Mentale Modelle der IT-Sicherheit bei der Nutzung mobiler Endgeräte

Zinaida Benenson
Universität Erlangen-Nürnberg
zinaida.benenson@cs.fau.de

Olaf Kroll-Peters
EnBW AG
o.kroll-peters@enbw.com

Matthias Krupp
Universität Mannheim
matthias.krupp@web.de

Abstract: Mobile Endgeräte werden immer leistungsfähiger und damit wächst für die Nutzer auch das Gefahrenpotenzial durch typische IT-Sicherheitsbedrohungen. Obwohl die Verantwortung des Benutzers für die Einhaltung der IT-Sicherheit anerkannt und wissenschaftlich belegt ist, konzentriert sich die Forschung zur IT-Sicherheit im mobilen Umfeld meistens auf die technische Seite der Problematik. In dieser Arbeit wird der erste Schritt zur Untersuchung der Rolle der Benutzer in der IT-Sicherheit mobiler Endgeräte unternommen, indem anhand von Interviews entsprechende mentale Modelle erstellt werden. Als mentale Modelle werden Abbildungen der Realität im Bewusstsein des Menschen bezeichnet. Obwohl diese Abbildungen normalerweise ungenau und oft fehlerhaft sind, kann ihre Kenntnis zu Prognosen über Handlungen von Menschen verwendet werden. Mentale Modelle der IT-Sicherheit bilden die Grundlage für die Bemühungen der Nutzer (oder für das Fehlen solcher Bemühungen), die IT-Sicherheit ihrer Systeme zu gewährleisten.

1 Einleitung

Die Anzahl sowie Leistungsfähigkeit mobiler Endgeräte nimmt im Verlauf der letzten Jahre immer stärker zu und damit wächst auch die Anzahl der IT-Sicherheitsbedrohungen in diesem Bereich [Jun11, BFH+11]. Auf der einen Seite sind die Anwender technischen Bedrohungen wie Malware, das Abhören der Datenübermittlung und das Ausspähen von Standortinformationen ausgesetzt. Auf der anderen Seite bestehen auch menschliche Bedrohungen wie Verlust, Diebstahl, Fehlbedienung und Social Engineering. In beiden Fällen nehmen Benutzer einen bedeutenden Anteil für das Umsetzen von IT-Sicherheit mobiler Endgeräte ein. Zum Beispiel ist zum Installieren der mobilen Malware meistens nach wie vor die aktive Teilnahme der Benutzer notwendig.

Bisher ist die Rolle der Benutzer in der Sicherheit mobiler Endgeräte nicht ausreichend bekannt. In dieser Arbeit unternehmen wir die ersten Schritte zur Feststellung mentaler Modelle der IT-Sicherheit bei der Benutzung mobiler Endgeräte. Mentale Modelle charakterisieren die individuelle Repräsentation und das Verständnis von Realität, beeinflusst durch Erfahrungen, Empfindungen und Informationen, im Bewusstsein von Menschen.

Im Abschnitt 2 wird zunächst ein Überblick über verwandte Arbeiten zu mentalen Modellen der IT-Sicherheit gegeben. Dann wird im Abschnitt 3 unsere Untersuchung zur Ermittlung mentaler Modelle der IT-Sicherheit bei der Benutzung mobiler Endgeräte vorgestellt. Anschließend werden im Abschnitt 4 die Ergebnisse der Arbeit diskutiert und schließlich im Abschnitt 5 weiterführende Arbeiten vorgeschlagen.

2 Mentale Modelle in der IT-Sicherheit

Erste mentale Modelle für den Themenkomplex der IT-Sicherheit erstellten Camp et al. [ALC07, Cam09]. Sie unterscheiden fünf Metaphern der IT-Sicherheit: physische Sicherheit (z.B. Schlösser), medizinische Infektionen (Viren), kriminelles Verhalten (Einbrecher), Kriegsführung und wirtschaftliches Versagen (Schwachstellen in der Software).

Implizite Beschreibungen der mentalen Modelle der IT-Sicherheit finden sich häufig in Publikationen zum Themenkomplex der Mensch-Computer-Interaktion. So fanden Sasse et al. [SBW01] heraus, dass die Kenntnisse der Nutzer nicht ausreichend sind, um die bestehenden Sicherheitsbedrohungen richtig einzuordnen. Norman [Nor09] beobachtet, dass die Anwender sogar die Installation essentieller Sicherheitspatches abgelehnt haben aus Angst etwas Falsches zu installieren. Ihr mentales Modell lautet: „Installieren neuer Software ist gefährlich“. Häufig sind die Anwender aufgrund fehlender Kenntnisse nicht in der Lage zwischen sicheren und unsicheren Installationsanfragen zu unterscheiden.

Inakkurate mentale Modelle schaffen oft weitere Gefahrenquellen [RHJ+10]. Unter anderem erstellen Anwender eigene Regeln im Umgang mit IT-Systemen, wie z.B. nur scheinbar sichere Passwörter, die ihnen besser im Gedächtnis bleiben [AS99, FH07, FCB07].

Für die Anwender ist ihr sicherheitskonformes Handeln eine Kosten-/Nutzen-Kalkulation [Her09]. Werden die Kosten als zu hoch wahrgenommen, entsteht die Vorstellung „Sicherheitsmechanismen sind ein Hindernis, das es zu umgehen gilt“. Nach Ansicht von Lampson [Lam09] hat sich bei vielen Anwendern ein „Sag OK zu jeglichen Sicherheitsfragen“-Modell entwickelt. Die zunehmende Anzahl von Checkboxen, die eine Rückmeldung der Nutzer haben möchten, haben dazu geführt, dass die Anwender herausgefunden haben, welchen Knopf sie drücken müssen, um ungestört ihrer Arbeit weiter nachgehen zu können [SEA+09, KFR10].

Ein weiterer Einflußfaktor auf das Bild der IT-Sicherheit vieler Anwender ist ihr soziales Umfeld.

Verhalten sich Anwender sicherheitsbewusst, werden sie oft als „paranoid“ oder „pedantisch“ beschrieben [SBW01, WS01] oder als eine Person, die niemandem vertraut. Da die Anwender sehr viel Wert darauf legen von ihrem Umfeld akzeptiert zu werden, gehen sie sogar so weit offen zuzugeben, dass sie stolz darauf sind, Sicherheitsmechanismen nicht zu verstehen oder nicht zu befolgen [SBW01].

Die obigen Publikationen beschreiben mentale Modelle der Anwender zur IT-Sicherheit der „klassischen“ Rechnersysteme. Bei der Nutzung mobiler Endgeräte fehlen jedoch bisher mentale Modelle der IT-Sicherheit. Im folgenden Abschnitt wird unser Vorgehen zur

Erstellung solcher mentalen Modelle sowie die daraus resultierenden Ergebnisse vorgestellt.

3 Studien zur IT-Sicherheit bei der Nutzung mobiler Endgeräte

Ein erster Überblick über den Themenkomplex „Anwender und ihr mobiles Endgerät“ wurde durch die Erstellung einer Pilotstudie verschafft. In der Hauptuntersuchung wurden anschließend mentale Modelle der IT-Sicherheit bei der Nutzung mobiler Endgeräte erstellt. Beide Untersuchungen wurden anhand eines Fragebogens als Leitfaden-Interviews durchgeführt.

3.1 Pilotstudie

In der Pilotstudie wurde die Nutzung mobiler Endgeräte betrachtet. Es haben sich zwei mentale Grundmodelle bei der Nutzung mobiler Endgeräte herauskristallisiert. Zum einen gibt es Anwender, die ihr Endgerät nur als konventionelles Telefon-Gerät sehen. *Trotz eines deutlich größeren Funktionsumfanges*, nutzen sie ihr Gerät fast ausschließlich zum Telefonieren oder Schreiben von Kurznachrichten. Zum anderen gibt es Nutzer, die ihr Endgerät als Smartphone sehen. Bei diesen übersteigt die tägliche Nutzung deutlich den Rahmen konventioneller Telefon-Geräte: sie surfen im Internet, schreiben E-Mails oder tauschen sich über soziale Netzwerke aus. Diese mentalen Grundmodelle („Telefon“ vs. „Smartphone“) wurden in der Hauptuntersuchung detaillierter betrachtet.

Weiter konnte in der Pilotstudie festgestellt werden, dass sich Nutzer wenig mit der IT-Sicherheit ihres Endgeräts befassen. Sie fühlen sich oft sicher bei der Nutzung ihres mobilen Endgeräts, ohne sich in den Themenkomplex einzuarbeiten oder eigene Anstrengungen für IT-Sicherheit im mobilen Umfeld zu unternehmen.

3.2 Hauptuntersuchung

Das Ziel der Hauptuntersuchung war eine detaillierte Beschreibung der Sichtweise der Nutzer auf die IT-Sicherheit ihrer mobilen Endgeräte.

3.2.1 Hypothesen

Auf Grundlage der Untersuchungen und Ergebnisse der Pilotstudie wurden unter anderem folgende Hypothesen aufgestellt:

- H1: Benutzer, die ihr Gerät als Smartphone sehen, haben ein größeres *Sicherheitsbewusstsein* als Benutzer, die ihr Gerät als Telefon sehen.

- H2: Benutzer, die ihr Gerät als Smartphone sehen, fühlen sich weniger sicher, als Benutzer, die ihr Gerät als Telefon sehen.
- H3: Benutzer sehen sich selbst nicht für die Sicherheit ihrer Geräte verantwortlich.
- H4: Benutzer bringen Probleme bei der Benutzung ihres Endgeräts nicht mit IT-Sicherheit in Verbindung.
- H5: Um für ihre IT-Sicherheit im mobilen Umfeld zu sorgen, ist die Hauptanstrengung der Benutzer der *bewusste Umgang* mit dem Gerät.

Die beiden Begriffe „Sicherheitsbewusstsein“ und „bewusster Umgang“ werden weiter unten erläutert. Eine ausführliche und vollständige Beschreibung der Hypothesen und der dazugehörigen Ergebnisse findet sich in Krupp [Kru11].

3.2.2 Versuchsbeschreibung

Um die aufgestellten Hypothesen zu evaluieren, wurden persönliche Leitfragen-Interviews mit 24 Versuchspersonen durchgeführt. Das Alter der Befragten lag zwischen 18 und 50 Jahren, die Hälfte war männlich und fünf waren beruflich im IT-Umfeld tätig.

Die Interviews orientierten sich an einem zweiteiligen Fragebogen (s. Anhang A). Die Schwierigkeit einer aussagekräftigen Evaluation besteht darin, dass sich die Teilnehmer dem Untersuchungsfokus und der Untersuchungssituation nicht bewusst sein dürfen, da sie sich sonst anders verhalten als bei einer Entscheidungsfindung im Alltag [RWN02]. Daher wurde bei der Erstellung der Fragen darauf geachtet, dass die Teilnehmer zumindest von Anfang an nicht wussten, dass sie in Bezug auf IT-Sicherheit untersucht wurden.

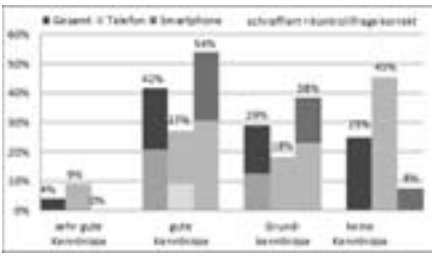
Im ersten Teil der Interviews stand die Nutzung mobiler Endgeräte im Fokus. Hierbei wurden die Teilnehmer unter anderem zu regelmäßig genutzten Diensten, zu Eigenschaften, die sie mit der Nutzung mobiler Endgeräte verbinden, zu Problemen bei deren Nutzung und Kenntnissen zum Schutz mobiler Endgeräte befragt. Weiterhin wurde gefragt zu welchem Anteil sie sich selbst und die Hersteller von Programmen oder Hardware in der Verantwortung für die Umsetzung von IT-Sicherheit bei mobilen Endgeräten sehen.

Der zweite Teil des Fragebogens konzentrierte sich auf die Anstrengungen der Befragten zur Sicherstellung von IT-Sicherheit. Hierbei mussten sie angeben wie groß ihr Interesse an der Sicherheit ihres Endgerätes ist und welche Anstrengungen sie für die Umsetzung unternehmen. Ob sie sich bei der Nutzung ihres Endgeräts sicher fühlen und welche Daten ihrer Meinung nach auf dem Endgerät bedroht sind. Abschließend wurde eine Frage zu einer erweiterten Sicherheitseinstellung gestellt, um die Selbsteinschätzung der Befragten bezüglich ihrer Kenntnisse besser einordnen zu können.

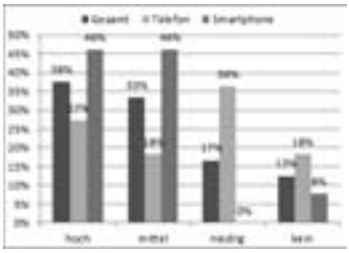
3.2.3 Evaluierung der Hypothesen

H1: Benutzer, die ihr Gerät als Smartphone sehen, haben ein größeres Sicherheitsbewusstsein als Benutzer, die ihr Gerät als Telefon sehen. Unter Sicherheitsbewusstsein

verstehen wir einen Komplex aus dem Wissen über die IT-Sicherheit und dem Interesse an IT-Sicherheit. Insgesamt sahen elf Befragte ihr Endgerät als konventionelles Telefon und 13 als Smartphone. Sieben der 13 Befragten (54 %), die ihr mobiles Endgerät als Smartphone sehen, gaben an, dass sie über gute Kenntnisse zum Schutz mobiler Endgeräte verfügen würden (s. Abbildung 1(a)). Fünf der Smartphone-Benutzer (38 %) ordneten sich mit Grundkenntnissen ein. Die Hälfte dieser Benutzer beantwortete die Kontrollfrage korrekt.



(a) Wie schätzen Sie ihr Wissen bezüglich des möglichen Schutzes ihres mobilen Endgeräts ein?



(b) Wie schätzen Sie ihr Interesse bezüglich der Sicherheit von mobilen Endgeräten und ihrer Daten ein?

Abbildung 1: Ergebnisse zu Hypothese 1

Bei den 11 Befragten, die ihr Endgerät als Telefon sehen, gaben lediglich vier Befragte an, dass sie mindestens gute Kenntnisse über den Schutz mobiler Endgeräte verfügen. Nur einer dieser Anwender konnte ebenfalls die Kontrollfrage korrekt beantworten.

Zu den insgesamt schlechteren Kenntnissen der Telefon-Anwender kommt hinzu, dass diese im Allgemeinen kein all zu großes Interesse an der Sicherheit ihres Endgeräts haben. Abbildung 1(b) zeigt, dass sechs der elf Befragten nur ein geringes bzw. gar kein Interesse an der Sicherheit ihres Endgeräts haben.

Bei den Befragten, die ihr Endgerät als Smartphone sehen, ist das Interesse sichtbar stärker ausgeprägt. Sechs Studienteilnehmer gaben ein mittleres, weitere sechs ein hohes Interesse an.

Die Teilnehmer wurden in einer offenen Frage zu ihnen bekannten Bedrohungen im mobilen Umfeld befragt. Die Gruppierung der Antworten ergab eine Übereinstimmung zu den sechs Gruppierungen des „Malicious Mobile Threats Report 2010/2011“ von Juniper [Jun11]: Abhören von Datenübermittlungen, Ausnutzung/Fehlverhalten, Erstellung von Bewegungsprofilen/Ortung, Direkte Angriffe, Malware sowie Verlust/Diebstahl.

Korreliert man die Anzahl der genannten Bedrohungsklassen der Anwender mit deren selbst eingeschätzten Kenntnissen, zeigt sich, dass viele Anwender, die sich mit guten Kenntnissen einordneten, mehr Bedrohungen nennen konnten (s. Abbildung 2).

Vergleicht man die Ergebnisse der beiden mentalen Grundmodellen, so wird deutlich, dass die Smartphone-Anwender mehr Bedrohungen als die Telefon-Anwender nennen konnten und ihre Kenntnisse verhältnismäßig gut eingeschätzt haben. Hierzu besteht jedoch weiterer Forschungsbedarf, da die Anzahl der Befragten insgesamt zu gering war.

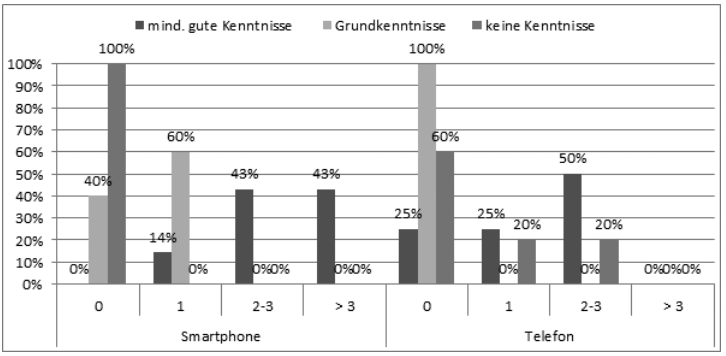
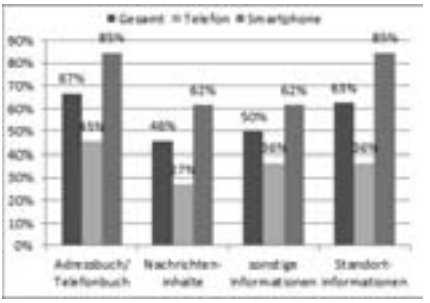


Abbildung 2: Anzahl der genannten Bedrohungen in Relation zu den eingeschätzten Kenntnissen

Zusammenfassend zeigen die Ergebnisse, dass Anwender, die ihr mobiles Endgerät als Smartphone sehen, bessere Kenntnisse zum Schutz und ein größeres Interesse an der Sicherheit mobiler Endgeräte haben. Somit konnte die erste Hypothese belegt werden.

(a) Fühlen Sie sich bei der Benutzung ihres Endgeräts sicher?



(b) Welche Daten auf ihrem Endgerät sind ihrer Meinung nach bedroht?

Abbildung 3: Ergebnisse zu Hypothese 2

H2: Benutzer, die ihr Gerät als Smartphone sehen, fühlen sich weniger sicher, als Benutzer, die ihr Gerät als Telefon sehen. 17 der 24 Befragten gaben an, dass sie sich bei der Nutzung ihres mobilen Endgeräts sicher fühlen (s. Abbildung 3(a)).

Dies zeigt ein insgesamt hohes Sicherheitsgefühl der Anwender. Die Betrachtung der beiden Grundmodelle zeigt, dass sich deutlich weniger Smartphone-Anwender bei der Nutzung ihres Endgeräts sicher fühlen. Gründe für die Unsicherheit sind nach Ansicht dieser Nutzer die Überwachung von Datenflüssen und das Aufzeichnen von Standortdaten.

Das höhere Sicherheitsempfinden der Telefonanwender führten diese darauf zurück, dass sie mit ihrem Endgerät nicht ins Internet gehen. Als weitere Gründe gaben sie an, dass sie nicht wichtig genug für einen Angreifer wären und dass sie keine wichtigen Daten auf

ihrem Endgerät hätten.

Abbildung 3(b) zeigt, dass nach Ansicht aller Befragten besonders das Adressbuch und Telefonbuch sowie die Standortinformationen auf dem mobilen Endgerät bedroht sind. Die Telefon-Anwender sehen durchschnittlich deutlich weniger Daten auf dem mobilen Endgerät bedroht. Damit kann die zweite Hypothese belegt werden.

H3: Benutzer sehen sich selbst nicht für die Sicherheit ihrer Geräte verantwortlich. Um herauszufinden bei wem die Befragten die Verantwortung für die Sicherheit mobiler Endgeräte sehen, wurden sie gebeten, den Programmherstellern, Hardwareherstellern und sich selbst einen prozentualen Anteil der Verantwortung zuzuteilen. Es zeigte sich, dass nach Ansicht der Befragten fast die Hälfte der Verantwortung auf die Programmhersteller fällt (s. Abbildung 4). Die Hersteller von Hardware und den Benutzer selbst sehen die Befragten zu jeweils einem Viertel in der Verantwortung.

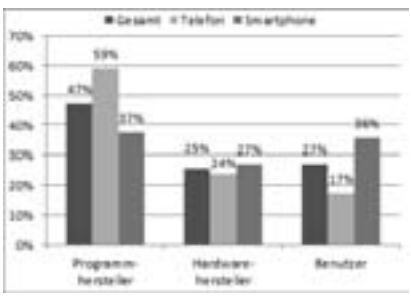


Abbildung 4: Wer sollte für die Sicherheit von mobilen Endgeräten verantwortlich sein?

Anwender, die ihr Gerät als Telefon sehen, sehen den Benutzer am wenigsten in der Verantwortung für die Sicherheit. Dagegen sehen die Smartphone-Nutzer die Programmhersteller und den Benutzer zum gleichen Prozentanteil verantwortlich.

Anhand dieser Ergebnisse kann die dritte Hypothese belegt werden, denn die Benutzer zeigen eine deutliche Präferenz dazu, den Programm- und Hardwareherstellern die Verantwortung für die Sicherheit ihrer Geräte zu geben. Jedoch sehen insbesondere Smartphone-Anwender einen Teil der Verantwortung bei sich selbst. Inwieweit sie bereit sind, diese Verantwortung zu übernehmen, bedarf weiterer Forschung.

H4: Benutzer bringen Probleme bei der Benutzung ihres Endgeräts nicht mit IT-Sicherheit in Verbindung. Im Zuge des ersten Teils der Befragung wurden die Teilnehmer gefragt, ob sie bei der Nutzung ihrer Geräte bisher Probleme hatten. Sieben der 24 Befragten gaben ein Problem an. Die geschilderten Probleme ließen sich alle auf die Bedienung bzw. Eigenheiten des Endgeräts zurückführen, wie z.B. das Aufhängen bzw. Abstürzen des Geräts, eine schlechte Akkulaufzeit, Probleme mit dem Betriebssystem oder ein unzureichender Funktionsumfang.

Als die Teilnehmer im zweiten Teil der Befragung explizit zu sicherheitskritischen Problemen bei der Nutzung mobiler Endgeräte befragt wurden, gab ein Teilnehmer an, dass er bisher ein sicherheitskritisches Problem hatte. Durch das versehentliche Klicken eines Hyperlinks beim Surfen im Internet sei er in eine Abo-Falle geraten. Bei der allgemein gehaltenen Frage zu Problemen bei der Nutzung gab er dieses Problem jedoch nicht an.

Auch in der Pilotstudie wurde die Beobachtung gemacht, dass mehrere Teilnehmer zwar Probleme bei der Nutzung mit ihrem Endgerät angaben, dabei aber keine Sicherheitsprobleme erwähnten. Zwei Benutzer gaben auch dort sicherheitskritische Probleme erst dann an, als sie explizit darauf angesprochen wurden.

Somit kann belegt werden, dass die sicherheitskritischne Probleme sich bei der Nutzung mobiler Endgeräte nicht in den mentalen Modellen der Anwender verankert haben. Das könnte damit zusammenhängen, dass die Teilnehmer bisher sehr wenig mit solchen Problemen konfrontiert wurden.

H5: Um für ihre IT-Sicherheit im mobilen Umfeld zu sorgen, ist die Hauptanstrengung der Benutzer der bewusste Umgang mit dem Gerät. Die Interviewpartner wurden gebeten, anhand vorgegebener Sicherheitsvorkehrungen anzugeben, welche Anstrengungen sie unternehmen, um für die eigene IT-Sicherheit im mobilen Umfeld zu sorgen.

Bewusster Umgang mit dem Gerät ist die populärste Sicherheitsmaßnahme (s. Tabelle 1). Nur 8 % der Befragten gaben an, dass sie sich nie mit dem bewussten Umgang ihres Endgeräts auseinandersetzen. Während die Mehrzahl der Smartphone-Anwender versucht immer auf einen bewussten Umgang zu achten, gaben 64 % der Telefon-Anwender an, sich gelegentlich darum zu kümmern. Unter bewusstem Umgang verstehen die Teilnehmer, dass sie unter anderem bei der Nutzung ihres Endgeräts darauf achten, welche Applikationen sie installieren und nutzen und dass sie verantwortungsbewusst im Internet unterwegs sind.

Des Weiteren informiert sich nur ein Viertel nicht über IT-Sicherheitsrisiken. Hierunter ist fast die Hälfte aller Anwender, die ihr Endgerät als Telefon sehen. Die restlichen Befragten informieren sich in der Regel gelegentlich über aktuelle Gefahren.

Technische Sicherheitsmaßnahmen werden seltener eingesetzt. 38 % aller Befragten nutzen regelmäßig den Passwortschutz auf ihren mobilen Endgeräten und 21 % nutzen ihn gelegentlich. Insbesondere fallen die 62 % der Smartphone-Anwender auf, die den Passwortschutz regelmäßig einsetzen. Ähnliche Werte gelten für Updates, Virenscanner sind weniger populär. Im PC-Umfeld dagegen gibt es regelmäßig Studien, die zeigen, dass über 75 % einen Virenscanner auf ihrem PC installiert haben [BIT10, BSI11]. Gründe für diese Ergebnisse könnten u.a. in den Voreinstellungen der Geräte liegen, wurden in dieser Arbeit jedoch nicht weiter untersucht.

Somit konnte die fünfte Hypothese belegt werden. 88 % der Teilnehmer gaben an wenigstens gelegentlich auf den bewussten Umgang mit dem mobilen Endgerät zu achten. Nach

	mentales Grob-model	Ich versuche immer auf dem aktuellsten Stand zu sein	Ich kümmere mich gelegentlich um die Thematik	Ich kümmere mich gar nicht um die Thematik	Weiß ich nicht
Passwortschutz	Gesamt	38%	21%	25%	17%
	Telefon	9%	27%	45%	18%
	Smartphone	62%	15%	8%	15%
Updates	Gesamt	42%	21%	21%	17%
	Telefon	9%	27%	45%	18%
	Smartphone	69%	15%	0%	15%
Virenscanner	Gesamt	21%	13%	42%	25%
	Telefon	9%	18%	55%	18%
	Smartphone	31%	8%	31%	31%
bewusster Umgang	Gesamt	46%	42%	8%	4%
	Telefon	9%	64%	18%	9%
	Smartphone	77%	23%	0%	0%
Informieren über IT-Sicherheitsrisiken	Gesamt	17%	50%	25%	8%
	Telefon	0%	36%	45%	18%
	Smartphone	31%	62%	8%	0%

Tabelle 1: Welche eigenen Anstrengungen unternehmen Sie um für ihre IT-Sicherheit im mobilen Umfeld zu sorgen?

Ansicht der Interviewpartner sind sie so lange sicher vor Bedrohungen, so lange sie sich vorsichtig und gewissenhaft verhalten sowie selbst keine Fehlerzustände verursachen.

4 Mentale Modelle der Sicherheit mobiler Endgeräte

Unsere Untersuchung zeigt, dass die Benutzer der mobilen Endgeräte in zwei Kategorien unterteilt werden können, die sich deutlich hinsichtlich ihrer Einstellung zur IT-Sicherheit ihrer Geräte unterscheiden. Die *„mein Gerät ist ein Telefon“*-Einstellung ist unabhängig vom Funktionsumfang des Geräts und hängt mit einem niedrigeren Sicherheitsbewusstsein und einem höheren Sicherheitsgefühl zusammen, als die *„mein Gerät ist ein Smartphone“*-Einstellung. Insbesondere „Telefon-Benutzer“ sehen sich selbst nicht für die Sicherheit ihrer Geräte verantwortlich und befassen sich insgesamt wenig mit der Thematik.

Es zeigte sich, dass viele Nutzer ein *„solange ich nicht ins Internet gehe, bin ich sicher“*-mentales Modell haben. Außerdem glauben viele Benutzer, dass sie persönlich nicht bedroht sind, da sie nicht wichtig genug sind oder keine wichtigen Daten auf ihrem Gerät speichern. Hier sind die Parallelen zur Risikoeinschätzung in der PC-Welt deutlich sichtbar [Sch08, Wes08].

Im Allgemeinen scheinen die Benutzer jedoch weniger Parallelen zwischen der PC-Welt und der mobilen Welt zu ziehen, da sie die Probleme bei der Nutzung mobiler Endgeräte nicht mit IT-Sicherheit sondern ausschließlich mit der Bedienung und den Eigenheiten der Geräte in Verbindung bringen. Außerdem werden technische Schutzmaßnahmen in der mobilen Welt deutlich weniger eingesetzt als in der PC-Welt.

Zum Schutz im mobilen Umfeld beschränken sich die Anstrengungen zur Zeit fast ausschließlich auf den bewussten Umgang mit dem Gerät. Die Befragten gaben unter anderem an, dass sie sichere Applikationen nutzen, auf unseriöse Dienste verzichten und nicht ungeachtet jegliche Links anklicken würden. Zusätzlich hielten sie ihr Datenvolumen so niedrig wie möglich und achten darauf, nicht ungeschützt über Verbindungsprotokolle wie beispielsweise Bluetooth oder WLAN erreichbar zu sein.

Es scheint, dass viele Benutzer ein *„ich werde Gefahren für mein Gerät auf jeden Fall erkennen können"*-mentales Modell haben. Ob dieses Modell tatsächlich funktioniert, ist zweifelhaft, wenn man Parallelen zur PC-Welt zieht [DTH06, DHC06, SEA+09, RHJ+10]. Es ist auch unklar, ob die meisten Anwender noch keine Sicherheitsprobleme mit ihren Endgeräten hatten oder ob sie solche Probleme noch nicht erkannt haben.

5 Fazit und Weiterführende Arbeiten

Unsere Studie zeigte erste Einblicke darin, wie die Nutzer die Sicherheit ihrer mobilen Endgeräte wahrnehmen und wie sie ihre Geräte schützen.

Obwohl die Nutzer wissen, dass viele Daten auf ihrem mobilen Endgerät bedroht sind, fühlen sie sich bei der Nutzung zum Großteil sicher. Unternehmen die Befragten eigene Anstrengungen für den Schutz im mobilen Umfeld, konzentrieren sich diese häufig auf den bewussten Umgang mit dem Gerät. Anwender mit guten Kenntnissen nehmen zusätzlich zum Schutz technische Sicherheitsvorkehrungen, wie das Nutzen eines Passwortschutzes oder das regelmäßige Installieren von Updates, vor.

Insgesamt ergab unsere erste Untersuchung mehr Fragen als Antworten, so dass weiterer Forschungsbedarf besteht. Es ist z.B. nicht ausreichend bekannt, wie gut die Selbsteinschätzung der Nutzer zu ihren Sicherheitskenntnissen mit den tatsächlichen Kenntnissen korreliert.

Der bewusste Umgang mit dem mobilen Endgerät stellte sich als Hauptanstrengung der Nutzer zur Sicherstellung von IT-Sicherheit im mobilen Umfeld dar. Die Nutzer beschrieben den bewussten Umgang häufig damit, dass sie keine unseriösen Applikationen installieren, auf ihr Surfverhalten im Internet achten und nicht ungeschützt über Kommunikationsschnittstellen wie Bluetooth oder WLAN erreichbar sind. Hierbei ist von Interesse, ob die Anwender ein gemeinsames Bild des bewussten Umgangs haben und ob sie auch unsichere Handlungen mit dem bewussten Umgang verbinden. Darüber hinaus stellt sich die Frage, ob die Anwender tatsächlich über ausreichend Wissen verfügen, um die Unterscheidung zwischen sicheren und unsicheren Applikationen, Links und Einstellungen des Geräts vornehmen zu können.

Ein weiterer Punkt für zukünftige Untersuchungen ist die Frage, ob die Nutzer unterschiedliche Sichtweisen auf PCs und auf mobile Endgeräte haben. Moderne mobile Endgeräte werden immer leistungsfähiger, haben einen immer größeren Funktionsumfang und ähneln immer mehr den PCs. Dennoch scheinen die Anwender noch wenige Parallelen zur PC-Welt zu ziehen und schützen sich im PC-Umfeld in viel stärkerem Maße, obwohl immer mehr Bedrohungen identisch sind.

Literatur

[ALC07] Farzaneh Asgharpour, Debin Liu und L. Jean Camp. Mental models of security risks. In *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security*, FC'07/USEC'07, Seiten 367–377, Berlin, Heidelberg, 2007. Springer-Verlag.

[AS99] Anne Adams und Martina Angela Sasse. Users are not the enemy. *Commun. ACM*, 42:40–46, December 1999.

[BFH+11] M. Becher, F.C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck und C. Wolf. Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices. In *Security and Privacy (SP), 2011 IEEE Symposium on*, Seiten 96–111, may 2011.

[BIT10] BITKOM. Internet-Sicherheit. Studie, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V., Februar 2010.

[BSI11] BSI. Mit Sicherheit. BSI Jahresbericht 2010, Bundesamt für Sicherheit in der Informationstechnik, Juli 2011.

[Cam09] L. J. Camp. Mental models of privacy and security. *Technology and Society Magazine, IEEE*, 28(3):37–46, Fall 2009.

[DHC06] Julie S. Downs, Mandy B. Holbrook und Lorrie Faith Cranor. Decision strategies and susceptibility to phishing. In *Proceedings of the second symposium on Usable privacy and security*, SOUPS '06, Seiten 79–90, 2006.

[DTH06] Rachna Dhamija, J. D. Tygar und Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, CHI '06, Seiten 581–590, 2006.

[FCB07] Alain Forget, Sonia Chiasson und Robert Biddle. Helping users create better passwords: is this the right approach? In *Proceedings of the 3rd symposium on Usable privacy and security*, SOUPS '07, Seiten 151–152, 2007.

[FH07] Dinei Florencio und Cormac Herley. A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web*, WWW '07, Seiten 657–666, 2007.

[Her09] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop*, NSPW '09, Seiten 133–144, 2009.

[Jun11] Juniper Networks. *Malicious Mobile Threats Report 2010/2011: An Objective Briefing on the Current Mobile Threat Landscape Based on Juniper Networks Global Threat Center Research*. Juniper Networks, Inc., 2011.

[KFR10] R. Kainda, I. Flechais und A.W. Roscoe. Security and Usability: Analysis and Evaluation. In *Availability, Reliability, and Security, 2010. ARES '10 International Conference on*, Seiten 275–282, 2010.

[Kru11] Matthias Krupp. Die Verantwortung von Nutzern zur Umsetzung von IT-Sicherheit, Masterarbeit, 2011.

[Lam09] Butler Lampson. Privacy and security: Usable security: how to get it. *Commun. ACM*, 52:25–27, November 2009.

[Nor09] Donald A. Norman. THE WAY I SEE IT: When security gets in the way. *interactions*, 16:60–63, November 2009.

[RHJ+10] Fahimeh Raja, Kirstie Hawkey, Pooya Jaferian, Konstantin Beznosov und Kellogg S. Booth. It's too complicated, so i turned it off!: expectations, perceptions, and misconceptions of personal firewalls. In *Proceedings of the 3rd ACM workshop on Assurable and usable security configuration*, SafeConfig '10, Seiten 53–62, 2010.

[RWN02] K. Rudolph, G. Warshawsky und L. Numkin. Security Awareness. In M.E. Kabay, Hrsg., *Computer Security Handbook*, Kapitel 29. John Wiley & Sons, Inc., Basel, 4. Auflage, 2002.

[SBW01] M. A. Sasse, S. Brostoff und D. Weirich. Transforming the 'Weakest Link' – a Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal*, 19:122–131, July 2001.

[Sch08] Bruce Schneier. The psychology of security. http://www.schneier.com/essay-155.html, Januar 2008.

[SEA+09] Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri und Lorrie Faith Cranor. Crying wolf: an empirical study of SSL warning effectiveness. In *Proceedings of the 18th conference on USENIX security symposium*, SSYM'09, Seiten 399–416, Berkeley, CA, USA, 2009. USENIX Association.

[Wes08] Ryan West. The psychology of security. *Commun. ACM*, 51:34–40, April 2008.

[WS01] Dirk Weirich und Martina Angela Sasse. Pretty good persuasion: a first step towards effective password security in the real world. In *Proceedings of the 2001 workshop on New security paradigms*, NSPW '01, Seiten 137–143, 2001.

A Anhang

Fragebogen zur Nutzung von mobilen Endgeräten

Einleitung zum Fragebogen:

Ziel des Fragebogens ist es das Verhalten von Anwendern im Umgang mit mobilen Endgeräten (Handys und Smartphones) zu untersuchen.

Der Fragebogen besteht aus zwei Teilen. Der erste Teil besteht aus einigen einleitenden und grundlegenden Fragen zur Nutzung von mobilen Endgeräten. Im zweiten Teil steht darauf aufbauend die weitere Nutzung von mobilen Endgeräten im Fokus.

Hinweis zum Datenschutz:

Die Daten werden anonymisiert erhoben und dienen nur zu Forschungszwecken. Der Fragebogen ist so konzipiert, dass kein Rückschluss auf den Befragten möglich ist.

Falls Sie eine Frage nicht beantworten möchten oder können, lassen Sie die Antwort einfach offen.

Vielen Dank für ihre Bereitschaft den Fragebogen auszufüllen!

Teil A

1. Ihr Geschlecht:
   ❒ Weiblich ❒ Männlich

2. Ihr Alter:
   ❒ jünger als 21 ❒ 21 - 25
   ❒ 26 - 30 ❒ 31 - 35
   ❒ 36 - 40 ❒ 41 - 45
   ❒ 46 - 50 ❒ 51 - 55
   ❒ 56 - 60 ❒ 61 oder älter

3. Welchen Beruf üben Sie aus? Welche Fachrichtung?

4. Besitzen Sie privat ein mobiles Endgerät (Handy oder Smartphone)?
   ❒ Ja ❒ Nein

5. Spielt das Betriebssystem ihres mobilen Endgeräts für Sie eine relevante Rolle?
   ❒ Ja ❒ Nein

6. Welche Eigenschaften (Spaß, Erreichbarkeit, Streß etc.) verbinden Sie mit der Nutzung ihres Endgeräts?

7. Besitzt ihr Endgerät die Möglichkeit eigenständig Applikationen zu installieren?
   ❒ Ja ❒ Nein

8. Welche Dienste nehmen Sie privat am meisten in Anspruch?

9. Welche Dienste wünschen Sie sich zusätzlich?

10. Besitzen Sie neben ihrem privaten mobilen Endgerät auch ein Firmengerät?
    ❒ Ja ❒ Nein

11. Wenn ja, wie unterscheidet sich die Benutzung?

12. Welche der folgenden Programme nutzen Sie? (Mehrfachnennungen sind möglich)

privates Endgerät:	*Firmenendgerät:*
❒ E-Mail	❒ E-Mail
❒ Internet	❒ Internet
❒ Geldgeschäfte über Internet, z.B. Onlinebanking	❒ Geldgeschäfte über Internet, z.B. Onlinebanking
❒ Soziale Netzwerke	❒ Soziale Netzwerke
❒ Virenscanner	❒ Virenscanner
❒ Routenplaner	❒ Routenplaner

13. Hatten Sie bisher Probleme bei der Benutzung ihres Endgeräts?
    ❒ Ja ❒ Nein

14. Wenn ja, welche?

15. Wie schätzen Sie ihr Wissen bezüglich des möglichen Schutzes ihres mobilen Endgerätes ein?
    ❒ Sehr gute Kenntnisse ❒ Gute Kenntnisse
    ❒ Grundkenntnisse ❒ Keine Kenntnisse

16. Beurteilen Sie die Wichtigkeit von Benutzbarkeit im Bezug auf IT-Sicherheit auf folgender Skala:

Benutzbarkeit ist wichtiger	gleich wichtig	Sicherheit ist wichtiger

17. Wer sollte für die Sicherheit von mobilen Endgeräten verantwortlich sein? (Bitte verteilen Sie **insgesamt** 100 % auf die drei angegebenen Antwortmöglichkeiten)
    - Hersteller von Programmen ____ %
    - Hersteller von Hardware ____ %
    - Benutzer ____ %

18. Welche Bedrohungen, speziell bezogen auf mobile Endgeräte, kennen Sie?

Teil B

1. Wie schätzen Sie ihr Interesse bezüglich der Sicherheit von mobilen Endgeräten und ihrer Daten ein?

   ❒ hoch ❒ mittel
   ❒ niedrig ❒ kein

2. Hatten Sie auf Ihrem mobilen Endgerät schon einmal Sicherheitsprobleme?

   privates Endgerät: *Firmenendgerät:*
   ❒ Ja ❒ Ja
   ❒ Nein ❒ Nein
   Wenn ja, welche? Wenn ja, welche?

3. Hatten Sie schon einmal Probleme mit sensiblen Daten von sich?

   ❒ Ja ❒ Nein

4. Wenn ja, welche?

5. Fühlen Sie sich bei der Benutzung ihres Endgeräts sicher?

   ❒ Ja ❒ Nein

   Begründung:

6. Welche Daten auf ihrem Endgerät sind ihrer Meinung nach bedroht (Mehrfachnennungen sind möglich)?

   ❒ Adressbuch/Telefonbuch
   ❒ Nachrichteninhalte (SMS/E-Mail)
   ❒ sonstige gespeicherte Informationen (Notizen, etc.)
   ❒ Standortinformationen
   ❒ weitere:

7. Welche eigenen Anstrengungen unternehmen Sie, um für IT-Sicherheit im **mobilen Umfeld** zu sorgen (Mehrfachnennungen sind möglich und erwünscht)?

	Ich versuche immer auf dem neuesten Stand zu sein	Ich kümmere mich gelegentlich um die Thematik	Ich kümmere mich gar nicht um die Thematik	Weiß ich nicht
Virenscanner	❒	❒	❒	❒
Passwortschutz	❒	❒	❒	❒
Updates	❒	❒	❒	❒
bewusster Umgang	❒	❒	❒	❒
Verschlüsselung	❒	❒	❒	❒
Informieren über IT-Sicherheitsrisiken	❒	❒	❒	❒

8. Was verstehen Sie unter dem Begriff *Remote Wipe*?