Verbesserung des IT-Risikomanagements durch Berücksichtigung von Persönlichkeitsprofilen

Diplomarbeit

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

vorgelegt von

Name: Mayer Vorname: Björn

[redacted] [redacted] [redacted] [redacted]

Erstprüfer: Prof. Dr. Michael H. Breitner

Hannover, den 08.10.2010

Inhaltsverzeichnis

1. Einleitung

1.1. Problemstellung und Ziel

In der heutigen Gesellschaft ist Information längst zu einem der wichtigsten Produktionsfaktoren geworden. Um die große Menge an Informationen verarbeiten zu können, sind IT-Systeme sowohl aus dem betrieblichen wie auch aus dem privaten Alltag nicht mehr wegzudenken. Insbesondere für Unternehmen ist der Einsatz von Informations- und Kommunikationstechnologien dabei nicht nur selbstverständlich, sondern nahezu unverzichtbar. Gleichzeitig steigen für Unternehmen die Anforderungen an den Schutz der vorhandenen Informationen. Das für den Schutz externer Informationen, wie Kunden- oder Patientendaten, notwendige Bewusstsein für Informationssicherheit ist in den meisten Unternehmen durchaus vorhanden, insbesondere auch, weil sie gesetzlich dazu verpflichtet werden. Die Sicherheit der internen Informationen dagegen wird häufig nur stiefmütterlich behandelt. Dabei sichern gerade die vertraulichen internen Informationen wichtige Wettbewerbsvorteile, durch die Unternehmen überhaupt erst am Markt bestehen können.[1] Zudem wird im Umgang mit Informationssicherheit oftmals nur der technische Aspekt der Informationssicherheit berücksichtigt. So ist die Verwendung von Firewalls und Antivirus-Software längst selbstverständlich. Dem Risikofaktor Mensch haben die meisten Unternehmen dagegen nur wenig entgegenzusetzen. In einer Studie von CSO Interchange aus dem Jahr 2005, gaben nahezu 100 Prozent der befragten CSOs (Chief Security Officers) an, sie seien auf Angriffe durch Spam, Würmer, Hacker u. ä. gut vorbereitet. 88 Prozent Befragten hatten allerdings keine ausreichende Abwehrstrategie bezüglich der Risiken, die vom Faktor Mensch ausgehen können, wie z. B. unsachgemäße oder unachtsame Nutzung sowie Social Engineering.[2]

Der Risikofaktor Mensch stellt in Bezug auf die IT-Sicherheit damit das wohl größte und am wenigsten greifbare Risiko dar. Angriffe und Bedrohungen können sowohl von externen Personen (unternehmensfremden oder aber auch Geschäftspartnern) als auch von unternehmenseigenen Mitarbeitern ausgehen. Nicht jede Bedrohung muss dabei ein gezielter und vorsätzlich ausgeführter Angriff sein. Häufig sind es Nichtwissen und Nachlässigkeit der eigenen Mitarbeiter, die diese zum Risikofaktor werden lassen. Je nach Situation, helfen dann auch technische Vorkehrungen nicht mehr, um das entstandene Risiko zu managen.

[1] Vgl. Friedmann (2010)
[2] Vgl. CSO Interchange (2005)

Eine vollständige Absicherung eines IT-Systems kann jedoch nicht erreicht werden ohne die Verfügbarkeit der Ressourcen in erheblichem Maße einzuschränken. So könnte man theoretisch zwar den Zugriff auf Daten weitestgehend sperren, ohne einen Zugriff auf diese, wird allerdings auch die dahinter stehende Information als solche nutzlos.

Informationssicherheit und die damit verbundenen Risiken angemessen zu steuern, ist das Ziel des IT-Risikomanagements. Dieses kann sich dabei unterschiedlichen Steuerungsinstrumenten bedienen. In dieser Arbeit sollen Persönlichkeitstests für den Umgang mit den potentiellen Risiken, die von den eigenen Mitarbeitern ausgehen können, herangezogen werden. Allgemein können Persönlichkeitsprofile einem Personalmanager bei der Entscheidung unterstützen, Positionen im Unternehmen richtig zu besetzen. Inwiefern Persönlichkeitsprofile die IT-Sicherheit verbessern können, soll im Rahmen der vorliegenden Arbeit herausgearbeitet und beleuchtet werden. Der Schwerpunkt liegt dabei insbesondere auf dem Einsatz von Persönlichkeitsprofilen im Rahmen der Vergabe von Rollen in einem rollenbasierten Berechtigungskonzept.

1.2. Aufbau und Struktur

Am Anfang der Arbeit steht die Betrachtung der Grundlagen zum Thema IT-Sicherheit. Der Schwerpunkt soll allerdings auf der Betrachtung der Risiken liegen, die von dem wichtigsten Risikofaktor ausgehen, dem Menschen.

Im dritten Kapitel soll das Persönlichkeitsmodell NEO-PI-R vorgestellt werden. Zunächst werden die Dimensionen des Modells, insbesondere die für die IT-Sicherheit wichtigen Facetten erläutert. Anschließend soll darauf eigegangen werden, wie anhand dieses Modells Persönlichkeitsprofile erstellt werden können.

Parallel dazu wird im vierten Kapitel die rollenbasierte Zugriffskontrolle (RBAC) vorgestellt und kurz die ökonomischen Aspekte dieses Konzeptes beleuchtet.

Im fünften Kapitel folgt dann eine Zusammenführung der vorangegangenen Inhalte. Die Persönlichkeitsprofile sollen für die Zuordnung von Benutzern zu Rollen im Rahmen des IT-Risikomanagements herangezogen werden. Anforderungen an ausgewählte Rollen und Vorgehensweisen bei Abweichungen sollen festgelegt werden.

In einem abschließenden Kapitel sollen die wichtigsten Erkenntnisse der Arbeit nochmals zusammengefasst und ein kurzer Ausblick auf zu erwartende Entwicklungen gegeben werden.

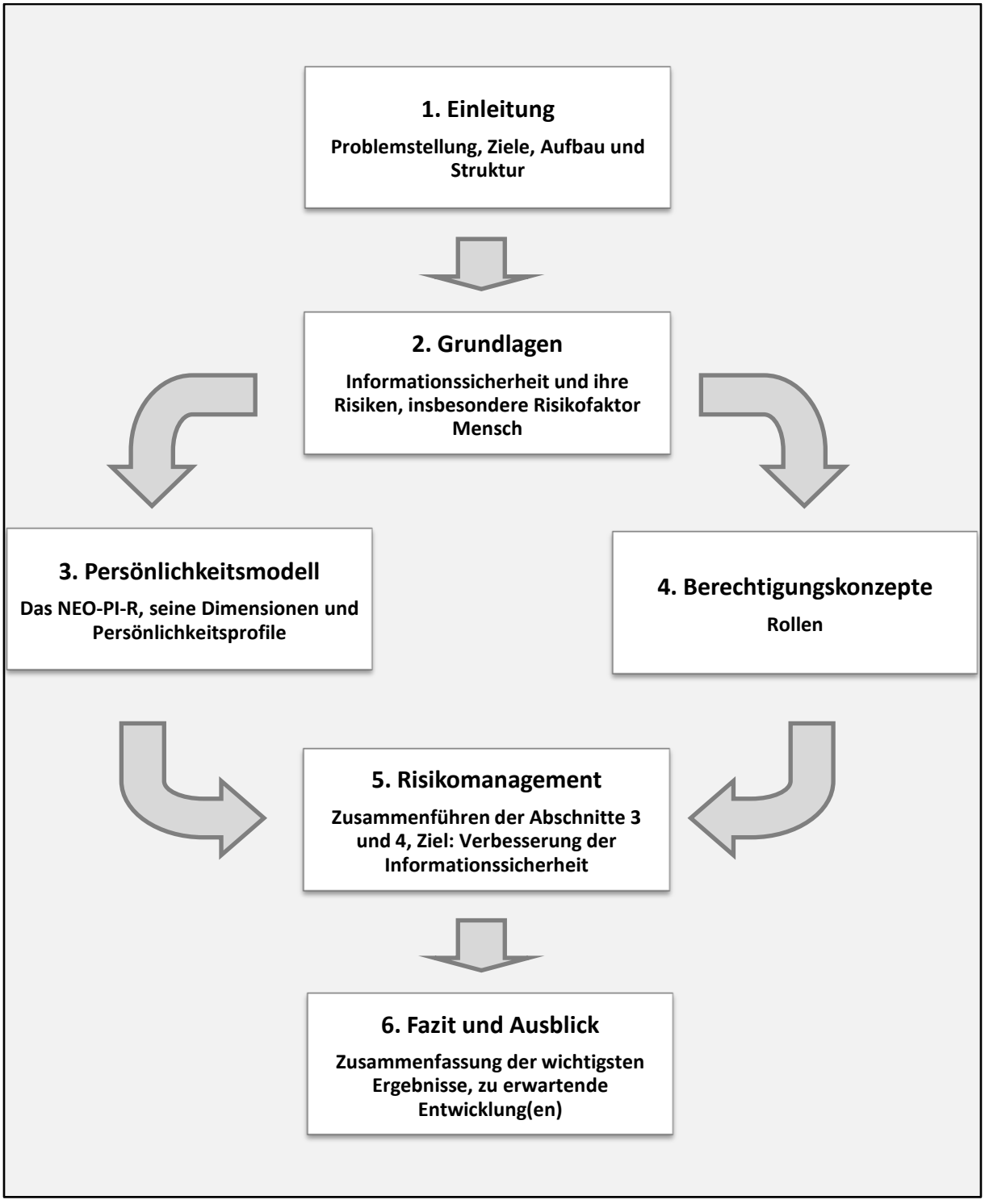

Abb. 1: Graphische Darstellung der Struktur der Arbeit
Quelle: Eigene Darstellung

Sensibilisierungsmaßnahmen nicht zielführend erscheinen, sollte über sogenannte Kompensationsstrategien nachgedacht werden.[134]

In einem ersten Schritt könnte geprüft werden, den Mitarbeiter auf eine andere Stelle im Unternehmen zu versetzen, auf die sein Persönlichkeitsprofil (besser) passt.

Sollte eine Versetzung nicht möglich oder sinnvoll sein, könnte eventuell eine Abänderung der Stellenbeschreibung erfolgen, so dass diese eher zum Persönlichkeitsprofil des entsprechenden Mitarbeiters passt. Diese Veränderung würde allerdings eine Modifikation, bzw. das Erstellen einer neuen Rolle im RBAC-System notwendig machen. Des Weiteren würde dieses Vorgehen einen zusätzlichen Kostenaufwand bedeuten, dessen Verursachung gerechtfertigt sein muss. Eine Rechtfertigung, zumindest hinsichtlich des Kostenaufwandes könnte vorliegen, wenn eine Entlassung für das Unternehmen zu teuer wäre.

Der zuletzt genannte Schritt sollte allerdings nur als ein letzter Ausweg in betrachtet werden. Stellt ein Mitarbeiter ein untragbar hohes Risiko dar, sollte sich ein Unternehmen von ihm trennen. Eine Entlassung eines Mitarbeiters aufgrund seines Persönlichkeitsprofils ist allerdings aus ethischer und arbeitsrechtlicher Sicht höchst fragwürdig. Zudem hätte dieser Umstand schon bei der Personalauswahl auffallen müssen.

Daher erübrigt sich die Anwendung von Kompensationsstrategien bei potentiellen Mitarbeitern, da sie für die Besetzung einer Rolle gar nicht erst in Erwägung gezogen werden.

6. Fazit und Ausblick

Diese Arbeit zielt darauf ab, Persönlichkeitsprofile zur Unterstützung des IT-Risikomanagements zu beleuchten und dessen möglichen Beitrag für eine Verbesserung der IT-Sicherheit aufzuzeigen und zu prüfen.

Dazu wurden zunächst die Bedeutung von Informationen für Unternehmen sowie die im Zusammenhang mit diesem wichtigen Produktionsfaktor verbundenen Herausforderungen eingegangen. Dabei wurde der Schutzbedarf von Informationen aufgezeigt und die Schutzziele der IT-Sicherheit daraus abgeleitet. Der Fokus lag insbesondere auf der Betrachtung des Menschen, der als besonderer Risikofaktor identifiziert werden konnte. Den

[134] Vgl. Howard und Howard (2002), S. 223f.

Schwerpunkt bildeten dabei die vorhandenen und die potentiellen Mitarbeiter eines Unternehmens.

Das Risikopotential, welches von diesen Personengruppen ausgeht, wurde im Kern auf die vier Kategorien, Böswilligkeit, Fahrlässigkeit, Unwissenheit und das Social Engineering, zurückgeführt. Die Erkenntnisse daraus eröffneten die Fragestellung, wie der Risikofaktor Mensch im Rahmen des IT-Risikomanagements berücksichtigt werden kann. Es wurde gezeigt, dass durch den Einsatz technischer Maßnahmen gewisse Sicherheitsgrundfunktionen erfüllt werden können. Die Zugriffskontrolle bzw. Rechteverwaltung ist dabei eine der wichtigen Grundfunktionen im Sinne der IT-Sicherheit. So kann in einem rollenbasierten Berechtigungskonzept durch eine geeignete Zuordnung von Rollen an Mitarbeiter, das durch diese entstehende Gefahrenpotential deutlich eingeschränkt werden.

Daran anknüpfend stellte sich die Frage, inwieweit Persönlichkeitsprofile bei der Zuordnung der Rollen herangezogen werden können. Zur Beantwortung dieser Fragestellung wurde das Persönlichkeitsmodell NEO-PI-R herangezogen. Dabei konnte gezeigt werden, dass sich aus dem NEO-PI-R eine Reihe von sicherheitsrelevanten Persönlichkeitsmerkmalen herausfiltern lassen, die im Rahmen der vorliegenden Arbeit als wesentliche Einflussfaktoren für die IT-Sicherheit eingestuft wurden.

In einem nächsten Schritt wurde dann die rollenbasierte Zugriffskontrollstrategie (Role-Based Access Control, RBAC) und die damit verbundenen Möglichkeiten sowie Vor- und Nachteile vorgestellt und die ökonomischen Auswirkungen skizziert. Dabei konnte gezeigt werden, dass die rollenbasierte Zugriffskontrolle (RBAC) eine auf die Bedürfnisse des zivilen Unternehmensumfeldes zugeschnittene Zugriffskontrollstrategie ist. Anhand der Zuordnung von Mitarbeitern zu Rollen, können Zugriffsrechte sicher und effizient verwaltet werden. Zudem werden die wichtigen Sicherheitsprinzipien der minimalen Rechte und der Aufgabentrennung durch eine RBAC-Strategie unterstützt. Sie ist daher den älteren DAC- und MAC-Strategien überlegen.

Zur Integration der Persönlichkeitsprofile in eine RBAC-Strategie wurden die Erkenntnisse aus dem Persönlichkeitsmodell NEO-PI-R und die rollenbasierte Zugriffkontrolle abschließend zusammengeführt. Dabei wurden die Ausprägungen der als sicherheitsrelevant eingestuften Persönlichkeitsfacetten vor dem Hintergrund der Rollenvergabe diskutiert. Anhand von ausgewählten Rollen wurde beispielhaft aufgezeigt, wie solche

Anforderungsprofile aussehen könnten. Darüber hinaus wurden Vorschläge unterbreitet, wie Anforderungsprofile sinnvoll in das RBAC-Berechtigungskonzept integriert werden könnten.

Zusammenfassend lassen sich folgende Ergebnisse festhalten: Persönlichkeitstests lassen sich auf die Erhebung der sicherheitsrelevanten Facetten reduzieren. Allerdings nur unter dem Vorbehalt, dass nicht mehr das ganze Persönlichkeitsbild betrachtet und damit eventuelle Wechselwirkungen ausgeblendet werden. Eine ähnliche Problematik wirft auch der Vorschlag einer „Automatisierung" des Prozesses zur Erhebung der Persönlichkeitsprofile und der Zuordnung von Rollen auf. Zum einen bedarf der automatisierte Rollen-Zuordnungsprozess einer in ihrer Höhe noch schwer zu beziffernden Investition, zum anderen stellt sich die Frage, ob auf eine Experteneinschätzung durch psychologisch ausgebildetes Personal tatsächlich verzichtet werden kann. Fragwürdig bleibt zudem, welche Konsequenzen aus der Erkenntnis von Diskrepanzen zwischen dem Persönlichkeitsprofil eines (potentiellen) Stelleninhabers und dem Anforderungsprofil einer Rolle gezogen werden sollen. Was z. B. soll mit den Beschäftigten passieren, wenn sie die Rolle bisher ohne „Sicherheitsvorfälle" ausgeübt haben, bei Überprüfung Ihres Profils aber ein potentielles Sicherheitsrisiko festgestellt wird? Zudem können die Mitarbeiter zwar durch Schulungen und Awareness-Kampagnen besser für das Thema IT-Sicherheit sensibilisiert und vorbereitet werden, in wie weit die Persönlichkeitseigenschaften dadurch aber beeinflusst werden können, kann im Rahmen dieser Arbeit nicht beantwortet werden.

Abschließend lässt sich festhalten, dass die Anwendung von Persönlichkeitsprofilen im Rahmen des IT-Risikomanagements eine Erhöhung der IT-Sicherheit bringen *kann*, wenn bei der Vergabe von Rollen auf die Ausprägung der sicherheitsrelevanten Facetten geachtet wird. Allerdings ist fraglich, wie viel *zusätzliche* Sicherheit dadurch am Ende gewonnen werden kann. Eigentlich sollte schon bei der Einstellung geprüft werden, ob ein Mitarbeiter für eine bestimmte Funktion geeignet ist oder nicht und nicht erst bei der Zuordnung der Rolle.

Die in dieser Arbeit hervorgebrachten Erkenntnisse eröffnen gleichzeitig neue weiterführende Fragestellungen und damit den Bedarf für weitere Forschungsansätze.

So gilt es in einem weiteren Schritt zu prüfen, in wieweit die in dieser Arbeit herausgearbeiteten Persönlichkeitsmerkmale die richtige Einschätzung des Risikopotentials eines Mitarbeiters ermöglichen und die auf den ersten Blick nicht relevanten Merkmale tatsächlich ausgeblendet werden können, ohne den Test zu verfälschen.

Des Weiteren gilt es zu prüfen, welche Investitionen mit der Integration von Persönlichkeitsprofilen in die Rollenvergabe, je nach Unternehmensgröße und -struktur, tatsächlich verbunden sind. Um Anforderungsprofile zu erstellen, müssen Spezialisten herangezogen werden, die das Unternehmen sehr gut kennen. Sie müssen detaillierte Kenntnisse über die Prozesse und Rollen im Unternehmen haben, um die Risiken, die mit den Rollen verbunden sind einschätzen zu können. Letztlich wird die Festlegung der Anforderungsprofile selbst, eine hoch komplexe Aufgabe darstellen, die einer Entscheidung bedarf, welche Ausprägungen hinsichtlich der Persönlichkeitsmerkmale ein Risiko für eine Rolle darstellen. Zudem sind Wechselwirkungen zwischen einzelnen Facetten zu betrachten und gegebenenfalls auch Toleranzbereiche festzulegen. Weiterhin ist die Bereitstellung von Personal für die Erhebung der Persönlichkeitsprofile erforderlich. Außerdem wird Fachpersonal benötigt, das sowohl eine korrekte Auswertung, als auch eine korrekte Einschätzung zu einem Persönlichkeitsprofil liefern kann. Das Vorhandensein von solchen psychologischen Fachkompetenzen dürfte, wenn überhaupt, nur in Unternehmen mit großen Personalabteilungen gegeben sein. Der Arbeitsaufwand solcher Spezialisten wird einen erheblichen Kostenfaktor darstellen, der sich schnell vervielfachen kann, wenn die Fachkompetenz im eigenen Unternehmen nicht vorhanden ist und stattdessen in Form von externen Beratern beschafft werden muss.

Dem gegenüber sollte der erwartete Zugewinn an IT-Sicherheit näher betrachtet werden, den eine Integration von Persönlichkeitsprofilen in die Rollenvergabe bringen könnte. Dies ist eine allgemein verbreitete Problematik bei Investitionen in die IT-Sicherheit. Es stellt sich immer die Frage, welchen Gegenwert (Return on Security Investment, RoSI) ein Unternehmen für die getätigte Investition erhält. Insbesondere auf dem Gebiet der IT-Sicherheit erweist es sich als durchaus schwierig, den RoSI abzuschätzen. Kann bei einem Eintreten von Sicherheitsvorfällen ein großes Schadensausmaß abgewendet werden, so hat sich die Investition in die jeweiligen Sicherheitsmaßnahmen schnell ausgezahlt. Es ist aber im Vorfeld nun mal nicht bekannt, ob der entsprechende Sicherheitsvorfall eintreten wird oder nicht. Das ist der Grund dafür, weshalb in der Praxis Überlegungen zu Investitionen in die IT-Sicherheit i. d. R. erst nach dem Auftreten von Schäden erfolgen. Dieses hat im Wesentlichen dazu geführt, dass viele der technischen Sicherheitsmaßnahmen, die heute in Unternehmen eingesetzt werden, sich längst in der IT-Sicherheit etabliert haben. Auch wenn in dieser Arbeit der Risikofaktor Mensch in Zusammenhang mit rollenbasierter Zugriffsstrategie im Vordergrund stand, soll an dieser Stelle darauf hingewiesen werden, dass nur ein Zusammenspiel von vielen Sicherheitsmaßnahmen die Sicherheit von IT-Systemen

gewährleisten kann. Dazu gehören beispielsweise der heutzutage selbstverständliche Einsatz von Firewalls, Intrusion Detection Systemen, die Möglichkeit zur Verschlüsselung bei Kommunikation und Datenspeicherung, Backup- und Recovery-Systeme und viele mehr. Die physische Absicherung von Unternehmensressourcen ist gleichermaßen von Bedeutung. So sind auch Maßnahmen wie beispielsweise Zugangskontrollen und Brandschutz ebenso zu beachten.

Was den Risikofaktor Mensch betrifft, so wird er immer das schwächste Glied der Sicherheitskette darstellen. Das Kapitel zur Persönlichkeitspsychologie hat ansatzweise gezeigt, wie komplex der Mensch in seiner Persönlichkeit sein kann. Diese Komplexität in der Praxis im Rahmen der Zugriffskontrolle zu integrieren, dürfte ein äußerst schwieriges Unterfangen sein. Zudem hängt der Erfolg einer solchen Vorgehensweise maßgeblich von der Einschätzung der Persönlichkeitsprofile und der im Anforderungsprofil abgebildeten Risiken ab. Zudem muss weiterer Forschungsaufwand betrieben werden, um festzustellen, ob diese Art der Verbesserung des IT-Risikomanagements ökonomisch sinnvoll ist. Vielleicht wird diese Idee von einigen Unternehmen als Chance eingestuft, das eigene IT-Risikomanagement zu optimieren. Andere wiederum werden sie verwerfen. Letztendlich könnte auch eine gewisse „Mischung“ entstehen, indem Persönlichkeitsprofile für die Rollenvergabe nur in Verbindung mit hochriskanten Rollen eingesetzt werden. Eine Befragung von Unternehmen im Rahmen einer Studie könnte einen ersten Aufschluss zu den hier aufgeworfenen Fragen geben. Was der Einbezug von Persönlichkeitsprofilen in die IT-Sicherheit wirklich bringt, wird sich daher erst in der Zukunft zeigen.