

Grundlagen der IT Sicherheit

Eine Einführung für Nichtfachleute

Hier lesen Sie:

Wer für IT Sicherheit verantwortlich ist
Seite 1

Bedrohungen für IT Systeme
Seite 3

Risikoanalyse und Schutzbedarf
Seite 5

Über den Autor
Seite 6

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)

❖ Einführung

Diese Publikation wendet sich an Führungskräfte und Manager aus dem nicht technischen Bereich, die sich mit dem Thema der Sicherheit in der Informationstechnologie beschäftigen. Es soll eine generelle Einführung in die Thematik der Sicherheit in der Informationstechnologie gegeben werden, ohne dabei auf technische Aspekte im Detail einzugehen.

Für weitere, technische Informationen zu der Thematik wenden Sie sich am besten an einen Dienstleister Ihres Vertrauens oder ein Beratungsunternehmen für IT Sicherheit. Beispielhaft kann hier die Adresse <http://www.she.net> für einen solchen Anbieter genannt werden.

Weitere Informationen erhalten sich auch vom Bundesamt für Sicherheit in der Informationstechnologie (<http://www.bsi.bund.de>).

Private Anwender können sich nähere Informationen unter der Adresse <http://www.bsi-fuer-buerger.de> (eine Webseite des Bundes-

amtes, die sich an den privaten Anwender wendet) besorgen. Den Fragebogen, den ich auf meiner Homepage <http://www.hg-schaller.de> veröffentlicht habe, soll als erster Einstieg und zur Sensibilisierung für dieses Thema dienen.

❖ Haftungsausschluss

Die nachfolgenden Informationen wurden sorgfältig recherchiert und geprüft. Jedoch kann ich für Richtigkeit, Vollständigkeit und Aktualität der enthaltenen Informationen keine Garantie oder Haftung übernehmen.

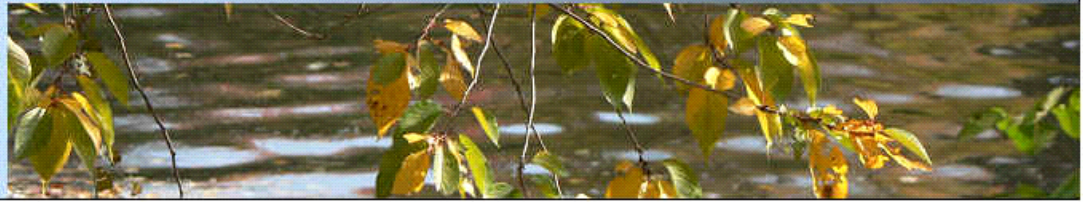
Die gegebenen Informationen stellen den Stand der mir verfügbaren Informationen zum 15. April 2006 dar, und unterliegen keiner ständigen Kontrolle und werden nicht laufend aktualisiert.

Insbesondere sind die Angaben zu rechtlichen Aspekten eine unverbindliche Information, die in keiner Weise geeignet ist, eine rechtliche Beratung zu ersetzen. Für eine rechtliche Beratung wenden Sie sich bitte an einen Anwalt Ihres Vertrauens.

❖ Verantwortung für IT Sicherheit

Die Verantwortung für die Sicherheit in der Informationstechnik für ein Unternehmen liegt bei der Geschäftsführung. Diese kann die Verantwortung unter gewissen Einschränkungen an einen Beauftragten für IT Sicherheit delegieren. Der IT Sicherheitsbeauftragte muss nach persönlichen und fachlichen Kriterien für die übertragene Aufgabe geeignet sein, er hat nach Benennung Anspruch auf angemessene Schulung und Ausstattung. Durch die Benennung eines Verantwortlichen für die IT Sicherheit entfällt für die Geschäftsführung keinesfalls die Pflicht, die Arbeit des IT Sicherheitsbeauftragten für die Delegation der Verantwortlichkeit für IT Sicherheit (an einen IT Sicherheitsbeauftragten):

- ⇒ Eignung des Beauftragten
- ⇒ Anspruch auf Schulungen
- ⇒ Anspruch auf angemessene Ausstattung
- ⇒ Regelmäßigen Kontrolle durch Geschäftsführung



Hier lesen Sie:

Wer für IT Sicherheit verantwortlich ist
Seite 1

Bedrohungen für IT Systeme
Seite 3

Risikoanalyse und Schutzbedarf
Seite 5

Über den Autor
Seite 6

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)

beauftragten regelmäßig zu kontrollieren. Unterbleibt diese Kontrolle, so kann die Geschäftsführung, je nach Umständen auch der Geschäftsführer persönlich, für Folgeschäden haftbar gemacht werden. Eventuell kommen auch persönliche strafrechtliche Konsequenzen in Betracht.

Eine persönliche Haftung bzw. strafrechtliche Verfolgung von Mitgliedern der Geschäftsführung bzw. der IT Sicherheitsverantwortlichen ist in der Praxis bisher in Deutschland noch nicht in spektakulären Fällen publik geworden. Neben diesen dramatischen Szenarien kann es durch mangelnde IT Sicherheit zu erheblichen materiellen und immateriellen Schäden (wie Vertrauens- und Image-

Wer interessiert sich für die IT Sicherheit eines Unternehmens?

- ⇒ Banken, Kreditgeber
- ⇒ Wirtschaftsprüfer
- ⇒ Datenschutzaufsicht (staatlich)
- ⇒ Gewerbeaufsicht, berufsständische Kammern, FDA, Arzneimittelaufsicht
- ⇒ Ausschreibungen, Kunden
- ⇒ Versicherungen
- ⇒ Staatsanwalt
- ⇒ Betriebsrat

verluste, Umsatzverluste etc.) kommen. Dabei muss es noch nicht einmal zu einem Schadensfall gekommen sein, schon alleine die Tatsache, dass ein Unternehmen nicht in der Lage ist, ein stimmiges IT Sicherheitskonzept nach zu weisen, kann zu nachhaltigem Vertrauensverlust bei Kunden, Geschäftspartnern, Banken, Behörden etc. und damit zu Schäden für das Unternehmen führen.

Als Nachweis eines geeigneten IT Sicherheitskonzeptes kann eine Selbsterklärung gemäß dem IT Grundschutzhandbuch des BSI = Bundesamt für Sicherheit in der Informationstechnologie (gegebenenfalls ergänzt durch ein Eigen-Audit / externes Audit durch einen IT Si-

cherheitsdienstleister) dienen.

Zu den Aufgaben des Managements im Bereich der IT Sicherheit gehören insbesondere folgende Punkte:

- ⇒ Übernahme der Gesamtverantwortung für IT Sicherheit
- ⇒ Kosten der IT Sicherheit gegen Nutzen abwägen
- ⇒ IT Sicherheit integrieren
- ⇒ Erreichbare IT Sicherheitsziele setzen
- ⇒ IT Sicherheit steuern und aufrechterhalten
- ⇒ Vorbildfunktion

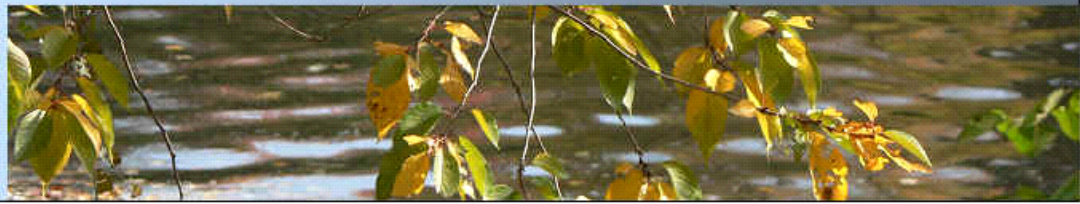
Das Management muss sich daher entsprechende (Grund-) Kenntnisse aneignen, um die grundle-

Relevante Gesetze (IT Sicherheit):

- ⇒ Europäische Richtlinie über Datenschutz bei der elektronischen Kommunikation
- ⇒ Bundesdatenschutzgesetz
- ⇒ Telekommunikationsgesetz
- ⇒ Strafgesetzbuch
- ⇒ Bürgerliches Gesetzbuch
- ⇒ Gewerbeordnung
- ⇒ Handelsgesetzbuch
- ⇒ Urhebergesetz
- ⇒ Jugendschutzgesetz
- ⇒ Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)

Konsequenzen bei mangelhafter IT Sicherheit

- ⇒ Überprüfung durch Behörden
- ⇒ Entzug Gewerbebescheinigung
- ⇒ Einschränkung / Verlust des Versicherungsschutzes
- ⇒ Reputationsverlust
- ⇒ schlechtere Kreditkonditionen (Basel II)
- ⇒ Schadenersatz
- ⇒ Bußgeld / Haft- bzw. Geldstrafe
- ⇒ Arbeitsgerichtsverfahren (Beweisproblematik)



Hier lesen Sie:

**Wer für IT Sicherheit verantwortlich ist
Seite 1**

**Bedrohungen für IT Systeme
Seite 3**

**Risikoanalyse und Schutzbedarf
Seite 5**

**Über den Autor
Seite 6**

**Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)**

genden Aufgaben, insbesondere die Überwachung des IT Sicherheitsbeauftragten wahrnehmen zu können.

❖ **Bedrohungen eines IT Systems**

Die Grundbedrohungen, denen ein IT System ausgesetzt ist, sind:

- ⇒ unbefugter Informationsgewinn (Verlust der **Vertraulichkeit**)
- ⇒ unbefugte Modifikation von Informationen (Verlust der **Integrität**)
- ⇒ unbefugte Beeinträchtigung der Funktionalität (Verlust der **Verfügbarkeit**)

Die intensive IT Unterstützung der Geschäftsprozesse ist in einem modernen Unternehmen heutzutage unverzichtbar. Dieses bedeutet andererseits, dass Unternehmen dementsprechenden Risiken ausgesetzt sind: Diebstahl von Kunden- und Forschungsdaten (digitalen Vermögenswerten) durch Dritte oder Verfälschung der Daten oder IT Anwendungen durch dazu unbefugte Personen. Darunter fällt auch das Risiko, dass Mitarbeiter des Unternehmens Programme oder Daten unter Verletzung des Urheberrechtes Dritter (aus dem Internet herunter geladen) wider-

rechtlich auf das IT System des Unternehmens einspielen. Damit kann das Unternehmen unter Umständen schadenersatzpflichtig werden.

IT Risiken

- Datenverlust
- Verfälschung von Daten
- Spionage
- = **Verlust digitaler Unternehmenswerte**
- Datenmissbrauch
- Urheberrechtsverletzungen
- = **(Straf-) rechtliche Relevanz**

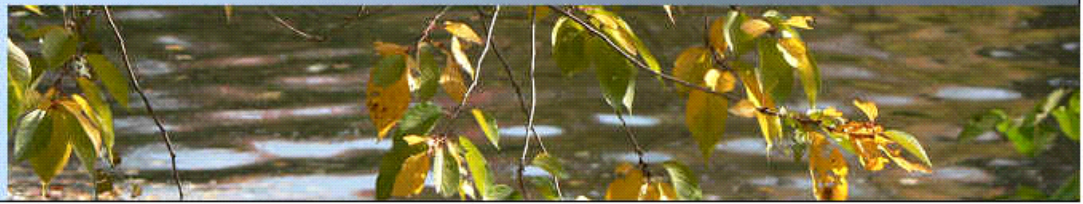
Der dritte Bereich der IT Risiken ist der Bereich „Verfügbarkeit“. Dazu gehört, dass die eingesetzten Programme zur Geschäftsabwicklung und zur Kommunikation einwandfrei funktionieren und die damit verwalteten Daten ordnungsgemäß zur Verfügung stehen. Ein Beispiel für die damit verbundenen Problematik: ein Hersteller pharmazeutischer Produkte muss zulassungsrelevante Daten aus dem Labor, und das sind Daten, die heutzutage häufig digital erhoben werden, für einen Zeitraum von 20 Jahren so archivieren, dass sie jederzeit im Originalzustand wieder hergestellt werden können. Ansonsten drohen Strafen wie der Widerruf der Zulassung. Das kann in der

Praxis so weit gehende Folgen haben, dass das Unternehmen in seiner wirtschaftlichen Existenz gefährdet wird.

Ähnliche Anforderungen, wenn auch in der Regel mit nicht so drastischen Ausmaßen und Konsequenzen, bestehen für Daten im Bereich der Finanzadministration (insbesondere Steuern) und im Vertragswesen. Daher ist das Management verpflichtet, diesem Aspekt besondere Aufmerksamkeit zu widmen.

Der Schutz gegen Datenverlust, allgemeiner gesehen, die Gewährleistung der Verfügbarkeit der IT Systeme, kann, je nach den definierten Anforderungen an Verfügbarkeit und (Langzeit) Datenspeicherung, zu sehr hohen Kosten führen. Hier ist an Schutzmaßnahmen gegen eine große Bandbreite von Bedrohungen zu denken, die vom Diebstahl über Fehlbedienung von Programmen bis zu Ereignissen von Elementargewalt (Brand, Wasser, Krieg) reichen.

Generell gilt: die Bedrohungen der IT Systeme können auch mit den besten Sicherheitssystemen nur gemindert, aber nie



Hier lesen Sie:

Wer für IT Sicherheit verantwortlich ist
Seite 1

Bedrohungen für IT Systeme
Seite 3

Risikoanalyse und Schutzbedarf
Seite 5

Über den Autor
Seite 6

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)

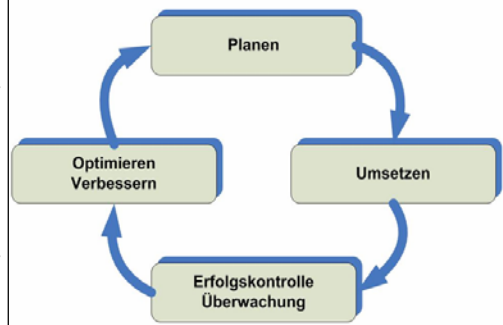
völlig ausgeschaltet werden.

❖ **Management der IT Sicherheit**

Es ist nicht möglich, alle Risiken für die IT Sicherheit zu eliminieren. IT Sicherheit muss daher unter den Aspekten der Kosten-Nutzen Analyse effizient gemanagt werden. In jedem größeren Unternehmen sollte daher

der Aufbau der IT Sicherheitsorganisation festgelegt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Standard für den Aufbau eines ISMS erarbeitet.

Lebenszyklus-Modell eines IT-Sicherheitskonzeptes



mischen Prozess unterworfen. Die Dynamik eines IT Sicherheitsprozesses besteht aus den Schritten:

BSI - Standard 100-1:

Managementsysteme für Informationssicherheit (ISMS) Der vorliegende BSI-Standard 100-1 definiert

- ⇒ Planung der IT Sicherheitsstrategie,
- ⇒ Umsetzung der Planung bzw. Durchführung des Vorhabens,
- ⇒ Erfolgskontrolle bzw. Überwachung der Zielerreichung und
- ⇒ Beseitigung von erkannten Mängeln und Schwächen bzw. Optimierung und Verbesserung.

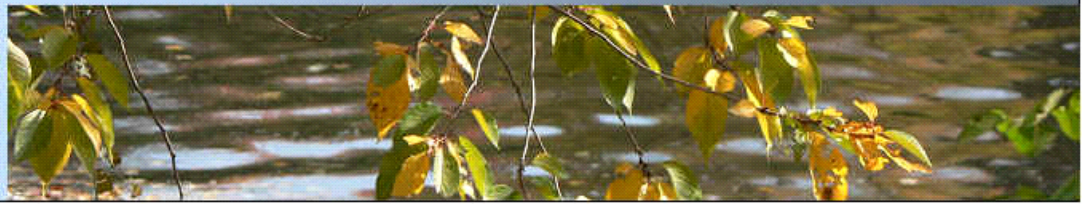
IT-Sicherheitsstrategie als zentrale Komponente des ISMS



ein Managementsystem für Informationssicherheit (ISMS) existieren. Zentrale Aufgabe eines ISMS ist es, die Ziele der IT Sicherheit unter den gegebenen Rahmenbedingungen (technische und finanzielle Ressourcen, Zeit etc.) zu einer IT Sicherheitsstrategie zusammen zu führen. Die IT Sicherheitsstrategie wird in der IT Sicherheitsrichtlinie schriftlich dokumentiert. In dieser Richtlinie werden das IT Sicherheitskonzept und der Auf-

bau der IT Sicherheitsorganisation festgelegt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat einen Standard für den Aufbau eines ISMS erarbeitet. Der vorliegende BSI-Standard 100-1 definiert allgemeine Anforderungen an ein ISMS. Er ist vollständig kompatibel zum ISO-Standard 27001 und berücksichtigt weiterhin die Empfehlungen der ISO-Standards 13335 und 17799. Er bietet Lesern eine leicht verständliche und systematische Einführung und Anleitung, unabhängig davon, mit welcher Methode sie die Anforderungen umsetzen möchten. IT Sicherheit ist jedoch kein statischer Zustand, sondern ist einem dyna-

Die Dynamik in der IT Sicherheit wird eine Veränderung der Anforderungen, Veränderungen in den Bedrohungsszenarien und dem technischen Fortschritt verursacht. So wichtig technische Lösungen für die IT Sicherheit auch sein mögen: durch reine technische Maßnahmen kann keine IT Sicherheit erreicht werden. Die Bausteine eines IT Sicherheitskonzeptes



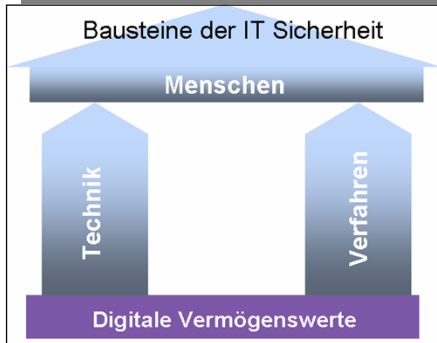
Hier lesen Sie:

Wer für IT Sicherheit verantwortlich ist
Seite 1

Bedrohungen für IT Systeme
Seite 3

Risikoanalyse und Schutzbedarf
Seite 5

Über den Autor
Seite 6



sind die drei wesentlichen Elemente:

Technische Maßnahmen (wie z.B. Firewalls, Virenscanner etc.),
Prozeduren (wie z.B. SOPs für Datensicherung, Zugangsrichtlinien, Management digitaler Rechte etc.) und
Menschen (Passworte, Hacking, Diebstahl etc.).
Alle diese drei Komponenten müssen als Bausteine zueinander passen und gemeinsam gemagnt werden, um ein dem Schutzbedürfnis der digitalen Vermögenswerte eines Unternehmens angepassten Sicherheitsstandard zu gewährleisten.

❖ **Risikobewertung und Schutzbedarf**

Die Maßnahmen, die ein Unternehmen ergreifen muss um ein ausreichendes Niveau in der IT Sicherheit zu erreichen, richten sich nach den individuellen Gegebenheiten. Wichtigste Faktoren sind dabei das Risiko das

für das Unternehmen in jedem der drei vorgenannten Risikobereiche - Vertraulichkeit - Verfügbarkeit - Integrität - besteht.

Im Rahmen einer Risikoanalyse werden zunächst

die potentiellen Risiken für den Verlust von Integrität der Daten, den Verlust der Verfügbarkeit und den Verlust der Vertraulichkeit aufgelistet.

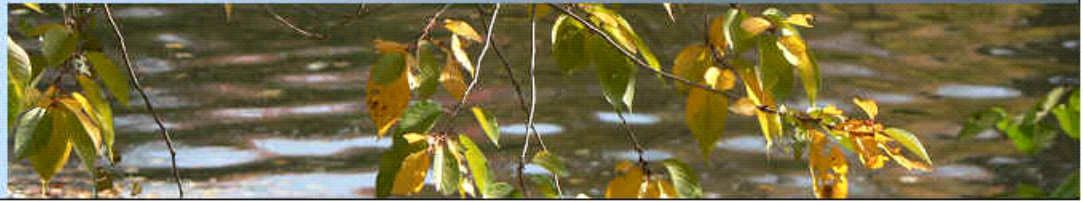
Anschließend werden die bestehenden Risiken hinsichtlich der Eintrittswahrscheinlichkeit des Schadensereignisses und andererseits hinsichtlich des Effektes beim Eintritt des Schadens bewertet. Schadensrisiken, die vermutlich mit hoher Wahrscheinlichkeit eintreten können und andererseits einen hohen (negativen) Effekt nach sich ziehen, bedeuten, dass dieses

Risiko in die Schutzbedarfsklasse „Sehr hoch“ einzustufen ist. Unwahrscheinliche Ereignisse mit zusätzlich auch geringem Schadensereignis sind in die niedrigste Schutzbedarfsklasse „niedrig-mittel“ einzustufen.

Im Rahmen der Konzeption von Sicherheitssystemen in der Informationstechnik werden voneinander unterschieden: Daten, Applikationen (die Programme), Systeme (wie Hardware, Rechner und Datenträger) und IT Räume. Zunächst wird die Schutzbedarfsklasse der Daten und der Applikationen ermittelt. Die jeweils höchste Schutzbedarfsklasse dieser Daten und Applikationen bestimmt die Schutzbedarfsklasse der Systeme, und diese wiederum bestimmt die Schutzbedarfsklasse der IT Räume.

Hinsichtlich der Kommunikationssysteme unter-

Risikoanalyse			
hinsichtlich: Integrität – Verfügbarkeit - Vertraulichkeit			
Effekt eines Schadensereignisses	Hoch	Schutzbedarfsklasse Hoch	Schutzbedarfsklasse Sehr Hoch
	Mittel		
	Niedrig	Schutzbedarfsklasse Niedrig-Mittel	
Effekt Wahrscheinlichkeit	Unwahrscheinlich	Wahrscheinlich	Sehr wahrscheinlich
Wahrscheinlichkeit Schadensereignis			



Hier lesen Sie:

**Wer für IT Sicherheit verantwortlich ist
Seite 1**

**Bedrohungen für IT Systeme
Seite 3**

**Risikoanalyse und Schutzbedarf
Seite 5**

**Über den Autor
Seite 6**

Risikobewertung

- ⇒ Wie intensiv nutzt mein Unternehmen die vorhandene IT-Infrastruktur (intern wie extern)?
- ⇒ Wie abhängig ist mein Kerngeschäft von der Verfügbarkeit der internen IT-Infrastruktur?
- ⇒ Wie abhängig ist mein Kerngeschäft von der Verfügbarkeit des Internets (E-Mail, Online-Banking, Online-Bestellung, Web-Shop etc.)?
- ⇒ Welche digitalen Vermögenswerte besitzt mein Unternehmen?
 - Forschungsdaten
 - Kundendaten
 - Artikeldaten etc.
- ⇒ Gibt es für mein Unternehmen gesetzliche Auflagen zum Datenschutz?
- ⇒ Was kosten mich (direkt messbar UND indirekt)
 - X Stunden Produktivitätsausfall ?
 - Missbrauch vertraulicher Daten ?
 - Entwendung digitaler Vermögenswerte ?

pfligt im Bereich der IT Sicherheit drohen Konsequenzen die von einer persönlichen Haftpflicht bis zu strafrechtlichen Konsequenzen reichen können.

❖ Über den Autor

Dr. Hansgeorg Schaller, Promotion an der Universität Mainz in analytischer Chemie.

Langjährige Tätigkeit bei der Firma Chrompack als Chromatographiespezialist sowie als Vertriebsleiter Deutschland.

Anwenderbetreuung, Kurse in GC, HPLC, GPC, Fehlersuchetechniken, DIN/ISO 9001 Systeme für die Qualitätssicherung.

Anschließend Konzentration auf das e-Business bei den Firmen eLabsEurope (Internet-Marktplatz) und ELEMICA (EDI-Plattform) als Sales Manager und Director Commercial Solutions.

Seit Anfang des Jahres 2005 tätig als Vertriebsbeauftragter für LIM-Systeme bei einem IT-Dienstleister im Rhein-Neckar Raum.

Schwerpunkt: Vertrieb und Marketing von IT Beratungsleistungen und einer hoch komplexen Software.

Kontakt:
post(at)hg-schaller.de
Bitte (at) durch @ ersetzen.

scheidet man im Allgemeinen lediglich zwei Schutzbedarfsklassen: „kritisch“ und „unkritisch“. Sobald ein Kommunikationssystem Daten übermittelt, die als „Schutzbedarfsklasse Hoch“ definiert sind, fällt das Kommunikationssystem in die Klassifizierung „kritisch“.

❖ Zusammenfassung

Erst wenn alle IT Anwendungen im Unternehmen bekannt sind und ihr spezifischer Schutzbedarf ermittelt worden ist, so kann ein sinnvolles IT Sicherheitskonzept erstellt werden. Ein IT Sicherheitskonzept ist ein integ-

riertes Konzept, das die Elemente Technik (Ressourcen), Prozeduren (Arbeitsanweisungen) und Menschen umfassen muss. IT Sicherheit kann niemals durch (isolierte) technische Maßnahmen erreicht werden.

Der Aufwand, der für IT Sicherheit erbracht werden muss, richtet sich nach gesetzlichen Anforderungen, Schadenswahrscheinlichkeit und Schadenseffekt. Es ist die originäre Verantwortung der Geschäftsführung, ein adäquates IT Sicherheitskonzept zu implementieren, im Betrieb zu überwachen und permanent zu optimieren. Bei einer Verletzung der Aufsichts-

Dr. Hansgeorg Schaller
<http://www.hg-schaller.de>
[post\(at\)hg-schaller.de](mailto:post(at)hg-schaller.de)