Anhang

Interessante Tools und Frameworks

„Ein Mann, der recht zu wirken denkt, muss auf das beste Werkzeug halten."
Johann Wolfgang von Goethe, Faust I

Werkzeuge

In diesem Kapitel werden wir exemplarisch einen Blick auf einige Tools und Frameworks werfen, die den Risikomanagement-Prozess erleichtern sollen. Dabei gilt es, den Blick für die Möglichkeiten zu öffnen. Ein vollständiger oder gar abschließender Überblick ist in einem Buch weder sinnvoll noch möglich – der technische Fortschritt nagt zu schnell am Inhalt. Eine umfangreichere Liste mit Tools und Frameworks finden Sie daher im Forum zu diesem Buch.

Das folgende Kapitel wird nur wenige Produkte exemplarisch herausgreifen und ähnlich wie in Kapitel 5 als Steckbrief mit den wichtigsten Eckdaten vorstellen. Während der Recherche zu diesem Buch ist die Liste mit Tools und Frameworks, die interessant sein könnten so lang geworden, dass eine vollständige Behandlung den Rahmen gesprengt hatte. Viele Tools sind in ihrer

S. Klipper, *Information Security Risk Management,* DOI 10.1007/978-3-8348-9870-8,

Nutzbarkeit darüber hinaus so eingeschränkt, dass es wenig erbaulich ist sie hier im Buch vorzustellen.

Eine vollständige Liste finden Sie in der Rubrik *„Tools und Software“*, die Sie im Anwenderforum zum Buch finden:

https://psi2.de/Risikomanagement-das-Buch
(Webseite mit Anwenderforum zum Buch)

Neben Beiträgen zu den hier vorgestellten Methoden finden Sie ebenso Informationen zu den Tools, die hier nicht zum Zuge gekommen sind. Sollten Sie ein Tool kennen, dass dort noch nicht aufgeführt ist, sind Sie herzlich eingeladen, Ihr Wissen mit den anderen Forenteilnehmern zu teilen.

Steckbriefe

Verschaffen Sie sich den Überblick

Die Steckbriefe sollen Ihnen als Nachschlagemöglichkeit und Ideengeber dienen und Sie dabei unterstützen sich einen ersten Überblick zu verschaffen. Im Folgenden sind die vorgestellten Tools daher jeweils auf einem zweiseitigen Steckbrief beschrieben. Es wird jeweils angegeben, bei welchen Schritten des Risikomanagementprozesses das Tool Sie unterstützt. Sie erhalten jeweils Informationen zu Lizenz, Hersteller und Systemvoraussetzungen. Zu jedem Tool folgt schließlich ein Web-Tipp – wie gewohnt mit einem QR-Code über den Sie mit Ihrem Smart-Phone direkt auf die verlinkte Webseite gelangen (siehe die Hinweise in Abschnitt 1.4). Die Links führen jeweils zum passenden Beitrag auf der Webseite zum Buch, wo sie auch eine aktuelle Link-Liste finden. So gelangen Sie jeweils zügig zu den Webseiten mit den aktuellsten Informationen und können sich mit anderen Usern austauschen.

Auswahl des richtigen Tools

Welches Tool oder Framework für Sie und die Situation in Ihrer Firma oder Behörde das richtige ist, hängt von den unterschiedlichsten Faktoren ab, die nicht unbedingt nur etwas mit dem Risikomanagementprozess zu tun haben. Persönliche Vorlieben und Abneigungen sind hier ebenso zulässig, wie bereits gemachte Erfahrungen mit einer Software. In manchen Unternehmen sind Checklisten das Mittel der Wahl.

Übersicht

m Folgenden betrachten wir einige ausgewählte Tools, die jeweils als Beispiel für einzelne Abschnitte in diesem Buch stehen. Alle Tools unterstützen natürlich bei den genannten Phasen des Risikomanagementprozesses.

Security Risk Management Guide (SRMG)

Der Security Risk Management Guide ist ein Leitfaden, der mehrere Tools beinhaltet. Sie stehen exemplarisch für die Assessment-Methoden:

⇒ 5.20 Risikoindizes
⇒ 5.21 Auswirkungs-Wahrscheinlichkeits-Matrix

Security Assessment Tool (MSAT)

Das Security Assessment Tool hilft bei vielen Phasen des Risiko-Assessments. Es dient als Beispiel für die folgenden Abschnitte im Buch:

⇒ Fallbeispiel 4: High-Level Risiko-Assessment
⇒ 5.5 Strukturierte und semistrukturierte Interviews

Common Vulnerability Scoring System (CVSS)

Das Common Vulnerability Scoring System dient der systematischen Bewertung von Schwachstellen und ist ein Beispiel für Abschnitt

⇒ 5.20 Risikoindizes.

Risk Management Framework (chaRMe)

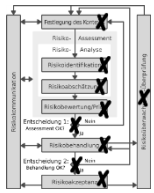
Das Risk Management Framework chaRMe dient der Implementierung eines ISMS nach ISO/IEC 27001 und unterstützt bei der Durchführung eines Risiko-Assessments. Es dienst als Beispiel für die Integration der IT-Grundschutzkataloge. Vergleiche hierzu:

⇒ Kapitel 4 ISO 27005 und BSI IT-Grundschutz

Weitere Tools

Neben diesen Tools werden einige weitere kommerzielle Risiko-Management-Tools genannt und jeweils kurz vorgestellt. Weitere aktuelle Informationen finden Sie jeweils auf der Webseite zum Buch.

Security Risk Management Guide (SRMG)



Unterstützt bei:
Festlegung des Kontexts, Risikoanalyse (Risikoidentifikation, Risikoabschätzung), Risikobewertung/Priorisierung, Entscheidung 1, Risikobehandlung, Entscheidung 2, Risikoakzeptanz, Überwachung und Überprüfung

Version und Hersteller:
- ✓ *SRMG Version 1.2*
- ✓ *Microsoft*

Lizenz:
- ✓ *Creative Commons Attribution-NonCommercial 2.5 Generic*

Systemvoraussetzungen:
- ✓ *Windows 2000 Service Pack 4, Windows Server 2003 oder Windows XP*
- ✓ *Microsoft Office 2003 (Word, Excel)*

Web-Tipp:
https://psi2.de/RM-SRMG
(SRMG im Forum zum Buch)

Vertiefungslektüre

Wie der Name schon sagt handelt es sich beim SRMG in erster Linie um ein Handbuch zum Risikomanagement aus Microsoft-Sicht. Es stellt also im Grunde einen ganz eigenen Standard dar, wie man sich mit Risikomanagement befassen kann. Auf ca. 130 Seiten befasst sich der Guide selbst mit fast allen Punkten, die wir auch in diesem Buch besprochen haben. Es handelt sich daher um eine exzellente Vertiefungslektüre die viele zusätzliche Anregungen und Beispiele bietet.

Tools

Der SRMG liefert vier Office-Tools mit, mit deren Hilfe man sich durch den Risikomanagementprozess arbeiten kann:

- ⇒ Tool 1 – Vorlage zur Datensammlung
- ⇒ Tool 2 – Risiko Level Zusammenfassung
- ⇒ Tool 3 - Detailed Level Risk Prioritization
- ⇒ Tool 4 – Projektplan

Tool 1

Das *Data Gathering Template* (SRMGTool1-Data Gathering Tool.doc) unterstützt insbesondere bei der Festlegung des Kontexts.

Tool 2

In der Phase des Risiko-Assessments unterstützt das *Summary Level Risk Analysis Worksheet* (SRMGTool2-Summary Risk Level.xls) bei der ersten Iteration des Risikomanagementprozesses.

Tool 3

Das *Detail Level Risk Analysis Worksheet* (SRMGTool3-Detailed Level Risk Prioritization.xls) liefert eine detaillierte Systematik Abschätzung und Priorisierung der Risiken und passt gut zu den in Kapitel 5 vorgestellten Methoden (unter Anderem 5.20 Risikoindizes und 5.21 Auswirkungs-Wahrscheinlichkeits-Matrix).

Tool 4

Schließlich liefert der *Sample Project Schedule* (SRMGTool4-Sample Project Schedule.xls) einen rudimentären Projektplan.

Weitere Inputs

Der SRMG liefert für interessierte Leser vor allem weitere Inputs und zusätzliche Anwendungsbeispiele, wie man Risikomanagement umsetzen kann. Ebenso sind einige Listen mit beispielhaften Bedrohungen, Schwachstellen und Assets enthalten.

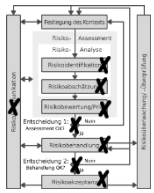
Entscheidungsvorbereitung

In Chapter 5 widmet sich der SRMG ausführlich dem Thema Entscheidungsvorbereitung, das in die folgenden sechs Phasen aufgeteilt wird:

- ⇒ Funktionale Anforderungen definieren
- ⇒ Maßnahmen auswählen
- ⇒ Maßnahmen und Anforderungen gegenüberstellen
- ⇒ Abschätzen der Risikoreduktion
- ⇒ Abschätzen der Kosten
- ⇒ Festlegung der Risikostrategie

Während dieser Phasen sammelt das Risikomanagement-Team alle für eine Entscheidung wichtigen Informationen zu den betrachteten Risiken und gibt eine Empfehlung zur Risikobehandlung ab. Insbesondere In Chapter 5 liefert der SRMG Lösungsansätze, die über die aus ISO/IEC 27005 hinausgehen.

Security Assessment Tool (MSAT)



Unterstützt bei:
Risikoanalyse (Risikoidentifikation, Risikoabschätzung), Risikobewertung/Priorisierung, Entscheidung 1, Risikobehandlung, Entscheidung 2, Risikoakzeptanz, Risikokommunikation

Version und Hersteller:
- ✓ *MSAT Version 4.0*
- ✓ *Microsoft*

Lizenz:
- ✓ *Microsoft Lizenz (kostenlos)*

Systemvoraussetzungen:
- ✓ *Microsoft Windows ab Windows 2000/XP*
- ✓ *.NET Framework Version 3.5*

Web-Tipp:
https://psi2.de/RM-MSAT
(MSAT im Forum zum Buch)

Unterstützung fürs Assessment

Das Microsoft Security Assessment Tool soll Organisationen darin unterstützen, Schwachstellen in der aktuellen IT-Sicherheitsumgebung zu bewerten. Auch wenn für Deutschland keine Unterstützung mehr für das Tool gibt und die Microsoft Webseite behauptet, das Microsoft Security Assessment Tool würde in Deutschland für Kunden in Deutschland keine Auswertung mehr liefern: Wer des Englischen mächtig ist, bekommt auch hierzulande einen Bericht.

Mehr als 200 Fragen

MSAT ist eine Assessment-Methode die auf Fragebögen setzt und damit zu den Interview-Methoden zählt (siehe 5.5). MSAT umfasst mehr als 200 Fragen zu Infrastruktur, Anwendungen, Betrieb und Mitarbeitern. MSAT beleuchtet in den Fragen die folgenden Themengebiete:

⇒ Infrastruktur
⇒ Anwendungen
⇒ Betrieb
⇒ Mitarbeiter

Risikoindizes

Nach der Beantwortung der Fragen liefert das Tool in den Berichten unter anderem die zwei Risikoindizes (siehe 5.20):

⇒ Business Risk Profile, BRP
⇒ Defense-in-Depth-Index (DiDI)

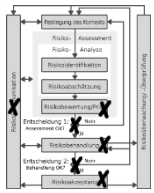
Mit dem BRP wird das geschäftliche Risiko ermittelt; Der Defense-in-Depth-Index bewertet, wie ausgereift die Sicherheitsarchitektur des betrachteten Unternehmens ist.

Übersichten, Tipps und Prioritätenliste

Darüber hinaus beinhaltet ein Bericht eine ganze Reihe von grafischen Übersichten, Best Practices und Handlungsempfehlungen zu den zuvor abgefragten Themengebieten. Am Ende des Berichts steht eine Liste priorisierter Maßnahmen, die für die betrachtete Organisation in Zukunft am wichtigsten sind.

MSAT deckt potenzielle Risikobereiche großflächig ab, statt ins Detail zu gehen. Der Ergebnisbericht soll als vorläufiger Leitfaden dienen, um zu ermitteln, welche Bereiche in Zukunft einer besonderen Aufmerksamkeit bedürfen.

Common Vulnerability Scoring System (CVSS)



Unterstützt bei:
Risikobewertung/Priorisierung, Entscheidung 1, Risikobehandlung, Entscheidung 2, Risikoakzeptanz, Risikokommunikation

Version und Hersteller:
- ✓ *CVSS v2*
- ✓ *Forum of Incident Response and Security Teams (FIRST)*

Lizenz:
- ✓ *Offenes Framework*
- ✓ *CVSS-Rechner mit unterschiedlichen Lizenzen erhältlich*

Systemvoraussetzungen:
CVSS-Rechner sind für unterschiedliche Plattformen und als Web-Anwendung erhältlich

Web-Tipp:
https://psi2.de/RM-CVSS
(CVSS im Forum zum Buch)

Risikoindex

Mit CVSS-Scores werden üblicherweise Soft- oder Hardware-Schwachstellen bewertet. CVSS-Scores gehören zu den Risikoindizes, wie wir sie in Steckbrief 5.20 kennengelernt haben. Das Common Vulnerability Scoring System (CVSS) ist ein offenes Framework, das Schwachstellen aus verschiedenen Perspektiven mit einem standardisierten Wert einordnet. Dieser setzt sich aus mehreren anderen Werten (Subscores) zusammen, die drei Gruppen angehören: Base, Temporal und Environmental – also Basis, Temporär und Umgebung. Der CVSS-Score selbst ist dann

eine Zahl zwischen 0 und 10. Die drei Subscores werden als Zahlwert oder als Vektor dargestellt.

Base Score Metrics

Mit den Base Score Metrics wird bewertet, wie leicht oder schwer ein Angriff auf eine Schwachstelle durchzuführen ist und welchen Schaden man dadurch anrichten kann.

Environmental Score Metrics

Die Environmental Score Metrics berücksichtigen, inwieweit ein Unternehmen oder eine Behörde einem Angriff ausgeliefert ist und welchen Schutzbedarf es hat.

Temporal Score Metrics

Die Temporal Score Metrics schließlich bewerten, ob eine Schwachstelle bereits gepatcht ist oder nicht. Handelt es sich nur um eine Idee für einen Angriff oder wurde schon bewiesen dass der Angriff funktioniert?

Transparenz

Mit CVSS-Scores kann man Entscheidungen bezüglich der Priorisierung von Schwachstellen transparent machen.

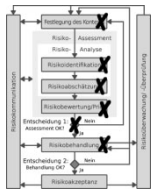
CVSS-Rechner

Damit die Arbeit mit den Vektoren leichter fällt, gibt es eine ganze Reihe von Tools, mit denen man schnell produktiv werden kann.

Fazit

Mein Favorit ist der Plattform unabhängige CVSS-Calculator von Goebel Consult. Für private Nutzung und für die Nutzung in Unternehmen bis 49 Mitarbeitern ist das Tool kostenlos und es kann CVSS-Vektoren mit cut-and-paste verarbeiten.

Risk Management Framework chaRMe



Unterstützt bei:
Festlegung des Kontexts, Risikoanalyse, Risikobewertung/Priorisierung, Entscheidung 1 und Risikobehandlung

Version und Hersteller:
- ✓ *chaRMe Version 0.7*
- ✓ *secopan UG (haftungsbeschränkt)*

Lizenz:
- ✓ *GNU Affero General Public License (AGPL) Version 3*

Besondere Systemvoraussetzungen:
chaRMe läuft in einer eigenen virtuellen Maschine und benötigt daher eine VMware Virtualisierungsumgebung. Das Tool kann als Online-Demo ausprobiert werden.

Web-Tipp:
https://psi2.de/RM-chaRMe
(chaRMe im Forum zum Buch)

Online-Demo

chaRMe ist ein Open Source Framework, das bei der Implementierung eines ISMS nach ISO/IEC 27001 unterstützt. In der aktuellsten Version 0.7.1 es auch als Online-Demo verfügbar.

Anmeldung

Wer das Tool ausprobieren möchte, muss sich registrieren. Hat man diesen Schritt hinter sich, kann man sich am System anmelden und landet direkt im Hauptmenü.

Der erste Eindruck

Das Hauptmenü ist aufgeräumt und übersichtlich. Es dient hauptsächlich dazu, Assessments anzulegen und zu verwalten.

Daneben stehen die Menüpunkte Gefährdungen, Maßnahmen und Assets zur Verfügung.

Gefährdungen

Hinter der Schaltfläche Gefährdungen verbirgt sich eine Teilmenge der Gefährdungen aus den BSI IT-Grundschutzkatalogen. Damit geht das Tool einen ähnlichen Weg, wie er auch in Kapitel 4 vorgeschlagen wurde.

Maßnahmen

Als Maßnahmen wurden die Controls der ISO/IEC 27002 erfasst. Darüber hinaus können jederzeit zusätzliche Maßnahmen definiert werden, die sich aus dem Risikomanagementprozess ergeben.

Assets

In der Ansicht Assets schließlich können die Assets definiert und mit den Gefährdungen verknüpft werden.

Assessment

Herzstück von chaRMe ist die Durchführung von Assessments. Von der Festlegung des Kontexts bis zur Risikobehandlung wird der Risikomanagementprozess nachgebildet:

- ⇒ Definition des Geltungsbereichs
- ⇒ Compliance Anforderung definieren
- ⇒ Inventar erfassen
- ⇒ Risikoanalyse
- ⇒ Globale Maßnahmen festlegen
- ⇒ Weitere Maßnahmen
- ⇒ Risikobehandlung
- ⇒ Dokumentation

Fazit

chaRMe ist bereits in seiner Version 0.7 eine echte Unterstützung fürs Risikomanagement und wird bereits erfolgreich in mehreren deutschen Unternehmen eingesetzt und ist auf dem besten Weg in Richtung einer Version 1.0.

Weitere Tools

Im Folgenden finden Sie eine Übersicht über weitere Risikomanagement-Tools. Es handelt sich dabei überwiegend um kostspielige Enterprise-Lösungen, deren Kauf für den Einzelfall genau abzuwägen ist.

Kleine Marktübersicht

Mehr als eine kleine Marktübersicht kann diese Auflistung allerdings nicht sein. In der Vergangenheit hat sich leider gezeigt, dass auch vielversprechende Lösungen im Sande verlaufen sind und von neuen verdrängt wurden. Bisher hat sich kein Produkt so positionieren können, dass man nicht daran vorbei käme. Aus diesem Grund findet sich der aktuelle Abschnitt auch im Anhang. Es handelt sich damit nicht um ein Kapitel im eigentlichen Sinne, sondern um zusätzliche Informationen.

Secricon Risk Management Software

Hersteller:
Secricon GmbH

Es handelt sich bei der Secricon Risk Management Software streng genommen um mehrere Tools: Entweder als webbasierte Datenbank-Lösung oder in Excel-Form. Die Software ist dabei Teil einer Beratungsleistung.

Web-Tipp:
https://psi2.de/RM-Secricon
(Weitere Informationen im Forum zum Buch)

Lumension Risk Manager

Hersteller:
Lumension INC.

Lumension Risk Manager ist eine Software, die Unternehmen dabei unterstützt ihre Prozesse bei Audit und Risikomanagement zu organisieren.

Web-Tipp:
https://psi2.de/RM-Lumension
(Weitere Informationen im Forum zum Buch)

Proteus

Hersteller:
Infogov Ltd

Proteus ist eine webbasierte Software für Information Risk Management, Compliance und Security. Sie unterstützt bei Compliance und Business Impact Analysen, Risk Assessment, Business Continuity und Incident Management.

Web-Tipp:
https://psi2.de/RM-Proteus
(Weitere Informationen im Forum zum Buch)

Modulo Risk Manager (NG)

Hersteller:
Modulo

Der Risk Manager (Next Generation) ist eine Plattform zur Konsolidierung und Verbesserung der Prozesse zu IT-Governance, Risikomanagement und Compliance.

Web-Tipp:
https://psi2.de/RM-Modulo
(Weitere Informationen im Forum zum Buch)

STEAM

Hersteller:
Acuity Risk Management

Die Risikomanagement Software STEAM ist als leistungsfähige Mehrbenutzerversion erhältlich, kann jedoch auch für kleinere Organisationen als Single-User-Version erworben werden. STEAM bietet Risk Management, Compliance Management, Events Management und Metrics Management unter einem Dach und unterstützt damit das gesamte Risiko-Assessment.

Web-Tipp:
https://psi2.de/RM-STEAM
(Weitere Informationen im Forum zum Buch)

risk2value

Hersteller:
avedos business solutions GmbH

„Integriertes Governance-, Risiko- und Compliance-Management statt zahlreicher Insellösungen“, das verspricht das Management-System aus dem Hause avedos.

Web-Tipp:
https://psi2.de/RM-risk2value
(Weitere Informationen im Forum zum Buch)

BPSResolver ERM

Hersteller:
BPSResolver

Das Enterprise Risk Management von BPSResolver unterstützt bei der Identifikation, Analyse und Behandlung von Risiken. Die Software kann „out of the box“ erworben werden oder als angepasste Unternehmenslösung inklusive Produktschulung. ERM ist Teil einer modular aufgebauten Produktreihe für Governance, Risk und Compliance.

Web-Tipp:
https://psi2.de/RM-BPSResolver
(Weitere Informationen im Forum zum Buch)

Risk Watch

Hersteller:
Riskwatch International

Im September 2010 hat Riskwatch die neue Version seiner Software für Security Risk-Assessment und Risikoanalyse vorgestellt.

Web-Tipp:
https://psi2.de/RM-Riskwatch
(Weitere Informationen im Forum zum Buch)

Risk Management Studio

Hersteller:
Stiki Information Security

Risk Management Studio ist für Unternehmen und Behörden, die Unterstützung bei Asset Management und Risk-Assessment benötigen. Das Risk Management Studio enthält darüber hinaus Tools, die beim Projektmanagement, bei Audit und Reporting helfen.

Web-Tipp:
https://psi2.de/RM-Studio
(Weitere Informationen im Forum zum Buch)

RA2 Art of Risk

Hersteller:
ÆXIS Security Consultants

RA2 art of risk ist ein einfaches Risikomanagement Tool, das bei der Implementierung eines ISMS mit Risikomanagementsystem unterstützt.

Web-Tipp:
https://psi2.de/RM-
(Weitere Informationen im Forum zum Buch)

OCTAVE

Hersteller:
Carnegie Mellon Universität in Zusammenarbeit mit CERT/CC

OCTAVE ist eine Methode zur Evaluation der IT-Sicherheit von Organisationen. Sie liefert als Ergebnis eine strategische Beurteilung und Planung für Informationssicherheit. Basis der Beurteilung ist eine Risikoanalyse, für deren Durchführung das DFN-CERT Formulare zur Verfügung stellt.

Web-Tipp:
https://psi2.de/RM-OCTAVE
(Weitere Informationen im Forum zum Buch)

Zusammenfassung

Gratwanderung

Eine Marktübersicht im Bereich von Risikomanagement-Software unterliegt einem Problem: Keines der Tools kann man uneingeschränkt empfehlen – schon gar nicht generell. Dazu sind die Anforderungen in Unternehmen und Behörden zu unterschiedlich. Was für das eine Unternehmen die perfekte Software ist, kann im anderen Unternehmen zu Frust und Enttäuschung führen. Daher sind Empfehlungen in diesem Fall schwer vorstellbar und müssen auf den Einzelfall beschränkt bleiben. Trotz allem gehört es zu der Beschäftigung mit Information Security Risk Management dazu, dass man sich mit den Möglichkeiten der Softwareunterstützung beschäftigt. Dieser Anhang besteht dabei aus zwei Anteilen: vier konkrete Beispiele und elf Anregungen:

4 Beispiele

Die ersten vier vorgestellten Tools dienen als konkrete Beispiele für einige Abschnitte des Buchs. Daher wurden sie etwas genauer beschrieben. Insbesondere sind sie frei verfügbar[37].

11 Anregungen

Die darüber hinaus kurz vorgestellten Tools sollen Ihnen einen ersten Anhaltspunkt geben, was der Markt sonst noch zu bieten hat. Mit den Beiträgen aus dem Forum zum Buch können Sie sich weitere Informationen zu den Tools heranziehen. Sie finden dort auch Hinweise auf weitere Softwareprodukte.

Markt in Bewegung

Die Europäische Agentur für Netzwerk- und Informationssicherheit (ENISA) stellt seit einigen Jahren eine Übersicht über Risikomanagement-Tools zur Verfügung, die einen Markt in Bewegung dokumentiert. Viele der dort aufgeführten Tools sind bereits vom Markt verschwunden oder werden bereits seit Jahren nicht mehr gepflegt. Diesem Änderungsdruck kann ein gedrucktes Buch nicht standhalten. Nutzen Sie daher zur weiteren Recherche das Forum zum Buch als erste Anlaufstelle für zusätzliche und vor allem aktuelle Informationen.

---

[37] Details siehe Lizenzbestimmungen der Hersteller.

Anhang

Sachwortverzeichnis

"Einmal ausgesprochen, fliegt ein Wort unwiderruflich davon."
Horaz

Mit einem Sachwortverzeichnis kann man verschiedene Ziele verfolgen. Ein Hauptziel ist es, ein Nachschlagen von Sachwörtern zu ermöglichen. Damit soll verhindert werden, dass die Prophezeiung von Horaz auch für geschriebene Worte in Erfüllung geht. Ein anderes Ziel kann es sein, Lust zu machen, an einer bestimmten Stelle nachzuschlagen, ein weiteres, eine Stelle wiederzufinden, an die man sich nicht mehr richtig erinnern kann. Neben vielen anderen Verweisen enthält es auch die Stichworte, die im gesamten Buch jeweils am Seitenrand enthalten sind. So finden Sie schnell, was Sie suchen.

S. Klipper, *Information Security Risk Management,* DOI 10.1007/978-3-8348-9870-8,

Anhang

Abkürzungsverzeichnis

„Die Jüngeren rennen zwar schneller, aber die Älteren kennen die Abkürzung."
Ursula von der Leyen

A

AG
: Aktiengesellschaft

ALARP
: As low as reasonably practicable

ALE
: Annual Loss Expectancy

B

BDSG
: Bundesdatenschutzgesetz

BIA
: Business Impact Analysis

BSI
: Bundesamt für Sicherheit in der Informationstechnik

BRP
: Business Risk Profile

C

CD
: Committee Draft

chaRMe
: --

CISO
: Chief Information Security Officer

S. Klipper, *Information Security Risk Management,* DOI 10.1007/978-3-8348-9870-8,

CCP
Critical Control Points

CVSS
Common Vulnerability Scoring System

D

DiDI
Defense-in-Depth-Index

DIS
Draft International Standard

E

ETA
Event Tree Analysis

F

FCD
Final Committee Draft

FDIS
Final Draft International Standard

FMEA
Failure Mode and Effects Analysis

FMECA
Failure Mode Effects and Criticality Analysis

FN
Frequency, N

FTA
Fault Tree Analysis

G

GNU
GNU is not UNIX

H

HACCP
Hazard Analysis and Critical Control Points

HAZOP
Hazard and Operability

HRA
Human Reliability Analysis

I

ICT
Information and Communications Technology

IRBC
Information and Communications TechnologyReadiness for Business Continuity

ISMS
Information Security Management System

ISO
International Organization for Standardization

IEC
International Electrotechnical Commission

ITIL
Information Technology Infrastructure Library

L

LOPA
Layer of Protection Analysis

M

MSAT
Microsoft Security Assessment Tool

N

NASA
National Aeronautics and Space Administration

NP
New Project

O

OSSIEM
Open Source Security Information and Event Management

P

PDCA
Plan Do Check Act

PDF
Portable Ducument Format

PHA
Preliminary Hazard Analysis

Q

QR
Quick Response

R

RCA
Root Cause Analysis

RCM
Reliability Centered Maintenance

RCO
Real Cost of Ownership

ROISI
Return on Information Security Investment

ROSI
Return on Security Investment

RZ
Rechenzentrum

S

SA
Sneak Analysis

SANS
System Administrator, Networking and Security

SCI
Sneak Circuit Analysis

SIEM
Security Information and Event Management

SPAM
Spiced Pork and Meat

SRM
Security Risk Management

SRMG
Security Risk Management Guide

SWIFT
Structured what if

T

TAM
Threat Analysis & Modeling

TBO
Total Benefit of Ownership

TEI
Total Economic Impact

TCO
Total Cost of Ownership

U

URL
Uniform Resource Locator

W

WD
Working Document

WLAN
Wireless Local Area Network

Anhang

Literaturverzeichnis

„Von den meisten Büchern bleiben nur Zitate übrig.
Warum nicht gleich nur Zitate schreiben?“
Stanisław Jerzy Lec

1. **Klipper, Sebastian.** *Konfliktmanagement für Sicherheitsprofis.* Wiesbaden : Vieweg+Teubner, 2010.
2. **Thaler, Richard H. und Sunstein, Cass R.** *Nudge - Wie man kluge Entscheidungen anstößt.* Berlin : Econ, 2009.
3. **Klipper, Sebastian.** Business-Case Information-Security. <*kes*> *Die Zeitschrift für Informations-Sicherheit.* 2009, Ausgabe Nr. 3.
4. **(ISO), International Organization for Standardization.** *International Standard ISO/IEC 27001:2005(E) – Information technology; Security techniques; Information security management systems; Requirements.* 2005.
5. —. *International Standard ISO/IEC 27005:2008(E) – Information technology; Security techniques; Information security risk management.* 2008.

S. Klipper, *Information Security Risk Management,* DOI 10.1007/978-3-8348-9870-8,

6. —. *International Standard ISO/IEC 27000:2009(E) – Information technology; Security techniques; Information security managementsystems; Overview and vocabulary.* 2009.

7. —. *International Standard ISO/IEC 13335-1:2004 – Information technology; Security techniques; Management of information and communications tchnology security - Part 1.* 2004.

8. —. *International Standard ISO/IEC 27002:2005(E) – Information technology; Security techniques; Code of practice for information security management.* 2005.

9. —. *International Standard ISO/IEC TR 18044:2004 – Information technology; Security techniques; Information security incident management.* 2004.

10. —. *ISO Guide 73:2009 – Risk management Vocabulary.* 2009.

11. —. *ISO Guide 2:2004 – Standardization and related activities; General vocabulary.* 2004.

12. —. *International Standard ISO 20000: – Information technology; Service management.* 2005-2010.

13. —. *International Standard ISO 31000:2009 – Risk management; Principles and guidelines.* 2009.

14. —. *International Standard ISO/IEC 31010:2009 – Risk management; Risk assessment techniques.* 2009.

15. **Rumpel, Rainer und Glanze, Richard.** e-Journal of Practical Business Research. *Verfahren zur Wirtschaftlichkeitsanalyse von IT Sicherheitsinvestitionen.* [Online] 2008. http://www.e-journal-of-pbr.de/downloads/wirtschaftlichkeititsecurityrumpelglanze.pdf.

16. **Institute, SANS.** The Top Cyber Security Risks. [Online] 2009. http://www.sans.org/top-cyber-security-risks/?ref=top20.

17. —. Top 20 Internet Security Problems, Threats and Risks. [Online] 2001-2007. http://www.sans.org/top20/2007/.

18. —. Top Ten Cyber Security Menaces for 2008. [Online] 2008. http://www.sans.org/press/top10menaces08.php.

19. **(BSI), Bundesamt für Sicherheit in der Informationstechnik.** *BSI-Standard 100-1, Managementsysteme für Informationssicherheit (ISMS), Version 1.5.* 2008.

20. —. *BSI-Standard 100-2, IT-Grundschutz Vorgehensweise, Version 2.0.* 2008.

21. —. *BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5.* 2008.

22. **Alle, Bianca.** *Effektivität von Brainstorming-Gruppen.* München : GRIN Verlag, 2010.

23. **Mayer, Horst O.** *Interview und schriftliche Befragung: Entwicklung, Durchführung und Auswertung.* München : Oldenbourg, 2009.

24. **Bogner, Alexander, Littig, Beate und Menz, Wolfgang.** *Experteninterviews: Theorien, Methoden, Anwendungsfelder.* Wiesbaden : VS Verlag, 2009.

25. **(IEC), International Electrotechnical Commission.** *Hazard and operability studies (HAZOP studies) - Application guide.* 2001.

26. **Müller, Klaus-Rainer.** *IT-Sicherheit mit System.* Wiesbaden : Vieweg+Teubner, 2008.

27. **Junginger, Markus.** *Wertorientierte Steuerung von Risiken im Informationsmanagement.* Wiesbaden : DUV Verlag, 2005.

28. **Hachtel, Günter und Holzbaur, Ulrich.** *Management für Ingenieure.* Wiesbaden : Vieweg+Teubner, 2010.

29. **Talbot, Julian.** *Security Risk Management: Body of Knowledge.* s.l. : John Wiley and Sons Ltd., 2009.

30. **Ewert, Bernd.** Der Weg zur Risikolandkarte. *<kes> Die Zeitschrift für Informations-Sicherheit.* 2009, Ausgabe Nr. 3.

31. **Homburg, Christian.** *Quantitative Betriebswirtschaftslehre: Entscheidungsunterstützung durch Modelle.* s.l. : Gabler, 2000.

32. **Schulz von Thun, Friedemann.** *Miteinander reden 1 - Störungen und Klärungen.* Reinbek : rororo, 2009.

33. **Michael, Helisch und Dietmar, Pokoyski.** *Security Awareness.* Wiesbaden : Vieweg+Teubner, 2009.

34. **Schwan, Robert.** *Das Konzept des Total Cost of Ownership(tco) in der IT.* s.l. : GRIN Verlag, 2007.

35. **Wild, Martin und Herges, Sascha.** Total Cost of Ownership (TCO) – Ein Überblick, , Seite 7. *Arbeitspapiere WI - Universität Mainz.* 2000, Nr. 1/2000.

36. **Tipton, Harold F. und Krause, Micki.** *Information Security Management Handbook.* s.l. : CRC Press, 2004.

37. **Mizzi, Adrian.** *Return on Information Security Investment, MBA Dissertation.* s.l. : Bezug über www.lulu.com/content/809262.

38. **Microsoft.** TechNet. *Leitfaden zum Sicherheitsrisikomanagement.* [Online] Dezember 2004.

39. **Kossakowski, Klaus-Peter.** Aktion und Reaktion: Das Risiko-Thermostat. *<kes> Die Zeitschrift für Informations-Sicherheit.* 2009, Ausgabe Nr. 1.

40. **Haas, Marcus und Schreck, Jörg.** Kriterien für IT-Compliance-Tools. *<kes> Die Zeitschrift für Informations-Sicherheit.* 2009, Ausgabe Nr. 3.

41. **Kossakowski, Klaus-Peter.** Top-Ten reichen nicht. *<kes> Die Zeitschrift für Informations-Sicherheit.* 2008, Ausgabe Nr.4.

Anhang

GNU General Public License

Die im Buch verwendeten Graphiken, und stammen aus der Software Wordpress 2.9 und stehen unter der GNU General Public License (GPL). Das Symbol wurde auch in der veränderten Form mit einem §-Symbol verwendet.

http://fsf.org
(Webseite der Free Software Foundation)

Version 2, June 1991
Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin St, Fifth Floor, Boston, MA 02110, USA
Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software — to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is

S. Klipper, *Information Security Risk Management,* DOI 10.1007/978-3-8348-9870-8,

covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU General Public License Terms and Conditions for Copying, Distribution, and Modification

0.

This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you". Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1.

You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program. You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2.

You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

1. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

2. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

3. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work

are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program. In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3.

You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

1. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

2. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

3. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.) The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable. If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4.

You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5.

You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6.

Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7.

If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly

through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8.

If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9.

The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10.

If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

11.

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.