# Cloud Computing im Mittelstand: Die Sicherheit muss im Mittelpunkt stehen

Ein Strategiepapier erstellt im Auftrag von DTS Systeme GmbH

November 2014

crisp RESEARCH

## Key Takeaways

- Die digitale Transformation sorgt für einen stetig wachsenden Vernetzungsgrad zwischen Unternehmen, ihren Partnern und Kunden. Diese Verbindungen müssen hochgradig abgesichert werden. Cloud-Infrastrukturen bilden die Basis für eine ganzheitliche zentralisierte Sicherheitsstrategie.
- Die maximale Vernetzung bei gleichzeitigem Austausch geschäftskritischer Informationen über öffentliche Datenverbindungen bietet Angreifern mehr Potential und sorgt für neuartige Formen der Bedrohung.
- Zwar haben sich die Sicherheitslösungen zum Schutz der Informationstechnologie in den vergangenen Jahren stetig verbessert. Gleichzeitig ist jedoch auch die Bedrohung durch Cyberkriminelle gewachsen, die versuchen, diese Sicherheitsmaßnahmen zu überwinden.
- Hochstandardisierte Public Cloud Angebote sind nicht in der Lage die Anforderungen von mittelständischen Unternehmen zu erfüllen. Dabei existieren Cloud Computing Deployment-Modelle und Services, welche den spezifischen Anforderungen an den Datenschutz, die Compliance, IT-Governance und IT-Sicherheit entsprechen.
- Mittelständische Unternehmen müssen sich selbstkritisch hinterfragen, ob sie über die notwendigen Kenntnisse und das Personal verfügen, um ihre IT-Infrastrukturen zukünftig gegenüber neuartigen Bedrohungsszenarien schützen zu können.

# Inhaltsverzeichnis

# Sicherheit gewinnt immer mehr an Gewicht

**Durch die zunehmende Vernetzung und Digitalisierung der Geschäftsprozesse verändert sich der Charakter der IT-Landschaften vom geschlossenen System hin zu hybriden IT-Infrastrukturen.** Diese Veränderungen bringen neue Bedrohungsszenarien mit sich, auf die Anwenderunternehmen im Rahmen Ihrer Sicherheitsstrategie reagieren müssen. Nicht nur Großunternehmen, sondern auch der Mittelstand gerät immer stärker ins Visier von Cyberkriminellen. Gleichzeitig werden die Angriffe ausgeklügelter und betreffen immer häufiger auch die Produktionssysteme von Unternehmen.

## IT-Sicherheit als Wettbewerbsfaktor

In Zeiten einer immer engeren Zusammenarbeit zwischen Unternehmen nimmt die Informationssicherheit einen deutlich höheren Stellenwert ein.

Jedoch sollte dabei beachtet werden, dass die Kette immer nur so stark ist wie ihr schwächstes Glied. Unternehmen achten daher mittlerweile verstärkt darauf, wie ihre Geschäftspartner mit den zu schützenden und in der Regel streng vertraulichen Daten umgehen. In diesem Kontext ist eine Tendenz erkennbar, dass bereits bei den ersten Gesprächen zum Aufbau von Geschäftsbeziehungen sehr genau geprüft wird, welche Sicherheitsvorkehrungen getroffen werden. Hierbei empfehlen sich Unternehmen, die klaren Richtlinien und zugehörige technische Lösungen im Einsatz zu haben, als verlässliche Partner und werden vor denen bevorzugt, die auf diese Fragestellungen keine Antworten haben.

## Die Bedrohungsszenarien im Zeitalter der Vernetzung verändern sich

Heutzutage ist der Wert des digitalen Eigentums um ein Vielfaches höher, als noch vor ein paar Jahren, das heißt im Umkehrschluss aber auch, dass im Falle eines Vorfalles der potenzielle Schaden höher ist.

Sicherheitslösungen zum Schutz der Informationstechnologie haben sich in den letzten Jahren stetig verbessert. Gleichzeitig ist jedoch auch die Bedrohung durch Cyberkriminelle gewachsen, die versuchen, diese Sicherheitsmaßnahmen zu überwinden. IT-Abteilungen müssen auf diese neuen Szenarien proaktiv agieren und damit sicherstellen, dass ständig aktuelle Sicherheitsmaßnahmen eingesetzt werden, die sich nicht durch Angreifer aushebeln lassen.

Auf Public Cloud basierende Geschäftsanwendungen bieten an dieser Stelle ein potentielles Angriffsziel und können zum Einfallstor werden. Insbesondere dann, wenn sie nicht die Compliance- und IT-Sicherheitsanforderungen erfüllen und direkt von den Fachabteilungen ohne Kenntnisse der IT-Abteilungen eingekauft wurden.

Gleichzeitig bieten Cloud-Applikationen neue Angriffspotentiale auf:

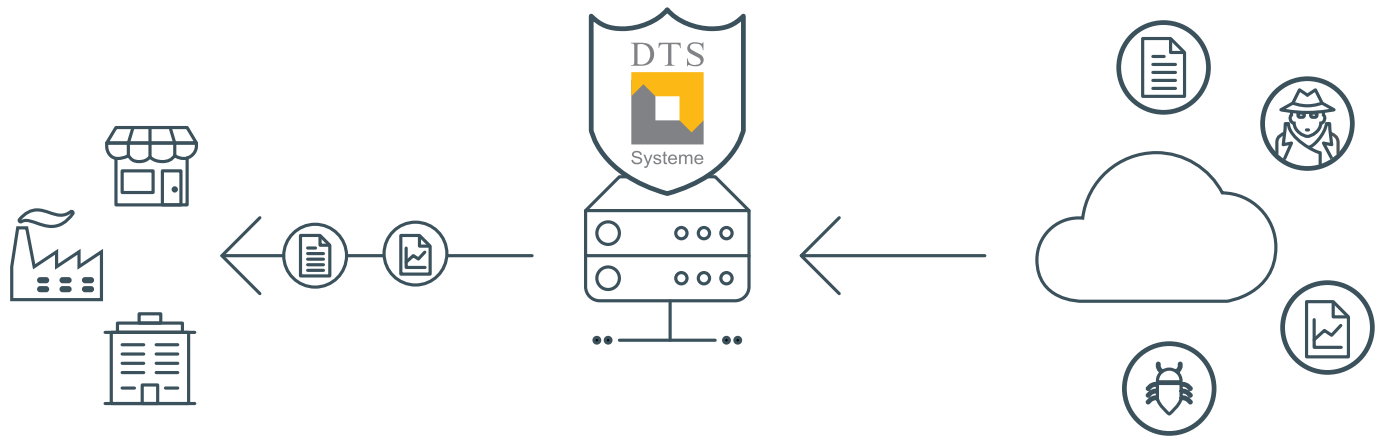
- Die Hypervisor
- Die Netzwerk- und Kommunikationsinfrastruktur
- Die Managementinfrastruktur für das Deployment und die Steuerung der Cloud-Services

Werden Geschäftsapplikationen in der Public Cloud betrieben, haben die für die Sicherheit verantwortlichen Mitarbeiter keine direkte Kontrolle mehr über die oben genannten Bereiche und müssen sich auf den Cloud-Anbieter verlassen. Dieser unmittelbare Kontrollverlust wiegt schwer und ist einer der Hauptgründe, warum sich viele Unternehmen gegen den Einsatz von Public Cloud-Services entscheiden. Wo Großkonzerne deutlich mehr Einfluss auf den Public Cloud-Anbieter nehmen können, haben kleinere und mittelständische Unternehmen keine Möglichkeiten ihre Anforderungen an die individuellen Sicherheitsmaßnahmen durchzusetzen. Eine Zusammenarbeit auf Augenhöhe findet unter diesen Umständen nicht statt.

### Sicherheit in der Cloud

Trotz dieser organisatorischen Umstellung sind Cloud Anbieter in der Lage ihre IT-Infrastrukturen deutlich stärker vor Bedrohungen abzusichern und damit für eine höhere Sicherheit zu sorgen als es bei einem mittelständischen Unternehmen der Fall ist. Das liegt zum einen an den regelmäßigen Investitionen die gezielt in die Sicherheitsinfrastruktur vorgenommen werden. Zum anderen an den Kernkompetenzen der Mitarbeiter, die für den Schutz der Infrastruktur und Services zuständig sind.

## Security-as-a-Service




QUELLE: Crisp Research 2014

In diesem Zusammenhang erhält Security-as-a-Service (SECaaS) eine stetig wachsende Bedeutung. In diesem Modell werden Sicherheitslösungen aus den Rechenzentren eines Service-Anbieters nahtlos in die Kundeninfrastruktur integriert und nach Nutzung abgerechnet. Sicherheit wird demnach als Service aus der Cloud genutzt ohne die ansonsten notwendige Hard- und Software für die eigene lokale Infrastrukturseite einzukaufen.

Unternehmen profitieren von SECaaS u.a. durch:

- Ständig aktuelle Virus Definitionen und Updates
- Schnellere Bereitstellung von Sicherheitslösungen
- Zugriff auf deutlich mehr Sicherheitsexpertise
- Eigene Administration ausgewählter Bereiche. Zum Beispiel die Firewall-Regeln
- Regelmäßige Audits nach Compliance Vorgaben (BSI, Basel, SOX, usw.)

Unternehmen erhalten somit die Möglichkeit hochentwickelte Sicherheitstechnologien einzusetzen, die sonst nur Großkonzernen vorbehalten sind.

Zu SECaaS Lösungen zählen bspw.:

- Authentifizierung
- Antivirus
- Anti-Malware und Spyware
- Intrusion Detection und Prevention
- Next Generation Firewall
- Security Information and Event Management (SIEM)
- Mobile Device Management
- Vulnerability Management
- Web Application Firewall
- DDOS Protection
- Device Control
- Data Loss Prevention (DLP)
- Verschlüsselung
- Anti-Spam
- Webfiltering

SECaaS Lösungen sind also das Mittel der Wahl, um die Sicherheit von IT-Infrastrukturen dem eigenen Bedarf und Möglichkeiten anzupassen, ohne direkt hohe Investitionskosten zu verursachen.

# Managed Cloud-Services erhöhen die Sicherheit

**Cloud-Services haben einen entscheidenden Einfluss auf die digitale Transformation von Unternehmen.** Die Vernetzung mit Partnern und Lieferanten, über nahtlos ineinandergreifende automatisierte Prozesse, sind heutzutage ein Muss, um auf die sich ständig verändernden Marktbedingungen reagieren zu können. Ebenso verhält es sich mit dem Aufbau und der Pflege von Kundenbeziehungen und beim Marketing. Cloud-Infrastrukturen unterstützen hierbei, um kurzfristig Kampagnen umzusetzen und Lastspitzen abzufangen.

## Verbesserung der Datensicherheit

In Zeiten einer immer engeren Zusammenarbeit zwischen Unternehmen nimmt die Informationssicherheit einen deutlich höheren Stellenwert ein. In diesem Zusammenhang spielt die Datensicherheit eine besondere Rolle. Unternehmen müssen hierbei sämtliche technische und organisatorische Maßnahmen ergreifen, um Vertraulichkeit, Verfügbarkeit und Integrität der IT-Systeme sicherzustellen. Managed Cloud-Infrastrukturen leisten einen entscheidenden Beitrag für eine Verbesserung der Sicherheit, indem die untereinander vernetzten Parteien und Systeme auf einer einheitlich zentralisierten Sicherheitsinfrastruktur zusammengeführt werden. Damit profitieren alle von denselben Sicherheitsstandards und das über alle Rechenzentren eines Anbieters hinweg.

Weiterhin muss eines besonders hervorgehoben werden: Cloud Anbieter investieren pro Jahr Millionen in die Absicherung ihrer IT-Infrastrukturen und beschäftigen zahlreiche Sicherheitsexperten, um sich gegen Cyber- und Hackangriffe zu schützen. Ein mittelständisches Unternehmen ist nicht in der Lage, diese Investitionen zu tätigen, um eine gleichwertige Sicherheit zu gewährleisten. Alleine die Daten im eigenen Besitz zu wissen, bedeutet nicht, dass diese auch vor Angriffen und Spionage geschützt sind.

# Ausblick

**Sicherheit ist ein zentraler Aspekt bei der Auslagerung von IT-Infrastrukturen und ein Kernargument, IT-Services weiterhin im eigenen Haus zu betreiben.** Mittelständische Unternehmen gehen mit diesem Thema immer noch sehr fahrlässig um. Das Zeitalter der digitalen Transformation fordert aber weitaus mehr Kenntnisse, als das simple Konfigurieren der Firewall oder des Virenfilters. Die umfangreiche Vernetzung und der Austausch geschäftskritischer Daten über öffentliche Verbindungen sorgen für eine neue Form von Bedrohungen und öffnen den potentiellen Angreifern mehr Türen.

Vor diesem Hintergrund ist zu konstatieren, dass es in Zukunft für die meisten Unternehmen nur unter extrem hohem Ressourcen-Einsatz möglich sein wird sich mit eigenen Bordmitteln gegen diese Bedrohungen zu schützen. Fraglich ist daher, ob Mitteleinsatz und Ergebnis in einem gesunden Verhältnis stehen, da die Sicherheit von Daten und Applikationen in fast keinem Unternehmen zum Kerngeschäft gehört.

IT-Sicherheit gehört in die Hände von Experten, die sich auf dieses Thema fokussieren und über die notwendigen Ressourcen verfügen. Anbieter von Managed Security Services werden so zukünftig zu einer der tragenden Säulen im Kontext von IT-Sicherheit im deutschen Mittelstand werden.

# Über DTS Systeme GmbH

**Als klassischer Systemintegrator unterstützt die DTS Systeme GmbH ihre Kunden seit mehr als 30 Jahren bei der Optimierung von Kernprozessen, der Beratung, Konzeption, Beschaffung, Implementierung und dem Betrieb von IT-Umgebungen.**

Durch das exzellente Zusammenspiel der verschiedenen Abteilungen (Business Units) Systemintegrator, Managed Service Anbieter und einer professionellen Security Abteilung, bietet die DTS Systeme GmbH für ihre Kunden maßgeschneiderte Lösungsszenarien für aktuelle und zukünftige Anforderungen der Enterprise IT aus einer Hand. Mobility, Business Continuity und Disaster Recovery sind u.a. Themen die aufgrund ihrer hohen Komplexität einen Partner benötigen, der in der Lage ist, die gestellten Anforderungen von der Planung bis zur Umsetzung auf höchstem Niveau zu begleiten und zu realisieren. Da DTS zusätzlich noch ISP mit einem eigenen Glasfasernetz ist und ein 24x7 Helpdesk in deutscher Sprache realisiert hat, erhalten Kunden mit hohen Anforderungen eine professionelle Unterstützung.

Eigene Hochleistungs-Rechenzentren in Herford, Hamburg und das leistungsstarke DataCenter des Schwesterunternehmens in Münster sorgen dafür, dass DTS vielseitige Lösungsszenarien anbieten kann. Die ganzheitliche Betrachtung einer IT-Landschaft steht dabei im Vordergrund und ist somit für den Kunden die optimale und effizienteste Lösung.

Eine sehr hohe Security Kompetenz ermöglicht es der DTS Systeme GmbH Lösungen im Bereichen Endpoint Security, Content Security, Network Security und Risk & Compliance anzubieten und betreut in diesem Bereich große internationale Unternehmen.

Mit über 150 Mitarbeitern an 6 Standorten in Herford, Berlin, Bochum, Bremen, Hamburg, Hannover und dem Schwesterunternehmen ICSmedia in Münster bietet die DTS Systeme GmbH Know How in der Beratung, Installation und Betreuung von Informations- und Kommunikationslösungen und organisiert kritische Teilbereiche oder auch die komplette IT-Infrastruktur.

# Autoren

**René Büst**
Senior Analyst & Cloud Practice Lead
rene.buest@crisp-research.com

René Büst ist Senior Analyst und Cloud Practice Lead bei Crisp Research mit dem Fokus auf Cloud Computing und IT-Infrastrukturen. Er ist Mitglied des weltweiten Gigaom Research Analyst Network, Top Cloud Computing Blogger in Deutschland und gehört weltweit zu den Top 50 Bloggern in diesem Bereich. Darüber hinaus zählt er zu den weltweiten Top Cloud Computing Influencers und den Top 100 Cloud Computing Experten auf Twitter. Seit über 16 Jahren konzentriert er sich auf den strategischen Einsatz der Informationstechnologie in Unternehmen und setzt sich zudem mit dem IT-Einfluss auf unsere Gesellschaft sowie disruptiven Technologien auseinander.

René Büst ist Autor zahlreicher Cloud Computing und Technologie Fachartikel, Referent sowie Teilnehmer in Expertenrunden. Auf CloudUser.de schreibt er über die Themen Cloud Computing, IT-Infrastrukturen, Technologien, Management und Strategien. Er hat einen Abschluss als Dipl.-Informatiker (FH) in Technische Informatik von der Hochschule Bremen sowie einen M.Sc. in IT-Management and Information Systems von der FHDW Paderborn.

**Steve Janata**
Vorstand & Senior Analyst
steve.janata@crisp-research.com

Steve Janata ist Vorstand und Senior Analyst bei Crisp Research. Steve leitet die Research-Projekte zu den Themenbereichen Cloud Computing, Digital Customer Experience und Mobility. Er berät und unterstützt IT-Anwender und -Anbieter auf dem Weg in die Digitale Ökonomie.

Vor seiner Tätigkeit bei Crisp Research war Steve als Senior Advisor und Practice Lead „Cloud Computing & Innovation“ bei Experton Group tätig. Er verfügt über 15 Jahre Berufserfahrung als Analyst und Strategieberater in der IT-Branche. Im Rahmen seiner Beratungsmandate war Steve u.a. für Firmen wie IBM, Microsoft, T-Systems und Telefonica tätig. Steve Janata ist Autor zahlreicher Studien und Fachartikel. Als Experte für die Themen Cloud, Channel und Digitale Wirtschaft ist er ein gefragter Sprecher und Moderator auf Konferenzen und Events. Darüber hinaus ist Herr Janata Vorstandsmitglied des Managerkreises Rhein/Main der Friedrich Ebert Stiftung.

# Über die Crisp Research AG

Crisp Research ist ein europäisches IT-Research- und Beratungsunternehmen. Mit einem Team erfahrener Analysten, Berater und Software-Entwickler bewertet Crisp Research aktuelle und kommende Technologie- und Markttrends. Crisp Research unterstützt Unternehmen bei der digitalen Transformation ihrer IT- und Geschäftsprozesse. Cloud Computing und Digital Business Transformation sind dieThemenschwerpunkte von Crisp Research.

Wir verfügen in unseren Crisp Labs über ein innovatives Team an Software-Entwicklern und –Architekten, um neue Cloud-Servicesund Technologien unter Live-Bedingungen zu evaluieren.

Weißenburgstraße 10
D-34117 Kassel

**TEL** +495612207 – 4080
**FAX** +495612207 – 4081

MAIL info@crisp-research.com
WEB crisp-research.com
crisp-analytics.com
TWITTER twitter.com/crisp_research

# Copyright

**Erstellt im Auftrag von:**

DTS Systeme GmbH
Schrewestraße 2
D - 32051 Herford

**Telefon:** +49 (0) 52 21 / 101-3000
**Telefax:** +49 (0) 52 21 / 101-3001
**Email:** info@dts.de



**Gestaltung, Layout & Infografiken:**

Hellwig & Buntenbruch
**MAIL** info@hellundbunt.de
**WEB** hellundbunt.de

Weißenburgstraße 10
D-34117 Kassel
**TEL** +49 561 2207 – 4080
**FAX** +49 561 2207 – 4081

**MAIL** info@crisp-research.com
**WEB** crisp-research.com crisp-analytics.com
**TWITTER** twitter.com/crisp_research

crisp
RESEARCH