

Mit dem Internet hat sich als erstes der E-Mail Dienst entwickelt. Hier tauschen Menschen E-Mail sehr einfach und schnell aus. Durch den E-Mail-Dienst ist der medienbruchfreie Austausch von Daten sehr einfach geworden.

Als weiterer wichtiger Dienst im Internet hat sich das World Wide Web (WWW) entwickelt. Das World Wide Web ist ein riesiges verteiltes System, das aus Millionen von Clients und Servern besteht, die auf verknüpfte Dokumente zugreifen. Die Server verwalten die Dokumente, während die Clients den Benutzern eine einfache Schnittstelle für die Darstellung und den Zugriff auf diese Dokumente bereitstellen. Seine enorme Beliebtheit ist auf die Tatsache zurückzuführen, dass die genutzten Browser für Benutzer leicht zu bedienen sind, und dass es eine unglaubliche Fülle von Informationen über jedes erdenkliche Thema zur Verfügung stellt und eine Vielzahl von nützlichen Diensten bietet.

**Anforderungen an die IT-Sicherheit für das Internet**

Die Anforderungen an die IT-Sicherheit im Zeitalter des Internets haben sich wegen neuen Angriffsmodellen im Lauf der Zeit sehr stark verändert.

## 3.1 Phase: Perimeter Sicherheit

Am Anfang haben sich Unternehmen ans Internet angeschlossen, um am E-Mail- und Web-System teilhaben zu können. Zusätzliche habe die Unternehmen die Möglichkeit genutzt, einfach mit ihren Niederlassungen und anderen Organisationen über das Verbundnetz Internet schnell und preisgünstig kommunizieren zu können.

Das Abwehrmodell sah so aus, dass verhindert werden musste, dass Fremde aus dem Internet ins eigene Unternehmensnetz zugreifen konnten und dass die ausgetauschten Daten nicht von anderen gelesen und manipuliert werden konnten. Durch die freie Internet-Infrastruktur, war die Wahrscheinlichkeit eines Zugriffes auf die übertragenden Daten über Router, Mailgateways, usw. stark gestiegen. Die Sicherheitskonzepte folgten der Idee der Perimeter Sicherheit, d.h., die Organisationen haben sich durch zentrale Firewalls und VPNs von den anderen abgegrenzt.

**Firewall-Systeme**

Die Firewall hat dabei das Ziel, die Kommunikation auf das Notwendigste für den eigentlichen Geschäftszweck des Unternehmens zu reduzieren. Das Notwendigste ist z.B., welche Rechner müssen und dürfen ins Internet, welche Internet-Dienste werden wirklich gebraucht, welche Person sollte in welchem Zeitfenster z.B. im Internet surfen dürfen. Usw. [3].

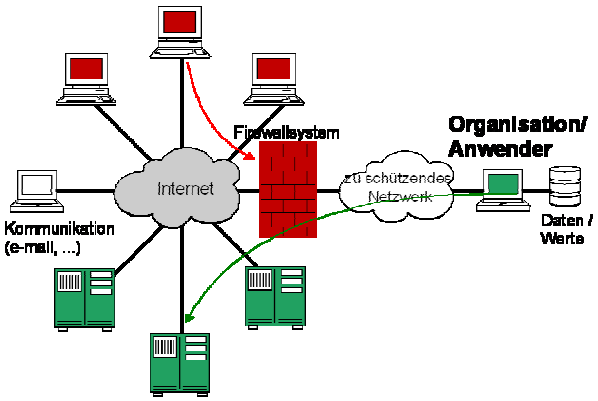


Abb. 2: Firewall-System zum Schutz einer Organisation

**Virtuell Private Networks (VPN) – SSL und IPSec**

Bezüglich der Verschlüsselung der Daten zwischen dem Browser zum Web-Server hat sich der SSL(TLS)-Standard als HTTPS etabliert. Hier wird oberhalb des Transport-Protokolls eine Sicherheitsschicht für die HTTP Kommunikation eingeführt. Hauptaufgaben der Sicherheitsschicht sind: Die Authentikation der Kommunikationspartner unter Verwendung von asymmetrischen Verschlüsselungsverfahren und Zertifikaten. Die vertrauliche Ende-zu-Ende-Datenübertragung mit Hilfe symmetrischer Verschlüsselungsverfahren unter der Nutzung eines gemeinsamen Sitzungsschlüssels. Die Sicherstellung der Integrität der transportierten Daten unter Verwendung von Message Authentication Codes. Statistisch nutzen leider nur 4 % die SSL(TLS)-Sicherheitsdienste, HTTPS und 96 % der HTTP Kommunikation läuft ungesichert. Außerdem werden sehr oft Cryptoprofile ausgewählt und genutzt, die nicht den heutigen Sicherheitsansprüchen genügen [4]. Durch die SSL(TLS)-Sicherheitsdienste kann verhindert werden, dass Passwörter, Kreditkarteninformationen usw. mitgelesen werden können. In diesem Bereich würde eine höhere Nutzungsrate von SSL die Risiken zusätzlich minimieren.

Für die IT-Sicherheit der Datenkommunikation von Niederlassungen über das Internet spielt der IPSec-Standard eine besondere Rolle. IPSec (Internet Protocol Security) ist ein Sicherheitsstandard für den geschützten IP-Datentransfer. IPSec ergänzt das bestehende IPv4 um folgende Sicherheitsfunktionen: Jedes Paket kann gegen Manipulation und Wiedereinspielung geschützt sowie verschlüsselt werden. Außerdem kann die IP-Kommunikation gegen Verkehrsflussanalyse geschützt und die Kommunikationspartner (Personen oder VPN-Gateways) können authentisiert werden. Statistisch nutzen leider nur ca. 2 % IPSec Kommunikation im Internet.

**Welche Probleme haben diese IT-Sicherheitsmechanismen heute?**

Dadurch, dass immer mehr PC im Internet angeschlossen sind, haben sich die Angriffsmodelle sehr stark verändert.

- Die PCs, Notebooks, usw. können zunehmend über GSM, UMTS, … an der zentralen Firewall vorbei ins Internet und stellen somit eine Hintertüren (Back Door) und damit eine Risiko dar.

- Viele Angriffe finden über die erlaubte Firewall-Kommunikation auf der Anwendungsebene statt!

- Die Anzahl der Schwachstellen durch Softwarefehler wird immer größer.

- Diese Rechnersysteme befinden sich wegen der erhöhten Mobilität der Mitarbeiter außerhalb der Kontrolle der Firmen und können kompromittiert werden! Beispiele sind: Außendienstmitarbeiter nutzen ihre Rechnersysteme in vielen unterschiedlichen Umgebungen

mit unterschiedlichen Sicherheitsanforderungen. Heimarbeiter nutzen ihre PCs für private Zwecke. Mitarbeiter nehmen ihre Firmen-Notebooks mit nach Hause.

### 3.2 Phase: Anti-Malware und Software-Upgrades

Die Entwicklung von verteilten Softwareangriffen ist dramatisch gestiegen. Dadurch, dass die Betriebssysteme und Anwendungen immer komplexer und dadurch die Anzahl der Softwarefehler immer größer werden, haben sich Viren, Würmer und Trojanische Pferde immer erfolgreicher verteilen können.

**Software-Upgrades**

Als IT-Sicherheitsmechanismen wird zum einen versucht, durch schnelle zur Verfügungsstellung von Software-Upgrades, die bekanten Schwachstellen, die meist durch Softwarefehler entstehen, zu stopfen und dadurch die Angriffspunkte zu verringern. Leider gibt es viele Benutzer, die diese Software-Upgrades nicht oder nicht schnell genug einspielen und damit leicht angreifbar sind. Die Bekanntgabe der Software-Upgrades ruft auch die Angreifer auf, schnelle Strategien zu entwickeln und umzusetzen, um mit diesen Angriffen Geld zu verdienen oder Schaden anzurichten.

**Anti-Malware**

Anti-Mailware-Lösungen wie Virenscanner sorgen auf den IT-Systemen (PC, Notebook, Handy, …) und wenn möglich an zentraler Stelle dafür, dass Malware (Viren, Würmer und Trojanische Pferde), die Schwachstellen ausnutzt, erkannt und verhindert wird. Dies geschieht in der Regel mit Hilfe von Signaturen, die die Malware eindeutig identifiziert. Die Hersteller müssen die Malware kennen, damit sie in der Lage sind, diese Signaturen zu erstellen. Dazu haben die Hersteller von Anti-Malware sognannte Malware-Traps im Internet positioniert und arbeitet sehr eng mit ihren Kunden zusammen, die bei ersten Auftreten von neuer Malware diese direkt an den Herstellen senden.

Außerdem sorgt eine **Personal Firewall** dafür, dass die Angriffsfläche auf dem IT-System insgesamt kleiner wird.

Welche Probleme haben diese IT-Sicherheitsmechanismen heute?

- Immer mehr Malware wird durch intelligente Entwickler, die dafür sehr gut bezahlt werden und professionell sowie international operieren, weltweit hergestellt und verbreitet. Die Anzahl der neuen Malware und die Schnelligkeit der Verbreitung macht es den Anti-Malware-Hersteller sehr schwer, schnell die geeigneten neuen Signaturen für die Erkennung von neuer Malware flächendeckend zu verteilen.

- Die Tatsache, dass wir heute sehr viele und sehr große Botnetze haben, zeigt, dass wir mit dieser IT-Sicherheitstechnologie auf Grenzen stoßen. Millionen Rechner sind mit „Trojanischen Pferden“ verseucht! Sehr große Botnetze kontrollieren unsere IT-Systeme (PCs, Notebook, …). Unsere IT-Systeme werden fremd-gesteuert, sie spammen, sie werden für Pfishing Angriffe genutzt und werden als DDoS-Hilfsmittel verwendet, usw. Das Schadenpotential der Botnetze ist gewaltig!

### 3.3 Phase: Präventive Sicherheitsmechanismen

Was ist das grundsätzliche Problem, was wir mit modernen Angriffen und IT-Sicherheitsmechanismen heute haben? Neue Angriffe kommen immer schneller, aber nicht die passenden IT-Sicherheitsmechanismen, die dagegen wirken können. IT-Sicherheitsmechanismen wie Anti-Malware rennen den Angriffen hinterher, doch ohne nachhaltigen Erfolg. Unsere IT-

Sicherheitsprobleme werden jedes Jahr größer und nicht kleiner! Das System ist aus dem Gleichgewicht. Der Level an Vertrauenswürdigkeit und IT-Sicherheit unserer IT-Systeme ist heute ungenügend!

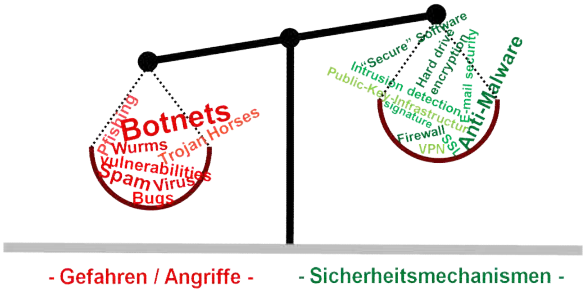


Abb. 3: Die Gefahren/Angriffe sind stärker als die IT-Sicherheitsmechanismen

Wir müssen heute feststellen, dass es nicht möglich ist, große Softwareprogramme, wie heutige Betriebssysteme und Anwendungen fehlerfrei zu schreiben. Und es scheint sich auch in den nächsten Jahren nichts daran zu ändern. Wir müssen unsere Strategie bezüglich IT-Sicherheitsmechanismen ändern! Es ist viel besser, wenn wir proaktive IT-Sicherheitsmechanismen etablieren und nutzen.

Jeder Sicherheitsexperte weiß, dass es keine 100ige Sicherheit gibt, egal wie gut die IT-Sicherheitsmechanismen sind. Aber wir als vernetzte Wissens- und Informationsgesellschaft müssen wieder auf ein angemessenes Sicherheitsniveau kommen, damit wir das zukünftige Potential nutzen können. Und hier spielt eine Sicherheitsplattform auf der Basis von Trusted Computing eine wichtige Rolle. Mit Hilfe von Sicherheitsplattformen können wir das Risiko minimieren!

**Sicherheitsplattform / Trusted Computing**

Trusted Computing ist der Begriff für die Idee, IT-Technologie grundsätzlich vertrauenswürdiger zu machen. Insbesondere die IT-Sicherheit verteilter Anwendungen soll mit wirtschaftlich vertretbarem Aufwand verbessert werden, d.h., es soll keine massive Veränderung existierender Hard- bzw. Software notwendig sein. Eine der Hauptideen ist die Nutzung einer manipulationssicheren Hardware-Komponente, des sog. Trusted Platform Module (TPM). Das TPM mit seinen Funktionen soll softwarebasierten Angriffen entgegenwirken. Die TPM-Spezifikationen wurden bereits von vielen Herstellern umgesetzt. Fast jedes aktuelle Notebook hat einen solchen Sicherheitschip (TPM). Das TPM wirkt als vertrauenswürdiger Anker in einem Rechnersystem (Root of Trust). Beginnend mit dem Startvorgang werden alle Hardwareelemente und Softwarekomponenten (BIOS, Betriebssystem, Anwendungsprogramme etc.) mit Hilfe von Hashfunktionen gemessen und ihre Zustände im Platform Configuration Register (PCR) des TPM gespeichert. Die Systemkonfiguration des Rechnersystems ist also jederzeit komplett mess- und damit auch überprüfbar [6]. In der Automobilindustrie entspräche dies der Arbeit eines Kontrolleurs, der die gesamte Montage eines Wagens protokolliert und hinterher anhand einer zertifizierten Liste von Kontrollnummern aller Teile (z. B. des Fahrgestells) die „Integrität“ des Autos beweisen kann. Wird ein Teil ersetzt, wäre das Auto nicht mehr im Originalzustand und im Vergleich mit der Liste nicht mehr vertrauenswürdig. Die Systemkonfigurationsüberprüfung durch das TPM erfolgt in identischer Weise. Damit können sich Rechnersysteme gegenüber einem Benutzer oder anderen Rechnersystemen hinsichtlich ihrer Systemkonfiguration „ausweisen“. Dieser Vorgang wird Attestation genannt. Außerdem bietet das TPM die Möglichkeit, Daten zu versiegeln und vertraulich zu speichern. Dabei werden die Daten während der Verschlüsselung an die Systemkonfiguration gebunden. Dieser Vorgang wird Sealing genannt. Er stellt sicher, dass auf versiegelte Daten nur wieder zugegriffen werden kann, wenn sich das IT-System in einem

bekannten Zustand (Systemkonfiguration) befindet. Dem entspricht im übertragenen Sinn die Möglichkeit, genau zu prüfen, ob z. B. das Bremssystem unverändert und damit funktionsfähig ist.

**Die Sicherheitsplattform als Teil der Trusted-Computing-Idee**

Trusted-Computing-Funktionen lassen sich bisher nur als Werkzeuge verwenden, um mehr Vertrauenswürdigkeit in IT-Systemen zu generieren. Der Begriff steht allerdings nicht nur für Sicherheitschips wie das TPM. Er ist vielmehr ein Oberbegriff für sämtliche Funktionen, die mit Hilfe neuer Methoden größere IT-Sicherheit herstellen. Ein TPM-Modul allein bringt noch keine höhere IT-Sicherheit, sondern ist im Prinzip ein passives Bauteil, welches IT-Sicherheitsdienste bietet. Um es vertrauenswürdig zu nutzen, wird eine Sicherheitsplattform benötigt, die genau diese Eigenschaft garantiert. In der Analogie sind dies die Mitarbeiter, die den Aufbau des Wagens überwachen, zusammen mit den Testingenieuren, die die Echtheit und Funktionstüchtigkeit überprüfen. In der IT entsteht auf diese Weise eine betriebssystemähnliche Sicherheitsplattform. Aktuelle Betriebssysteme können nicht als Sicherheitsplattform genutzt werden, da sie durch ihren monolithischen Aufbau einfach zu kompromittieren sind, wobei Viren und Trojaner vertrauenswürdige Zustände vortäuschen können, die nicht den realen Zuständen entsprechen. Eine Sicherheitsplattform setzt somit oberhalb der Hardware und unterhalb der herkömmlichen Betriebssysteme an und hat die Aufgabe, selbst möglichst unanfällig gegen Angriffe zu sein und auf dieser Grundlage sicherheitskritische Vorgänge zu kontrollieren. Um diese Vorgaben zu erfüllen, sollte eine Sicherheitsplattform aus einer sehr geringen Codebasis bestehen und weit weniger komplex sein als etablierte Betriebssysteme. Diese „Minimalisierung“ senkt die Fehlerwahrscheinlichkeit wesentlich und erhöht gleichzeitig die Vertrauenswürdigkeit. Durch Virtualisierungstechniken ist eine Sicherheitsplattform in der Lage, mehrere Applikationen und/oder Betriebssysteme parallel, vollständig in ihren Speicherbereichen getrennt auszuführen. Es ist also möglich, einzelne sichere Applikationen in so genannten Compartments – d.h. vollständig vom etablierten Betriebssystem abgeschottet – parallel auszuführen. Die Vertrauenswürdigkeit der Applikationen wird durch die Messmöglichkeit des TPM überprüfbar. Mit anderen Worten: Auch wenn das etablierte Betriebssystem durch Malware kompromittiert ist, droht keine Gefahr, da alle sicherheitskritischen Vorgänge in isolierten Bereichen von sicheren Anwendungen ausgeführt werden. Die Compartments können entweder reine sichere Applikationen enthalten, die an die Sicherheitsplattform angepasst wurden, oder schlanke Betriebssysteme mit Standardapplikationen. Im zweiten Fall misst das TPM das Betriebssystem zusammen mit der Anwendung, um jederzeit die Integrität nachweisen zu können (Abb. 4).

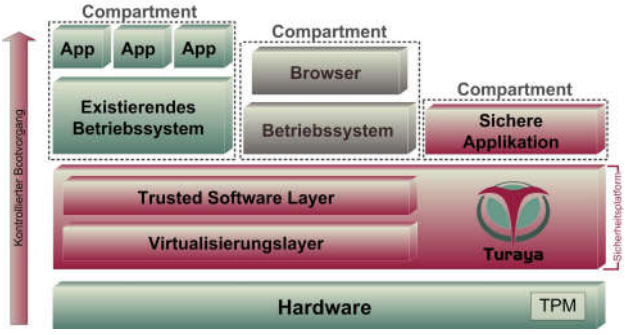


Abb. 4: Systemarchitektur der Sicherheitsplattform Turaya

Eine Sicherheitsplattform in Kombination mit der Trusted-Computing-Technologie (TPM und dessen Funktionalitäten) bietet ein breites Spektrum an Gestaltungsmöglichkeiten für vertrauenswürdige Anwendungen. Auf diese Weise lassen sich z. B. Endbenutzersysteme einrichten, die Daten sicher verwalten und speichern. Schadsoftware kommt gar nicht erst in Berührung mit sicherheitsrelevanten Daten. Server- und Clientsysteme lassen sich zuverlässig authentifizieren; so kann beispielsweise der Bank-Server beim Online-Banking jederzeit seine

Identität nachweisen, was die Gewähr bietet, dass die Bankdaten vertrauenswürdig verarbeitet werden. Damit erreichen wir einen Quantensprung in der IT-Sicherheit und Vertrauenswürdigkeit für unsere IT-Systeme!

**Weitere Beobachtungen von ungelösten Problemen im Bereich der IT-Sicherheit!**

1. Sicherheitsinfrastrukturen

Wir haben immer noch keine angemessene international verfügbare PKI-Infrastruktur, um z.B. ID-, E-Mail-, Signatur-Sicherheitssystem, usw. für die international agierende Informationsgesellschaft anbieten zu können. Wir müssen auch auf der Netzwerk Infrastrukturebene zusammenarbeiten, um gegen Spam, Botenetze, DDoS, Cyber-War Aktivitäten nachhaltig vorgehen zu können. Eine Herausforderung in diesem Bereich ist, eine internationale Zusammenarbeit zu etablieren, die die Völkergemeinschaft akzeptiert und eine hohe Vertrauenswürdigkeit erzielen kann.

2. Identifikationsmanagement

Eines der größten Probleme im Internet ist, dass wir sehr unterschiedliche und begrenzte Identifikationsbereiche etablieren, die nur im Unternehmens- und Kundenumfeld gültig sind. Föderationen sind noch nicht verbreitet genug! Auch im Bereich der Authenikation sind die Passworte immer noch das Mittel, um sich zu authentisieren. Hier brauchen wir neue Lösungen, die eine passende IT-Sicherheit bieten. Der elektronische Personalausweis ist für Anwendungen in Deutschland ein vielversprechender Ansatz.

3. E-Mail-Sicherheit

Im Bereich der E-Mail-Sicherheit ist es noch nicht zu einem Durchbruch gekommen. Weniger als 4 % der E-Mails werden mit PGP-, S/MIME-, oder Passphrase-gestützte-Verschlüsselungssystemen verschlüsselt. Weniger als 6 % der E-Mail werden digital signiert. In machen Bereichen, z.B. im Finanzbereich werden schon mehr als 10% der E-Mails signiert. Aber auch hier können nur weniger als 4 % die Signaturen verifizieren. Der Anteil der Spam-Mails, die im Internet versuchen durchzukommen, ist größer als 90 %. Hier ist dringend ein gemeinsames Vorgehen der globalen Player im Internet notwendig!

4. Medien-Kompetenz der Benutzer

Wir brauchen eine Internetkultur, in der wir sicher mit dem Internet umgehen können. Erst dann können wir das Potential, welches das Internet bietet, voll ausschöpfen. Unsere Online-Kompetenz muss gestärkt werden. Dazu müssen wir für einen richtigen, bewussten Umgang geschult werden, das heißt, wir müssen die Regeln und richtigen Verhaltensweisen verinnerlichen, um die Risiken und Gefahren erkennen und abschätzen zu können.

Regeln und richtige Verhaltensweisen verinnerlichen: Wir Menschen haben Instinkte, die umgangssprachlich oft als „ein sicheres Gefühl für etwas“ bezeichnet werden und Verhaltensweisen des Menschen meinen, die ohne reflektierte Kontrolle ablaufen. Wir haben uns aber auch Gewohnheiten zugelegt. Unter Gewohnheit verstehen wir, eine unter gleichen Bedingungen entwickelte Reaktionsweise. Bewusst gelernte Verhaltensweisen werden zu nützlichen Gewohnheiten oder Fähigkeiten. Also Gewohnheiten sind erworbene Verhaltensweisen, die so lange praktiziert worden sind, dass sie wie angeboren wirken. Diese Verhaltensweisen werden natürlich und automatisch angewendet, ohne bewusst darüber nachzudenken. Hier drängt sich wieder der Vergleich mit dem Straßenverkehr auf: Unabhängig davon, in welcher Form wir daran teilnehmen; als Fußgänger, Fahrrad- oder Autofahrer müssen wir die Verkehrsregeln beherrschen. Das lernen wir von Kindesbeinen an. Unsere Eltern haben uns in den ersten Jahren an die Hand genommen und uns gezeigt, wie wir über die Straße gehen können. Wir haben gelernt, dass wir die

richtige Stelle finden müssen, um eine Straße zu überqueren: eine Ampel, einen Zebrastreifen oder eine übersichtliche Stelle. Wir haben gelernt, dass wir erst nach links und dann nach recht schauen müssen, ob ein Auto zu sehen ist. Wir haben aber auch gelernt abzuschätzen, wie lange es dauert, bis ein gerade heranfahrendes Auto unsere Position erreicht hat.

Verhaltensweisen, die wir für das Internet verinnerlichen sollten, sind z.B.: Schütze Deinen Rechner immer mit Anti-Virus, Anti-Spyware, Personal Firewall und E-Mail Filtern. damit Angriffe verhindert werden können. Schaue Dir Deine empfangenden E-Mail immer richtig an. Wenn Du den Sender nicht kennst oder der angegebenen Sender wahrscheinlich die E-Mail nicht gesendet hat, lösche sie. Klicke nie auf einen Link in einer E-Mail, wenn Du nicht 100% sicher bist, von wem sie kommt. Gebe nie Kennungen, Passwörter oder persönliche Informationen preis. Wenn Du vertrauliche Informationen versenden möchtest, müssen diese vorher verschlüsselt werden.

5. Grenzen übergreifende Verfolgung von Angriffen

Ein Problem für die Bekämpfung der Computer-Kriminalität ist, dass die internationalen Strafverfolgungsbehörden schlecht vernetzt sind. Die Kriminellen sind vor allem in Ländern mit laxer Strafverfolgung aktiv. Der Spammer sitzt in Russland und nutzt Server in Korea, usw. Eine gemeinsame Verfolgung von Straftätern kann das Angriffspotential deutlich dämpfen.

6. Robustheit der Kommunikations- und Informationsinfrastruktur

Wir brauchen für das Internet eine höhere Robustheit, um die Verfügbarkeit zu stärken. Herausforderung in diesem Bereich sind: Die Einführung DNSSEC, Secure BGP und IPv6. Außerdem müssen wir geeignete Mechanismen gegen DDoS-Angriffe einführen.

7. Globale Privatheit

Insbesondere über das „Mobile Internet“ und den angebotenen ortsabhängige Diensten, aber auch den vielen „Web 2.0 Anwendungen“ werden die Anforderungen an den Datenschutz, an die Privatheit der Benutzer sehr viel höher. Wie diese hohen Anforderungen vertrauenswürdig durch die großen Player wie Facebook, Google, Myspace, usw. garantiert werden können, bleibt noch ungewiss.

# 4 Allgegenwärtige, intelligente Wissens- und Informationstechnologien (Zukunft)

Wie wird sich die IT in der Zukunft verändern? Auf welche Angriffsmodelle müssen wir uns in der Zukunft einstellen? Welche IT-Sicherheitsmechanismen brauchen wir, um uns angemessen schützten zu können?

Wie die Zukunft tatsächlich aussieht, wissen wir alle nicht. Dennoch ist es möglich, bestimmte Trends vorherzusagen. Im Folgenden werden einige Ideen diskutiert, die vom Zukunftsforscher Lars Thomsen, prognostiziert werden (www.future-matters.com).

1. Schnellere Innovationen

Zukünftig werden Wissen und neue Informationen sehr viel schneller über das Internet verbreitet. Heute werden neue Ideen überwiegend über wissenschaftliche Printmedien verteilt. Die sehr schnelle Verteilung über das Internet hat den Effekt, dass wir viel schneller und viel mehr innoviert werden. Dieser Effekt sorgt dafür, dass wir Personen brauchen, die diesen hohen Anforderungen genügen. Da diese immer höheren Fähigkeiten auf einer Anzahl von Personen begrenzt bleiben, wird der Kampf um diese Personen international immer größer. Der fähige Mitarbeiter der Zukunft

wird sich mit seinen IT-Intelligenzen, so flexible wie möglich an die IT-Systeme seiner Auftraggeber anschließen, um möglichst optimiert seine Dienste anbieten zu können.

2. Alterspyramide

Die Alterspyramide sorgt dafür, dass in unserer Gesellschaft doppelt so viele Menschen das Berufsleben verlassen als neue dazukommen. Dies wird dafür sorgen, dass die Menschen, die von den Hochschulen kommen, sich nicht bei den Firmen bewerben müssen, sondern, dass sich die Firmen bei den Hochschulabgängern bewerben. Wie bei den schnelleren Innovationen, wird dies die IT-Anbindung zu Unternehmen radikal verändern und damit neue Angriffsmodelle hervorrufen sowie innovative IT-Sicherheitssysteme nötig machen.

3. Mehr Prozessoren, Leistung und Kommunikationsbandbreite auf einer Person

Wenn die heutigen Prozessoren auf Personen aufgeteilt werden müssen, dann würden jeder Person 70 Prozessoren zugeordnet. Das sind die Prozessoren aus den PCs, den Notebooks, die SmartHandies aber auch aus dem Auto, der TV-Anlage, der Musik-Anlage, Kühlschrank, Wecker, usw. In 10 Jahren werden es 1.000 Prozessoren sein, die im Schnitt auch eine 1.000 fache Leistung erbringen werden. Außerdem wird es in 10 Jahren billiger sein, eine Wand als Monitor auszurichten, als eine Holzvertäfelung anfertigen zu lassen. Die Kommunikation der Prozessoren untereinander wird immer schneller und sehr vielfältig werden. Mit dieser Entwicklung werden die Dinge „smart“, d.h. Autos, TV-Anlagen, Musik-Anlagen, Kühlschränke, Wecker, usw. werden sich als intelligente Instanzen eigenständig im Internet bewegen.

4. Sehr viel mehr Leistung, sehr viel mehr IT-Intelligenz

Heute werden Rechner zwar immer schneller, aber noch nicht wirklich intelligenter. Wenn ich heute PowerPoint aufrufe, dann werden mir zwar einige hilfreiche Features angeboten, aber Denken muss ich noch selber. Wenn ein heutiger Prozessor eine Intelligenz einer Fliege wiederspiegelt, dann werden die Prozessoren in 10 Jahren die Intelligenz eines Menschen anbieten können. Wenn ich in 10 Jahren eine PowerPoint-Präsentation über IT-Sicherheit vorbreiten möchte, werde ich das meinem PowerPoint-Agenten sagen, und er wird mir einen guten Vorschlag unterbreiten, möglicherweise auch einige Alternativen. Er wird sich ansehen, was ich in den letzten 30 Jahren schon alles gemacht habe, er wird im Internet suchen, was es an aktuellen Themen gibt und welche anderen Informationen in diesem Bereich zur Verfügung stehen. Ähnlich wie ein menschlicher Assistent, der mich schon einige Zeit kennt, wird er meine Vorlieben an Farben, Gestaltung und Dynamik berücksichtigen.

Wenn ich meine Präsentation halten muss, dann werde ich meinen Speicher-Agenten bitten, dies zu organisieren und auf der in der Nähe stehenden Monitorwand anzeigen zu lassen. Mein Speicher-Agent wird auch dafür sorgen, dass am Ende die Präsentation in der Monitorwand nicht reproduzierbar gelöscht wird.

Wenn ich meinen E-Mail-Client aufrufe, dann wird mir von meinem E-Mail-Agenten mitgeteilt, dass ich 80 E-Mail hatte, von denen 45 schon beantwortet werden konnten, 15 gelöscht wurden, weil sie „Spam“ waren, bei 10 E-Mails wird mir ein Vorschlag für die mögliche Antwort unterbreitet, bei 5 E-Mails muss ich einen geeigneten Hinweis geben, damit der E-Mail-Agent einen Vorschlag erarbeiten kann und 5 E-Mails sind privat, um die ich mich selbst kümmern kann. Wenn ich will, kann ich diese E-Mail von meinem Private-Agenten bearbeiten lassen.

**Neue Angriffsmodelle und neue IT-Sicherheitsmechanismen**

Die Angriffsmodelle werden sich wieder ändern und deutlich raffinierter und komplexer werden. Z.B. der Zugriff auf einen intelligenten Agenten von mir, kann Antworten geben, die sonst nur ich geben kann. Damit haben wir eine neue Dimension von IT-Angriffen auf Intelligenzen.

Die IT-Sicherheitsmechanismen, die hier gebraucht werden, müssen sehr objektorientiert auf vertrauenswürdigen Instanzen für eine hohe und verteilte IT-Sicherheit sorgen. Meine Daten, meine Informationen, mein Wissen und meine IT-Intelligenzen werden sich irgendwo im Internet sicher und verfügbar befinden müssen. Der Zugriff darauf wird 100% gewährleistet sein müssen.

## 5 Zusammenfassung

Die Werte und auch die Abhängigkeiten, die über IT zur Verfügung stehen, werden weiter rasant steigen und bekommen mit IT-Intelligenzen in der Zukunft eine neue Dimension. Gleichzeitig wird damit auch, wie in der Vergangenheit, das Angriffspotential sehr stark wachsen. Die Herausforderungen der IT-Sicherheit im Lauf der Zeit werden immer größer, internationaler und sehr viel komplexer. Da aber nur bei einer angemessenen IT-Sicherheit und Vertrauenswürdigkeit der IT-Systeme und -Dienste diese genutzt werden, müssen wir uns den Herausforderungen stellen und passende innovative IT-Sicherheitslösungen entwickeln und zur Verfügung stellen. Nur so können wir unseren Platz in der vernetzten Wissens- und Informationsgesellschaft finden.

## Literatur

[1] N. Pohlmann, C. Ruland: "Datensicherheit bei Kommunikation über Datex-P", DATACOM – Fachzeitschrift für die elektronische Datenkommunikation, DATACOM-Verlag, 01/1989

[2] S. Dierichs, N. Pohlmann: „Netz-Deutschland“, iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 12/2005

[3] N. Pohlmann: "Firewall-Systeme - Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrution Detection-System, Personal Firewalls", MITP-Verlag, Bonn 2003

[4] D. Petersen, N. Pohlmann: „Seeming Secure Layer – Erschreckende Sicherheitsdefizite bei Internet-Anwendungen”, iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 01/2009

[5] M. a Campo, N. Pohlmann: "Virtual Private Network (VPN)“, MITP-Verlag, Bonn 2003

[6] N. Pohlmann, Helmut Reimer: "Trusted Computing - Ein Weg zu neuen IT-Sicherheitsarchitekturen”, Vieweg-Verlag, Wiesbaden 2008