

# Vertrauenswürdige Netzwerkverbindungen mit Trusted Computing

## Sicher vernetzt?

**Die Zeiten in denen per Post alle wichtigen Informationen von Firma zu Firma oder Niederlassung gesendet wurden sind gezählt. Für besonders sichere Sendungen wurde ein eigener Postdienst genutzt. E-Mail und verteilte Netze bieten für die grundlegende Übermittlung von Informationen schon heute eine Abbildung der Aufgaben der Post in der elektronischen Welt. Es bleibt die Frage wie es möglich ist Vertrauenswürdigkeit und Sicherheit auf hohem Niveau zu gewährleisten.**

Mitarbeiter nutzen ihr Notebook zuhause oft ohne wirkungsvolle Schutzmaßnahmen. Daraus folgt eine erhöhte Gefahr der Kompromittierung, wie der Zeitraum für die Ausnutzung von neu bekannten Schwachstellen in Softwaresystemen (derzeit 6,4 Tage, Tendenz sinkend) eindrucksvoll beweist. Zurück im Unternehmen schleusen sie so unbewusst Viren und andere Malware, vorbei an Firewalls und Virensclannern, ins Firmennetz ein.

Problematisch ist, dass es heutzutage nur wenige, sinnvolle Möglichkeiten der Absicherung von Intranets gibt und diese dem Anspruch hoher Sicherheit nicht gerecht werden. Methoden des Zugriffschutzes von Netzwerken, wie z.B. VPN, basieren auf reiner Nutzerauthentifizierung und bieten nicht die Möglichkeit der Überprüfung der Vertrauenswürdigkeit der für den Zugriff genutzten Geräte.

Diese Sicherheitsproblematik ist allerdings noch wesentlich globaler zu betrachten. Statische Netz-Infrastrukturen mit klaren Systemgrenzen sind in den vergangenen Jahren heterogenen und dynamischen Netzen gewichen. Klassische, örtlich begrenzte Intranets verteilter Niederlassungen auf der ganzen Welt werden zu großen Firmennetzen zusammengeschaltet (z.B. Autohersteller mit Zweigstellen und Geschäften). Heimarbeiter oder Außendienstmitarbeiter benötigen einen sicheren Zugriff auf Daten im Firmennetz. Durch die Vielzahl von Verbindungspunkten und deren räumliche Distanz ist der Aufwand eines komplett eigenständigen physikalischen Netzwerks (Corporate Network), nicht mehr zu rechtfertigen. Die einzige und kostengünstigere Alternative bietet hier das Internet, dessen umfassende behördliche und industrielle Nutzung im Sicherheitsbereich durch den Mangel an Sicherheit nur eingeschränkt nutzbar ist.

Heutige Netzwerke erfordern somit neue Konzepte um sichere Kommunikation zu ermöglichen. Dazu gehört die Nutzung von „intelligenten Netzwerkgeräten“, die die Vertrauenswürdigkeit der angeschlossenen Geräte garantieren und somit die Gefahr durch kompromittierte oder vorgetäuschte Geräte minimieren können.

Diese neuen Konzepte verlagern also die Aktionen zum Schutz des Netzes auf die im Netz angeschlossenen Geräte. Zusätzlich findet ein Wechsel von der Reaktion auf Gefahren hin zur Prävention statt. Während heutzutage ein Intrusion-Detection-System (IDS) versucht anhand von abnormalen Messwerten im Netzwerkverkehr kompromittierte Geräte zu erkennen, d.h. ein durch Malware infiziertes Gerät muss sich erst „falsch“ verhalten bevor es entdeckt wird (Reaktion), verhindern die neuen Konzepte, dass Computersysteme aufgrund einer fehlerhaften Konfiguration und somit einer eventuellen Kompromittierung überhaupt in das Netz gelangen können (Prävention).

### Trusted Network Connect (TNC)

An dieser Stelle setzt die Trusted Network Connect (TNC) Spezifikation der Trusted Computing Group (TCG) [TCG06] an. Anwendungen auf Basis der Spezifikation können die Integrität (Vertrauenswürdigkeit) der angeschlossenen Endgeräte in einem Netzwerk überprüfen und anhand dieser Prüfung den Zugriff auf das Netzwerk gewähren oder ggf. unterbinden. Als nicht-vertrauenswürdig eingestufte Geräte können bis zu der Wiederherstellung der Integrität vom restlichen Netz isoliert werden. Die Prüfung der Vertrauenswürdigkeit kann alle Systemkomponenten der Endgeräte umfassen. So können auf der Hardwareebene die angeschlossenen Geräte mit ihrer Firmware und auf Applikationsebene die eingesetzte Software mit deren Konfigura-

tion überprüft werden. Welche Konfiguration aus Hard- und Software in einem Netzwerk erlaubt ist, kann vom Netzbetreiber über Policies festgelegt werden. Diese Policies können beispielsweise die Präsenz eines Virensclanners mit aktueller Virensignatur vorschreiben oder die Nutzung lokal angeschlossener Drucker verbieten.

Um eine Vertraulichkeitsprüfung durchzuführen, werden auf Client- (z.B. einem Notebook) und Serverseite Mechanismen zur Messung und Überprüfung der von den Policies vorgeschriebenen Parameter benötigt. Auf Clientseite müssen sogenannte „Integrity Measurement Collectors (IMC)“ für jede zu überprüfende Komponente Messdaten sammeln und diese zur Überprüfung an den Server senden. Dort vergleichen die „Integrity Measurement Validators (IMV)“ die Daten mit den in der Policy festgelegten Werten. Dieser Austausch von Messdaten erfolgt solange bis der Server eine Entscheidung über die Integrität, und somit über die Vertrauenswürdigkeit des Clients treffen kann. Durchgesetzt werden die Entscheidungen durch einen „Policy Enforcement Point (PEP)“. Ein PEP kann beispielsweise in einem Access Point eines WLAN-Netzes oder in einem Gateway integriert sein. Neben der Gewährung oder Verweigerung eines Zugriffs bietet TNC die Möglichkeit das Endgerät in einem geschützten Netzbereich zu isolieren. So kann ein eventuell kompromittiertes Gerät im Netzwerk keinen Schaden anrichten. Zusätzlich kann in diesem Bereich ein begrenzter Internet-Zugang ermöglicht werden um z.B. auf Patches und Virensignaturen zugreifen und nach einer erneuten Überprüfung erfolgreich Zugriff auf das Netz erhalten zu können. TNC ist darauf ausgerichtet, dass es vorhandene Technologien wie Virtual Private Networks (VPN) oder Authentifikationsverfahren wie

802.1x nutzt. Das heißt, dass vorhandene Systeme im Idealfall nicht ersetzt, sondern nur um die TNC-Funktionen erweitert werden müssen.

Zusätzlich bietet TNC eine optionale Anbindung an das Trusted Platform Module (TPM) der TCG. Dadurch wird über die eindeutigen

Microsoft und Cisco, sind grundsätzlich proprietär und selten kompatibel zueinander. Die TNC-Spezifikation bietet die z.Z. einzige offene Alternative. Diese Offenheit ermöglicht von vornherein eine Interoperabilität zu anderen TNC-konformen Produkten für sämtliche Hersteller und Plattformen.

norbert.pohlmann@informatik.fh-gelsenkirchen.de  
 Institut für Internet-Sicherheit  
 Fachhochschule Gelsenkirchen  
 Neidenburger Str. 43,  
 D - 45877 Gelsenkirchen  
 www.internet-sicherheit.de

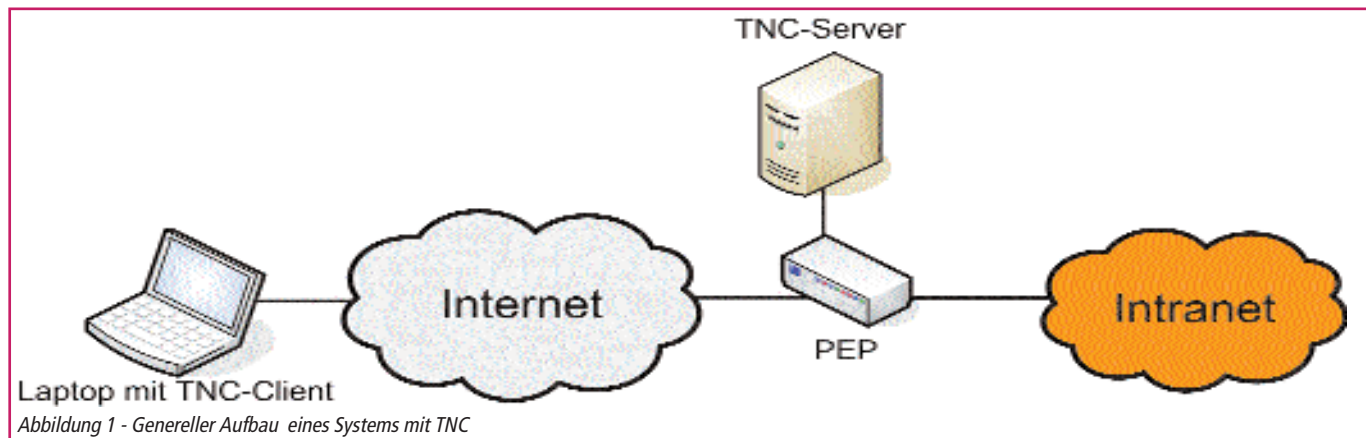


Abbildung 1 - Genereller Aufbau eines Systems mit TNC

Schlüssel des TPMs eine festen Zuordnung einer Verbindung (z.B. VPN) an ein bestimmtes System möglich.

### TNC Marktreife

Aufgrund der noch sehr jungen Spezifikation befinden sich keine TNC-kompatiblen Produkte auf dem Markt. Seit Anfang des Jahres 2006 haben mehrere Mitglieder der TCG wie Juniper Networks [JUN06] und Check Point eine Erweiterung ihrer Produkte um TNC-Funktionalität angekündigt. Anfang September 2006 hat Juniper zusätzlich eine Kooperation mit Symantec im Bereich TNC angekündigt [JUN062].

### Alternative Techniken

Neben dem TNC-Ansatz existieren weitere Ansätze einer sicheren Zugriffskontrolle; unter anderem Lösungen der Firmen Microsoft und Cisco. Microsoft verfolgt mit der „Network Access Protection (Microsoft NAP)“ eine eigene Lösung. NAP soll mit Microsoft Vista und der darauf aufbauenden Server-Version verfügbar sein. Die Steuerung des Netzwerkzugriffs erfolgt mittels vorhandener Technologien wie VPN oder 802.1x. Hierbei ist Microsoft NAP zwar hardwareunabhängig, setzt aber zwingend Software von Microsoft voraus. [MS04] Die „Network Admission Control (NAC)“ von Cisco ist Teil der „Self-Defending Network“-Strategie [NAC04]. Bei diesem Ansatz wird im ganzen Netz spezielle, NAC-fähige, Hardware benötigt. Alle alternativen Produkte, auch die von Mi-

### Fazit

Das Marktpotential von Lösungen auf Basis der TNC Technologie ist sehr groß. Die verstärkte Nutzung des Internets als auch die zunehmende Wichtigkeit von Intranets im Zusammenhang mit einer immer stärkeren Vermaschung zeigt, dass eine Erhöhung der Vertrauenswürdigkeit von Netzwerkverbindungen unabdingbar ist. Die TNC-Spezifikation der Trusted Computing Group könnte hier eine offene Alternative zu in Entwicklung befindlichen proprietären Lösungsansätzen bieten. Wichtig ist hierbei das TNC sein volles Potential nur mit Einsatz eines TPM erreichen kann da nur dann eine vertrauenswürdige Messung der Komponenten möglich ist.

Quellen:  
 [TCG06]: <https://www.trustedcomputinggroup.org>  
 [DuD02] Michael Hartmann - Trusted Network Connect - Netzwerkhygiene auf hohem Niveau, 2005  
 [NAC04] Cisco NAC – Network Admission Control - [http://www.cisco.com/global/AT/pdfs/prospekte/Security\\_CNAC\\_032004.pdf](http://www.cisco.com/global/AT/pdfs/prospekte/Security_CNAC_032004.pdf)  
 [JUN06] „Juniper Networks to Support Trusted Network Connect (TNC) Open Standards for UAC“ <http://www.juniper.net/company/press-center/pr/2006/pr-060501.html>  
 [JUN062] Juniper und Symantec gehen Allianz ein - <http://www.heise.de/newsticker/meldung/78113>  
 [MS04] Network Access Protection (NAP) <http://www.microsoft.com/germany/technet/sicherheit/newsletter/nap.msp>

Autoren: Marian Jungbauer  
 marian.jungbauer@internet-sicherheit.de  
 Prof. Dr. Norbert Pohlmann



### Datenschutzprüfungen durch die Aufsichtsbehörden

07.11.2006 in Hamburg  
 29.11.2006 in Köln

### Datenschutz Aktuell

09.11.2006 in Berlin  
 20.11.2006 in Köln

### 30. Datenschutzfachtagung (DAFTA) mit 25. RDV-Forum

15.-17.11.2006 in Köln

### Die ersten 100 Tage des betrieblichen Datenschutzbeauftragten

22.11.2006 in Berlin

### Datenschutz für Betriebsräte

11.-12.12.2006 in Köln

### Die praktische Umsetzung des Datenschutzes in Unternehmen

12.-13.12.2006 in Berlin

### Das Allgemeine Gleichbehandlungsgesetz: Auswirkungen auf die Datenschutzpraxis

28.11.2006 in Berlin  
 05.12.2006 in Stuttgart

weitere Informationen unter:  
 DATAKONTEXT-TAGUNGEN GmbH & Co. KG  
 Postfach 4128 · 50217 Frechen  
 Tel 02234/65633 oder 65638 · Fax 65635  
 tagungen@datakontext.com