Rechtliche Grenzen und ethische sowie moralische Bedenken der automatischen Identifikation unternehmensschädlicher Handlungen

Diplomarbeit

zur Erlangung des Grades eines Diplom-Ökonomen der
Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Lebek Vorname: Benedikt

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, den 24. August 2011

I. Inhaltsverzeichnis

1. Einleitung

In der modernen, global vernetzten Wirtschaftswelt werden nahezu alle Geschäftsprozesse auf elektronischem Weg vollzogen. Dabei entsteht eine große Menge sensibler Daten, die von hohem Wert für das jeweilige Unternehmen sind.[1] Es ist daher notwendig, diese Daten gegen Diebstahl, Verlust, Manipulation oder andere Attacken zu schützen. In diesem Zusammenhang rückt die Betrachtung von Angriffen aus dem Inneren des Unternehmens immer weiter in den Fokus. Diese Bedrohung durch Insider, also Personen, die Zugang zu Informationssystem, Daten oder Netzwerk der Organisation haben, ist nicht mehr zu verleugnen. Wie der Abb. 1 zu entnehmen ist, sehen die Teilnehmer des *2007 E-Crime Watch Survey* die eigenen Mitarbeiter als das zweitgrößte Risiko (19%) für die Cybersicherheit von Unternehmen nach Hackerangriffen (26%). Demnach stellen die Mitarbeiter eine deutlich größere Gefahr dar, als die nächst geringere Bedrohung durch z.B. Fremde Instanzen oder ehemalige Mitarbeiter, die jeweils von nur 6% der Befragten genannt wurden.[2]

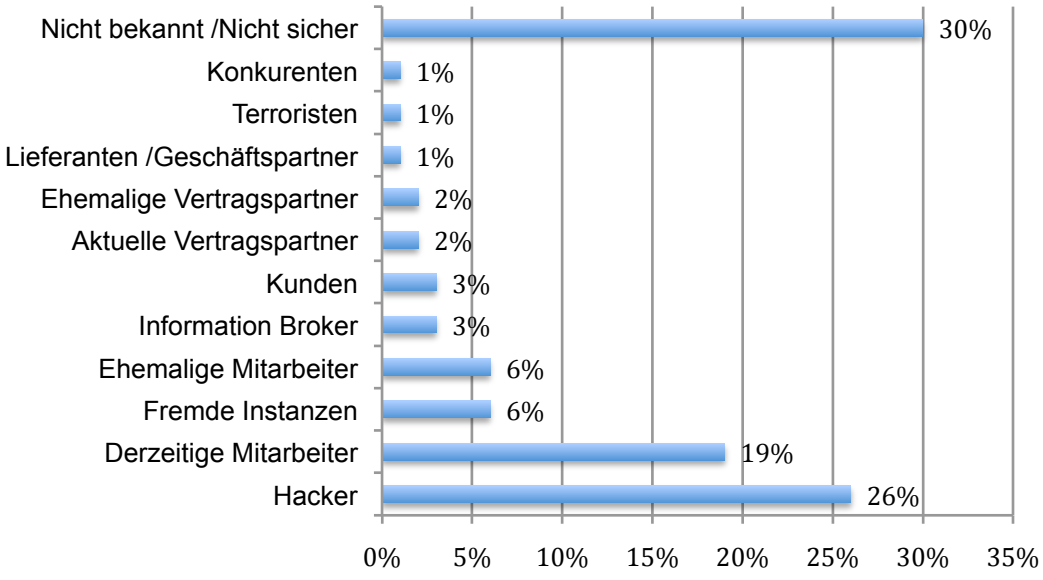

Abb. 1: Cyber Security Threats für Unternehmen
Eigene Darstellung auf Basis der Daten des 2007 e-Crime Survey[3]

[1] Sarkar, Assesing Insider Threats to Information Security Using Technical. Behavorial and Organisational Measures, 2010, S. 112.

[2] CSO Magazine, 2007 E-Crime Watch Survey.

[3] Vgl.: CSO Magazine, 2007 E-Crime Watch Survey, Vierter Abschnitt, Frage 1.

Als eine Folge wird die Einrichtung von Überwachungsmaßnahmen innerhalb des Unternehmens notwendig.[4] In der Praxis steht derzeit noch die Identifizierung von Tätern nach Vollzug der kriminellen oder der fehlerhaften Handlung im Vordergrund.[5] Jedoch liefern diese Methoden oftmals erst zu spät ein Ergebnis, sodass bereits ein irreparabler Schaden für das Unternehmen entstanden ist. In einer schnelllebigen Geschäftswelt in der Echtzeit-Informations- und -buchungssysteme eingesetzt werden, wird nach einer zeitnahen Identifikation von unternehmensschädlichen Handlungen verlangt.[6] In der Literatur wird daher bereits darüber diskutiert, wie potenzielle Betrüger schon vor der Tat identifiziert werden können. Dies basiert auf Verhaltensanalysen und setzt eine starke Überwachung der Mitarbeiter voraus, die auch auf teils sensible Datenquellen, wie beispielsweise E-Mail-Inhalte, zurückgreift. In den letzten Jahren ist die Zahl der Firmen, die Ihre Mitarbeiter elektronisch überwachen, stark gestiegen.[7] Laut dem *2007 Electronic Monitoring & Surveillance Survey* der American Management Association (AMA) überwachen zum Beispiel 43% der Firmen die E-Mails ihrer Mitarbeiter. Davon 96% die ein- und ausgehenden externen E-Mails und immerhin 58% auch die internen E-Mails zwischen einzelnen Mitarbeitern. Wenn es um die Methode der Überwachung geht, so besagt die Umfrage, dass 73% der Firmen eine automatische Kontrolle der E-Mails durchführen und 40% eine manuelle Kontrolle.[8] Eine solch intensive Mitarbeiterüberwachung stößt natürlich auf datenschutzrechtliche Grenzen und wirft ethische und moralische Bedenken auf. Es entsteht eine Spannung zwischen den Zielen der Unternehmen, die Bedrohung durch Insider abzuwehren und somit die Organisation und auch die Mitarbeiter, die keine betrügerischen Absichten haben, zu schützen und dem Recht des einzelnen Mitarbeiters auf Schutz seiner eigenen Privatsphäre oder dem Schutz der Privatsphäre der ihm nahestehenden Personen. Dass dieses Thema durchaus eine hohe Brisanz besitzt, zeigen die Fälle der Deutschen Telekom und der Deutschen Bahn, die im Jahr 2009 Schlagzeilen durch Verletzungen des Datenschutzrechtes machten,

---

[4] Vgl.: Islam et al., Fraud Detection in ERP Sytems Using Scenario Matching, 2010, S. 112.

[5] Vgl.: Greitzer et al., Combining Traditional Cyber Security Audit Data with Psychosicial Datan: Towards Predictive Modeling for Insider Threat Mitigiation, 2011, S. 89.

[6] Flowerday, Continuous auditing technologies and models: A discussion, 2010, S. 325.

[7] Vgl.: Tabak/Smith, Privacy and Electronic Monitoring in the Workplace: A Model of Managerial Cognition and Relational Trust Development, 2005, S. 173.

[8] Vgl.: AMA/e Policy Institute, Electronic Monitoring & Surveillance Survey, 2007, S. 4-5.

als diese unter anderem Kontodaten ihrer Kunden mit denen ihrer Zulieferer verglichen haben.[9] Vor dem Hintergrund der konkurrierenden Interessen von Arbeitgebern und Arbeitnehmer stellt sich die Frage, ob es möglich ist, ein kontinuierliches bzw. automatisches Fraud Auditing aufzubauen, welches insbesondere auch das Mitarbeiterverhalten überwacht und sowohl rechtlichen als auch moralischen Ansprüchen gerecht wird. Hierbei wird insbesondere das deutsche Recht berücksichtigt. Ziel dieser Arbeit wird es sein, diese Frage zu beantworten und anhand des Modells von Greitzer et al. (2010) zu demonstrieren, wo die Problemstellen liegen, und welche möglichen Lösungen sich anbieten.

Zunächst sollen dazu einige Grundlagen definiert werden, die für das allgemeine Verständnis dieser Arbeit notwendig sind. Im Anschluss an den Grundlagenteil werden mehrere Modelle zur automatischen Identifikation unternehmensschädlicher Handlungen durch Mitarbeiter vorgestellt, die in den letzten Jahren veröffentlicht wurden. Der Zweck dabei soll es sein, zu demonstrieren, dass es in diesem Bereich auf der einen Seite unterschiedlichste Ansätze gibt, auf der Anderen Seite allerdings auch Modelle zu finden sind, die gewisse Parallelen aufweisen. In diesem Zusammenhang werden die einzelnen Modelle in einer kurzen Gegenüberstellung anhand einiger Kriterien vergleichen. Besonders ausführlich betrachtet wird dabei das Modell von Greitzer/Frincke (2010)[10], da es das umfassendste und aktuellste der Modelle ist. Aus den Modellbeschreibungen wird auch hervorgehen, in wie weit die Themen Recht sowie Moral und Ethik bereits von unterschiedlichen Autoren berücksichtigt worden. Dies bietet eine Basis für das Verständnis der anschließenden Darstellung der in Deutschland geltenden rechtlichen Grenzen und ethischen sowie moralischen Bedenken. Im Anschluss daran soll das Modell von Greitzer/Frincke so erweitert werden, dass es den dargestellten rechtlichen und ethischen Rahmenbedingungen entspricht. Auf diese Weise wird eine mögliches Vorgehen zur automatischen Identifikation von unternehmensschädliche Handlungen durch Mitarbeiter demonstriert, dass rechtliche Grenzen einhält und ethische sowie moralische Bedenken berücksichtigt.

---

[9] Vgl.: Flegel, Privacy Compliant Internal Fraud Screening, 2010, S. 192.

[10] Greitzer et al., Combining Traditional Cyber Security Audit Data with Psychological Data: Towards Predictive Modeling for Insider Threat Mitigiation, 2010.

8. Fazit und Ausblick

Ziel dieser Arbeit war es, rechtliche Grenzen und ethische sowie moralische Bedenken bei der automatischen Identifikation von unternehmensschädlichen Handlungen aufzuzeigen und der Frage nachzugehen, wie ein System zur Vorhersage und Aufdeckung von Bedrohungen durch Insider ausgestaltet werden kann, so dass es diesen Rahmenbedingungen standhält. Bei der Betrachtung von sechs aktuellen Modellen zur Insider Threat Prediction und Detection wurde deutlich, dass es derzeit unterschiedlichste Herangehensweisen an dieses Thema gibt. Dabei sind jedoch die Aspekte von Recht sowie Moral und Ethik nicht ausreichend berücksichtigt. So geht der Großteil der Autoren gar nicht auf ethisch-moralische Bedenken ein und auch rechtliche Grenzen werden nur sehr oberflächlich behandelt. Wie aus der anschließenden Betrachtung des in Deutschland geltenden Datenschutzrechtes hervorgeht, ist es nicht ausreichend, Daten lediglich zu anonymisieren oder bestimmte Datenquellen nicht einzubeziehen, um rechtliche Konformität zu erlangen. Um ein rechtskonformes Modell bieten zu können, wurde daher in dieser Arbeit das Modell von Greitzer und Frincke (2010) modifiziert und erweitert. Hierbei wurden einzelne Elemente der anderen fünf Modelle, die in der Literaturanalyse beschrieben wurden, eingearbeitet. Die größte Erweiterung jedoch ist die Einführung einer menschlichen Komponente, welche für die Konfiguration und kontinuierliche Verbesserung und Anpassung der automatischen Komponente und der Datenquellen zuständig ist. Darüber hinaus ist sie für die Überprüfung und den Vollzug der automatisierten Entscheidungen aus rechtlichen Gründen notwendig. Im Gegensatz zu rechtlichen Grenzen, die auf der Prozessebene Anwendung finden, spielen Ethik und Moral auf einer übergeordneten Ebene eine Rolle. Ethisch-moralische Bedenken treten demnach dann auf, wenn es um die Frage geht, ob ein Insider Threat Prediction oder Detection System eingeführt werden soll. Hierbei steht die Abwägung der persönlichkeitsrechte der Mitarbeiter und anderer Insider gegenüber den Rechten weiterer Stakeholder, wie zum Beispiel den Eigentümern, im Vordergrund. Um ein Arbeitsklima des gegenseitigen Vertrauens zu schaffen und eine gute Sicherheitskultur innerhalb des Unternehmens zu entwickeln, ist es daher unabdingbar, Mitarbeiter nicht mit Überwachungsmaßnahmen zu konfrontieren, sondern diese aktiv am Sicherheitskonzept zu beteiligen.

Mit der Erweiterung und Modifizierung des Modells von Greitzer/Frincke (2010) wird eine Möglichkeit der Umsetzung eines Systems zur automatischen Identifikation unternehmensschädlicher Handlungen geboten, welches konkret die Vorgaben des deutschen Rechtsraumes berücksichtigt. Das erweiterte Modell besitzt dabei ein hohes Abstraktionsniveau, sodass es allgemeingültig ist. Für eine Umsetzung in der Praxis ist es daher in der weiteren Forschung notwendig, das Modell bis auf die Anwendungsebene herunterzubrechen und realisierbare Tools und Analyseverfahren zu entwickeln. Das wichtigste Ergebnis dieser Arbeit ist jedoch, dass gezeigt wurde, dass ein vollkommen automatisierter Prozess, zumindest nach deutschem Recht, nicht durchführbar ist und eine menschliche Komponente in jedem Fall notwendig ist. Dies fand bisher in der Literatur keine Berücksichtigung, was auch darauf zurückzuführen ist, dass man sich dort vornehmlich auf den US-amerikanischen Rechtsraum konzentriert. Zwar ist das Problem der rechtlichen Grenzen und ethischen sowie moralischen Grenzen bewusst, wird jedoch meist nur sehr oberflächlich behandelt. Wie bereits zu Beginn dieser Arbeit erwähnt wurde, stellen Angriffe aus dem Inneren eines Unternehmens eine starke Bedrohung da. Daher kann davon ausgegangen werden, dass die automatische Identifikation solcher Bedrohungen in den nächsten Jahren noch weiter an Bedeutung gewinnen wird. Um aber für die Praxis relevant zu werden, ist es notwendig, die rechtlichen und ethischen sowie moralischen Rahmenbedingungen in den bisher noch sehr theoretischen Modellen zu berücksichtigen. Es ist also unerlässlich, dass dieses Thema in der Zukunft intensiver vorangetrieben wird. Dabei muss allerdings bewusst sein, dass die datenschutzrechtliche und ethisch-moralische Diskussion auf den berechtigten Interessen unterschiedlicher Gruppen beruht. Rechtliche und ethisch-moralische Konformität der Insider Threat Prediction bzw. Detection ist also nicht allein durch technische Maßnahmen zu erreichen, sondern erfordert die Schaffung entsprechender organisatorischer Strukturen und Prozesse.