COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/mehr-sicherheit-durch-virtualisierung,2496453

Thomas Masicek, T-Systems:

Mehr Sicherheit durch Virtualisierung

Datum: 29.09.2011
Autor(en): Edmund E. Lindau

Kostendruck, Virtualisierung und die Einbindung mobiler Endgeräte sind für viele IT-Sicherheitsverantwortliche die größten Herausforderungen. Wie er diese Aufgaben meistert, schildert der T-Systems-Sicherheitsexperte und Country Security Officer Thomas Masicek im Interview.

CW: In der Vergangenheit wurde die Verfügbarkeit der IT durch teure redundante Komponenten und Ausfallstandorte stark abgesichert. Inwieweit lassen sich diese Kosten reduzieren?

Foto: Thomas Masicek, T-Systems

Thomas Masicek: Ohne etabliertes **Risikomanagement**[1] ist im Unternehmen oftmals nicht bekannt, welche Systeme und Applikationen kritisch für wertschöpfende Prozesse sind und wie lange diese maximal stillstehen dürfen. Somit bleiben für Unternehmen ohne Risikomanagement zwei mögliche Strategien: Entweder die gesamte Infrastruktur vollredundant aufzubauen oder gar keine Maßnahmen zu implementieren.

Beide Varianten stellen keine probate Lösung dar, da entweder die Kosten im Vergleich zum Nutzen viel zu hoch angesetzt sind oder das Risiko für ein Unternehmen aufgrund der hohen Eintrittswahrscheinlichkeit, als auch des Schadenpotenzials Schiffbruch zu erleiden, viel zu hoch ist.

Zur Umsetzung eines Risikomanagements stehen eine große Auswahl an Methoden und Werkzeugen zur Verfügung. Die am weitesten verbreitete Norm für IT-Risikomanagement ist **ISO/IEC 27005:2008**[2], welche in engem Zusammenhang mit dem bekannten Standard ISO/IEC 27001:2005 steht.

CW: Wie kann der Sicherheitslevel in virtualisierten Umgebungen verbessert werden?

Masicek: Während für physische Server gut abgesicherte Rechenzentren zur Verfügung stehen, wird diese Absicherung von virtualisierten Systemen durch die eingesetzte Virtualisierungssoftware realisiert. Darin besteht jedoch ein großes Risiko: Wie in jedem Betriebssystem werden auch in den eingesetzten Virtualisierungsprodukten immer wieder Schwachstellen entdeckt, die es einem Angreifer ermöglichen, aus einer virtuellen Umgebung ausbrechen und Zugriff auf die darunterliegende Virtualisierungsplattform zu erlangen. Dadurch sind nicht nur die Daten der virtuellen Systeme, die in virtuellen Disks abgelegt sind, sondern auch die Konfigurationen der virtuellen Maschinen gefährdet, kopiert oder manipuliert zu werden.

Patchmanagement als Grundlage für angemessene Sicherheit

Die Grundlage zur Sicherstellung eines adäquaten Sicherheitslevels in virtualisierten Umgebungen besteht somit in einem regelmäßigen und zeitnahen **Patchmanagement**[3] der Gastsysteme, als auch der Virtualisierungsumgebung selbst. Jedes virtuelle System, gerade wenn es Zugriff auf das Internet, als auch Zugang zum internen Firmennetzwerk hat, muss ordnungsgemäß gepatched und mit einer aktuellen Software zum Schutz vor Viren versehen sein.

Ebenso stellt die Aktivierung der in den gängigen Betriebssystemen integrierten Firewalls eine wichtige Maßnahme zur Absicherung des Systems dar. Dadurch wird verhindert, dass ein Hacker über das Internet Zugriff auf ein virtuelles System erlangen kann. Sollte dies einem Angreifer dennoch gelingen, kann der Schaden durch eine regelmäßige Aktualisierung der **Virtualisierungsoftware**[4], als auch durch eine saubere Konfiguration der Virtualisierungsplattform in Grenzen gehalten werden.

CW: Wie können Unternehmen mit dem Wildwuchs mobiler Endgeräte und den damit verbundenen Sicherheitsrisiken umgehen?

Masicek: Mobile Devices stellen nicht nur aufgrund der darauf gespeicherten Daten ein Risiko dar, da diese Geräte wenn überhaupt oftmals nur durch einfache Sicherheitsmechanismen abgesichert sind. Grundsätzlich weisen **Mobile Devices**[5] denselben Schutzbedarf wie Laptops auf. Für Smartphones und Tablets muss deshalb eine durch den Benutzer nicht änderbare Policy implementiert werden: Schutz vor unberechtigter Inbetriebnahme mittels PIN/Passwort, die automatische Gerätesperre bei Inaktivität, eine regelmäßige Softwareaktualisierung sowie die Verschlüsselung sensibler Daten.

Die Möglichkeit, ein Smartphone aus der Ferne löschen zu können, ist ebenfalls hilfreich, wenn Geräte verloren gehen oder gestohlen werden. Wichtig ist ebenfalls, dass die unternehmensweite Nutzung von Mobile Devices in einer Richtlinie geregelt ist.

Dieser Beitrag erschien zuerst bei unseren Kollegen von **Computerwelt.at**[6].

Links im Artikel:

[1] **https://www.computerwoche.de/schwerpunkt/r/Risikomanagement.html**
[2] **https://www.computerwoche.de/security/1868064/**
[3] **https://www.computerwoche.de/schwerpunkt/p/Patch-Management.html**
[4] **https://www.computerwoche.de/subnet/citrix/**
[5] **https://www.computerwoche.de/security/2484575/index8.html**
[6] **http://www.computerwelt.at/detailArticle.asp?a=136860&n=4&n2=0**
