VIRTUALISIERTE UMGEBUNGEN MIT REALEN RISIKEN

Die Nutzung virtualisierter Umgebungen bringt nicht nur Vorteile, sondern auch beträchtlich Risiken für die IT-Sicherheit.

| von IRENA IRMLER UND DENIZ WETZ

Virtualisierung ist ein zentraler Treiber der Informationstechnologie und stellt die Grundlage für die kostengünstige Bereitstellung von Technologien wie Cloud-Computing dar. Die größten Vorteile von Virtualisierung sind Effizienzsteigerungen, Kosteneinsparungen, Flexibilität und hohe Verfügbarkeiten. Daraus resultieren eine steigende Verbreitung und Weiterentwicklung solcher Plattformen, die auch für Behörden eine hohe Relevanz besitzen.

Wie in der freien Wirtschaft werden auch bei den Geschäftsprozessen der öffentlichen Verwaltung häufig besonders schützenswerte Informationen verarbeitet. Durch den Einsatz von Virtualisierungstechniken darf kein höheres Risiko für die Vertraulichkeit, Integrität und Verfügbarkeit dieser Informationen entstehen als beim klassischen Betrieb. Das muss durch spezifische Sicherheitskonzepte und -maßnahmen in virtualisierten Umgebungen gewährleistet werden.

GRUNDLAGEN DER VIRTUALISIERUNG

Unter Virtualisierung versteht man die Technologie, eine virtuelle statt einer physischen Version einer Komponente einzusetzen. Solche Komponenten können Server, Storage-Geräte oder Netzwerke sein. Durch Virtualisierung wird das Vorhandensein physischer Hardware simuliert – sie wird durch ein virtuelles Computersystem, die virtuelle Maschine (VM), ersetzt. Eine VM ist ein vollständig isolierter und gekapselter Software-Container mit einem eigenen „Gast"-Betriebssystem und Anwendungen. Einzelne VMs sind voneinander unabhängig. Der Hypervisor oder Virtual Machine Monitor, eine zusätzliche Software-Schicht, verwaltet die VMs und teilt ihnen bei Bedarf dynamisch Ressourcen (zum Beispiel Prozessorleistung, Arbeitsspeicher, Peripheriegeräte) zu. Dadurch können mehrere VMs auf einem physischen Server, dem sogenannten Host, betrieben werden. Es gibt zwei Arten der Virtualisierung: Während bei der sogenannten bare-mental- oder nativen Virtualisierung der Hypervisor direkt auf der Hardware läuft, setzt er bei der „gehosteten" Virtualisierung auf einem vollständigen Betriebssystem auf, das auf der Hardware betrieben wird (Abbildung 1). Die Haupteinsatzzwecke der Virtualisierung beziehen sich auf Server, Desktop, Netzwerk und Storage-Virtualisierung.

SICHERHEITSBEDROHUNGEN

Aus der Perspektive der IT-Sicherheit sind virtualisierte Umgebungen – zusätzlich zu den Bedrohungen klassischer Infrastrukturen – von weiteren Bedrohungen betroffen. Denn sie bieten neue Eintrittspunkte für Angriffe und beinhalten komplexere Verbindungsmuster. Herausforderungen für die IT-Sicherheit beziehen sich auf die unterschiedlichen Virtualisierungskomponenten: von den Hypervisoren über die VMs selbst bis zur Sicherung der virtuellen Netzwerke. Bewährte Virtualisierungslösungen bringen nicht nur die bekannten Funktionalitäten, sondern auch Schwachstellen mit ein.

Eine zentrale Eigenschaft virtualisierter Umgebungen ist die Multimandantenfähigkeit. Darunter versteht man, dass mehrere virtuelle Systeme auf derselben physischen Infrastruktur betrieben werden. Dabei werden Informationen unterschiedlicher Anwendungen, Geschäftsbereiche oder Organisationen von einem gemeinsamen Hypervisor verwaltet und teilen sich einen gemeinsamen physischen Speicher. Dadurch entstehen Ansatzpunkte für unbefugte Zugriffe auf sensible Daten.

HYPERVISOR ALS SINGLE POINT OF FAILURE

Als zentrale Steuerungs- und Managementeinheit stellt der Hypervisor eine besonders kritische Komponente dar. Er kontrolliert die Hardware und steuert die darauf laufenden VMs. Störungen oder erfolgreiche Angriffe auf den Hypervisor können die Verfügbarkeit der Ressourcen für die VMs einschränken und zu Datenverlust und Kompromittierung weiterer Systeme führen.

Mit steigender Anzahl von VMs werden die Umgebungen komplexer und immer schwieriger überschaubar. Das führt zu Fehlern bei der Konfiguration und im Betrieb. Falsche Einstellungen oder nicht ausreichend restriktive Zugriffsrechte können die Funktionalität des Hypervisors so beeinträchtigen, dass die Informationssicherheit der zugeordneten VMs gefährdet ist.

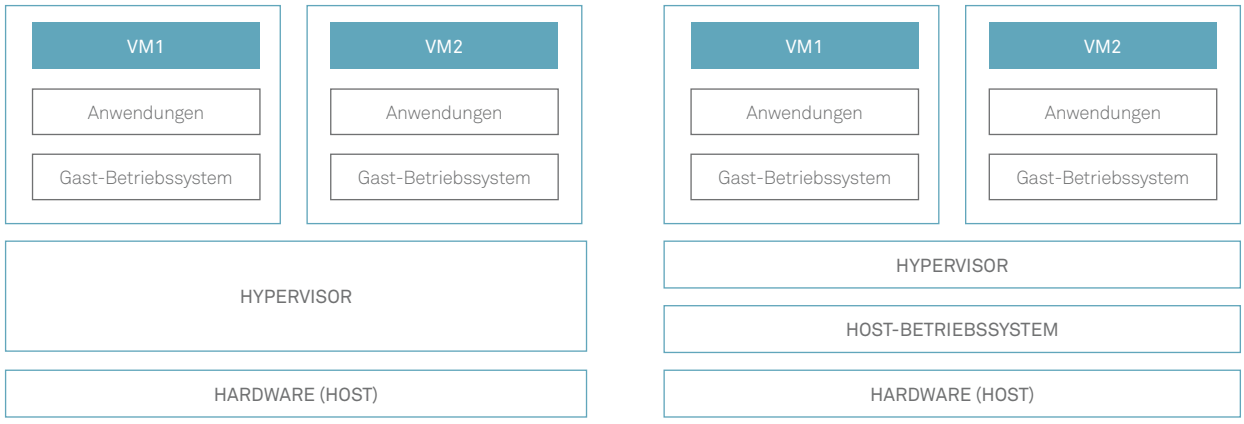

Abbildung 1: Struktur der beiden Virtualisierungsarten: native bzw. bare-metal- (links) und gehostete (rechts) Virtualisierung

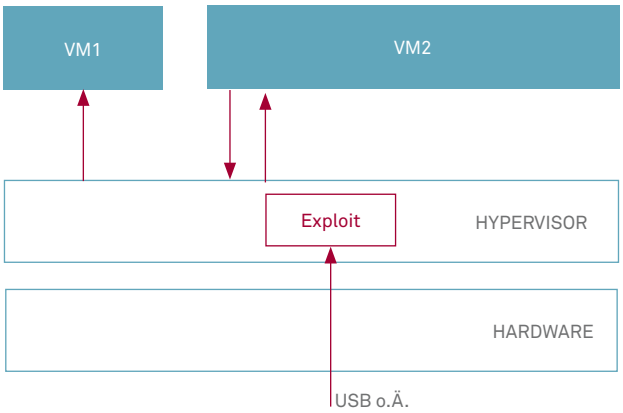

Abbildung 2: Virtual Machine Escape I: Hat ein Angreifer Zutritt zum Rechenzentrum, kann er per USB-Stick einen Exploit im Hypervisor installieren, welcher die Rechte einer bestimmten VM so erweitert, dass diese den Hypervisor steuern kann.

Mit der Verbreitung von Virtualisierung rücken Hypervisoren immer stärker in die Aufmerksamkeit von Angreifern. Möglichkeiten gibt es viele: Angriffe können per USB-Stick und Direktzutritt zum Rechenzentrum (Abbildung 2), über ein Netzwerk oder aus einer kompromittierten VM heraus erfolgen. Im regulären Betrieb erteilt der Hypervisor den VMs allgemeine Managementinstruktionen und ermöglicht ihnen Zugang zu den Hardware-Ressourcen wie Prozessoren, Speichern sowie Peripheriegeräten. Kompromittierte VMs können diese Kommunikationskanäle dazu nutzen, die Sicherheitsregeln des Hypervisors zu umgehen und dort ihre Rechte zu erweitern. Auf diese Weise können sie zum Beispiel privilegierten Zugriff auf die Hardware oder auf andere VMs erhalten (Abbildung 3). Zum Einsatz kommen dafür spezifische Exploits, das heißt eine gezielt entwickelte Software, die Schwachstellen im Programmcode des Hypervisors ausnutzt. Der unbefugte Zugriff einer kompromittierten VM auf den Hypervisor und die Ausweitung der Rechte werden „virtual machine escape“ oder „guest to host escape“ genannt. Ein berühmtes und ein aktuelles Beispiel solcher Angriffe sind Cloudburst[1] (2009) und „from nobody to root“[2] (Mai 2016).

Entsprechend präparierte VMs können über vorhandene Kommunikationskanäle auch sogenannte Seitenkanalangriffe durchführen: Aus dem Verhalten der gemeinsam genutzten Ressourcen ziehen sie Rückschlüsse auf Anwesenheit und Aktivität anderer VMs. Mit diesem Wissen können Angreifer unbemerkt sensible Informationen sammeln und die Leistung reduzieren, die der Hypervisor den Nachbar-VMs zuteilt (Abbildung 4). Der Zugriff einer bösartig agierenden VM auf andere VMs heißt „guest hopping“.

Der Hypervisor ist neben der Erstellung und Verwaltung auch für die Migration von VMs zuständig. Dabei bezeichnet Migration den Prozess, bei dem der Hypervisor VMs auf einen anderen physischen Host verschiebt. Mit einem kompromittierten Migrationsmodul kann ein Angreifer sämtliche Daten der migrierten VM abgreifen und Schad-Software weiterverbreiten.

Obwohl der Hypervisor die VMs voneinander isoliert, bietet er gleichzeitig eine software-basierte Verbindung und damit einen Angriffsvektor zwischen ihnen. Dieses Risiko sollten Betreiber und Nutzer im Hinterkopf behalten.

VIRTUELLE MASCHINEN

VMs werden über ein sogenanntes Image, das als Software-Paket vorliegt, erstellt. Integrität und Aktualität dieser Images sind fundamental für die gesamte Sicherheit der virtualisierten Umgebung. In öffentlichen Image-Repositories werden Images von VMs bereitgestellt. Dadurch können sich mit Schad-Software versehene VMs verbreiten. Das Erstellen von VMs über Images kann zu Schwachstellen augrund von veralteten Patch-Ständen der enthaltenen Betriebssysteme und Software-Komponenten führen. Gleiches gilt für VMs, welche sich über längere Zeit im Offline-Zustand befinden oder über ein Rollback in einen früheren Zustand versetzt werden. Zusätzlich kann ein Rollback zu Kompatibilitätsproblemen und Konfigurationsfehlern führen oder nicht angepasste Konfigurationen enthalten, woraus beispielsweise eine fehlende Beschränkung von Zugriffsrechten resultiert.

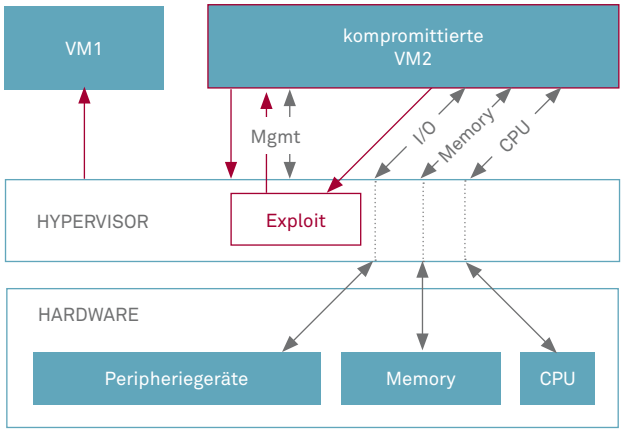

Abbildung 3: Virtual Machine Escape II: Der Angreifer nutzt die erlaubten Kommunikationskanäle zum VM-Management oder zur Zuweisung der Ressourcen, um einen Exploit zu installieren (in der Abbildung: I/O).

1 Detaillierte Informationen unter http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-PAPER.pdf [zuletzt geprüft am 13.02.2017].
2 Detaillierte Informationen unter http://blog.quarkslab.com/xen-exploitation-part-1-xsa-105-from-nobody-to-root.html [zuletzt geprüft am 13.02.2017].

VMs können im Rahmen der Erstellung, des Betriebs und von Migrationen verschiedene Zustände annehmen. Die Erkennung von Schad-Software ist schwieriger, wenn sich eine kompromittierte VM im Offline- oder im Suspended-Zustand befindet.

VMs beinhalten eine Vielzahl von Konfigurationsdateien, die auf Storage-Systemen abgelegt werden und unter Umständen einen besonders hohen Schutzbedarf haben, da sie unter anderem Passwörter, kryptografische Schlüssel oder sensible Anwendungsdaten enthalten.

VIRTUELLE NETZWERKE

Bei virtuellen Netzwerken handelt es sich um die Abbildung eines physischen Netzwerks in virtueller Form. Dabei stehen im virtuellen Netzwerk logische Netzwerkgeräte zur Verfügung, wie unter anderem logische Ports, Switches, Router und Firewalls, logischer Lastausgleich und logische VPNs.

Über eine sogenannten Netzwerk-Virtualisierungsplattform (ähnlich zum Hypervisor oder als dessen Bestandteil) können virtuelle Netze erstellt und konfiguriert werden. Die dadurch erzielbare Isolation der einzelnen (virtuellen) Netze vermindert zwar grundsätzlich nicht deren Sicherheit, allerdings kann ein Angreifer die darunter liegende gemeinsam genutzte Netzwerk-Virtualisierungsplattform angreifen und dort Schwachstellen und Dienste anderer virtueller Netze ausspähen. Zusätzlich können über ein kompromittiertes virtuelles Netz auch Seitenkanalangriffe auf andere virtuelle Netze gestartet werden. Klassische Angriffe wie zum Beispiel Denial-of-Service, Sniffing oder Spoofing gelten auch für virtuelle Netzwerke. Netzwerksicherheitstechniken für physische Netzwerke umfassen beispielsweise Intrusion-Detection-Systeme (IDS) oder Data-Loss-Prevention-Systeme (DLP). Diese können Angriffe innerhalb eines virtuellen Netzwerks nicht erkennen, da Datenpakete das physische Netz nicht passieren.

VIRTUELLER SPEICHER (STORAGE)

Virtualisierte Umgebungen mit großem Datenvolumen und rechenintensiven Anwendungen, die entsprechende Skalierungsmöglichkeiten bereitstellen, stellen besonders hohe Anforderungen an die sichere und performante Anbindung von Speichersystemen. Durch die Virtualisierung von Speichern werden Speichermedien wie Festplatten und Flash-Laufwerke von den physischen Servern abstrahiert und zu sogenannten Storage Pools zusammengefasst. Diese Storage Pools werden über eine entsprechende Software bereitgestellt und stellen eine Hypervisor-unabhängige

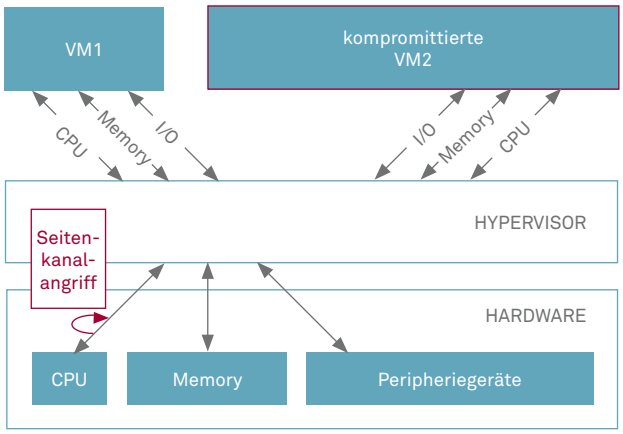

Abbildung 4: Guest Hopping: Bei einem Seitenkanalangriff extrahiert ein Angreifer Informationen im Rahmen der gemeinsamen Hardware-Nutzung oder beeinträchtigt die Verfügbarkeit der Nachbar-VM.

Ressource dar. Dieser Ansatz wird als Software-Defined Storage bezeichnet. Für virtuellen Storage sind die Sicherheitsbedrohungen und Schwachstellen der eingesetzten Storage-Technologien wie Network File System (NFS), Network Attached Storage (NAS), iSCSI und Fibre Channel SANs (Storage Area Network) zu beachten. Eine häufige Form von Angriffen auf ein SAN sind Spoofing-Angriffe. Dabei erspäht ein Angreifer unterschiedliche Erkennungsmerkmale der Teilnehmer, um diese zum Beispiel selbst zur Authentisierung zu nutzen und so Zugriff auf vertrauliche Daten zu erlangen. Ein weiterer Angriff sind Denial-of-Services(DoS)-Angriffe auf den Management-Port der SAN-Switches.

Ein weiteres Risiko stellt Datenremanenz dar. Das bedeutet, dass Daten trotz Löschen auf dem physischen Storage verbleiben (unter anderem ist das in manchen Fällen aufgrund der Wiederherstellbarkeit von Daten gewünscht). Insbesondere der in virtualisierten Umgebungen gemeinsam genutzte physische Speicher macht die Datenremanenz besonders gefährlich. Dadurch entsteht die Möglichkeit, dass Daten ohne Zustimmung für Dritte zugänglich werden oder auf kritische Daten durch Angriffe auf das Storage-Medium zugegriffen werden kann.

SCHUTZMASSNAHMEN

Gezielte und unter Berücksichtigung spezifischer Risiken geplante Maßnahmenpakete können Störungen und Angriffen weitgehend vorbeugen. Ausgefeilte Attacken sind dann so aufwendig, dass das Ergebnis den Zeit- und Ressourceneinsatz für den Angreifer nicht mehr rechtfertigt. In klassischen IT-Verbun-

den haben sich Sicherheitsstrategien bewährt, die vielfältige Technologien auf mehreren Schichten einsetzen. Sie adressieren alle bekannten Angriffsrichtungen und werden in einem ständigen Revisionsprozess auf Effektivität und Effizienz überprüft. Eine solche Taktik eignet sich auch für virtualisierte Umgebungen, wobei neben der Härtung der einzelnen Systeme, das heißt der VMs, und der Absicherung der Netze auch der Hypervisor geschützt werden muss.

SICHERER HYPERVISOR

Schwachstellen können bei komplexer Software mit umfangreicher Codebasis praktisch nicht vermieden werden. Daher gilt: Je knapper und einfacher der Quellcode ist, desto schwieriger ist es für Angreifer, Schwachstellen darin zu entdecken. Bei der Beschaffung der Software soll berücksichtigt werden, inwiefern die Hersteller auf eine reduzierte Angriffsoberfläche achten, ob sie aktiv nach Schwachstellen forschen und Patches zeitnah bereitstellen. Mittlerweile sind spezielle Virtualisierungslösungen erhältlich, die den Zugriff auf das Kernel des Hypervisors erheblich einschränken oder den Programmcode in Vertrauensschichten, sogenannte layers of trust, fragmentieren.

Anwender können Risiken begegnen, indem sie den Hypervisor sicher konfigurieren. Dabei deaktivieren sie nicht benötigte Hypervisor-Funktionalitäten, sorgen für eine klare Separierung der Netzwerke verschiedener Mandanten mithilfe von VLANs und insbesondere des sogenannten Management-Traffic, dem Datenstrom zur Administration einer virtualisierten Plattform. Darüber hinaus definieren und implementieren sie ein restriktives Berechtigungskonzept. Die Integrität der Kommunikation zwischen Hypervisor und VMs kann mithilfe von Tools zur „control flow integrity“ (CFI) sichergestellt werden: CFI prüft, ob die Ausführung eines Programms einem vorgeschriebenen Prozess, dem sogenannten control flow graph (CFG), folgt. Bei einer Abweichung vom CFG wird das Programm sofort angehalten.

Die herausragende Stellung des Hypervisors kann als Chance für Sicherheit begriffen werden: Speziell für virtualisierte Umgebungen entwickelte IDS erkennen Anomalien im Verhalten der überwachten Systeme und entdecken auch dort Kompromittierungen. Firewalls, Überwachungs- und Protokollierungstools können auf den gesamten virtualisierten Verbund skaliert werden. Gleichzeitig erzeugen sie Analysedaten, die das IDS für eine Angriffserkennung nutzen kann. Ferner sind manche Virenscanner auf virtualisierte Umgebungen zugeschnitten. Lösungen in diesem Bereich lassen sich unter dem Begriff „virtual machine introspection“ zusammenfassen.

SICHERE VMS, STORAGE UND NETZE

Sicherheitsmaßnahmen für VMs umfassen neben dem Einsatz üblicher Schutztechnologien (Software-Firewall, Virenschutz, Zugriffsschutz durch Verschlüsselung und Authentisierung, Integritätsprüfungen, Backup ...) auch virtualisierungsspezifische Aspekte, zum Beispiel eine Integritätsprüfung der Images für die Betriebssysteme der VMs.

Migrierte Daten sollten vor, während und nach der Migration vertraulich und integer bleiben. Um Datenremanenz zu verhindern, müssen am „alten“ Ort verbleibende Daten verlässlich entfernt werden.

Bekannte Mechanismen wie Authentisierung, Autorisierung, Verschlüsselung und Zoning dienen auch dazu, virtualisierten Storage angemessen abzusichern.

Auch wenn die Isolation von VMs ein zentrales Leistungsmerkmal des Hypervisors ist, empfiehlt sich eine zusätzliche Segmentierung in mehrere virtuelle Netze gemäß dem Schutzbedarf der Daten der Anwendungen auf den jeweiligen VMs. Dazu dienen neben den Zugangskontrolllisten der Firewalls und Router auch spezielle Konfigurationsparameter, die in sogenannte Inline-Appliances im Hypervisor oder an virtualisierten Netzwerkkomponenten zur Verfügung stehen.

Die dem Schutzbedarf angemessene Konfiguration, Segmentierung und Überwachung virtueller Maschinen, Netzwerke und Speicher stellt einen wichtigen Sicherheitsaspekt dar.

SICHERHEITSPRODUKTE

Es gibt spezielle Produkte, die die Sicherheitsanforderungen von virtualisierten Umgebungen umsetzen. Diese stellen verschiedene Sicherheitsfunktionen wie zum Beispiel IDS, Monitoring, Logging, Deep Packet Inspection (DPI) und Virenscanner bereit. Die Produkte werden zentral beispielsweise als Virtual Appliance in der virtualisierten Umgebung betrieben und bieten Schutz für alle virtuellen Maschinen auf einem Hypervisor. Im Fall von Virenscannern sind Produkte verfügbar, die zusätzlich Agenten auf den virtuellen Maschinen installieren, um weitere Erkennungsmöglichkeiten von Viren und Malware zu bieten (zum Beispiel Programmkontrolle, Zugriff auf Speicher und Prozesse). Vorteile dieser Produkte sind eine geringe Ressourcenbeanspruchung und die Möglichkeit der zentralen Administration.

SICHERE PROZESSE

Informationssicherheit muss ein grundlegendes Kriterium bei Planung, Beschaffung, Installation, Konfiguration, Betrieb und Änderung der IT-Architektur in der öffentlichen Verwaltung sein.

Die Prozesse, die zur Informationssicherheit in virtualisierten Umgebungen beitragen, unterscheiden sich nur in zwei Arbeitsfeldern von den Prozessen in klassischen Verbünden: Erstens erfordert die zentrale Position des Hypervisors als Dreh- und Angelpunkt einen reibungslosen Patch- und Änderungsmanagementprozess. Zweitens verlangt der Einsatz einer virtualisierten Umgebung ihre möglichst unterbrechungsfreie Verfügbarkeit (Cloud Resiliency): Effiziente Notfallprozesse müssen dafür sorgen, dass die Systeme auch im Störungsfall erreichbar und funktional sind. Das wird zum Beispiel durch Redundanz oder durch die automatisierte Migration einer nicht vertrauenswürdigen VM in ein von der Produktivumgebung abgetrenntes virtuelles Netz erreicht.

INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM (ISMS)

Das Etablieren von Sicherheitsprozessen ist nicht einfach: Sie stehen oft im Zielkonflikt mit Funktionalität, Benutzerfreundlichkeit und manchmal auch mit der Verfügbarkeit der Ressourcen, sodass hier eine stetige Abwägung getroffen werden muss. Außerdem erfordert Informationssicherheit Wissen und Know-how sowie zeitliche, personelle und finanzielle Ressourcen. Die Absicherung von virtualisierten Umgebungen erfordert mehr Expertise und höhere Investitionen, ist jedoch durch die beschriebenen Risiken in hohem Maße gerechtfertigt.

Gerade virtualisierte Umgebungen benötigen daher ein ISMS, das alle Anwendungen, Systeme, Verbindungen und deren Abhängigkeiten erfasst. Der Schutzbedarf muss für die dort erzeugten, verarbeiteten und genutzten Informationen festgestellt werden, wobei die Angemessenheit im Mittelpunkt der Erwägungen steht. Das ISMS unterstützt bei der Planung, Umsetzung und Kontrolle von Schutzmaßnahmen und etabliert einen kontinuierlichen Sicherheitsprozess. Dieser prüft die Wirksamkeit der getroffenen Maßnahmen vor dem Hintergrund des rapiden technologischen Fortschritts und sich wandelnder Umweltbedingungen – aus denen neue Bedrohungen und Risiken, aber auch Chancen entstehen können. Empfehlenswert ist es, das ISMS durch einen unabhängigen Gutachter bewerten zu lassen beziehungsweise eine Zertifizierung des IT-Verbundes gemäß dem IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) anzustreben.

FAZIT

Virtualisierte Umgebungen und deren stetige technische Weiterentwicklung stellen neue Herausforderungen an die IT-Sicherheit von Behörden. Daher müssen eigene und zusätzliche Sicherheitskonzepte und -maßnahmen für den Einsatz von virtualisierten Umgebungen erstellt und umgesetzt werden. Nur so kann eine ausreichende Informationssicherheit gewährleistet werden. ●

ANSPRECHPARTNER – JENS WESTPHAL
Abteilungsleiter
IT-Sicherheitsexperte
Public Sector Solutions Consulting