Nutzung von Persönlichkeitsmodellen für Awareness-Kampagnen zur Verbesserung der Sicherheit mobiler Systeme

Bachelorarbeit

zur Erlangung des akademischen Grades „Bachelor of Science (B.Sc.)“ im Studiengang Wirtschaftswissenschaft der Wirtschaftswissenschaftlichen Fakultät der Leibniz Universität Hannover

vorgelegt von

Name: Müller Vorname: Jan-Niklas

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

Prüfer: Prof. Dr. M. H. Breitner

Neustadt, d. 08.08.2013

Inhaltsverzeichnis

1. Einleitung

1.1 Relevanz des Themas

„Information ist das neue Öl“, waren die Worte von Neelie Kroes, der EU-Kommissarin für die Digitale Agenda. Diese Worte zeigen unverblümt den Wandel der materiellen Industriegesellschaft hin zur digital vernetzten Informationsgesellschaft.[1]

Informationen sind aus dem unternehmerischen Alltag nicht mehr wegzudenken und führen in Verbindung mit dem intelligenten Einsatz der Informations- und Kommunikationstechnologie zu einer Steigerung der Wettbewerbsfähigkeit. Informationen sind insbesondere im Dienstleistungssektor aber auch bei der Innovationstätigkeit eine relevante Ressource. Um im Sinne der Geschäftsprozesse des Unternehmens und der Globalität des Geschäftsalltags nicht durch Wettbewerber verdrängt zu werden, sollten Informationen jederzeit verfügbar sein.

Daraus ergibt sich die Nutzungsmöglichkeit mobiler Systeme, diese haben den inhärenten Vorteil, dass eine orts- und zeitunabhängige Nutzung der Daten und Informationen ermöglicht wird. Aus dieser erhöhten Verfügbarkeit, infolge der weltweiten Weiterentwicklung der Mobilfunkinfrastruktur, ergibt sich die Möglichkeit völlig neuartiger Wertschöpfung samt grundlegender unternehmerischer Aktivität. Sie profitieren von der gewonnen Mobilität per se sowie der Ubiquität der Datenverfügbarkeit. So sind bspw. geschäftsspezifische Daten während eines Meetings in den Vereinigten Staaten durch breitbandige Mobilfunknetze in kürzester Zeit auf dem mobilen Endgerät verfügbar. Abbildung 1 verdeutlicht die Relevanz und Aktualität, anhand der Anzahl der mobilen Endgeräte die mit dem Unternehmensnetzwerk verbunden sind.

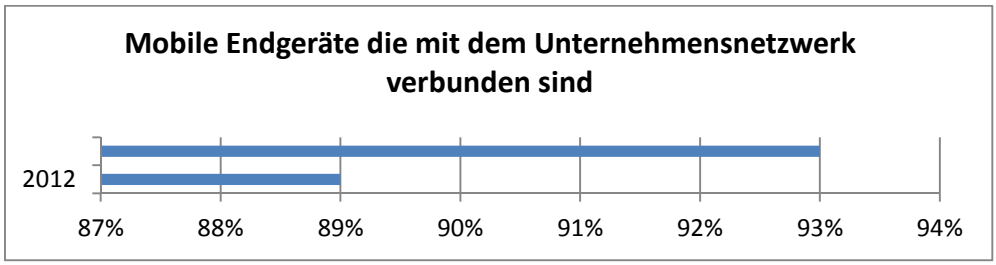

Abbildung 1: Prozentsatz der mobilen Endgeräte die mit Unternehmensnetzwerken verbunden sind
Quelle: In Anlehnung an Dimensional Research (2013)

[1] Vgl. Nicolas (2012)

Abbildung 1 zeigt, dass der Einsatz von mobilen Endgeräten im Unternehmensnetzwerk und damit mit Zugriff auf Unternehmensspezifische Daten allgegenwärtig ist. Unabhängig von ihrem positiven Beeinflussungspotential des unternehmerischen Erfolgs gehört das Mobile Computing aber auch zu den größten Gefahren im Unternehmen, wie Abbildung 2 belegt.

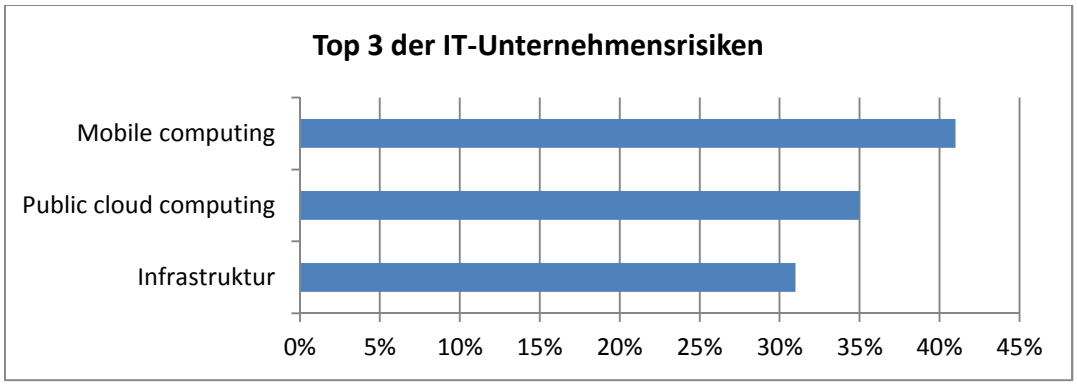

Abbildung 2: Die größten IT-Unternehmensrisiken
Quelle: Eigene Darstellung in Anlehnung an Symantec State of Mobility Survey (2012)

Aufgrund der mannigfaltigen Gefahrenpotentiale durch Malware und andere Bedrohungen im Umgang mit mobilen Endgeräten bedarf es eines ausgeklügelten Sicherungssystems. Gefahren und Bedrohungen für die Sicherheit der Informationen können dabei für das Unternehmen gravierende Folgen haben: Neben dem finanziellen Verlust zählt hierbei auch der Verlust von Image und Glaubwürdigkeit, was wiederum Einfluss auf monetäre Größen hat.[2] Die Informationssicherheit ist also im Unternehmen von eminenter Bedeutung. Dabei lag der Fokus bisher meist auf der technischen Absicherung mobiler Endgeräte. Insbesondere auf mobilen Endgeräten ist eine solche technische Absicherung, durch Virenprogramme oder ähnliches aber nur begrenzt möglich und bietet keinen ausreichenden Schutz.[3] Die Sicherheit mobiler Systeme und Informationssicherheit sind ferner im immensen Maße abhängig vom Faktor Mensch, seinem Benutzer. Die mangelnde Kompetenz, Fahrlässigkeit und Irrtümer machen die Nutzer in Organisationen zur größten Gefahrenquelle.[4]

Diese Benutzer haben innewohnende persönlichkeitspsychologische Eigenschaften und individuelle Charakteristika, die das Sicherheitsbewusstsein im Umgang mit

[2] Vgl. Bulgurcu et al. (2010), S. 524
[3] Vgl. Fox und Kaun (2005), S. 329
[4] Vgl. <kes>/ Microsoft (2004)

Daten, Informationen und der Informationstechnik, also insbesondere bei mobilen Endgeräten, determinieren. Persönlichkeitsmodelle ermöglichen es dann mithilfe von Fragebögen die Personen zu identifizieren, die bestimmte sicherheitsrelevante Charakteristika aufweisen und dadurch Risikofaktoren darstellen.

Diese identifizierten Risikopersonen können dann durch gezielte sowie effektiv und effizient aufgebaute Awareness-Kampagnen angesprochen werden. Durch diese Maßnahmen und die Lernelemente einer solchen Kampagne kann bei den Mitarbeitern langfristig und nachhaltig das nötige Sicherheitsbewusstsein sowie eine geeignete Sicherheitspolitik manifestiert werden.

Hierbei werden der interdisziplinäre Charakter und die Schnittstellenfunktion der Wirtschaftsinformatik deutlich. Die Wirtschaftsinformatik wird hier durch persönlichkeitspsychologische und lerntheoretische Aspekte ergänzt und erweitert.

Ziel der Arbeit ist es also ein umfassendes Konzept zu entwickeln, welches darstellt, wie Persönlichkeitsmodelle für Awareness-Kampagnen genutzt werden können, sodass sich die Sicherheit der mobilen Endgeräte und damit die Informationssicherheit erhöht.

1.2 Struktur und Aufbau der Arbeit

Zunächst wird sich im zweiten Kapitel mit den allgemeinen Grundlagen zu mobilen Systemen und der Sicherheit mobiler Endgeräte beschäftigt. Anschließend wird eine Einführung in die Persönlichkeitspsychologie sowie ihrer Entwicklung gegeben, woraufhin unterschiedliche Persönlichkeitsinventare vorgestellt und verglichen werden. Das zweite Kapitel wird dann mit der Beschreibung der Notwendigkeit und unterschiedlichen Konzepten sowie Erfolgsfaktoren von Awareness-Kampagnen abgeschlossen.

Im dritten Kapitel wird dann hinsichtlich der Erstellung von Persönlichkeitsprofilen zunächst das Fünf-Faktoren-Modell erläutert und dieses dann in Hinblick auf seinen Einfluss auf die Angriffsvektoren und allgemeinen Bedrohungen der mobilen Sicherheit analysiert.

In Kapitel 4 wird dann das UCIT-Modell zunächst allgemein erläutert. Daraufhin wird eine Variation dieses Modells zu einem konzeptionellen Prozess-Modell beschrieben, mit dem die Beziehungen zwischen Persönlichkeitsmodellen, Awareness-

Kampagnen und der Sicherheit bzw. den Bedrohungen mobiler Endgeräte dargestellt werden kann. Daraufhin wird diese Konzeption anhand von Fallbeispielen exemplarisch beschrieben.

Daraufhin werden in Kapitel 5 Limitationen aufgezeigt und die Arbeit wird kritisch diskutiert.

Schließlich endet diese Arbeit in Kapitel 6 mit einem Fazit, indem die wichtigsten Erkenntnisse zusammengefasst und ein Ausblick auf zukünftige Entwicklungen wird ebenfalls in diesem Kapitel thematisiert.

2. Grundlagen

2.1 Sicherheit Mobiler Systeme

2.1.1 Mobile Systeme

Mobile Systeme, auch Mobile Computing genannt, setzen sich zusammen aus einer „Gesamtheit von Geräten, Systemen und Anwendungen, die einen mobilen Benutzer mit den auf seinen Standort und seine Situation bezogenen sinnvollen Informationen und Diensten versorgt.“[5] Daraus ergibt sich der Vorteil, dass bestimmte Dienste mithilfe von mobilen Endgeräten orts- und zeitunabhängig ausgeführt werden können und eine Verbesserung der Mobilität des Nutzers gewährleistet werden kann.[6] Die persönliche- und die Endgeräte-Mobilität wird somit gesteigert. Ferner erhält der Nutzer eine erhöhte Erreichbarkeit, Lokalisierbarkeit und Identifizierbarkeit durch die Nutzung mobiler Geräte.[7]

Mobile Systeme setzen sich zusammen aus Drahtlosen Netzen und unterschiedlichen Arten von mobilen Endgeräten.

Durch die Interaktion der mobilen Endgeräte mit drahtlosen Netzwerken kann ein zeit- und ortsunabhängiger Zugriff auf bestimmte Informationen und Netzwerke ermöglicht werden.[8] WLAN, Bluetooth und IrDA gelten als drahtlose lokale Netze, GSM, UMTS und LTE sind Mobilfunknetze. Das BSI unterscheidet bei drahtlosen Verbindungen in den Weitbereich und Nahbereich. Der Nahbereich wie WLAN, Bluetooth und IrDA dient dabei größtenteils der Synchronisation von Daten. GSM

[5] Vgl. Bollmann und Zeppenfeld (2010), S. 4
[6] Vgl. Schill und Springer (2012), S. 365
[7] Vgl. Lehner (2003), S. 9ff.
[8] Vgl. Schön (2012), S. 289

Des Weiteren ist der Einfluss von Belohnungen und Sanktionen auf die Einstellung und das Verhalten der Mitarbeiter interessant. Es könnte untersucht werden ob Belohnungen oder Sanktionen die Motivation und damit die Einstellung der Mitarbeiter ebenfalls nachhaltig beeinflussen können. Diese Sanktionen und Belohnungen könnten dann bei einer Awareness-Maßnahme als Motivationsunterstützung und Verhaltensbeeinflussung verwendet werden. Bei der weiteren Entwicklung und Verwendung des Prozess-Modells sollte diese Tatsache berücksichtigt werden, um die Erfolgsaussichten nachhaltig zu erhöhen.

Außerdem sollte beachtet werden, dass insbesondere die Awareness-Kampagne an die spezifischen Eigen- und Besonderheiten des Unternehmens bzw. der Organisation angepasst werden muss. Die verwendeten Methoden und Maßnahmen müssen an den unternehmerischen Bezugsrahmen angepasst werden. Für den Erfolg der Kampagne ist es essentiell, dass die unterschiedlichen Erfolgsfaktoren unternehmensspezifisch verwendet werden. Auch die individuellen Phasen müssen an das entsprechende Unternehmen angepasst werden. So ist bspw. Öffentlichkeitsarbeit nicht in jeder Branche und nicht in jedem Unternehmen sinnvoll. Es lässt sich also festhalten, dass kein „one-size-fits-it-all-approach“ möglich ist, sondern sowohl die Awareness-Kampagne, als auch die Persönlichkeitsanalyse an den speziellen und situativen unternehmensexternen und –internen Kontext angepasst werden muss.

6. Fazit und Ausblick

Ziel dieser Arbeit war es zu zeigen, dass die „Nutzung von Persönlichkeitsmodellen für Awareness-Kampagnen zur Verbesserung der Sicherheit mobiler Systeme“ dienlich ist.

Einleitend wurde die Relevanz des Themas beschrieben und erläutert. Zu diesem Zweck wurde gezeigt, dass Informationen in der heutigen Zeit bedeutende Treiber des Erfolgs von Unternehmen und Branchen sind. Daher ist es charakterisierend, dass mobile Systeme, wegen ihrer Ubiquität diese Entwicklung verstärken. In Bezug darauf, kann die Sicherheit der Informationen und der informationenverarbeitenden mobilen Endgeräte als elementar konstatiert werden. Es wurde gezeigt, dass Persönlichkeitsmerkmale und Awareness-Kampagnen Einflussfaktoren der Sicherheit mobiler Systeme darstellen. Somit wurde die Abhängigkeit der

Informationssicherheit vom Faktor Mensch und seinen wesenseigenen Persönlichkeitsmerkmalen nachgewiesen.

Zunächst wurden grundlegende Informationen über mobile Systeme, Persönlichkeitspsychologie, Persönlichkeitsmodelle und Awareness-Kampagnen zusammengetragen und aufbereitet. Beim Vergleich unterschiedlicher Persönlichkeitsmodelle, welche Ausprägungen des Fünf-Faktoren-Modells messen, wurde deutlich, dass das NEO-FFI einen umfassenden und gleichzeitig ökonomisch sinnvollen Persönlichkeitsfragebogen darstellt. Dieser ist insbesondere aufgrund seiner universellen Einsetzbarkeit, schnellen Bearbeitungszeit und Bestätigung der Gütekriterien, für den Einsatz in Unternehmen prädestiniert. Resultierend lässt sich festhalten, dass das NEO-FFI ein effizientes und effektives Persönlichkeitsmessverfahren darstellt.

In Kapitel 3 wurden weiterhin die fünf Dimensionen, Neurotizismus, Extraversion, Offenheit für Erfahrungen, Verträglichkeit und Gewissenhaftigkeit des Fünf-Faktoren-Modells betrachtet und ihre differierende Wirkung auf die Angriffsvektoren gezeigt. So steht bspw. Gewissenhaftigkeit in positiver Verbindung mit der Sicherheit mobiler Endgeräte. Aus diesen Wirkungszusammenhängen ergeben sich für Unternehmen spezifische Bedrohungen der Informationssicherheit mobiler Systeme.

In Kapitel 4 wurde dann eine Variation des UCIT-Modells zu einem Ablauf- bzw. Prozess-Modells vorgestellt. Mithilfe dieses Modells wurde gezeigt, in welcher Form Persönlichkeitsmodelle, Angriffsvektoren der mobilen Sicherheit und Awareness-Kampagnen in Verbindung gebracht werden können. Dabei hat sich gezeigt, dass die Analyse der Persönlichkeit durch Persönlichkeitsmodelle und die Bewertung der Bedrohungen mobiler Systeme zu einer zielgerichteten und systematischen Awareness-Kampagne führen kann. Durch diese ausführliche vorgelagerte Analyse, die einen interdisziplinären Charakter aufweist, können Awareness-Kampagnen nachhaltig optimiert, verbessert und die Erfolgswahrscheinlichkeit erhöht werden.

Was die umfassende Sicherheit der Informationen und mobilen Systeme betrifft, so konnte gezeigt werden, dass durch die Anpassung und Optimierung einer solchen Maßnahme an die verschiedenen spezifischen Bedrohungen und Besonderheiten der Mitarbeiter in einer nachhaltigen, effektiven sowie effizienten Verbesserung der Sicherheit mobiler Systeme resultieren kann.

Andererseits wurde auch festgestellt, dass der Erfolg der Awareness-Maßnahme darüber hinaus von zahlreichen weiteren Erfolgsfaktoren abhängt, die situativ und organisationsspezifisch angepasst und ausgearbeitet werden müssen.

Abschließend kann festgestellt werden, dass eine Analyse der Persönlichkeit der Mitarbeiter, mithilfe des NEO-FFI Persönlichkeitsinventars, für Awareness-Kampagnen zur Verbesserung der Sicherheit mobiler Systeme sinnvoll ist. Mithilfe der Persönlichkeitseigenschaften kann dann die Erfolgswahrscheinlichkeit einer Awareness-Kampagne und ferner die Informationssicherheit mobiler Systeme grundlegend determiniert und erhöht werden.

Insofern steht zu hoffen, dass dieses Forschungsgebiet Gegenstand weiterer Untersuchungen wird, da davon auszugehen ist, dass Menschen bzw. Mitarbeiter mit ihren vielfältigen Wesensmerkmalen weiterhin die Sicherheit mobiler Systeme bestimmen. Zwar werden die technischen Absicherungsmöglichkeiten effektiver, aber einen umfassenden Schutz werden diese in Zukunft wohl auch nicht bieten können. Daraus ergibt sich auch zukünftig die Notwendigkeit des Einsatzes von Persönlichkeitsmessverfahren. Aufbauend auf den Ergebnissen dieser Analysen, können Awareness-Maßnahmen gezielt und optimiert durchgeführt werden. Dadurch kann dann eine erhöhte Sensibilität der spezifischen Mitarbeitergruppe im Umgang mit mobilen Endgeräten erreicht werden. Durch diese Sensibilisierung wird überdies nicht nur die Sicherheit der mobilen Systeme gewährleistet, sondern ferner die Informations- und Datensicherheit des gesamten Unternehmens.