



Michael LANG · Hans LÖHR

IT-Sicherheit

Technologien und Best Practices
für die Umsetzung im Unternehmen

HANSER

HANSER

IT-Sicherheit

Technologien und Best Practices für die Umsetzung im Unternehmen

Herausgegeben von
Michael Lang und Hans Löhr

Mit Beiträgen von
Daniel Angermeier, Martin Braun, Hans Höfken, Thomas Jansen, Stefan Karg, Nicolai Kuntze, Hagen Lauer, Thomas Lohre, Markus Nauroth, Jutta Pertenaïs, Norbert Pohlmann, Andreas Reisch, Marko Schuba, Christoph Skornia, Fabian Topp, Marcel Winandy

Alle in diesem Buch enthaltenen Informationen, Verfahren und Darstellungen wurden nach bestem Wissen zusammengestellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund sind die im vorliegenden Buch enthaltenen Informationen mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Herausgeber, Autoren und Verlag übernehmen infolgedessen keine juristische Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieser Informationen – oder Teilen davon – entsteht.

Ebenso übernehmen Herausgeber, Autoren und Verlag keine Gewähr dafür, dass beschriebene Verfahren usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Buch berechtigt deshalb auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dieses Werk ist urheberrechtlich geschützt.

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Buches, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren) – auch nicht für Zwecke der Unterrichtsgestaltung – reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© 2022 Carl Hanser Verlag München, www.hanser-fachbuch.de

Lektorat: Sylvia Hasselbach

Copy editing: Sandra Gottmann, Wasserburg

Umschlagdesign: Marc Müller-Bremer, www.rebranding.de, München

Umschlagrealisation: Max Kostopoulos

Titelmotiv: © stock.adobe.com/blackboard

Ausstattung patentrechtlich geschützt. Kösel FD 351, Patent-Nr. 0748702

Print-ISBN: 978-3-446-47223-5

E-Book-ISBN: 978-3-446-47347-8

E-Pub-ISBN: 978-3-446-47511-3

Inhalt

Titelei

Impressum

Inhalt

Vorwort

1 IT-Sicherheit konsequent und effizient umsetzen

Norbert Pohlmann

1.1 Einleitung

1.1.1 Chancen durch die Digitalisierung

1.1.2 Risiken durch die Digitalisierung

1.1.3 IT-Sicherheitsbedürfnisse als Grundwerte der IT-Sicherheit

1.2 Beispiele von aktuellen Angriffsvektoren

1.3 IT-Sicherheitsstrategien

1.3.1 Vermeiden von Angriffen

1.3.2 Entgegenwirken von Angriffen

1.3.3 Erkennen von Angriffen

1.3.4 Reaktion auf Angriffe

1.4 Umsetzung eines angemessenen IT-Sicherheitslevels

1.5 IT-Sicherheitsmechanismen, die gegen Angriffe wirken

1.6 Die wichtigsten Punkte in Kürze

1.7 Literatur

2 Grundprinzipien zur Gewährleistung der IT-Sicherheit

Hagen Lauer, Nicolai Kuntze

2.1 Einleitung

2.1.1 Trends

2.1.2 Herausforderungen

2.1.3 IT-Sicherheit vs. Sicherheit

2.1.4 Schutzziele

2.2 Grundprinzipien der IT-Sicherheit

2.2.1 Kenne die Bedrohungen

2.2.2 Sicherheit und Wirtschaftlichkeit

2.2.3 Keine „Security through Obscurity“

2.2.4 Security by Design

2.2.5 Prinzip der geringsten Berechtigung

2.2.6 Trennung der Verantwortlichkeiten

2.2.7 Zugriffskontrolle

2.2.8 Defense in Depth

2.2.9 Der Mensch als Faktor

2.2.10 Design for Resilience

2.3 Literatur

3 Organisation des IT-Sicherheitsmanagements im Unternehmen

Markus Nauroth

3.1 Einführende Bemerkungen

3.2 Imperative des IT-Sicherheitsmanagements

3.2.1 Sicherheit ist aktiv und proaktiv

3.2.2 Routine

3.2.3 Sicherheit liegt in der Verantwortung eines jeden

3.2.4 Worst-Case-Szenario

3.2.5 Es bedarf vieler Unterstützer

3.2.6 Denken wie ein Angreifer

3.2.7 Mehrschichtige Verteidigung verwenden

3.3 Grundlegende Pfeiler einer IT-Sicherheitsorganisation

**3.3.1 Gängige Organisationsstrukturen nach
organisatorischem Reifegrad**

3.3.2 Das Information Technology Risk Council (ITRC)

3.4 Die Rolle des CISO: Wie man eine Führungsrolle im Sicherheitsbereich gestaltet

3.4.1 Die richtige CISO-Rolle für Ihr Unternehmen entwerfen

3.5 Finale Anmerkungen

4 Rechtliche Rahmenbedingungen der IT-Sicherheit

Thomas Jansen

4.1 Einleitung

4.2 Vertrags- und haftungsrechtliche Risiken

4.2.1 Allgemeine Sorgfaltspflichten

4.2.2 Pflichten zur Gewährleistung der IT-Sicherheit

4.2.3 Haftung für Verstöße gegen IT-sicherheitsrechtliche Anforderungen

4.2.4 Anforderungen der DSGVO an technische und organisatorische Schutzmaßnahmen zum Schutz der IT-Sicherheit

4.2.5 Anforderungen des TKG und des TTDSG an technische und organisatorische Schutzmaßnahmen zum Schutz der IT-Sicherheit

4.2.6 Empfehlungen des BSI in Bezug auf technisch-organisatorische Maßnahmen

4.3 Straf- und ordnungswidrigkeitsrechtliche Folgen bei der Verletzung der IT-Sicherheit

4.3.1 Strafrechtliche Normen zum Schutz vor Cyberkriminalität

4.3.2 Strafrechtliche Verantwortlichkeit der einzelnen Akteure

4.4 Das IT-Sicherheitsgesetz (ITSiG 2.0)

4.5 Die wichtigsten Punkte in Kürze

4.6 Literatur

5 Standards und Zertifizierungen

Thomas Lohre

5.1 Einleitung

5.2 Standards

5.2.1 Synergien zwischen Standards auflösen und nutzen

5.2.2 Zertifizierung/Testierung

5.3 Kompetenznachweise für Beteiligte der Informationssicherheit

5.4 Die wichtigsten Punkte in Kürze

5.5 Literatur

6 Datenschutz und Informationssicherheit: ungleiche Zwillinge

Stefan Karg

6.1 Einleitung

6.2 Rechtlicher Rahmen

6.3 Strategische/präventive Aspekte

6.3.1 Risikomanagement

6.3.2 Regelmäßige Überprüfung der Maßnahmen

6.3.3 Entwicklungsprozess

6.4 Operative Aspekte: technische und organisatorische Maßnahmen

6.4.1 Schutz der Vertraulichkeit

6.4.2 Schutz der Integrität

6.4.3 Schutz der Verfügbarkeit und Belastbarkeit

6.4.4 Vorfallsbehandlung (Incident Management)

6.5 Organisationsaspekte

6.6 Fazit

6.7 Literatur

7 Sicherheit durch Bedrohungs- und Risikoanalysen stärken

Daniel Angermeier

7.1 Einleitung

7.2 Nutzen und Mehrwert von Bedrohungs- und Risikoanalysen

7.3 Ablauf von Bedrohungs- und Risikoanalysen

7.4 Einbindung in Unternehmensprozesse

7.4.1 Anforderungsanalyse und Konzeptphase

7.4.2 Tests planen und priorisieren, Testergebnisse bewerten

7.4.3 Schwachstellen bewerten und behandeln

7.4.4 Laufende Systeme bewerten

7.5 Auswahlkriterien für geeignete Methoden

7.6 Die wichtigsten Punkte in Kürze

7.7 Literatur

8 Mittels Reifegradanalysen den IT-Security-Level nachhaltig und belastbar steigern

Martin Braun

8.1 Einleitung

8.2 Aufgabe und Wirkung einer Reifegradanalyse

8.2.1 Aufgabe der Reifegradanalyse

8.2.2 Die Reifegradanalyse hat unterschiedliche Aufgaben

8.2.3 Reifegradanalyse auch als Messinstrument der Belastbarkeit der Kernprozesse

8.2.4 Wirkung der Reifegradanalyse

8.3 Den Reifegrad des IT-Security-Prozesses ermitteln

8.3.1 Definition des IT-Security-Reifegrad-Levels 0: Initial

8.3.2 Definition des IT-Security-Reifegrad Level 1: wiederholbar

8.3.3 Definition des IT-Security-Reifegrad-Levels 2: definiert

8.3.4 Definition des IT-Security-Reifegrad-Levels 3: gemanagt

8.3.5 Definition des IT-Security-Reifegrad-Levels 4: optimiert

8.4 Durch eine kontinuierliche Reifegradmessung das IT-Risiko minimieren

8.4.1 Gesamtheitliche Betrachtung der Perspektiven

8.4.2 Perspektive Business

8.4.3 Perspektive Organisation und IT

8.5 Fazit

9 Der Chief Information Security Officer in der Praxis

Andreas Reisch

9.1 Einleitung

9.2 Business und IT, woher – wohin – mit wem?

9.3 Wozu gibt es nun den CISO?

9.4 Die persönliche Verantwortung des CISO

9.5 Verantwortung des Unternehmens

9.6 Das ISMS

9.7 Culture, Communication & Awareness

9.8 Assessments

9.9 Approvals und Information Security Consulting

9.10 Information Security Consulting

9.11 Lohnt sich das SOC?

9.12 IS-Operations

9.13 Fazit

10 Irgendwas ist immer – Informationssicherheit aus Sicht des CISO der Allianz Technology

Fabian Topp

10.1 Einleitung

10.2 Vernetzung – hilf mir, es selbst zu tun

10.3 Personal – die schlechten sind die teuersten Mitarbeiter

10.4 No Risk (no Privacy, no Audit, ...), no Fun

10.4.1 Organisation ist ein Mittel, die Kräfte des Einzelnen zu
vervielfältigen

10.4.2 Mehr als die Summe seiner Teile

10.5 Ende gut, alles gut?

11 Entwicklung sicherer Software

Nicolai Kuntze, Hagen Lauer

11.1 Einleitung

11.2 Vorgehensmodelle der Softwareentwicklung

11.3 Secure Development Lifecycles

11.4 Requirements Engineering

11.5 Architektur und Entwurf

11.6 Implementierung

11.7 Coding-Standards

11.8 Wahl der Programmiersprache

11.9 Tests

11.10 Code Reviews

11.11 Static Code Analysis

11.12 Formale Analyse

11.13 Validierung

11.14 Maintenance

11.15 Die wichtigsten Punkte in Kürze

11.16 Literatur

12 Cybersicherheit in Produktion, Automotive und intelligenten Gebäuden

Marko Schuba, Hans Höfken

12.1 Einleitung

12.1.1 Automatisierungstechnik

12.1.2 Spezifische Anforderungen der Automatisierungstechnik

12.1.3 Spezifische Eigenschaften der Automatisierungstechnik

12.2 Schöne neue Welt – das Internet der Dinge

12.2.1 Internet der Dinge (IoT)

12.2.2 IoT-Chancen für die Automatisierungstechnik

12.2.3 IoT-Risiken für die Automatisierungstechnik

12.3 Was läuft schief?

12.3.1 Zu viel Vertrauen in andere

12.3.2 Zu wenig Management-Fokus

12.3.3 Sicherheits-Features zu teuer oder nicht genutzt

12.3.4 Es ist noch nie etwas passiert – und das bleibt auch so

12.3.5 Never change a running system

12.3.6 Sensibilisierung und Weiterbildung zu teuer/aufwendig

12.4 Was ist zu tun?

12.4.1 Cybersicherheit allgemein

12.4.2 Cybersicherheit in der Automatisierung

12.5 Praxisbeispiel: Einführung von Cybersicherheit in der Produktion (Orientierung an ISA/IEC 62443)

12.5.1 Audit

12.5.2 Festlegen eines Sicherheitslevels

12.5.3 Risikobeurteilung

12.5.4 Defense in Depth

12.5.5 Zonierung

12.5.6 Patchmanagement

12.5.7 Dienstleister

12.6 Zusammenfassung und Fazit

12.7 Literatur

13 Edge Computing: Chancen und Sicherheitsrisiken

Marcel Winandy

13.1 Einleitung

13.2 Was ist Edge Computing?

13.2.1 Das Internet der Dinge

13.2.2 Von der Cloud zur Edge

13.2.3 Impulsgeber für IoT Edge Computing

13.3 Chancen und Sicherheitsrisiken

13.3.1 Eröffnung neuer Möglichkeiten durch IoT Edge Computing

13.3.2 IoT Edge Computing bringt auch neue Sicherheitsrisiken

13.4 Entwicklung sicherer Edge-Computing-Plattformen

13.4.1 Security-by-Design-Prinzipien

13.4.2 Privacy-by-Design-Prinzipien

13.4.3 Spezielle Entwicklungsprinzipien für Edge Computing

13.5 Technologien für sichere Edge-Computing-Plattformen

13.5.1 Sicherheitskerne

13.5.2 Trusted Execution Environments

13.5.3 Kryptoagilität

13.6 Die wichtigsten Punkte in Kürze

13.7 Literatur

14 IT-Sicherheit in Vergabeverfahren

Jutta Pertenais

14.1 Einleitung

14.2 Vergabeverfahren in Deutschland

14.2.1 Grundsätze und Aspekte

14.2.2 Verfahrensarten

14.2.3 Elektronische Vergabepattformen

14.3 IT-Sicherheit im Vergabeverfahren

14.3.1 TOM im Vergabeverfahren

14.3.2 Die Gestaltung der Vergabeunterlagen

14.3.3 Die Planung des Vergabeverfahrens

14.3.4 Die Verfahrensdurchführung

14.3.5 Die elektronische Kommunikation

14.3.6 Der Umgang mit Verschlusssachen

14.4 Kennzeichen von Geschäftsgeheimnissen

14.5 Rechtsschutzmöglichkeiten

14.6 Strafbarkeit im Vergabeverfahren

14.7 Bietertipps zum Umgang mit Vergabestellen und zur Erstellung von Angeboten

14.8 Die wichtigsten Punkte in Kürze

14.9 Literatur

15 Sicherheit in der Cloud

Christoph Skornia

15.1 Einleitung

15.2 Nutzungsmodelle

15.2.1 Servicemodelle

15.2.2 Bereitstellungsmodelle

15.3 Risiken des Cloud Computing

15.3.1 Überblick

15.3.2 Beispiele

15.4 Sicherheitsmaßnahmen

15.4.1 Sicherheitsrahmen

15.4.2 Zugangskontrolle

15.4.3 Datensicherheit

15.4.4 Monitoring und Überwachung

15.5 Zusammenfassung

15.6 Die wichtigsten Punkte in Kürze

15.7 Literatur

Herausgeber, Autorin und Autoren

Vorwort

Informationen sind die wertvollsten Güter für Unternehmen. Die zur Informationsverarbeitung eingesetzten IT-Systeme sind heutzutage zentraler Bestandteil jedes Unternehmens und bilden die Grundlage für nahezu alle Geschäftsprozesse. Ohne sie funktioniert fast nichts mehr.

Kommt es zu Störungen in der IT, kann dies im schlimmsten Fall das komplette Unternehmen zum Stillstand bringen und existenzbedrohend sein. Gleiches gilt, wenn Informationen des Unternehmens oder dessen Kunden verloren gehen, gestohlen werden, manipuliert werden oder nicht mehr verarbeitet werden können.

Daher ist es für Unternehmen existenziell bedeutend, die Sicherheit der Informationen, Systeme und Produkte zu gewährleisten. Dies trifft heute mehr denn je zu, denn mit zunehmender Vernetzung wächst auch die Angriffsfläche: Jedes vernetzte Gerät ist ein potenzielles Einfallstor für Gefährdungen, und das erhöht das Risiko zusätzlich.

Doch wie können Sie Ihr Unternehmen vor diesen Gefährdungen schützen und Sicherheit gewährleisten?

Die Antwort auf diese Frage – und viele hilfreiche Impulse und Best Practices zur Umsetzung – erhalten Sie in diesem Buch.

Wir freuen uns, dass dazu 16 ausgewiesene Experten/Expertinnen als Autoren/Autorinnen an diesem Buch mitgewirkt haben, um Ihnen die relevanten Aspekte zur IT-Sicherheit von Unternehmen zu beschreiben.

Wir wünschen Ihnen viel Spaß beim Lesen des Buches und viel Erfolg beim Umsetzen der dabei gewonnenen Erkenntnisse!

Ihre Herausgeber

Michael Lang und Hans Löhr

1 IT-Sicherheit konsequent und effizient umsetzen

Norbert Pohlmann



In diesem Beitrag erfahren Sie,

- welche Chancen und Risiken die fortschreitende Digitalisierung mit sich bringt,
- welche Angriffsvektoren heute für erfolgreiche Angriffe genutzt werden,
- welche IT-Sicherheitsstrategien helfen, Risiken zu reduzieren und mit verbleibenden Risiken umzugehen, und
- welche IT-Sicherheitsmechanismen gegen welche Angriffe wirken.

1.1 Einleitung

Wir befinden uns gerade in einer digitalen Transformation, die mit einer radikalen Umgestaltung unseres Alltags und unserer Arbeitswelt sowie aller Geschäftsmodelle und Verwaltungsprozesse einhergeht. Wirtschaftskraft und Wohlstand sowie die Leistungsfähigkeit unserer modernen Gesellschaft werden durch den gelungenen digitalen Wandel bestimmt.

1.1.1 Chancen durch die Digitalisierung

Die Digitalisierung eröffnet über alle Branchen und Unternehmensgrößen hinweg enorme Wachstumschancen und führt zu immer besseren Prozessen, die die Effizienz steigern und Kosten reduzieren. Die Digitalisierung beschleunigt auf allen Ebenen, und der Wertschöpfungsanteil der IT in allen Produkten und Lösungen wird immer größer (Pohlmann 2020) (siehe [Bild 1.1](#), obere Kurve).

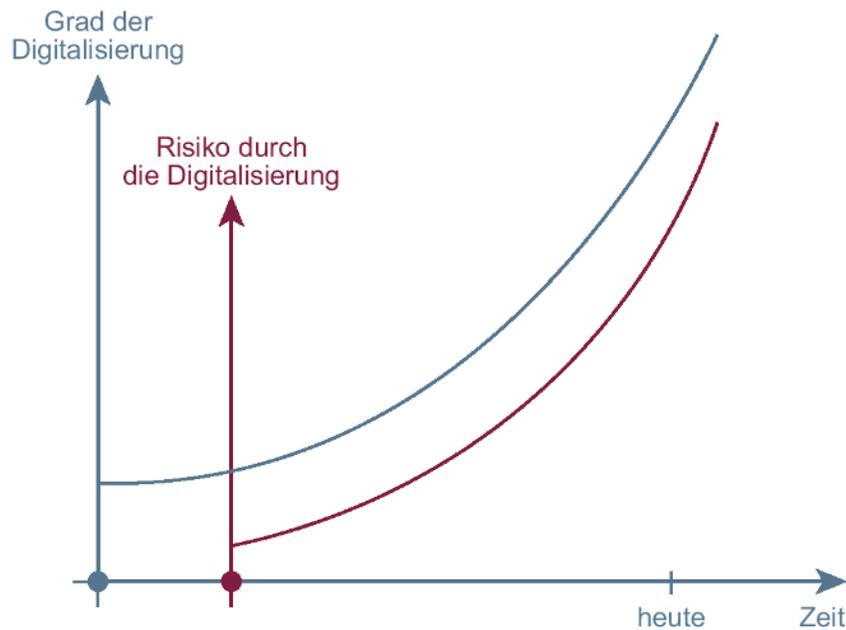


Bild 1.1 Entwicklung der Digitalisierung und des korrespondierenden Risikos

Mögliche Erfolgsfaktoren der Digitalisierung sind vielfältig:

- Mit 5G- und Glasfasernetzen erhöhen sich Kommunikationsgeschwindigkeit und -qualität, wodurch neue Anwendungen möglich werden.
- Smarte Endgeräte wie Smartwatches, Smartphones, PADS oder IoT-Geräte bringen viele neue sinnvolle Anwendungen mit sich.
- Zunehmend leistungsfähige zentrale IT-Systeme wie Cloud-Systeme, Edge-Computing oder Hyperscaler schaffen Innovationen mit großen Potenzialen.
- Da immer mehr Daten zur Verfügung stehen, ist die Verwendung von KI (ML ...) ein weiterer Treiber von neuen Geschäftsmodellen (Pohlmann 2019a).

- Moderne Benutzerschnittstellen, wie Sprache und Gestik, vereinfachen die Bedienung der smarten Endgeräte.
- Die Optimierung von Prozessen schafft ein enormes Rationalisierungspotenzial, das es zu heben gilt, um wettbewerbsfähig zu bleiben und Wachstumschancen zu nutzen.
- Neue Optionen wie Videokonferenzen und Cloud-Anwendungen ermöglichen, im Homeoffice zu arbeiten und damit die Personenmobilität zu reduzieren sowie letztendlich die Umwelt zu schonen.

1.1.2 Risiken durch die Digitalisierung

Wir müssen aber auch feststellen, dass seit Beginn der IT – sowie jetzt mit der zunehmenden Digitalisierung – die IT-Sicherheitsprobleme jedes Jahr größer werden und auf absehbare Zeit definitiv nicht abnehmen. Eine wichtige Erkenntnis ist, dass die heutigen IT-Architekturen unserer Endgeräte, Server, Netzkomponenten und zentralen IT-Dienstleistungen nicht sicher genug konzipiert und aufgebaut sind, um den Angriffen intelligenter Hacker erfolgreich entgegenzuwirken. Die Vielzahl der lokalen und zentralen Anwendungen, die unterschiedlichen Zugänge zum Internet, die Masse der IT-Systeme und IT-Infrastrukturen sowie die zunehmenden Abhängigkeiten innerhalb der Supply Chain machen die Komplexität der IT immer größer und damit auch die Anfälligkeit für bösartige Angriffe. Täglich können wir den Medien entnehmen, wie sich kriminelle Hacker die unzureichende Qualität der Software zunutze machen, indem sie Malware

installieren und damit Passwörter sowie Identitäten stehlen, Endgeräte ausspionieren oder die IT-Systeme verschlüsseln, um Lösegeld für die notwendigen Schlüssel zur Entsperrung zu erpressen. Aufgrund der generierten Datenmengen werden die Angriffsziele mit fortschreitender Digitalisierung kontinuierlich lukrativer.

Die Robustheit und Resilienz unserer IT-Systeme sind nicht hinreichend, und der Level an IT-Sicherheit entspricht nicht dem „Stand der Technik“. Mit dem höheren Grad an Digitalisierung steigt momentan das Risiko eines Schadensfalls (siehe [Bild 1.1](#), untere Kurve). Daraus ergibt sich in der Konsequenz, dass durch Diebstahl, Spionage und Sabotage der deutschen Wirtschaft jährlich ein Gesamtschaden von mehr als 220 Milliarden Euro entsteht.

1.1.3 IT-Sicherheitsbedürfnisse als Grundwerte der IT-Sicherheit

IT-Sicherheitsbedürfnisse sind Grundwerte der IT-Sicherheit, die mithilfe von IT-Sicherheitsmechanismen befriedigt werden können. IT-Sicherheitsbedürfnisse werden auch als IT-Sicherheitsziele bezeichnet.

- **Gewährleistung der Vertraulichkeit**

Vertraulichkeit ist wichtig, damit keine unautorisierten Personen oder Organisationen in der Lage sind, übertragene oder gespeicherte Informationen zu lesen.

- **Gewährleistung der Authentifikation**