Whitepaper

# Bitdefender®

# Virtualisierung: Neue Sicherheits-Herausforderungen für Unternehmen

## Eine Umfrage bei deutschen IT-Entscheidungsträgern

# Executive Summary

Virtualisierung ist in deutschen Unternehmen mittlerweile zu einem strategischen Faktor geworden, dennoch können bislang viele die notwendigen Sicherheitsanforderungen nicht erfüllen, die eine solche Umgebung mit sich bringt. Das ist das Ergebnis einer Bitdefender-Umfrage bei 100 IT-Entscheidungsträgern deutscher Unternehmen mit mehr als 1.000 PC-Arbeitsplätzen. Hybride Infrastrukturen sind mittlerweile ein wichtiger Bestandteil in einer großen umfassenden Architektur im Unternehmensumfeld geworden, dieser neuen Welt müssen sich CIOs anpassen. Die Umfrage, die von iSense durchgeführt wurde, zeigt die wichtigsten Sicherheitsbedenken und Probleme auf. Welche Cyber-Bedrohungen können Unternehmen heutzutage noch nicht abwehren? Was sind die Hauptanliegen hinsichtlich des Sicherheitsmanagements von hybriden Infrastrukturen? Warum haben IT-Entscheider Angst um ihre Jobs?

# Die wichtigsten Erkenntnisse

- 34 Prozent der IT-Entscheidungsträger befürchten hohe finanzielle Entschädigungszahlungen im Falle eines Sicherheitsvorfalls, 44 Prozent der Befragten haben sogar Angst, ihren Job zu verlieren.
- Ein Drittel der Entscheider ist hinsichtlich des Sicherheitsmanagement von hybriden Infrastrukturen „besorgt“ oder „sehr besorgt“.
- Die größten Sicherheitsbedenken bei der Migration von Daten in ein Hybrid-Modell sind: die Sicherheit der gespeicherten Daten (78 Prozent), die Sicherheit der Daten während der Datenübertragung (60 Prozent), die vergrößerte Angriffsfläche (64 Prozent), der mangelnde Einblick in virtuelle Instanzen (58 Prozent) und die Sicherheit von Backups und Snapshots (33 Prozent).
- Die wichtigsten Sicherheitsprobleme nach der Migration in eine hybride Infrastruktur sind: Zugriff von unautorisierten Geräten (37 Prozent), fehlende Richtlinien (36 Prozent), mangelnde Transparenz (34 Prozent), zusätzliche Kosten (32 Prozent) und mangelnde Verfügbarkeit (28 Prozent). IT-Experten sind nicht in der Lage, Workloads über Clouds zu überwachen (35 Prozent), 38 Prozent der Umfrageteilnehmer stimmen zu, dass die Netzwerkkontrolle und -überwachung in der Cloud nicht ausreichend ist.
- Cyber-Bedrohungen auf die Unternehmen nicht vorbereitet sind: Phishing (44 Prozent), physische Sicherheit (42 Prozent), externe Angriffe (41 Prozent), Insider-Sabotage (37 Prozent), Malware / Viren / Intrusionen (35 Prozent).

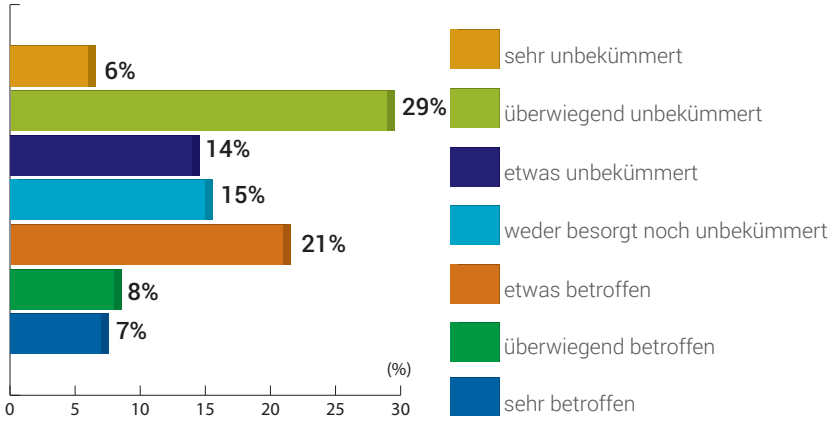
Wie Gartner kürzlich in einem Bericht prognostizierte, wird die Cloud bis 2020 am häufigsten in der hybriden Form genutzt werden. Bis zum Ende dieses Jahrzehnts werde der reine Betrieb aus der Cloud weitgehend verschwinden. Das Beratungsunternehmen schätzt, dass bis 2019 mehr als 30 der 100 größten Anbieter neue Investitionen in Software von Cloud-First auf Cloud-Only verschoben haben.

„Abgesehen davon, dass viele Organisationen mit einer „No-Cloud-Politik" tatsächlich eine Nutzung der Cloud als Schatten-IT haben, glauben wir, dass diese Position zunehmend unhaltbar wird", erläutert Jeffrey Mann, Research Vice President bei Gartner. „Die Cloud wird zunehmend die Standardoption für eine Software-Implementierung sein. Das gleiche gilt für kundenspezifische Software, die sich immer öfter zu einer Variante der öffentlichen oder privaten Cloud entwickeln wird." Bis 2020 wird eine Unternehmenspolitik ohne Cloud so selten vorkommen wie heute eine Unternehmenspolitik ohne Internet, ist sich Gartner sicher. „Technologieanbieter werden zunehmend davon ausgehen können, dass ihre Kunden Cloud-Kapazitäten nutzen." [1]

Die Cloud-Akzeptanz und die künftige stärkere Nutzung von hybriden Infrastrukturen bringen unbekannte Sicherheitsanforderungen mit sich. Diesen müssen CIOs mit neuen, bahnbrechenden Technologien entgegentreten, die in der Lage sind, Zero-Day-Exploits, Advanced Persistant Threats (APTs) und andere verheerende Arten von Internetkriminalität zu bekämpfen.

Die Bitdefender-Studie hat ergeben, dass ein Drittel der IT-Entscheidungsträger im Falle eines Sicherheitsvorfalls befürchten, finanzielle Entschädigungen zahlen zu müssen, 44 Prozent haben Angst um ihren eigenen Job. Darüber hinaus sind 36 Prozent der IT-Entscheidungsträger besorgt oder sehr besorgt hinsichtlich des Sicherheitsmanagements von hybriden Infrastrukturen.

**Bedenken hinsichtlich des Sicherheitsmanagements hybrider Infrastrukturen (%)**



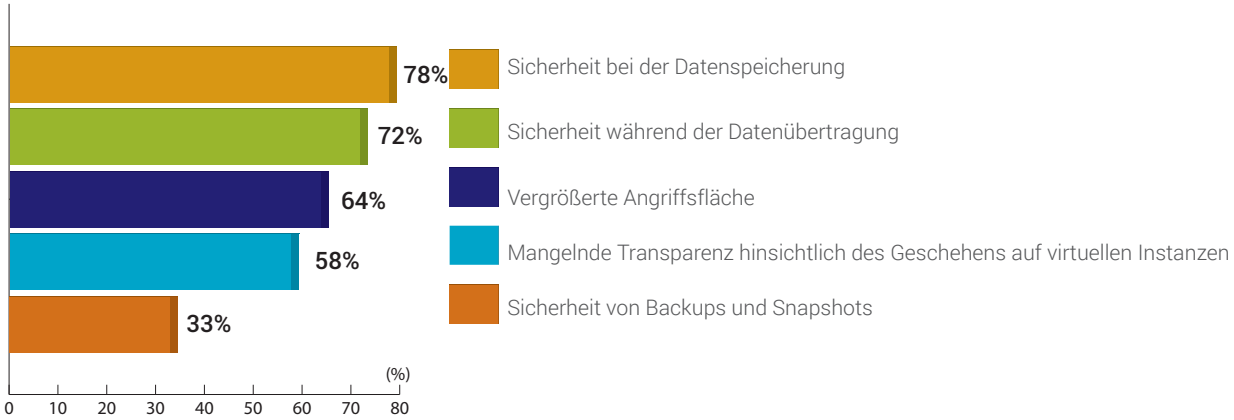

In den letzten beiden Jahren sind die Sicherheitsvorfälle und -verletzungen in Unternehmen durch die signifikante Zunahme der dokumentierten APT (Advance Persistent Threat)-Angriffe auf Top-Konzerne oder staatliche Einrichtungen (wie APT-28[2]) deutlich gestiegen. Diese Art von Angriffen dient dazu, über einen längeren Zeitraum an sensible Daten zu gelangen oder industrielle Prozesse lahm zu legen. Daher haben Sicherheitsthemen eine immer höhere Priorität, wobei in den meisten Unternehmen auf Vorstandsebene die Beschlüsse gefasst werden. Sowohl IT-Entscheider als auch CEOs sind nicht nur wegen der Kosten, die ein Sicherheitsvorfall zur Folge hat (nicht verfügbare Ressourcen und / oder verlorenes Geld), besorgt, sondern auch, weil die Reputation eines Unternehmens gefährdet ist, wenn Kundendaten verloren gehen oder in die Hände von Kriminellen gelangen. Wie sich in der Vergangenheit gezeigt hat, ist die Medienberichterstattung über einen Sicherheitsvorfall umso größer, je komplexer die Malware ist, die sie verursacht hat. Darüber hinaus hat die Migration von Unternehmensinformationen von traditionellen Rechenzentren in die Cloud-Infrastruktur die Angriffsfläche der Unternehmen deutlich erhöht und damit neue Bedrohungen und weitere Sorgen für die CIOs hinsichtlich der Sicherheit ihrer Daten mit sich gebracht.

Die Umfrage von Bitdefender zeigt, dass die größten Sicherheitsbedenken der IT-Entscheider bei der Datenmigration in ein hybrides Modell die Sicherheit während der Datenspeicherung (78 Prozent) betreffen. Die Sicherheit der Daten während der Übertragung (72 Prozent) und die vergrößerte Angriffsfläche (64 Prozent) stehen ebenfalls ganz oben auf der Liste der Sicherheitsbedenken.

Security-Spezialisten empfehlen, dass eine Organisation, die sich für eine hybride Cloud-Lösung entschieden hat, zunächst eine Datenanalyse vornehmen sollte, bei der die Daten hinsichtlich ihrer Sensibilität – sowohl für das Unternehmen als auch seine Kunden – bewertet werden. Kritische, persönliche und private Daten, die sich auf geistiges Eigentum beziehen, müssen vor Ort gespeichert werden und dürfen nur autorisierten Mitarbeitern zugänglich gemacht werden.

1 "Gartner Says By 2020, a Corporate No-Cloud Policy Will Be as Rare as a No-Internet Policy Is Today", June 22, 2016, http://www.gartner.com/newsroom/id/3354117
2 http://download.bitdefender.com/resources/media/materials/white-papers/en/Bitdefender_In-depth_analysis_of_APT28%E2%80%93The_Political_Cyber-Espionage.pdf

**Die wichtigsten Sicherheitsbedenken bei der Migration von Daten in ein Hybrid-Modell (%)**




Die Sicherheit der Daten während der Speicherung oder der Übertragung sind die größten Anliegen von CIOs bei der Verschiebung von IT-Architekturen hin zu den neuesten öffentlichen Cloud-Services, die gemeinsam mit eigenen privaten Rechenzentren genutzt werden. Die Sicherheitsspezialisten von Bitdefender empfehlen, dass jeder Datentransfer zwischen dem Client und dem Cloud-Dienstleister verschlüsselt sein sollte, um Man-in-the-Middle-Angriffe zu vermeiden, die alle gesendeten Daten abfangen und entschlüsseln können. Zudem sollten alle lokal oder in der Cloud gespeicherten Daten verschlüsselt werden, um sicherzustellen, dass Cyberkriminelle diese - im Falle eines Angriffs oder eines unberechtigten Zugriffs - nicht lesen können.

Frühere Umfragen haben ergeben:

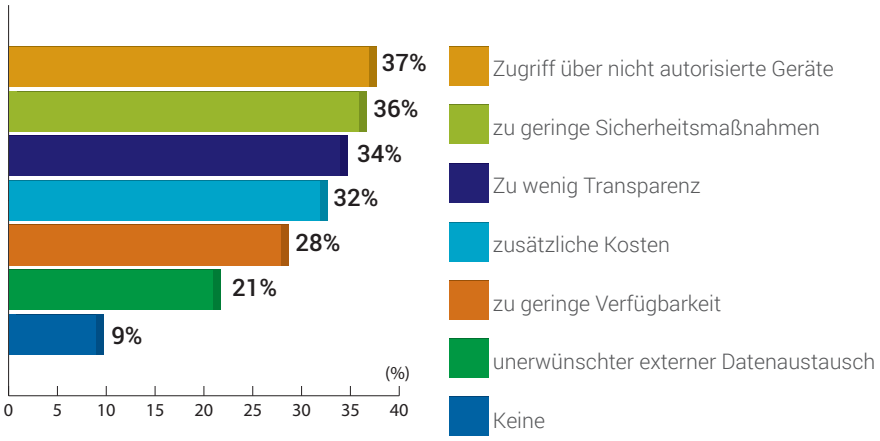
1. Die Cloud-Nutzung wird für eine wachsende Zahl von Unternehmen Realität. Dabei geben die meisten Unternehmen an, dass Cloud-Sicherheitsvorfälle aufgetreten sind. Fast die Hälfte der gemeldeten Vorfälle ist auf unerwünschte externe Freigaben sowie auf einen Zugriff mit nicht autorisierten Geräten zurückzuführen. [3]

2. Die Hauptgründe bei der Auswahl eines bestimmten Cloud-Anbieters sind für Unternehmen Effizienz (41 Prozent der Befragten) und Kosten (37 Prozent), gefolgt von Reputation und Kundenservice. Sicherheit wird lediglich an fünfter Stelle genannt. Security comes only fifth.[4]

Die wichtigsten Sicherheitsprobleme nach der Migration in eine hybride Infrastruktur sind laut der Bitdefender-Umfrage: der Zugriff über nicht autorisierte Geräte (37 Prozent), fehlende Richtlinien (36 Prozent), zu geringe Transparenz (34 Prozent), zusätzliche Kosten (32 Prozent) und eine mangelnde Verfügbarkeit (28 Prozent).


3 "Report on mitigating risks for cloud applications". Cloud Security Alliance and Bitglass conducted a survey of 176 IT security leaders, https://pages.bitglass.com/Mitigating-Risk-For-Cloud-Applications.html
4 "The 2016 global cloud data security study", Gemalto and Ponemon Institute, 2016. Ponemon Institute surveyed 3,476 IT and IT security practitioners in the United States, United Kingdom, Australia, Germany, France, Japan, Russian Federation, India and Brazil.

**Haupt- (Sicherheits-) Probleme nach der Migration auf hybride Infrastrukturen * (%)**




* - Mehrfachnennung möglich

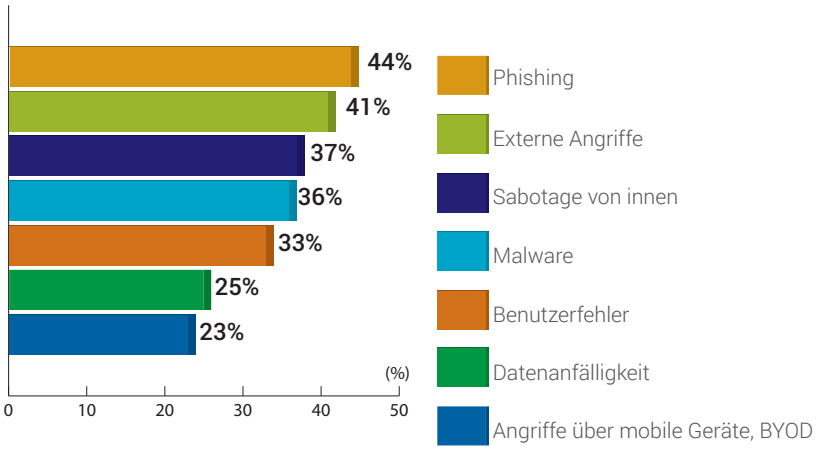
Der Zugriff auf jede Art von Daten, ob in der privaten oder öffentlichen Cloud gespeichert, sollte über mehrere Authentifizierungsmechanismen erfolgen, so die Sicherheitsspezialisten von Bitdefender. Diese Mechanismen sollten über Benutzernamen und Passwörter hinausgehen. Für den Zugriff auf kritische Daten sollten Zwei-Faktor-Authentifizierung oder sogar biometrische Daten eine zusätzliche Kontrolle und Genehmigung für qualifizierte und freigeschaltete Mitarbeiter bieten.

Nur autorisierte Mitarbeiter benötigen einen Zugriff auf kritische und sensible Daten, und dies auch nur unter Einhaltung von strengen Sicherheitsprotokollen und erweiterten Authentifizierungsmechanismen. Neben der Zwei-Faktor-Authentifizierung kann für kritische Systeme auch eine Zwei-Personen-Authentifizierung eingerichtet werden, ähnlich wie bei Finanzinstituten, in denen große Transaktionen stets von zwei oder mehreren Personen genehmigt werden müssen.

Überraschenderweise werden zusätzliche Aufwendungen ebenfalls als Sicherheitsproblem wahrgenommen. Viele IT-Entscheidungsträger befürchten, dass ihr Budget nicht ausreicht, um alle Cyber-Bedrohungen zu bekämpfen, zu erkennen oder zu verhindern, oder dass sie künftige Erweiterungen nicht berücksichtigen können. Einige Befragte geben zu, dass sie unterbesetzt sind. So könnten zusätzliche Investitionen sogar zu neuen Sicherheitsproblemen führen.

Die Bitdefender-Umfrage zeigt, dass Unternehmen nicht vorbereitet sind auf: Phishing (44 Prozent), physische Sicherheitsvorfälle (42 Prozent), externe Angriffe (41 Prozent), interne Angriffe (37 Prozent), Malware / Viren / Intrusionen (36 Prozent), Benutzerfehler (33 Prozent), Datenanfälligkeit (25 Prozent) und mobile Geräteangriffe oder BYOD (23 Prozent).

**Cyber-Bedrohungen, die Unternehmen nicht handhaben können sind (%)***




* - Mehrfachnennung möglich

Phishing-Angriffe sowie externe und interne Attacken stellen ein erhebliches Risiko dar und zählen zu den wichtigsten Bedrohungen für Unternehmen, auf die sie nicht vorbereitet sind. Viele CIOs sind sich nicht darüber bewusst, dass sich Cyber-Kriminelle virtuell lange Zeit in Organisationen aufhalten können, ohne entdeckt zu werden – APTs werden oftmals genutzt, um eine Entdeckung zu vermeiden.

Cyber-Kriminelle versuchen von sich und dem was sie tun abzulenken, während diese Cyber-Attacken Auswirkungen auf Geschäftsentscheidungen, Fusionen / Übernahmen und die Wettbewerbsposition haben.[5]

„Um die Risiken von internen Angriffen und Benutzerfehlern einzugrenzen, sollten Unternehmen strenge Richtlinien und Protokolle etablieren. Sie müssen die Möglichkeiten der Mitarbeiter hinsichtlich der Nutzung der Ausrüstung und Infrastruktur sowie die Privilegien innerhalb des Firmennetzwerkes einschränken", erklärt Bogdan Botezatu, Senior E-Threat-Spezialist bei Bitdefender. „Die IT-Abteilung muss Richtlinien für eine ordnungsgemäße Verwendung der Geräte schaffen und sicherstellen, dass diese auch umgesetzt werden."

Informationssicherheits-Teams und die Infrastruktur sind an die neuen digitalen Geschäftsanforderungen anzupassen, gleichzeitig muss mit der zunehmenden Advanced-Threat-Umgebung entsprechend umgegangen werden, empfiehlt Gartner. Verantwortliche für Sicherheit und Risiko müssen mit den neuesten Technologien ausgestattet werden, um effektive Sicherheits- und Risiko-Management-Programme zu implementieren und aufrechtzuerhalten, die gleichzeitig Möglichkeiten der Digitalisierung vorantreiben und die Risiken verwalten.[6]

Allmählich springen Unternehmen auf den Zug der „hybriden Cloud-Nutzung" auf. Dennoch schätzt Gartner, dass es bis zum Mainstream noch drei bis fünf Jahre dauern wird. Bis Ende 2015 haben sie bislang nur 15 Prozent der Unternehmen eingesetzt. Die Nachfrage nach Hybrid-Cloud-Angeboten wird aber jährlich um durchschnittlich 27 Prozent ansteigen und damit das Wachstum des gesamten IT-Marktes übertreffen, wie die Forscher von MarketsandMarkets ermittelten. Das Unternehmen erwartet, dass der Hybrid-Cloud-Markt von $25 Milliarden US-Dollar im Jahr 2014 auf $85 Milliarden US-Dollar im Jahr 2019 ansteigen wird. [7]

So hat sich die hybride Infrastruktur zu der größten umfassenden Architektur im Unternehmensumfeld entwickelt, bei der der Hypervisor als Vermittler zwischen den virtualisierten Endpunkten und der physischen Hardware dient. Bislang hat die Endpoint Security jedoch nicht den gleichen Paradigmenwechsel erlebt. Die herkömmliche Sicherheit auf Netzwerkebene kann zwar als virtuelle Anwendung ausgeführt werden, führt jedoch im Wesentlichen die Überprüfung des Netzwerkverkehrs genauso wie vorher aus. Herkömmliche Sicherheitsagenten, die in geschützten Systemen laufen, lagern ihre Scans für mehr Leistung zwar auf virtuelle Appliances aus, unterliegen aber weiterhin den technischen Einschränkungen, die mit dem Betrieb innerhalb der Endpunkt-Betriebssysteme einhergehen.

„Da die Applikationen mittlerweile unternehmenskritisch und Desktop-Server in formale Rechenzentren umgezogen sind, ist die Anzahl der physischen Server in einem Rechenzentrum exponentiell gewachsen und die Verwaltung dieser Umgebung komplex und teuer", erläutert Viorel Canja, Leiter Antimalware und Antispam Labs bei Bitdefender. „Heutzutage wandeln sich Rechenzentren von isolierten Systemen hin zu verknüpften Pools mit virtualisierten Ressourcen, die von mehreren Standorten gemeinsam genutzt werden. Ein komplett virtualisiertes Rechenzentrum ist längst keine Zukunftsvision mehr, sondern Wirklichkeit geworden. Doch während die Vorteile der Virtualisierung von Anwendungen, Desktops, Hardware oder Netzwerken selbstverständlich sind, ist die Sicherheit bislang an diesem neuen Paradigma gescheitert."

Bisher war das Konzept der Endpoint Security auf Sicherheitsagenten beschränkt, die innerhalb eines Host-Betriebssystems auf Endpunkten laufen - den Windows- und Linux-Servern sowie Desktop-Betriebssystemen, auf die alle modernen Organisation angewiesen sind.

Bitdefender hat die technischen Herausforderungen bei[8] der Erstellung einer Anwendung für das Root-Problem gelöst, die den Rechenzentrumsbetreibern Transparenz gewährt und ihnen erlaubt, auf Informationen unterhalb des Betriebssystems zu reagieren. Das Unternehmen ist der einzige Security-Anbieter, der Sicherheit auf dem Ring-1-Level bietet.

„Die Hypervisor Introspection ist ein wichtiger Schritt und revolutioniert die Sicherheit wie wir sie bislang kennen", erklärt Viorel Canja[9]. „Die Virtualisierungstechnologie entwickelt sich weiter, mit einem erhöhten Automatisierungsgrad und umfassenden Rahmenbedingungen für eine effizientere Verwaltung der virtualisierten Umgebung. In diesem Zusammenhang ist die Hypervisor-basierte Introspektionstechnik eine zukunftssichere Weiterentwicklung mit zahlreichen Anwendungsmöglichkeiten in anderen Bereichen und Branchen."

http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf
5 "Creating trust in the digital world", EY's Global Information Security Survey, 2015, http://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2015/$FILE/ey-global-information-security-survey-2015.pdf
http://www.gartner.com/newsroom/id/3347717
6 "Gartner Identifies the Top 10 Technologies for Information Security in 2016", June 15, 2016, http://www.gartner.com/newsroom/id/3347717
http://blogs.wsj.com/cio/2015/10/20/special-report-cios-say-hybrid-cloud-takes-off/
7 SPECIAL REPORT: CIOs Say Hybrid Cloud Takes Off, WSJ, http://blogs.wsj.com/cio/2015/10/20/special-report-cios-say-hybrid-cloud-takes-off/
8 http://businessinsights.bitdefender.com/hypervisor-introspection-fighting-apts-in-business-environment-part-1
9 http://businessinsights.bitdefender.com/hypervisor-introspection-security-virtualized-environments

# Methodik

Die Umfrage wurde im November 2016 von iSense Solutions im Auftrag von Bitdefender bei 100 IT-Sicherheitsexperten (CISOs - 15 Prozent, CIOs / CEOs - 12 Prozent, IT-Manager / Direktoren - 39 Prozent, IT-Systemadministratoren - 25 Prozent, IT - 5 Prozent und andere) durchgeführt, die in Unternehmen mit 1.000 und mehr PC-Arbeitsplätzen in Deutschland über alle Branchen hinweg tätig sind.

Rund 49 Prozent der befragten Organisationen haben über 3.000 Beschäftigte, 6 Prozent zwischen 2.000 und 2.999 sowie 45 Prozent zwischen 1.000 und 1.999.

Fast die Hälfte der Befragten stammt aus der IT-Hard- und -Software / Elektronik- und Elektrotechnikindustrie, 20 Prozent aus der Fertigung, 16 Prozent aus dem Verkehrswesen, 10 Prozent aus der Telekommunikationsbranche, 4 Prozent aus der Automobilindustrie, alle anderen stammen aus Marketing, Medien, Bau, Einzelhandel, Vertrieb oder anderen Branchen. Der durchschnittliche Anteil der Mitarbeiter, die in den befragten Organisationen an Computern arbeiten, liegt bei 70 Prozent.

# Über Bitdefender

Bitdefender ist ein globales Sicherheits-Technologie-Unternehmen und bietet wegweisende End-to-End Cyber-Security-Lösungen sowie Advanced Threat Protection für über 500 Millionen Nutzer in über 150 Ländern.  Seit 2001 ist Bitdefender ein innovativer Wegbereiter der Branche, indem es preisgekrönte Schutzlösungen für Privat- und Geschäftsanwender einführt und entwickelt. Zudem liefert das Unternehmen Lösungen sowohl für die Sicherheit hybrider Infrastrukturen als auch für den Schutz von Endpunkten. Als führendes Security-Unternehmen pflegt Bitdefender eine Reihe von Allianzen sowie Partnerschaften und betreibt eine umfassende Forschung & Entwicklung. Weitere Informationen sind unter www.bitdefender.de verfügbar.

Autor: Răzvan Mureşan

Bitdefender ist ein international aufgestellter Anbieter von Sicherheitstechnologien, dessen Lösungen über ein umfangreiches Netzwerk aus Partnern, Händlern und Wiederverkäufern in über 100 Ländern verfügbar sind. Seit 2001 hat Bitdefender immer wieder mit preisgekrönter Sicherheitstechnologie für Unternehmen und Privatanwender überzeugen können und ist einer der führenden Anbieter von Sicherheitslösungen für Virtualisierungs- und Cloud-Technologien. Bitdefender-Technologie landet regelmäßig an der Spitze einschlägiger Tests und setzt den Maßstab in Sicherheitsstandards, die durch intensive Forschung& Entwicklung, Kooperationen und Partnerschaften selbst den höchsten Ansprüchen gerecht werden. Das gleiche gilt für die strategischen Partnerschaften mit den weltweit führenden Virtualisierungs- und Technologieanbietern. Weitere Informationen unter http://www.bitdefender.de/



BD-Business-Nov.18.2016-TK#: 70585