# Das unterschätzte Security-Risiko:

## Clients, Drucker und Multifunktionsgeräte im Unternehmensnetzwerk

IDC White Paper, gesponsert von HP Inc.

Matthias Zacher

September 2017

IDC
ANALYZE THE FUTURE


## In diesem White Paper

Informationssicherheit und IT-Security stehen derzeit ganz oben auf der Agenda der CIOs, IT-Leiter und IT-Security-Verantwortlichen. Das Thema ist vielschichtig und komplex. Trotz aller Maßnahmen kann heute niemand mehr mit 100-prozentiger Sicherheit sagen, ob seine IT tatsächlich sicher ist. Derzeit treiben folgende drei Themen die Informationssicherheit und IT-Security in allen Unternehmen weiter voran:

1. Die digitale Transformation: Die stärkere Integration von IT und Geschäftsprozessen innerhalb der Unternehmen und über Unternehmensgrenzen hinaus lässt klassische perimeterbasierte Schutzkonzepte immer stärker erodieren. Mobile Endgeräte, das Internet der Dinge und die wachsende Zahl IP-basierter Geräte müssen abgesichert werden. In neuen digitalen Wertschöpfungsketten sind viele Teilnehmer unbekannt. Daraus folgen neue Anforderungen an den Schutz und die Abwehr.

2. Cyberangriffe: Die Anzahl, Intensität und Vielfalt der Angriffe wächst Tag für Tag. Neben breit gestreuten Attacken treten immer häufiger zielgerichtete Angriffe auf. Das erfordert einen veränderten Umgang mit der Informationssicherheit. Hierzu zählen neue technische Lösungsansätze, eine ganzheitliche Sichtweise, Risikoklassifizierungen der IT und Wiederherstellungsmechanismen.

3. Compliance und regulatorische Anforderungen: Gesetzliche und regulatorische Anforderungen wie das Bundesdatenschutzgesetz (neu), die EU-Datenschutzgrundverordnung und die Richtlinien über kritische Infrastrukturen fordern von den Unternehmen Schritte und Maßnahmen, um compliant zu sein.

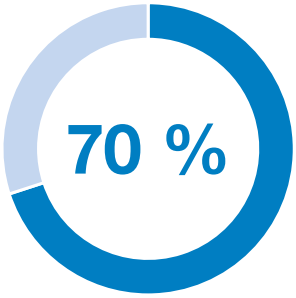
Die unterschiedlichen Endgeräte benötigen künftig mehr Aufmerksamkeit als bisher, denn sie dienen Angreifern immer häufiger als Einfallstore in die Unternehmen. Zwar ist in den meisten Unternehmen ein Basisschutz der Endgeräte vorhanden, eine umfassende Betrachtung des Schutzes über den gesamten Lifecycle von PCs, Druckern und Multifunktionsgeräten fehlt aber häufig. Der Grund: Viele Unternehmen sehen hier nur ein geringes Risiko für den Verlust von Daten oder für Angriffe auf die Unternehmens-IT. Die Folge ist eine mangelhafte Awareness und somit ein erhöhtes Gefährdungsrisiko.

Vor diesem Hintergrund hat IDC im Juli 2017 204 Unternehmen des gehobenen Mittelstands und Großunternehmen in Deutschland befragt, um zu ermitteln, wo sie beim Schutz ihrer Clients stehen und welche Maßnahmen zu ihrem Schutz geplant sind. Ein Schwerpunkt liegt dabei auf Druckern und Multifunktionsgeräten. Dieses White Paper fasst die wichtigsten Einschätzungen der befragten IT- und Security-Verantwortlichen insbesondere mit Blick auf den Schutz vor Cyberrisiken und die Umsetzung von Compliance zusammen und gibt Empfehlungen, wie Unternehmen den Schutz der Clients erfolgreich gestalten können.

# Cyberrisiken bei Clients – komplex und vielschichtig

## Jede IP-Adresse ist ein potenzielles Angriffsziel

Unternehmen sind angreifbar und werden täglich angegriffen. Somit verwundert es nicht, dass mehr als 70 Prozent der befragten Unternehmen Sicherheitsvorfälle in der Verarbeitung von digitalen Daten verzeichnet haben oder Sicherheitsvorfälle nicht ausschließen können.




70 Prozent der befragten Unternehmen haben Sicherheitsvorfälle in der Verarbeitung von digitalen Daten verzeichnet oder können Sicherheitsvorfälle nicht ausschließen

Die weltweit erfolgreichen Attacken mit der Ransomware „WannaCry“ auf Unternehmen und Organisationen, die Rückkehr der Ransomware „Locky“ und anderer Malware belegen deutlich, dass Security-Richtlinien und Konzepte Mängel aufweisen. Daran wird sich mittelfristig nichts ändern. Im Gegenteil, die Bedrohungen wachsen, denn Angreifer suchen permanent nach neuen Methoden, Zielen und Wegen. Sie erweitern, modifizieren und passen ihre Angriffsszenarien kontinuierlich an. Technische und nicht-technologische Angriffsmethoden, das sogenannte „Social Engineering“ bzw. „Social Hacking“, gehen hier Hand in Hand. Die Angriffsfläche für Hacker wächst kontinuierlich. Netzbasierte Endgeräte rücken zunehmend in den Fokus von Angreifern. IDC prognostiziert beispielsweise, dass die Zahl der an das Internet angeschlossenen IoT-Geräte im Jahr 2020 bei 30 Milliarden liegen wird. Alle Geräte mit einer IP-Adresse können angegriffen werden, egal ob es sich um Wearables, Thermostate, Kassenterminals, Sensoren, elektronische Waagen oder eben Drucker und Multifunktionsgeräte handelt. Nun kommt es darauf an, die Angriffsfläche so klein wie möglich zu halten, Systeme permanent zu überwachen und Wiederherstellungspläne verfügbar zu haben.

## Die Gefahr, die von Druckern ausgeht, wird unterschätzt

Drucker stellen also zunehmend ein Sicherheitsrisiko dar. Diese Einschätzung hat u. a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) im Februar 2017 veranlasst, Empfehlungen für den Umgang mit Druckern und Multifunktionsgeräten im Netzwerk zu veröffentlichen. Das BSI schätzt darin, dass die Gefahr wächst, Drucker als Angriffswaffe zu benutzen, dass aber im Gegensatz zu anderen Komponenten der Infrastruktur, beispielsweise PCs oder Server, der Sicherheit von Druckern und Multifunktionsgeräten meist nur eine geringe Beachtung geschenkt wird.


50 Prozent der Unternehmen betrachten Drucker nicht als Sicherheitsrisiko

Unsere aktuelle Befragung bestätigt diese Einschätzung. Die Gefahr, die von Druckern als Einfallstor in die Unternehmens-IT ausgeht, wird immer noch deutlich unterschätzt: 50 Prozent der befragten Unternehmen betrachten Drucker nicht als Sicherheitsrisiko. Das ist fahrlässig, denn auch Drucker sind potenzielle Quellen für die Verletzung von Datenschutzbestimmungen, den Verlust von Daten oder für Angriffe auf die IT des Unternehmens.

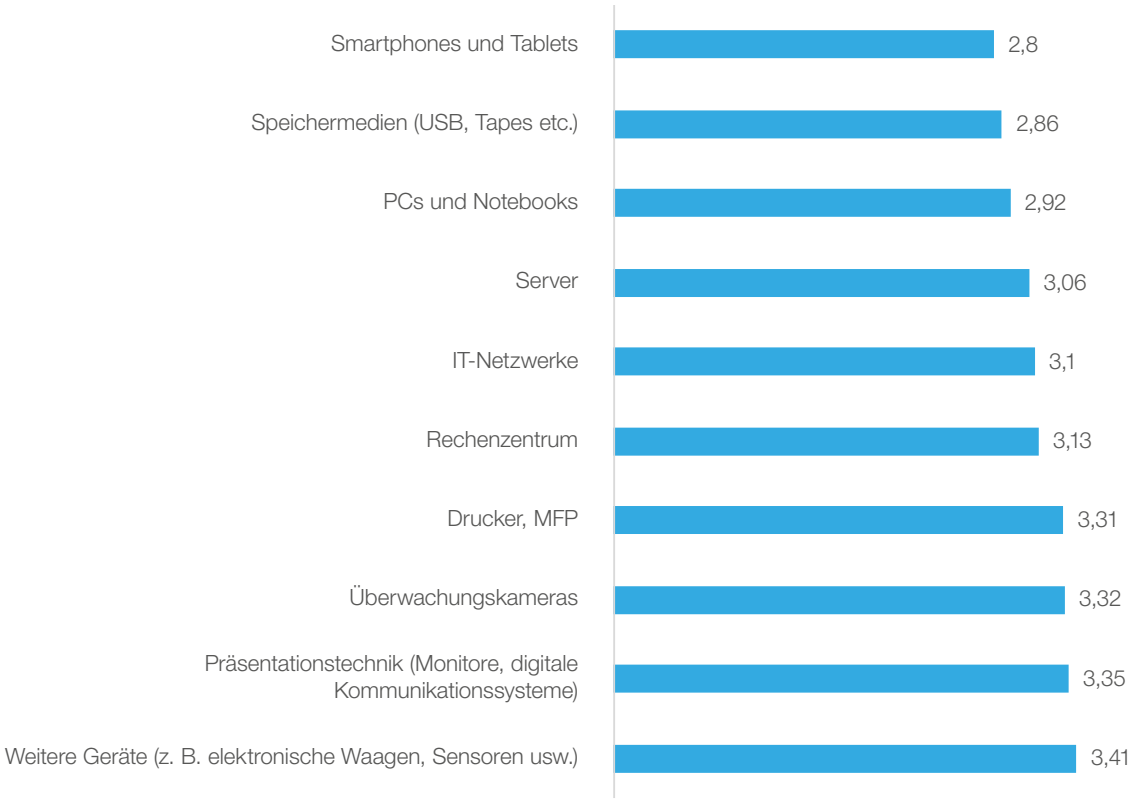
Das größte Risiko für den Verlust von vertraulichen digitalen Daten sehen die Unternehmen bei Smartphones und Tablets, Speichermedien sowie PCs und Notebooks. Bei diesen Geräten handelt es sich mit Ausnahme der PCs um mobile Endgeräte, die unterschiedlich stark in Unternehmensnetzwerke eingebunden und darin abgesichert sind.

Den Einschätzungen der Unternehmen zufolge unterliegen Server, IT-Netzwerke und Rechenzentren einem eher mittleren Restrisiko. Diese Komponenten sind das Herzstück der IT. Hier kennen sich die Unternehmen gut aus und für diese Komponenten wenden sie die meiste Zeit zur Absicherung auf.

Das Restrisiko, das von Druckern, Multifunktionsgeräten, Präsentationstechnik sowie weiteren Geräten ausgeht, wird als eher gering eingeschätzt. Ein wesentlicher Grund liegt darin, dass die Unternehmen bei diesen Geräten – im Gegensatz zu Servern, PCs und Notebooks – hier keine oder nur eine geringe Zahl von Angriffen registriert haben. Sie wiegen sich hier in Sicherheit, wo keine ist. Diese Risikobewertung zu Druckern etc. ist fahrlässig und muss schnellstens korrigiert werden.

## Abbildung 1

Restrisiko für den Verlust von vertraulichen digitalen Daten – Drucker und Peripheriegeräte werden unterschätzt




N = 204 Unternehmen, 1 = Risiko sehr hoch, 5 = Risiko sehr gering

Quelle: IDC, 2017

Unternehmen mit einer anteilig höheren Druckerdurchdringung als der Durchschnitt bewerten die Risiken von Druckern etc. höher als die anderen Unternehmen. Sie haben somit erkannt, dass der Absicherung der Drucker ebenso viel Aufmerksamkeit geschenkt werden muss wie den anderen Komponenten der IT.

## Drei Risiken im Lifecycle von Druckern und Peripheriegeräten

Während PCs und Notebooks gut in Wartungs-, Update- und Patchprozesse eingebunden sind, zeigen sich bei Druckern deutliche Lücken im Lifecycle. Dabei handelt es sich häufig um Wissenslücken bzw. fehlende Transparenz. Diese Wissenslücken bergen verschiedene Risiken in sich:

Risiko 1: Zu Beginn des Lifecycles wird eine Risikoklassifizierung vorgenommen. Diese wird über den Lifecycle nicht geändert oder modifiziert. Viele Unternehmen nehmen einmal jährlich eine Risikobewertung und Klassifizierung ihrer IT vor. Die Druckerumgebungen werden hierbei in der Regel nicht berücksichtigt, da sie an den Managed-Print-Services-Dienstleister ausgelagert sind.

Risiko 2: Die Betriebssoftware und die Konfiguration der Drucker werden nach der Erstinstallation häufig nicht mehr „angefasst". Das führt dazu, dass Drucker und Multifunktionsgeräte mit alten oder veralteten Releases arbeiten. Oftmals auch dann, wenn diese kompromittiert worden sind. Zudem haben nur 38 Prozent der Befragten alle Standardpasswörter geändert. Das ist ein höchst fahrlässiges Verhalten, das sich aber mit wenig Aufwand beheben lässt.

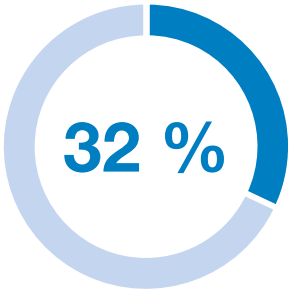
Risiko 3: Eine unzureichende Protokollierung und ein unzureichendes Monitoring der Prozesse und Dienste verringert das Nachvollziehen aller Aktivitäten. Das ist umso schwieriger, wenn nicht alle benötigten Services, Ports und Protokolle der Druckeranwendungen geschlossen werden. Das ist lediglich bei 40 Prozent der befragten Unternehmen der Fall.

Viele Unternehmen nutzen Managed Print Services für ihre Druckerumgebungen. Die Verträge haben häufig eine Laufzeit von fünf Jahren. Die Vertragsdetails „ruhen" in den Unternehmen und sind den IT-Verantwortlichen verständlicherweise dann nicht mehr im Detail bekannt. Die typische Reaktion von IT-Leitern auf die Frage nach Details ist in vielen Fällen folgende: „Da muss ich mal nachfragen, was die machen und was vertraglich abgedeckt ist." Die geschilderten Risiken sind im Wesentlichen das Resultat unzureichender Prozesse. Hier ist eine Korrektur des eingeschlagenen Weges erforderlich.

## Informationssicherheit bei Clients mit Löchern

Für eine umfassende Informationssicherheit sind mehrere Faktoren ausschlaggebend. Ein wichtiger Baustein für eine hohe Informationssicherheit ist ein zentrales Konzept, das alle Bereiche der Unternehmens-IT umfasst, also vom Rechenzentrum über die Server bis hin zu den Clients, Druckern, Mobile Devices und Peripheriegeräten.

Lediglich 63 Prozent der Unternehmen verfügen über ein zentrales Konzept




Nur 32 Prozent der Unternehmen verfügen über eine klar nachvollziehbare Wartungs- und Update-Historie ihrer Drucker


53 Prozent der Unternehmen vernachlässigen das Thema Datenschutz bei der Planung und Einführung neuer Technologien und Businessprozesse

für Informationssicherheit, das alle Systeme und Geräte umfasst. 31 Prozent hingegen verfügen lediglich über Konzepte für einzelne Anwendungen und Systeme. Dieses Vorgehen ist dann richtig und sinnvoll, wenn zuvor eine Risikoklassifizierung der einzelnen Bestandteile der IT vorgenommen worden ist. Wenn die Unternehmen die unterschiedlichen Konzepte aber nicht an einer zentralen Stelle zusammenführen und abstimmen, bleibt die Gefahr groß, Lücken und somit potenzielle Angriffspunkte nicht ausreichend abzusichern.

Ein zweiter wichtiger Baustein ist die frühzeitige Einbindung der Themen Datenschutz, Informationssicherheit und IT-Security bei der Planung und Einführung neuer Technologien und Businessprozesse, am besten gleich von Anfang an. Allerdings findet sich dieser Aspekt derzeit nur bei 47 Prozent der Unternehmen im Pflichtenheft. Für neue Projekte im Rahmen der digitalen Transformation, beispielsweise für Lieferketten, Businessnetzwerke, bei IoT-Plattformen oder im E-Commerce, ist es unerlässlich, Security-Aspekte gleich vom ersten Tag an zu berücksichtigen und einzubinden. Denn in vielen dieser Geschäftsmodelle sind die Teilnehmer unbekannt und somit zunächst nicht vertrauenswürdig. Alle Aktivitäten, die diese Teilnehmer durchführen, müssen auf diese Prämisse hin abgestimmt sein.

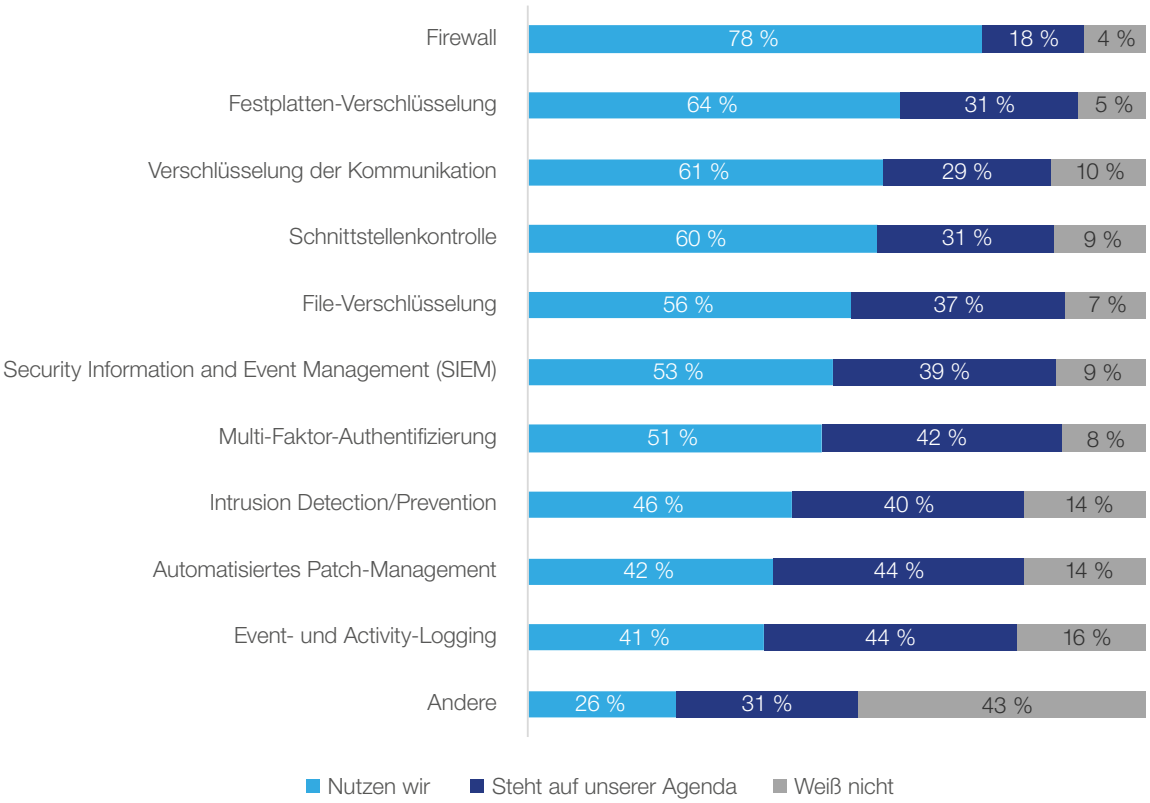
## Security-Basis-Schutz ist flächendeckend vorhanden, aber das reicht nicht aus für den Schutz vor aktuellen Bedrohungsszenarien

Aus einer Technologieperspektive betrachtet haben die meisten Unternehmen zahlreiche Lösungen zum Schutz ihrer Clients und Drucker eingeführt.

## Abbildung 2

Security-Maßnahmen

*Welche Security-Maßnahmen hat Ihr Haus für Clients umgesetzt und welche planen Sie?*




N = 204 Unternehmen

Quelle: IDC, 2017

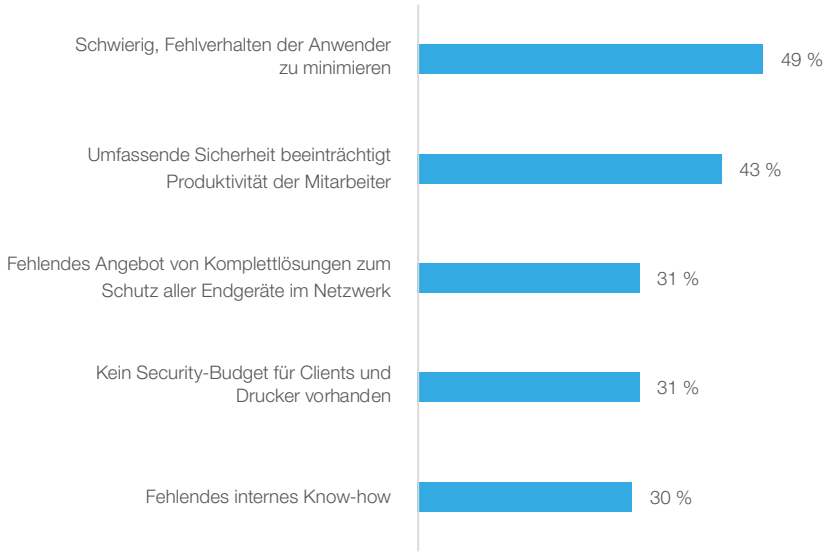
Firewalls, Verschlüsselung und Schnittstellenkontrolle sind wichtige Maßnahmen und dementsprechend häufig anzutreffen. Allerdings setzen viele Unternehmen Security-Lösungen in unterschiedlichen Bereichen ein. Dort, wo es Lücken gibt, ist geplant, diese zu schließen. Next-Gen-IT-Security-Ansätze wie Intrusion Detection/Prevention werden immer häufiger genutzt, sind allerdings bei vielen Unternehmen noch in der Planung. Hier gilt es, zügig zu handeln, denn nur mit einem Mix aus klassischen Schutzmethoden und proaktiven Security-Ansätzen lässt sich ein maximaler Schutz erzielen.

## Fachanwender sind häufig unzureichend sensibilisiert

Es liegt in der Natur der Dinge, dass ein enger Zusammenhang zwischen der Client-Security und dem Verhalten der Endanwender bzw. Fachanwender besteht. Die Aussage, dass die Mitarbeiter ein sehr schwaches Glied in der Security-Kette sind, ist nicht neu und bestätigt sich immer wieder. Viele Schadens-Vorfälle entstanden und entstehen durch den häufig unüberlegten Klick auf einen Link in einer E-Mail. Analysen und Studien haben mehrfach gezeigt, dass ein Fünftel bis ein Viertel der Empfänger von Phishing-Mails diese Mails öffnen und durchschnittlich 10 bis 12 Prozent auf Links und Attachments klicken. Es wird auch mittelfristig zu den wichtigen Aufgaben von IT-Abteilungen gehören, das Fehlverhalten von Anwendern zu minimieren. Knapp 50 Prozent der Befragten sehen darin eine der größten Herausforderungen.

## Abbildung 3

Minimierung des Anwenderfehlverhaltens bleibt größte Herausforderung bei Endgeräten




N = 204 Unternehmen, Top-5-Nennungen

Quelle: IDC, 2017

In den Zeiten von Home-Office, Bring-Your-Own-Device und Co. gewinnt die Fragestellung von starken Security-Maßnahmen vs. geringere Produktivität zusätzlich an Bedeutung. Für die IT-Abteilungen gilt es hier, das richtige Maß zu finden, um die Mitarbeiter nicht zu stark einzuschränken – bei gleichzeitig hoher Security. Das ist eine komplexe Aufgabe. 43 Prozent der Befragten sehen darin eine große Herausforderung. Die Spannbreite starker Security-Maßnahmen ist weit und reicht von der Standardisierung von Hardware über eng gefasste Richtlinien für die Nutzung von IT, Zutrittsbeschränkungen, den physischen Schutz der Geräte etc. bis hin zu Realtime-Sandboxing bei der Nutzung von Cloud-Ressourcen. Somit ist das in der Tat eine

Herausforderung, die sich nicht nur auf Endgeräte beschränkt. Knapp ein Drittel der Unternehmen verfügt nicht über ein eigenes Security-Budget für Clients und Drucker. Hier sollte die Budgetplanung auf jeden Fall verbessert werden und auch Clients und Drucker einschließen.

Grundsätzlich minimieren eine durchgängige Security-Kette und eine hohe Standardisierung das Risiko von Fehlverhalten. Die Maßnahmen sollten von Aktivitäten zur Awareness-Steigerung flankiert werden, um einzudämmen, dass Mitarbeiter aller Hierarchiestufen auf Links in Dokumenten und E-Mails klicken.

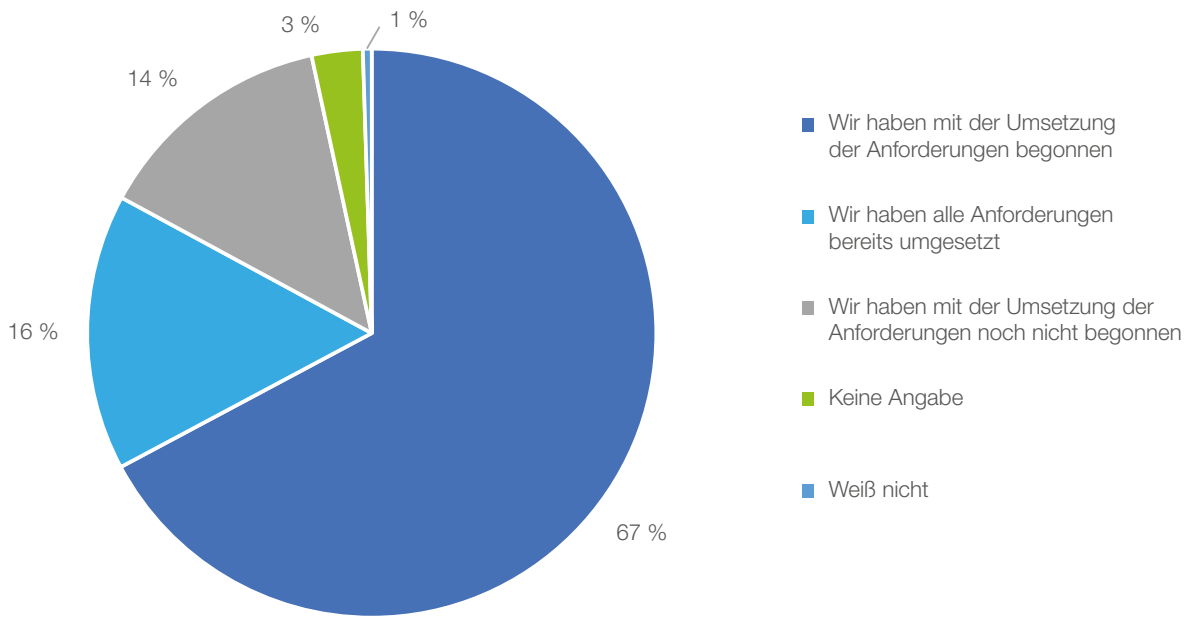
## Compliance stellt höhere Security-Anforderungen

### Unternehmen beim Bundesdatenschutzgesetz (neu) in Verzug

Informationssicherheit beschränkt sich nicht nur auf Maßnahmen zur Sicherstellung eines unterbrechungsfreien Geschäftsbetriebs. Ebenso wichtig ist das Umsetzen staatlicher und regulatorischer Anforderungen. In den Jahren 2017 und 2018 zwingen die EU-Datenschutzrichtlinie und das Bundesdatenschutzgesetz (neu) zu umfassenden Analysen und in vielen Fällen zur vollständigen Überarbeitung ihrer Datenschutzmaßnahmen. Das Bundesdatenschutzgesetz (neu) betrifft alle Unternehmen mit Sitz in Deutschland, die personenbezogene Daten von EU-Bürgern verarbeiten. Alle Unternehmen unterliegen künftig einer Meldepflicht innerhalb von 72 Stunden für Verstöße.

## Abbildung 4

Erst ein Sechstel erfüllt die Anforderungen aus dem Bundesdatenschutzgesetz (neu)




N = 204 Unternehmen

Quelle: IDC, 2017

Die befragten Unternehmen tun sich schwer mit der Erfüllung der Anforderungen. Zwar erfüllen 16 Prozent der Organisationen bereits alle Anforderungen, aber zwei Drittel haben mit der Umsetzung der Anforderungen erst begonnen und weitere 14 Prozent haben noch keine Aktivitäten gestartet. Unsere Gespräche mit IT-Leitern und Security-Verantwortlichen lassen den Schluss zu, dass viele Unternehmen bis Ende Mai 2018 nicht vollständig compliant sein werden.


48 Prozent haben eine Risikobewertung der Drucker durchgeführt

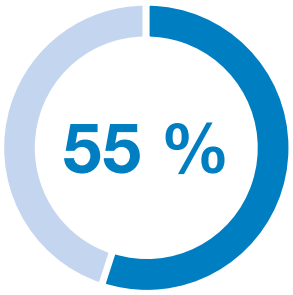
Zwei Herausforderungen treten in diesen Gesprächen immer wieder zu Tage: Das Thema hat die Aufmerksamkeit des Managements mit Blick auf Ende Mai 2018 erst sehr spät erreicht. Nun allerdings erleichtert die Unterstützung durch das Management die Aktivitäten. Mit der Umsetzung der Aktivitäten wird sehr häufig der IT-Leiter beauftragt, obwohl es sich hier um kein IT-Projekt im eigentlichen Sinne handelt.

Bei Verstößen gegen die Bestimmungen drohen hohe Bußgelder, wobei bis zu 20 Mio. Euro oder 4 Prozent des Umsatzes angesetzt werden können. Die Bußgelder werden erhoben, wenn Unternehmen die Richtlinien nicht einhalten – selbst wenn kein konkreter Sicherheitsvorfall vorliegt. Hinzu kommt der Reputationsverlust, Ausgleichszahlungen für Kunden und entgangener Umsatz bei Verlust von Kunden. In Extremfällen kann ein endgültiges Verbot der Datenverarbeitung ausgesprochen werden.

Beispiele aus anderen europäischen Ländern zeigen, dass Verstöße ernst genommen und geahndet werden. So wurde beispielsweise kürzlich in Frankreich ein Bußgeld von 40.000 Euro verhängt. Auch in Deutschland werden nach und nach die Ressourcen für Überprüfungen und Auditierungen aufgebaut. Ein Grund mehr, in den Bemühungen bei der Umsetzung der Anforderungen nicht nachzulassen.

## KRITIS rückt zunehmend in den Fokus

Eine weitere gesetzliche Anforderung findet in der Öffentlichkeit deutlich weniger Aufmerksamkeit. Sie betrifft die Betreiber kritischer Infrastrukturen (KRITIS). Verbindlich ist hier das IT-Sicherheitsgesetz vom Juli 2015. Kritische Infrastrukturen sind in acht Sektoren gegliedert und in fast allen Branchen vorhanden. Mehr als die Hälfte der Unternehmen sind Betreiber kritischer Infrastrukturen. Daraus ergeben sich organisatorische und technische Anforderungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse.




55 Prozent der Befragten zählen sich zu Betreibern kritischer Infrastrukturen

Die Anforderungen beschränken sich nicht nur auf die IT, sondern umfassen weitere technologisch-operative Systeme wie vernetzte Steuer- und Leitsysteme im Energie- und Transportwesen (Umspannwerke, Sortieranlagen etc.) oder die vernetzte Medizintechnik in Krankenhäusern. Die Vorgaben des IT-Sicherheitsgesetzes sind für alle Sektoren bindend. Für einige der Sektoren gelten darüber hinausgehende Vorgaben. Für alle Sektoren gilt bei der Umsetzung von IT-Sicherheitsmaßnahmen den „Stand der Technik" zu berücksichtigen, branchenspezifische Sicherheitsstandards umzusetzen und der Meldepflicht nachzukommen. 72 Prozent der Unternehmen sind die Übergangsfristen, die für ihren Sektor relevant sind, bekannt. Sie sind nun herausgefordert, zügig mit der Erfüllung der allgemeinen und sektorenspezifischen Anforderungen zu beginnen. Damit vermeiden sie es, in eine ähnlich zeitkritische Situation zu kommen, die sich für viele Unternehmen bei der Umsetzung des Bundesdatenschutzgesetzes (neu) abzeichnet.

## Lösungsansätze für eine höhere Informationssicherheit

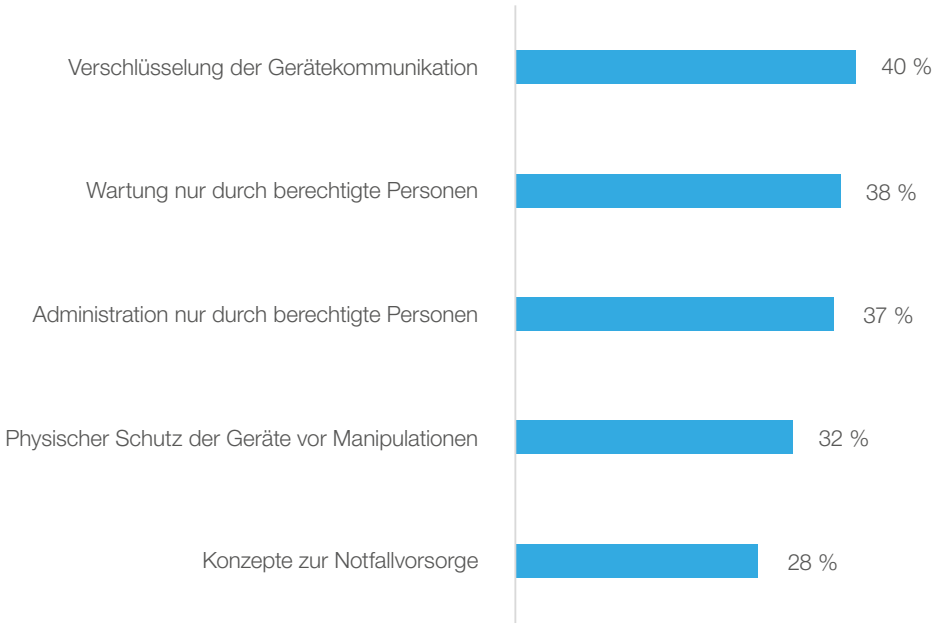
### Verschlüsselung, Notfallvorsorge und Berechtigungsrichtlinien stärken die Sicherheit im Umgang mit Endgeräten

Den Unternehmen stehen viele unterschiedliche konzeptionelle Maßnahmen und Lösungsansätze zur Verfügung, die sie bei der Schaffung einer höheren Informationssicherheit unterstützen. Auf konzeptioneller Seite zählen zu solchen Maßnahmen die Verschlüsselung von Daten, Geräten und Übertragungswegen bei Clients und Druckern. Daten sind permanent in Bewegung. Aus diesem Grund war zu erwarten, dass Verschlüsselung bereits flächendeckend umgesetzt wurde.

Das ist nicht der Fall: Lediglich 64 Prozent der Befragten verschlüsseln die Festplatten ihrer Clients, und bei Druckern ist das nur in 54 Prozent der Unternehmen der Fall. Sehr positiv ist der Umstand einzuschätzen, dass ca. 30 Prozent sowohl die Verschlüsselung ihrer Clients als auch ihrer Drucker auf der Agenda haben. Werden diese Pläne umgesetzt, wäre eine fast vollständige Verschlüsselung der Festplatten im gehobenen Mittelstand und bei Großunternehmen erreicht.

## Abbildung 5
Richtlinien

*Welche organisatorischen Richtlinien sind aus Ihrer Sicht am besten geeignet, um die Sicherheit im Umgang mit allen Endgeräten zu verbessern?*




N = 204 Unternehmen, Top-5-Nennungen

Quelle: IDC, 2017

Bedenklich ist allerdings die Tatsache, dass knapp 10 Prozent der Befragten keine verbindliche Aussage zum Stand der Verschlüsselung treffen können. Einen hohen Schutz erzielen Unternehmen am besten mit konzeptionellen und technischen Maßnahmen, die aufeinander abgestimmt sind.
Bei vielen Unternehmen hat es sich in der Praxis zudem bewährt, die Maßnahmen mindestens einmal pro Jahr einem Review zu unterziehen. Damit stellen sie sicher, dass sie ihre Informationssicherheit mit der allgemeinen Sicherheitslage in Einklang bringen.

## Druckersicherheit gehört auf den Prüfstand

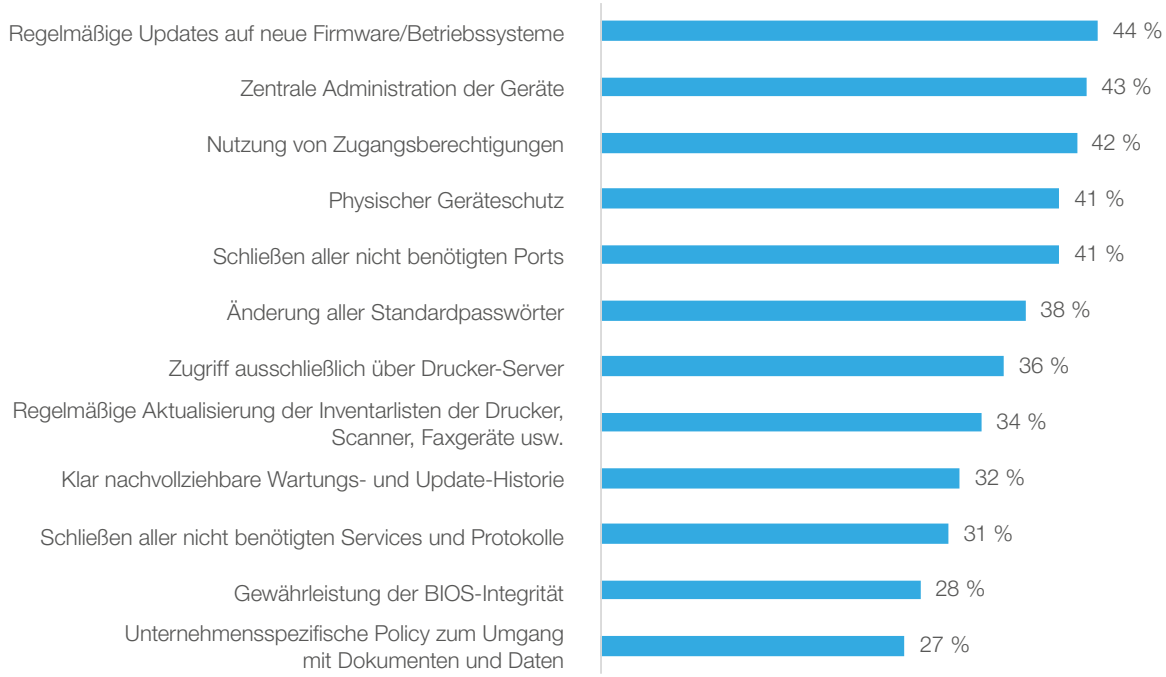
Im Zuge der Umsetzung des Bundesdatenschutzgesetzes (neu) und der zu beobachtenden wachsenden Zahl von Angriffen auf Drucker ist es empfehlenswert, über die bereits genannte Risikobewertung der Drucker hinaus konkrete Schritte in Betracht zu ziehen.

Die Befragung zeigt deutlich, dass wichtige Aktivitäten lediglich bei einer Minderheit der Unternehmen umgesetzt worden sind. So fahren beispielsweise nur 44 Prozent der Unternehmen regelmäßige Updates ihrer Drucker-Firmware/Betriebssysteme und lediglich 43 Prozent verfügen über eine zentrale Administration der Geräte. In vielen Firmen gibt es noch nicht konsolidierte Druckerparks, die eine zentrale Administration erschweren. Somit verwundert es nicht, dass lediglich 34 Prozent eine regelmäßige Aktualisierung der Inventarlisten der Drucker, Scanner, Faxgeräte usw. durchführen. Abbildung 6 zeigt weitere Maßnahmen zur Erhöhung der Druckersicherheit auf.

## Abbildung 6

Security-Maßnahmen für Drucker

*Welche Maßnahmen zum Schutz der Drucker haben Sie umgesetzt?*




N = 204 Unternehmen

Quelle: IDC, 2017

Neben diesen druckernahen Aktivitäten gehören unternehmensspezifische Policies zum Umgang mit Dokumenten und Daten ebenfalls auf den Prüfstand. Das haben bisher 27 Prozent der Unternehmen umgesetzt.

## FAZIT

Die digitale Transformation, Cyberrisiken und Compliance-Anforderungen haben die Aufmerksamkeit vieler Unternehmen mit Blick auf eine hohe Informationssicherheit geschärft. Allerdings ist eine umfassend geschlossene Security-Kette nur in wenigen Fällen vorhanden.

Während das Rechenzentrum und die Server in fast allen Unternehmen gut abgesichert sind, zeigen sich bei Clients, Druckern und weiteren Geräten bei einer Betrachtung über den gesamten Security-Lifecycle deutliche Lücken.

Basisschutz und Standard-Security-Lösungen sind in vielen Organisationen vorhanden. Das allein reicht aber allenfalls aus, um großflächig angelegte „Wald- und Wiesenangriffe“ abzuwehren. Viele Unternehmen drehen an einzelnen Stell-schrauben und vernachlässigen dabei den Gesamtblick in Bezug auf neuere und komplexe Angriffsszenarien.

Clients, Drucker usw. werden immer häufiger zum Angriffsziel. Das hat viele Gründe: Diese Geräte sind in jedem Unternehmen in großer Zahl vorhanden, heterogene Geräteparks erschweren die Absicherung und besonders Drucker und Peripherie-geräte werden vielfach nicht über den gesamten Lebenszyklus gepatcht.

Hier sind mehr Pragmatismus und vorausschauende Aktivitäten erforderlich. Umfassender Schutz der Clients gehört in jedes Pflichtenheft. Aktuelle Firmware, Patches, klare Zugriffsrechte und physischer Schutz zählen zum Einmaleins der Security. Mit diesen Richtlinien und Maßnahmen stärken die Unternehmen ihre Informationssicherheit auch in Richtung Compliance. Das ist ein Aspekt, der immer wichtiger wird und eine enge Abstimmung zwischen dem Risk Management und der IT verlangt.

Grundsätzlich gilt auch in den nächsten Jahren: Ein Gesamtlösungsansatz zur Informationssicherheit ist Voraussetzung, um alle Komponenten, Lösungen und Prozesse zu erfassen und davon die erforderlichen Richtlinien abzuleiten.

# EMPFEHLUNGEN

## 1. Führen Sie regelmäßig Risikoklassifizierungen Ihrer IT durch

Die Sicherheitslage und die Bedrohungsszenarien wandeln sich kontinuierlich. Halten Sie Schritt und passen Sie Ihre Aktivitäten an die Erfordernisse an. Ein Mix aus regelmäßigen Bewertungen und Klassifizierungen und aus Ad-hoc-Aktivitäten nach sich rasch verbreitenden Vorfällen ist eine bewährte Vorgehensweise.

## 2. Überprüfen Sie, wie umfassend Clients, Drucker und weitere IT-basierte Geräte in das Security-Konzept eingebunden sind

Clients, Drucker und weitere Geräte sind in unterschiedlichem Maße eng in die Security-Konzepte integriert. Es ist durchaus sinnvoll, verschiedene Geräteklassen mit unterschiedlichen Sicherheitsklassen zu versehen. Ziel der Konzepte muss aber immer eine einheitliche Sicht auf die Informationssicherheit sein, über alle Geräteklassen und deren vollständigen Security-Information-Lifecycle hinweg.

## 3. Verbinden Sie Basismaßnahmen und fortgeschrittene Maßnahmen für einen erhöhten Schutzbedarf Ihrer PCs, Laptops, Smartphones, Drucker und Peripheriegräte

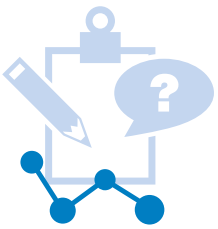
Unternehmen erweitern derzeit etablierte Security-Maßnahmen wie Antimalware und Firewall um neue sogenannte Next-Gen-Lösungen wie Intrusion und Breach Detection. Ein mehrgleisiger Ansatz bietet einen wirksamen Schutz.

## 4. Integrieren Sie Risikomanagement und Compliance in die Informationssicherheit

Das Einhalten regulatorischer und gesetzlicher Anforderungen darf als wichtiger Treiber der Informationssicherheit nicht unterschätzt werden. Starten Sie frühzeitig bei der Umsetzung der Anforderungen, um zum Stichtag compliant zu sein. Sichern Sie sich frühzeitig die Unterstützung des Managements, um zusätzliches Budget zu erhalten.

## 5. Patchen Sie regelmäßig

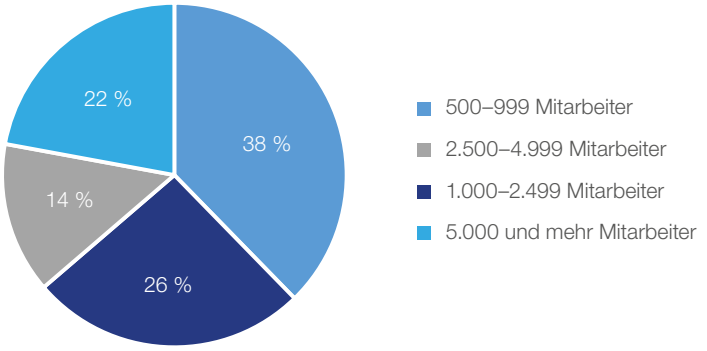
Unternehmen tun sich oft schwer, vom Hersteller empfohlene Maßnahmen umzusetzen. Hier besteht aber viel Potenzial für höheren Schutz. Sie sind kostengünstig umzusetzen. Bringen Sie einfach Routine in diese Aufgaben.



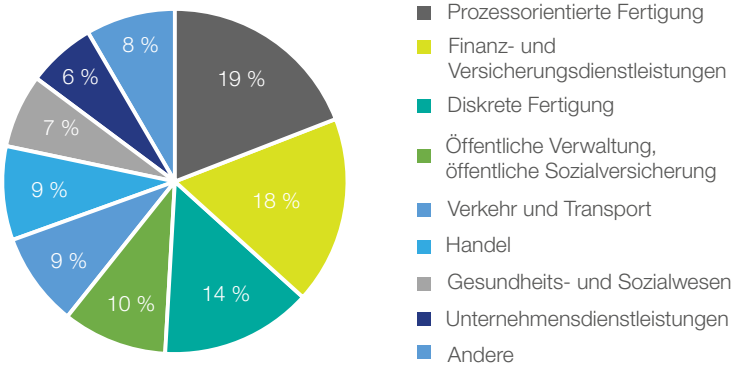
# METHODIK

Die Ergebnisse dieses Papers basieren auf einer Befragung von 204 IT- und Security-Entscheidern aus Unternehmen aller Branchen mit mehr als 500 Mitarbeitern in Deutschland im Juli 2017.

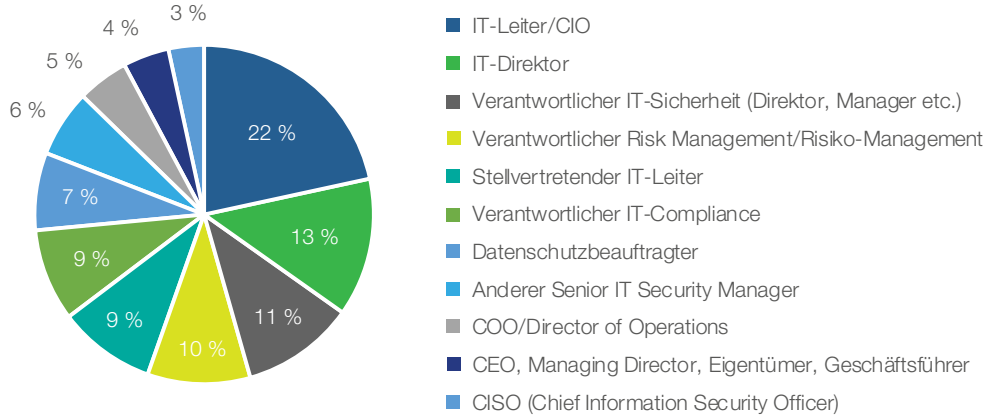
Mitarbeitergrößenklassen




Branchen




Funktion



## ÜBER IDC

IDC ist der weltweit führende Anbieter von Marktinformationen, Beratungsdienstleistungen und Veranstaltungen auf dem Gebiet der Informationstechnologie und der Telekommunikation. IDC analysiert und prognostiziert technologische und branchenbezogene Trends und Potenziale und ermöglicht ihren Kunden so eine fundierte Planung ihrer Geschäftsstrategien sowie ihres IT-Einkaufs. Durch das Netzwerk der mehr als 1100 Analysten in über 110 Ländern mit globaler, regionaler und lokaler Expertise kann IDC ihren Kunden umfassenden Research zu den verschiedensten Segmenten des IT-, TK- und Consumer-Marktes zur Verfügung stellen. Seit mehr als 50 Jahren vertrauen Business-Verantwortliche und IT-Führungskräfte bei der Entscheidungsfindung auf IDC.

Weitere Informationen sind auf unseren Webseiten unter www.idc.com oder www.idc.de zu finden.

## COPYRIGHT-HINWEIS



Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte:
Katja Schmalen, Marketing Director, +49 69 90502-115 oder kschmalen@idc.com.



IDC Central Europe GmbH
Hanauer Landstr. 182 D
60314 Frankfurt am Main

T: +49 69 90 50 2-0
F: +49 69 90 50 2-100
E: info_ce@idc.com

IDC
ANALYZE THE FUTURE