MICHAELWIESNER

VdS-Richtlinien 3473

Workshop zur LeetCon 2017

Michael Wiesner GmbH, 18.10.2017

Vorstellung

Michael Wiesner

- „Der Navigator für Informationssicherheit im Mittelstand“ seit 1994
- Berater, Auditor, Penetrationstester
- Co-Autor VdS-Richtlinien 3473 & 10010
- Lead Auditor ISO 27001 & VdS 3473, CISM, CRISC, T.I.S.P., OSCP, …

Agenda

- Einführung
- Erfahrungen
- Entwicklungen
- Q&A

Workshop:
Es darf mitgearbeitet werden!

Einführung

VdS 3473

- Cyber-Security für kleine und mittlere Unternehmen (KMU) 07/2015
- „für kleine und mittlere Unternehmen (KMU), den gehobenen Mittelstand, Verwaltungen, Verbände und sonstige Organisationen“
- Öffentlich und kostenfrei (www.vds.de/cyber/)
- 38 Seiten, davon 28 Seiten Anforderungen

Herkunft

VdS Schadenverhütung

- Gesamtverband der Deutschen Versicherungswirtschaft (GDV)
- VdS Schadenverhütung 100% Tochter
- „Technischer Arm“ der Versicherungswirtschaft

Herkunft

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

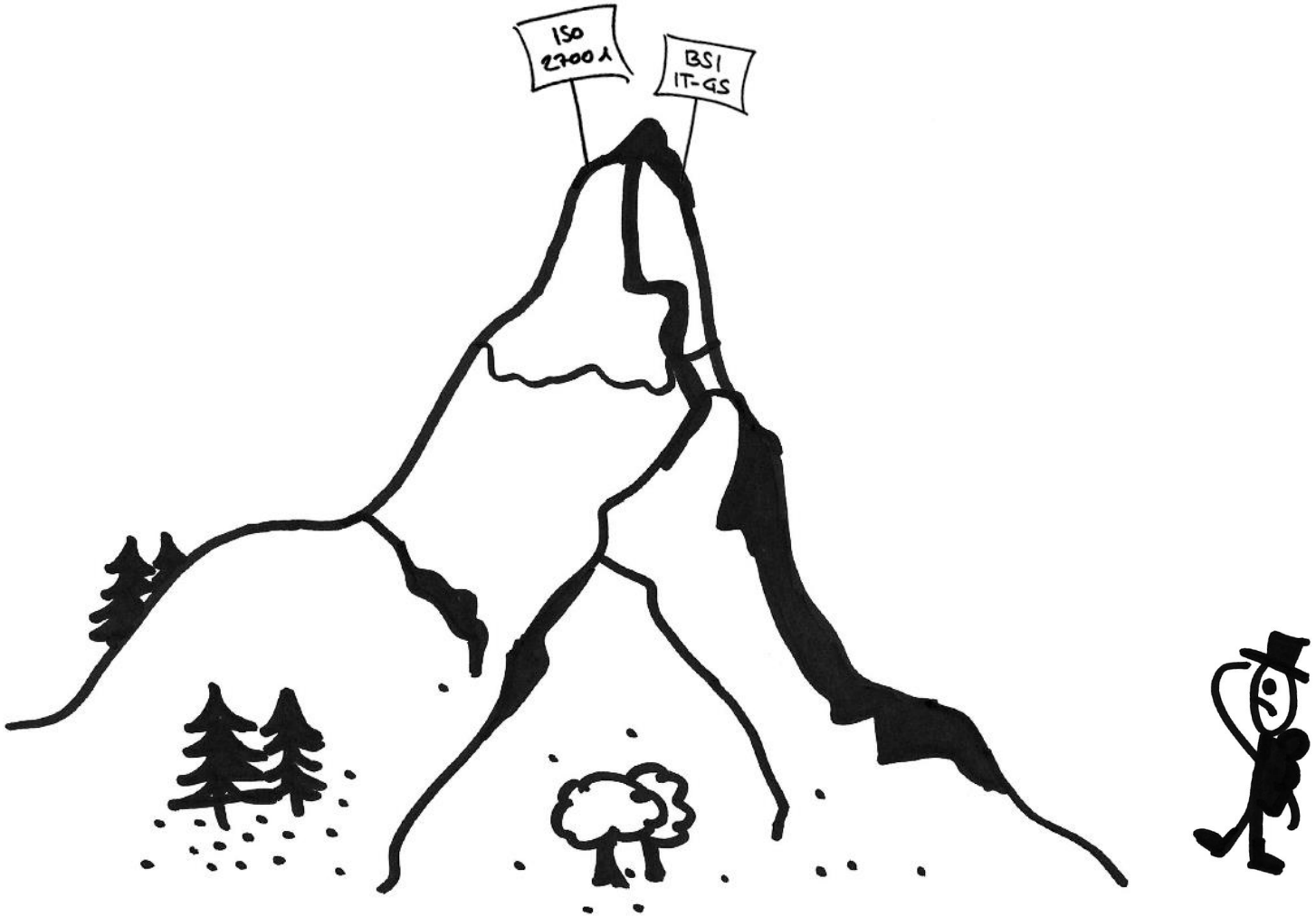
Herkunft

- 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?

Herkunft

- 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

Herkunft



Eigenschaften

- Informationssicherheitsmanagementsystem (ISMS)
- Verantwortlichkeiten, Leitlinie und Richtlinien zur Informationssicherheit
- Verfahren, Risikoanalyse und -behandlung
- Risikobasierte organisatorische und technische Maßnahmen (kritisch, unkritisch)
- Kontinuierlicher Verbesserungsprozess (KVP)

Eigenschaften

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

Eigenschaften

- Geltungsbereich: Komplette Informationsverarbeitung (am Standort)
- Organisatorische und technische Grundanforderungen
- Kritische und unkritische IT-Ressourcen
- Basisschutz für unkritische IT-Ressourcen
- Zusatzmaßnahmen für kritische IT-Ressourcen
- Risikoanalyse zur „Kompensation“

Stärken

- Versicherungswirtschaft als „Treiber“
- Erfahrungen aus Schäden fließen ein
- Minimalisierter Aufwand
  („so viel wie nötig, so wenig wie möglich“)
- Zertifizierungsfähig

Schwächen

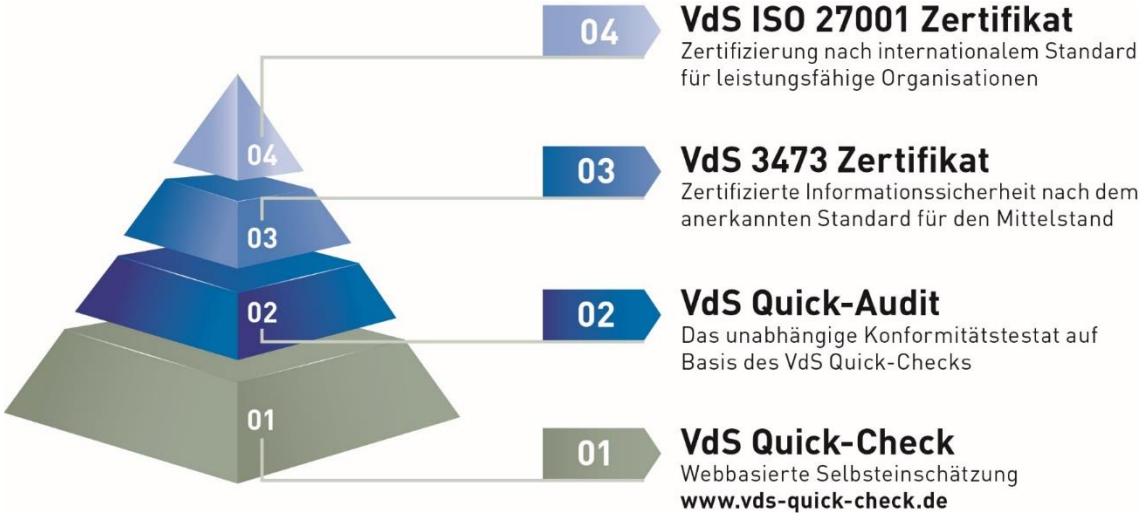
- ~~Sehr jung → wenig Praxiserfahrung~~
- Bekanntheitsgrad
- Geringeres Sicherheitsniveau als ISO 27001 und BSI IT-Grundschutz (?)

Kompatibilität

- Maßnahmen sind aufwärtskompatibel zu ISO 27001 und BSI IT-Grundschutz
- Verfahren aus etablierten Standards werden empfohlen (z.B. ISO 9001)

Kompatibilität

Zertifizierung



Quelle: VdS

Erfahrungen

Unternehmen

- Originär für kleine und mittlere Unternehmen <249/500 Beschäftige, <50 mio. Umsatz
- Funktioniert auch mit >5000 Beschäftigen, >50 mio. Umsatz und mehreren (int.) Standorten
- Wird als „Baseline“ genutzt und durch ergänzende Maßnahmen angepasst (z.B. bei Teilbereichen mit ISO 27001-Anforderung)

Branchen

- Produzierendes Gewerbe/ Industrie
- Anlagen- und Maschinenbau
- Banken- und Versicherungswirtschaft
- Ver- und Entsorgungsunternehmen
- Stadtverwaltungen, Gemeinden, Kommunen
- Transport & Logistik
- Gesundheitswesen
- …

Aufwände

Einführung

- 5 - 30 (externe) Beratertage zur Einführung
- 10 – 60 (interne) Personentage für ISB
- 1 - 18 Monate Umsetzungszeit
- Zusätzliche Aufwände bei größeren oder komplexen Unternehmen (z.B. zusätzliche Gremien, wie ISMT, Internationalisierung, …)

Aufwände

Betrieb

- 1 - 3 Personentage pro Monat für ISB
- 0,5 - 1 Personentag pro Monat für IST
- Zusätzliche Aufwände bei größeren oder komplexen Unternehmen (z.B. zusätzliche Gremien, wie ISMT, Internationalisierung, …)

Probleme

Fähigkeiten des Unternehmens

- Mangelndes Engagement des Topmanagements
- Unzureichende Fähigkeiten im Change- bzw. Projektmanagement
- Fehlende oder unzureichend wahrgenommene Verantwortlichkeiten
- Unzureichende Steuerung und Kommunikation von Dokumenten, Verfahren, etc.

Probleme

Fähigkeiten der Mitarbeiter

- Führungsschwäche bei Topmanagement oder Personalverantwortlichen
- Unzureichende kommunikative Kompetenz (insbesondere bei IT-Verantwortlichen oder (designierten) ISB)
- Mangelnde Fachkompetenz

Probleme

Herangehensweise

- Initialer Reifegrad wird zu hoch angesetzt
- Unreflektiertes Übernehmen von Templates
- Aufbau eines Paralleluniversums anstatt Integration in bestehende Abläufe
- Unzureichende Ressourcen (Tagesgeschäft)
- Unzureichende Beachtung interner (politischer) Gegebenheiten

Unterstützung

- VdS 3473 Wiki
  https://www.3473-wiki.de
- Gefährdungskataloge des BSI
  https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/Gefaehrdungskataloge/gefaehrdungskataloge_node.html
- Ishikawa-Diagramm
  https://de.wikipedia.org/wiki/Ursache-Wirkungs-Diagramm

Entwicklungen

Richtlinien

- Große Anerkennung und Akzeptanz bei Institutionen, Behörden, Verbänden, Unternehmen
- Basis für Leitfäden, Konzepte, Mini-ISMS (DSGVO)
- Integration in Umsetzungs-Tools (z.B. DocSetMinder, verinice)
- Große Anzahl von Implementierungsprojekten, aktuell noch wenige Zertifizierungen

VdS

- Leitfaden zur Interpretation und Umsetzung für industrielle Automatisierungssysteme
- Mapping-Projekt mit BSI IT-Grundschutz
- Synopse-Projekt VdS 3473 – ISO 27001
- VdS 10010 zur Umsetzung der DSGVO, basierend auf 3473-Struktur

Versicherer

- Musterbedingungen für Cyber-Versicherungen
- VdS 3473 (Quick-Audit oder Zertifizierung) teilweise Voraussetzung für Abschluss einer Cyber-Police
- Rabatte auf Cyber-Versicherungen bei vorhandener Zertifizierung

Ausblick

- Weitere Leitfäden zur Umsetzung (z.B. Gesundheitswesen, Kommunen)
- Revision und Überführung in 10000er-Reihe (2018?)
- Anerkannter Stand der Technik?

Q&A

Vielen Dank!

Michael Wiesner GmbH

Am Eichhölzchen 22

D-35708 Haiger

+49 (0) 2773 8132623 0

+49 (0) 2773 8132623 9

info@michael-wiesner.info