Schriftenreihe Risikomanagement
herausgegeben von
Prof. Dr. Bettina Schiller, Dr. Christian Brünger, Dr. Peter Becker
Forschungszentrum für Risikomanagement, Universität Paderborn

Band 2

Nadia Khelil,
Christian Brünger

Compliance-Risiken im Friendly-Hacking

Eine Untersuchung strafrechtlicher Regelungen

Shaker Verlag
Aachen 2012

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

Printed in Germany.

ISBN 978-3-8440-0909-5
ISSN 2193-2123

Shaker Verlag GmbH • Postfach 101818 • 52018 Aachen
Telefon: 02407 / 95 96 - 0 • Telefax: 02407 / 95 96 - 9
Internet: www.shaker.de • E-Mail: info@shaker.de

Vorwort

Die Sicherheit und die Absicherung von IT-Systemen und Netzwerken zählen zu den wesentlichen Herausforderungen des Zeitalters der Informationstechnologie. Der Zugriff und die Verfügbarkeit von Informationen stellen einen Wert dar, der über den Wert materieller Güter hinausgehen kann. Daher besteht für bestimmte Informationen ein starkes Schutzinteresse, welches in IT-Systemen und Netzwerken zu realisieren ist. Zudem stellen Informationsverarbeitungssysteme, wie ERP-, CRM-, DMS- und PPS-Systeme, eine zentrale und wichtige Ressource für Unternehmen dar, die für die Aufrechterhaltung des Geschäftsbetriebs zwingend erforderlich ist. Ein Ausfall dieser Systeme führt zu einer Beeinträchtigung oder gar Unterbrechung des Geschäftsbetriebs. Technische Defekte oder Bedienungsfehler können zu dem Ausfall solcher Informationsverarbeitungssysteme führen. Jedoch kann auch eine unzureichende Sicherheit des IT-Systems oder Netzwerks eine Ursache für einen Systemausfall sein, beispielsweise durch eine Denial-of-Service (DoS) Attacke, die zur Beeinträchtigung bestimmter Bereiche des IT-Systems führen kann. Die Sicherheit von IT-Systemen und Netzwerken ist somit auch vor solchen Aspekten der Betriebskontinuität von besonderer Relevanz.

Die Schaffung von IT-Sicherheit umfasst sowohl die Implementierung und angemessene Konfiguration technischer Lösungen als auch die Umsetzung organisatorischer Maßnahmen und letztlich auch die Sensibilisierung der involvierten Mitarbeiter einer Organisation für Risiken. Firewalls, Intrusion Detection Systeme oder Intrusion Prevention Systeme sind nur einige Beispiele von technischen Methoden und Lösungen, die zur IT-Sicherheit beitragen. Eine Belastungsprobe der implementierten Maßnahmen oder das Erkennen von Sicherheitslücken kann u.a. durch Penetrationstests oder Friendly-Hacking Aktionen erfolgen. Auch wenn die Überprüfung der IT-Sicherheit im Interesse des Unternehmens ist, können hierdurch weitere Risiken, insbesondere Compliance-Risiken, entstehen. Besonders die Nichteinhaltung (Non-Compliance) von strafrechtlichen Regelungen des StGB ist in diesem Zusammenhang relevant. Die vorliegende Publikation zeigt Compliance-Risiken auf, die im Zusammenhang mit Friendly-Hacking auftreten und nennt Maßnahmen, mit denen diese Risiken reduziert werden können.

Der zweite Band unserer Schriftenreihe Risikomanagement ist durch eine interdisziplinäre Zusammenarbeit der wissenschaftlichen Disziplinen Jura, Wirtschaftswissenschaften insb. Risikomanagement und Informatik entstanden. Es soll Lesern aus den Bereichen Geschäftsführung, IT-Leitung, IT-Sicherheit, IT-Administration, Risikomanagement und IT-Beratung eine Hilfestellung sein, um StGB-relevante Compliance-Risiken im Kontext von Friendly-Hacking zu erkennen und entsprechend zu steuern.

Paderborn, im April 2012

Prof. Dr. Bettina Schiller
Dr. Peter Becker
Dr. Christian Brünger

Inhaltsverzeichnis

Abbildungsverzeichnis