Kurzvorstellung der

VdS-Richtlinien 3473

„Cyber-Security für kleinere und mittlere Unternehmen (KMU)“

Copyright dieser Unterlagen

- Sie dürfen:
  - Das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten und zwar für beliebige Zwecke, sogar kommerziell.
  - Das Material beliebig bearbeiten, verändern und darauf aufbauen und zwar für beliebige Zwecke, sogar kommerziell.
- Dabei gelten die folgenden Bedingungen:
  - Sie müssen angemessene Urheber- und Rechteangaben machen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
  - Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie nicht mehr das Logo der VdS Schadenverhütung GmbH verwenden.
  - Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter dieser Lizenz verbreiten.

Um was geht es?

- Die VdS-Richtlinien 3473 definieren zertifizierbare Mindestanforderungen an die Informationssicherheit und sind speziell auf KMU zugeschnitten.
  Sie bieten genau das Schutzniveau, das kleine und mittlere Unternehmen benötigen, ohne sie finanziell oder organisatorisch zu überfordern.
- Diesen Unterlagen stellen die VdS 3473 kurz vor. Sie sollen Sie neugierig machen, die VdS 3473 zu lesen und mindestens Teilaspekte von ihr zu implementieren.

Die harten Fakten

- jung:
  - Erstveröffentlichung am 01.07.2015
  - erste Audits im November 2015
- kurz:
  - 38 Seiten, davon 11 Seiten Vorwort, Inhaltsverzeichnis und Glossar
- Herkunft Versicherungsbranche:
  - herausgegeben von der VdS Schadenverhütung GmbH
  - die VdS Schadenverhütung GmbH ist eine 100%ige Tochter des Gesamtverband der Deutschen Versicherungswirtschaft e.V. GDV
- Intention:
  - Versicherungsfähigkeit von Unternehmen/Institutionen in Bezug auf Cyber-Risiken festzustellen

Eigenschaften

- definiert ein vollständiges ISMS
  - Leitlinie, Richtlinien, Verfahren (ISO-Pyramide)
  - Informationssicherheitsbeauftragter (ISB) und Informationssicherheitsteam (IST)
  - kontinuierlicher Verbesserungsprozess (KVP)
  - berücksichtigt organisatorische und technische Maßnahmen
- Fokus: einfache, schnelle Implementierung
  - sehr eindeutige Sprache (MUSS/DARF NICHT/SOLLTE/SOLLTE NICHT/KANN)
  - minimalisierter Analyse- und Dokumentationsaufwand
- Definition von Zielen anstelle von Maßnahmen
  - möglichst große Freiheit bei der Implementation
- geringeres Schutzniveau als ISO bzw. BSI GS

Let's take a closer look...

- Scope/Anwendungsbereich: kann frei definiert werden
- IT-Ressourcen werden nur in "kritisch" und "alle“ unterschieden
- kritische IT-Ressourcen müssen vom Unternehmen ermittelt werden
- für alle Ressourcen wird ein einfacher Basisschutz definiert (Minimalprinzip)
  - die Maßnahmen des Basisschutzes müssen nur umgesetzt werden, sofern dies technisch möglich ist
  - wenn Maßnahmen nicht umgesetzt werden obwohl dies möglich wäre, muss das Unternehmen eine entsprechende Risikoanalyse und -behandlung durchführen
- für kritische Ressourcen werden erweiterte Maßnahmen gefordert
  - zusätzliche technische und organisatorische Maßnahmen
  - individuelle Risikoanalyse und -behandlung

Etablieren der VdS 3473

Phasen	Einzelschritte zur Einführung ISMS
Organisation der Informationssicherheit	• Festlegung von Verantwortlichkeiten, Bereitstellung von Ressourcen, Ernennung Informationssicherheitsbeauftragten, Etablieren des Informationssicherheitsteams • Erstellung der Informationssicherheitsleitlinie • Erstellung von Richtlinien zur Informationssicherheit
Identifikation von kritischen IT-Ressourcen	• Identifikation zentraler Geschäftsprozesse und Prozesse mit hohem Schadenspotential • Identifikation besonders schützenswerter Informationen • Identifikation der kritischen IT-Systeme, mobile Datenträger und Verbindungen sowie weiteren kritischen Teilen der IT-Infrastruktur
Implementierung des Basisschutzes	• Implementierung einfacher Maßnahmen, z. B. Updates, Beschränkung des Netzwerkverkehrs, Protokollierung, …
Implementierung Maßnahmen für kritische IT-Ressourcen (falls vorhanden)	• individuelle Risikoanalyse und -behandlung • Umsetzung von erhöhten Anforderungen an die Datensicherung, Robustheit

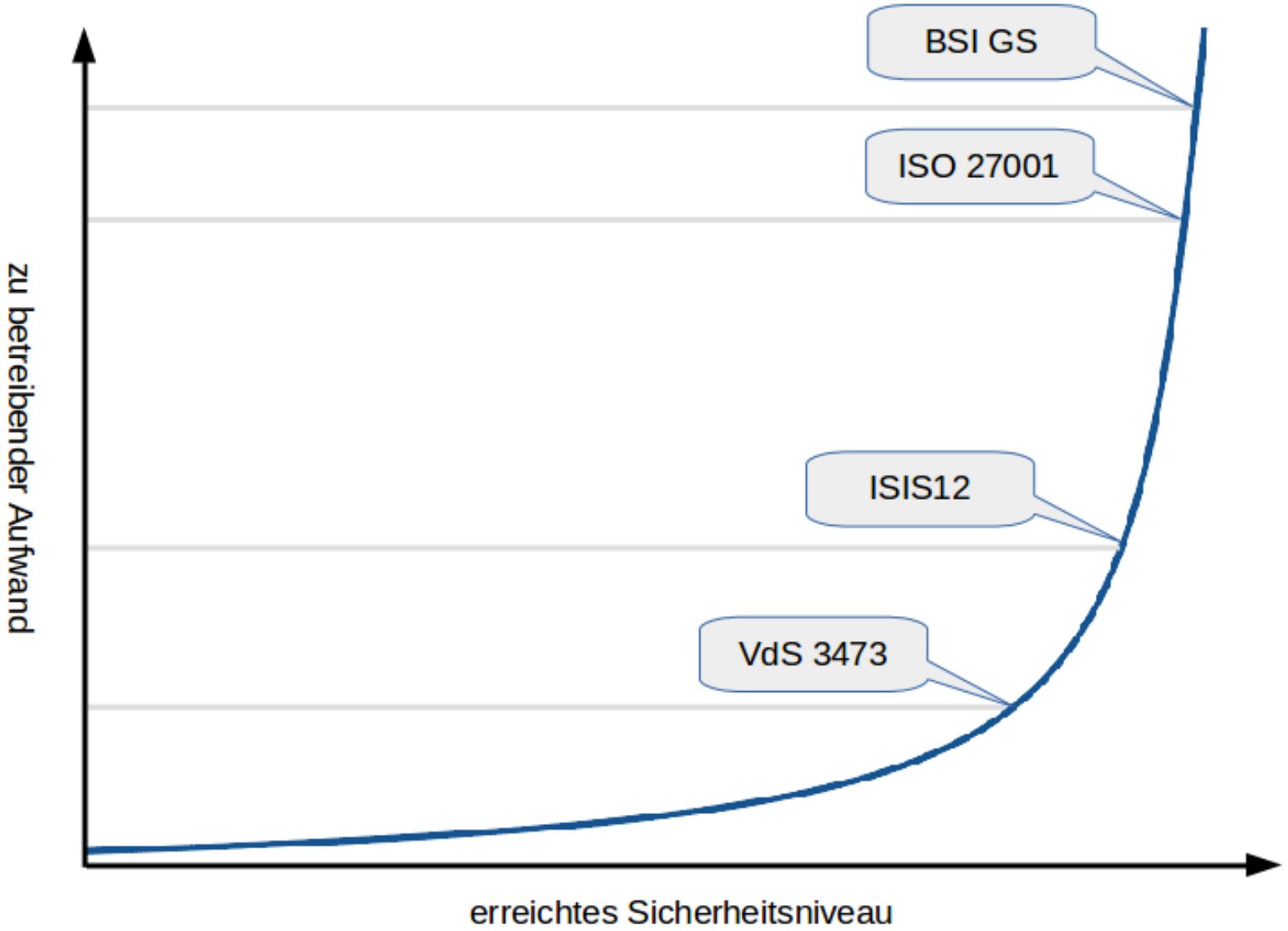
Kompatibilität!

- die Umsetzung der "großen" Normen wird an vielen Stellen der VdS 3473 explizit empfohlen
- wenn sich das Unternehmen sie die „großen“ Normen entscheidet, wird zumindest die Umsetzung einiger weniger Kernaspekte dieser Normen gefordert
- Maßnahmen sind aufwärtskompatibel zu ISO 27001 und den BSI Grundschutznormen

"Die 3473 ist das erste Basislager
für den Gipfelsturm zur ISO 27001."

Mark Semmler, Projektleiter der VdS 3473

Sicherheit vs. Aufwand (eine grobe Orientierung)



VdS 3473: Stärken und Schwächen

Standard	Stärken	Schwächen
VdS 3473	• für KMU konzipiert • kann für die Versicherungswirtschaft als Basis für die Bewertung von Risiken herangezogen werden • kann die Basis für den individuellen Versicherungsschutz sein • Knowhow aus Schäden können unmittelbar in die Aktualisierung des Standards einfließen • kompatibel mit den anderen Standards (Einstieg) • konkret auditierbare Vorgaben • minimalisierter Aufwand	• Standard ist aktuell nicht international anerkannt • Standard ist noch sehr jung (nicht flächendeckend eingeführt) • geringeres Sicherheits-niveau als ISO 27001 oder BSI GS durch minimalisierte Analyse und Dokumentation

VdS 3473: hier kostenfrei verfügbar

http://vds.de/fileadmin/vds_publikationen/vds_3473_web.pdf

Umsetzungshilfen im WWW

- Webseite verfügbar mit umfangreichen Hilfestellungen für die Implementierung:
  - ausführliche Kommentierung der Maßnahmen und Empfehlungen
  - Vorlagen für die Erstellung der Leitlinie, der Richtlinien und Verfahren
  - Hintergrundartikeln z. B. zu Risikoanalysen und Konzepten
  - Empfehlungen für die Vorgehensweise und das Projektmanagement

https://www.3473-wiki.de