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

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting

Frankfurt a.M., 10. - 11.11.2016

VdS 3473 – Informationssicherheit für KMU

Michael Wiesner

Michael Wiesner GmbH

Michael Wiesner

- Informationssicherheit seit 1994
- Berater, Auditor, Penetrationstester
- Co-Autor VdS-Richtlinien 3473
- Lead Auditor ISO 27001 & VdS 3473, CISM, CRISC, T.I.S.P., OSCP, …
- Blog: www.michael-wiesner.info

Motivation

80 PROZENT DER DEUTSCHEN UNTERNEHMEN SETZTEN PCS EIN

Ohne Computer geht nichts mehr

Datum: 26.03.2004 10:30 Uhr

Das statistische Bundesamt hat erforscht, wieviele Computer in Firmen ihren Dienst verrichten. Ergebnis: Die überwältigende Mehrheit der Unternehmen verlässt sich auf die digitalen Knechte.

Handelsblatt, 2004

GmbHG §43

"(1) Die Geschäftsführer haben in den Angelegenheiten der Gesellschaft die Sorgfalt eines ordentlichen Geschäftsmannes anzuwenden.

(2) Geschäftsführer, welche ihre Obliegenheiten verletzen, haften der Gesellschaft solidarisch für den entstandenen Schaden."

AktG §91 II

- "Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."

BDSG §9

- "Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die **technischen und organisatorischen Maßnahmen zu treffen**, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten"

Lagebild

Bedrohungen	2012	2013	2014	2015
Denial of Service (DoS, DDoS)	→	→	→	→
Botnetze	↗	→	→	↗
Spam	→	↘	↗	↗
Hacktivismus		→	→	→
Drive-by-Exploits	↗	↗	→	↗
Schadprogramme	→	↗	↗	↗
Exploit-Kits		↗	→	↗
Identitätsdiebstahl	→	↗	↗	↗
Schwachstellen	→	↗	→	↗
Advanced Persistent Threats (APT)		↗	→	↗

Gefährdungsbarometer ↗ steigend → gleichbleibend ↘ sinkend

BSI (2015)

Internet Security Days 2016: Cyber-Angriffe der Geheimdienste vor allem gegen den Mittelstand

22.09.2016 11:53 Uhr – Jürgen Seeger vorlesen

Die heute gestarteten ISD leitete der Vizepräsident des Bundesamts für den Verfassungsschutz mit einer Analyse der Bedrohungslage durch russische und chinesische Cyber-Spionage ein. Ziel seien vor allem mittelständische Firmen.

heise.de (2016)

Management von Informationssicherheit

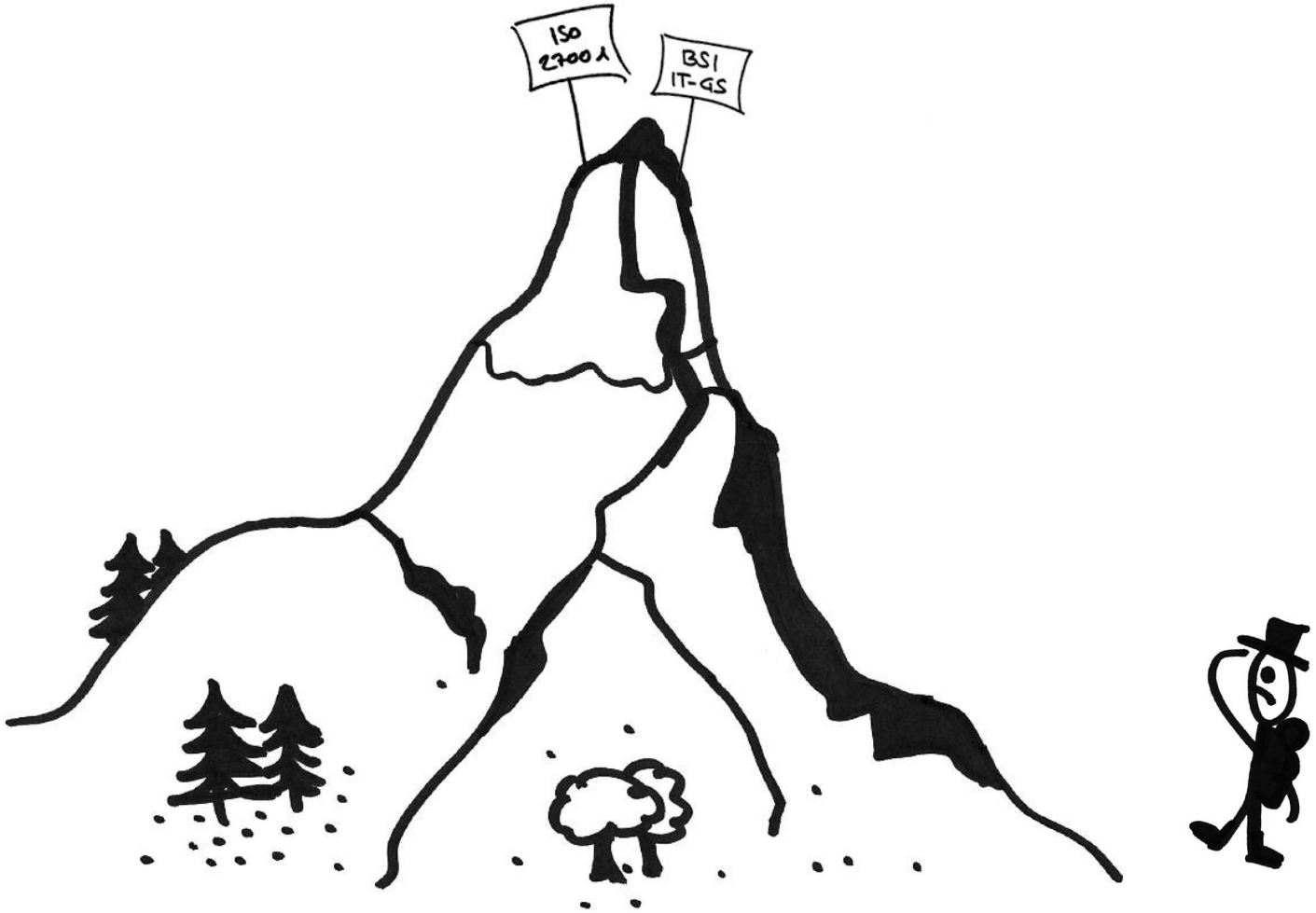
ISO 27001

- Internationaler Standard für Informationssicherheitsmanagement
- Schwerpunkt auf Prozesse
- Wesentlich: Risikoanalyse- und Behandlung
- Sehr generischer Ansatz
- ~30 Seiten

IT-Grundschutz

- Deutscher Standard zur Erreichung eines mittleren Schutzniveaus für IT-Systeme (BSI 100-1/2/3)
- Bundesamt für Sicherheit in der Informationstechnik (BSI)
- Ursprünglich für Bundesbehörden
- IT-Grundschutz-Kataloge (>5000 Seiten)

Das Problem



Herkunft

VdS Schadenverhütung

- 100% Tochter des GDV
- Gesamtverband der Deutschen Versicherungswirtschaft
- "Technischer Arm" der Versicherungswirtschaft

"Der Brandschutz des 21. Jahrhunderts"

- Jedes Unternehmen hat **Brandschutzvorkehrungen**
- Die meisten haben sich gegen **Brandschäden versichert** (Gebäudeversicherungen, Inhaltsversicherungen, Betriebsunterbrechungsversicherung, …)
- Warum nicht auch gegen **Cyber-Gefahren** (z.B. Hackerangriff) versichern?

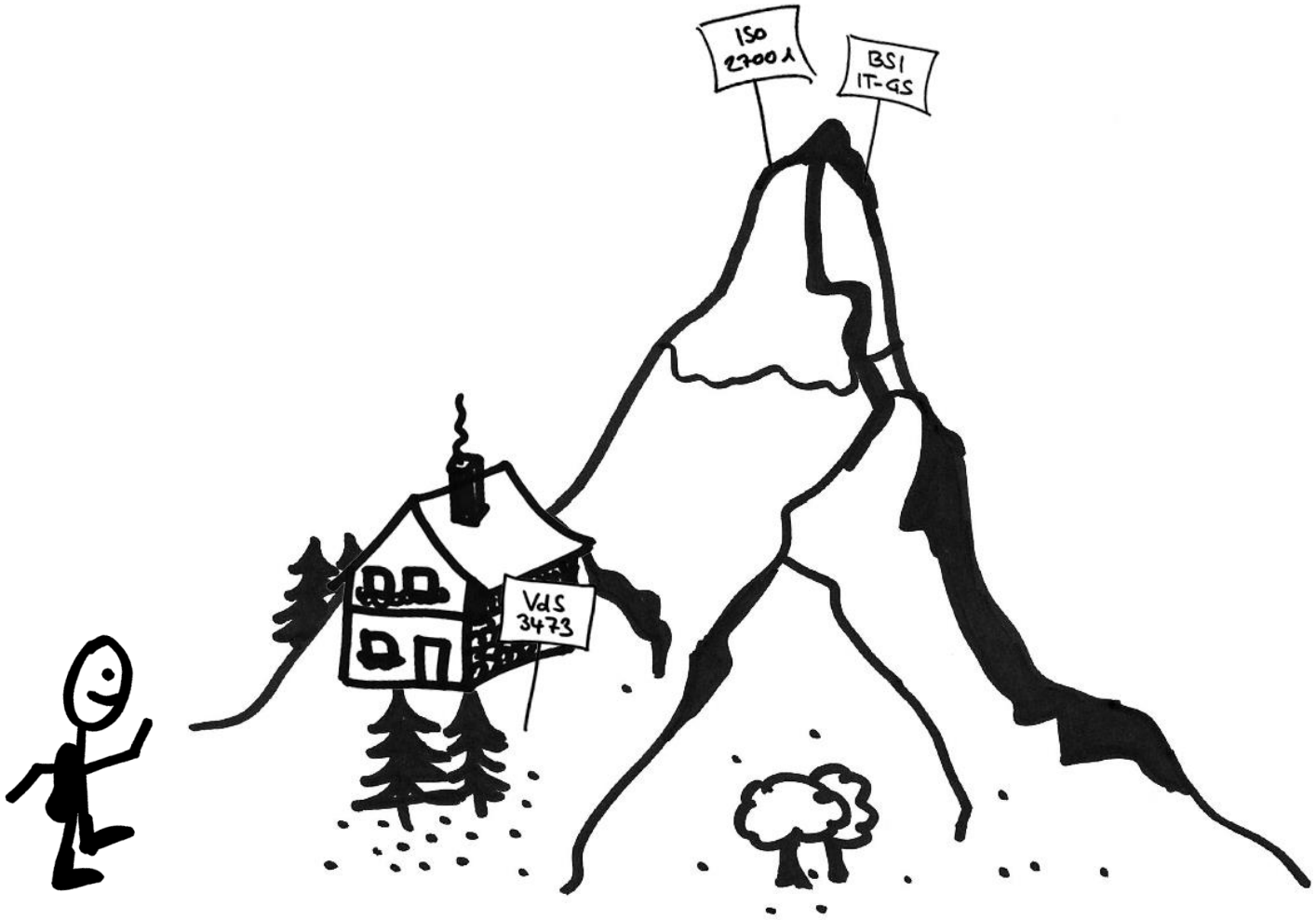
Risiken

- Wie lässt sich das **Risiko einschätzen**, dass ein Unternehmen Opfer eines Hackerangriffs wird?
- Wir lässt sich das **Restrisiko** auf ein akzeptables Niveau senken? →
  Nur Restrisiken werden versichert!
- Wie kann der **Nachweis** darüber erbracht werden?

Ziele

- Unternehmen müssen **Mindeststandards** in Bezug auf Informationssicherheit einhalten
- Die Einhaltung und Wirksamkeit muss nach einem standardisierten Verfahren **überprüft** werden können
- Die Umsetzung muss für möglichst viele Unternehmen mit **überschaubarem Aufwand** möglich sein

Die Lösung



Eigenschaften

Eigenschaften

- **Jung**
  - Erste Veröffentlichung am 01.07.2015
  - Erste Audits im November 2015
  - Erstes Zertifikat im Dezember 2015
- **Kurz**
  - 38 Seiten gesamt
  - 28 Seiten Anforderungen

Eigenschaften

- Komplettes Informationssicherheits-managementsystem (ISMS)
- Definition von Verantwortlichkeiten
- Leitlinie und Richtlinien zur Informationssicherheit
- Organisatorische und technische Maßnahmen
- Kontinuierlicher Verbesserungsprozess (KVP)

Eigenschaften

- Einfache, schnelle Implementierung
- Eindeutige Sprache (MUSS, DARF NICHT)
- Minimalistischer Analyse- und Dokumentationsaufwand
- Definition von Zielen, Freiheit bei der Umsetzung
- Pareto-Prinzip (80/20)

Eigenschaften

- Geltungsbereich: Komplette Informationsverarbeitung
- Organisatorische und technische **Grundanforderungen**
- **Kritische** und **unkritische** IT-Ressourcen
- **Basisschutz** für unkritische IT-Ressourcen
- **Zusatzmaßnahmen** für kritische IT-Ressourcen

Kritische IT-Ressourcen

Kritische IT-Ressourcen

- Wie kann man zuverlässig **kritische IT-Systeme**, **mobile Datenträger** und **Verbindungen** finden?
- BSI 100-2, BSI 100-4, ISO 22301 funktionieren → zu aufwändig für KMU!
- VdS 3473 liefert Minimalansatz (**kein Anspruch auf Vollständigkeit!)**

Kritische Prozesse

- "Das Unternehmen MUSS seine **zentralen Geschäftsprozesse** und sein **Prozesse mit hohem Schadenspotential** identifizieren und dokumentieren"
  (🗎 Kapitel 9.1)

Kritische Prozesse

- **Zentrale Geschäftsprozesse**
  - Von **zentraler Bedeutung** für das Unternehmen
    - Womit verdient das Unternehmen Geld?
    - Wie verdient das Unternehmen auch morgen noch Geld?
- **Prozesse mit hohem Schadenspotential**
  - Fehlfunktion oder Ausfall resultiert in einem "**katastrophalen Schaden**" (🗎 Kapitel 3: Glossar)

Katastrophaler Schaden

- **Leib und Leben von Personen**
  - Menschen kommen ums Leben
- **Zentrale Geschäftsprozesse/Werte**
  - Kommen zum erliegen, Rückkehr unmöglich
- **Rechtskonformität**
  - Gesetze […] werden gebrochen, Haftung ruinös
- **Schadenshöhe**
  - Schaden kann nicht behoben werden

Kritische Informationen

- "Das Unternehmen MUSS jene Informationen ermitteln, die besonders geschützt werden müssen. Besonders zur schützen sind alle Informationen, bei denen folgende Faktoren zu **katastrophalen Schäden** führen können:" (🗎 Kapitel 9.2)

Kritische Informationen

1. Unberechtigte Einsicht → Vertraulichkeit
2. Verfälschung →Integrität
3. Dauerhafter Verlust → Langzeitverfügbarkeit
4. Kurzzeitige Nichtverfügbarkeit → Unmittelbare Verfügbarkeit

Kritische Informationen

- "Um die kritischen Informationen zu ermitteln MÜSSEN die **zentralen Geschäftsprozesse** und die **Prozesse mit hohem Schadens-potential** untersucht werden […)"
  (🗎 Kapitel 9.2)

Kritische Informationen

- Vorsicht bei der Definition von **besonders schützenswerten Informationen!**
- Art und Umfang der Informationen berücksichtigen (🗎 Kapitel 9.2)
- Bsp.:
  - Kundendaten ↔ Kundendatenbank
  - Produkt In Entwicklung ↔ Produkt am Markt
  - Kleinprojekte ↔ Großprojekte

Kritische IT-Systeme, …

- "IT-Systeme, mobile Datenträger und Verbindungen sind kritisch, wenn sie kritische Informationen verarbeiten, speichern oder übertragen" (🗎 Kapitel 9.3)
- Unterstützende IT-Infrastruktur ist kritisch
- Bestimmung der **maximal tolerierbaren Ausfallzeit** (MTA)

Vergleich

Stärken

- Versicherungswirtschaft als "Treiber"
- Erfahrungen aus Schäden fließen ein
- Kompatibel mit anderen Standards
- Minimalisierter Aufwand
- Zertifizierung möglich

Schwächen

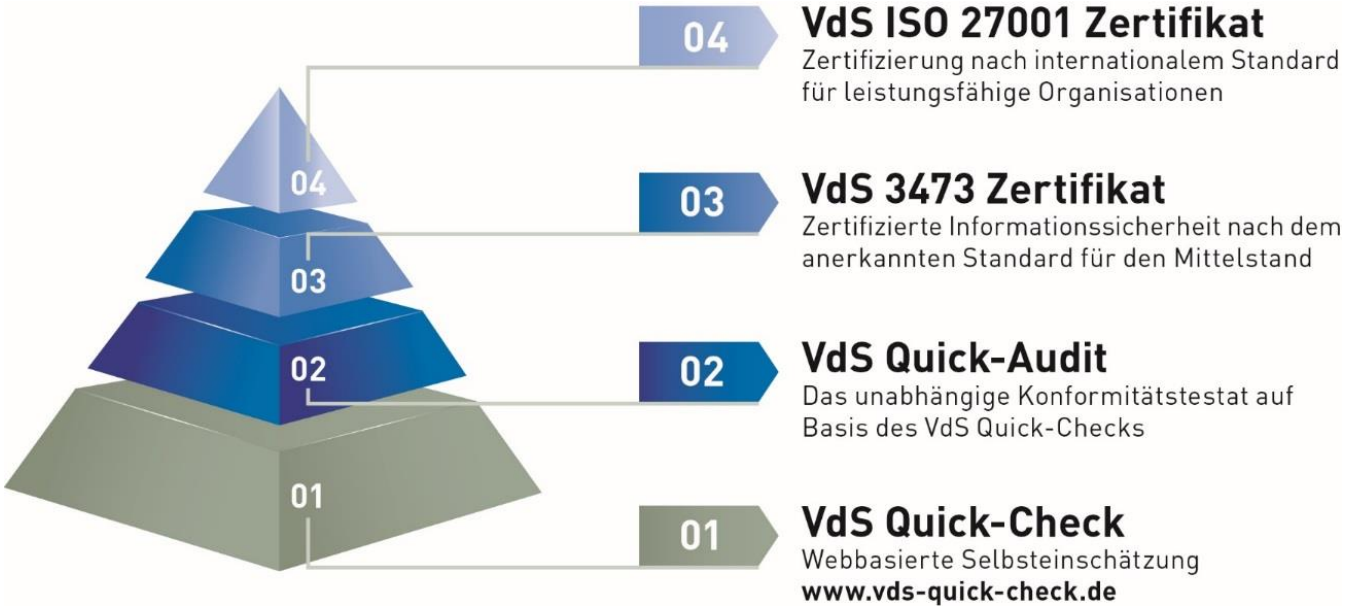
- Noch nicht international anerkannt (wir arbeiten daran!) Stand 03/2015: Englische und türkische Übersetzung
- Jung → wenig Praxiserfahrung
- Geringeres Sicherheitsniveau als ISO 27001 und BSI IT-Grundschutz (?)

Kompatibilität

- Verfahren aus etablierten Standards werden empfohlen (z.B. ISO 9001, BSI 100-X, …)
- Maßnahmen sind aufwärtskompatibel zu ISO 27001 und BSI IT-Grundschutz
- Aktuell: Mapping-Projekt VdS 3473 – ISO 27001: Bestimmung eines möglichen Upgrade-Pfades

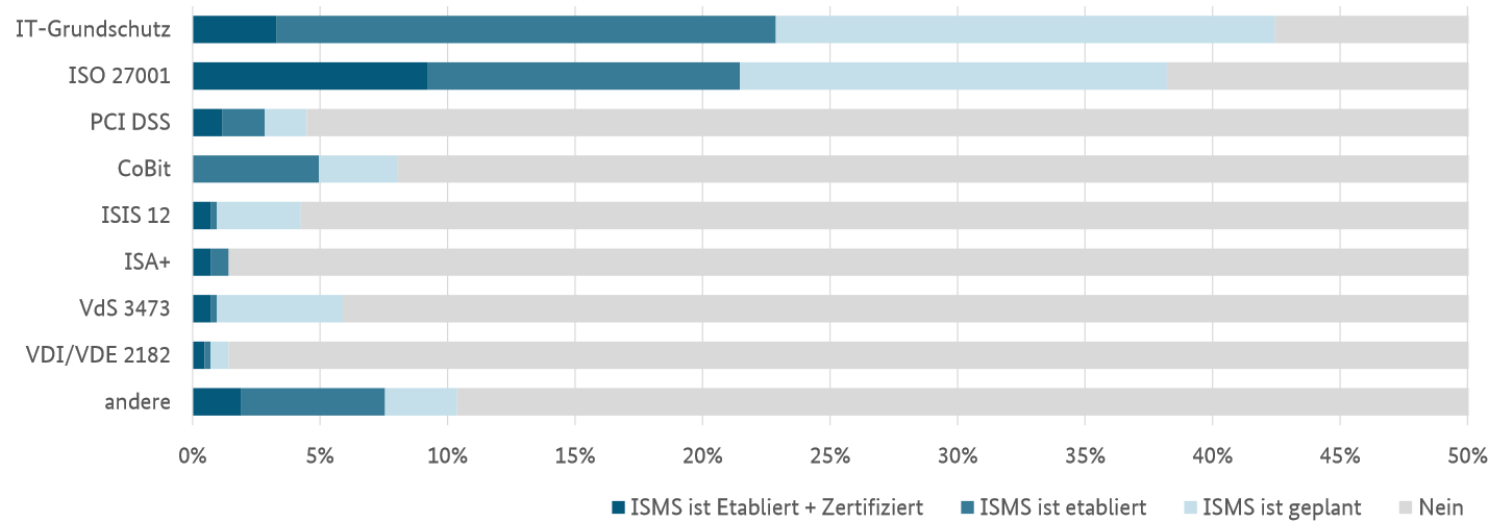
Zertifizierung

Zertifizierung



Zertifizierung

Wird in der jeweiligen Institution ein Managementsystem für Informationssicherheit (ISMS) betrieben?



Bundesamt für Sicherheit in der Informationstechnik

Frage 11 | Basis: n = 424, Mehrfachnennung möglich

Bundesamt für Sicherheit in der Informationstechnik | Ergebnisse der Cyber-Sicherheits-Umfrage 2015 | 05.10.2015 | Seite 29

Links

VdS Schadenverhütung GmbH
http://www.vds.de/cyber

Michael Wiesner GmbH
https://www.michael-wiesner.info

3473 Gurus GbR
https://www.3473-wiki.de