Ein Verlagsbeihefter der Heise Zeitschriften Verlag GmbH & Co. KG

iX extra Security

Sicherheit rund um die Cloud und die Virtualisierung

Veranstaltungen

1. – 5. März 2010, San Francisco
RSA Conference
www.rsaconference.com

2. – 6. März 2010, Hannover
CeBIT 2010
www.cebit.de

27. – 29. April 2010, London
Infosecurity Europe
www.infosec.co.uk

iX extra Security zum Nachschlagen:
www.heise.de/ix/extra/security.shtml

Wolken-schichten

Die vier Ebenen der Sicherheit in der Cloud

Bei der Nutzung von Diensten „aus der Wolke“ gehen mit den bestechenden Vorteilen neue Risiken einher, denn Anwender müssen sich damit abfinden, die Kontrolle über die Ressourcen abzugeben. Umso wichtiger ist es, alle Sicherheitsaspekte zu kennen – nur so kann man Service-Providern die richtigen Fragen stellen und eigene Schutzmaßnahmen umsetzen.

An der Beschäftigung mit dem Konzept des Cloud Computing kommt kein Unternehmen mehr vorbei. Nach dem Hype 2009 um die Dienste aus der Wolke nennen Fachleute wie die des Analystenhauses Gartner das Paradigma des Cloud Computing an erster Stelle der auch 2010 bedeutenden strategischen Technologien. Die Marktforscher definieren das Konzept als Computing-Stil, bei dem skalierbare und flexible, IT-gestützte Fähigkeiten als Dienst über das Internet an Kunden geliefert werden – sei es unternehmensintern oder extern.

Das National Institute of Standards and Technology (NIST) beschreibt die grundlegenden Charakteristika: Ein Konsument kann Ressourcen eines Cloud-Computing-Systems wie Rechenleistung oder Speicher nach seinem aktuellen Bedarf anfordern. Dafür steht ihm ein schneller Netzwerkzugriff zur Verfügung. Die Ressourcen des Wolkenanbieters sind in einem Pool zusammengefasst, aus dem er mit einem Mehrmandantenmodell verschiedene Konsumenten bedient. Diese Ressourcen können schnell, flexibel und unter Umständen automatisch bereitgestellt werden. Schließlich überwachen die Systeme automatisiert die Serviceausführung und optimieren die Nutzung.

Sicherheitsrelevante Bereiche

Trotz der Vorteile des Modells – geringere Investitionsrisiken, bessere Performance oder auch reduzierte Betriebskosten –, stellte das Marktforschungsinstitut IDC in einer Umfrage fest, dass sich viele Organisationen nicht zur Nutzung von Cloud Computing entschließen können. Hauptgründe sind Sicherheitsbedenken und die Gefahr der Verletzung gesetzlicher Richtlinien (fehlende Compliance).

Solange Unternehmen keine ausgereiften Sicherheitslösungen einsetzen können, die den grundlegenden Charakteristika von Cloud-Computing-Systemen angepasst sind, werden sie das volle Potenzial

der Cloud-Dienste auch nicht nutzen können, stellen Dr. Werner Streitberger und Angelika Ruppel, die Autoren der Studie des Fraunhofer Instituts für sichere Informationstechnologie „Cloud Computing Sicherheit“, fest. Durch den hohen Automatisierungsgrad der Systeme verlieren die Konsumenten nämlich die Kontrolle über die Ressourcen. Außerdem gibt es neue Schwachstellen und Bedrohungen, etwa wenn ein Angreifer die Rolle eines Anwenders übernimmt und Zugriff auf die Daten eines Konsumenten erlangt.

Die Fraunhofer-Studie soll die verschiedenen Sicherheitsfelder kategorisieren, die speziell in Cloud-Computing-Systemen eine Rolle spielen. Die Forscher definieren die vier Bereiche Infrastruktur, Anwendungen und Plattform, Verwaltung und Compliance. Sie orientieren sich dabei an den Schichten des Bezugsmodells.

Für am wichtigsten erachten die Autoren die Sicherheit der Infrastruktur, denn dabei geht es um die Kernkomponenten physikalische Sicherheit, Host, Virtualisierung und das Netzwerk. Im Allgemeinen haben Benutzer von Cloud-Diensten keinen Einfluss auf den Schutz dieser Komponenten, doch sollten sie sich der möglichen Sicherheitsbedrohungen auf dieser Ebene bewusst sein und bei der Wahl eines Providers dessen Security-Maßnahmen abfragen, so die Forscher. Die physikalische Sicherheit umfasst die Gebäude und Gebäudetechnik, wobei hier die Stromversorgung und Kühlung der Rechner, aber auch die Zutrittskontrolle am Gebäude, Videoüberwachung sowie Ort und Aufbau der Objekte relevant sind.

Im Mittelpunkt der Schutzmaßnahmen

Die zentralen Server stellen besondere Anforderungen an die Sicherheit im Hinblick auf den Schutz der verarbeiteten Daten, die Verfügbarkeit und die Zuverlässigkeit der Ausführung von Anwendungen. Gerade bezüglich des letztgenannten Aspekts hat es in der Vergangenheit Engpässe aufgrund der übermäßigen Nutzung von Ressourcen gegeben. Auslöser dafür waren unter anderem verteilte Denial-of-Service-Angriffe. Deshalb lautet die Empfehlung für Anwender, Provider nach Verfahren zur Verhinderung des „Verhungerns“ von Anwendungen zu fragen und nach Prozessen zum Isolieren unterschiedlicher Benutzerapplikationen voneinander. Des Weiteren sollten auch Maßnahmen zum Abschotten der Hosts zum Einsatz kommen und der Zugriff auf sie im Rechenzentrum sorgfältig geregelt sein.

Die Studie geht davon aus, dass Virtualisierung hauptsächlich zum Isolieren von Benutzerumgebungen dient. Deshalb stellt diese Technik einen wichtigen Grundbaustein dar. Bedrohungen auf dieser Ebene haben ihren Ursprung häufig in der Verwaltung der Zugriffsberechtigungen. Vor dem Einsatz von Cloud-Systemen muss genau festgelegt sein, welcher Benutzer Rechte für das Verwalten der virtuellen Maschinen hat, wie Dateiberechtigungen der Virtual Machines definiert sind und welche Rechte das Gastbetriebssystem besitzt. Im Rahmen der Netzwerksicherheit sollte der Cloud-Anbieter die Verfahren und Systeme zum Schutz des Netzwerks offenlegen, ebenso wie die Technologien, um Denial-of-Service-, Man-in-the-Middle-Angriffe oder Port Scanning zu verhindern.

Sicherheitsrisiken im Bereich der Anwendung und der Plattform entstehen bei der Entwicklung und Nutzung von Cloud-Diensten, stellen die Fraunhofer-Researcher fest. Ihren Ursprung können sie sowohl in der Infrastruktur als auch in der als Service bereitgestellten Anwendung und der dazu gehörigen Plattform haben. Hier geht es in erster Linie um die Sicherheit aller Informationen, einschließlich eventuell vorhandener Konfigurations- und Metadaten, die in Cloud-Systemen gespeichert, verarbeitet und zwischen den Systemen und deren Services ausgetauscht werden. Ziel ist die Gewährleistung der Vertraulichkeit und Integrität dieser Daten.

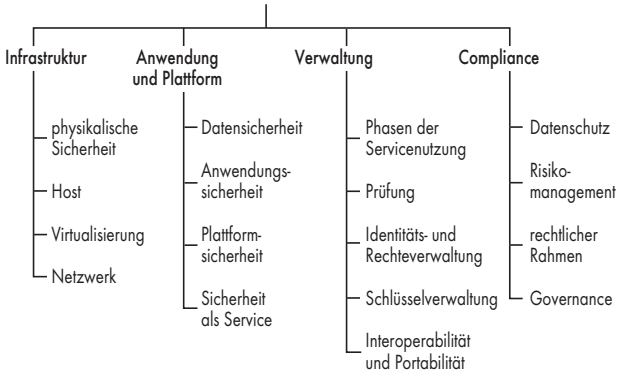
Cloud-Konsumenten empfiehlt die Studie, vor dem Übermitteln der Daten an den Cloud-Anbieter diese zu klassifizieren und genau festzulegen, welche der Anbieter speichern darf. Zusätzlich sollte feststehen, mit welchen Sicherheitsmaßnahmen Übermittlung und Speicherung der Daten erfolgen. Dies können Richtlinien sein, die ein Provider unterstützen muss. In den Sicherheits-Policies ist etwa die Verwendung bestimmter Verschlüsselungstechniken wie PKI (Public Key Infrastructure) vorgeschrieben. Üblicherweise tauschen dann Anbieter und Konsument die Schlüssel für die sichere Übertragung und Speicherung der Daten. Eine andere Möglichkeit wäre die sogenannte Datenminimierung, bei der der Konsument wichtige Informationen (Kundendaten) aus den Datensätzen, die in der Wolke verarbeitet werden, entfernt oder austauscht und nur unternehmensintern vorhält.

Der Schutz von Anwendungen umfasst die Berücksichtigung von Sicherheitsaspekten bei der Entwicklung von Services, aber auch für den authentifizierten Zugang zu den Cloud-Diensten. Neben Vertraulichkeit und Integrität geht es dabei um die Gewährleistung der Verfügbarkeit und Authentizität. Vier Bereiche seien hier relevant, stellen die Autoren fest:

– Nachrichten: Die Übertragung sollte verschlüsselt und unter Verwendung von Webservice-Sicherheitsstandards (zum Beispiel WS-Security) erfolgen. Ein Schutz gegen erneutes Verschicken derselben Nachricht (Replay-Angriff) muss vorhanden sein. Zusätzlich ist es wichtig, dass die Messages signiert sind und gegen ein Schema (etwa XML-Schemastandards) validiert werden, um zum einen den Sender identifizieren und zum anderen fehlerhafte Nachrichten vor der Verarbeitung erkennen zu können.

– Sitzung: Anbieter protokollieren häufig die Sitzungen (Zeitspanne zwischen dem Aufbau und dem Abbruch der Verbindung zur Cloud) mit, um auf dieser Basis abzurechnen. Hier gilt es, eine böswillige Übernahme einer nicht mehr aktiven Sitzung zu verhindern.

Taxonomie der Sicherheitsaspekte von Cloud-Computing-Systemen



Quelle: Fraunhofer SIT

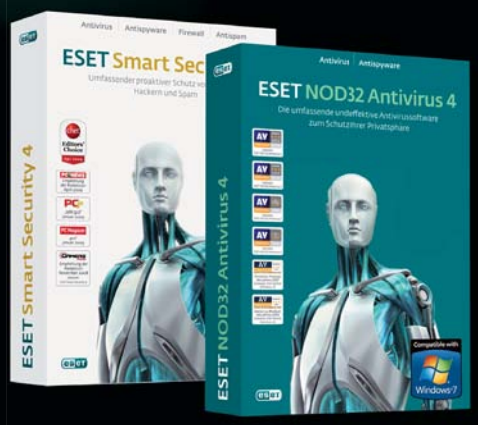
CeBIT

HANNOVER
2.– 6. 3. 2010
cebit.com

Besuchen Sie uns!
Halle 11 Stand D36

IT-Profis der ganzen Welt setzen auf ESET!

IT-Experten der ganzen Welt wählen ESET zum Nr.1-Unternehmen in der Security Software Branche*



ESET Smart Security 4
Antivirus/ Antispyware/Personal Firewall/Antispam

ESET NOD32 Antivirus 4
Antivirus/ Antispyware

Evaluierungslizenzen jetzt anfordern!

eset®

*Ergebnis der Marktanalyse von United Consultants im 2009
* 125 Millionen Computer weltweit werden durch ESET geschützt

www.eset.de

– Konfiguration: Es muss ein Schutz gegen böswillige Veränderung der Konfiguration vorhanden sein, beispielsweise durch eine spezielle Administrationsschnittstelle, die nur wenigen Benutzern zugänglich ist.
– Ausnahmen: Sogenannte Exceptions dürfen andere, nicht betroffene Benutzer bei der Ausführung der Services nicht beeinträchtigen.

Entwicklung vor Angriffen schützen

Zu den weiteren Bedrohungen der Anwendungssicherheit gehören Malware-Infektionen, Medienbrüche bei der Datenverarbeitung durch die Anwendung, der bereits erwähnte Man-in-the-Middle-Angriff oder andere Risiken für Webanwendungen.

Plattformsicherheit muss man vor allem Entwicklern von Cloud-Diensten bieten, die etwa Microsoft Azure, Google App Engine oder Force.com für ihre Arbeit nutzen. Sie können von deren Sicherheitsfunktionen profitieren – oder im Fall einer Bedrohung davon betroffen sein. Hier ist das Isolieren der Anwendung und Daten eine essenzielle Forderung. Genauso wichtig ist aber der Einsatz von sicheren Entwicklungsprozessen seitens der Plattform.

Vor allem neuartige Angriffsvarianten auf der Grundlage sogenannter Seitenkanalattacken stellen eine Gefahr dar. Seitenkanalattacken sind auf Messungen (etwa des Stromverbrauchs oder der benötigten Rechenzeit) und Dateninterpretation beruhende Angriffe auf Hardware-Sicherheitsmodule, werden aber auch leider erfolgreich zur Überwindung der Isolation der Benutzerumgebungen eingesetzt.

Als nächsten Bereich auf dieser Schicht nennt das Fraunhofer-Institut Sicherheit als Service. Sie umfasst verschiedene Modelle, mit denen der Anbieter Sicherheitsfunktionen als Mehrwertdienst, den meist ein Cloud-Benutzer bezahlt, den bestehenden Maßnahmen hinzufügen kann. Damit soll ein zusätzlicher Schutz entstehen, ohne dass der eigentliche Dienst geändert wird. Diese Art von Services bieten entweder die Cloud-Provider selbst an oder vertrauenswürdige Dritte. Beispiele dafür gibt es im Bereich Identitäts- und Zugangsverwaltung durch Single-Sign-On-Services oder in der Verwaltung der Instanzen eines Dienstes, um gleichbleibend hohe Verfügbarkeit zu gewährleisten.

Eine der größten Herausforderungen vom Standpunkt der Sicherheit stellt der Studie zufolge die Verwaltung der Cloud-Services selbst dar. Das liegt zum einen daran, dass Cloud-Anbieter diesen Bereich derzeit noch unzureichend unterstützen, zum anderen stehen den Benutzern noch keine Werkzeuge zur Verfügung, mit denen sie eine integrierte und effiziente Verwaltung ihrer Services durchführen können. Die Forscher gehen davon aus, dass es auch noch einige Zeit dauern wird, bis dieser Mangel behoben ist.

Susanne Franke ist freiberufliche IT-Fachjournalistin und Übersetzerin.

Unbeschwert auf Wolken

Informationssicherheit und Software as a Service

Unternehmen, die sich für Cloud Computing als Alternative zum Eigenbetrieb von Hard- und Software interessieren, müssen ihre Sicherheitskonzepte sorgfältig auf das neue Modell abstimmen. Je intensiver die Nutzung von Software as a Service ausfallen soll, desto höher ist der Anfangsaufwand für organisatorische und technische Sicherheitsmaßnahmen.

In „Software as a Service“ (SaaS) sehen viele Unternehmen erhebliches Einsparpotenzial. Die Verantwortlichen wollen weniger in IT investieren und keine eigenen Ressourcen dafür bereitstellen, sondern vielmehr IT-Leistungen als Betriebsausgaben verbrauchsabhängig abrechnen. Es geht zum Beispiel um die Flexibilität, Anwendungen abhängig vom Bedarf „aus der Cloud“ hinzubuchen und wieder abbestellen zu können. Die Angebote dazu reichen vom Bereitstellen von Speicherplatz bis hin zu komplexen Anwendungen jeder Art – Office-Lösungen, E-Mail, Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), Supply Chain Management, Informations- und Ressourcenmanagement sowie Business Intelligence.

Informationssicherheit und Datenschutz geraten durch diesen Trend in eine schwierige Situation: Während aus Compliance-Gründen und aus dem Zwang zur Risikovorsorge heraus immer mehr Kontrolle über IT-Infrastruktur, Daten und Anwendungen gefragt ist, verlagern sich die Unternehmen gleichzeitig aus finanziellen Gründen auf Betriebsformen, die die Voraussetzungen für die klassischen Kontrollmechanismen eines Administrators verschlechtern. Ein Beispiel für solche Betriebsformen ist die beschriebene Nutzung von Cloud Computing, ein anderes die zunehmende Einbindung von privaten Notebooks und mobilen Endgeräten in Firmennetze.

CIOs und CSOs bleibt also nichts anderes übrig, als ihre Sicherheitsstrategien für Konzepte zu öffnen, in denen eine vollständige technische Überwachung und Steuerung unternehmenskritischer Infrastrukturen erschwert ist. Im Falle der SaaS-Nutzung zieht dies organisatorische Maßnahmen und eine verstärkte Verlagerung auf vertragliche Formen der Risikovorsorge nach sich.

Datenrückholung muss möglich sein

Die European Network and Information Security Agency (ENISA) hat zu diesem Themenkreis im November 2009 die Risikoanalyse „Cloud Computing – Benefits, Risks and Recommendations for Information Security“ durchgeführt (www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment). Neben dem allgemeinen Kontrollverlust zählt sie eine Reihe weiterer Risiken auf. Der erste Punkt betrifft die Gefahr, vom Dienstleister abhängig zu werden, wenn die Portabilität der ausgelagerten Daten nicht gewährleistet

TWINBLADE™

HÖCHSTE DICHTE MIT 0.35HE PRO NODE

Leistungsstark.
Intelligent.

Mit der neuen BladeServer Familie steht eine umfassende Auswahl für jede Anwendungsapplikation zur Verfügung. Der neue TwinBlade™ Server arbeitet mit 10 Doppel Bladeeinschüben und je zwei Intel® Xeon® Prozessoren 5500/5600.

Somit kann der TwinBlade™ an die erforderliche Leistung, Skalierbarkeit und Flexibilität ideal angepasst werden. Maximale Dichte und rechenbetonte Leistung unterstützt der TwinBlade™ in einem 7 HE Rackmount Gehäuse. Somit ergibt sich pro Nodes eine Dichte von 0.35HE/Node.

Zusätzliche Kostenersparnisse werden durch eine einfache Wartung und dem internen Management erzielt. Durch Strom und platzsparende Komponenten wird der ROI (Return-of-Invest) schon nach wenigen Monaten erreicht.

CPI Eagle TwinBlade™ 710E

- 19"/7 HE Rackmount
- Max. 10 Doppel-Blade Einschübe
- Zwei Intel® Xeon® Prozessoren 5500/5600 Quad-/Hexa-Core, 240 Cores pro Blade Gehäuse
- Intel® 5500 Chipsatz
- 256 GB DDR3 ECC reg. Speicher pro TwinBlade™ Einschub
- Max. 4x 2000 Watt red. Netzteile (93 % hoch Effizient)
- Management Modul mit KVM-over-IP
- Redundante Gigabit Ethernet, 10-Gigabit Ethernet, Fibre Channel over Ethernet (FCoE) oder Infiniband Switches

CeBIT
HANNOVER, GERMANY
2–6 MARCH 2010
SUPERMICRO STAND
HALLE 17, STAND D70

Testen Sie unseren SERVER KONFIGURATOR

CPI Computer Partner Handels GmbH
Kapellenstr. 7
D - 85622 Feldkirchen/München

Telefon +49 (0)89 - 96 24 41-0
Telefax +49 (0)89 - 96 24 41-33
Hotline 0800 - 100 82 69
E-mail sales@cpigmbh.de

CPI server&storage

www.cpigmbh.de

ist. Der Aufwand, die Daten in eigene Systeme zurückzuführen oder sie einem anderen Service-Provider zu übergeben, wird dann zu hoch, und die gewünschte Flexibilität und das Einsparpotenzial sind gefährdet. Eine zusätzliche Schwierigkeit entsteht, wenn man beim Anbieter eine sichere Isolierung der eigenen Daten, Management-Zugänge und weiterer Ressourcen von denen anderer Kunden durchsetzen will.

Die ENISA-Autoren verweisen beispielsweise darauf, dass virtuelle Platten mehrerer Kunden bei einem SaaS-Anbieter innerhalb des Bereichs einer einzigen LUN (Logical Unit Number) eines Storage Area Networks (SAN) liegen können. Ein Angreifer könnte das Mapping der Platten manipulieren und so Zugriff auf fremde Daten erhalten – ein unwahrscheinlicher, aber eben denkbarer Fall.

Ein weiterer kritischer Bereich ist der Studie zufolge die Compliance des Anbieters zu Vorgaben, die für den Kunden gelten. Dabei spielen vor allem die jeweiligen Datenschutzregeln eine wichtige Rolle. Noch komplizierter wird die Situation, wenn der Dienstleister selbst weitere fremde Dienstanbieter oder Webservices nutzt und in diesem Zusammenhang die Daten des Kunden unbekannten Dritten zugänglich macht.

Generell sieht die ENISA im Cloud-Modell allerdings nicht nur Risiken, sondern auch Vorteile – so können große Service-Provider für ihre Rechenzentren oft leistungsfähigere Sicherheitssysteme anschaffen als beispielsweise kleine Unternehmen und die Kosten verteilen. Dieser Vorteil betrifft insbesondere den kritischen Bereich der Applikationssicherheit, der nach Möglichkeit Mechanismen zur Betrugserkennung umfassen sollte.

Die Sicherheitsziele bleiben

Lagert ein Unternehmen den Betrieb von Anwendungen an externe Dienstleister aus, bleibt es dennoch prinzipiell für die vier wichtigsten Sicherheitsziele im Umgang mit Informationen verantwortlich: Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität der Daten.

Um die mit diesen Zielen verbundene Sorgfaltspflicht zu erfüllen, müssen Cloud-Anwender ihre Anbieter sorgfältig auswählen, deren Leistung überwachen sowie geeignete Verträge und Service-Level-Agreements aushandeln. Darüber hinaus müssen sie ihre Arbeitsorganisation anpassen und in Zusammenarbeit mit dem Dienstleister den Transport der Daten übers öffentliche Netz sichern, wobei auch die Management- und Reporting-Zugänge für die gebuchten Dienste eine Rolle spielen.

Die IT-Abteilungen kommen dabei nicht umhin, sich mit den Verantwortlichen für Qualitätsmanagement und mit Rechtsberatern abzustimmen. Wie komplex die Lage ist und wo die interne Technik Voraussetzungen schaffen muss, zeigt ein genauer Blick auf jedes der vier vertrauten Sicherheitsziele und seine spezifische Bedeutung im SaaS-Sicherheitsmodell.

Bei der Verfügbarkeit von Applikationen „as a Service“ denken die meisten SaaS-Kunden zunächst nur an Aspekte wie die Erreichbarkeit der Dienste, die Verarbeitungsgeschwindigkeit der produktiven und für die Sicherheit zuständigen Server, Speicherplatz, Bandbreite, Support, hinreichenden Service rund um die Uhr und eventuelle Backup-Fenster. Ein Teil dieser Anforderungen lässt sich mit vertrauten Techniken erfüllen, die auch der Anbindung von externen Büros und Partnerunternehmen dienen.

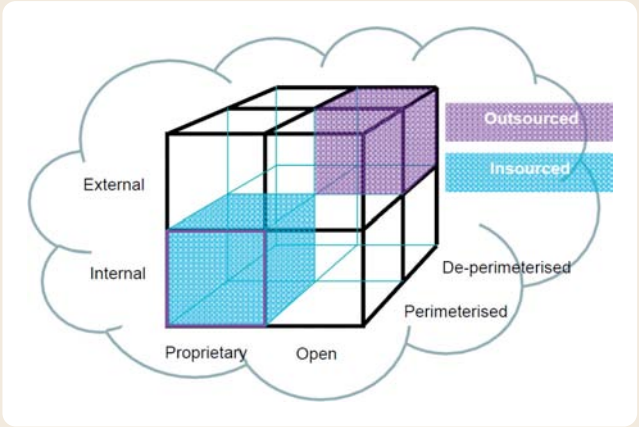
Die nötigen Service-Level-Agreements, die die übrigen Bereiche abdecken, können sich an Verträge anlehnen, wie sie für die Zusammenarbeit mit Hosting-Anbietern und Internet-Providern bestehen, sind aber weit umfangreicher und komplexer. Bei SaaS kommen zum Beispiel abhängig von der Art der gebotenen Leistung Verfügbarkeitsaspekte hinzu, die dann zutage treten, wenn die Zusammenarbeit nicht mehr funktioniert: Wie erhält der Kunde Zugriff auf Daten, die nur beim Anbieter gespeichert sind?

Die ständige Verfügbarkeit der Daten auch im Falle eines Versagens auf der Seite des Anbieters lässt sich mit möglichst häufigen Backups der Nutzdaten nach dem Prinzip der redundanten Datenhaltung in Repositories beim Kunden selbst oder bei einem weiteren Dienstleister sicherstellen. In diesen Zusammenhang gehört ein weiterer wichtiger Punkt, den unter anderem die erwähnte ENISA-Studie diskutiert: die fachgerechte Löschung der Daten. Wenn beispielsweise der Anbieter oder der Kunde seinen Betrieb einstellen muss oder das Verhältnis zwischen beiden Partnern gestört ist, muss sichergestellt sein, dass Informationen mit zertifizierten Löschtechniken unwiederbringlich von den Datenspeichern entfernt werden.

Beim Kunden selbst gilt, dass er die Verbindung ins Internet noch mehr als beim Eigenbetrieb als kritisches Strukturelement ansehen und redundant auslegen muss.

Vertraulichkeit, Integrität und Authentizität von Informationen in Verbindung mit der SaaS-Nutzung herzustellen, ist eine vielschichtige Herausforderung. In einem Risiko-Assessment für diesen Bereich muss der Anbieter eine ganze Liste von Fragen zufriedenstellend beantworten können: Welche Daten des Kunden können seine Mitarbeiter gegebenenfalls sehen? Sind die Autorisierungs- und Authentifizierungssysteme des Anbieters tatsächlich leistungsfähig genug, unberechtigte Zugriffe – auch durch andere Kunden oder Angestellte des Dienstleisters – auszuschließen? Lässt sich ein beim Kunden vorhandenes Single-Sign-On-System auf die beim Anbieter genutzten Systeme ausdehnen?

Die Sicherheitsverantwortlichen beim Kunden müssen die Möglichkeit haben, Zugriffsrechte für Mitarbeiter auf den Systemen des Anbieters schnell und flexibel zu setzen, zu löschen und zu ändern. Der Management-Zugang muss hier streng separierte Rollen und Rechte für alle beteiligten Systemverwalter,



Quelle: Jericho-Forum

Das „Cloud Cube Model“ des Jericho-Forums: Daten sind beim Cloud Computing in unterschiedlichen Bereichen verschieden stark exponiert. Um zu wissen, welche Daten mit welchem Sicherheitsaufwand an Dienstleister übergeben werden können, ist zunächst eine Klassifizierung notwendig.

sowohl beim Anbieter als auch beim Kunden, zur Verfügung stellen und darf nicht weniger Optionen bieten als ein internes Management-System.

Das Jericho-Forum (www.opengroup.org/jericho) – neben der Cloud Security Alliance (www.cloudsecurityalliance.org) eine der wichtigsten Institutionen, die sich um die Sicherheit des Cloud Computing und die damit verbundenen Standards und Best Practices kümmern – weist im Zusammenhang mit seinem „Cloud Cube Model" zur SaaS-Nutzung darauf hin, wie intensiv sich ein Anwender vor der Buchung solcher Dienste mit der Kategorisierung seiner Daten befassen muss.

Je sensibler und vertraulicher die zum Outsourcing vorgesehenen Daten sind, desto größer wird der Aufwand zur Sicherung. Diese Feststellung mag simpel erscheinen, spiegelt aber die Erkenntnis wider, dass nur wenige Unternehmen bisher eine stringente Klassifizierung der in ihrem Netz vorhandenen Informationen durchgeführt haben. Während bei der externen Bearbeitung einer Kundendatenbank das Risikopotenzial und damit der Schutzbedarf leicht einzuschätzen sind, fällt dies beispielsweise bei unstrukturierten Office-Daten viel schwerer.

Verschlüsselung, Autorisierung und hoch entwickelte Authentifizierung sind die Kerntechniken einer „sicheren" Zusammenarbeit mit einem SaaS-Provider. Damit lassen sich sowohl Daten auf dem Transportweg von und zum Provider, als auch die auf fremden Servern abgelegten Daten sichern. Nicht nur der Anbieter, sondern ebenso der Anwender sollte deshalb in der Lage sein, mit einer auf Zertifikaten basierenden Verschlüsselung zu operieren – und er sollte über ein Key-Management-System verfügen, weil die Verwaltung der Schlüssel, wie die Cloud Security Alliance rät, möglichst nicht beim SaaS-Anbieter stattfinden sollte. Zur Verwaltung von Schlüsseln in Cloud-Umgebungen gibt es bereits Standards, darunter das OASIS Key Management Interoperability Protocol (KMIP), der IEEE-Standard 1619.3 für das Key-Management beim Speichern von Daten, und XKMS zur Verwaltung und Validierung von Schlüsseln in SOA-Umgebungen.

Ein Muss: Zuverlässige Authentifizierung

Was die Authentifizierung betrifft, so ist Identity Federation die Technik der Wahl, denn sie erlaubt die sichere Übertragung der Identitätsinformationen vom Kunden zum Service-Provider. Welche Standards hier eine Rolle spielen und die Arbeit erleichtern – etwa die mit den Standards der Open-Authentication-Initiative kompatible Authentifizierung, OpenID und für die Übertragung die Security Assertion Markup Language (SAML) sowie die Web Services Federation Language (WS-Federation) – listet das Dokument „Security Guidance for Critical Areas of Focus" der Cloud Security Alliance im Detail auf. Plug-ins und Serviceschnittstellen erlauben die Einbindung von Benutzerdaten aus Directories, Meta-Directories und Datenbanken. Kommen Webservices ins Spiel, die selbstständig Daten austauschen, müssen sich die beteiligten Sicherheitsfachkräfte beim Anwender und beim Anbieter intensiv in die Thematik der XML-Sicherheit einarbeiten oder entsprechend geschulte Berater hinzuziehen.

Vor diesem Hintergrund gilt: Ein Unternehmen kommt umso leichter mit den Herausforderungen der Einbindung von SaaS-Lösungen zurecht, je moderner sein internes Sicherheitskonzept bereits ist. Vor allem Nachholbedarf auf dem Gebiet der Verschlüsselung und Authentifizierung kann beim Übergang zu SaaS paradoxerweise zunächst technischen Investitions- und Restrukturierungsbedarf im Netz des Anwenders generieren. Insgesamt gilt, dass die Auswahl eines SaaS-Dienstleisters mit großer Sorgfalt erfolgen muss – Zertifizierungen der eingesetzten Sicherheitssysteme, interne Organisation nach ISO 27001, nachweisbar konsequentes Qualitätsmanagement, aussagekräftige Reports, gut erreichbarer Support und „weiche" Faktoren wie die Möglichkeit, sich die Systeme beim Dienstleister einmal selbst anzusehen, gehören zu den wichtigsten Bewertungskriterien. (ur/sf)

Bettina Weßelmann ist freie IT-Fachjournalistin.

Ungeteilter Schutz

Sicherheit in virtualisierten Umgebungen

Virtualisierung und Sicherheit lassen sich nur schwer miteinander verbinden, heißt es landläufig. Das muss jedoch nicht zwingend so sein, sofern Unternehmen bereits bei der Planung berücksichtigen, dass Security nicht allein durch die Produkte, sondern durch eine konsequent verfolgte Strategie erreicht wird.

Wie wichtig eine gute Strategie zum Schützen der Infrastruktur ist, kann man nicht oft genug betonen. Wer eine gleichmäßige Absicherung gegen alle Gefahren mit hoher Eintrittswahrscheinlichkeit oder Schadenshöhen erreichen will, kommt um eine gute Planung und regelmäßige Kontrollen der Umsetzung nicht herum (Abb. 1). Virtualisierte Umgebungen haben fast immer einen sehr hohen Schutzbedarf, sie gehören also zu den Bereichen der IT-Landschaft, die besonders sorgfältig abzusichern sind.

Die Versprechen der Anbieter von Virtualisierungsprodukten hören sich immer gleich an: mehr Daten und Leistung auf einer Hardware, in einem Raum, auf einem Speicher, sowie Standardisierung zugunsten der Verringerung der Arbeitslast von Administratoren. Die schlechte Nachricht verschweigen die Hersteller häufig: Der Bedarf an Sicherheit für diese Ressourcen ist gleichzusetzen mit dem kombinierten Schutzbedarf aller ehemals auf eigener Hardware laufenden Anwendungen.

Es gibt aber auch die gute Nachricht: Die Zentralisierung infolge der Virtualisierung hat den Vorteil, dass man Sicherheitsmaßnahmen gleichzeitig auf alle Applikationen anwenden kann. Bei den meisten Betreibern virtueller Umgebungen war früher ein geringerer Anteil an Anwendungen auf Hardware installiert, die durch mehrfache Auslegung hochverfügbar betrieben wurde. Da nun fast alle Applikationen in einem Cluster laufen, kommt ihnen zugute, dass die Wege zum SAN (Storage Attached Network) mehrfach vorhanden sind, dass ein RAID (Redundant Array of Independent Disks) in Betrieb ist sowie dass die Anwendungen dynamisch von Server zu Server „wandern“ und diese eventuell in unterschiedlichen Serverräumen in verschiedenen Gebäuden stehen.

Die Virtualisierung hat einige Vorgänge verändert. Beispielsweise koordiniert der Hypervisor nun das Backup, und viele Anwendungen benötigen auf dem Gast keinen Agenten. Auch lassen sich Snapshots der laufenden Umgebungen jederzeit auf neuer Hardware starten. Damit ist das größte Problem bei der Strategie der Backup-Notfallvorsorge gelöst. Wo früher identische Hardware beschafft werden musste, weil der Server mit einer anderen Netzwerkkarte nicht mehr booten wollte, kann sich der Administrator nun darauf verlassen, dass die virtuelle Umgebung selbst auf dem Server der übernächsten Generation für den Gast identisch aussieht. Lieferverträge, die garantierte Konfigurationen der Hardware auch Jahre nach dem ursprünglichen Kauf vorsehen, sind damit überholt.

Es ist spannend zu beobachten, wie die Virtualisierung einen Trend umkehrt, der seit über 30 Jahren kaum aufzuhalten schien – nämlich die immer weitere Verteilung der Ressourcen auf zunehmend kleinere Einheiten. Wo zu IT-Urzeiten noch der Mainframe die Existenz von schwarzer Materie bewies, stehen heute „bunte Kistchen“ in großer Zahl mit jeweils einem eigenen kleinen Netzteil, eigenem Speicher und eigenen Netzwerkanschlüssen.

Nun wird aber wieder aufgeräumt. Im Rechenzentrum ersetzt eine Farm (neudeutsch Cluster oder noch neuer Cloud) den Host. Sie enthält PC-CPUs mit Komponenten, die in einigen Punkten denen der Endverbrauchergeräte ähneln – dafür gibt es aber viele davon in einem Gehäuse, Rack genannt, eventuell mit einem redundanten Netzteil und teilweise auch wieder mit gemeinsamen Netzwerkanschlüssen. Man kann den Hosts vieles vorwerfen, Unzuverlässigkeit und Datenverlust gehört sicher nicht dazu. Wer mit einer aktuellen Konfiguration die damals bereits üblichen Zahlen für Verfügbarkeit und Sicherheit vor Übergriffen von einem Gast auf

SICHERHEITS-APPLIANCES FÜR VIRTUALISIERTE UMGEBUNGEN

Hersteller	Produkt	Website
Altor Networks	VF 3.0	altornetworks.com
Art of Defence	Hyperguard	www.artofdefence.com/de
Astaro	Security Gateway Virtual-Appliance	www.astaro.de
Check Point	Security Gateway VPN-1 Virtual Edition	www.checkpoint.com
Clavister	Virtual Security Gateway	www.clavister.de
Clearswift	Web Appliance	www.clavister.com
gateProtect	VMA-250, VMX-800, -2500	www.gateprotect.de
IBM	Proventia Virtualized Network Security Platform	www.ibm.com
Kerio Technologies	WinRoute Firewall	www.kerio.de
Linogate	Defendo VM	www.linogate.de
McAfee	Total Protection for Virtualization	www.mcafee.com/de
Reflex Systems	vTrust	www.reflexsystems.com
Securepoint	SecurePoint 10	www.securepoint.de
SmoothWall	Guardian	www.smoothwall.net
Stonesoft	StoneGate Firewall/VPN	www.stonesoft.de
Third Brigade	Deep Security Virtual Appliance	www.thirdbrigade.com
Trend Micro	InterScan	www.trendmicro.de

Die Übersicht der Anbieter erhebt keine Anspruch auf Vollständigkeit.

Drei aktuelle Angriffe - itWatch schützt

Angriffe über pdf Dateien - itWatch schützt:
Alle eingehenden pdf Dateien werden durch inhaltliche Patternprüfung auf schadhaften Code geprüft. Nicht nur Dateien, die über USB Sticks oder andere Datenträger (CD / DVD) eingelesen werden, sondern auch die, die von Anwendungen wie E-Mail-Client oder Browser auf den PC gebracht werden.

Schwachstelle im Internet Explorer – itWatch schützt:
Die Schwachstelle des IEs kann nur Schaden anrichten, weil der Angreifer die Rechte des angemeldeten Benutzers übernimmt. Mit der itWatch Applikationskontrolle kann der Rechteraum des IEs so eingeschränkt werden, dass er nur Konfigurationsdaten lesen darf, keine Schreibrechte auf anderen ausführbaren Dateien hat und solche auch nicht erstellen oder ausführen kann.

USB-Hardware-Verschlüsselung unsicher – itWatch schützt:
Der aktuell gemeldete Angriff auf selbst verschlüsselnde USB-Sticks lässt das Vertrauen in diese Technologie weiter sinken. Die Softwarelösung der itWatch schützt sowohl vor USB-Dumpern als auch vor Angriffen auf den Stick, da der Schlüssel nur im Kopf des Anwenders bekannt ist.

itWatch unterstützt WhiteIT:
WhiteIT will eine Strategie zur Bekämpfung von Kinderpornographie entwickeln und umsetzen. itWatch trägt neben der patentierten Inhaltsprüfung Echtzeitmonitoring und Forensik auf dem Endgerät bei. Dateiarchive und verschlüsselte Inhalte werden sicher auf frei definierbare schädliche Inhalte geprüft und im Trefferfall mit geeigneten Maßnahmen bekämpft.

itWatch GmbH

Endpoint Security, die mitdenkt

+49 (0) 89 620 30 100 - www.itWatch.de - Info@itWatch.de

Besuchen Sie uns auf der CeBIT, 02.-06.03.2010, Halle 11, Stand B10

den anderen erreichen möchte, benötigt die gesamte Trickkiste der Nachkommen.

Sicherer mit VMSafe-Schnittstelle

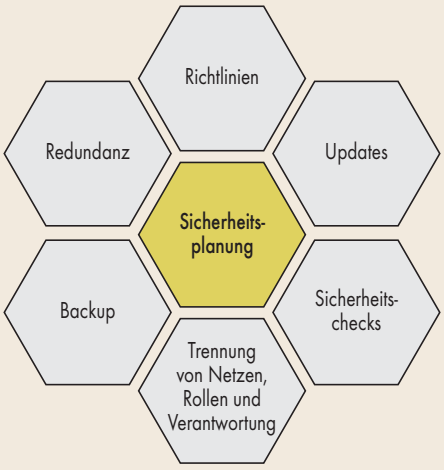
Der Anbieter, der seit Jahren die Innovation der gesamten Branche antreibt und den Sicherheitsaspekt von Anfang an klar im Blick hatte, ist VMware. Mit der lang erwarteten und letztes Jahr vorgestellten VMSafe-Programmierschnittstelle bietet das Unternehmen den Herstellern von Sicherheitssoftware einen direkten Zugang zu den Gästen.

So reicht es, den Virenscanner einmal pro Umgebung zu installieren. Über VMSafe kann diese eine Instanz des Scanners in allen Gästen die Festplatten durchsuchen und diese permanent bei allen Zugriffen auf die gelesenen oder geschriebenen Daten in Augenschein nehmen (Abb. 2). Der zusätzliche Vorteil hierbei ist, dass ein Angreifer oder ein Virus diese Sicherheitsmaßnahmen nur sehr schwer ausschalten kann.

Wenn die Software, die den Rechner schützen soll, auf das zu sichernde Betriebssystem aufbaut, besteht immer das Risiko, dass der Schutz umgangen wird, indem die Schad- die Sicherheitssoftware abschaltet. Das ist meistens kaum schwerer, als ein Fenster auf dem Bildschirm zu schließen – zumindest nach erfolgreicher Übernahme des Systems. Da die Schutzsoftware nun in einem anderen Gast läuft und der Hypervisor nur die Daten vom zu schützenden Gast an die Sicherheitssoftware übergibt, ist dies nicht mehr möglich.

Ein erfolgreicher Angriff gegen die Schutzsoftware bringt dem Angreifer keine Rechte auf dem Hypervisor, sondern nur auf einem anderen Gast. Der Gast wiederum kann eventuell keine Verbindung zum Angreifer aufbauen, und so verhindert die geschickte Planung der Architektur, dass aus dem Angriff ein aktiv zu nutzender Kommandokanal entsteht. Nur wenn der Angreifer auch die weiteren Befehle und möglichst deren Ausgaben von und zum Ziel transportieren kann, ist er in der Lage, das System zu seinen Zwecken zu missbrauchen. VMSafe erlaubt auch die zentrale Überwachung des Netzverkehrs und des RAMs.

Erste Produkte von McAfee und IBM nutzen diese Schnittstelle darüber hinaus, um die Verwaltung der Gäste noch weiter zu zentralisieren. Die vielen über eine zentrale Oberfläche gesteuerten Hypervisoren helfen nicht bei der Verwaltung der Gäste. Der Hypervisor ist nur eine virtuelle und gut zu verwaltende Hardware. Die Management-Konsole hat auf die auf dieser angenommenen Hardware laufenden Betriebssysteme und die darauf aufsetzenden Anwendungen kaum Einfluss. So muss der Administrator trotz Vir-



Die Planung der Sicherheit sollte alle Aspekte beachten und sie vom ersten Schritt an in die Umgebung integrieren (Abb. 1).

tualisierung die Zählung, Überwachung und Steuerung des Gastes in jedem einzelnen erneut einrichten. An diesem Punkt unterschied sich bisher die virtuelle Umgebung nicht von der in den 90er-Jahren etablierten IT-Welt aus kleinen und kleinsten physikalisch getrennten Recheneinheiten.

Jedes Schräubchen ist wichtig

Die Sicherheit der IT ist von der jeder einzelnen Komponente abhängig. So wie die Gäste jederzeit mit frischen Patches versorgt werden müssen, sind auch die Wirte auf aktuellem Stand zu halten. Bei den Gästen gibt es für die meisten Betriebssysteme etablierte Verfahren dafür, allerdings fehlt ihnen häufig die Möglichkeit, zusätzlich die Anwendungen, kleine Hilfsprogramme und die sonstigen auf dem System ausführbaren Programme zu betrachten.

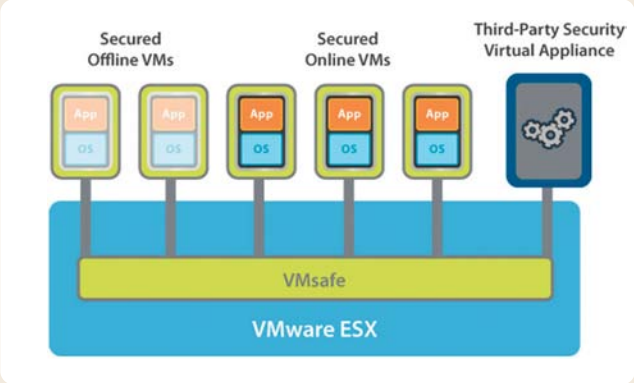
So kann es passieren – und ist in den meisten Betrieben leider der Standard –, dass das Betriebssystem zwar „nur“ seit zwei oder drei Monaten nicht aktualisiert wurde, die sonstige Software aber seit Jahren im wahrsten Sinne des Wortes vor sich hingammelt. Angreifer nutzen diese Tatsache gern für erfolgreiche Einbrüche. Hier hilft nur eine vollständige Inventarisierung aller ausführbaren Dateien und Netzwerkdienste mit dem Ziel, diese mit einer Liste von verwundbaren Versionen abzugleichen.

Für die Wirte ist diese Aufgabe verhältnismäßig einfach, denn hier kommt die gesamte Software aus einer Hand. Benachrichtigungen über Schwachstellen gehen an alle registrieren Anwender, und es gibt eine offizielle Verteilung der Updates mit Prüfsummen. Insgesamt können Systemverantwortliche in einer virtualisierten Umgebung Updates sehr viel schneller einspielen. Sofern mehrere Wirte sich die Arbeit teilen, verschieben sie ihre Gäste so, dass immer einer vollständig frei ist. Auf die Art kann die zentrale Verwaltung der Hypervisoren einen nach dem anderen aktualisieren und durchstarten, ohne den laufenden Betrieb zu unterbrechen. Dies geschieht sinnvollerweise zu einer Zeit, zu der die Last gering ist, denn das Verschieben von flüchtigem Speicher und CPU-Zuständen erfordert Rechenzeit und Bandbreite auf dem Netzwerk.

Bei den Gästen ist das Testen der Updates „am lebenden Herzen“ möglich. So lässt sich ein Klon eines Gastes erzeugen und darauf das Update installieren. Funktioniert er weiterhin zuverlässig und übersteht alle Tests, wird er entweder zum neuen produktiven Gast, oder der Verantwortliche wiederholt die Prozedur auf dem Ursprungs-Image. Damit lassen sich auch Server in Testzyklen einbinden, die man bisher aus Mangel an einer Testumgebung (oder weil eine solche schlicht zu teuer war) nicht aktualisieren konnte.

Eine andere zentrale Aufgabe ist die Verwaltung von Anmeldevorgängen mit dem Abgleich mit einem zentralen Verzeichnis aller Personen und Dienstkonten. Dieses Verzeichnis muss auch Informationen darüber enthalten, wer welche Rechte auf welchem System hat. Dabei sollten die Verantwortlichen Rollen definieren und besonders berechtigte Administratoren diesen Rollen Personen zuordnen. Diese besondere Berechtigung ist wichtig, denn eine Domäne, in der alle Administratoren auch Rechte vergeben können oder gar über dem Berechtigungsmodell stehen, ist aus Sicherheitssicht nicht nur unbefriedigend, sondern ebenso riskant. Administratoren sollten nur Rechte auf Systemen haben, die sie verwalten, und sie dürfen keine Chance haben, sich selbst darüber hinausgehende Rechte zu verschaffen.

Nach diesem Muster sollte auch das Berechtigungskonzept



Quelle: VMware

VMSafe als ein Beispiel, wie eine durch den Hypervisor zentral für alle Gäste betriebene Sicherheitslösung funktionieren kann. Der Virenscanner läuft in einem Gast und sichert alle anderen Gäste ab (Abb. 2).

in der virtuellen Umgebung aufgebaut sein: Wenige verwalten die Rechtevergabe und viele verwalten die in Gruppen eingeteilten Komponenten. So sollte nicht jeder Administrator in der Lage sein, die Hypervisoren zu managen. Für diese Aufgabe sollte es eine eigene Gruppe geben.

Ebenso wenig wie jeder Administrator Domänen-Admin sein soll, ist es anzuraten, dass jeder Verwalter der virtuellen Umgebung alle Rechte in der Managementkonsole hat. Auf die Größe der Organisation und der IT-Mannschaft angepasst, sollte das Berechtigungskonzept nur die benötigten Rechte an die handelnden Personen übergeben.

Eine gute Architektur zahlt sich aus

Nicht nur die Details des Schutzes sind in einer guten Strategie zur Absicherung dieser zentralen Umgebung wichtig, auch eine gute Architektur muss vorhanden sein. Das bedeutet, dass jede Komponente für sich sicher sein sollte, denn Lücken bei ihnen lassen sich immer ausnutzen. Eine sichere Architektur sorgt dann dafür, dass ein Einbruch auf einem System sich möglichst wenig auf die anderen Elemente der Landschaft auswirkt. Deswegen muss die Planung eine Abschottung der Komponenten voreinander vorsehen.

Als Beispiel sei der Virenscanner auf Gast 1 genannt, der zentraler Virenscanner für die Gäste 1 bis 300 ist. Wenn alle Gäste ihre Netzwerkanschlüsse nun in einem gemeinsamen Netzwerk haben, kann ein Angreifer sein Angriffsprogramm auf Gast 2 einschmuggeln, von dort transportiert es der Hypervisor zu Gast 1. Bei der Untersuchung des Programms durch den Virenscanner wird eine Schwachstelle des Scanners ausgenutzt. Der Angreifer erlangt so die volle Kontrolle über Gast 1 und, da er mit ihm über das Netzwerk reden kann, das er auch für die Kommunikation mit Gast 2 nutzt, hat er Gast 1 erfolgreich übernommen. Wären die beiden Gäste in unterschiedlichen Netzen eingetragen, hätte der Angreifer nicht mit Gast 1 kommunizieren und den Angriff erfolgreich durchführen können.

Der Plan des Netzwerkes sollte also so gestaltet sein, dass nur Gäste, die zwingend Daten austauschen müssen, dies können. Firewalls kontrollieren die Übergänge zwischen solchen Netzwerkzonen. Auch sollten Gäste und Hypervisoren im produktiven Betrieb niemals Daten austauschen. Es ist keine Netzwerkverbindung zwischen dem Netz der Hypervisoren und ihrer Verwaltungsoberfläche sowie den Netzen der Gäste notwendig. Diese Abschottung der Kommunikation war früher bei Hosts üblich. Heute müssen die Architekten der Umgebungen dies einplanen.

Diese Trennung ist so wichtig, dass die Innenrevision sie als Prüfziel in die regelmäßigen IT-Sicherheitsprüfungen aufnehmen muss, ebenso wie das Berechtigungsmodell und die Anforderung, dass nur aktuelle Software eingesetzt wird.

Fazit

Sicherheit ist dann kosteneffizient, wenn die Verantwortlichen sie von Anfang an in das Design der Umgebung einplanen. Auch bei virtualisierten Umgebungen ist darauf zu achten, dass so weit als möglich getrennt wird, was nicht zwingend zusammen gehört. Dies gilt für Netze, Gäste, administrative Rechte und Speicher. Mit den aktuell zur Verfügung stehenden Techniken ist ein sehr hohes Schutzniveau realisierbar und sollte in Anbetracht des hohen Schutzbedarfs auch angestrebt werden. Dennoch ist es mit gewissen Risiken verbunden, Gäste unterschiedlicher Sicherheitszonen auf einer Umgebung zu betreiben. (sf/ur)

Christoph Puppe ist Sicherheitsberater und Penetrationstester bei der HiSolutions AG in Berlin.