Abstract

Das vorliegende Werk betrachtet abweichendes Verhalten Unternehmensangehöriger mit Bezug zu Informations- und Kommunikationssystemen. Die unternehmenspragmatisch ausgelegte Begriffsdefinition umfasst dabei sowohl Rechtsverstöße, d. h. Computersabotage, Betrug und Geheimnisverrat, als auch nicht kriminalisierte, aber doch unternehmensschädigende Verhaltensweisen wie etwa die missbräuchliche private Nutzung eines betrieblich zur Verfügung gestellten Internetzugangs. Die Aufmerksamkeit der breiten Öffentlichkeit, in der Wissenschaft und in Unternehmen, richtet sich in erster Linie auf außerhalb der Unternehmensgrenzen zu lokalisierende Bedrohungen durch Virenprogrammierer oder Hacker. Computerbezogene Delikte werden jedoch in der Mehrzahl der Fälle von den eigenen Mitarbeitern begangen. Vor allem die schwerwiegenden Schädigungen lassen sich zunehmend auf ‚autorisierte' Systemanwender zurückführen.

Zur Klärung der Ursachen und Entstehungsbedingungen von ‚Computer Related Occupational Deviance' wird zunächst ein Erklärungsmodell konstruiert, welches über eine Makro-, Meso- und eine Mikroebene die drei analysierten Schichten Gesellschaft, Unternehmung und Individuum miteinander in Verbindung bringt und die Entstehung abweichender Verhaltensweisen prozesshaft als logische Kette aufeinander folgender Wirkungen interpretiert. Eine wichtige Erkenntnis besteht darin, dass steigende Komplexität und Spezifität organisationsinterner Strukturen und Prozesse infolge einer Individualisierung, Rationalisierung und Technologisierung der Unternehmensumwelt in Verbindung mit rational und opportunistisch agierenden Akteuren die Gefahr der Entstehung von Systemschwachstellen und damit das Viktimisierungsrisiko eines Unternehmens erhöhen. Dessen systematische Reduktion zum Ziel hat der Präventionsteil der Arbeit. Nach einem Vergleich verschiedener Risikoanalyseverfahren wird die Szenarioanalyse als geeignete Methode zur Aufdeckung und Behebung von Sicherheitslücken beschrieben. Darüber hinaus werden in Ergänzung bekannter Referenzwerke für die in der Unternehmenspraxis beliebten Grundschutz-Ansätze unter konsequenter Fortführung der dem konstruierten Erklärungsmodell zugrunde liegenden rationalistischen Logik Vorschläge im Sinne heuristischer Handlungsempfehlungen abgeleitet. Die Maßnahmen zielen darauf ab, die Wahrscheinlichkeit abweichenden Verhaltens durch Verschlechterung des wahrgenommenen Kosten-Nutzen-Verhältnisses von Tatgelegenheiten zu reduzieren.