– Presseinformation der Controlware GmbH –

Praxistipps der Controlware Experten:
Virtuelle IT-Umgebungen methodisch absichern

Dietzenbach, 16. März 2010 – Controlware, renommierter deutscher Systemintegrator und IT-Dienstleister, konzipiert und realisiert Security-Architekturen für virtuelle IT-Umgebungen. So komplex die Aufgabenstellung ist: Die wichtigsten Grundprinzipien der Absicherung virtueller Umgebungen lassen sich in zehn kurzen Tipps zusammenfassen.

1. Virtualisierung ist Teamwork

In großen Unternehmen übernehmen oft die Server-Administratoren die führende Rolle in Virtualisierungsprojekten. Die Security-Verantwortlichen werden zu spät oder gar nicht hinzugezogen. Die Folge: Neue Systeme werden nicht Policy-konform konfiguriert und weisen zum Teil gravierende Sicherheitslücken auf. Binden Sie das Security-Team bereits in den ersten Projektphasen in die Konzeption ein!

2. Passen Sie Ihre vorhandene IT-Security an die virtuelle Umgebung an

Bewährte Firewall- und IPS/IDS-Lösungen (Intrusion Prevention/Detection System) sowie Virenschutzprodukte sind für die Absicherung virtueller Umgebungen unverzichtbar. Voraussetzung ist, dass die Konfiguration der Security-Systeme an die neuen Gegebenheiten angepasst und wo notwendig konzeptionell erweitert wird.

3. Nutzen Sie alle Sicherheitsfunktionen Ihrer virtuellen Systeme

Führende Virtualisierungshersteller haben das Thema Sicherheit lange vernachlässigt. Das ändert sich jetzt. Viele Virtualisierungslösungen werden aktuell mit Sicherheits-Features ausgestattet, exemplarisch sei die VMsafe-Schnittstelle von VMware genannt. Halten Sie sich unbedingt über neue Versionen und Funktionalitäten auf dem Laufenden!

Controlware GmbH
Waldstraße 92 • D-63128 Dietzenbach
Tel.: +49 6074 858-00 • Fax: +49 6074 858-220

4. Arbeiten Sie eng mit Ihren Security-Lieferanten zusammen

Ebenso wie die Virtualisierungsanbieter bringen aktuell auch IT-Security-Hersteller verstärkt Sicherheitstechnologien für virtuelle Umgebungen auf den Markt. Bleiben Sie auch bei diesen Neuentwicklungen up to date!

5. Behalten Sie stets alle Angriffspunkte im Auge

Virtuelle IT-Infrastrukturen sind von mehreren Seiten angreifbar: Hacker können zum Beispiel die virtuellen Systeme oder den Hypervisor attackieren oder die virtuellen Maschinen als Zugangstor zum Netzwerk missbrauchen. Es gilt, alle Angriffspunkte im Auge zu behalten – etwa indem Sie Ihre virtuelle Umgebung regelmäßig nach Hypervisor-Rootkits durchsuchen!

6. Regeln Sie die Zugriffsrechte

Definieren Sie für virtuelle IT-Umgebungen eindeutige, rollenbasierte Zugriffsrichtlinien und setzen Sie diese beispielsweise mithilfe einer Network Access Control (NAC)-Lösung und starker Mehr-Faktor-Authentisierung durch. Nur so können Sie verhindern, dass etwa Mitarbeiter oder Dritte virtuelle Maschinen kopieren oder Snapshots freigeschalteter Systeme anfertigen!

7. Verschlüsseln Sie

Tipp für sicherheitskritische Umgebungen: Setzen Sie geeignete Verschlüsselungsverfahren in Ihrer virtuellen IT-Infrastruktur ein, um die virtuelle Umgebung vor Lauschangriffen und Man-in-the-Middle-Attacken zu schützen.

8. Implementieren Sie physikalische Zugangskontrollen

Virtuelle Systeme sind mobil: Hat ein Datendieb Zugang zum Serverraum, kann er VMs einfach auf einen USB-Stick ziehen und herausschmuggeln. Dies lässt sich mit physikalischen Zugangskontrollen wie 3D-Gesichtserkennung oder Venen- und Iris-Scannern wirkungsvoll unterbinden.

9. Sparen Sie nicht an der Hardware

Nur stabile Systeme sind auch sichere Systeme. Billig-Server sind ein schlechtes Fundament für virtualisierte Umgebungen. Investieren Sie in Markenkomponenten, damit die Hardware nicht zum Single-Point-of-Failure wird.

10. Ziehen Sie erfahrene Virtualisierungs- und IT-Security-Experten zu Rate

Die Umstellung auf virtuelle Server und die Absicherung der Netzinfrastrukturen sind äußerst komplexe Aufgabenstellungen, mit denen Sie die Weichen in Ihrem Rechenzentrum auf Jahre hinaus stellen. Suchen Sie sich dafür einen erfahrenen Partner, der als Systemintegrator sowohl im Bereich Virtualisierung als auch im Bereich IT-Security hohe Kompetenz besitzt und herstellerunabhängig agiert.

ca. 4.000 Zeichen (inkl. Leerzeichen)

Über Controlware GmbH

Die Controlware GmbH, Dietzenbach, ist einer der führenden unabhängigen Systemintegratoren in Deutschland. Das 1980 gegründete Unternehmen unterstützt seine Kunden mit Komplettlösungen und Dienstleistungen in der Informationstechnologie. Das Portfolio erstreckt sich von der Beratung und Planung über Installation und Wartung bis hin zu Management, Überwachung und Betrieb von Kundennetzen durch das firmeneigene Network Operating Center. Zentrale Geschäftsfelder der Controlware sind die Bereiche Communication Solutions, Information Security, Physical Security, IT-Management und Application Delivery. Controlware unterhält als Systemintegrator enge Partnerschaften mit national wie international führenden Herstellern sowie mit innovativen Newcomern der Branche. Das 580 Mitarbeiter starke Unternehmen verfügt mit elf Standorten in Deutschland über ein bundesweit flächendeckendes Vertriebs- und Servicenetz und ist mit eigenen Niederlassungen in Europa, Nordamerika, Asien und Australien vertreten. Zu den Tochterunternehmen der Controlware zählen die Networkers AG, die ExperTeach GmbH und die Productware GmbH.

Pressekontakt:
Stefanie Zender
Controlware GmbH
Tel.: +49 6074 858-246
Fax: +49 6074 858-220
e-mail: stefanie.zender@controlware.de
www.controlware.de (Homepage)

Belegexemplare bitte an:
Bernd Jung
H zwo B GmbH
Tel.: +49 9131 81281-22
Fax: +49 9131 81281-28
e-mail: info@h-zwo-b.de
www.h-zwo-b.de (Homepage)