

FH Schmalkalden  
FB Informatik

**Netzwerk- und Datensicherheit des iPhone  
sowie ausgewählte Anwendungen im Beruf und Alltag**

von

Mark Kießling  
Matrikel-Nr.: xxxxxx

erstellt im Rahmen der Veranstaltung:  
Prof. Dr. Dietmar Beyer  
IT-Sicherheit  
Wintersemester 2008/09

Anschrift des Bearbeiters:

Goetheallee 2  
98693 Ilmenau

Abgabe: 27.03.2009

---

## Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b> .....	<b>2</b>
<b>2</b>	<b>Informationssicherheit</b> .....	<b>3</b>
2.1	Vertraulichkeit .....	3
2.2	Integrität .....	3
2.3	Verfügbarkeit .....	3
2.4	Datenschutz .....	4
<b>3</b>	<b>Anwendungsszenarien des iPhone</b> .....	<b>4</b>
3.1	Beruf .....	5
3.2	Alltag .....	8
3.3	Allgemeine Sicherheitsmaßnahmen .....	9
<b>4</b>	<b>Bekannte Probleme des iPhone</b> .....	<b>11</b>
<b>5</b>	<b>Risikoanalyse und -bewertung</b> .....	<b>14</b>
5.1	PEN-Test .....	14
5.2	Risikobewertung .....	16
<b>6</b>	<b>Fazit</b> .....	<b>17</b>
<b>7</b>	<b>Literaturverzeichnis</b> .....	<b>18</b>

# 1 Einleitung

Diese Arbeit befasst sich mit einem der wohl wichtigsten Gebiete der Informatik, der IT-Sicherheit. Sie betrifft alle Personen, die mit elektronischer Datenverarbeitung in Berührung kommen und hat so in den letzten Jahrzehnten sowohl den Privat- als auch den Geschäftsbereich durchdrungen. Informationen werden zunehmend zu wertvollen Wirtschaftsfaktoren und bilden in vielen Unternehmen sogar die Existenzgrundlage. So sind Erfahrungswerte, Geschäftsprozesse oder Entwicklungspläne häufiger nur noch elektronisch vorhanden und können dadurch nicht mehr ausschließlich über räumliche Zugangsbeschränkungen geschützt werden. Ist erst eine Sicherheitslücke gefunden, ermöglicht es dem Eindringling dank schneller Netzwerktechnik große Datenmengen in kürzester Zeit zu stehlen oder nachhaltigen Schaden anzurichten. Keineswegs ist dieser unberechtigte Zugriff immer sofort ersichtlich, sondern erfolgt in der Regel unauffällig, um nicht auf Gegenmaßnahmen zu stoßen. Auch Privatpersonen müssen sich zwangsläufig mit IT-Systemen auseinandersetzen und besitzen zunehmend digitale Informationen von hohem Schutzinteresse. Fallen sensible Daten, wie Bankinformationen, Unbefugten in die Hände, so könnten diese per Onlinezugang auf die Konten zugreifen und Geld stehlen. Zudem kann unberechtigter Zutritt auf den heimischen Computer auch zu größeren immateriellen Schäden führen, wenn z.B. die digitalen Fotos der letzten Jahre oder ein selbst geschriebenes Buch zerstört werden. Gerade im Privatbereich finden Sicherheitstechniken und Backupstrategien wenig Anwendung, sodass die Verluste oft auch endgültig sind.

Im zweiten Kapitel erfolgt zunächst eine kurze Einführung in ausgewählte Zielstellungen der Informationssicherheit, welche sowohl für geschäftliche als auch für private Datenverarbeitungsvorgänge von Bedeutung sind. Kapitel drei befasst sich mit Anwendungsmöglichkeiten, die das iPhone den betreffenden Nutzern bietet und geht auf Sicherheitsaspekte ein, die dieses Gerät bereits werksseitig erfüllt. In Abschnitt vier werden die Mängel des iPhone, in Bezug auf seine Geschäftstauglichkeit hin, beleuchtet. Die Grundlage hierfür bildet ein Report der Berlecon Research GmbH. Anschließend geht Kapitel fünf auf Risikoanalysen und -bewertungen ein, die ein Teilgebiet firmenspezifischer Sicherheitskonzepte darstellen. Ob dieses Sicherheitskonzept wirksam ist, kann mit Hilfe des in diesem Kapitel näher beschriebenen PEN-Tests überprüft werden.

## 2 Informationssicherheit

Die Informationssicherheit ist ein wesentlicher Aspekt der IT-Sicherheit und bezieht sich auf Systeme die Informationen lagern und verarbeiten. Kaum ein Unternehmen kann heutzutage auf elektronische Datenverarbeitungsanlagen verzichten, da diese es ermöglichen viele Geschäftsprozesse sehr effizient abzuwickeln. Dies stellt unter anderem einen wichtigen Wettbewerbsfaktor dar. Um aus Informationssystemen langfristig einen Vorteil zu erlangen, haben sich drei international anerkannte Sachziele herauskristallisiert, auf die im Folgenden eingegangen wird.<sup>1</sup>

### 2.1 Vertraulichkeit

Die Vertraulichkeit von Informationen ist nicht nur wünschenswert, sondern wird in Deutschland auch durch Rechtsnormen vorgegeben. Es soll sichergestellt werden, dass Informationen nur einem beschränkten Personenkreis zugänglich sind. Die Weitergabe oder gar Veröffentlichung soll dabei wirkungsvoll verhindert werden. Grundlegende Techniken zur Erreichung dieses Ziels sind kryptografische Verfahren, wie das Verschlüsseln von Daten und Datenströmen sowie das Abgrenzen von Benutzergruppen durch geeignete Maßnahmen wie z.B. Passwörter oder biometrische Merkmale.<sup>2</sup>

### 2.2 Integrität

Integrität bezeichnet die Korrektheit der Daten in einem System. Ohne die entsprechenden Befugnisse und Berechtigungen darf keine Modifikation oder Löschung von Daten erfolgen. Dieses Ziel schließt auch Datenmanipulation mit ein, die auf technischen Fehlern beruhen, versehentlich oder vorsätzlich geschehen. Eine technische Möglichkeit Datenveränderungen zu erkennen, ist das Bilden von Prüfsummen.<sup>3</sup>

### 2.3 Verfügbarkeit

Datenverarbeitungsanlagen sind Betriebsmittel, die möglichst jederzeit verfügbar und funktionsbereit sein sollten. Die Verfügbarkeit ergibt sich dabei durch das Verhältnis von „einsatzfähiger Zeit“ zur „Gesamtzeit“ ausgedrückt in Prozent. Je weiter sich die Verfügbarkeit an 100 %

---

<sup>1</sup> Vgl. Hungenberg, Informationssicherheit: Einleitung, 2000, Online-Dokument.

<sup>2</sup> Vgl. Bundesamt für Sicherheit in der Informationstechnik, Sicherheit im Internet, 23.April 2007, Online-Dokument; Hungenberg, Informationssicherheit: Sachziele, 2000, Online-Dokument.

<sup>3</sup> Vgl. Bundesamt für Sicherheit in der Informationstechnik, Sicherheit im Internet, 23.April 2007, Online-Dokument; Hungenberg, Informationssicherheit: Sachziele, 2000, Online-Dokument.

annähern soll, desto aufwendiger werden die erforderlichen Maßnahmen. Einerseits muss ein zuverlässiges und ausfallsicheres System eingesetzt werden, andererseits sollten vorab Maßnahmen geplant werden, die im Falle eines Ausfalls greifen. Dazu gehören u.a. Backupstrategien und Ersatzhardware.<sup>4</sup>

## 2.4 Datenschutz

Der Datenschutz ist kein international anerkanntes Ziel, aber in Deutschland und einigen anderen Ländern gesetzlich vorgeschrieben. Zweck dieser Gesetze ist die Wahrung von Persönlichkeitsrechten und Schutz der personenbezogenen Daten. Im Unternehmensumfeld ergeben sich dabei bereits Einschränkungen, was die Erfassung von personenbezogenen Daten betrifft. Ohne das Vorliegen einer konkreten Zweckbindung ist dies bereits unzulässig. Des Weiteren unterliegen diese persönlichen Daten einem besonders hohen Schutzinteresse, welches zu beachten gilt. Gelangen solche durch fahrlässige Sicherheitslücken im Unternehmen nach Außen, kann dies rechtliche Konsequenzen und Schadensersatzansprüche nach sich ziehen.

Wird die IT-Infrastruktur einer Firma verändert oder erweitert, sollte den zuvor genannten Punkten immer erneut Beachtung geschenkt werden. Lassen sich neue Geräte oder Komponenten nicht vollständig an das selbst definierte Sicherheitskonzept anpassen, ist Vorsicht geboten. Unter diesem Gesichtspunkt wird auch das iPhone aus dem Hause Apple betrachtet, welches sowohl hohes Potential für geschäftliche Anwendungsszenarien bietet, aber auch aufgrund von Schwachstellen zu einer Gefahr für das Unternehmen werden kann.

## 3 Anwendungsszenarien des iPhone

Erst nach Unterstützung von Drittanbietersoftware und einem größeren Update der Firmware konnte das iPhone seit Sommer 2008 auch über den mitgelieferten Funktionsumfang hinaus für verschiedenste Aufgaben eingesetzt werden. Durch diese Erweiterung wurde das Gerät erst für Businessanwendungen interessant, da ihm vorher wichtige grundlegende Integrationsmöglichkeiten wie z.B. verschlüsselte Netzwerkanbindung via VPN fehlten.<sup>5</sup> Apple verfolgt aber weiterhin eine strenge Vertriebspolitik, welche ausschließlich Applikationen aus dem App Store, dem herstellereigenen Softwareshop, für die Installation auf dem iPhone zulässt.

---

<sup>4</sup> Vgl. Hungenberg, Informationssicherheit: Sachziele, 2000, Online-Dokument; Bundesamt für Sicherheit in der Informationstechnik, Sicherheit im Internet, 23.April 2007, Online-Dokument.

<sup>5</sup> Vgl. Lange, 01.August 2008, S. 24.

### 3.1 Beruf

Mit Erscheinung der Firmware 2.0 und dem Software Development Kit können Programmierer seit Anfang März 2008 eigene Applikationen für das iPhone schreiben. So reagierten viele Softwarehersteller umgehend damit, ihre Businesslösungen auch für das iPhone anzupassen. Die Anwendungsvielfalt ist innerhalb kürzester Zeit auf über 15.000 Programme<sup>6</sup> angestiegen, welche übersichtlich in Rubriken gegliedert sind. Im nachfolgenden wird auf einige ausgewählte Lösungen eingegangen, welche eher in mittelständigen und großen Unternehmen Einsatz finden.

*Mobiles CRM*<sup>7</sup> – *update.seven touch*, Salesforce CRM Mobile<sup>8</sup>

Die Firma update software AG<sup>9</sup> bietet branchenorientierte CRM-Lösungen an und war eines der ersten Unternehmen, welches seine web-basierenden Anwendungen für die Nutzung mit einem iPhone angepasst hat. Unter mobilem CRM versteht man die Bearbeitung, Verwaltung und Dokumentation der Kundenbeziehungen von unterwegs. In nebenstehender Abbildung (Abb. 1)<sup>10</sup> wird ersichtlich, für welche Personengruppe in Verbindung mit dem Komplexitätsgrad des Geschäftsprozesses das iPhone geeignet erscheint, und ob die Systemanbindung eine permanente Onlineverbindung benötigt. Gerade für Unternehmen mit verstärktem Außendienst im Bereich Beratung, Verkauf und Service kann dies einen großen

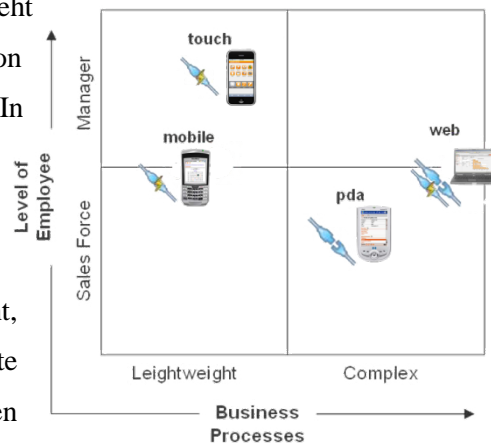


Abb. 1

Wettbewerbsvorteil bewirken. Aus der direkten Datenanbindung zum CRM-System und dem Innendienst ergeben sich vor allem auch Geschwindigkeitsvorteile im Workflow. Dadurch können Kundenanfragen oder Aufträge sofort weitergeleitet werden und die Auftragsbestätigung erreicht den Außendienstmitarbeiter vielleicht noch ehe er den Kundenbesuch beendet. Durch Medienumbrüche in der Auftrags- und Serviceabwicklung kommt es auch immer noch zu Situationen, in denen verschiedene Mitarbeiter andere Informationsstände eines Kunden besitzen. Dies wird durch den zentralen Ansatz des CRM wirksam verhindert. Die speziell für das iPhone entwickelte Oberfläche wurde an das gewohnte

<sup>6</sup> Vgl. Apple Inc., Apple – iPhone, o.J., Online-Dokument.

<sup>7</sup> Customer Relationship Management.

<sup>8</sup> Vgl. salesforce.com Germany GmbH, Product Tour: Salesforce for iPhone, o.J., Online-Dokument.

<sup>9</sup> Vgl. update software AG, update - Ihr kompetenter Partner für CRM, o.J., Online-Dokument.

<sup>10</sup> Vgl. Quelle: Witvoet, Mobile CRM, 2009, S. 9, Online-Dokument.

Layout des Handys angepasst, welches durch einfache Menüführung und Übersichtlichkeit aufwartet. Typische Geschäftsfälle, wie die Abfrage von Kundenterminen, direkte Telefonanwahl, Navigation zur Kundenadresse sowie Klassifizierung der Wichtigkeit des Kunden, werden bereitgestellt. Im Rahmen dieser Studienarbeit kann Aufgrund des Umfangs nicht weiter auf die Vorzüge des mobilen Kundenbeziehungsmanagement eingegangen werden.<sup>11</sup> Doch bietet gerade diese Verwendungsart von mobilen Endgeräten die größten Wachstumsaussichten im Geschäftsbereich. Unternehmen wie die Deutsche Bank, der Axel Springer Verlag oder die HSBC Group erwägen eine Einführung des iPhone als Standard-Business-Handy.<sup>12</sup>

#### *Microsoft Exchange ActiveSync*

ActiveSync wurde von Microsoft entwickelt, um Informationen zwischen PC's und mobilen Endgeräten auszutauschen. Die Firma Apple hat sich diese Anwendung für das iPhone lizensieren lassen und mit der Firmware 2.0 dem Benutzer verfügbar gemacht. Die dadurch ermöglichte Anbindung an den firmeneigenen Exchange Server ist ein wichtiger Schritt für eine geschäftliche Nutzung des Gerätes. Über diese geschaffene Schnittstelle können E-Mails, Kalendereinträge, Aufgaben und Kontaktdaten synchronisiert werden. Auch der Zugriff auf ein globales Firmenkontaktverzeichnis wird ermöglicht. Geht das Handy verloren oder wird gestohlen, lassen sich über eine so genannte Remote-Wipe-Funktion vertrauliche Daten per Fernzugriff vom Gerät löschen.<sup>13</sup>

#### *iControl, iOutBank*

Sowohl iControl, als auch iOutBank sind iPhone-Anwendungen, die eine Schnittstelle zum Onlinebanking liefern. Sie ermöglichen es jederzeit die eigene Finanzlage zu überprüfen und übliche Banktransaktionen durchzuführen. Abgerundet werden diese Funktionen durch eine automatische Budgetbuchung von Kontoumsätzen, die Übermittlung von Aktienkursen und die Unterstützung von standardisierten Datenaustauschformaten wie dem XML-Format.<sup>14</sup>

---

<sup>11</sup> Vgl. update software AG, update.seven touch, o.J., Online-Dokument; Witvoet, Mobile CRM, 2009, S. 3-6, Online-Dokument.

<sup>12</sup> Vgl. Bremmer, 22.August 2008, S.7.

<sup>13</sup> Vgl. Apple Inc., Apple - iPhone - Unternehmen – Integration, o.J., Online-Dokument.

<sup>14</sup> Vgl. Hoang, Hoang – iControl, o.J., Online-Dokument; stoeger it GmbH, OutBank - Die Mobile Banking Software, o.J., Online-Dokument.

*SuitePhone by Netsuite – ERP, CRM und Ecommerce*

Der Anbieter Netsuite bietet Firmenkunden ein Komplettsystem an, welches alle grundlegenden geschäftlichen Vorgänge organisiert. Speziell für das iPhone wurde das Produkt SuitePhone entwickelt, dessen serverseitige Anpassung für die korrekte Darstellung und Steuerung der Funktionalitäten im Safari-Browser<sup>15</sup> sorgt. Über die bereits erwähnten CRM-Fähigkeiten hinaus können Netsuite-Kunden auch auf ERP-Funktionalitäten zugreifen und somit Kapital, Betriebsmittel und Personal verwalten. Selbst die Administration und Pflege von Webshops wird zur Verfügung gestellt. Eine Nutzung all dieser Möglichkeiten setzt allerdings immer voraus, dass das betreffende Unternehmen bereit ist, die eigene Firmenstruktur mit ihren Geschäftsprozessen auf das webbasierende Netsuiteportal abzubilden. Auf der einen Seite stellt sich die Frage der Kosten für die Dienstleistung, auf der anderen Seite muss dem Anbieter großes Vertrauen entgegen gebracht werden, da er tiefen Einblick in die internen Unternehmensabläufe erhält. In diesem Zusammenhang sollte abgewogen werden, ob es effizienter ist, nur ausgewählte Funktionsbereiche wie das CRM auszulagern und eine Schnittstelle zur firmeneigenen ERP-Lösung zu schaffen. Denkbar wäre auch einzelne Module eines bereits vorhandenen Systems, wie z.B. SAP, über eine Web-Oberfläche zugänglich zu machen, was dann allerdings zwangsläufig zu erhöhten Sicherheitsanforderungen führt.<sup>16</sup>

*i-Clickr*

Durch gezielte Software-Erweiterungen kann das iPhone auch Zusatzhardware entbehrlich machen. Diesen Ansatz verfolgt das Tool „i-Clickr PowerPoint Remote“, welches das iPhone zu einer Präsentationsfernbedienung für Microsoft PowerPoint umfunktioniert. Die Kommunikation zwischen Smartphone und PC erfolgt dabei über den etablierten WLAN-Standard IEEE-802.11 im AdHoc-Betrieb. Nachteilig an dieser ressourcensparenden Lösung ist der erhöhte Installations- und Konfigurationsaufwand. Sowohl auf dem iPhone, als auch auf dem PC muss i-Clickr installiert werden, zudem muss eine AdHoc-Verbindung zwischen den beteiligten Geräten aufgebaut sein. Anschließend lassen sich typische Befehle, wie das Weiterschalten von Folien, direkt über den Touchscreen des iPhone absetzen.<sup>17</sup>

---

<sup>15</sup> Webbrowser der Firma Apple für das hauseigene Betriebssystem Mac OS X.

<sup>16</sup> Vgl. NetSuite Inc., Introducing SuitePhone, o.J., Online-Dokument.

<sup>17</sup> Vgl. Senstic Inc., i-Clickr PowerPoint Remote, o.J., Online-Dokument.

## 3.2 Alltag

Jenseits vom beruflichen Nutzen hat sich das iPhone bereits im Privatbereich einen Namen gemacht. Laut einer Studie der Nielsen Company hatte das Smartphone bereits Anfang Juli 2008 einen Marktanteil von 0,3 % in Europa. Davon verwenden 63 % der Nutzer ihr Gerät ausschließlich privat. Die am meisten verwendeten Zusatzfunktionen sind der MP3-Player (74 %), WLAN (64 %) und die integrierte Kamera (54 %). Darüber hinaus kann das iPhone durch Applikationen aus dem AppStore um fast jede denkbare Funktion erweitert werden.<sup>18</sup>

Aufgrund der Vielfalt an Anwendungen, wird in dieser Arbeit nur auf einige ausgewählte Vertreter eingegangen, die zum Teil technische Voraussetzungen des iPhone nutzen.

### *Cycorder*

Fast alle auf dem Markt befindlichen Handys mit integrierter Kamera bieten auch die Funktion Videoclips aufzunehmen. Das iPhone unterstützt dies von Herstellerseite aus nicht. Um die Funktionslücke zu schließen, hat der Programmierer Jay Freeman die Software Cycorder entwickelt. Dieses, zudem noch kostenlose Programm, zeichnet Videos auf und speichert selbige anschließend auf dem internen Speicher.

### *Around Me*

Around Me der Firma Tweakersoft eröffnet dem iPhone-Besitzer die Möglichkeit standortbezogene Dienste kostenlos in Anspruch zu nehmen. Entsprechend der aktuellen Position des Nutzers werden nahegelegene Geschäfte, Tankstellen und Restaurants aufgelistet. Dazu bedient sich die Software an den Koordinaten des integrierten GPS-Moduls und ruft anschließend über eine bestehende Internetanbindung entsprechende Datenbanken des Herstellers ab.

### *Path Tracker*

Die Softwarelösung Path Tracker wendet sich an Personen, die ihre zurückgelegten Wegstrecken erfassen möchten. Egal ob beim Joggen, Fahrradfahren, Segeln oder Wandern, es wird regelmäßig die aktuelle Position erfasst und gespeichert. Die so aufgezeichneten Routen können über einen Path-Tracker-Account anderen Nutzern zur Verfügung gestellt werden oder lassen sich in geeignetes Kartenmaterial einpflegen.

### *Fahrplan*

Dieses kostenlose Programm war schon nach kurzer Zeit auf Platz eins der nützlichen iPhone-Tools. Die Funktionsweise ist simpel. Der Nutzer trägt alle Haltestellen der öffentlichen

---

<sup>18</sup> Vgl. The Nielsen Company GmbH, Nielsen veröffentlicht iPhone-Statistik, 2008, Online-Dokument.

Verkehrsmittel ein, die für ihn als Zustieg in Betracht kommen. Danach kann die Software jederzeit – eine Internet-Verbindung vorausgesetzt – die aktuellen Fahrpläne abrufen.<sup>19</sup>

#### *Labyrinth Lite*

Eine sehr breite Palette an Unterhaltungsprogrammen wurde speziell für das iPhone entwickelt und die Auswahl ist bereits auf über 1000 Spiele angestiegen. Viele dieser Applikationen setzen dabei auf eine intuitive Steuerung über den Touchscreen oder den integrierten Lagesensor. Ein Vertreter dieser Spiele ist Labyrinth Lite, in dem eine Stahlkugel um Wände und Löcher herum ins Ziel balanciert werden muss (siehe Abb. 2)<sup>20</sup>. Gesteuert wird die Kugel dabei durch leichte Neigung des iPhone, genauso wie es bei dem realen Geschicklichkeitsspiel der Fall ist.<sup>21</sup>



Abb. 2

### **3.3 Allgemeine Sicherheitsmaßnahmen**

Erst mit der Firmware 2.0 wurden von Apple die Weichen in Richtung Enterprise gestellt. Die neu hinzugekommenen Sicherheitsmerkmale sind im Geschäftsumfeld bereits etabliert und keine proprietären Eigenentwicklungen des Herstellers Apple. Die nachfolgenden Funktionen stellen ein Mindestmaß an Sicherheit zur Verfügung, ohne dieses von einem geschäftlichen Einsatz generell abgesehen werden sollte.

#### *IPSec VPN (Cisco)*

IPsec ist ein Sicherheitsprotokoll, das direkt auf der Vermittlungsschicht des TCP/IP Protokolls aufsetzt. Eine über IPsec verwaltete Verbindung kann verschlüsselt erfolgen (Vertraulichkeit) und auf Prüfsummen basierend die korrekte Datenübermittlung (Integrität) gewährleisten. Auf diesem zugrundeliegenden Protokoll baut das Softwareprodukt VPN<sup>22</sup> des Herstellers Cisco seine Verbindungen auf. Hierbei stehen zwei grundsätzliche Methoden zur Verfügung. Zum einen die Site-to-End-Verbindung, bei der die Kommunikation über ein Transportnetzwerk (i.d.R. das Internet) zu einem Einwahlknoten der Firma weitergeleitet wird. Zum anderen die End-to-End-Verbindung, bei der die Einwahl ins Firmennetzwerk direkt vor Ort erfolgt.<sup>23</sup>

<sup>19</sup> Vgl. Riebartsch, 2009, S. 54-57.

<sup>20</sup> Vgl. Quelle: Zehden, 2009, S.49.

<sup>21</sup> Vgl. Zehden, 2009, S. 49-57; Woods, iPod Touch: Konkurrenz für PSP und Nintendo DS, 2008, Online-Dokument.

<sup>22</sup> virtuelles privates Netz.

<sup>23</sup> Vgl. Wohlgemuth, IP-Sec, o.J., Online-Dokument.

### *WPA2 Enterprise mit 802.1X-Authentifizierung*

Für die Einbindung von Endgeräten in funkbasierende Netzwerke (WLANs) haben sich Verschlüsselungsstandards etabliert, welche sowohl das Einwählen Unbefugter als auch das Mitlesen von Datenverkehr unterbinden sollen. WPA2 setzt dabei auf die Verschlüsselungsmethode AES<sup>24</sup> und implementiert grundlegende Funktionen des Sicherheitsstandards IEEE 802.11i.<sup>25</sup> Neben der Vertraulichkeit und der Autorisierung, die WPA2 gewährleistet, wird eine Authentifizierung des Nutzers über den IEEE 802.1X – Standard durchgeführt. Ziel dabei ist es, die behauptete Identität des anmeldewilligen Gerätes zu überprüfen und entsprechend im Rahmen der Autorisierung Rechte einzuräumen. WPA2 gilt im Gegensatz zu Verschlüsselungsmethoden wie WEP<sup>26</sup> als hinreichend sicher.<sup>27</sup>

### *Kennwort- und Code-Richtlinien*

Damit Kennwörter ihrem Zweck der Authentifizierung des Nutzers nachkommen können, müssen sie bestimmte Mindestanforderungen erfüllen. Welche Anforderungen dabei durchgesetzt werden, legen die Kennwortrichtlinien fest. Verstößt ein vom Nutzer gewähltes Passwort gegen eine der Vorgaben, wird es nicht zugelassen. Typische Richtlinienbestandteile sind maximales Kennwortalter, minimale Kennwortlänge und Komplexitätsvoraussetzungen. Letztere Vorgabe würde eine Wörterbuchattacke (siehe 5.1 Pen-Test) problemlos abwehren, wenn sowohl Zahlen als auch Sonderzeichen im Kennwort verwendet werden müssen.<sup>28</sup>

### *Remote-Wipe-Funktion*

Geht ein mobiles Endgerät wie das iPhone verloren, ist es i.d.R. wünschenswert, die darauf befindlichen vertraulichen Daten vor Zugriffen Fremder zu schützen. Die Remote-Wipe-Funktion geht sogar einen Schritt weiter, indem sie per Fernzugriff alle Daten auf dem iPhone löscht. Zur Nutzung dieses Feature muss das iPhone im Vorfeld für die Synchronisation mit einem Microsoft Exchange-Server eingestellt werden. Bei Bekanntwerden des Verlustes wird das iPhone einfach aus der Geräte-Liste des Exchange-Servers gelöscht. Anschließend wird ein Löschbefehl ausgesendet, der einen sofortigen Neustart des iPhone auslöst und es bis zur

---

<sup>24</sup> Advanced Encryption Standard.

<sup>25</sup> Vgl. Janssen, WPA2, 2005, Online-Dokument.

<sup>26</sup> Wired Equivalent Privacy, wurde bereits mehrfach geknackt und gilt als unsicher.

<sup>27</sup> Vgl. Arx, WLAN Sicherheit - Angriffsvektoren gegen WEP, WPA und WPA2, 2007, Online-Dokument.

<sup>28</sup> Vgl. Microsoft Deutschland GmbH, Kennwortrichtlinien, o.J., Online-Dokument.

nächsten Synchronisation mit iTunes<sup>29</sup> unbrauchbar macht. Bei der besagten Verbindung mit iTunes wird dann der Löschvorgang vollständig abgeschlossen.<sup>30</sup>

## 4 Bekannte Probleme des iPhone

Nachdem bereits größere Unternehmen, wie die HSBC Group, einen Umstieg vom Blackberry zum iPhone erwägen, stellt sich die Frage, ob das iPhone in Bezug auf die Geschäftstauglichkeit seinen Konkurrenten zumindest ebenbürtig ist. Dabei gilt es, in den Bereichen Datenabgleich, Integration in die Unternehmensinfrastruktur, Sicherheitsrichtlinien und Praxistauglichkeit, einen großen Erfahrungsvorsprung aufzuholen. Ein Report der Berlecon Research GmbH hat sich ausführlich mit dem Thema „iPhone im Unternehmenseinsatz“ befasst. Im Fazit der Studie wird den Unternehmen geraten, mit der Einführung des besagten Smartphones zu warten, bis alle aufgetretenen Probleme behoben sind.<sup>31</sup> Die geäußerte Kritik lässt sich in fünf Punkten zusammenfassen:

### 1. *Provider Anbindung*

In Deutschland ist die Deutsche Telekom AG der Exklusiv-Vertreiber für iPhones und bietet diese in Tarifkombinationen an, welche eher auf Privatpersonen abzielen. Auch Unternehmen, die Rahmenverträge mit anderen Anbietern geschlossen haben, wechseln nur ungern aufgrund eines Mobiltelefons den Vertragspartner. Allerdings hat nach dem Erscheinen des Reports im Juli 2008 der Anbieter T-Mobile nun auch Tarife für Geschäftskunden ins Produktportfolio aufgenommen, was diesen Kritikpunkt etwas abschwächt.

### 2. *Bindung an ActiveSync beziehungsweise Microsoft Exchange*

Da ActiveSync kein offener Standard ist, sondern ein Softwareprodukt aus dem Hause Microsoft, schließt diese Synchronisationsart Firmen aus, die Groupware anderer Hersteller verwenden. Lotus Domino von IBM oder Novell Groupwise müssten beispielsweise über Drittanbietersoftware oder ein Webinterface angebunden werden. Erschwerend kommt hinzu, dass Drittanbietersoftware auf dem iPhone nicht als Hintergrundprozess laufen kann, was eine Entwicklung für betreffende Anbieter in hohem Maße einschränkt. Gerade Anwendungen, die eine stetige Überwachungsfunktion ausüben sollen, so wie es auch für den Empfang von Push-Mails nötig ist, sind

---

<sup>29</sup> proprietäre Synchronisationsanwendung des iPhone-Herstellers Apple.

<sup>30</sup> Vgl. Hieber, Remote Wipe: Der Microsoft Kill Switch fürs iPhone, 2008, Online-Dokument; Carius, Remotewipe im Detail, o.J., Online-Dokument.

<sup>31</sup> Vgl. Berlecon Research, iPhone 2.0 im Unternehmenseinsatz, 2008, Online-Dokument.

auf dem iPhone im Grunde nicht nutzbar.<sup>32</sup> Kostengünstig lösen lässt sich diese Problematik zurzeit nur durch das Anmieten der fehlenden Software (z.B. einen Exchangeserver) über das Internet. Diese so genannten SaaS<sup>33</sup>-Angebote ersparen die Anschaffungs-, Betriebs- und Wartungskosten und reduzieren dadurch die Gesamtkosten um mehr als 70 %, die im Vergleich für einen eigenen Server anfallen würden.<sup>34</sup> Ob die Einbettung des iPhone in die Firmeninfrastruktur solche Zusatzausgaben und erhöhten Sicherheitsanforderungen rechtfertigt, sollte im Vorfeld über eine Kosten-Nutzen-Analyse ermittelt werden.

### 3. *Unzureichende Administration*

Zwar bietet das iPhone seit der Firmware 2.0 bereits einige Funktionen an, welche die Verwaltung der Geräte vereinfachen, allerdings fehlt nach wie vor ein einheitliches Gesamtkonzept. Im Vergleich dazu ist bei einem BlackBerry von der Firma Research In Motion nur eine Anwendung nötig, um Softwareverteilung, Konfiguration und Endgeräte-Policy<sup>35</sup> zu realisieren. Firmenspezifische Konfigurationsprofile, die an ein iPhone geleitet werden sollen, müssen per E-Mail verschickt oder per Webabruf bereitgestellt werden. Selbst nach dieser Verteilung ist nicht sichergestellt, ob die Vorgaben vom Benutzer des Gerätes eingehalten werden. Zum einen kann die Annahme des Profils verweigert werden und zum anderen lassen sich Sicherheitsfunktionen, wie das Gerätepasswort, nachträglich wieder deaktivieren.<sup>36</sup>

### 4. *Gefährliche Sicherheitslücken*

Immer wieder wurden in der Vergangenheit kritische Sicherheitslücken aufgedeckt, die es ermöglichten Sicherheitsbeschränkungen zu umgehen, Schadcode auszuführen oder das Gerät gänzlich außer Betrieb zu setzen.<sup>37</sup> Diese wurden in den nachfolgenden Firmware-Updates meist geschlossen. Eine von Mitarbeitern des Fraunhofer-Instituts (SIT<sup>38</sup>) entdeckte Lücke, wurde auch ein Jahr nach ihrer Veröffentlichung von Apple nicht behoben. Beim Betreten einer manipulierten Webseite mit dem iPhone wählte dieses selbständig eine ausgewählte Nummer (zumeist kostenpflichtig), ohne dass es der

---

<sup>32</sup> Vgl. Bremmer, Apple iPhone noch nicht reif für Großunternehmen, 2008, Online-Dokument.

<sup>33</sup> Software as a Service.

<sup>34</sup> Vgl. Wessels, 5.Dezember 2008, S.27.

<sup>35</sup> zentrale Richtlinien, die Geräteeigenschaften vorgeben oder Sicherheitsmerkmale durchsetzen.

<sup>36</sup> Vgl. Lange, Kann sich iPhone 2.0 im Unternehmen behaupten?, o.J., Online-Dokument.

<sup>37</sup> Vgl. heise Security, iPhone-Update schließt kritische Sicherheitslücken, 2008, Online-Dokument.

<sup>38</sup> Sichere Informationstechnologie.

Besitzer verhindern konnte.<sup>39</sup> Allein das Auftreten von Sicherheitslücken muss für das betreffende Unternehmen kein schlechtes Indiz darstellen. Zu 100 % fehlerfreier Programmcode ist bei komplexen Softwareprojekten zwar wünschenswert, aber leider nicht wirtschaftlich realisierbar. Weitaus wichtiger für die Beurteilung des betrachteten Unternehmens ist die Größe der Zeitfenster vom Bekanntwerden einer Lücke bis zur Behebung selbiger. Reagiert ein Hersteller zu spät oder gar nicht auf solche Schwachstellen, erhöht sich das Risiko einer kriminellen Ausnutzung von Tag zu Tag. In diesem Zusammenhang sollte auch eine Risikobewertung, als Bestandteil eines Sicherheitskonzeptes erfolgen, worauf im Punkt 5.2 näher eingegangen wird.

#### 5. *Softwareverteilung über Apple*

Apple beschränkt Softwarebezüge bewusst auf den eigenen App Store, um dadurch eine Kontrolle über die verfügbaren Applikationen zu besitzen. Stark fehlerhafte oder schädliche Software kann so, eine gründliche Analyse von Apple vorausgesetzt, nicht auf ein iPhone gelangen, da sie gar nicht erst im App Store gelistet wird. Diese Maßnahme verhindert aber die in größeren Unternehmen gängige Verteilungspraxis von Programmen. In der Regel wird über einen Push-Dienst die Software auf das Gerät gespielt, ohne den Nutzer in den Installationsprozess einzubeziehen. Diese Vorgehensweise erhöht die Sicherheit enorm, da hierdurch ein einheitlicher aktueller Softwarestand auf allen Geräten gewährleistet werden kann. Soll allerdings nur eine sehr kleine Menge von iPhones eingesetzt werden, hält sich der Aufwand für die manuelle Softwareinstallation und -pflege in Grenzen.

#### *Fehlende Zusatznutzen für „Mobile Mitarbeiter“*

Andere Smartphone-Hersteller haben ihre Geräte so konzipiert, dass sie bei Anschluss an einen Rechner einheitlich als Massenspeicher-Medium erkannt werden und sich somit als transportabler Datenspeicher eignen. Das iPhone benötigt für diese Aufgabe eine Zusatzsoftware, sonst ist kein Datentransfer möglich. Auch die Nutzung als UMTS-Modem ist nicht vorgesehen, was für die UMTS-Verbindung eines Notebooks unterwegs zusätzliche Hardware erforderlich macht. Eine Studie<sup>40</sup> des Institutes WirelessInfo.com führte realitätsnahe Messungen bezüglich der Akkulebensdauer durch, in der verschiedene Nutzungsszenarien ausgewertet wurden. Je nach Nutzungsintensität sinkt die Akkulebenszeit auf wenige Stunden herab und übersteht daraufhin nicht einmal einen vollständigen Arbeitstag. Ein weiteres Manko

---

<sup>39</sup> Vgl. Das Fraunhofer-Institut für Sichere Informationstechnologie, Sicherheitslücke: iPhone wählt selbständig Abzocke-Nummer, 2008, Online-Dokument.

<sup>40</sup> Vgl. Padilla, Apple iPhone 3G Cell Phone Review - Battery Life, 2008, Online-Dokument.

gegenüber vergleichbaren Geräten ist der fest eingebaute Akku, den nur der Hersteller Apple selbst wechseln kann. Damit entfällt eine gern genutzte Möglichkeit, die Betriebszeit durch Ersatzakkus zu verlängern.<sup>41</sup>

In verschiedenen Artikeln zur Geschäftstauglichkeit des iPhone fällt das Fazit recht eindeutig aus. Es wird von einem produktiven Einsatz mehrheitlich abgeraten. Die betrachteten Kritikpunkte wiegen zum Teil so schwer, dass sich das iPhone bestenfalls in sehr kleiner Stückzahl einsetzen lässt, weil dadurch der gesonderte Verwaltungsaufwand überschaubar bleibt. Bis zur Behebung der aufgezeigten Mängel sollte mit einer Einführung noch gewartet werden. Schon aufgrund der Sicherheitserweiterungen als Bestandteil der Firmware Version 2.0 lässt sich erahnen, dass eine Weiterentwicklung in Richtung Businessstauglichkeit seitens Apple angestrebt wird.

## **5 Risikoanalyse und -bewertung**

Soll ein neues mobiles Endgerät wie das iPhone in einem Unternehmen zum Einsatz kommen, bedarf es einer gründlichen Risikoanalyse und -bewertung. Die Risikoanalyse hat grundsätzlich die Aufgabe, die Eintrittswahrscheinlichkeiten und Schadenshöhen möglicher Gefahren zu ermitteln und zu beurteilen. Nach erfolgter Bewertung der Risiken können dann verschiedenste strategische und organisatorische Maßnahmen ergriffen werden, um wirtschaftliche Schäden für das Unternehmen zu minimieren. Eine Möglichkeit, zielgerichtet nach IT-Schwachstellen im Unternehmen zu suchen, ist der so genannte Penetrations-Test. Dieser kann zum einen bestehende Sicherheitsvorkehrungen auf ihre Wirksamkeit hin überprüfen und zum anderen neue Gefahrenklassen aufdecken, die bisher gar nicht in Erwägung gezogen wurden.<sup>42</sup>

### **5.1 PEN-Test**

Wenn es einem unbefugten Personenkreis gelingt in die Netze oder Systeme eines Unternehmens einzudringen, kann dies mitunter schwerwiegende Folgen nach sich ziehen. Die Bandbreite der Nachwirkungen erstreckt sich von „unbedeutend“ bis hin zu „existenzbedrohend“, je nachdem welche Daten ausgespäht, manipuliert oder vernichtet wurden. Der Penetrations-Test, im Folgenden nur noch als PEN-Test bezeichnet, versucht genau dieses Szenario real umzusetzen. Der einzige Unterschied dabei ist, dass der Angreifer eine Vergütung erhält und dafür auch keine schädigenden Handlungen ausführt, wenn er die Chance dazu hätte. Grundsätzlich darf sich der Beauftragte aller Werkzeuge und Möglichkeiten

---

<sup>41</sup> Vgl. Lange, Kann sich iPhone 2.0 im Unternehmen behaupten?, o.J., Online-Dokument.

<sup>42</sup> Vgl. S4P solutions for partners ag, IT-Risikoanalyse, o.J., Online-Dokument.

bedienen, die auch einem echten Angreifer zur Verfügung stehen. Als Ergebnis dieses Tests werden die identifizierten Schwachstellen einer Risikobewertung unterzogen, in welcher entschieden wird, wie weiter zu verfahren ist.<sup>43</sup>

Die Arbeit des PEN-Testers besteht zunächst daraus, sich einen Zugangskanal zum Firmennetz zu suchen. Dies geschieht im einfachsten Fall durch einen so genannten Portscanner, der die nach Außen bereitgestellten Dienste des Unternehmens analysiert. Mithilfe eines Vulnerability-Scanners<sup>44</sup> lassen sich die Dienste bereits auf bekannte Sicherheitslücken hin überprüfen. Gerade in diesem frühen Stadium des Tests werden oft bereits Mängel ersichtlich, die auf veralteten Versionsständen der Dienste beziehungsweise nachlässiger Aktualisierung selbiger beruhen. Anhand der BugTraq ID<sup>45</sup>, die ein Vulnerability-Scanner ausgibt, ist es nun möglich auf der Seite von SecurityFocus ([www.securityfocus.com/bid](http://www.securityfocus.com/bid)) detaillierte Informationen zu gefundenen Sicherheitslücken abzurufen. Mithilfe von relevanten Suchwörtern lässt sich nun im Nachgang ein Angriffstool finden, welches exakt diese Lücke ausnutzt und das Zielsystem kompromittiert.<sup>46</sup>

Dies war nur ein kleiner Auszug, wie ein PEN-Tester bei seiner Arbeit vorgehen würde. Idealerweise, für das betreffende Unternehmen, sollte es der Tester allerdings schwieriger haben in das System einzubrechen. Lassen sich keine vermeintlichen Sicherheitslücken finden, wäre der nächste Schritt das Knacken von Zugangskennwörtern einzelner Dienste. Dabei gibt es zwei verschiedene Ansätze. Zum einen die Brute-Force-Methode, welche der Reihe nach alle möglichen Zahlen-, Zeichen- und Buchstabenkombinationen durchprobiert und zum anderen die Wörterbuch-Methode. Letztere verwendet als Grundlage eine Sammlung ausgewählter Begriffe, die gern als Passwort verwendet werden oder basiert tatsächlich auf vollständigen Wörterbüchern. An dieser Stelle wird bereits ersichtlich, dass sich real existierende Wörter, egal welcher Sprache, keineswegs als sicheres Passwort eignen.

Sollte auch das Knacken des Zugangskennwortes erfolglos bleiben, ist die Arbeit eines PEN-Testers noch längst nicht beendet. Weitere Anlaufpunkte bieten sich ihm beispielsweise durch das Mitschneiden von Datenströmen, welche das gewünschte Kennwort enthalten können. Dieser Vorgang, der als „Sniffen“ bezeichnet wird, gestattet dem Angreifer das Kennwort nachträglich zu extrahieren, was sich durch den Direktzugriff wesentlich effizienter gestaltet.

---

<sup>43</sup> Vgl. Rey, 2005, S. 1-2.

<sup>44</sup> Softwarekombination bestehend aus Portscanner, Diensterkennung, Betriebssystemerkennung und Sicherheitslückenabgleich mit externen Datenbanken.

<sup>45</sup> 5-stellige Nummer.

<sup>46</sup> Vgl. Rey, 2005, S. 22-42.

Häufige Probleme die auftreten können sind z.B. strenge Passwort-Policies<sup>47</sup> oder schlichtweg die Abweisung von Geräten die dem Netzwerk nicht bekannt sind und/oder zu viele gescheiterte Login-Versuche aufweisen.<sup>48</sup>

In diesem Zusammenhang eignen sich auch mobile Endgeräte, wie ein Notebook oder das iPhone als zweckdienliches Mittel, wenn diese schwächere Sicherheitsmerkmale als die restliche Firmeninfrastruktur aufweisen. Oftmals sind Zugangskennungen, wie beispielsweise der WLAN-Schlüssel, bereits im System hinterlegt und gestatten dem Finder/Dieb des Gerätes bereits problemlosen Firmenzugriff auf Ebene der jeweiligen Benutzerrechte. Dieser, zunächst eingeschränkte Zugang, kann durch weiterführende Maßnahmen zur Ausweitung der Rechte eingesetzt werden. Eine wirkungsvolle Gegenmaßnahme wäre u.a. ein Gerätekennewort, welches per Endgeräte-Policy verbindlich durchgesetzt wird. Dieses würde bereits das Einschalten durch nicht autorisierte Personen verhindern. Genau diese verbindliche Durchsetzung lässt das iPhone derzeit nicht zu, da der Besitzer des Gerätes immer über die vollständigen Admin-Rechte verfügt. Diese ermöglichen es ihm bestehende Sicherheitsprofile zu löschen und Gerätekennewörter abzuschalten.<sup>49</sup> Weitere Ansätze des PEN-Tests, wie beispielsweise das kompromittieren von Netzwerkschnittstellen (z.B. Router), sind aufgrund des Umfangs nicht Bestandteil dieser Arbeit.

## 5.2 Risikobewertung

Ist ein Analyseverfahren wie der PEN-Test abgeschlossen, muss nun eine Bewertung aller gefundenen Probleme erfolgen. Bei der Bewertung von Risiken werden auch kritische Faktoren, wie Kosten und Nutzen herangezogen. Übersteigen die Kosten für die Absicherung eines angebotenen Dienstes beispielsweise den Nutzwert, ist es u.U. wirtschaftlicher, diesen nicht mehr bereitzustellen.

Grundlage für alle bisherigen Schritte sollte immer das firmenspezifische Sicherheitskonzept darstellen. Dieses wird geplant, umgesetzt, überwacht und fortlaufend optimiert. Die Risikobewertung ist nur ein Teilschritt dieses Konzeptes, welcher bezüglich des PEN-Tests in den Bereich der Erfolgskontrolle fällt. Die Vorgehensweisen, die bei dem vorher beschriebenen Testangriff gewählt wurden, geben bereits Aufschluss darüber an welchen Stellen Verbesserungen erfolgen könnten.<sup>50</sup> Werden nicht benötigte Dienste abgeschaltet, die

---

<sup>47</sup> Richtlinien wie z.B. Mindestlänge die bei der Passwortvergabe eingehalten werden müssen.

<sup>48</sup> Vgl. Rey, 2005, S. 44-47.

<sup>49</sup> Vgl. Bremmer, 14.November 2008, S.23.

<sup>50</sup> Vgl. [http://www.bsi.bund.de/literat/bsi\\_standard/standard\\_1001.pdf](http://www.bsi.bund.de/literat/bsi_standard/standard_1001.pdf).

verbleibenden durch Patches und Updates aktuell gehalten und eine strenge Passwort-Policy im Unternehmen eingeführt, erhöht dies die Sicherheit bereits maßgeblich.<sup>51</sup> Auch sollten Pressemitteilungen über neu entdeckte Sicherheitslücken stets verfolgt werden, um schnelle Reaktionen zu ermöglichen.

## 6 Fazit

Trotz der immer wieder auftretenden Probleme im Bezug auf Sicherheit, erwägen viele größere Unternehmen die Einführung des iPhone als Businesshandy. Sollten große Institute, wie die Deutsche Bank oder die HSBC Group, ihre Erwägungen in die Tat umsetzen, wäre dies ein schwerer Schlag für den derzeitigen Marktführer Blackberry. Die Kaufabsichten (siehe Abb. 3)<sup>52</sup> lassen einen leichten Aufwärtstrend zugunsten des iPhone erkennen. Dennoch

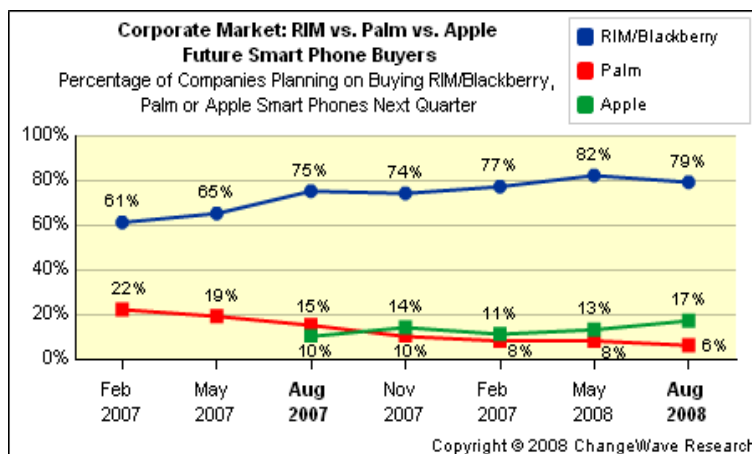


Abb. 3

ändern wenn Apple weitere Entwicklungen in Richtung Businessstauglichkeit anstrebt und damit überzeugen kann. Die am 17. März 2009 vorgestellten Neuerungen der nachfolgenden Firmware 3.0 lassen diese Weiterentwicklung allerdings vermissen.<sup>54</sup>

kann die Haltung der Unternehmen dem iPhone gegenüber, als eher reserviert bezeichnet werden, was aber auch dem Umstand geschuldet ist, dass Unternehmer sehr jungen Plattformen allgemein nicht viel Vertrauen entgegenbringen.<sup>53</sup> Dies könnte sich

<sup>51</sup> Vgl. Ray, 2005, S. 39-40.

<sup>52</sup> Vgl. Vatter, 2008, Online-Dokument.

<sup>53</sup> Vgl. Müller, CTIA: iPhone noch uninteressant für Unternehmen, 2007, Online-Dokument.

<sup>54</sup> Vgl. Apple Inc., Apple - iPhone - Vorschau auf das iPhone OS 3.0, 2009, Online-Dokument.

## 7 Literaturverzeichnis

**Apple Inc** (17. März 2009), *Apple - iPhone - Vorschau auf das iPhone OS 3.0*, abgerufen am 20. März 2009 von [www.apple.com](http://www.apple.com): <http://www.apple.com/de/iphone/preview-iphone-os/>.

**Apple Inc** (o.J.), *Apple - iPhone - Unternehmen – Integration*, abgerufen am 23. Januar 2009 von [www.apple.com](http://www.apple.com): <http://www.apple.com/de/iphone/enterprise/integration.html>.

**Apple Inc** (o.J.), *Apple – iPhone*, abgerufen am 04. Januar 2009 von [www.apple.com](http://www.apple.com): <http://www.apple.com/de/iphone>.

**Arx, Y.** (Juni 2007), *WLAN Sicherheit - Angriffsvektoren gegen WEP, WPA und WPA2*, abgerufen am 03. Februar 2009 von [www.securitymanager.de](http://www.securitymanager.de): [http://www.securitymanager.de/magazin/artikel\\_1498\\_hakin9\\_wlan\\_sicherheit.html](http://www.securitymanager.de/magazin/artikel_1498_hakin9_wlan_sicherheit.html).

**Berlecon Research** (August 2008), *iPhone 2.0 im Unternehmenseinsatz*, abgerufen am 25. Januar 2009 von [www.berlecon.de](http://www.berlecon.de): <http://www.berlecon.de/iphone>.

**Bremmer, M.** (03. September 2008), *Apple iPhone noch nicht reif für Großunternehmen*, abgerufen am 24. Januar 2009 von [www.computerwoche.de](http://www.computerwoche.de): [http://heftarchiv-cw.computerwoche.de/knowledge\\_center/mobile\\_wireless/1872818/](http://heftarchiv-cw.computerwoche.de/knowledge_center/mobile_wireless/1872818/).

**Bremmer, M.** (02. Juli 2008), *Deutsche Bank will iPhone als Firmen-Handy zulassen*, in *Computerwoche*, Heft 27, München, S. 8.

**Bremmer, M.** (22. August 2008), *HSBC erwägt weltweiten Umstieg auf iPhone*, in *Computerwoche*, Heft 34, München, S. 7.

**Bremmer, M.** (14. November 2008), *Kultobjekt mit schwachen Geschäftsfunktionen*, in *Computerwoche*, Heft 46, München, S. 23.

**Bundesamt für Sicherheit in der Informationstechnik** (23. April 2004), *Sicherheit im Internet*, abgerufen am 14.03.2009 von <http://www.bsi.de/literat/faltbl/F29Internet.htm>.

**Carius, F.** (o.J.), *Remotewipe im Detail*, abgerufen am 26. Januar 2009 von [www.msxfaq.de](http://www.msxfaq.de): <http://www.msxfaq.de/mobil/remotewipe.htm>.

**Das Fraunhofer-Institut für Sichere Informationstechnologie** (20. November 2008), *Sicherheitslücke: iPhone wählt selbständig Abzocke-Nummer*, abgerufen am 24. Januar 2009

von [www.sit.fraunhofer.de](http://www.sit.fraunhofer.de):

<http://www.sit.fraunhofer.de/pressedownloads/pressemitteilungen/iPhoneHack.jsp>.

**heise Security** (15. September 2008), *iPhone-Update schließt kritische Sicherheitslücken*, abgerufen am 24. Januar 2009 von [www.heise.de](http://www.heise.de): <http://www.heise.de/security/iPhone-Update-schliesst-kritische-Sicherheitsluecken--/news/meldung/115983>.

**Hieber, C.** (17. Oktober 2008), *Remote Wipe: Der Microsoft Kill Switch fürs iPhone*, abgerufen am 26. Januar 2009 von [www.iphone-ticker.de](http://www.iphone-ticker.de): <http://www.iphone-ticker.de/2008/10/17/remote-wipe-der-microsoft-kill-switch-furs-iphone/>.

**Hoang, T.** (o.J.), *Hoang – iControl*, abgerufen am 23. Januar 2009 von [www.hoang.de](http://www.hoang.de): [https://www.hoang.de/index.php?option=com\\_content&task=view&id=35&Itemid=49](https://www.hoang.de/index.php?option=com_content&task=view&id=35&Itemid=49).

**Hungenberg, T.** (Juni 2000), *Informationssicherheit: Einleitung*, abgerufen am 22. Januar 2009 von [www.demonium.de](http://www.demonium.de): <http://www.demonium.de/th/home/sicherheit/einleitung.phtml>.

**Hungenberg, T.** (03. August 2000), *Informationssicherheit: Sachziele*, abgerufen am 22. Januar 2009 von [www.demonium.de](http://www.demonium.de): <http://www.demonium.de/th/home/sicherheit/grundlagen/sachziele.phtml>.

**Informationstechnik, B. f.** (2008), *BSI-Standard 100-1*, (B. f. Informationstechnik, Hrsg.), abgerufen am 28. Januar 2009 von [www.bsi.bund.de](http://www.bsi.bund.de): [http://www.bsi.bund.de/literat/bsi\\_standard/standard\\_1001.pdf](http://www.bsi.bund.de/literat/bsi_standard/standard_1001.pdf).

**Janssen, W.** (08. April 2005), *WPA2*, abgerufen am 03. Februar 2009 von [www.at-mix.de](http://www.at-mix.de): <http://www.at-mix.de/wpa2.htm>.

**Lange, A.-K.** (01. August 2008), *Berlecon zum iPhone in Unternehmen*, in Computerwoche, Heft 31/32, München, S. 24.

**Lange, A.-K.** (o.J.), *Kann sich iPhone 2.0 im Unternehmen behaupten?*, abgerufen am 24. Januar 2009 von [www.pcwelt.de](http://www.pcwelt.de): [http://www.pcwelt.de/start/mobility\\_handy\\_pda/pda\\_smartphone/news/172474/kann\\_sich\\_iphone\\_20\\_im\\_unternehmen\\_behaupten/index2.html](http://www.pcwelt.de/start/mobility_handy_pda/pda_smartphone/news/172474/kann_sich_iphone_20_im_unternehmen_behaupten/index2.html).

**Microsoft Deutschland GmbH** (o.J.), *Kennwortrichtlinien*, abgerufen am 03. Februar 2009 von [www.technet.microsoft.com](http://www.technet.microsoft.com): <http://technet.microsoft.com/de-de/library/cc783512.aspx>.

**Müller, P.** (25. 10 2007), *CTIA: iPhone noch uninteressant für Unternehmen*, abgerufen am 28. Januar 2009 von [www.macwelt.de](http://www.macwelt.de): [http://www.macwelt.de/artikel/Online-Artikel/350063/ctia\\_iphone\\_noch\\_uninteressant\\_fuer\\_unternehmen/1](http://www.macwelt.de/artikel/Online-Artikel/350063/ctia_iphone_noch_uninteressant_fuer_unternehmen/1).

**NetSuite Inc.** (o.J.), *Introducing SuitePhone*, abgerufen am 24. Januar 2009 von [www.netsuite.com](http://www.netsuite.com): <http://www.netsuite.com/portal/landing/suitephone.shtml>.

**Padilla, A.** (11. Juli 2008), *Apple iPhone 3G Cell Phone Review - Battery Life*, abgerufen am 21. Januar 2009 von [www.wirelessinfo.com](http://www.wirelessinfo.com): <http://www.wirelessinfo.com/content/Apple-iPhone-3G-Cell-Phone-Review/Battery-Life.htm>.

**Rey, E./ Thumann, M./ Baier, D.** (2005), *Mehr IT-Sicherheit durch Pen-Tests*, Friedr. Vieweg & Sohn Verlag / GWV Fachverlage GmbH, Wiesbaden.

**Riebartsch, V.** (Januar 2009), Hrsg. Macwelt, *Top-Software für iPod Touch und iPhone – Kleine Helfer*, in Macwelt Sonderheft iPHONE & IPOD Spezial , Heft 1, München, S. 54-57.

**S4P solutions for partners ag** (o.J.), *IT-Risikoanalyse*, abgerufen am 23. Januar 2009 von [www.sforp.de](http://www.sforp.de): <http://www.sforp.de/jsp/epctrl.jsp?mod=sforp000157&cat=sforp000051&pri=sforp>.

**salesforce.com Germany GmbH** (o.J.), *Product Tour: Salesforce for iPhone*, abgerufen am 22. Januar 2009 von [www.salesforce.com](http://www.salesforce.com): <http://www.salesforce.com/products/mobile/iPhone/>.

**Senstic Inc** (o.J.), *i-Clickr PowerPoint Remote*, abgerufen am 23. Januar 2009 von [www.senstic.com](http://www.senstic.com): <http://www.senstic.com/iphone/iClickr/iClickr.aspx>.

**stoeger it GmbH** (o.J.), *OutBank - Die Mobile Banking Software*, abgerufen am 23. Januar 2009 von [www.outbank.de](http://www.outbank.de): <http://www.outbank.de>.

**The Nielsen Company GmbH** (22. Juli 2008), *Nielsen veröffentlicht iPhone-Statistik*, abgerufen am 24. Januar 2009 von [www.nielsen.com](http://www.nielsen.com): [http://de.nielsen.com/news/NMRPressemeldung\\_22.07.2008.shtml](http://de.nielsen.com/news/NMRPressemeldung_22.07.2008.shtml).

**update software AG** (o.J.), *update - Ihr kompetenter Partner für CRM*, abgerufen am 22. Januar 2009 von [www.update.com](http://www.update.com): <http://www.update.com/CRM-Software/CRM-Anbieter/-6412-34-34-de-hq-/cms.html>.

**update software AG** (o.J.), *update.seven touch*, abgerufen am 22. Januar 2009 von [www.update.com](http://www.update.com): [http://www.update.com/CRM-Software/Produkte/update\\_seven\\_touch/-6412-899-899-de-hq-/cms.html](http://www.update.com/CRM-Software/Produkte/update_seven_touch/-6412-899-899-de-hq-/cms.html).

**Vatter, A.** (03. September 2008), *iPhone in der Geschäftswelt immer gefragter*, abgerufen am 30. Januar 2009 von [www.onlinekosten.de](http://www.onlinekosten.de): <http://www.onlinekosten.de/news/artikel/31184/0/iphone-in-der-Geschaeftswelt-immer-gefragter>.

**Wessels, I.** (05. Dezember 2008), *iPhone im Firmennetz*, in *Funkschau*, Heft 24, Poing, S. 27.

**Witvoet, O.** (14. Januar 2009), *Mobile CRM*, abgerufen am 22. Januar 2009 von [www.update.com](http://www.update.com):  
[http://www.update.com/em/downloads/3980/whitepaper\\_mobile\\_crm\\_deu.pdf](http://www.update.com/em/downloads/3980/whitepaper_mobile_crm_deu.pdf).

**Wohlgemuth, H.** (o.J.), *IP-Sec*, abgerufen am 03. Februar 2009 von [www.virenschutz.info](http://www.virenschutz.info):  
<http://www.virenschutz.info/IP-Sec-vpn-21.html>.

**Woods, P.** (13. Oktober 2008), *iPod Touch: Konkurrenz für PSP und Nintendo DS*, abgerufen am 24. Februar 2009 von [www.macwelt.de](http://www.macwelt.de): [http://www.macwelt.de/artikel/\\_News/360514/ipod\\_touch\\_konkurrenz\\_fuer\\_psp\\_und\\_nintendo\\_ds/1](http://www.macwelt.de/artikel/_News/360514/ipod_touch_konkurrenz_fuer_psp_und_nintendo_ds/1).

**Zehden, M.** (Januar 2009), Hrsg. Macwelt, *20 Top Games aus dem AppStore – Ich will Spaß!*, in *Macwelt Sonderheft iPHONE & iPOD Spezial*, Heft 1, München, S. 49-53.