Patrick Michaelis

Der „Stand der Technik“ im Kontext regulatorischer Anforderungen

Das IT-Sicherheitsgesetz (ITSiG) verpflichtet eine Reihe von Unternehmen, bei der Umsetzung von Sicherheitsmaßnahmen den jeweiligen „Stand der Technik“ einzuhalten. Für die betroffenen Unternehmen bedeutet dies, dass sie im Falle einer Nachweispflicht darlegen müssen, dass ihre Maßnahmen den Anforderungen des Gesetzes genügen und die Zuweisung zu der Generalklausel „Stand der Technik“ rechtfertigen. In diesem Beitrag wird eine Methodik für die Bestimmung des „Stands der Technik“ von IT-Sicherheitsmaßnahmen aus vorhandenen Überlegungen anderer Fachrichtungen abgeleitet.

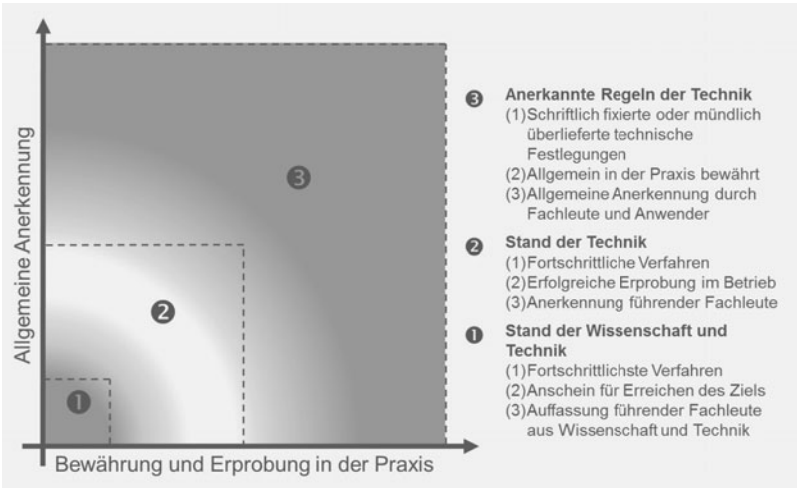
1 Einleitung

Informationssicherheit ist nicht nur durch Angriffe Dritter, durch Ausfälle und unzureichendes Design gefährdet, sondern gleichermaßen auch durch Unwissenheit, Beliebigkeit und Trägheit von Mitarbeitern und Organisationen.

Einen Ausweg aus der Problematik eröffnet das IT-Sicherheitsgesetz (ITSiG) durch regulatorische Vorgaben. Bestimmte Anforderungen an technische und organisatorische Maßnahmen, dem Nachweis dienende Dokumentationen sowie Bußgelder sollen helfen, die Bereitschaft innerhalb der Unternehmen für Verbesserungen der Informationssicherheit zu erhöhen.

Zur Sicherstellung eines hohen Schutzniveaus fordert das ITSiG je nach Branche die Einhaltung oder zumindest die Berücksichtigung des „Stands der Technik“. Der „Stand der Technik“ ist dabei keine unmittelbar messbare Größe. Der Begriff dient im Kontext des ITSiG vielmehr als Grundlage für die Festlegung beabsichtigter Maßnahmen und deren branchenspezifische Präzisierung.

Abbildung 1 | Schema zur Zuweisung der Generalklauseln



2 Generalklauseln und ihre Einordnung

Als unbestimmter Rechtsbegriff gliedert sich der „Stand der Technik“ in den Kanon der Generalklauseln zwischen den „allgemein anerkannten Regeln der Technik“ und dem „Stand der Wissenschaft und Technik“ ein. Der Übergang zwischen den einzelnen Regeln und Standards ist dabei erfahrungsgemäß fließend, was einen Unsicherheitsfaktor für alle einschlägigen Planungen darstellt. Im Interesse der vom ITSiG betroffenen Unternehmen ist diesem Umstand sachgerecht zu begegnen.

Folgt man der Definition im Handbuch der Rechtsförmlichkeit des BMVJ[1] in Verbindung mit der DIN EN 45020[2] („Normung und damit zusammenhängende Tätigkeiten – Allgemeine Begriffe“), so erfolgt die Zuweisung einer Maßnahme zu einer der Generalklauseln, basierend auf den jeweils vorhandenen Erkenntnissen und Erfahrungen zu den beabsichtigten Sicherheitsmaß-

Patrick Michaelis, CISSP®, CSSLP®

Principal bei The Auditing Company, Sachverständigen-Sozietät Dr. Schwerhoff. und fachlich verantwortlich für den Bereich Informationssicherheit.

E-Mail: michaelis@schwerhoff.com

1 BMJV, „Handbuch der Rechtsförmlichkeit“, 3. Aufl. Seite 84 ff

2 Siehe u.a. http://fachinfo.bistech.de/pdf/727/Begriffe+der+Normung

nahmen. Eine Maßnahme kann sich je nach ihrer Verbreitung und Verfügbarkeit vom „Stand der Wissenschaft und Technik“ zum „Stand der Technik“ wandeln oder vom jeweiligen „Stand der Technik“ übergehen in die Klausel „allgemein anerkannte Regeln der Technik“.

Unter die „anerkannten Regeln der Technik“ fallen solche Maßnahmen, die sich bewährt und durchgesetzt haben und die schon „*von der Mehrheit repräsentativer Fachleute als Wiedergabe des Standes der Technik angesehen werden*“. Dagegen ist der „Stand der Technik“ nach DIN EN 45020 als ein zu einem bestimmten Zeitpunkt bewährtes und in der Praxis erprobtes Stadium von Maßnahmen, die auf „*den diesbezüglichen gesicherten Erkenntnissen von Wissenschaft, Technik und Erfahrung*“ basieren, anzusehen.

Maßnahmen können also von einer Generalklausel in eine andere übergehen, sobald die spezifische Anerkennung im Markt und die Bewährung in der Praxis steigen. Je geringer das notwendige Expertenwissen ist, um eine Maßnahme zu verstehen und je größer die Verbreitung und Verfügbarkeit ist, desto eher wird davon auszugehen sein, dass es sich bei der Maßnahme um eine „anerkannte Regel der Technik“ handelt. Man sieht, bei der Zuweisung einer der Generalklauseln ist Vorsicht geboten.

In der Literatur (und in der gelebten Praxis der Informationssicherheit) wird der „Stand der Technik“ häufig schon dann als gegeben angenommen, wenn eine Sicherheitsmaßnahme sich im Markt etabliert hat und ausreicht, aktuelle Bedrohungen abzuwehren oder bekannte Risiken zu vermindern. Insbesondere in kleinen und mittleren Unternehmen (KMU) wird hier vielfach ohne weiteres auf die Aussagen zum „Stand der Technik“ von Produktherstellern, IT-Systemhäusern oder Verkaufsliteratur vertraut. Das führt oft dazu, dass Wege eingeschlagen werden, die den Anforderungen des IT-Sicherheitsgesetzes an die Einhaltung des „Stands der Technik“ nicht genügen.

Sofern einschlägige internationale, europäische und nationale Normen sowie Standards oder technische Richtlinien des Bundesamts für Sicherheit in der Informationstechnik (BSI) vorhanden sind, können diese als Anhaltspunkt für eine Auswahl geeigneter Maßnahmen dienen. Jedoch sorgt der konstante technologische Fortschritt dafür, dass auch offizielle Rahmenwerke und Konzepte unbedingt einer regelmäßigen Aktualisierung bedürfen. Die implizite Annahme, dass Standards und Normen für sich allein den „Stand der Technik“ darstellen, erscheinen dabei überaus bedenklich, da diese Generalklausel das obere Ende des technisch Möglichen aber praktisch Bewährten zu einem bestimmten Zeitpunkt abbildet.[3]

Daher ist schon zu Beginn der jeweils anstehende Planung eine individuelle auf den Fall zugeschnittene Untersuchung erforderlich, ob und inwieweit die jeweilige Maßnahme oder das Maßnahmenbündel zu einem bestimmten Zeitpunkt nach gesetzlicher Vorschrift geeignet, erforderlich und angemessen ist.[4]

3 Methodik für die Bestimmung des „Stands der Technik“

Dokumentationen und Nachweise des „Stands der Technik“ erfordern eine Methodik, die es dem jeweiligen Unternehmen erlaubt, die anstehenden technischen und organisatorischen Sicherheitsmaßnahmen nachvollziehbar und in einer Form darzustellen, die sachkundigen Dritten die Möglichkeit gibt, sie unabhängig zu prüfen und zu bewerten.

Der Leitfaden „Schritte zur Ermittlung des Stands der Sicherheitstechnik“ (SFK-GS-33)[5] der Störfall-Kommission und die „Handlungsempfehlung zur Ermittlung des Standes der Technik“ (TRGS 460)[6] der Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) geben den Rahmen für die hier im Überblick dargelegte Methodik.

Zu dokumentieren ist, dass Maßnahmen dem „Stand der Technik“ entsprechend geplant und umgesetzt sind und sich in der Praxis bewährt haben[7]. Hierbei wird im Rahmen der Dokumentation eine formale Ebene und eine fachlich-inhaltliche Ebene voneinander unterschieden[8]. Die formale Ebene legt die Grundlage für eine spätere Betrachtung der Verhältnismäßigkeit der Umsetzung. Ziel der fachlich-inhaltlichen Ebene ist die Zuweisung der Maßnahme zu ihrer Generalklausel und der Nachweis ihrer praktischen Eignung.

Die Methodik bedient sich dabei einem mehrstufigen Verfahren, in dem Untersuchungsbereiche definiert werden, deren Bewertung anhand standardisierter Anforderungen und Kriterien vorgenommen wird.

Der Übergang einer Maßnahme von einer Generalklausel zu einer anderen ist dabei fließend. Daher kann auch für den sachkundigen Experten die Abgrenzung zwischen dem „Stand der Technik“ und den „anerkannten Regeln der Technik“ eine echte Herausforderung sein. Für die Nachvollziehbarkeit sind daher folgende Bereiche zu untersuchen:

- Eignung
- Fortschrittlichkeit
- Allgemeine Anerkennung
- Bewährung und Erprobung in der Praxis

Bei der Prüfung des „Stands der Technik“ ist bei entsprechender Eignung anzunehmen, dass sich die Fortschrittlichkeit umgekehrt proportional zu den beiden letztgenannten Untersuchungsbereichen verhält. Mit zunehmender allgemeinen Anerkennung und praktischer Bewährung einer Maßnahme ist davon auszugehen, dass es sich um eine „anerkannte Regel der Technik“ handelt. Der „Stand von Wissenschaft und Technik“ gibt die fortschrittlichste Generalklausel wieder.

4 Vergleich mit alternativen Maßnahmen

Nur der direkte Vergleich von Maßnahmen oder Maßnahmenbündeln untereinander erlaubt eine zutreffende Einordnung von Sachverhalten in den genannten Untersuchungsbereichen „All-

3 Vgl. auch Seibel, „Abgrenzung der allgemein anerkannten Regeln der Technik vom Stand der Technik“, NJW 41/2013, Seite 3000 ff.

4 Vgl. „Leitfaden: Schritte zur Ermittlung des Standes der Sicherheitstechnik“ (SFK-GS-33) unter http://www.kas-bmu.de/publikationen/sfk/sfk_gs_33.pdf

5 Siehe SFK-GS-33

6 Siehe „Handlungsempfehlung zur Ermittlung des Standes der Technik“ (TRGS 460) unter http://www.baua.de/de/Themen-von-A-Z/Gefahrstoffe/TRGS/TRGS-460.html

7 Vgl. BMJV, „Handbuch der Rechtsförmlichkeit“, 3. Aufl. Seite 84 ff

8 Vgl. TRGS460, Seite 23

gemeine Anerkennung“ und „Bewährung und Erprobung in der Praxis“.

Denn in der Regel gibt es für zu lösende Anforderungen zum Schutz von Unternehmenswerten unterschiedliche Ansätze und verschiedene technische Möglichkeiten der Umsetzung. Es bietet sich dabei an, im Rahmen einer konkreten Fragestellung zum „Stand der Technik“ neben

- der Beschreibung der umgesetzten Maßnahmen,
- des Aufwands für die Umsetzung und den Betrieb,
- den durch sie zu schützenden Unternehmenswerten und
- der Größe des Betroffenenkreises,

eine Datenbasis weiterer möglicher alternativer Sicherheitsmaßnahmen zu erheben.

In diese sind neben den branchenüblichen Maßnahmen auch Normen und Standards (ISO, DIN, BSI-TR, etc.) einzubeziehen. Leitlinien, regulatorische Vorgaben oder vertragliche Anforderungen geben Hinweise auf entsprechende Quellen. Zudem sollten etablierte Fachzeitschriften und Branchenveröffentlichungen als Quelle für Erkenntnisse und Erfahrungen aus Wissenschaft und Forschung herangezogen werden.

Über den Vergleich mit branchenüblichen und branchenübergreifenden Maßnahmen und die sachgerechte Abgrenzung des „Stands der Technik“ von den anderen Generalklauseln erreicht der Sachverständige zugleich auch eine Begründung der jeweils zu prüfenden Umsetzung und die erforderliche Darstellung von deren Verhältnismäßigkeit.

Für die Darstellung der Verhältnismäßigkeit erfordert die Auswahl der Maßnahmen eine Einschätzung, inwieweit die jeweilige Maßnahme für den angestrebten Schutz sowohl technisch geeignet, erforderlich und angemessen ist.

Eine Maßnahme ist

- geeignet, wenn sie den Schutz gegen Beeinträchtigungen der Schutzziele kausal bewirkt oder zumindest fördert,
- erforderlich, wenn es zur Erreichung des angestrebten Ziels keine mindestens gleichwertige geeignete Maßnahme gibt, die zudem effizienter ist (weniger benötigte Ressourcen und/oder höhere Qualität),
- angemessen, wenn der von der Maßnahme kausal bewirkte oder zumindest geförderte Schutz in einem wirtschaftlich vertretbaren Verhältnis zum Wert der Funktionsfähigkeit aller beeinflusster informationstechnischer Systeme, Komponenten oder Prozesse steht.

Um sicherzustellen, dass ein direkter Vergleich von Maßnahmen sinnvoll ist sowie für die Zuweisung der Maßnahmen zu einer der Generalklauseln, ist jedoch zunächst nur eine Aussage zur Eignung erforderlich.

Denn folgt man der Gesetzesbegründung zu § 8a ITSiG , so ist der Stand der Technik „*der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt.*“

Die Eignung einer Maßnahme ergibt sich dabei aus der Abschätzung zur Wirksamkeit und Zuverlässigkeit der gewählten Lösungen, Prozesse, Systeme oder gewählten Einsatzszenarien in Bezug auf die Schutzziele.

Abbildung 2 | Bewertung der Eignung einer Maßnahme

Bewertung	Beschreibung
++	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

5 Fachlich-inhaltliche Betrachtung der Bewertungskriterien

Um die Messbarkeit, Vergleichbarkeit und Nachvollziehbarkeit der Prüfungsergebnisse insgesamt sicherzustellen, muss systematisch vorgegangen werden. Die Systematik dient auch der weiteren Konkretisierung der Einordnungskriterien für die Generalklauseln.

Entwicklungsstand und Fortschrittlichkeit werden über die individuelle Bewertung und Abwägung vergleichbarer Kriterien ermittelt. Neben der Eignung werden hier die oben genannten Bereiche „Allgemeine Anerkennung“ und die „Bewährung und Erprobung in der Praxis“ untersucht.

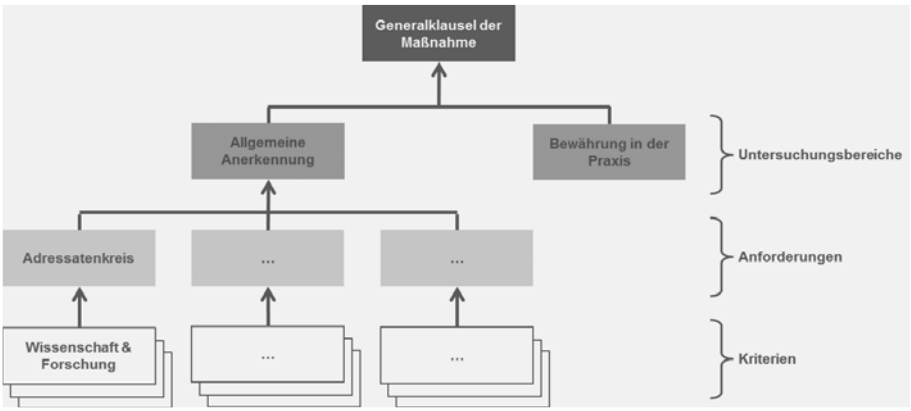
Eine Eignung kann angenommen werden, wenn die Maßnahme oder das Maßnahmenbündel eine positive Wirkung auf die Schutzziele (Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit) im Hinblick auf die zu schützenden Unternehmenswerte hat. Bei der Untersuchung wird daher der Einfluss für alle vier Grundwerte gesondert betrachtet und die Konsequenz der Umsetzung bewertet. Als praktikable Bewertung hat sich ein fünfstufiges System bewährt, das eine einfache qualitative Einschätzung der Eignung zulässt.

Die konkrete Maßnahme oder das Maßnahmenbündel setzt sich dabei aus *Verfahren, Einrichtungen und Betriebsweisen* zusammen. Eine Dokumentation und Einordnung dieser Bereiche hilft bei der Vergleichbarkeit und späteren Beurteilung. Eine Definition kann in Anlehnung an SFK-GS-33[9] wie folgt gegeben werden:

- Verfahren betrachten spezifische technische Lösungen und zusammenhängende Arbeitsabläufe und -prozesse, die zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen angewendet werden.
- Einrichtungen sind Hardware, Software, bauliche Einrichtungen sowie institutionelle (Gesetze, Normen, organisatorische Strukturen) und personelle (Anzahl und Wissen der IT-Mitarbeiter) Gegebenheiten, die zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen angewendet werden.
- Eine Betriebsweise beschreibt den Zweck (Einzweck/ Mehrzweck, konkret/übergreifend) oder den zeitlichen Einsatz (kontinuierlich/periodisch, automatisch/ manuell) von informationstechnischen Systemen, Komponenten oder Prozessen.

9 Siehe SFK-GS-33, Seite 20

Abbildung 3 | Ableitung der Kriterien für den Stand der Technik



6 Bewertung

Zur abschließenden Bewertung der Untersuchungsbereiche „Allgemeine Anerkennung" und die „Bewährung und Erprobung in der Praxis" wird in Anlehnung an gängige Reifegradmodelle eine qualitative Metrik entwickelt, die zum einen eine Vergleichbarkeit zwischen den Maßnahmen, zum anderen aber auch eine Adaption auf den jeweiligen Kontext des zu schützenden Systems zulässt. Recherche und Abwägung führen zu Bewertungen einzelner Anforderungen durch spezifische Aussagen und Nachweise. Ausgehend von den Rechercheergebnissen erfolgt die Einordnung des Untersuchungsbereichs in den jeweiligen Reifegrad.

Die einzelnen Untersuchungsbereiche werden durch Anforderungen spezifiziert und den Anforderungen wiederum Kriterien zugeordnet (siehe auch Abbildung 3). Die Kriterien lassen sich dabei auf die drei Generalklauseln abbilden, sodass eine Kumulierung der Ergebnisse die sachgerechte Zuweisung der Maßnahme zu einer der Klauseln erlaubt.

Anforderungen und ihre Kriterien sind so formuliert, dass sie anhand von Recherchen validierbar sind und sich im Prüfverfahren leicht abbilden lassen. Der Reifegrad, also die Erfüllung der Kriterien, wird für jede Anforderung einzeln bestimmt. Es wird dabei nicht nur die Existenz einer Maßnahme im Markt und ihre technische Fortschrittlichkeit beurteilt, sondern auch Aspekte wie beispielsweise die Adaption und Verfügbarkeit im Markt und der Status der Standardisierung. Ein Reifegrad gilt nur dann als erreicht, wenn sowohl die ihm zugeordneten als auch die in der niedrigeren Reifegrad-Stufe beschriebenen Kriterien nachweislich erreicht werden. Die Reifegrade bauen dementsprechend aufeinander auf.

Abbildung 4 | Beispiel einer Bewertung

Allgemeine Anerkennung	Reifegrad		
	(1)	(2)	(3)
Adressatenkreis	☐	☒	☐
Dokumentation	☐	☐	☒
Standardisierung	☐	☒	☐
Adaption im Markt	☐	☒	☐
...	☐	☐	☐

Sind die Anforderungen und ihre Reifegrade bestimmt, lassen sich die Ergebnisse zu einer Bewertung des jeweiligen Untersuchungsbereichs zusammenfassen. Die Ergebnisse beider Untersuchungsbereiche können dann in der Darstellung aus der ersten Abbildung eingeordnet werden. Die Mehrstufigkeit in der Bewertung erlaubt dann einerseits ein zuverlässiges Urteil darüber, ob die Maßnahme die Anforderungen der Schutzziele erfüllt und andererseits eine differenzierte Einschätzung der Fortschrittlichkeit der vorgesehenen Maßnahmen.

Die Bewertung und damit Klassifizierung einer Maßnahme als „Stand der Technik" erfolgt dann, wenn für beide Untersuchungsbereiche der überwiegende Teil an Anforderungen den Reifegrad erreicht hat, der dieser Generalklausel entspricht.

7 Praxisbeispiel

In § 13 Abs. 7 TMG wird die Berücksichtigung des „Stands der Technik" gefordert und insbesondere auf die „*Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens*" verwiesen. Die Gesetzesbegründung[10] zum ITSiG konzentriert sich hierbei insbesondere auf Webseitenbetreiber. Für diese ist nach Bewertung durch die hier vorgestellte Methodik die alleinige Verwendung des Verschlüsselungsprotokolls „*Transport Layer Security (TLS)*" in der Version TLSv1.2 mit der Unterstützung sogenannter „*forward secrecy*" vorzusehen.

Betrachtet man die Protokolloptionen für die Verschlüsselung der Datenübertragung, so sind technisch die Versionen „*Secure Socket Layer (SSL)*" in den Versionen SSLv2 und SSLv3 sowie die Versionen TLSv1.0, TLSv1.1 und TLSv1.2 möglich. Im Rahmen des Vergleichs der Optionen ergibt bereits die Untersuchung der Eignung, dass SSLv2 und SSLv3 aufgrund der bekannten Schwächen zum Verlust der entsprechenden Schutzziele führen und somit ausscheiden. Die Erweiterungen in TLSv1.2 und die Verwendung von „*forward secrecy*" verbessern dagegen die Berücksichtigung der Schutzziele – auch gegenüber der Vorgängerversion TLSv1.1.

Für die Einordnung von „*TLSv1.2 mit forward secrecy*" und die unterstützten Verschlüsselungsverfahren in eine der Generalklauseln sind die entsprechenden Anforderungen in den Untersuchungsbereichen „Allgemeine Anerkennung" und „Bewährung und Erprobung in der Praxis" zu untersuchen. Marktuntersuchungen zeigen[11], dass TLSv1.2 bei etwa 75 % der Webseiten als Protokoll eingesetzt wird und ca. 49 % „*forward secrecy*" unterstützen. Da jedoch noch bei etwa 98 % der Webserver TLSv1.0 konfiguriert ist, weisen beispielsweise die Kriterien für die Anforderung „*Adaption am Markt*" darauf hin, dass „*TLSv1.2 mit forward secrecy*" noch nicht in die Klausel „Anerkannte Regel der Technik" einzuordnen ist.

10 BMI, GE IT-Sicherheitsgesetz, 8.12.2014
11 URL: www.trustworthyinternet.org/ssl-pulse/

Im Untersuchungsbereich „Bewährung und Erprobung in der Praxis“ zeigt sich in der Anforderung „*Generation*“, dass TLSv1.2 die aktuellste verabschiedete Protokollversion ist. Demnach werden die Vorgängerversionen nicht in die Klausel „Stand der Technik“ einzuordnen sein. In gleicher Weise werden die weiteren Anforderungen beider Untersuchungsbereiche untersucht und bewertet.

Neben der Eignung werden somit die Untersuchungsbereiche „Allgemeine Anerkennung“ und die „Bewährung und Erprobung in der Praxis“ objektiv und vergleichbar bewertet. Die Anforderungen sind dabei weitestgehend generalisiert und lassen eine standardisierte Dokumentation zu.

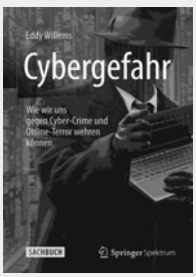
8 Zusammenfassung

Mit dieser neuen, hier nur skizzierten Methodik soll der Herausforderung für Unternehmen begegnet werden, den formellen Nachweis des „Stands der Technik“ und die Abgrenzung zwischen dem „Stand der Technik“ und den „anerkannten Regeln der Technik“ gesetzeskonform und praxistauglich zu führen. Wegen der fließenden und sich ständig ändernden Abgrenzung der Generalklauseln bedarf es im Rahmen der Nachweispflicht des ITSiG einer Bewertung des „Stands der Technik“, die es den Unternehmen ermöglicht, seine umgesetzten technischen und organisatorischen Maßnahmen nachvollziehbar darzustellen, so dass ein sachkundiger Dritter sie fundiert und notfalls gerichtsfest überprüfen kann. Da die Generalklausel „Stand der Technik“ das obere Ende des technisch Möglichen und praktisch Bewährten abbildet, stellt die stichtagsbezogene Abgrenzung zwischen dem „Stand der Technik“ und den „anerkannten Regeln der Technik“ eine besondere Herausforderung dar und sollte je nach Kritikalität und Schutzbedarf der Daten und Anwendungen sogar durch sachkundige Experten, wie z.B. Sachverständige, begründet und anhand nachvollziehbarer und vergleichbarer Kriterien dokumentiert werden.

Springer Spektrum

springer-spektrum.de

Was Sie über Viren, Spam und Datenklau wissen sollten



Eddy Willems; Thorsten Urbanski
Cybergefahr
Wie wir uns gegen Cyber-Crime und Online-Terror wehren können
1. Aufl. 2015.
XVIII, 188 S. 61 Abb. Brosch.
€ (D) 19,99 | € (A) 20,55 | *sFr 21,50
ISBN 978-3-658-04760-3 (Print)
€ (D) 14,99 | *sFr 17,00
ISBN 978-3-658-04761-0 (eBook)

- So schützen Sie sich vor Cyber-Crime
- Ohne technische Vorkenntnisse verständlich

Man kann online wählen, Rechnungen bezahlen und Tickets kaufen – aber wie sicher ist das? Überall lauern Viren, Spam, Hackerangriffe und sogar Cyber-Spione. Wie kann man sich schützen und wie sollte man dem Phänomen Cyber-Crime begegnen? Der bekannte Security-Experte Eddy Willems gibt einen Überblick über Online-Gefahren und Möglichkeiten, sich vor ihnen zu schützen. Er erläutert spannend die Vergangenheit, Gegenwart und Zukunft des Cyber-Crime.

€ (D) sind gebundene Ladenpreise in Deutschland und enthalten 7 % MwSt. € (A) sind gebundene Ladenpreise in Österreich und enthalten 10 % MwSt.
Die mit * gekennzeichneten Preise sind unverbindliche Preisempfehlungen und enthalten die landesübliche MwSt. Preisänderungen und Irrtümer vorbehalten.

Jetzt bestellen: springer-spektrum.de

A21538