KONICA MINOLTA

# WARUM IT-SYSTEME AUSFALLEN UND WAS DAS FÜR IHR UNTERNEHMEN BEDEUTET

## Ein Überlebensleitfaden für KMUs

DIE 5 WICHTIGSTEN URSACHEN FÜR IT-AUSFÄLLE

**KONICA MINOLTA**

Giving Shape to Ideas

# INHALT

# VERLORENE PRODUKTIVITÄT IST DAS GRÖSSTE RISIKO BEI SYSTEMAUSFÄLLEN – ODER NICHT?

In Zeiten hoch dynamischer Märkte und starker Nachfrageschwankungen müssen kleine und mittlere Unternehmen eine starke Wettbewerbsposition erobern und verteidigen. Business Continuity ist der Schlüssel dazu. Es ist nicht auszudenken, was geschieht, wenn Ihre IT-Umgebung nicht ordnungsgemäß funktioniert oder ständig ausfällt!

Ausfallzeit ist das größte Problem, dem Unternehmen im Alltag gegenüberstehen. Je nach der Dauer des Ausfalls können die Folgen für kleine und mittlere Unternehmen (KMUs) katastrophal sein. Systemausfallzeit bedeutet Produktivitätseinbußen und Ineffizienz – unabhängig davon, ob die Ursache ein Hardwareausfall, ein Systemabsturz oder einfach ein menschlicher Fehler ist. Die Aufrechterhaltung einer funktionsfähigen IT-Infrastruktur ist eine erhebliche Herausforderung für ein Unternehmen. Häufig wird eine Abwägung zwischen dieser Herausforderung und dem Risiko von Systemausfällen und den potenziellen finanziellen Folgen durch Reparaturen, Serviceunterbrechungen und verlorene Produktivität vorgenommen.

Ihre Kunden verlassen sich auf Sie und Sie verlassen sich auf Ihre Kunden. Stellen Sie sich vor, welche verheerenden Auswirkungen ein Vorfall mit Datenverlust auf Ihre Geschäftsbeziehungen hätte! Vergessen Sie auch nicht die Geschäftschancen, die Sie aufgrund von Systemausfallzeiten nicht nutzen können. Die Rufschädigung, die Ihr Unternehmen erleidet, und die Kosten, die entstehen, können langfristig vernichtend sein. Laut Aberdeen Group[1] betragen die Kosten für Ausfallzeiten für ein KMU, dessen Jahresumsatz unterhalb von € 45 Millionen liegt, im Schnitt etwa € 7.700 pro Stunde. Bei einer Betriebszeit von 99,9 % sind das mehr als € 68.000 pro Jahr – ein Betrag, der bei KMUs für das Überleben des Unternehmens entscheidend sein kann.

Es versteht sich daher von selbst, dass Sie Ihr Unternehmen vor Ausfallzeiten schützen müssen, um für die Zukunft vorzusorgen. Schutz vor Datenverlust ist der Schlüssel dazu, dass ein KMU in einem stark wettbewerbsorientierten Markt überleben kann, und ein unverzichtbarer erster Schritt hin zu hoher Sicherheit der gesamten IT. Verwaltete Services vereinen ausgezeichnete Hardware- und Softwarekomponenten in einem integrierten Angebot, das das IT-Management vereinfacht und die übergreifende Sicherheit und Transparenz verbessert.

Im Folgenden sind einige häufige Ursachen für IT-Ausfälle und geeignete Gegenmaßnahmen beschrieben.

## MIT IT-AUSFÄLLEN VERBUNDENE RISIKEN

- **Einnahmeeinbußen**
- **Reparaturkosten**
- **Verlust von Mitarbeitern und/oder sinkende Arbeitsmoral der Mitarbeiter**

- **Verlorene Geschäftschancen**
- **Vertrauensverlust bei Kunden und/oder Lieferanten**
- **Schädigung des Marken- und Firmenimages**
- **Schlechte Publicity**

BIS, Calculating the Cost of Downtime in Your Business, April 2016

1 Aberdeen Group, Building a Fast Lane to Better Data Center Performance, Juni 2016

# FÜNF HÄUFIGE URSACHEN FÜR IT-AUSFÄLLE UND GEEIGNETE GEGENMASSNAHMEN

Der Schutz der IT-Infrastruktur, der Informationsressourcen und einer zunehmend mobilen Belegschaft ist bei vielen Unternehmen das wichtigste strategische IT-Projekt. Das Ausmaß und die Vielfalt von IT-Sicherheitsbedrohungen zeigen, wie schwierig es ist, ein modernes Unternehmen zu schützen. Und die sicherheitsbezogenen Herausforderungen wachsen mit jeder zusätzlichen Anwendung, jedem weiteren mobilen Endgerät und jedem neuen Benutzer.

### 1. Datenverlust durch Fehler beim Backup

Datenverlust kann viele unterschiedliche Ursachen haben: Ein Mitarbeiter löscht versehentlich ein Dokument, ein Server fällt aus oder es treten Fehler bei anderen Technologiekomponenten auf. Die Konsequenzen können sehr weitreichend sein (siehe Abbildung auf Seite 3). Für den Schutz Ihres Unternehmens gegen den Verlust wichtiger Daten, die Sie täglich nutzen, ist ein funktionierendes und zuverlässiges Backup von kritischer Bedeutung.

In erster Linie muss sichergestellt werden, dass Backups regelmäßig ausgeführt werden. Im Idealfall sollten sich Backups in keiner Weise auf Ihre Geschäftsabläufe auswirken. Durch regelmäßige Tests Ihrer Backup-Funktionalität können Probleme festgestellt und behoben werden, bevor sie Ihr Unternehmen beeinträchtigen[2].

### 2. Serverabsturz aufgrund von Viren und Malware

Viren- oder Malware-Angriffe gehören zu den schlimmsten Szenarios, die für Ihr System auftreten können. Sie können dazu führen, dass alle Ihre vertraulichen Firmendaten verloren gehen oder veröffentlicht werden. Die Komplexität erhöht sich noch weiter, da verschiedene Typen von Viren unterschiedliche Schäden verursachen. Das Ergebnis ist jedoch immer das gleiche: Die Wiederherstellung kostet Sie sehr viel Geld. Ganz zu schweigen von dem Aufwand, den Sie betreiben müssen, wenn bei einem Serverabsturz das gesamte System neu aufgesetzt werden muss.

Zum Schutz Ihres Unternehmens vor Viren- und Malware-Angriffen muss Ihre Antivirensoftware immer auf dem aktuellsten Stand gehalten werden, damit sie auch die neuesten Bedrohungen ausfindig machen kann. Darüber hinaus tragen regelmäßige Überprüfungen des gesamten Systems zu einem noch besseren IT-Schutz bei. Unterziehen Sie auch Ihre Software-Firewall einer sorgfältigen Untersuchung. Nicht jede Sicherheitssoftware bietet Schutz gegen unterschiedlichste verdächtige Programme.

### 3. Vernachlässigung des Upgrades der IT-Infrastruktur

Es ist extrem wichtig, die IT-Infrastruktur zeitnah zu aktualisieren: Alte Systeme stürzen häufig ab, Anwendungen laufen langsam, die Anzahl der Sicherheitslücken steigt an, der Speicherplatz wird knapp, die Software ist am Ende ihrer Lebensdauer. Dies sind nur einige Warnhinweise, die Sie nicht ignorieren sollten. Es ist jedoch sehr zeitaufwendig, die Gültigkeit der Lizenzen für schnell veraltende IT-Hardware und Software zu überwachen. Für alle Ihre IT-Lösungen ist eine eigene Lizenz erforderlich. Die Verwaltung aller dieser Lizenzen ist mühsam und kostspielig.

Die Auslagerung der täglichen Wartungsaktivitäten für Ihre IT- und Anwendungsinfrastruktur an über Fernzugriff verwaltete IT-Services ist ein bewährtes Mittel zum Schutz Ihres Unternehmens vor IT-bezogenen Risiken. Durch die Implementierung einer verwalteten IT-Lösung können Sie von der Leistungsstärke des Anbieters der verwalteten Services profitieren.

2 Entech, Lessons to Learn from the Top 3 SMB IT Failures, Juli 2016

### 4. Heterogene IT-Umgebungen

Die Komplexität von IT-Landschaften steigt immer weiter an. Kontinuierlich werden neue Komponenten wie Hardwareplattformen, Betriebssysteme, Datenbanken, SaaS und On-Premises-Anwendungen, IaaS sowie Infrastrukturen im Rechenzentrum hinzugefügt. Das heißt, dass neue Standards für IT-Sicherheit und -Management erforderlich sind. Und was noch wichtiger ist: Viele unterschiedliche Systeme, Anwendungen und Plattformen bedeuten zahlreiche potenzielle Fehlerquellen. Es ist für Ihre IT-Abteilung sehr schwierig, alle Komponenten zu überwachen und zu verwalten.

Durch Konsolidierung und Standardisierung von Teilen Ihrer IT-Infrastruktur können Sie die Komplexität deutlich reduzieren. Eine gemeinsame API-Plattform und ein Cloud-basierter Ansatz verbessern die Situation noch weiter[3].

### 5. Menschliche Fehler

Die meisten IT-Ausfälle lassen sich zumindest teilweise auf menschliche Fehler zurückführen[4]. Ob ein Mitarbeiter bei kritischen IT-Abläufen versehentlich falsche Eingaben macht, Server schlecht konfiguriert sind oder standardisierte Prozeduren bzw. Dokumentation fehlt – all dies kann verheerende Auswirkungen auf das gesamte IT-System haben.

Strenge Richtlinien müssen definiert werden. Alle Mitarbeiter mit der Befugnis zur Konfiguration von Servern und Systemen müssen diese Richtlinien kennen und immer wieder auf verbotene Praktiken und die Folgen bei Zuwiderhandlungen hingewiesen werden. Menschliche Fehler können zwar nicht vollständig vermieden werden; die damit verbundenen Risiken lassen sich jedoch verringern.

3 IDG, How to reduce IT complexity and increase agility, August 2015
4 Harvard Business Review, The Biggest Cybersecurity Threats Are Inside Your Company, September 2016

# DISASTER RECOVERY – JEDE MINUTE ZÄHLT

Bei unternehmenskritischen IT-Ausfällen ist die Wiederherstellbarkeit für kleine und mittlere Unternehmen von höchster Priorität. Eine wichtige Voraussetzung für den Schutz Ihres Unternehmens ist eine gut durchdachte Disaster-Recovery-Strategie. Für KMUs sind Kosten, Wiederherstellungsgeschwindigkeit und Zuverlässigkeit die wichtigsten Faktoren für das Disaster Recovery[5]. Es ist jedoch nicht überraschend, dass Unternehmen häufig verschiedene Lösungen für Disaster Recovery miteinander kombinieren, z. B. On-Premises-Elemente zusammen mit physischen Datenträgern außerhalb des Standorts, nur physische Datenträger außerhalb des Standorts, nur On-Premises-Elemente oder On-Premises- und Cloud-Elemente. Angesichts der ständigen Zunahme mobiler und virtueller Arbeitsabläufe ist ein funktionierendes Disaster Recovery für Ihr Unternehmen von grundlegender Bedeutung. Dabei geht es jedoch nicht nur um Wiederherstellung, sondern auch um Vorsorge.

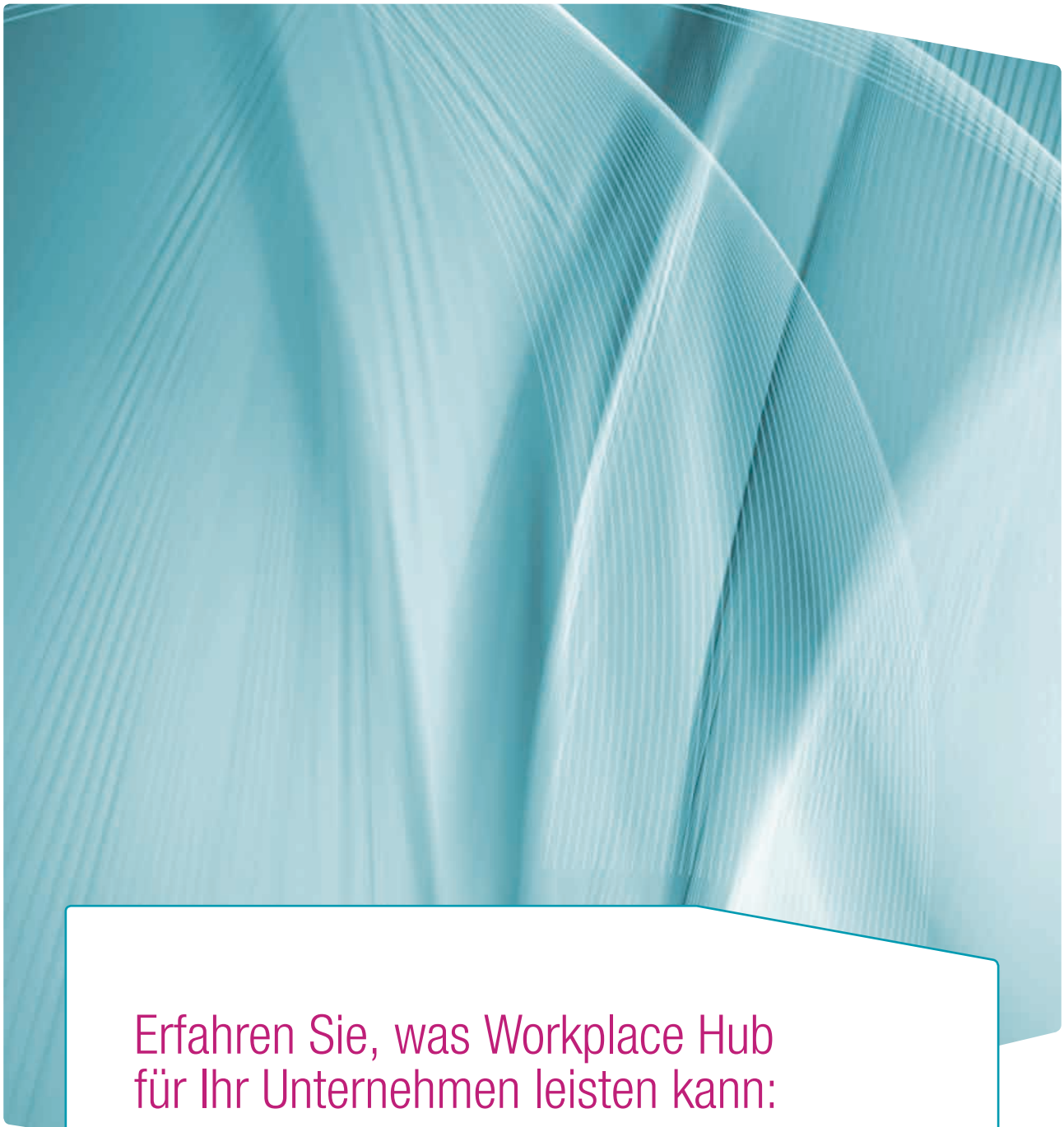
# BRINGEN SIE IHR UNTERNEHMEN MIT DER RICHTIGEN LÖSUNG VORAN

IT-Infrastruktur, Administratorfunktionen und Benutzerumgebungen sind wichtige Elemente einer IT-Lösung, müssen aber durch spezialisierte verwaltete IT-Services und Support unterstützt werden. Kontinuierliches Sicherheitsmanagement, Virtualisierung von Desktop-PCs, regelmäßige Speicherüberwachung und Backups sind Beispiele für Services im Hintergrund, die für den reibungslosen Betrieb eines Unternehmens unerlässlich sind – ggf. mit menschlichen Support-Services in Reserve.

Workplace Hub von Konica Minolta ist eine umfassende Lösung mit Komponenten mehrerer Anbieter, die die verschiedenen Bereiche Ihrer IT-Infrastruktur vereint. Sie vereinfacht die Planung, das Management und die Erweiterung Ihrer IT-Umgebung. Nachdem Workplace Hub installiert wurde, überwacht Konica Minolta das System über Fernzugriff und sorgt für die Identifikation und Behebung von Problemen, bevor diese sich negativ auf Ihr Unternehmen auswirken. Proaktive Verwaltung und Überwachung reduzieren das Risiko, dass in der Zukunft IT-Störungen auftreten.

Sparen Sie Geld für Ihr Unternehmen, befreien Sie sich von lästigen IT-Aufgaben und bleiben Sie der Konkurrenz einen Schritt voraus.

5 Zetta, STUDY: Vast Majority (84%) of SMBs Report that IT Downtime Would Result in Moderate to Catastrophic Loss, März 2016



Erfahren Sie, was Workplace Hub
für Ihr Unternehmen leisten kann:

**workplacehub.konicaminolta.de**

**Konica Minolta**
**Business Solutions Deutschland GmbH**
Europaallee 17
30855 Langenhagen · Deutschland
Tel: +49 (0) 511 74 04-0
Fax: +49 (0) 511 74 10 50
www.konicaminolta.de/business

WEITERE INFORMATIONEN
HTTP://WORKPLACEHUB.KONICAMINOLTA.EU