



Die sichere Cloud für Verwaltungen

20. Europäischer Verwaltungsreformkongress, Bremen 05. März 2015

Thomas Langkabel, NTO, Microsoft Deutschland GmbH

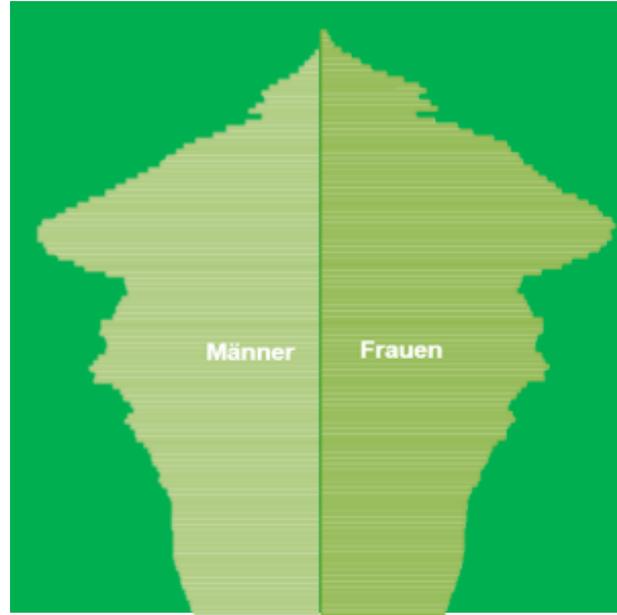
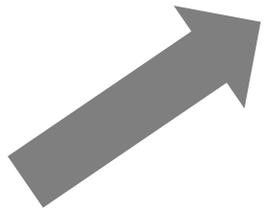
A photograph of three gliders flying in a bright blue sky with scattered white clouds. The gliders are colored red, black, and green. The red glider is at the top, the black one is in the middle, and the green one is on the right. They are all in flight, angled downwards.

Warum überhaupt Cloud für Verwaltungen?

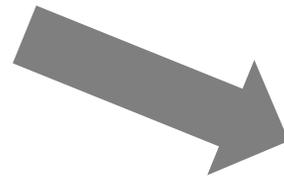
Gesellschaftliche Veränderungen...



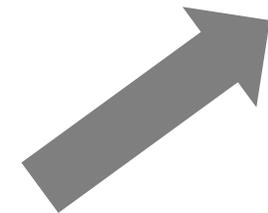
Wachsende Bedeutung
von Zusammenarbeit &
Information



Demografischer Wandel



„Konsumerisierung“
der IT



Rasanter Wandel der Arbeits- und Geschäftswelt



Klassischer Arbeitsstil

65% der Unternehmen bringen mindestens eine Social Plattform zum Einsatz



Durchschnitt der täglich genutzten Privatgeräte
4



84% der Organisationen haben verteilte Arbeitsplätze

Anwender werden "social"

44% der Verbraucher nutzen soziale Medien für Beschwerden



20% erwarten eine Antwort binnen 1h über soziale Medien



Vernetzte
Wissensarbeit
wird immer
wichtiger



Mobile
Endgeräte
&
„BYOD“



Digitale
Generation
ist da



Technologische
Innovationen
kommen in
immer kürzeren
Zyklen

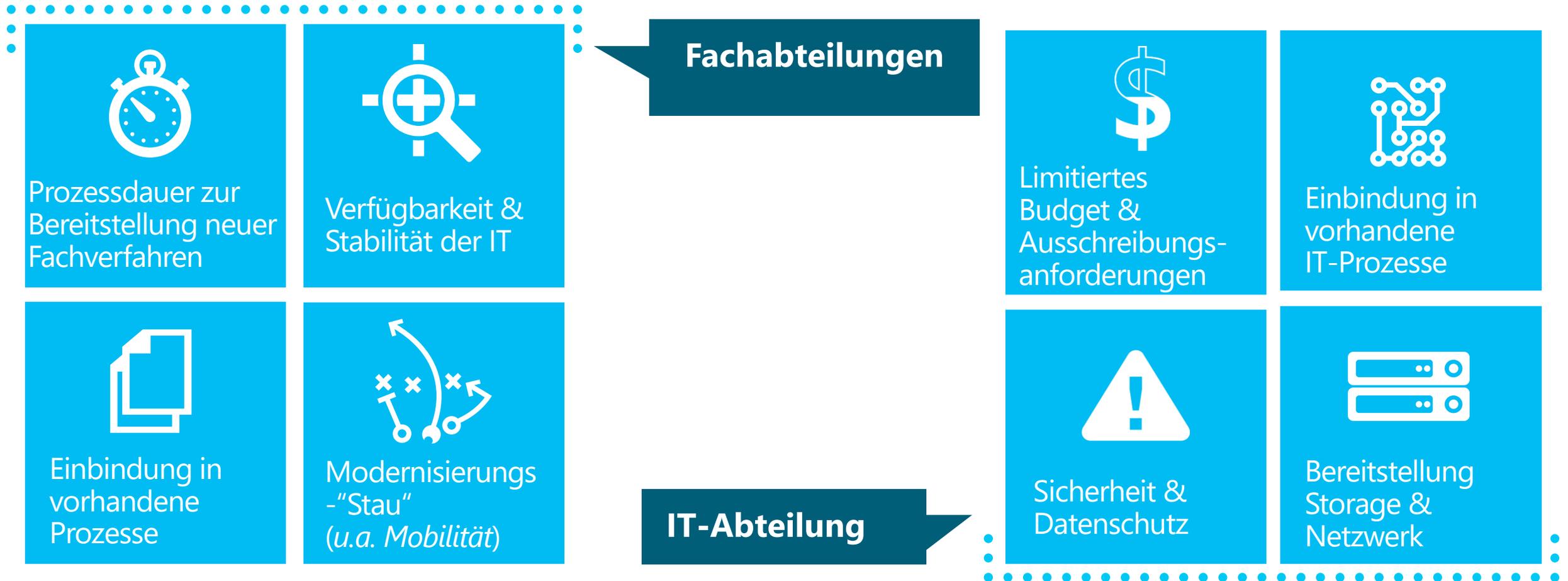


Demografischer
Wandel
&
Hoher
Kostendruck

**Cloud Computing ist
eine Antwort auf
diese Trends**

Grenze
zwischen
Arbeit und
Freizeit
verschwimmt

Die Anforderungen in deutschen Behörden an die IT & Infrastruktur



Modernisierungsblocker Heute

... und wie man trotzdem innovative Projekte beschleunigt



Lösungsentwicklung mit der Cloud

Anwendungs- dienste



Daten- dienste



Infrastruktur- dienste



Apps



Cloud Dienste zur Erweiterung des Rechenzentrums

Anwendungsdienste



cloud services



caching



identity



service bus



media



mobile services



web sites



integration



hpc



analytics

Datendienste



SQL database



HDInsight



table



blob storage

Infrastrukturdienste



virtual machines



virtual network



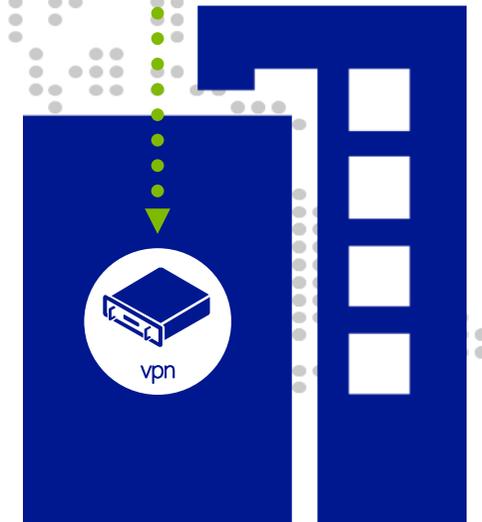
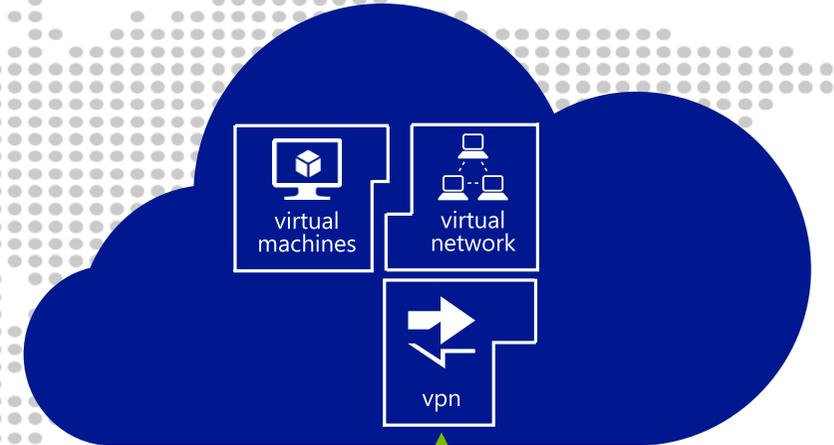
vpn



traffic manager



cdn





„Ich glaube an den
eigenen Server.
Die Cloud ist eine
vorübergehende
Erscheinung.“

(frei nach) Wilhelm II.

*„Ich glaube an das Pferd. Das Automobil ist eine
vorübergehende Erscheinung.“*

... so kann man sich verschätzen

A photograph of three colorful kites (red, black, and green) flying in a bright blue sky with scattered white clouds. The kites are positioned in the upper middle section of the frame. The red kite is at the top, the black kite is in the middle, and the green kite is on the right side.

„Die Cloud“? Was ist das eigentlich?

Hosting- und Betriebsmodelle

Hosting Modell

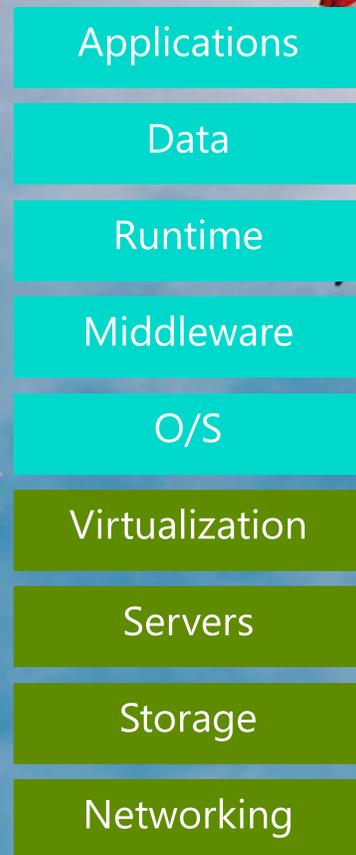
Eigenes RZ

Der Kunde ist verantwortlich für alles



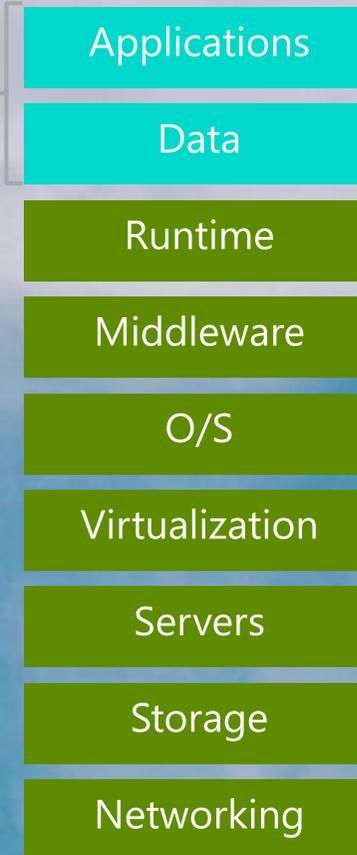
Infrastructure (as a Service)

Kunde ist verantwortlich für Plattform und Anwendungen



Platform (as a Service)

Kunde



Dienst Modell

Software (as a Service)

Cloud Anbieter



Dimensionen

- Generation 3 Container mit bis zu 2.400 Servern; Rüstzeit ~3 Std.; Wartung erst wenn 30-40% der Server im Container defect sind
- In Dublin laufen 400.000 physikalische Server in der Microsoft Cloud
- 30 Personen vor Ort in Dublin; drei weltweit verteilte Network Operations Center für die Administration der Cloud-Services
- Microsoft betreibt über 100 Rechenzentren und das zweitgrößte Dark-Fiber Glasfasernetzwerk auf dem Planeten; 1200 Ausstiegspunkte ins Internet (u.a. Frankfurt; Hamburg; Amsterdam, etc.); Mindestbandbreite 4 TBit/s; innerhalb der Microsoft Rechenzentren 60-80 Tbit/s
- Möglichkeit der Anbindung des Kundenrechenzentrums per dedizierter Leitung mit Dienstgütevereinbarung (Express Route)
- Grüner RZ Betrieb (Wasserkraft; Außenluftkühlung; PUE bis 1,05)
- SLA mindestens 99,9% oder sogar 99,95% (bei ausgewählten Azure Szenarien)

Beispiele

Niedersächsischer Landesbetrieb für Wasserwirtschaft, Küsten- und Naturschutz
NLWKN

Übersicht Karte Messwerte Warnmeldungen Hinweise App NLWKN Links

Meldestufen

- Zurzeit sind für diesen Pegel keine aktuellen Daten verfügbar.
- Dieser Pegel hat derzeit keine Meldestufe überschritten.
- Bordvoller Abfluss und stellenweise Beginn der Ausuferung. Beginn des Hochwassermelddienstes (Vorwarnstufe).
- Ausuferungen hauptsächlich in land- und forstwirtschaftlichen Flächen.
- Überflutung größerer Flächen und Überflutung einzelner Grundstücke, Straßen und Keller möglich.

POLIZEI Nordrhein-Westfalen

Brems Dich – rette Leben!

In dringenden Fällen:
Polizei 110

Zu den Messstellen

Das war ein guter Tag für die Verkehrssicherheit in Deutschland
Innenminister ziehen positive Bilanz des ersten bundesweiten Blitz-Marathons

Positive Zwischenbilanz beim ersten bundesweiten Blitz-Marathon
Innenminister Jäger und ADAC-Präsident Meyer: Wichtige Aktion für mehr Verkehrssicherheit

Erster bundesweiter Blitzmarathon gestartet

A photograph of three gliders flying in a bright blue sky with scattered white clouds. The gliders are positioned in a loose triangle: a red one at the top, a black one at the bottom left, and a green one at the bottom right. The text 'Die sichere Cloud für Verwaltungen' is overlaid in white at the bottom of the image.

Die sichere Cloud für Verwaltungen

Bedenken und Fragen unserer Kunden

Bietet die Microsoft Cloud eine **sichere und wirtschaftliche Plattform** für unser Krankenhaus?
Sind **Sozialdaten** geschützt?

Warum sollte ich **Microsoft** vertrauen?
Bei der ganzen **NSA Debatte** fällt das schwer.

Ist die Microsoft Cloud überhaupt **ausgereift** und gibt es bereits **Referenzkunden**?

Wie kann ich **Planungssicherheit** bei Microsofts "Mobile first – Cloud first" Strategie finden? **Muss** ich etwa in die **Cloud**? Gibt es einen Weg zurück?

Ist Microsoft der **richtige Partner** für **eine Plattform** vom **PC** über das **Tablet** bis hin zum **Smartphone**?

Ist Microsoft überhaupt noch **innovativ genug** für unsere **zukünftige strategische Ausrichtung**?

Sicherheit beginnt mit Erfahrung

5.8+ Milliarden
Suchanfragen pro Monat weltweit



250+
Millionen
aktive Nutzer



400+
Millionen
aktive Nutzer



2.4+ Millionen
emails pro Tag

Microsoft
Exchange
Hosted Services

10+ Trillionen
Objekte in Microsoft Azure
Speicher

Microsoft Azure



48+
Millionen
Nutzer in 41
Märkten



50+
Millionen
aktive Nutzer



1 von 4
Unternehmenskunden



50+ Milliarden
Verbindungsminuten jeden
Monat



200+ Cloud Dienste

1+ Milliarde Kunden · 20+ Millionen Unternehmen · 90+ Märkte weltweit

Eine vertrauenswürdige Cloud



Cyber-Security 

Höchstmögliche Sicherheit durch jahrzehntelange Erfahrung in der Erstellung sicherer Software und sicherer IT-Services. [Security Development Lifecycle mündet in ISO Standard 27034](#)

Datenschutz 

Datenschutz ist nicht nur im Bereich Online-Dienste für Microsoft eine der höchsten Prioritäten. Keine Werbung oder Data-Mining mit Kundendaten.

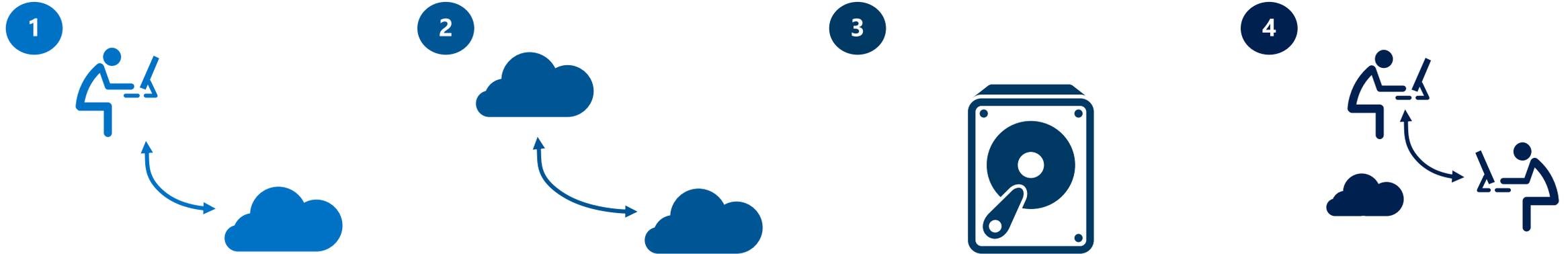
Konformität 

Klares Bekenntnis zu Industriestandards und strikte Beachtung interner Organisationsstandards.

Transparenz 

Veröffentlichung des Security Development Lifecycle (SDL), Offenlegung unserer Best Practices im Betrieb von Diensten, Freigabe unserer Law Enforcement Transparency Reports und unsere Trust Center für Office 365 und Azure.

Schutz durch Verschlüsselung



Datenverkehr zwischen Nutzer und Dienst

Datenverkehr zwischen Rechenzentren

Gespeicherte Daten

Ende-zu-Ende Kommunikations-Verschlüsselung zwischen Nutzern

Schutz vor Abhören der Kommunikation und Sicherstellung der Transaktionsintegrität

Schutz vor Abfangen der Daten

Schutz vor Diebstahl von physikalischen Medien

Schutz vor Abfangen oder Manipulation der Daten

Microsoft's Crypto-Roadmap

| Dezember 2013 Verpflichtung | Kalenderjahr 2014 Fortschritt | Kalenderjahr 2015 & Zukunft |
|---|--|--|
| <ul style="list-style-type: none"> Wir werden Kundendaten zu/von Microsoft standardmäßig verschlüsseln Alle wichtigen Plattform-, Produktivitäts- und Kommunikationsdienste verschlüsseln Kundendaten zwischen Rechenzentren Übergabe von Inhalten (z.B., Mailverkehr) zwischen großen Partnern wird transportverschlüsselt Wir werden die bestmögliche Verschlüsselung nutzen um diese Kanäle zu schützen, einschließlich Perfect Forward Secrecy und Schlüssel mit 2048 Bit Länge All das wird bis Ende 2014 zum Einsatz kommen, vieles davon früher | <ul style="list-style-type: none"> 100% standardmäßige Verschlüsselung von Kundendaten zu/von Microsoft 90+% aller Dienste planmäßig mit bestmöglicher Verschlüsselung 90+% aller Dienste planmäßig mit Verschlüsselung zwischen Rechenzentren Mailverkehr mit Mail Providern jetzt verschlüsselt, sofern von ihnen unterstützt. Wesentliche internationale eMail arbeiten zusammen. | <ul style="list-style-type: none"> Erprobung weiterer Verschlüsselungstechnologien Andauernde Integrationsarbeit mit zugekaufter Technologie (Skype, Yammer, Nokia etc.) |

IT-Sicherheit in Microsoft RZ

Wesentliche Sicherheitsmerkmale:

- Geographisch verteilte und sich gegenseitig absichernde Rechenzentren (in Europa: Dublin in Irland und Amsterdam in den Niederlanden)
- Redundante Systeme innerhalb der Rechenzentren
- 9 Ebenen von Datensicherheit
- Verschlüsselte Datenkommunikation über SSL
- Betriebsprozesse an etablierten Konzepten (ITIL/MOF) ausgerichtet und laufend überprüft
- Permanenter Support, 24 Stunden am Tag, 365 Tage im Jahr
- Dienstgütevereinbarung (SLA) mit 99,9% garantierter Verfügbarkeit (SLAs auf [Produktseiten](#) verfügbar)
- SAS70- bzw. SSAE 16- und ISO 27001/2 27018 -Zertifizierung für die Rechenzentren

Deutsches Whitepaper zu Sicherheitsfeatures der Microsoft Online Services ist [online](#) verfügbar



Datenschutz als Entwurfskriterium

Eingebauter Datenschutz



- Datenschutzerfordernisse werden im Entwicklungsprozess ermittelt und umgesetzt
- Datenschutzfunktion und Kontrollen werden in Produkten und Diensten eingebaut

Keine Werbung



- Wir entwickeln keine Werbeprodukte, die die Auswertung der Daten unserer Kunden nutzen
- Kein Durchsuchen von eMails oder Dokumenten zu Werbezwecken

Transparenz



- Bereitstellung von Informationen über die geografische Lokation gespeicherter Daten, wer Zugriff darauf hat und wann
- Information an Kunden zu Änderungen im Bereich Sicherheit und Datenschutz, Audit Ergebnisse auf Anfrage

Gelebter Datenschutz



Umfassendes
Datenschutzprogramm
seit mehr als 10 Jahren

40+ Vollzeit
Datenschutzfachleute

Mehrere hundert
weitere mit
datenschutz-
bezogener
Verantwortung

Verpflichtung zu
internationalen
Standards und
Konformität

Fortlaufende interne
und externe
Auditierung unserer
Cloud-Dienste



Neue Maßnahmen
zur Absicherung
von Kundendaten
im Licht der Fragen
zu Regierungs-
handeln

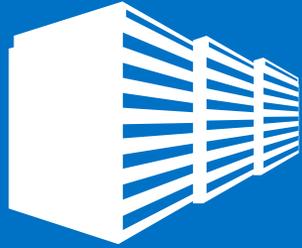
Ausgleich zwischen
Datenschutz- und
nationalen
Sicherheits-
anforderungen

Stärkung der
Verschlüsselung von
Kundendaten über alle
Dienste hinweg

Einzigster Cloudanbieter
der die strengen EU
Standards für
internationale
Datenverarbeitung
umsetzt

Gelebte Transparenz

Wo werden Daten gespeichert?



Azure Kunden können die Region festlegen, in der ihre Daten gespeichert werden (Europa, US, Asien)

Eindeutige Karten zu Daten und geografischen Bereichsgrenzen

Wer hat Zugriff und wie erfolgt er?



Zugriff auf Kundenkerndaten nur zur Problembehebung und zum Schutz vor Schadsoftware

Zugriff auf Kundenkerndaten nur durch Schlüsselpersonal mit Ausnahmegenehmigung

Transparenz über Unterauftragnehmer

Vertragsbedingungen binden auch Subunternehmer

Worüber wird man informiert?



Information zu Änderungen der Datenlokationen

Information zu neuen Unterauftragnehmern

Wir stellen auf Anforderung Zusammenfassungen unserer Auditierungsberichte zur Verfügung.

Auskunftsuchen von Behörden



Eingebaute weltweite Konformität



- Befähigung von Kunden zur Konformität mit internationalen Standards, z.B. ISO 27001, ISO 27018, EUMC, HIPAA, FISMA
- Vertragliche Verpflichtung zu Datenschutz, Datensicherheit und Umgang mit Kundendaten durch Regelungen zur Auftragsdatenverarbeitung

Instrumente für Kunden zur Umsetzung interner Richtlinien



- Administratoren-Instrumente wie Data Loss Prevention, Archiving, E-Discovery zur Umsetzung organisatorischer Konformität

Datenschutzkonformität

- Microsoft Trust-Center als Security, Privacy und Compliance Portal
- Auftragsdatenverarbeitung nach BDSG §11
- EU Safe Harbor und EU Standardvertragsklauseln
Microsoft Online Information Security Policy
nach ISO 27002
- Audit „Summary Report“ der letzten zwei Audits
- ISO27001, ISO 27018, SAS70 Typ II bzw. SSAE 16 –
für alle Datacenter und Services wie Office 365 oder
den Windows Azure Kern Diensten
- > Erfüllung aller Anforderungen der Orientierungshilfe Cloud Computing



Sichere Cloud – standardbasiert, überprüfbar

Compliance



ISO 27001 Security techniques

– Information
security
management
systems –
Requirements

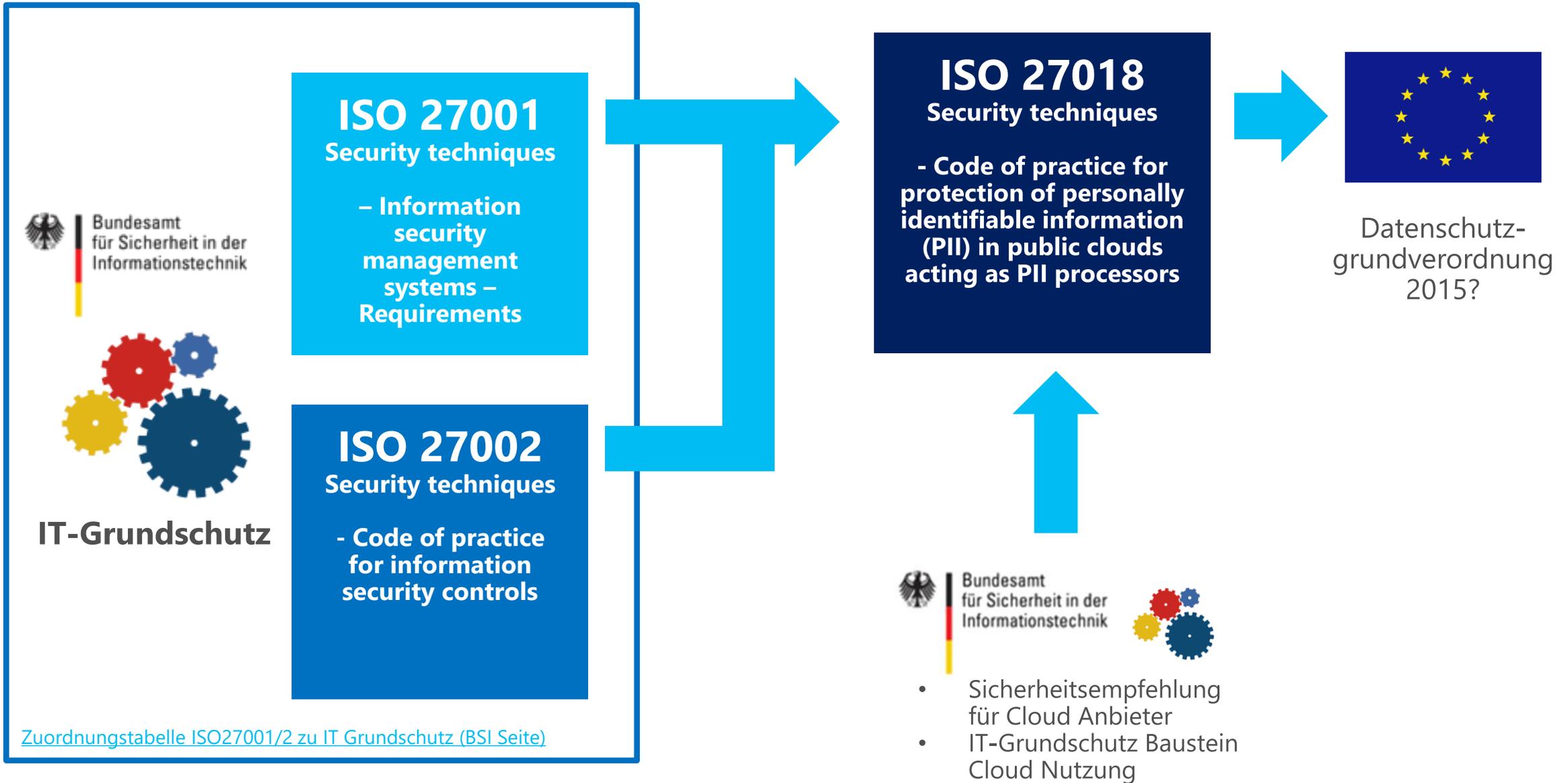
Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation

ISO 27002 Security techniques

- Code of practice
for information
security controls

11 Überwachungsbereiche mit 39 Hauptkategorien (Kontrollzielen), untersetzt mit 133 Sicherheitsmaßnahmen zur Erreichung der Kontrollziele

Sichere Cloud – standardbasiert, überprüfbar



[Zuordnungstabelle ISO27001/2 zu IT Grundschutz \(BSI Seite\)](#)

- Sicherheitsempfehlung für Cloud Anbieter
- IT-Grundschutz Baustein Cloud Nutzung

Sichere Cloud – standardbasiert, überprüfbar

ISO 27018
Security techniques

- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors



CG BUSINESS CONSULTING
FOR SUCCESSFUL BUSINESS MANAGEMENT SYSTEMS

Home About ISO Products ISO Info Centre Testimonials Client Case Studies Contact

Microsoft leading privacy in the Cloud as it adopts ISO 27018 Standard

Newsletter Whitepaper Jobs Shop

CIO Events CIO-Netzwerk Benchmarks Bildung

Themen, Personen, Firmen

Einneutliche Richtlinie für personenbezogene Daten

Microsoft setzt ersten internationalen Cloud-Datenschutzstandard um

20. Februar 2015 Von Klaus Manhart

Als einer der ersten Provider setzt der IT-Konzern Microsoft die neuesten internationalen Datenschutzstandards für Cloud Computing ein. Was aber bedeutet das konkret für Unternehmen?

Empfehlen Der von Microsoft verwendete Standard **ISO/IEC 27018** wurde von der

By Ms. Smith Follow

real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Februar 2015

Azure
Office 365
CRM Online
Intune



Microsoft Azure is first major cloud provider to adopt ISO 27018 privacy standard



RELATED

- Microsoft, Privacy, and the Cloud: Pick all Three
- Schools keep track of students' online behavior, but do parents even know?
- What to consider when negotiating a hybrid cloud SLA

Zusammenfassung

- Auseinandersetzung mit den Potenzialen und Herausforderungen der Cloud ist auch für die öffentliche Verwaltung unverzichtbar 
- Wir müssen differenziertere Diskussionen zur Ausgestaltung von Cloud Szenarien und zur Klassifikation von Daten und Anwendungen führen 
- Die sichere Cloud ist keine Utopie, sondern heute umsetzbar auf der Basis von Erfahrungen, verlässlicher und erprobter Technologie, internationalen Standards und umfassender Transparenz

Weiterführende Informationen

- [Orientierungshilfe Cloud Computing](#)
- [Deutschsprachiges Trust-Center für Office 365](#)
- [Deutschsprachiges Trust-Center für Microsoft Azure](#)
- [Leitfaden für Entscheidungsträger Datenschutz- und Informationssicherheit](#)
- [2014 Law Enforcement Request Report](#)

