T.I.S.P.®
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2011

Cloud Computing Security

Oliver Dehning
antispameurope GmbH
Geschäftsführer

Cloud Computing Security

- Cloud Computing
- Computing Security
- Cloud Security
  - Security in der Cloud?
  - Security aus der Cloud?

CLOUD COMPUTING

Definition

- „Cloud Computing ist ein Modell, das **on-demand** und **online** den Zugriff auf einen **gemeinsamen Pool** **konfigurierbarer** Computing-Ressourcen [...] ermöglicht.“

NIST; National Institute of Standards and Technology, USA

Servicemodelle

- IaaS – Infrastructure as a Service:
  - Virtualisierte Hardware-Ressourcen (Rechner, Netzwerk, Speicher)
- PaaS – Platform as a Service:
  - Programmier- oder Laufzeitumgebungen mit flexiblen, dynamisch anpassbaren Rechen- und Datenkapazitäten.
- SaaS – Software as a Service:
  - Online verfügbare Anwendungsprogramme

Liefermodelle

- Private Cloud:
  - Abstrahierte IT-Infrastrukturen innerhalb der eigenen Organisation
- Community Cloud:
  - Abstrahierte IT-Infrastrukturen wie bei der Public Cloud – jedoch für einen definierten Nutzerkreis (Community)
- Public Cloud:
  - Abstrahierte IT-Infrastrukturen für die breite Öffentlichkeit
  - Bereitgestellt über das Internet
- Hybrid Cloud:
  - Kombination aus Private und Public Cloud

Abgrenzung (Public) Cloud Computing

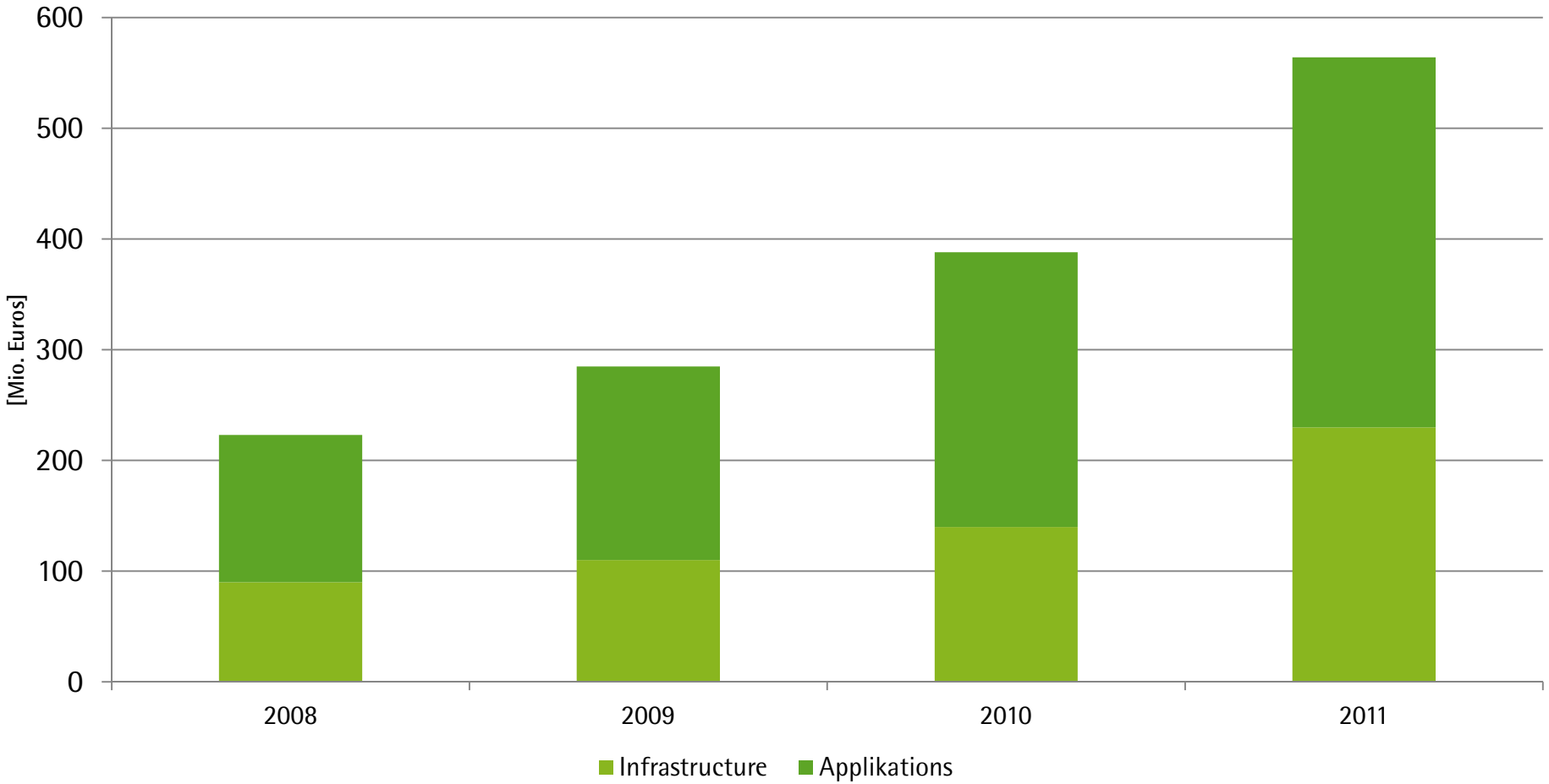
Dimension	Klassische IT	Public Cloud
Räumliche Begrenzung	Innerhalb eines physischen Perimeters, zentral, im eigenen Rechenzentrum	verteilt, nicht exakt einzugrenzen, im Internet
Besitz und Kontrolle der Ressourcen	private Ressourcen, Nutzer und Betreiber sind identisch, Insourced	öffentliche Ressourcen, Nutzer und Betreiber sind verschieden, Outsourced
Multi-Mandenten	Typisch ein einzelner Kunde / Einzelnutzung	Typisch mehrere Mandanten / gemeinsame Nutzung
Verbindung nach und von außen	geschlossene Systeme, Abschottung nach außen z.B durch Firewalls, Datenaustausch z.T. über proprietäre Standards	offene Systeme, einfacher Zugang und Datenaustausch aus dem Internet über standardisierte Schnittstellen, Web / Webservice
Spezialisierung	Kundenspezifische Systeme und Anpassungen, z.T. bis tief in das System	Commoditized (Massengut), im Prinzip für alle Nutzer gleich, kundenspezifische Anpassungen durch Parametrisierung
Dynamik	Statische Systeme, starre Architektur, Größenänderungen nur in Sprüngen möglich, lange Vorlaufzeiten für Bereitstellung	Hochdynamisch, flexibel, skalierbar, "On Demand"
Kosten	typisch CAPEX, hohe Initialkosten, schwer bestimmbare Folgekosten, Nutzungsende bedingt keinen Kostenstop	typisch OPEX, keine bis geringe Initialkosten, exakt bestimmbare Folgekosten, Kosten enden mit Nutzungsende

Vorteile von Cloud Computing

- Kosteneffizient
  - durch massierte Nutzung gleichartiger Hard- Software und Services (Economy of Scale)
- Flexibel, skalierbar
  - Dynamische Bereitstellung von Ressourcen nach Bedarf
- Robust
  - Redundanter Aufbau
  - Expertise durch höhere Spezialisierung, dadurch weniger Fehler / Fehlkonfigurationen

KMU profitieren in besonderem Maß von Cloud Computing

Cloud Computing in Deutschland



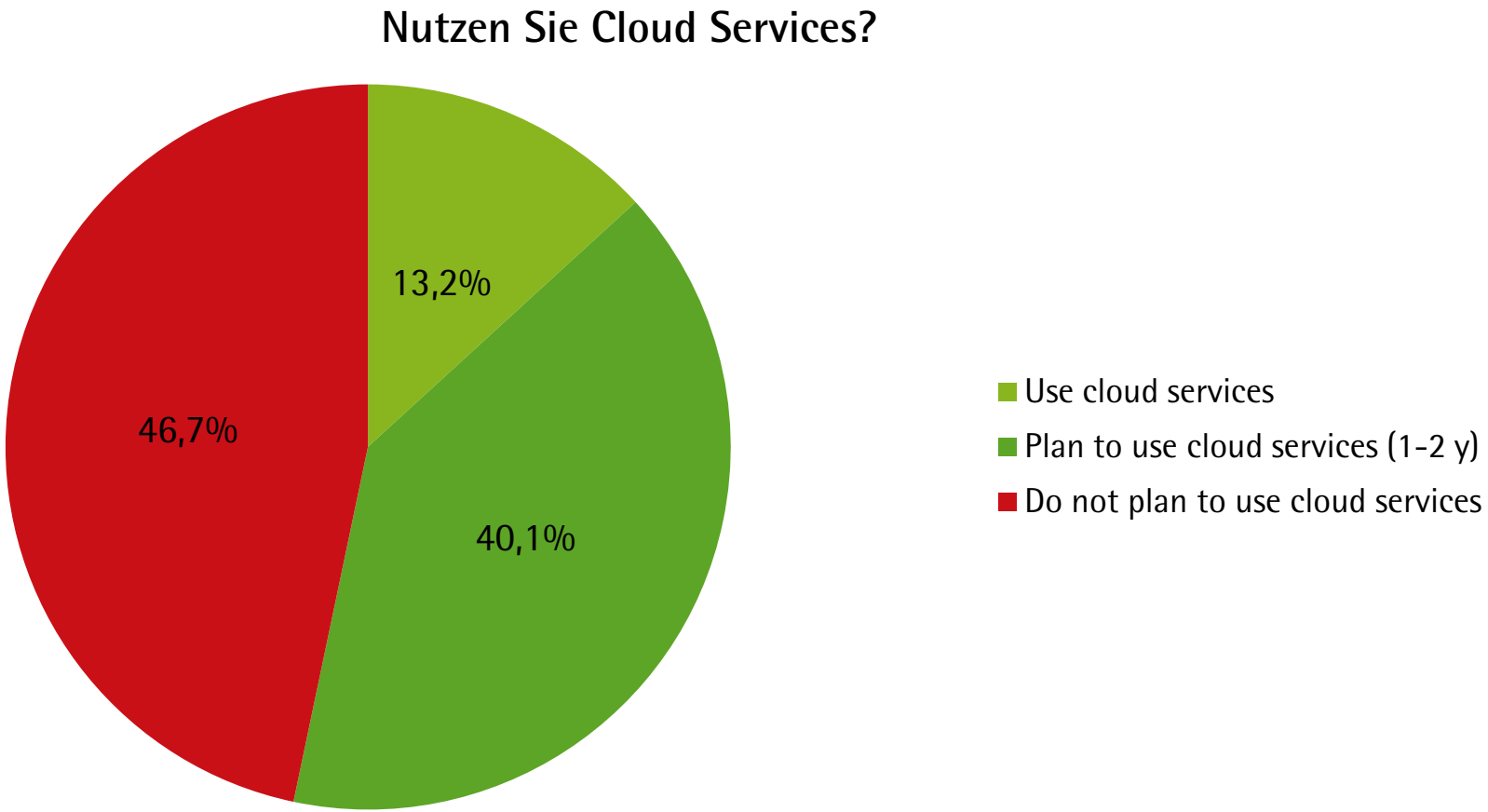
36% CAGR: Cloud Computing wird die IT-Branche nachhaltig verändern

Source: Bitkom, 2010

Treibende Trends

- Mobile Computing
- Social Networks
- Consumerization of IT
  - Bring your own device

Cloud-Nutzung in deutschen Unternehmen



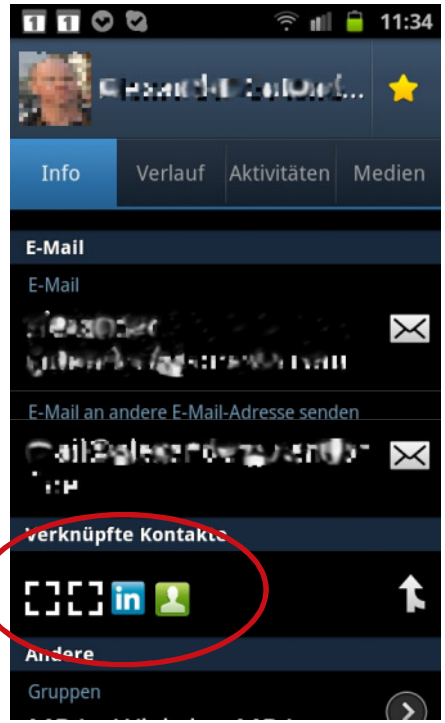
Die Mehrheit deutscher Unternehmen nutzt bereits Cloud Services oder plant die Nutzung.
Ein großer Teil lehnt Cloud Computing (noch) ab.

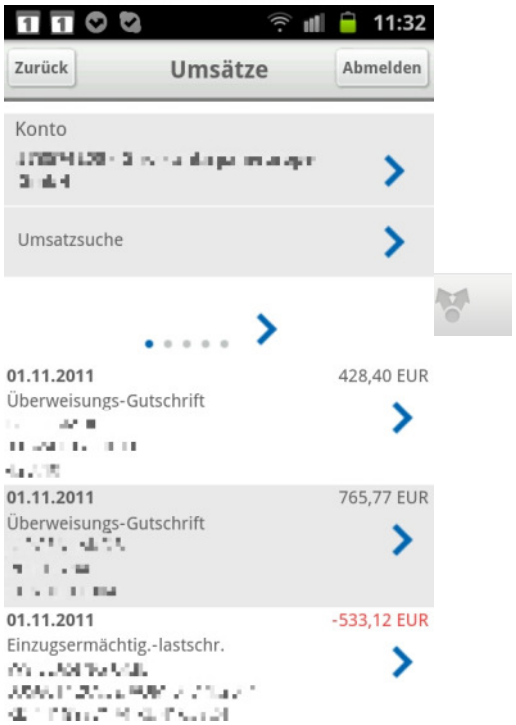
Source: IDC, Germany 2010

Faktische Marktbedeutung

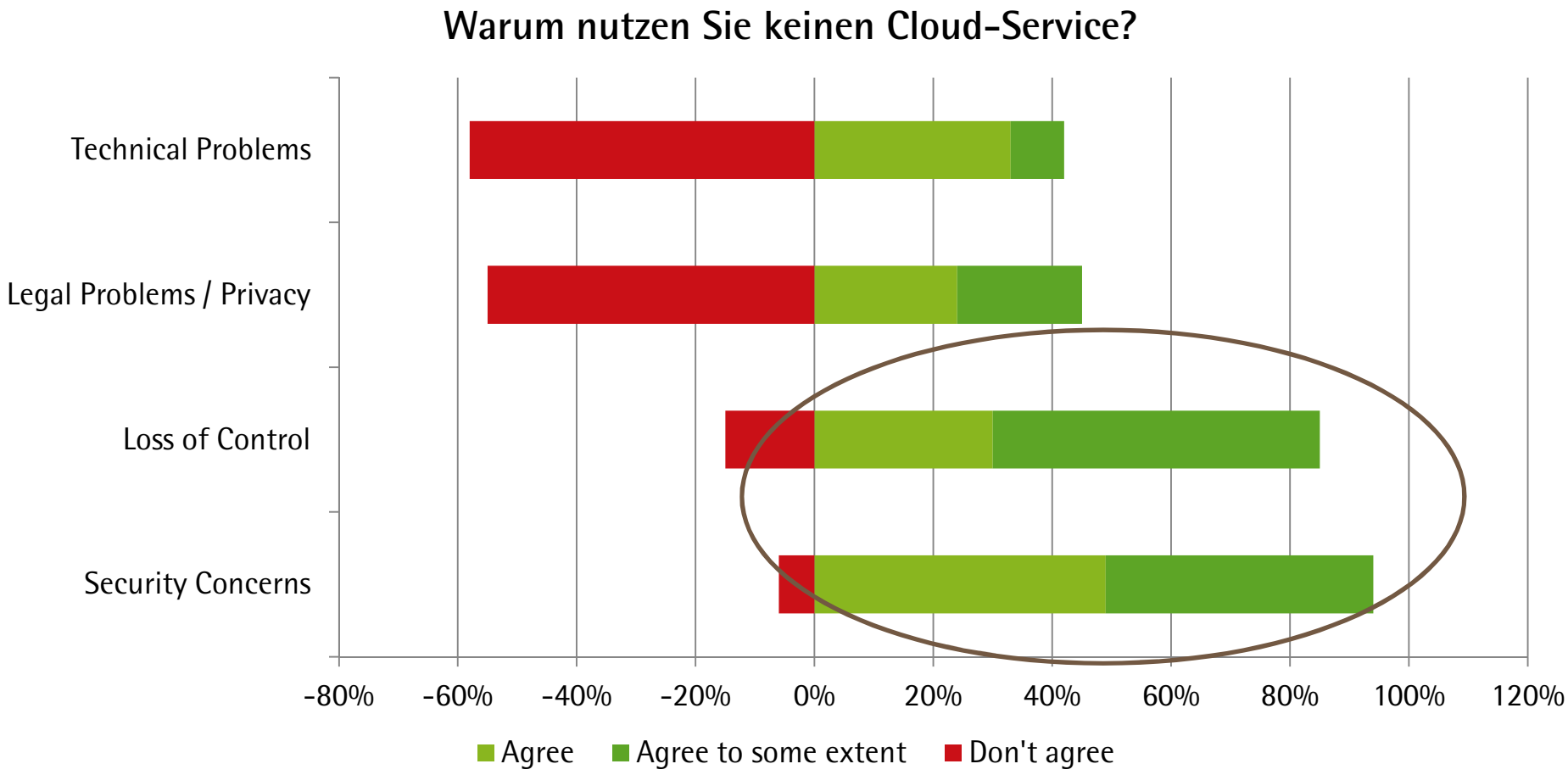
- "Both governments and SMEs face the reality that many of their employees will be using cloud-based services whether or not this is part of their official policy."
  (enisa: Cloud Computing - Benefits, risks and recommendations for information security; Nov. 2009)

- Wem gehören die Daten?
- Datentrennung?





Barrieren



Sicherheit und Transparenz sind essentiell

Source: FINAKI, Aug 2010

CLOUD SECURITY

Aufgaben der IT-Sicherheit

- Verfügbarkeit
- Vertraulichkeit
- Integrität
- Revisionssicherheit
- Transparenz

... von IT-Systemen und darin gespeicherten Daten.

Klassische Risiken

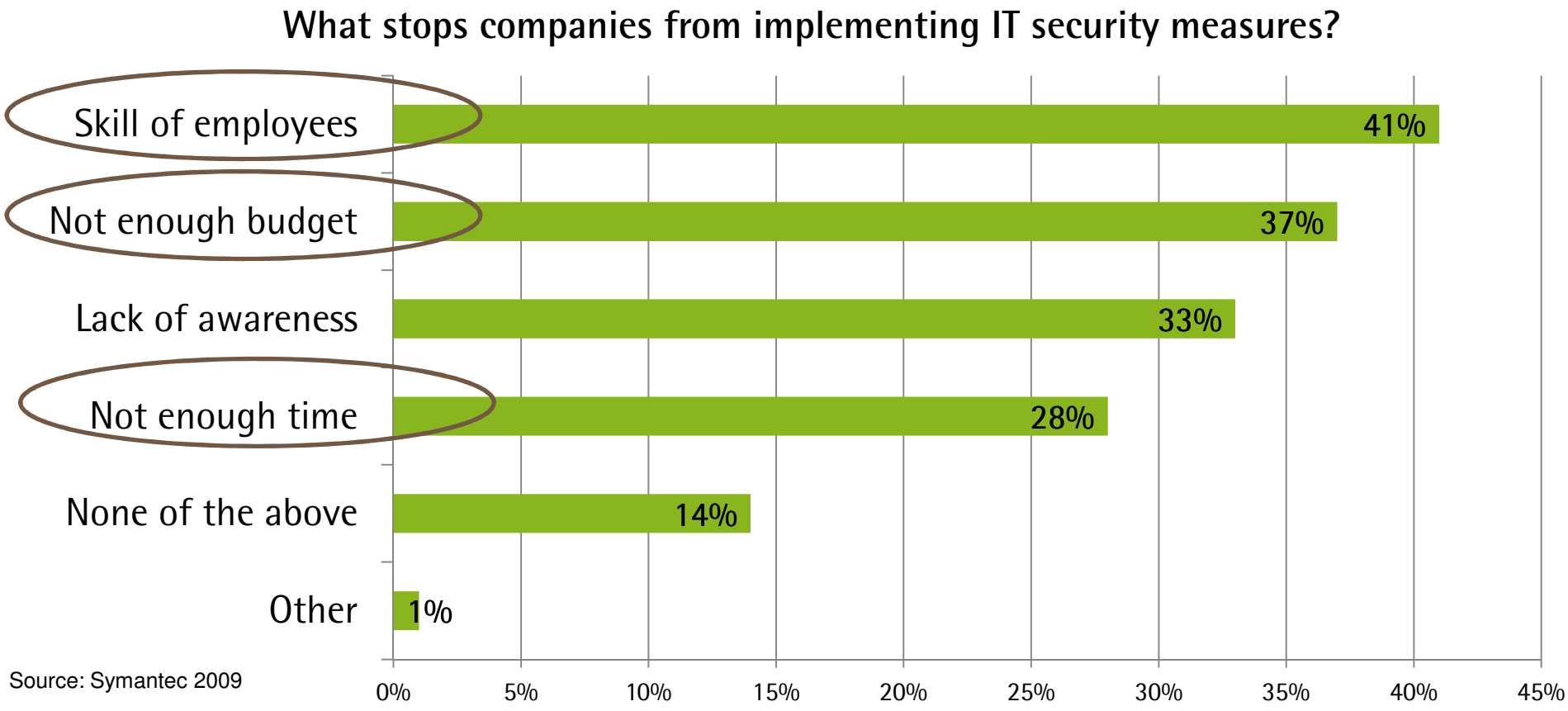
- Software-Fehler
- Hardware-Fehler
- Sicherheitslücken in der Software
- Sicherheitslücken beim Nutzer
- Malicious Insider
- Allgemeine Betriebsrisiken

Cloud-spezifische Herausforderungen

- Auflösung des Perimeter
  - Tatsächlicher Ort der Daten nur schwer kontrollierbar
  - Große Angriffsfläche
- Management Interfaces offen zum Internet
- Mehr-Mandanten-Systeme
  - Datentrennung, Isolationsfehler
- Loss of Governance, Kontrollverlust
  - Datenlöschung nur schwer kontrollierbar
  - Nachvollziehbarkeit von Verarbeitungswegen
  - Leistungsverweigerung des Anbieters
- Compliance-Risiken, Datenschutz
- Vendor Lock-In
- Massierung von Daten
  - Cloud-Services sind ein attraktives Angriffsziel

Also wird IT durch Cloud Computing unsicherer?

Unternehmen und IT Sicherheit



Cloud Security adressiert wesentliche Hindernisse für IT-Sicherheit

Cloud Computing verbessert die Sicherheit

- Robust
  - Mehrere Rechenzentren
  - Robuster RZ-Betrieb
    - Redundante Stromversorgung
    - Notstrom (Diesel)
  - Unzählig viele redundante Systeme je RZ
  - Mehrfachanbindung je RZ
  - Redundante Auslegung der Netz-Infrastruktur (Router etc.)
  - Effektives und effizientes Management von Updates und Einstellungen

Cloud Computing verbessert die Sicherheit

- Erprobte fail-over Mechanismen
  - Schutzmechanismen zur Erkennung von Fehlkonfigurationen
  - Kürzere Reaktionszeiten bei akuten Bedrohungen
  - Automatische Übernahme der Last
  - Rollback bei Fehlkonfigurationen
- 24/7 Überwachung und Betrieb

Cloud Computing verbessert Sicherheit

"... the ability of the cloud provider to dynamically reallocate resources for filtering, traffic shaping, authentication, encryption, etc, to defensive measures (e.g. against DDoS attacks) has obvious advantages for resilience."

Source: enisa Cloud Computing Security Risk Assessment

Cloud Computing macht Sicherheit günstiger

" ... put simply, all kinds of security measures are cheaper when implemented on a larger scale. Therefore the same amount of investment in security buys better protection."

Source: enisa Cloud Computing Security Risk Assessment

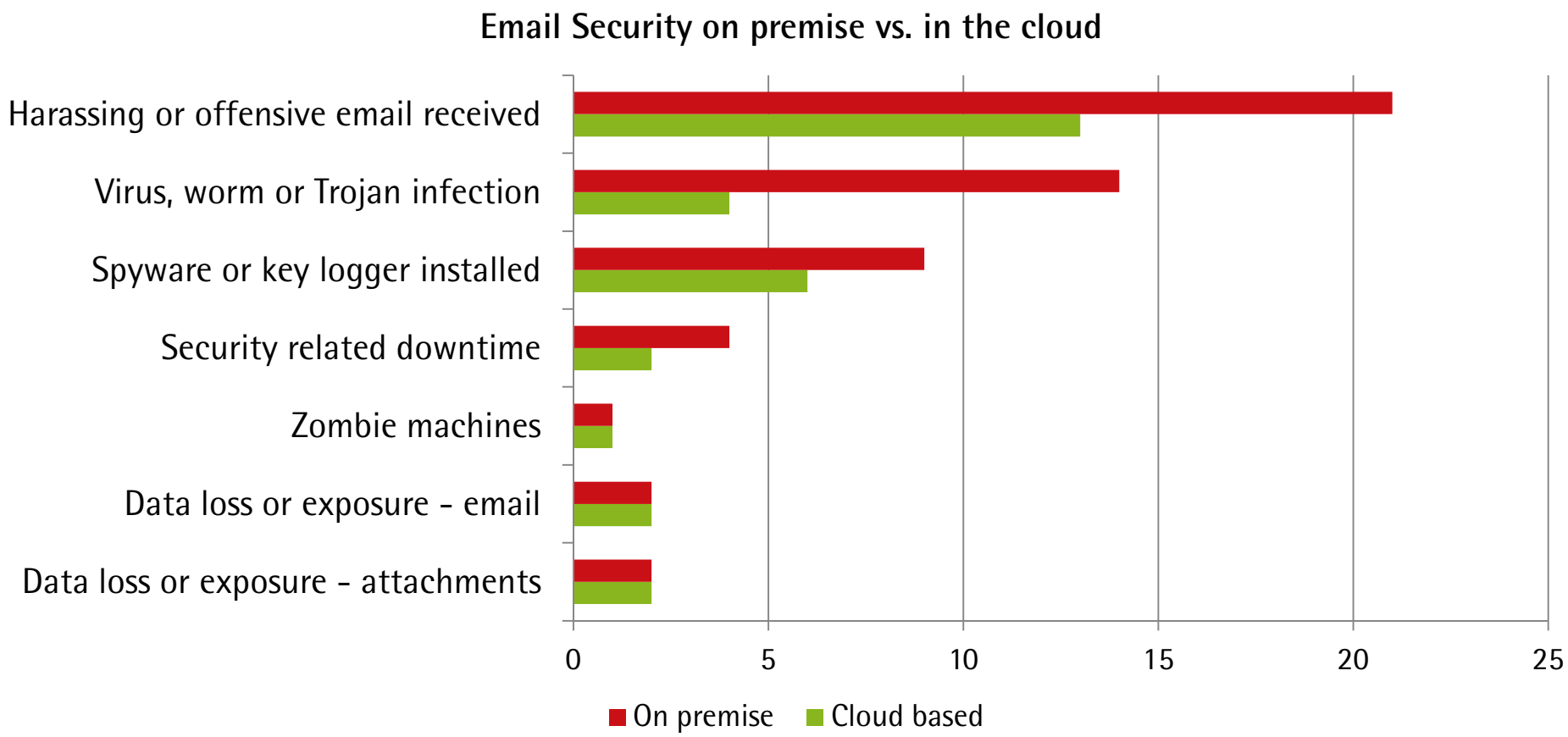
Beispiel: Spamfilter

Gehosteter Spamfilter Service (SaaS) im Vergleich zu on-premise Spamfilter

- 500 Nutzer

	On Premise	Cloud Service
Auslegung	2 Appliances	
TCO	• Energie: ca. 3400 kWh / Jahr, x 0,3 Euro / kwh (gekühlt): 1020 Euro / Jahr • Abschreibung: 800 Euro / Jahr • Wartung / Updates: 1400 Euro / Jahr • Administration (Überwachung, Konfiguration, etc.), 2 h / Woche, 40 Euro / h: 4000 Euro / Jahr • **Gesamt: 7220 Euro / Jahr**	**5000 Euro / Jahr**

Beispiel: Spamfilter



Source: Aberdeen Group, 2010

AKTUELLE VORFÄLLE BEI CLOUD PROVIDERN

Einbruch bei RSA

- März 2011: Hackereinbruch bei RSA
- SecurID Token gestohlen
- In Folge Hackereinbruch bei Lockheed Martin u.a., im Mai 2011
  - Attacke wurde allerdings frühzeitig erkannt
- Austausch von 40 Mio. Sicherheitsschlüsseln durch RSA

Ausspähung von Nutzerdaten bei Sony

- 17.-19. April 2011: 1. Hackerangriff
- Zugriff auf Nutzerkonten im Sony Entertainment Network (Playstation etc.)
- Daten von mehr als 70 Millionen Nutzern gestohlen
- Adressen, Geburtsdaten, Passwörter, z.T. Kreditkartendaten
- Benachrichtigung von Nutzern erst nach einer Woche
- Zeitweise Sperrung des gesamten Systems durch Sony

- 7.-10. Oktober 2011: Erneuter Zugriff von Hackern
- 93.000 Nutzerkonten betroffen
- Nutzung gestohlener Login-Daten aus „anderen Quellen“

Datenverlust bei Amazon

- 22.-25. April 2011: Massiver Hardware-Ausfall bei Amazon Web Services
  - U.a. E2C Cloud Services
- Dauer einige Stunden bis einige Tage
- Entsprechend langer Ausfall von Services nutzender Unternehmen
- Verlust eines Teils der gespeicherten Daten
  - Daten der letzten 11 Stunden vor Ausfall
  - Kein Backup durch Amazon
  - Amazon: „Backup ist Aufgabe der Nutzer“
- Weiterbetrieb auf anderen Knoten der Amazon Cloud nach kurzer Zeit möglich
  - Wenn die Kunden entsprechend vorbereitet waren

Offene Nutzerzugänge bei Dropbox

- 20.-21.6.2011: Sicherheitslücke bei Dropbox
- Login-in in jedes Benutzerkonto etwa 4 Stunden lang mit beliebigem Passwort möglich
- < 1% der Accounts wurden in dieser Zeit genutzt

Schlussfolgerungen

- Die Cloud ist nicht unfehlbar – auch wenn es zeitweise so scheint
- Cloud Computing ist noch jung
  - Viele Dinge passieren zum ersten Mal
  - Erfahrungen fehlen – auf Anbieter- und Nutzerseite
- Vorfälle machen Schlagzeilen – aber wie hoch sind die Auswirkungen tatsächlich?
  - Wie viele Vorfälle gibt es bei interner IT – mit welchen Auswirkungen?
- Stabilität und Sicherheit von Cloud Services sind schon jetzt generell höher als bei on-premise üblich
- Cloud Provider gehen generell sehr verantwortungsbewusst vor:
  - Schnelle Reaktion
  - Eingrenzung von Fehlern und Auswirkungen
  - Offene Kommunikation

EMPFEHLUNGEN

Empfehlungen (1)

- Awareness in der Organisation schaffen
- Cloud Services bewusst nutzen, klare Richtlinien definieren und durchsetzen
- Sorgfältige Auswahl des Anbieters
  - Beachtung aktueller und aussagekräftige Nachweise (bspw. Zertifikate) über die Infrastruktur, Sicherheitsmaßnahmen, Datenschutz etc.
  - Ohne weiteres ist (aus Datenschutzgründen) Auftragsdatenverarbeitung nur mit Auftragnehmern mit Sitz in der EU oder im EWR möglich
- Umsetzung abgestimmter Sicherheitsmaßnahmen zwischen Cloud-Anbieter und Cloud-Anwender

Empfehlungen (2)

- Transparente, detaillierte und eindeutige vertragliche Regelungen der Cloud-gestützten Datenverarbeitung, insbesondere betreffend:
  - Ort der Datenverarbeitung und Benachrichtigung über eventuelle Ortswechsel,
  - Portabilität und Interoperabilität,
  - Datenschutzrechtliche Verantwortung,
  - Kontrollrechte des Auftraggebers,
  - Mögliche Beauftragung von Subunternehmern,
  - Laufzeit und Rückgabe bzw. Löschung von Daten.
- Daten, soweit möglich, verschlüsseln
- Nach Vertragsschluss regelmäßig prüfen, ob der Anbieter die erforderlichen technischen und organisatorischen Maßnahmen einhält

Vielen Dank!

Oliver Dehning
antispameurope GmbH
Am Listholze 78
30177 Hannover

0511 – 260 905 0
dehning@antispameurope.com