

Steinbeis-Hochschule Berlin (Hrsg.) | Lars Geißler

Übersicht über das IT-Sicherheitsmanagement

Transfer-Dokumentation-Report

Impressum

© 2009 Steinbeis-Edition Stuttgart/Berlin

Alle Rechte der Verbreitung, auch durch Film, Funk und Fernsehen, fotomechanische Wiedergabe, Tonträger jeder Art, auszugsweisen Nachdruck oder Einspeicherung und Rückgewinnung in Datenverarbeitungsanlagen aller Art, sind vorbehalten.

TDR Transfer-Dokumentation-Report
Übersicht über das IT-Sicherheitsmanagement

Hrsg.: Steinbeis-Hochschule Berlin, Arbeitskreis TDR

Autor:

Lars Geißler

1. Auflage 2009 Stuttgart/Berlin

ISBN 978-3-941417-08-3

Satz und Gestaltung: Steinbeis-Edition

Druck: Digital Druck Straub GmbH & Co. KG, Ludwigsburg

www.steinbeis-edition.de

133386-2009-11

Übersicht über das IT-Sicherheitsmanagement

SteinbeisBBA

Transfer-Dokumentation-Report
Vertiefungsrichtung



Lars Geißler

Lars Geißler eignete sich, basierend auf einem Studium der Wirtschaftsinformatik (Schwerpunkt Security Management und Systemanalyse), über verschiedenste berufliche Wirkungsbereiche (sicherheitskritisches Forschungsprojekt im Luftfahrtbereich, SAP CERT, Software QA neofonie GmbH, u.a.) ein breites Wissen über das Themenfeld der IT-Security an. Er ist im Rahmen des Steinbeis Business Academy Security Programms als Dozent und bei der webXells GmbH als Geschäftsführer tätig.

Inhaltsverzeichnis

Abbildungsverzeichnis.....	IX
Wissen (vermitteln) alleine genügt nicht.....	X
Aufbau TDR	XI
Transferreport I (unternehmensbezogen)	XII
Transferreport II (projektbezogen)	XIII
Vorwort	XV
1 Einführung	1
2 Bestandteile des IT Security Managements	3
2.1 Organisatorische Sicherheit.....	3
2.1.1 Das CIA-Modell.....	3
2.1.2 Der PDCA-Zyklus.....	4
2.1.3 Die Sicherheitspyramide.....	5
2.1.4 Die Security-Policy	8
2.1.5 Die Sicherheitsorganisation.....	10
2.1.6 Compliance / Externe Sicherheitsanforderungen.....	14
2.1.7 IT Security Governance.....	14
2.1.8 Awareness	16
2.2 Technische Sicherheit	17
2.2.1 Der „sichere Betrieb“ von IT Systemen.....	17
2.2.2 Aktuelle Bedrohungen	21
2.3 Zusammenfassung	24
3 Sicherheitsstrategien, Vorgehensmodelle und Sicherheitspolitik im Unternehmen	26
3.1 Risk Management.....	26
3.2 Incident Management.....	32
3.3 Business Continuity.....	37
3.4 Sicherheitsarchitektur	41
3.5 Zusammenfassung	44
4 Praxisbeispiel: „Sicherung der IT einer Leitstelle“	45
4.1 Die Leitstelle, Lagenzentrum oder Joint Operation Center	45
4.2 Die Bedrohungsanalyse.....	52
4.3 Definition der Sicherheitsziele	56
4.4 Das IT-Sicherheitskonzept	57
4.5 Berichtswesen	60
4.6 Review (Nach dem Notfall ist vor dem Notfall)	63
4.7 Zusammenfassung	64

5 Selbstkontrollaufgaben.....	65
6 Glossar.....	68
7 Quellenverzeichnis	69

Abbildungsverzeichnis

Notizen

Abb. 1:	Einordnung von Sicherheitsmaßnahmen
Abb. 2:	Das CIA-Modell
Abb. 3:	PDCA-Zyklus nach ISO/IEC 27001:2005
Abb. 4:	Sicherheitspyramide nach Dr.-Ing. Klaus-Rainer Müller
Abb. 5:	Hierarchischer Aufbau der Sicherheitspolitiken nach ISO 13335-1
Abb. 6:	Sicherheitsorganisation nach Geschäftsbereichen
Abb. 7:	Sicherheitsorganisation nach geographischer Verteilung
Abb. 8:	Beziehung zwischen der Corporate, IT und Security Governance
Abb. 9:	Risikomanagementprozess
Abb. 10:	Beispiel eines Risikograph
Abb. 11:	Risikograph nach Maßnahmendurchführung
Abb. 12:	Strategie zur Risikosteuerung
Abb. 13:	Der Incident Management Prozess
Abb. 14:	Konzept der Sicherheitsarchitektur
Abb. 15:	Beispiel für ein Joint Operations Center
Abb. 16:	JOC Board
Abb. 17:	Umfeld des JOC
Abb. 18:	KRIMA von Siemens
Abb. 19:	Informations- und Datenmanagement im JOC
Abb. 20:	Mögliche technische Infrastruktur des Lagezentrums
Abb. 21:	Tier-Level im Überblick
Abb. 22:	Erstellung der Sicherheitskonzeption im Informationssicherheitsmanagement
Abb. 23:	Mögliche Bedrohungen für das Lagezentrum
Abb. 24:	Bedrohungsmatrix
Abb. 26:	Detaillierte Auswertung der Bedrohungsmatrix
Abb 27:	Möglicher Risikograph für das Lagezentrum

Wissen (vermitteln) alleine genügt nicht

Steinbeis ist und war von je her dem konkreten Transfer von Technologien und Wissen verpflichtet. Konkret bedeutet das v. a. auch die nutzenorientierte Anwendung von geschaffenem Wissen. Die Wissensvermittlung und das Wissen selbst sind notwendige, lange aber noch nicht hinreichende Bedingung für einen erfolgreichen Transfer.

Bei der Entwicklung des Konzepts des PKS (Projekt-Kompetenz-Studium) haben wir darauf geachtet, dass nicht nur die Aneignung, sondern insbesondere auch die Anwendung von vermitteltem Wissen systembedingt gegeben ist. Daher steht das von uns transferorientiert betreute und in einem Unternehmen (bzw. einer Organisation) durchgeführte Projekt im Mittelpunkt jedes SHB-Studiums.

Erste Erfahrungen im Bachelor-Studiengang haben gezeigt, dass reine stoff anbietende Lehrbriefe im PKS weniger geeignet sind. Wir entwickelten daher das Konzept der TDR (Transfer-Dokumentation-Report). Im Mittelpunkt der TDR steht konsequenterweise der praktische Transfer von bereits dokumentiertem (theoretischem) Wissen in die Praxis, d. h. in das Projekt und somit das Unternehmen. Die eigene Reflexion über sowie die Relevanz theoretischer Fundierung für das Projekt bzw. das Unternehmen wird im Report dokumentiert. Wird die gesamte Theorie notwendigerweise und klassisch in den Prüfungen abgefragt, stellt der Report für den Studenten und dessen Betreuer eine praxisorientierte Prüfung des Transfers dar.

Ich wünsche Ihnen (und auch uns), dass Sie durch die TDR relevantes Wissen für Ihren persönlichen Erfolg und den Ihres Unternehmens, noch besser, nutzenorientiert anwenden können.

Prof. Dr. Dr. h. c. mult. Johann Löhn
Präsident Steinbeis-Hochschule Berlin