IT-Sicherheitsrechtstag 2017

Gemeinsame Veranstaltung von TeleTrusT und BvD

Berlin, 07.11.2017

Maßnahmenermittlung nach dem Stand der Technik

Methodischer Ansatz zur Bestimmung des Technologiestands von technischen und organisatorischen Maßnahmen

Tomasz Lawicki

The Auditing Company

Sachverständigen-Sozietät Dr. Schwerhoff

Leitfragen des Vortrags

Warum ist "Stand der Technik" wichtig?

Was ist "Stand der Technik"?

Wie lässt sich der "Stand der Technik" bestimmen?

Wie lässt sich der "Stand der Technik" von anderen Technologieständen abgrenzen?

Motivation

Gesetzliche Vorgaben

DSGVO, IT-SiG, NIS-RL (Auszüge)

BSIG, §8a, Abs. 1 : "Betreiber kritischer Infrastrukturen sind verpflichtet... organisatorische und technische Vorkehrungen…zu treffen… Dabei soll der Stand der Technik eingehalten werden.

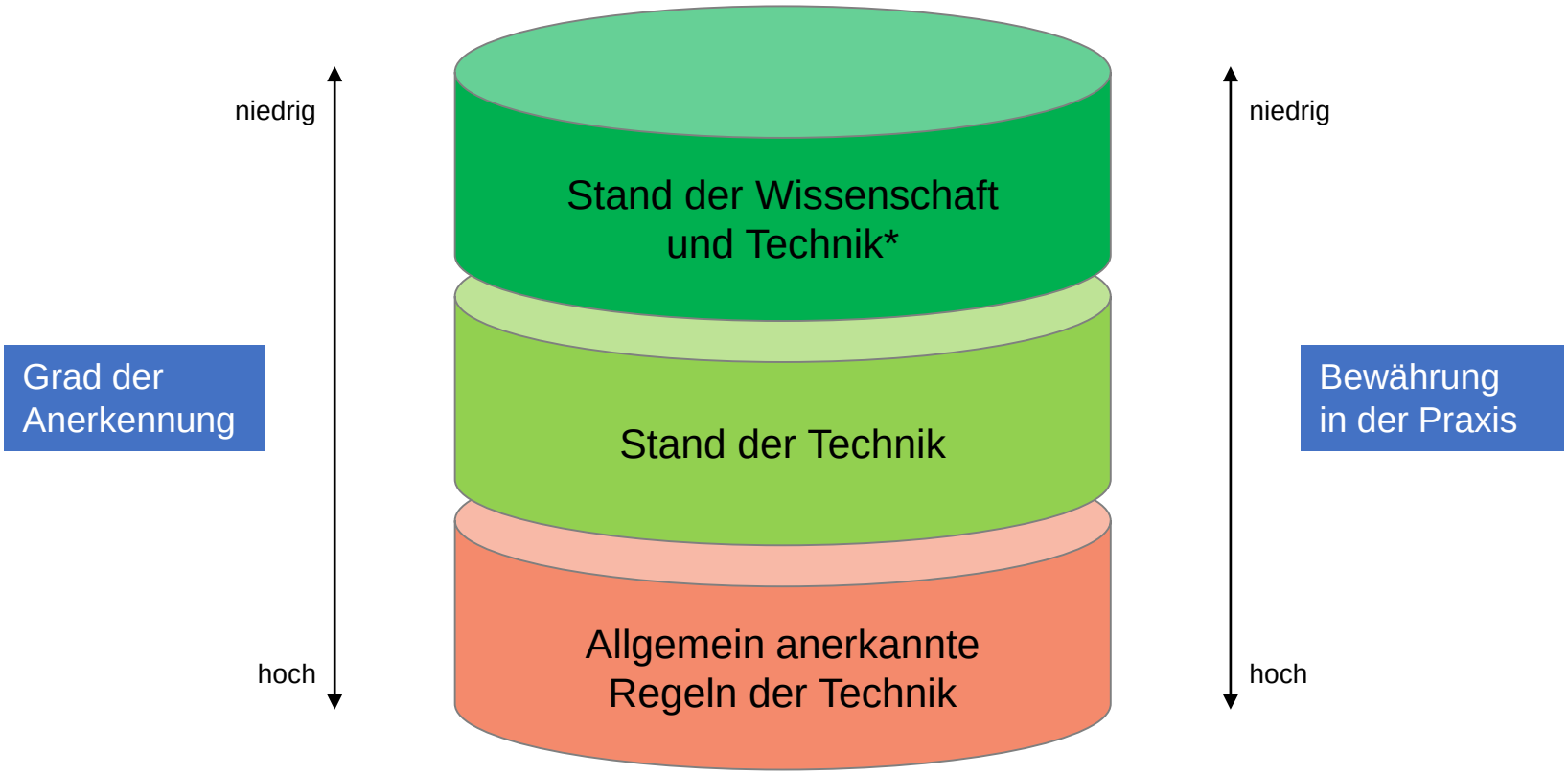
TMG, §13, Abs. 7 : "Diensteanbieter haben… sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist… Vorkehrungen… müssen den Stand der Technik berücksichtigen".

NIS-RL, Art 15: "…Diese Maßnahmen müssen unter Berücksichtigung des Stands der Technik ein Sicherheits-niveau der Netz- und Informationssysteme gewährleisten."

DSGVO, Art. 32, Sicherheit der Verarbeitung: "Unter Berücksichtigung des Stands der Technik … treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Sicherheitsmaßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; …"

Drei-Stufen-Modell der Technologiestände

In Anlehnung an Kalkar-Entscheidung



* auch als "Stand der Wissenschaft und Forschung" bezeichnet

Quelle: BVerfG, Beschluss vom 8. August 1978 – 2 BvL 8/77

Definitionen der Technologiestände

BMJ, Handbuch der Rechtförmlichkeit

Allgemein anerkannte Regeln der Technik sind schriftlich fixierte oder mündlich überlieferte technische Festlegungen für Verfahren, Einrichtungen und Betriebsweisen, die nach herrschender Auffassung der beteiligten Kreise (Fachleute, Anwender, Verbraucherinnen und Verbraucher und öffentliche Hand) geeignet sind, das gesetzlich vorgegebene Ziel zu erreichen und die sich in der Praxis allgemein bewährt haben oder deren Bewährung nach herrschender Auffassung in überschaubarer Zeit bevorsteht.

Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen und Betriebsweisen, der nach herrschender Auffassung führender Fachleute das Erreichen des gesetzlich vorgegebenen Zieles gesichert erscheinen lässt. Verfahren, Einrichtungen und Betriebsweisen oder vergleichbare Verfahren, Einrichtungen und Betriebsweisen müssen sich in der Praxis bewährt haben oder sollten – wenn dies noch nicht der Fall ist – möglichst im Betrieb mit Erfolg erprobt worden sein.

Stand von Wissenschaft und Technik umschreibt das höchste Anforderungsniveau und wird daher in Fällen mit sehr hohem Gefährdungspotenzial verwendet. Stand von Wissenschaft und Technik ist der Entwicklungsstand fortschrittlichster Verfahren, Einrichtungen und Betriebsweisen, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlich vertretbarer Erkenntnisse im Hinblick auf das gesetzlich vorgegebene Ziel für erforderlich gehalten werden und das Erreichen dieses Ziels gesichert erscheinen lassen.

Quelle: Bundesministerium für Justiz und Verbraucherschutz, Handbuch der Rechtsförmlichkeit, http://hdr.bmj.de/page_b.4.html

Motivation

Einhaltung oder mindestens Berücksichtigung des "Stands der Technik" von Maßnahmen ist gesetzlich verankert.

aber

- "Stand der Technik" ist keine direkt messbare Größe.
- Festgeschriebene Standards neigen zum "Altern" und sind nicht zwingend dem "Stand der Technik" gleichzusetzen.
- Technologiestände werden oft unzutreffend synonym verwendet.

RISIKEN

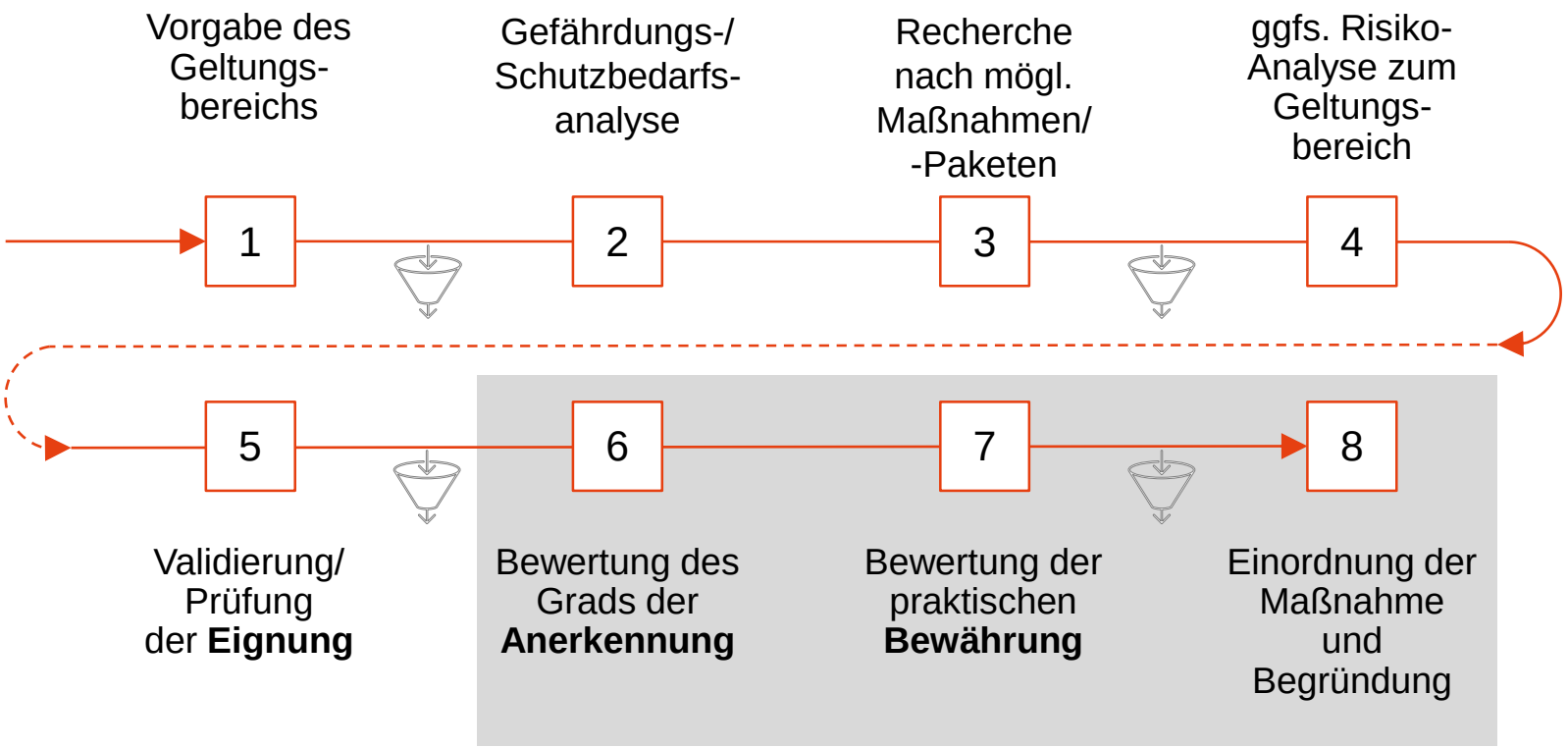
- Verfehlung der Nachweispflicht durch Unternehmen
- Interpretationsspielraum für Aufsichtsbehörde(n) und Judikative
- Bußgelder bei Zuwiderhandlungen und Verstoß gegen die gesetzlichen Auflagen

Der "Stand der Technik" von TOMs muss anhand einer Methode bestimmt sein, die die Vergleichbarkeit der Ergebnisse ermöglicht.

Methode

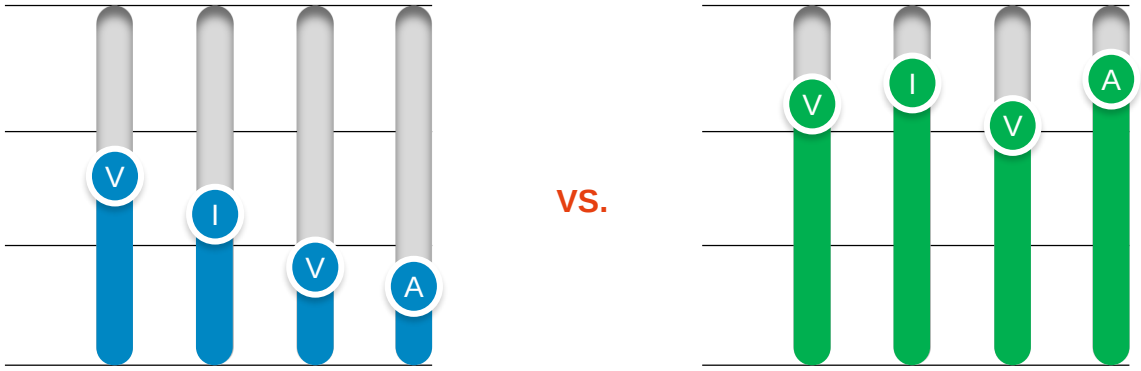
Bestimmung des Technologiestands

Allgemeine Vorgehensweise



Bestimmung des Technologiestands

Validierung der Eignung



Bewertung vor der Umsetzung **Bewertung nach der Umsetzung**

Die Eignung kann angenommen werden, wenn die Maßnahme oder das Maßnahmen-bündel eine positive Wirkung auf die Schutzziele (Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit) im Hinblick auf die zu schützenden Unternehmenswerte hat.

++	Maßnahme verbessert die Berücksichtigung des Schutzziels
+	Maßnahme sorgt für erstmalige Berücksichtigung des Schutzziels
o	Keine Veränderung
-	Maßnahme verschlechtert den Schutz
--	Maßnahme führt zu Verlust des Schutzziels

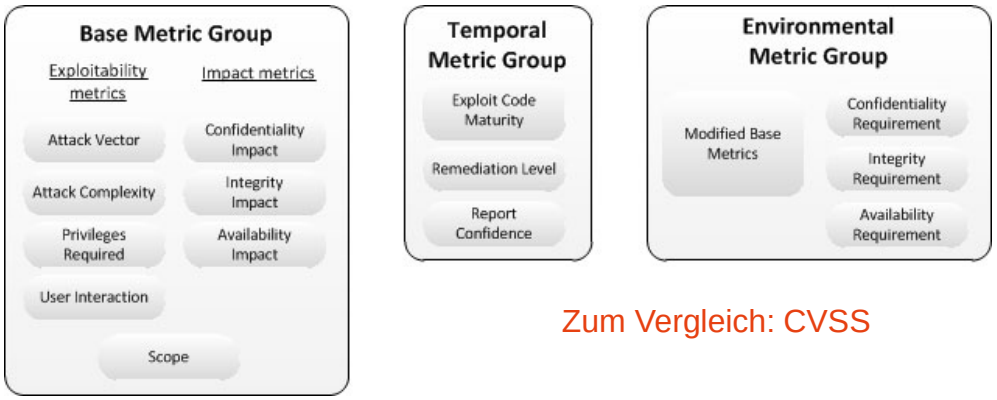
Bestimmung des Technologiestands

Validierung der Eignung in Anlehnung an CVSS

Ein Vergleich eines "Security Sensitivity Score" vor und nach Umsetzung einer Maßnahme ermöglicht eine Aussage zur "Eignung" einer Maßnahme im Hinblick auf die Reduzierung einer Bedrohung.

Als Grundlage für den Score könnte das Common Vulnerability Scoring System (übersetzt: "Allgemeines Verwundbarkeits-bewertungssystem", CVSS) als genutzt werden.

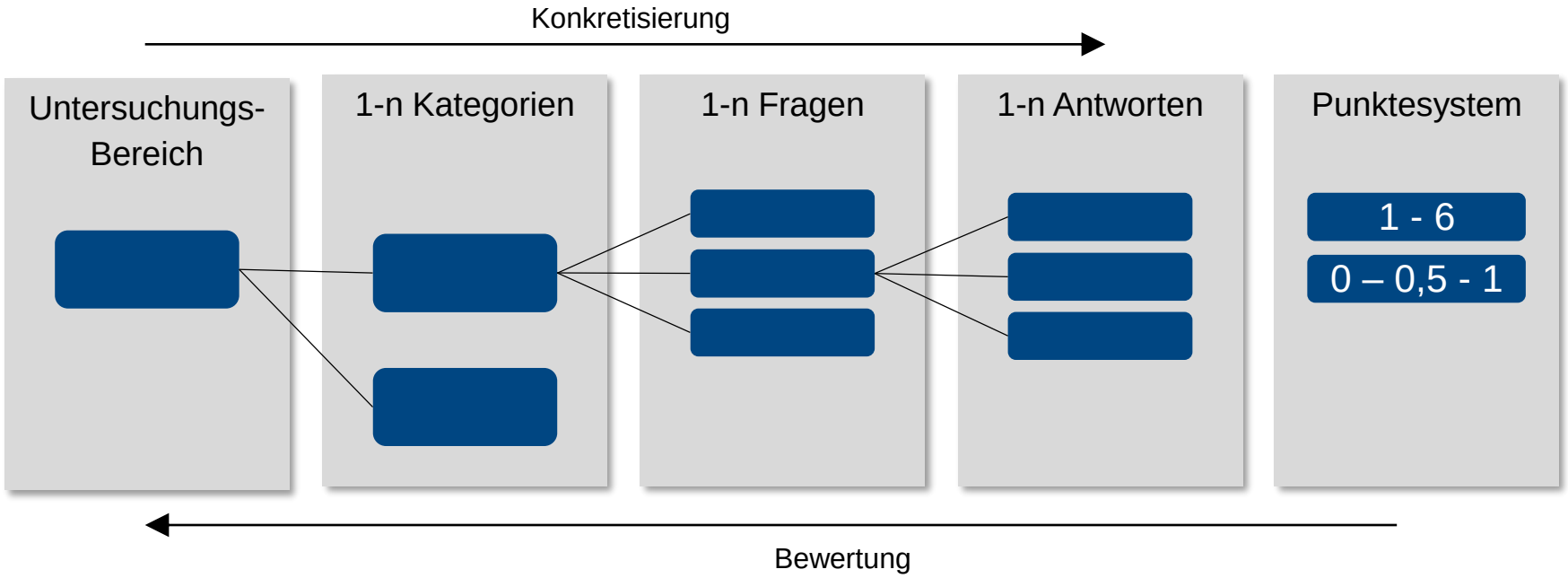
Gewichtung des Schutzziels 1=nicht wichtig 2=normal 3=sehr wichtig		
Basis	**Zeitlich**	**Umgebung**
Möglicher Verlust des Schutzziels 0=kein 1=teilweise 3=vollständig	Bekanntheit 1=Unbestätigte Möglichkeit 2=Bestätigte Möglichkeit 3=Bereits vorher eingetreten	Betroffene Umgebung 0= Effektiv ist 0% der Umwelt gefährdet. 1= Zwischen 1% - 25% der Gesamtumgebung ist gefährdet. 2=Zwischen 26% - 75% der Gesamtumgebung ist gefährdet. 3= Zwischen 76% - 100% der Gesamtumgebung ist gefährdet.
Schadenshöhe bei Verlust 0= keine Auswirkung 1= normal (spürbare Auswirkungen) 2= hoch (erhebliche Auswirkungen) 3= sehr hoch (existentiell bedrohlich)		
Wahrscheinlichkeit eines Verlusts 0=ausgeschlossen; 1=sehr selten (alle paar Jahrzehnte) 2=selten (alle paar Jahre) 3=häufig (mehrmals jährlich möglich)		



Zum Vergleich: CVSS

Bewertung des Technologiestands

Methodischer Ansatz für Bewertung der Anerkennung und Bewährung



Beispiel

Bewährung in der Praxis

Generations-ebene

In welchem Entwicklungsstadium befindet sich die Maßnahme?

- PoC 1 Pkt
- erste Version 2 Pkt
- Nachfolgeversion 3 Pkt
- eol 4 Pkt

Bestimmung des Technologiestands

Beispiel aus dem Arbeitskreis "Stand der Technik"

2.1 Fragen zum Grad der Anerkennung

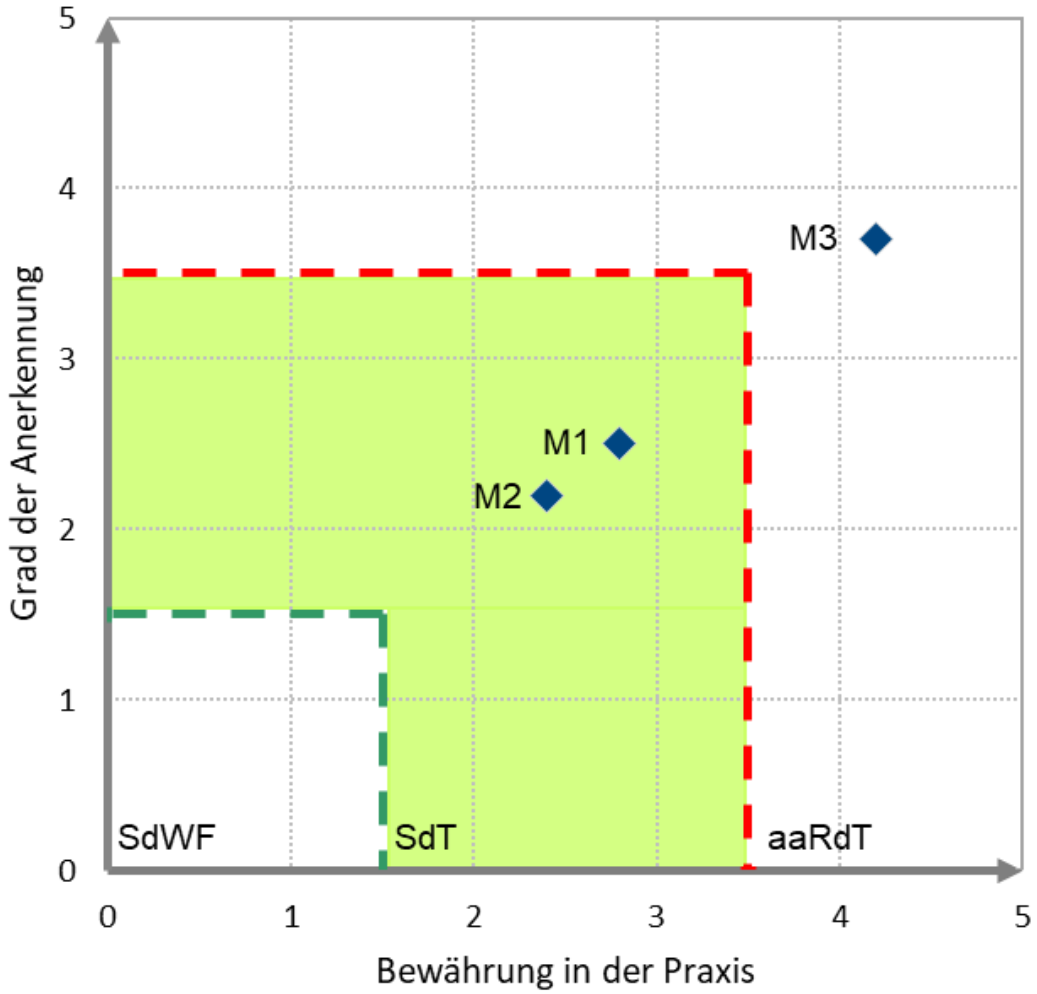
			Bewertung vom Ak SdT auszufüllen.		
1) Welche Dokumentation über die Maßnahme steht öffentlich zur Verfügung? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*					
☐ wiss. Publikation	☐ Fachmedien	☐ Massenmedien	*1*	*3*	*5*
[bitte begründen Sie Ihre Antwort hier]					
2) Nimmt die Maßnahme Bezug auf internationale oder nationale Normen? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*					
☐ nein, noch nicht normiert	☐ ja, eine	☐			
[bitte begründen Sie Ihre Antwort hier]					
3) Wurde die Maßnahme von anerkannten Gremien / Ve *bitte beantworten Sie die Frage, indem Sie die u.a. Käst*					
☐ nein	☐ ja, führenden	☐			
[bitte begründen Sie Ihre Antwort hier]					
4) Wird die Eignung der Maßnahme regelmäßig überpr *bitte beantworten Sie die Frage, indem Sie die u.a. Käst*					
☐ nein	☐ ja, herstellerseitig	☐			
[bitte begründen Sie Ihre Antwort hier]					

2.2 Fragen zur Bewährung in der Praxis

			Bewertung vom Ak SdT auszufüllen.		
1) Wie ist der Innovationsgrad der Maßnahme einzustufen? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*					
☐ hoch	☐ mittel	☐ gering	*1*	*3*	*5*
[bitte begründen Sie Ihre Antwort hier]					
2) Wo wurde die aktuelle Version der Maßnahme erprobt? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*					
☐ Laborbedingungen	☐ professioneller Einsatz	☐ Massenmarkt	1	3	5
[bitte begründen Sie Ihre Antwort hier]					
3) Existieren vergleichbare Maßnahmen am Markt? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*					
☐ nein	☐ wenige	☐ viele	1	3	5
[bitte begründen Sie Ihre Antwort hier]					
4) Wie oft wird die Maßnahme herstellerseitig konzeptionell aktualisiert? *bitte beantworten Sie die Frage, indem Sie die u.a. Kästchen ankreuzen*					
☐ häufiger als 1/Jahr	☐ jährlich	☐ seltener	1	3	5
[bitte begründen Sie Ihre Antwort hier]					
			Durchschnitt		

Bestimmung des Technologiestands

Einordnung der Maßnahme



Bestimmung des Technologiestands

Dokumentation der Ergebnisse

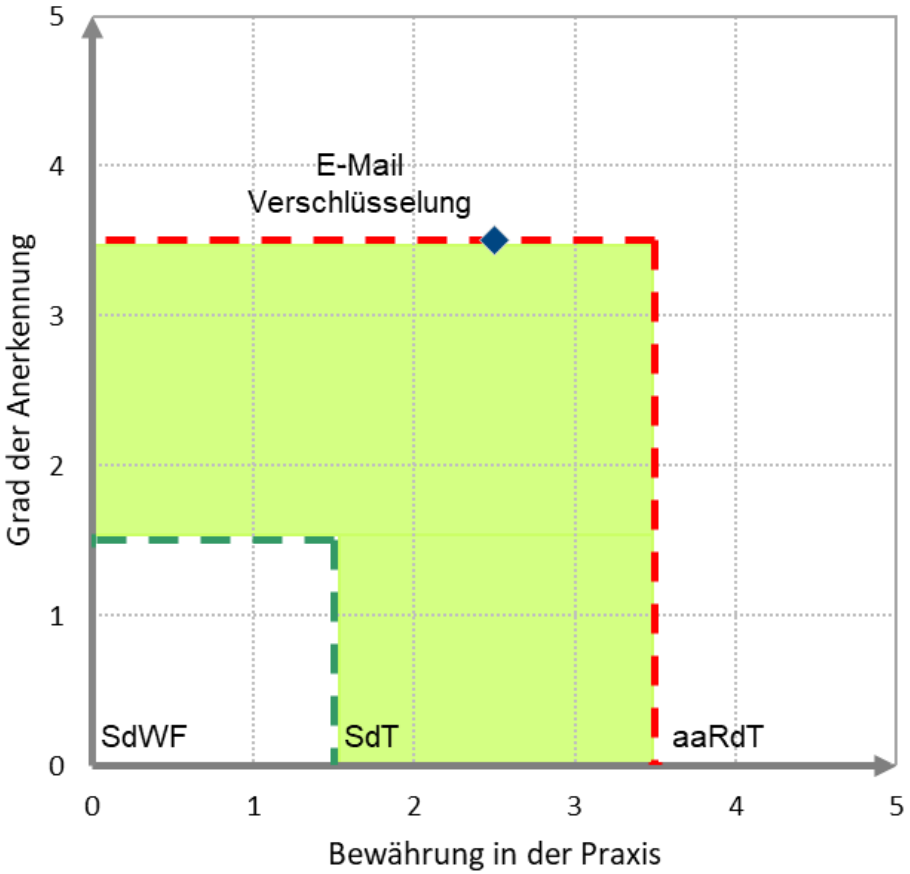
Laufende Nummer		Zu schützende Information / System						
		Größe des Betroffenenkreises - Einzelne Mitarbeitergruppe - Gesamtes Unternehmen - Außenstehende (z.B. Kunden)						
Maßnahmenbeschreibung/ Beurteilungskriterien		**Eigene Maßnahme** Kurzbeschreibung	**Branchenübliche Maßnahmen**			**Branchenübergreifende Maßnahmen**		
			Maßnahme ÜB1 Kurzbeschreibung	**Maßnahme ÜB2** Kurzbeschreibung	**Maßnahme ÜB3** Kurzbeschreibung	**Maßnahme ÜG1** Kurzbeschreibung	**Maßnahme ÜG2** Kurzbeschreibung	**Maßnahme ÜG3** Kurzbeschreibung
Kategorisierung	Verfahren - Technische Lösung - Prozess							
	Einrichtung - Institutionell - Personell							
	Betriebsweise - Einzweck/Mehrzweck - Konkret/Übergreifend - Kontinuierlich/Periodisch - Automatisch/Manuell							
Bewertung	Anerkennung der Maßnahme Reifegrad gem. Kriterien							
	Bewährung der Maßnahme Reifegrad gem. Kriterien							
	Eignung ++ Verbesserung + Erst-Schutz o Keine Änderung - Verschlechterung -- Verlust							
	Erforderlich Ja/Nein							
	Angemessen Ja/Nein							
Stand der Technik Ja/Nein								
Begründung								

Beispiele

Bestimmung des Technologiestands

Beispiel: Bewertung der Maßnahme "E-Mail-Verschlüsselung" im Arbeitskreis "Stand der Technik"

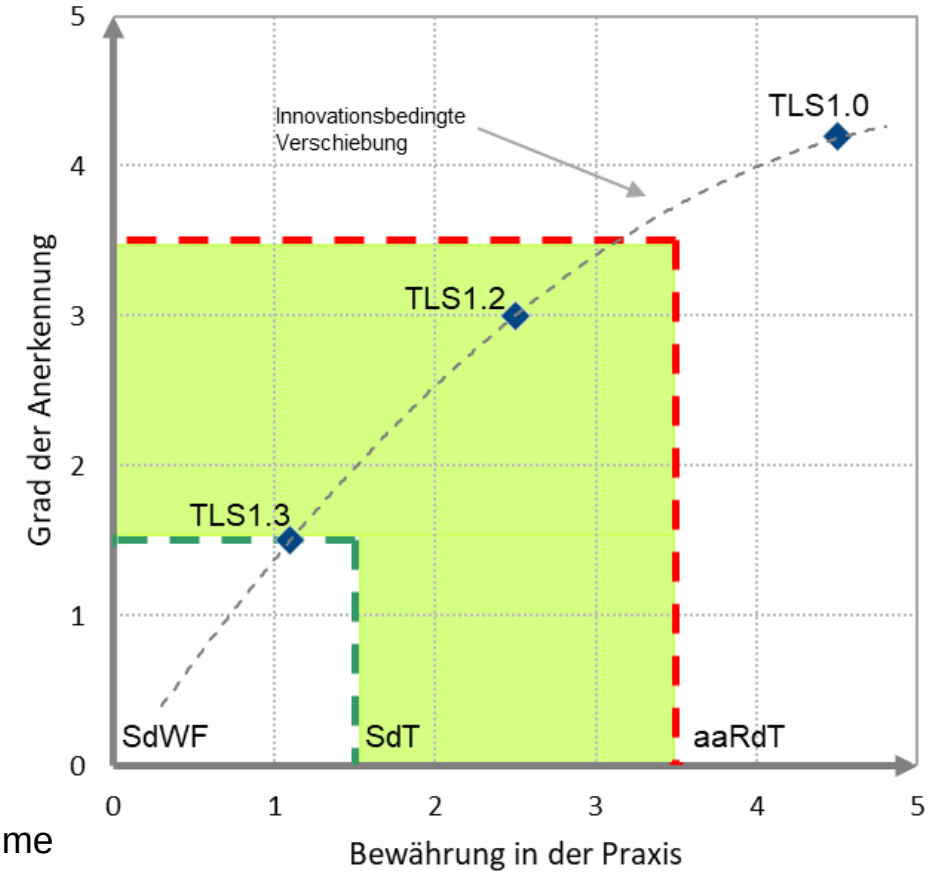
Geschäftliche E-Mails enthalten oft wichtige und schützenswerte Daten, zudem sind in der Regel schon E-Mail-Adressen personalisiert und E-Mails damit regelmäßig personenbezogene Daten, die gegen unbefugte Einsichtnahme oder Veränderung zu schützen sind. Die Schutzziele können generell durch Verschlüsselung der Übertragung von E-Mails und oder von E-Mail-Inhalten erreicht werden.



Bestimmung des Technologiestands

Beispiel: Verschlüsselung beim Aufruf von Internetseiten mit Transport Layer Security (TLS)

	TLS 1.0	TLS 1.2	TLS 1.3
Eignung	o	+	++
Grad der Anerkennung	4,2	3,0	1,5
Bewährung in der Praxis	4,5	2,5	1,1



Werden verschiedene Versionen einer Maßnahme miteinander verglichen, so lässt sich der Wechsel ihrer Technologiestände beobachten. (innovationsbedingte Verschiebung)


The
END

Vielen Dank !

TOMASZ LAWICKI

Associated Senior Auditor

The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff
Pickhuben 6,
D-20457 Hamburg

T: +49 40 37702-792
M: +49 151 177 14 217
E: lawicki@schwerhoff.com