

# **ICT-Security Management - Im Spannungsfeld zwischen Business und Technik**

**ISSS St. Galler Tagung  
10. März 2016**

Daniel Felix Maurer  
lic. phil. UZH  
Mitglied der Geschäftsleitung, Partner TEMET AG

# Ziele des Referats

- Aufzeigen der Wirkungsfaktoren des aktuellen Spannungsfeldes mit Bezug zur ICT-Security
  - Bildlich gesprochen «Kurz vor dem Vulkanausbruch»
- Bestimmen der Leitplanken für den Sicherheitsberater
  - Bildlich gesprochen «Hängebrücke über dem Höllenabgrund»
- Aktuelle Beispiele aus der Praxis
  - Bildlich gesprochen «Chaos pur»
- Lessons Learned
  - Bildlich gesprochen «Ausblick ins Paradies»
- Zusammenfassend: eine unabhängige Expertensicht auf das Thema

# Angaben zum Referenten

## Daniel Felix Maurer

- lic. phil. UZH, Informationssystem-Architekt
- 32 Jahre Tätigkeit in der IT
  - 14 Jahre Systemprogrammierer, IT-Projektleiter und Leiter der IT-Security Fachstelle bei einer Grossbank
  - 18 Jahre IT-Security Beratung bei Finanzinstituten und in der Verwaltung
- Mitglied der Geschäftsleitung und Partner TEMET AG
  - Seit November 2011
- Persönliche Schwerpunkte
  - Information Security Management Systems (ISMS)
  - Risk Management
  - Audits & Compliance
  - Cryptology & Cyber Security

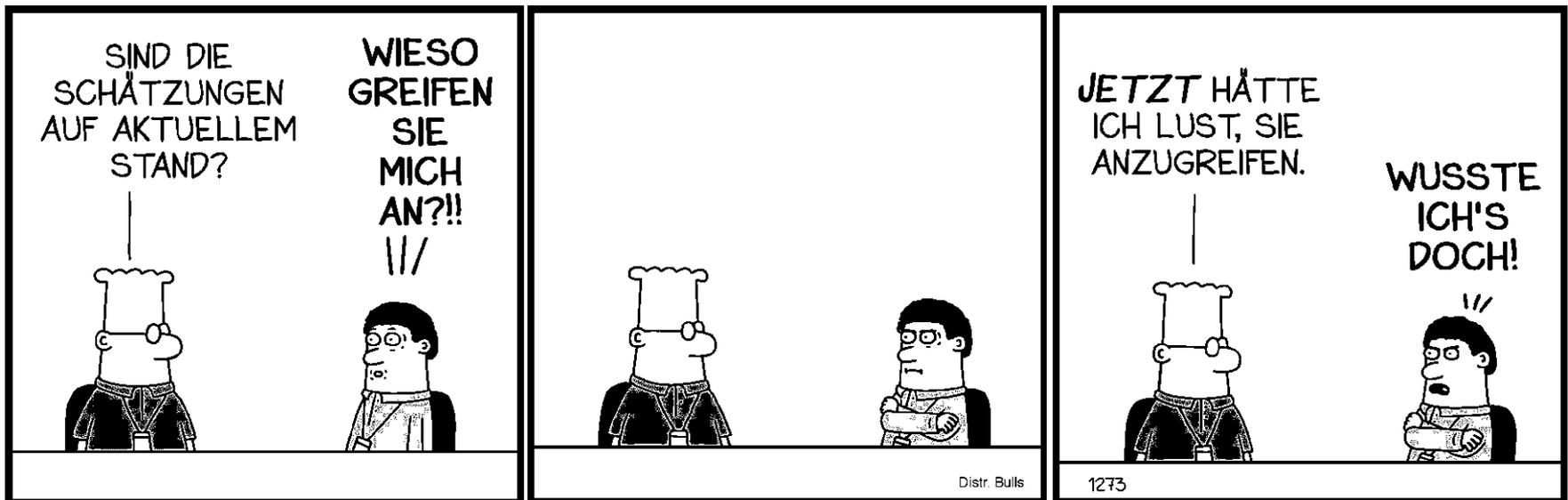
# Wer ist die TEMET AG

- Gründung: März 2010
- Inhabergeführte Aktiengesellschaft
- Sitz am Basteiplatz 5, im Herzen von Zürich
- Aktuell 12 Information Security Consultants
- Aktuell 56 Kunden aus Finanz, Verwaltung und Gesundheitswesen
- Die TEMET AG positioniert sich im Markt als herstellerneutrale und auf Informationssicherheit fokussierte Firma, deren Berater fachliche Expertise mit Projektmanagement-Kompetenz verbinden



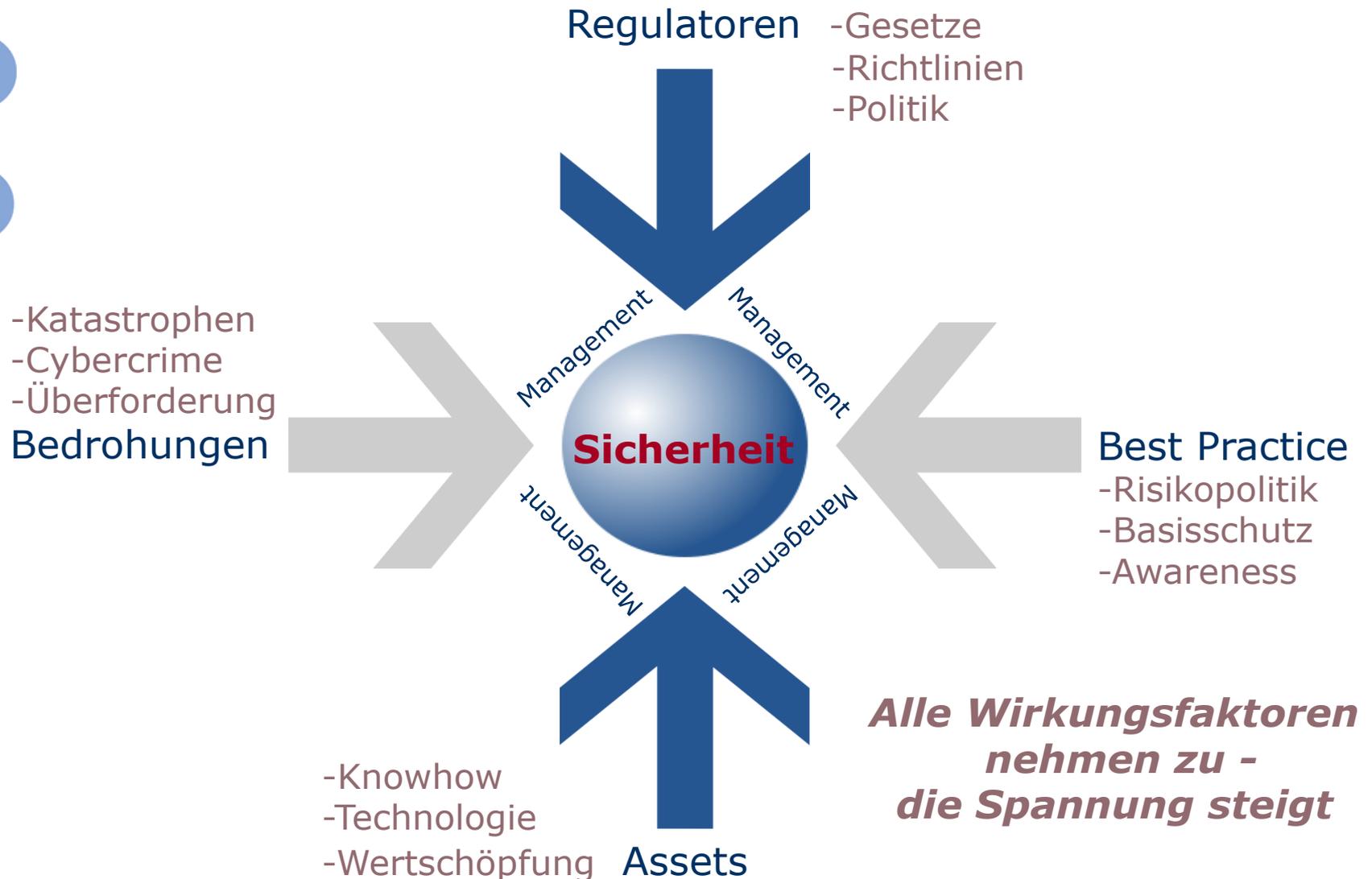
# Im Spannungsfeld zwischen Business und Technik

Beispiel 1 für gelungene  
Kommunikation



Scott Adams; United Features Syndicate Inc. 13. Mai 2015 © SZ.de

# Spannungsfeld 2016



# Leitplanken für die Sicherheitsberatung (... im Spannungsfeld ...)

- Eine **positive Grundeinstellung** ist von Vorteil
- Klare Worte sind geschätzt, Kritik darf/soll geäußert werden
- Man bewegt sich in grundsätzlich **engem Kostenrahmen**, aber Geld ist nicht das eigentliche Problem
- Die Mühlen malen langsam, nur wollen alle schon morgen am Ziel sein
- Business & Fach zeigen sich skeptisch («zuerst müssen die Prozesse stimmen»), die Technik möchte Nägel mit Köpfen machen («wir brauchen vor allem eine effiziente Infrastruktur»)
- Alle sind sich einig: **«Es ist bei der Security auch nicht anders als sonst!»**

# Beispiel aus der Praxis (1)

## Sicherheitskonzept Archivierung

### Branche; Auftrag gebende Stelle

- Krankenversicherer; GL (Governance, Risk, Compliance)

### Probleme

- Business/Fach wollen, dass die IT «irgendwie» **archiviert** (v.a. Verträge und Rechnungen), aber offenbar gibt es dabei noch einige **Gesetze** einzuhalten («verdienen kann man damit aber nichts»)
- IT archiviert fleissig und stösst zunehmend an Kapazitätsgrenzen («wohin mit den E-Mails und Web Content?»; «Logs archivieren? Wieso? Kein Platz, die löschen wir nach 30 Tagen!»)
- Es gibt mehrere DMS, den Anfang eines Records Management und vier unterschiedliche Archive, sowie einen Sponsor (Kundenportal)
- **Die Security soll vermitteln und erklären, um was es eigentlich geht**

### Lösungen

- Es geht um Ownership, Klassifizierung, Verdichtung von Daten
- Aufzeigen, dass **revisionssichere** Archive **wertbeständig** sind
- Gemeinsame Begrifflichkeit finden (ein Siko ist dafür gut geeignet!)

# Beispiel aus der Praxis (2)

## Prozessdesign Control Self Assessments

### Branche; Auftrag gebende Stelle

- Öffentliche Verwaltung; Fachstelle Informationssicherheit

### Probleme

- Ein Handbuch für Informationssicherheit (ISO/IEC 27001&2:2013) regelt seit 2014 den **Basisschutz** und muss auf Auftrag der politischen Exekutive in drei Jahren für die über **70 OE** umgesetzt werden (z.B. Forstwirtschaft, Wasserversorgung, Polizei, Spitäler)
- Es gibt viele **Konflikte** zwischen der IT und den Fachanwendungen
- Die Umsetzung muss aus den laufenden Budgets erfolgen
- Alle OE sind in einem zentral geführten Security Board vertreten, aber es gibt keine etablierte dezentrale Sicherheitsorganisation

### Lösungen

- Periodische Erfassung des Umsetzungsstands durch **Control Self Assessments** (frei konfigurierbare Kontrolllisten in Frageform)
- Aufbau **dezentraler** Sicherheitsverantwortung (AKV ISB)
- Aktiver Miteinbezug der **Linie** (Matrixorganisation reicht nicht!)

# Lessons Learned

## Zusammenarbeit (statt «Chäschtlidänke»)

- Der Trend geht in Richtung **integraler Sicherheit**
- Eine klug ausgestaltete Sicherheitspolitik ist für ein modernes Unternehmen ein **Wettbewerbsvorteil**
- **Sicherheit soll sich am Geschäft orientieren** – und nicht an einzelnen Geschäftsfällen
- Seitens Business und Fach sollen Lösungen gesucht und bevorzugt werden, welche **Sicherheit** und **Wertschöpfung** gleichermaßen befördern
- Die IT soll **Messbarkeit** und **Verlässlichkeit** höher gewichten als Technologievorsprung
- Der Sicherheitsberater soll sich aktiv in den Dialog einmischen und gleichzeitig eine gewisse Distanz bewahren («**Teilnehmende Beobachtung**»)

# Im Spannungsfeld zwischen Business und Technik

## Beispiel 2 für gelungene Kommunikation



Scott Adams; United Features Syndicate Inc. 4. Dezember 2013 © SZ.de

Daniel Felix Maurer  
Mobile +41 79 438 65 42  
[daniel.maurer@temet.ch](mailto:daniel.maurer@temet.ch)



**Besten Dank für Ihre  
Aufmerksamkeit!**

TEMET AG | Basteiplatz 5 | CH-8001 Zürich  
044 302 24 42 | [info@temet.ch](mailto:info@temet.ch) | [www.temet.ch](http://www.temet.ch)

044 302 24 42 | [info@temet.ch](mailto:info@temet.ch) | [www.temet.ch](http://www.temet.ch)  
TEMET AG | Basteiplatz 5 | CH-8001 Zürich