

Peter von Oppenkowski

**Analyse sicherheitsrelevanter
Geschäftsprozesse eines Anwendungsfalls
aus der Finanzbranche und Ermittlung der
hierfür geeigneten Methoden**

Bibliografische Information der Deutschen Nationalbibliothek:

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

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Copyright © 2011 Diplomica Verlag GmbH
ISBN: 9783842822931

Peter von Oppenkowski

**Analyse sicherheitsrelevanter Geschäftsprozesse eines
Anwendungsfalls aus der Finanzbranche und Ermittlung
der hierfür geeigneten Methoden**

Peter von Oppenkowski

Analyse sicherheitsrelevanter Geschäftsprozesse eines Anwendungsfalls aus der Finanzbranche und Ermittlung der hierfür geeigneten Methoden

Peter von Oppenkowski

Analyse sicherheitsrelevanter Geschäftsprozesse eines Anwendungsfalls aus der Finanzbranche und Ermittlung der hierfür geeigneten Methoden

ISBN: 978-3-8428-2293-1

Herstellung: Diplomica® Verlag GmbH, Hamburg, 2012

Zugl. Wilhelm-Büchner-Hochschule Darmstadt, Darmstadt, Deutschland, Diplomarbeit, 2011

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt 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.

Die Informationen in diesem Werk wurden mit Sorgfalt erarbeitet. Dennoch können Fehler nicht vollständig ausgeschlossen werden und der Verlag, die Autoren oder Übersetzer übernehmen keine juristische Verantwortung oder irgendeine Haftung für evtl. verbliebene fehlerhafte Angaben und deren Folgen.

© Diplomica Verlag GmbH

<http://www.diplomica.de>, Hamburg 2012

"You can't defend. You can't prevent.

The only thing you can do is detect and respond."

- Bruce Schneier

I. Danksagung

Mein erster und besonderer Dank gilt Herrn Prof. Dr. Thomas Freytag für die Betreuung meiner Diplomarbeit. Weiter danke ich ihm für seine inhaltlichen und konzeptionellen Ratschläge, die mir stets von großer Hilfe waren und mir die nötige Sicherheit zum Gelingen dieser Arbeit gegeben haben.

Ebenso bedanken möchte ich mich bei den beiden Herren Nicolai Kuntze und Roland Rieke vom Fraunhofer-Institut, die mich in das spannende Thema der IT-Sicherheit eingeführt und mir die Gelegenheit gegeben haben, einen Beitrag zu aktuellen Fragestellungen zu leisten.

Ich danke auch meiner Freundin, die mir, trotz dass sie sich in anderen Umständen befindet, während der ganzen Zeit Verständnis entgegengebracht und mir immer ein gutes Gefühl vermittelt hat. Zudem danke ich ihr für die Unterstützung beim Korrekturlesen.

Meinen Eltern möchte ich dafür danken, dass sie immer an mich glauben und mich - wo immer sie nur können - unterstützen.

Zu guter Letzt widme ich diese Arbeit meinem ersten Kind Eleni, dessen schon jetzt stolzer Papa sie noch in diesem Jahr willkommen heißen wird.

II. Inhaltsverzeichnis

I.	Danksagung	
II.	Inhaltsverzeichnis	
III.	Tabellenverzeichnis	
IV.	Abkürzungsverzeichnis	
V.	Abbildungsverzeichnis	
1	Einleitung	1
1.1	Motivation	2
1.2	Ziel und Vorgehensweise der Arbeit.....	3
1.3	Aufbau der Arbeit	3
2	IT-Sicherheit, Bedrohungen und Methoden	4
2.1	Problembereich IT-Sicherheit.....	4
2.1.1	<i>Grundwerte der IT-Sicherheit.....</i>	<i>6</i>
2.1.2	<i>Bedrohungen und Gefährdungen</i>	<i>7</i>
2.1.3	<i>Angriffe und Angreifer.....</i>	<i>8</i>
2.1.4	<i>Risiken und Schwachstellen</i>	<i>13</i>
2.2	Informationstechnologie bei FDL.....	15
2.2.1	<i>Betriebliche Anwendungen.....</i>	<i>16</i>
2.2.2	<i>Vernetzung und verteilte Systeme</i>	<i>17</i>
2.2.3	<i>Sicherheitskritische Geschäftsprozesse und Ereignisse</i>	<i>19</i>
2.2.4	<i>Datenschutz, Datensicherheit und Compliance</i>	<i>20</i>
2.3	Security Information and Event Management (SIEM)	22
2.3.1	<i>Einsatzumfeld von SIEM Lösungen.....</i>	<i>22</i>

2.3.2	<i>Funktionsweise von SIEMs</i>	23
2.3.3	<i>Collection</i>	24
2.3.4	<i>Normalization</i>	25
2.3.5	<i>Aggregation</i>	25
2.3.6	<i>Correlation</i>	26
2.3.7	<i>Reporting</i>	29
2.4	Modellierungsmethode UML	30
2.4.1	<i>Misuse Case Diagramm</i>	30
2.4.2	<i>Mal-Activity Diagramm</i>	31
2.5	Attack-Trees Methode	32
3	Anwendungsfall aus der Finanzbranche	33
3.1	Umfeld und Zugangssysteme der Bank.....	33
3.2	Internetbanking Anwendung.....	36
3.2.1	<i>Internetbanking Überweisung</i>	38
3.2.2	<i>Prozessablauf der Überweisung</i>	40
3.3	Bedrohungsanalyse.....	44
3.3.1	<i>Zugangsdaten des Kunden missbrauchen</i>	44
3.3.2	<i>Kunden austricksen und manipulieren</i>	47
3.3.3	<i>Banksystem kompromittieren</i>	50
3.3.4	<i>Kundenrechner infizieren</i>	51
3.4	Risikoanalyse und Sicherheitsanforderungen	52
3.4.1	<i>Analyse zu Zugangsdaten des Kunden missbrauchen</i>	52
3.4.2	<i>Analyse zu Kunden austricksen und manipulieren</i>	54
3.4.3	<i>Analyse zu Banksystem kompromittieren</i>	55
