IDC – LÖSUNGSÜBERSICHT

Geschäftsvorteile eines sicheren Rechenzentrums

Gesponsert von: Cisco

Pete Lindstrom Richard L. Villars
Matthew Marden
Dezember 2014

ÜBERBLICK

In der Welt der IT vollziehen sich derzeit tiefgreifende Veränderungen: Die unternehmensorientierte, Client/serverbasierte „zweite Generation der IT-Plattform" entwickelt sich zunehmend hin zu einem Modell auf der Grundlage von Mobility, Social Media, Big Data und Cloud, das IDC auch als „IT-Plattform der dritten Generation" bezeichnet. Praktisch alle aktuellen Business-Innovationen basieren darauf. Hunderttausende, wenn nicht sogar Millionen von Lösungen und Services verändern heute ganze Branchen, indem sie die Vorteile dieser neuen Plattform nutzen, um neue Kundenerlebnisse zu schaffen. In der Plattform der dritten Generation werden Rechenzentren durch die folgenden drei Merkmale charakterisiert:

- **Skalierbarkeit**: Die bis zu zehnfache Anzahl an Benutzern und/oder Datensätzen wird unterstützt, ohne dass die Hardware-Ausstattung im Rechenzentrum in einem vergleichbaren Ausmaß erweitert werden muss.
- **Geschwindigkeit:** Anwendungen und Services können bereits nach einigen Tagen/Wochen – nicht erst nach Jahren/Monaten – fertiggestellt oder aktualisiert werden, ohne dass der Bedarf für IT-Betriebspersonal oder -Entwickler ansteigt.
- **Reichweite:** Neue Services für Kunden werden ermöglicht, indem zahlreiche unterschiedliche interne und externe Anwendungen und Datenquellen koordiniert werden können, ohne dass darunter die Datenintegrität oder Benutzerfreundlichkeit leiden.

In dieser durch Mobility, Social Media, Cloud, Big Data und intelligente Industrie geprägten IT-Landschaft kann das Rechenzentrum nicht mehr nur der Ort sein, an dem das Unternehmen seine Server und Daten aufbewahrt. Da es nunmehr den ersten Berührungspunkt für die Interaktion mit Kunden darstellt, muss es in der Lage sein, Services hochgradig sicher und zuverlässig bereitzustellen. In immer mehr Branchen bildet das Rechenzentrum die Grundlage für neue Geschäftsmodelle.

Aufgrund der Veränderungen in den Rechenzentrumarchitekturen und der neuen Anwendungsfälle, die aus diesen Entwicklungen resultieren, sind Unternehmen zunehmend besorgt um die Sicherheit ihrer Rechenzentren. Die schwerwiegenden Sicherheitsvorfälle bei einigen der weltgrößten Einzelhandels- und Finanzkonzernen, die in jüngster Vergangenheit für Aufsehen sorgten, haben diese Bedenken zusätzlich verstärkt und führten dazu, dass das Thema Sicherheit mittlerweile auch auf Führungs- und sogar Vorstandsebene immer stärker priorisiert wird. Next-Generation Firewalls,

Sandboxing, sichere Web-Gateways und ähnliche Lösungen können die Sicherheit am Perimeter verbessern. Das Rechenzentrum ist in dieser Hinsicht jedoch mit völlig anderen Herausforderungen verbunden.

Zunächst einmal unterscheiden sich Management- und Bereitstellungsprozesse am Perimeter erheblich von den entsprechenden Prozessen im Rechenzentrum. Wie bereits erwähnt, sind Rechenzentren heute enorm dynamisch: Ständig werden neue Ressourcen erstellt, verschoben und wieder außer Betrieb genommen. Dies erfordert Security-Lösungen, die das Richtlinienmanagement und die Skalierung vereinfachen. Denn in einer solchen Umgebung ist die manuelle Durchführung dieser Aufgaben keine Option, sondern führt in der Regel zu einem Zusammenbruch des Sicherheitsstatus. Die Security-Lösungen müssen eng mit den anderen Komponenten des Rechenzentrums-Fabrics integriert sein, damit ein konsistenter Sicherheitsansatz und optimale Orchestrierung gewährleistet werden können.

Häufig ist zudem eine Vielzahl unterschiedlicher Technologien im Rechenzentrum im Einsatz, da nur wenige Unternehmen ein komplett neues Rechenzentrum errichten können. In den meisten Fällen laufen daher Alt- und Neusysteme nebeneinander, wobei die Anwendungen sowohl auf physischen als auch auf virtuellen Ressourcen ausgeführt werden. Security-Lösungen müssen diese uneinheitlichen Umgebungen ebenso unterstützen können wie intelligentere Umgebungen, die Software-defined Networking (SDN) zum Einsatz bringen und die Nutzung von NFV-Lösungen (Network Function Virtualization) von Netzwerk-Service-Providern vereinfachen. Diese intelligenten Netzwerkfunktionen erleichtern die Entwicklung und Unterstützung von Hybrid Clouds und geografisch verteilten Umgebungen, da sie die gesamte Infrastruktur als einen logischen Standort behandeln.

Bereitstellung und Management sind jedoch erst der Anfang. Die Auswirkungen der verschiedenen Verkehrsmuster im Rechenzentrum müssen ebenfalls berücksichtigt werden, insbesondere vor dem Hintergrund, dass sich der Großteil des Verkehrs im Rechenzentrum ausschließlich zwischen virtuellen Systemen bewegt, ohne je eine physische Appliance zu erreichen. Für ein sicheres Design des Rechenzentrums sind die Übersicht und Kontrolle über diesen Verkehr entscheidend. In einem optimalen Design erfolgt die Überwachung des Verkehrs zwischen virtuellen Systemen durch eine virtuelle Sicherheitsinstanz. Andernfalls muss der Datenverkehr zur Überprüfung aus dem virtuellen Segment heraus an eine physische Appliance geleitet werden, bevor er zurück an das virtuelle Ziel übermittelt wird. Dies beeinträchtigt jedoch die Performance und erzeugt Latenz. Wichtig außerdem: Geografisch verteilte und häufig migrierte Ressourcen erzeugen asymmetrische Verkehrsflüsse. Security-Lösungen müssen in der Lage sein, diese ohne Leistungseinbußen zu untersuchen.

Ein erheblicher Unterschied zum Perimeter besteht darüber hinaus im Hinblick auf den Anwendungsdatenverkehr im Rechenzentrum, da hier die unternehmensspezifischen Anwendungen gehostet werden. Für das Rechenzentrum sind herkömmliche Next-Generation Firewall (NGFW)-Technologien daher ungeeignet, da diese nur öffentliche Webanwendungen (z. B. Facebook, Twitter oder YouTube) – also vom Unternehmens-Edge ausgehende Bedrohungen – abdecken. Erforderlich wären jedoch Security-Lösungen, die einen Überblick über die unternehmensspezifischen Anwendungen bieten und gleichzeitig den zunehmenden Trend zur Digitalisierung von Unternehmensdaten unterstützen. Denn so kann der Sicherheitskontext ermittelt und optimale Performance sichergestellt werden.

Geschäftsvorteile eines sicheren Rechenzentrums

Zu allererst muss sichergestellt sein, dass die Security-Lösungen im Rechenzentrum in den zentralen Managementprozess eingebunden sind – entweder im Hinblick auf die allgemeine Sicherheit oder aus Sicht der SDN-Orchestrierung (Software-defined Networking). In einer Rechenzentrumsumgebung kann Sicherheit nicht manuell durch die IT-Teams konfiguriert werden. Security-Lösungen, die keine dynamische Bereitstellung und Skalierung entsprechend der Ressourcennutzung unterstützen, werden nicht eingesetzt.

Implementieren Unternehmen in ihren Rechenzentren richtliniengesteuerte, skalierbare und leistungsfähige Security-Produkte, können ihre Security-Teams deutlich effizienter arbeiten. Die ansonsten für die Überwachung und Erkennung von Sicherheitsbedrohungen benötigte Zeit können die Teams in Aufgaben mit höherer Wertschöpfung investieren. Richtliniengesteuerte Security-Lösungen steigern die Effizienz durch Automatisierung. Durch die Zentralisierung der Security-Lösungen im Rechenzentrum wird zudem eine stärker konsolidierte Umgebung geschaffen, die eine effizientere Erkennung von Sicherheitsbedrohungen ermöglicht und deren Beseitigung vereinfacht. Für die Security-Teams bedeutet das erhebliche Zeitgewinne. Denn nicht nur die Verwaltung der Security-Lösungen geht deutlich einfacher vonstatten, auch der Arbeitsaufwand für die Konsolidierung der Informationen aus voneinander getrennten Bereichen der Sicherheitsarchitektur im Rechenzentrum wird um ein Vielfaches reduziert.

Ebenso wichtig wie die Verwaltung ist die Effektivität der Absicherung. Die Lösungen müssen in der Lage sein, sowohl bekannte als auch unbekannte Bedrohungen zu erkennen und darüber hinaus Maßnahmen für deren Beseitigung unterstützen. Unternehmen erkennen mittlerweile den Wert von proaktiven Security-Lösungen und nehmen zunehmend Abstand von Ansätzen für den Bedrohungsschutz, in deren Rahmen Richtlinien nur reaktiv festgelegt werden. Wenn sie in der Lage sind, mehr Sicherheitsbedrohungen aufzuspüren, bevor diese Ausfälle oder Unterbrechungen mit Auswirkungen auf die Benutzer verursachen können, erzielen sie Effizienzgewinne sowohl bei den Security-Teams als auch im Geschäftsbetrieb.

Können Sicherheitsbedrohungen proaktiv erkannt und eingedämmt werden, müssen IT-Teams weniger wertvolle Arbeitszeit dafür aufbringen, Vorfälle zu beheben und aufwendige Bereinigungen durchzuführen. Das bedeutet: Die IT kann ihren Fokus wieder vollständig auf Aufgaben richten, die zur Produktivität des Unternehmens beitragen (z. B. Test und Entwicklung neuer Anwendungen und Services). Eine leistungsfähige Security-Lösung für das Rechenzentrum erleichtert es IT-Teams erheblich, Sicherheitsbedrohungen zu erkennen und Sicherheitsverletzungen und Infektionen vorzubeugen. Fortschrittliche Analysefunktionen unterstützen sie zudem dabei, die Auswirkungen für Benutzer so gering wie möglich zu halten, sollte es doch einmal zu einem Vorfall kommen. Die Reduzierung von Sicherheitsvorfällen auf ein Minimum bedeutet nicht nur erhebliche Zeitersparnisse der IT-Teams, auch damit verbundene Prüfungsanforderungen können leichter erfüllt werden.

Security-Lösungen für Rechenzentren verbessern darüber hinaus die Sicherheit und Performance von Business-Anwendungen. Dadurch steigt die Produktivität der Endbenutzer, da diese in erheblichem Maß von der Performance und Verfügbarkeit dieser – häufig vom Unternehmen selbst entwickelten – Anwendungen abhängig sind. Wird die Häufigkeit und Dauer von Wartungsarbeiten für diese Anwendungen reduziert, können sie produktiver arbeiten. Unternehmen, die auf die Sicherheit kritischer IT-Infrastruktur wie ihrem Rechenzentrum vertrauen, sind zudem meist offener für neue

Geschäftsmöglichkeiten. Dadurch können sie neue Einnahmequellen erschließen und stärker proaktive und zukunftsorientierte Strategien umsetzen. Für viele Unternehmen sind Ausfälle des Rechenzentrums eine anhaltende Sorge, da sie sofort Einnahmeausfälle zur Folge haben. Da sie ungeplante Ausfallzeiten aufgrund von Sicherheitsvorfällen jedoch auf ein Minimum reduzieren können, lassen sich dadurch auch Einnahmeausfälle minimieren, die durch den Ausfall der Systeme und Anwendungen entstehen, die ihre internen und externen Kunden nutzen.

Beispiel einer Security-Lösung: die Cisco Secure Data Center-Architektur

Der Ansatz von Cisco für skalierbare und dynamische Sicherheitsfunktionen in Rechenzentrumsumgebungen spiegelt sich im Großteil des Produktportfolios des Unternehmens wider. Integrationen zwischen den zentralen Netzwerkprodukten, den Unified Computing-Angeboten sowie den Virtualisierungs- und SDN-Portfolios liefern eine ganzheitliche Strategie für das Rechenzentrum. Security ist in den vergangenen 12 Monaten ein wichtiger Bestandteil der Kernstrategie von Cisco geworden und spielt deshalb auch eine wichtige Rolle in der Lösungspalette für Rechenzentren. Cisco Validated Designs (CVDs) bieten Best Practices für die einfache und effektive Bereitstellung von Cisco Security-Produkten und erleichtern es Kunden, die passenden Lösungen für ihre individuelle Umgebung zu ermitteln. Die Cisco Secure Data Center-Lösung setzt sich aus den drei Kernkomponenten Cisco ASA 5585-X, FirePOWER Services und ASAv zusammen:

- Die 5585-X Adaptive Security Appliance ist das High-End-Firewall-Produkt von Cisco. Sie wurde speziell für Rechenzentrumsumgebungen entwickelt und nutzt eine modulare Architektur mit zwei Blades für einen Durchsatz von bis zu 40 Gbit/s, 350.000 Verbindungen pro Sekunde und 10 Millionen gleichzeitigen Verbindungen als Standalone-Appliance mit 2 HE. Die Portdichte kann, falls erforderlich, durch zusätzliche E/A-Module erhöht werden. Die 5585-X unterstützt zudem Clustering von bis zu 16 einzelnen Appliances für eine lineare Skalierung des Durchsatzes auf bis zu 640 Gbit/s. Die Appliance kann als traditionelle Layer-2- oder Layer-3-Firewall und VPN-Konzentrator verwendet werden, durch Ergänzung von FirePOWER Services stehen zusätzlich erweiterte Funktionen zur Verfügung.
- FirePOWER Services für ASA Firewalls oder FirePOWER Standalone-Appliances bieten fortschrittliche Funktionen zur Bedrohungserkennung über eine Vielzahl von Anwendungsfällen hinweg, auch für das Rechenzentrum. Next-Generation IPS (NGIPS) und Advanced Malware Protection (AMP) schützen vor gezielten Angriffen mit benutzerspezifischer Malware. Das FireSIGHT Management Center führt Indications of Compromise über die gesamte Infrastruktur hinweg zusammen, um die Problembehebung zu beschleunigen und die Zugriffszeit für Angreifer so weit wie möglich einzuschränken. FirePOWER Services greifen zudem auf die Bedrohungsinformationen der Cisco TALOS Forschungsgruppe zurück, die Malware, Angriffe und andere Bedrohungen untersucht. Dies ermöglicht eine bessere Erkennung über den gesamten Kundenstamm hinweg.
- Die ASAv ist eine vollständig virtualisierte Instanz der physischen Cisco Adaptive Security Appliance. Die ASAv ist Hypervisor-unabhängig und bietet eine umfassendere Übersicht und Kontrolle über den gesamten Verkehr zwischen virtuellen Systemen – unabhängig von der Plattform. Richtlinienprofile können über Cisco Security Manager verwaltet werden, wodurch Konsistenz über physische und virtuelle Umgebungen hinweg gewährleistet wird, oder über den Cisco Application Policy Infrastructure Controller (APIC) für Application Centric Infrastructure (ACI)-Bereitstellungen. Mithilfe des APIC können Sicherheitsrichtlinien an bestimmte Anwendungen und Security-Services gebunden werden und je nach Netzwerkbedarf in Betrieb genommen oder außer Betrieb gesetzt werden.

IDC Methodik zur Quantifizierung der Geschäftsvorteile eines sicheren Rechenzentrums

Um den quantifizierbaren Nutzen von Security-Produkten für Rechenzentren (z. B. Die Architekturlösungen des Cisco Secure Data Center) zu ermitteln, hat IDC auf Basis von Kennzahlen die finanziellen Einsparungen berechnet. Dazu wurde eine Untersuchung herangezogen, die über die vergangenen zwei Jahre unter Benutzern dieser Art von Security-Produkten für Rechenzentren durchgeführt wurde. Dabei hat IDC wichtige Kennzahlen im Hinblick auf den IT-Aufwand für die Absicherung von IT- und Rechenzentrumsumgebungen analysiert, darunter die proaktive Erkennung von Bedrohungen durch IT-Sicherheitsteams, die Zeit, die IT-Sicherheitsteams benötigen, um auf Bedrohungen zu reagieren, die Kosten, die durch die Auswirkungen von Sicherheitsvorfällen im Rechenzentrum auf die Arbeitszeit von IT-Sicherheitsteams und Endbenutzern entstehen, sowie andere Kosten im Zusammenhang mit Sicherheitsverletzungen im Rechenzentrum. Dann hat IDC die Vorteile, die sich durch die Nutzung von Security-Produkten für Rechenzentren ergeben, in drei Hauptkategorien von Kosteneinsparungen unterteilt: Produktivitätssteigerungen bei IT-Mitarbeiten, Produktivitätssteigerungen bei Endbenutzer durch die Minimierung von Sicherheitsrisiken und Produktivitätssteigerungen bei Endbenutzern durch betriebliche Effizienz. Diese Ergebnisse wurden normiert, indem sie als finanzielle Vorteile für ein durchschnittliches Unternehmen mit 1.000 IT-Endbenutzern ausgedrückt wurden.

Kostenreduzierung

Unternehmen können mit Security-Produkten für Rechenzentren in vielerlei Hinsicht Kosteneinsparungen erzielen. Durch Upgrades auf Security-Produkte für Rechenzentren, die eine höhere Transparenz und Performance bieten, können Unternehmen die Kosten für sicherheitsbezogene Produkte reduzieren, u. a. da sie weniger Firewalls benötigen. Zusätzlich können die Hardware- und Softwarekosten durch eine bessere Integration zwischen den einzelnen Security-Produkten und der zugrunde liegenden Hardware und Software gesenkt werden. Beispielsweise können Unternehmen durch eine engere Integration der Security-Produkte im Rechenzentrum die Virtualisierung ausweiten und so Kosten senken. Security-Produkte für Rechenzentren mit einer höheren Performance können zur Reduzierung von Bandbreitenkosten beitragen oder Leistungssteigerungen im Netzwerk ermöglichen, ohne dass die Bandbreite erhöht werden muss. Da die Zahl schwerwiegender Sicherheitsvorfälle im Rechenzentrum reduziert wird, sinkt das Risiko für die Zahlung von Bußgeldern, Entschädigungszahlungen oder Gerichtsverfahren aufgrund von Sicherheitsverletzungen.

Produktivität der IT-Mitarbeiter

Zentralisierte und konsolidierte Security-Lösungen für Rechenzentren erhöhen die Effizienz und Produktivität der IT-Sicherheitsteams. Sie benötigen weniger Zeit für die Überwachung voneinander getrennter Lösungen und das Zusammentragen von Informationen aus diesen. Kann mithilfe von Security-Lösungen für Rechenzentren zudem die Anzahl der Sicherheitsverletzungen und Infektionen mit Auswirkungen auf die Benutzer reduziert werden, müssen die IT-Sicherheitsteams weniger Zeit in die Behebung von Ausfällen und die Bearbeitung von Servicedesk-Anfragen investieren. Die meisten Unternehmen verfügen in der Regel nur über wenige IT-Sicherheitsmitarbeiter. Wenn diese Mitarbeiter nun weniger häufig auf Sicherheitsvorfälle reagieren müssen und mehr Zeit für innovative, zukunftsorientierte, strategische Aufgaben haben, kann dies ein erheblicher Vorteil sein. Um die Vorteile der Zeiteinsparungen für IT-Mitarbeiter durch den Einsatz von Sicherheitsprodukten in

Rechenzentren zu quantifizieren, hat IDC die Zeiteinsparungen mit einem durchschnittlichen Gesamtgehalt von 100.000 US-Dollar pro Jahr multipliziert.

Risikominimierung/Benutzerproduktivität

Sind Security-Lösungen für Rechenzentren in der Lage, mehr Sicherheitsbedrohungen zu erkennen und abzuwehren, entstehen Produktivitätsvorteile für alle Mitarbeiter. Eine stärkere Sicherheit im Rechenzentrum bedeutet, dass Sicherheitsverletzungen und Infektionen weniger häufig die Verfügbarkeit von Business-Anwendungen beeinträchtigen, die über die Rechenzentren ausgeführt werden. Auch die Zeit, die benötigt wird, um diese Anwendungen wieder einsatzbereit zu machen, wird minimiert. So kommt es seltener zu Unterbrechungen für Endbenutzer, die von diesen Anwendungen abhängig sind, sodass die produktive Nutzung der Arbeitszeit erhöht wird. IDC misst die Auswirkungen der Produktivitätsgewinne der Benutzer und multipliziert die Zeit der höheren Verfügbarkeit von Anwendungen, Programmen und Daten, die Endbenutzer für ihre Arbeit benötigen, mit einem Gesamtgehalt von 67.500 US-Dollar pro Jahr, skaliert mit einem Produktivitätsfaktor, um die Tatsache zu berücksichtigen, dass Benutzer während der Unterbrechungen durch Sicherheitsvorfälle im Rechenzentrum weiterarbeiten können.

Geschäftlicher Nutzen

Die Untersuchungen von IDC zur Verwendung von Security-Produkten im Rechenzentrum zeigen, dass ein geschäftlicher Nutzen generiert werden kann, wenn der durch Sicherheitsbedrohungen bedingte Verlust von produktiver Arbeitszeit für Benutzer und IT-Mitarbeiter reduziert werden kann und die daraus resultierenden Kosten minimiert werden. Die Vorteile, die sich für die IT-Sicherheitsmitarbeiter ergeben, zeigen sich vor allem in der Zeit, die für die Reaktion auf Vorfälle benötigt wird: Bei den Unternehmen in den Untersuchungen konnte der Zeitaufwand für Reaktionen auf Vorfälle um durchschnittlich 62,9 % reduziert werden. Durch die Verwendung von Security-Produkten für Rechenzentren können Unternehmen zudem die Zeit für die Durchführung von Sicherheitsprüfungen (28,2 % weniger Zeitaufwand) und für die Verwaltung und Wartung von Sicherheitsverfahren (Effizienzgewinn von 15,0 %) minimieren.

TABELLE 1

Vorteile von Security-Produkten für Rechenzentren

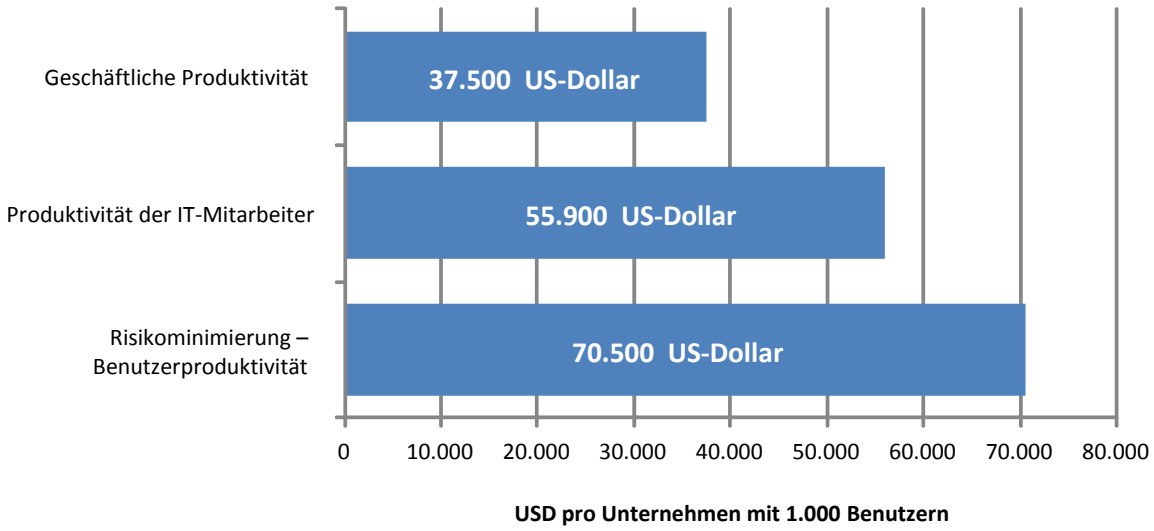
Produktivitätsvorteile für IT-Mitarbeiter	
Geringerer Zeitaufwand für Sicherheitsmanagement	15,0 %
Geringerer Zeitaufwand für die Reaktion auf Vorfälle	62,9 %
Geringerer Zeitaufwand für Sicherheitsprüfungen	28,2 %
Vorteile durch Risikominimierung	
Weniger Ausfallzeiten	51,9 %

Quelle: IDC, 2014

Die Untersuchungen von IDC ergaben, dass ein Unternehmen mit 1.000 Benutzern, das Security-Lösungen für Rechenzentren nutzt, aufgrund von weniger Sicherheitsvorfällen mit Auswirkungen für Benutzer, weniger Infektionen und weniger Ausfallzeit, Produktivitätsvorteile im Wert von 70.500 US-Dollar pro Jahr erzielen kann. Diese Security-Lösungen für Rechenzentren ermöglichen außerdem Zeiteinsparungen für IT-Sicherheitsteams und größere Effizienz. Für ein Unternehmen mit 1.000 Benutzern ergeben sich daraus Vorteile in Höhe von 55.900 US-Dollar pro Jahr. Durch die Steigerung der betrieblichen Effizienz, die zu Umsatzsteigerungen führt, können sich durch Sicherheitslösungen für Rechenzentren im Jahresdurchschnitt zusätzliche Vorteile von im Schnitt 37.500 US-Dollar pro Unternehmen mit 1.000 Mitarbeitern ergeben.

ABBILDUNG 1

Typische Vorteile für ein Unternehmen mit 1.000 Benutzern, die aus der Eingrenzung der Auswirkungen auf den Rechenzentrumsbetrieb durch Sicherheitsvorfälle resultieren



Quelle: IDC, 2014

Informationen zu IDC

Die International Data Corporation (IDC) ist der weltweit führende Anbieter von Marktforschung, Beratung und Events im Bereich der IT-, Telekommunikations- und Technologiebranche. IDC unterstützt IT-Experten, Führungskräfte und Investoren bei der faktenbasierten Entscheidungsfindung zu Technologieinvestitionen und Geschäftsstrategien. Über 1.000 IDC-Analysten liefern globales, regionales und lokales Know-how zu technologischen und geschäftlichen Potenzialen und Trends in über 110 Ländern weltweit. Seit 50 Jahren liefert IDC seinen Kunden strategische Einblicke als Grundlage für das Erreichen ihrer wichtigsten Geschäftsziele. IDC ist eine Tochtergesellschaft von IDG, dem weltweit führenden Anbieter für Medien, Marktforschung und Events im Bereich der Technologiebranche.

Weltweite Zentrale

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com