Diplomarbeit

Peter von Oppenkowski

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

Diplom.de

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.

ISBN: 9783842822931

Peter von Oppenkowski

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

Diplom.de

Diplomarbeit

Peter von Oppenkowski

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

Diplom.de

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

"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 Grundwerte der IT-Sicherheit 6

2.1.2 Bedrohungen und Gefährdungen 7

2.1.3 Angriffe und Angreifer 8

2.1.4 Risiken und Schwachstellen 13

2.2 Informationstechnologie bei FDL 15

2.2.1 Betriebliche Anwendungen 16

2.2.2 Vernetzung und verteilte Systeme 17

2.2.3 Sicherheitskritische Geschäftsprozesse und Ereignisse 19

2.2.4 Datenschutz, Datensicherheit und Compliance 20

2.3 Security Information and Event Management (SIEM) 22

2.3.1 Einsatzumfeld von SIEM Lösungen 22

2.3.2 Funktionsweise von SIEMs 23

2.3.3 Collection 24

2.3.4 Normalization 25

2.3.5 Aggregation 25

2.3.6 Correlation 26

2.3.7 Reporting 29

2.4 Modellierungsmethode UML 30

2.4.1 Misuse Case Diagramm 30

2.4.2 Mal-Activity Diagramm 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 Internetbanking Überweisung 38

3.2.2 Prozessablauf der Überweisung 40

3.3 Bedrohungsanalyse 44

3.3.1 Zugangsdaten des Kunden missbrauchen 44

3.3.2 Kunden austricksen und manipulieren 47

3.3.3 Banksystem kompromittieren 50

3.3.4 Kundenrechner infizieren 51

3.4 Risikoanalyse und Sicherheitsanforderungen 52

3.4.1 Analyse zu Zugangsdaten des Kunden missbrauchen 52

3.4.2 Analyse zu Kunden austricksen und manipulieren 54

3.4.3 Analyse zu Banksystem kompromittieren 55