

TeleTrust-interner Workshop

Berlin, 01.07.2025

AK "Stand der Technik"

Tomasz Lawicki

10 Jahre ist es her...



- Am 18.06.2015 wurde der Arbeitskreis "Stand der Technik" auf dem IWS 2015 initiiert.
- Nach einem Jahr intensiver Arbeit wurde die erste DE Version der Handreichung veröffentlicht.
- Nach weiteren zweieinhalb Jahren wurde die EN Version mit ENISA veröffentlicht. Kurz danach folgte die NL Version.
- Zum zehnjährigen Jubiläum des Arbeitskreises 'Stand der Technik' wurde die Handreichung umfassend überarbeitet und erneut erweitert.

Damals und heute...

2025

Seiten: 142

2021

Seiten: 108

2019

Seiten: 78

2016

Seiten: 62

TeleTrust - Bundesverband IT-Sicherheit e.V.	
Inhalt	
1	Einleitung
1.1	Gesetzliche Grundlagen
1.2	Branchenspezifische Sicherheitsstandards (BSI)
1.3	Angemessenheit der Maßnahmen
2	Bestimmung des Technologiestandes
2.1	Begrifflichkeit
2.2	Methode zur Einordnung des Technologiestandes
2.3	Prozess zur Qualitätsicherung der Handreichung
2.4	Geforderte Schutzziele
3	Technische und organisatorische Maßnahmen (TOM)
3.1	Allgemeine Hinweise
3.2	Technische Maßnahmen
3.2.1	Authentisierung
3.2.2	Bewertung und Durchsetzung starker Passwörter
3.2.3	Multifaktor-Authentisierung
3.2.4	Kryptographische Verfahren
3.2.5	Verschlüsselung von Datenströmen
3.2.6	Verschlüsselung von Daten und Ordern
3.2.7	Verschlüsselung von E-Mails
3.2.8	Schutz des elektronischen Datenverkehrs mit PKI
3.2.9	Einbau von verschlüsselten VPN-Lösungen (Layer 3)
3.2.10	Verschlüsselung auf Layer 2
3.2.11	Schutz in der Cloud gespeicherter Daten
3.2.12	Datenverarbeitung in der Cloud
3.2.13	Schutz möglicher Sprach- und Datendienste
3.2.14	Schutz der Kommunikation mittels Instant Messenger
3.2.15	Schutz mobiler Geräte
3.2.16	Routensicherheit
3.2.17	Netzwerküberwachung mit IDS
3.2.18	Schutz des Web-Datenverkehrs
3.2.19	Schutz von Web-Anwendungen
3.2.20	Schutz des Fernzugriffs auf Netz
3.2.21	Systemhärtung
3.2.22	Endpoint Detection & Response
3.2.23	Werkzeuge der Internetnutzung
3.2.24	Angriffserkennung und -abwehr
3.2.25	Verlässliche Datenverarbeitung
3.2.26	Sendeblock zur Schadcode-Abwehr
3.2.27	Cyber Threat Intelligence
3.2.28	Abrechnung administrativer IT-S
3.2.29	Überwachung von Verzeichnissen
3.2.30	Netzwerksegmentierung und Seg
3.2.31	Cloud-Sicherheitsplattform
3.2.32	Identifizierung
3.2.33	VCIH-Verschlüsselung mit SIP
3.2.34	Verschlüsselung (Layer 1)
3.3	Organisatorische Maßnahmen
3.3.1	Standards und Normen
3.3.2	Sicherheitsorganisation
3.3.3	Informationssicherheitsmanagem
3.3.4	Sichere Softwareentwicklung
3.3.5	Prozesszertifizierung
3.3.6	Schwachstellen- und Patchmanag
3.3.7	Risikomanagement
3.3.8	Personenzertifizierung
3.3.9	Abrechnung privater Benutzer

Handreichung Stand der Technik in der IT-Sicherheit

Technische und organisatorische Maßnahmen

2025

+129%

Inhaltsverzeichnis	
Grundsätze der Handreichung	5
1 Einleitung	6
1.1 Gesetzliche und regulatorische Grundlagen	6
1.2 Branchenspezifische Sicherheitsstandards (BSI)	12
1.3 Angemessenheit der Maßnahmen	12
2 Bestimmung des Technologiestandes	13
2.1 Begrifflichkeit	13
2.2 Methode zur Einordnung des Technologiestandes	15
2.3 Prozess zur Qualitätsicherung der Handreichung	17
2.4 Geforderte Schutzziele	18
3 Technische und organisatorische Maßnahmen (TOM)	19
3.1 Allgemeine Hinweise	19
3.2 Technische Maßnahmen	22
3.2.1 Authentisierung	22
3.2.2 Bewertung und Durchsetzung starker Passwörter	23
3.2.3 Multifaktor-Authentisierung	25
3.2.4 Kryptographische Verfahren	27
3.2.5 Verschlüsselung von Datenströmen	30
3.2.6 Verschlüsselung von Daten und Ordern	31
3.2.7 Verschlüsselung von E-Mails	32
3.2.8 Schutz des elektronischen Datenverkehrs mit PKI	34
3.2.9 Einbau von verschlüsselten VPN-Lösungen (Layer 3)	36
3.2.10 Verschlüsselung auf Layer 2	39
3.2.11 Schutz in der Cloud gespeicherter Daten	40
3.2.12 Datenverarbeitung in der Cloud	41
3.2.13 Schutz möglicher Sprach- und Datendienste	43
3.2.14 Schutz der Kommunikation mittels Instant Messenger	44
3.2.15 Schutz mobiler Geräte	46
3.2.16 Routensicherheit	46
3.2.17 Netzwerküberwachung mit IDS	46
3.2.18 Schutz des Web-Datenverkehrs	46
3.2.19 Schutz von Web-Anwendungen	46
3.2.20 Schutz des Fernzugriffs auf Netz	46
3.2.21 Systemhärtung	46
3.2.22 Endpoint Detection & Response	46
3.2.23 Werkzeuge der Internetnutzung	46
3.2.24 Angriffserkennung und -abwehr	46
3.2.25 Verlässliche Datenverarbeitung	46
3.2.26 Sendeblock zur Schadcode-Abwehr	46
3.2.27 Cyber Threat Intelligence	46
3.2.28 Abrechnung administrativer IT-S	46
3.2.29 Überwachung von Verzeichnissen	46
3.2.30 Netzwerksegmentierung und Seg	46
3.2.31 Cloud-Sicherheitsplattform	46
3.2.32 Identifizierung	46
3.2.33 VCIH-Verschlüsselung mit SIP	46
3.2.34 Verschlüsselung (Layer 1)	46
3.3 Organisatorische Maßnahmen	46
3.3.1 Standards und Normen	46
3.3.2 Sicherheitsorganisation	46
3.3.3 Informationssicherheitsmanagem	46
3.3.4 Sichere Softwareentwicklung	46
3.3.5 Prozesszertifizierung	46
3.3.6 Schwachstellen- und Patchmanag	46
3.3.7 Risikomanagement	46
3.3.8 Personenzertifizierung	46
3.3.9 Abrechnung privater Benutzer	46
3.3.10 Dark Web Monitoring	106
3.3.11 Umgang mit Dienstleistern	106
3.3.12 Software Bill of Materials (SBOM)	109
3.3.13 Open-Redundanz	111
3.3.14 Sensibilisierung der Anwender	112
3.3.15 Asset Management	116
3.3.16 Incident Management	116
3.3.17 Geschäftskontinuitätsmanagement (BCM)	118
3.3.18 Notfall- und Krisenmanagement	119
3.3.19 Notfallübungen	122
3.3.20 Technische Sicherheitsüberprüfung	123
4 Exkurse	127
4.1 Maßnahmen gegen Ransomware-Angriffe	127
4.2 Einordnung der Maßnahmen in ISO/IEC 27001:2022	132
4.3 Einordnung der Maßnahmen in das NIST-Rahmenwerk	132
4.4 Auswertung von KI auf Informationssicherheit	134
4.5 Absicherung der Lieferkette	138
Abbildungsverzeichnis	
Abbildung 1: Drei-Stufen-Theorie nach Kalkar-Entscheidung	13
Abbildung 2: Beispiel der Einordnung des Technologiestandes	16
Abbildung 3: Prozesskette für die Bewertung der Maßnahmen im Arbeitskreis	17
Abbildung 4: Aufbau und die Zusammenhänge von PKI-Komponenten	35
Abbildung 5: Gliederung des Informationssicherheitsmanagements Standards und Normen	53
Abbildung 6: Risikoprozess nach ISO/IEC 31000	98
Abbildung 7: Ransomware-Mitigation und Schutzmaßnahmen (Beispiel)	127
Tabellenverzeichnis	
Tabelle 1: Übersicht der ISO/IEC 27000-Reihe	82
Tabelle 2: Abgrenzung ISO/IEC 27001 vs. BSI-Grundschutz	83
Tabelle 3: Rollen und Zuständigkeiten innerhalb einer Sicherheitsorganisation	85
Tabelle 4: Abgrenzung BCM vs. Notfall- und Krisenmanagement	120
Tabelle 5: Zusammensetzung des Krisenstabs	124
Tabelle 6: Beispielhafte Fragestellungen bei Konfigurationsanalysen	125
Tabelle 7: Beispielhafte Fragestellungen bei Härtnungsüberprüfungen	129
Tabelle 8: Maßnahmen gegen Ransomware-Angriffe	131
Tabelle 9: Einordnung der Maßnahmen in ISO/IEC 27001:2022	131
Tabelle 10: Einordnung der Maßnahmen in das NIST-Rahmenwerk	133
Tabelle 11: Sicherheitsrisiken von KI-Modellen und Schutzmaßnahmen	137

"Stand der Technik (in der IT-Sicherheit)
bezeichnet die am Markt verfügbare Bestleistung
einer IT-Sicherheitsmaßnahme
zur Erreichung der gesetzlichen IT-Sicherheitsziele."

... aber es ändert sich so einiges.



 TeleTrust
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

$$\left\{ \begin{array}{l} \text{ } \\ \text{ } \end{array} \right.$$

Das Diagramm zeigt die Bewertung von Fachexperten basierend auf zwei Kriterien: 'Anerkennung durch Fachexperten' (Y-Achse) und 'Bewährung in der Praxis' (X-Achse). Die Achsen sind von 1 bis 5 skaliert. Ein grüner gestrichelter Bereich markiert den 'Markteintritt' (SdWF, SdT, SdT oder aaRT). Eine rote Linie markiert den Bereich 'keine oder kaum Anerkennung'.

[illegible]

Das Diagramm zeigt die Bewertung von Fachexperten basierend auf zwei Kriterien: 'Anerkennung durch Fachexperten' (Y-Achse) und 'Bewertung in der Praxis' (X-Achse). Die Y-Achse reicht von 1 bis 5, die X-Achse von 1 bis 5. Eine vertikale gestrichelte grüne Linie bei x=1.5 markiert den 'Markteintritt'. Eine horizontale gestrichelte grüne Linie bei y=3.5 markiert den 'SdT'. Ein Punkt bei (4, 4) ist mit einer blauen Raute markiert und als 'SdT oder aaRT' beschriftet. Ein roter Balken bei y=1.5 ist mit 'keine oder kaum Anerkennung' beschriftet.

5

Anwendungsbeispiele für die Handreichung

Argumentationshilfe in Richtung des Managements, um Verbesserung von Sicherheitsmaßnahmen zu begründen.

Referenzdokument für die Abschlüsse von Dienstleistungsverträgen mit Fokus auf Informationssicherheit



Orientierungshilfe bei bevorstehenden Transformationsprojekten und für Marktrecherche.

Schulungsgrundlage für Trainings in Unternehmen und Vorlesungen an Hochschulen

Ohne euch, würde das hier nicht funktionieren!

Karsten U. Bartels LL.M., Michael Barth, Christoph Bausewein, Ralf Benz Müller, Ulf Bernhardt, Oliver Dehning, Dennis Dominkovic, Sascha Dubbel, Oliver Falkenthal, Marco Fischer, Nancy Föllmer, Tobias Glemser, Erik Gremeyer, Steffen Heyde, Hubert A. Jäger, Malte Kahrs, Kristian Kißling, Ulrich Kohn, Robert Kolmhofer, Dominik Kowol, Pamela Krosta-Hartl, Michael Kynast, Thomas Lang, Alexander Leitner, Dr. Bernd Liedke-Deutscher LL.M., Janosch Maier, Karl-Ulrich Martin, Stefan Menge, Tobias Mielke, Siegfried Mueller, Benjamin Pfister, Johanna Rechberg, Peter Rost, Alexander Schlensog, Matthias Weigmann, Klaus Wilke, André Zingsheim, Dr. Holger Mühlbauer, Morad Abou Nasser

DANKE!

