

**Presseinformation vom 18. Februar 2010**

## **CeBIT 2010: Trend Micro präsentiert Sicherheit für die Cloud und virtuelle Umgebungen**

*Trend Micro Deep Security für physische, virtuelle und Cloud-basierende Server in Halle 11, D40; zahlreiche Vorträge zum Thema Sicherheit für virtualisierte Umgebungen*

**Trend Micro, Spezialist für Internet Content Security, präsentiert auf der CeBIT 2010 in Halle 11, D40 sein neuestes Angebot zur „Sicherheit für die Cloud“. Kern dieses Angebots bildet Trend Micro Deep Security, die erste Lösung am Markt überhaupt für den kompletten Malware-Schutz in dynamischen Rechenzentren. Darüber hinaus widmen sich die Trend Micro-Experten dem Thema Sicherheit in virtualisierten Umgebungen in zahlreichen CeBIT-Vorträgen.**

Laut Analystenberichten setzten 95 Prozent der Rechenzentren im Jahr 2009 Virtualisierungstechnologien ein. Gleichzeitig sind 60 Prozent der produktiven virtuellen Maschinen weniger sicher als physische Server, insbesondere weil sie speziellen Herausforderungen in Sachen Sicherheit ausgesetzt sind. Hinzu kommt: Durch Virtualisierungstechnologien und Cloud Computing verlassen Server den bisherigen Sicherheitsperimeter und werden unter Umständen zusammen mit unbekanntem oder infizierten Servern betrieben. Gefragt ist also ein umfassender Schutz für physische, virtuelle und Cloud-basierende Server.

Die Lösung Trend Micro Deep Security bietet diesen umfassenden Schutz durch eine modulare Architektur mit den folgenden Elementen: Deep Packet Inspection Engine inkl. Intrusion Detection/Prevention (IDS/IPS), Web Application-

Sicherheit und Anwendungskontrolle auf Netzwerkebene, Firewall, Integritätsüberwachung und Prüfung der Log-Einträge.

Version 7.0 von Trend Micro Deep Security enthält darüber hinaus virtuelle Sicherheitsappliances, die speziell für VMware VI3- und vSphere 4-Umgebungen konzipiert sind. Damit ist Trend Micro Deep Security 7.0 die erste Sicherheitslösung, die Schutzmechanismen auf Basis des VMsafe API direkt am Hypervisor mit zusätzlichen Sicherheitstechnologien auf virtuellen Maschinen koordiniert.

„Die VMsafe Security API ermöglicht Trend Micro, die inhärenten Eigenschaften der Virtualisierung in ihren Sicherheitsangeboten zu verwenden. Dieses offene Sicherheitskonzept ermöglicht ein Sicherheitsniveau in virtuellen Rechenzentren, das sich in herkömmlichen IT-Umgebungen nicht realisieren lässt, und Kunden erhalten die hoch sichere Plattform für die Virtualisierung geschäftskritischer Anwendungen: Skalierbarer Virenschutz ohne Agenten, Transparenz und kontinuierlicher Schutz virtueller Netzwerke. Wir freuen uns auf eine weiterhin gute Zusammenarbeit, um die Sicherheit in virtuellen Rechenzentren und Cloud-Umgebungen voranzutreiben“, sagt Martin Niemer, Group Manager Product Marketing bei VMware.

Mitenthalten in Version 7.0 sind ferner neue Funktionalitäten, um die Gesamtbetriebskosten durch ein verbessertes Management und vereinfachte Compliance zu senken. Zu diesen Funktionalitäten gehören unter anderem Event Tagging, um bessere Workflows zur Bearbeitung von Sicherheitsvorfällen zu ermöglichen, sowie die Definition eines „Referenzsystems“ oder Normalzustands, um die Zahl der False Positives zu reduzieren, die das Resultat gewöhnlicher System-Updates wie Patching sind. Weitere Verbesserungen sind Integritätsüberwachung, Prüfung der Log-Einträge und SIEM (Security Information & Event Management)-Integration.

## CeBIT-Vorträge: Sicherheit für virtualisierte Umgebungen

Dem Thema Sicherheit für virtualisierte Umgebungen widmet sich Trend Micro im Rahmen des mehrmals präsentierten Vortrags „Herausforderungen der Virtualisierungs-Sicherheit“:

- Virtualisation & Storage Forum, Halle 2, A30
  - Dienstag, den 2. März, 14.30 Uhr bis 14.50 Uhr
  - Mittwoch, den 3. März, 12 Uhr bis 12.20 Uhr
  - Donnerstag, den 4. März, 12.30 Uhr bis 12.50 Uhr
  - Freitag, den 5. März, 11 Uhr bis 11.20 Uhr
  - Samstag, den 6. März, 10 Uhr bis 10.20 Uhr
  
- Security World Konferenz, Convention Center, Raum 13/14
  - Donnerstag, den 4. März, 14.15 Uhr bis 15 Uhr
  
- CeBIT Kompetenz Studio – Live-Ausstrahlung, Studio Mittelstand, Halle 2, B31
  - Mittwoch, den 3. März, 10 Uhr bis 10.20 Uhr

### Über Trend Micro

Trend Micro, einer der international führenden Anbieter für Internet-Content-Security, richtet seinen Fokus auf den sicheren Austausch digitaler Daten für Unternehmen und Endanwender. Als Vorreiter seiner Branche baut Trend Micro seine Kompetenz auf dem Gebiet der integrierten Threat Management Technologien kontinuierlich aus. Mit diesen kann die Betriebskontinuität aufrechterhalten und können persönliche Informationen und Daten vor Malware, Spam, Datenlecks und den neuesten Web Threats geschützt werden. Unter <http://blog.trendmicro.de> informieren sich Anwender zu aktuellen Bedrohungen. Die flexiblen Lösungen von Trend Micro sind in verschiedenen Formfaktoren verfügbar und werden durch ein globales Netzwerk von Sicherheits-Experten rund um die Uhr unterstützt. Zahlreiche Trend Micro-Lösungen nutzen das Trend Micro™ Smart Protection Network™, eine wegweisende Cloud-Client-Infrastruktur, die für den Echtzeit-Schutz vor aktuellen und neuen Bedrohungen innovative, Cloud-basierende Reputationstechnologien und Feedback-Schleifen mit der Expertise der TrendLabs-Forscher kombiniert. Trend Micro ist ein transnationales Unternehmen mit Hauptsitz in Tokio und bietet seine Sicherheitslösungen über Vertriebspartner weltweit an. Weitere Informationen zu Trend Micro finden Sie im Internet unter [www.trendmicro.de](http://www.trendmicro.de).

#### Herausgegeben im Auftrag von:

Trend Micro Deutschland GmbH  
Hana Göllnitz  
Zeppelinstr. 1  
D-85399 Hallbergmoos  
Tel.: +49(0) 811 88 99 0 – 863  
Fax: +49(0) 811 88 99 0 – 799  
E-Mail: [hana\\_goellnitz@trendmicro.de](mailto:hana_goellnitz@trendmicro.de)  
Internet: [www.trendmicro.de](http://www.trendmicro.de)

#### Pressekontakt:

phronesis PR GmbH  
Marcus Ehrenwirth, Magdalena Brzakala  
Max-von-Laue-Str. 9  
D-86156 Augsburg  
Tel.: +49 (0) 821 444 800  
Fax: +49 (0) 821 444 80 22  
E-Mail: [info@phronesis.de](mailto:info@phronesis.de)  
Internet: [www.phronesis.de](http://www.phronesis.de)