



Mal ganz im Vertrauen gesagt: Wo ist Ihr Smartphone? Herausforderungen an die Unternehmenssicherheit

6. dtb-Forum

Darf ich mich vorstellen?

Frank Bittner

- Geschäftsführer OTARIS Interactive Services GmbH
 - 44 Jahre, Aprilscherz
 - Verheiratet
 - Zwei Kinder

- Bekennender „Smartphone Junkie“

Darf ich mich vorstellen?

Frank Bittner

- Geschäftsführer OTARIS Interactive Services GmbH

44 Jahre, Aprilscherz

- Verheiratet

- Zwei Kinder

- Bekennender „Smartphone Junkie“

**Was hat das mit IT-Sicherheit zu tun?
Ziemlich viel!**

Kurz zur OTARIS Interactive Services GmbH

- Kundenspezifische client- oder webbasierte Software-Lösungen für elektronische Geschäftsprozesse u.a. in den Branchen

- Telekommunikation
- Marktforschung
- Gesundheitswirtschaft
- Öffentlicher Bereich

- Unsere Lösungen zeichnen sich aus durch

- hohe Bedienbarkeit
- Zuverlässigkeit
- optimal abgestimmte Sicherheitskonzepte

- Mitglied und Regionalstelle von TeleTrust Deutschland e.V.



- TeleTrust wurde im Jahr 1989 gegründet, um verlässliche Rahmenbedingungen für den vertrauenswürdigen Einsatz von Informations- und Kommunikationstechnik zu schaffen
- Heute vertritt der Verband rund 100 Mitglieder aus Industrie, Wissenschaft und Forschung sowie öffentlichen Institutionen
- Als Regionalstelle Bremen vom IT-Sicherheitsverband TeleTrust Deutschland e.V. engagiert sich OTARIS für die Förderung von Vertrauenswürdigkeit und Sicherheit in elektronischen Geschäftsprozessen

Was haben Sie typischerweise bei sich?



Der Trend (I)

Jeder Zweite geht nie ohne sein Handy aus dem Haus

- Vor allem Jüngere haben das Gerät immer dabei
- 59 Millionen Bundesbürger besitzen derzeit ein Mobiltelefon
- BITKOM veröffentlicht Donnerstag Studie zu Informationsflut

Berlin, 30. März 2011 - Jeder zweite Handybesitzer (51 Prozent) geht nie ohne sein Mobiltelefon aus dem Haus. Das hat eine Studie im Auftrag des Hightech-Verbandes BITKOM ergeben. „Das Handy ist für viele Deutsche zum ständigen Begleiter geworden“, sagte BITKOM-Präsident Prof. Dr. August-Wilhelm Scheer. 83 Prozent aller Deutschen ab 14 Jahren besitzen ein Handy, das sind 59 Millionen Bundesbürger. Weil zahlreiche Nutzer ein Zweitgerät haben, gibt es insgesamt sogar mehr Handys als Einwohner.

Vor allem viele junge Menschen haben das Mobiltelefon immer dabei: 74 Prozent der 14- bis 29-jährigen Nutzer gehen nie ohne Handy aus dem Haus. Je älter die Handybesitzer, desto eher lassen sie das Gerät auch mal daheim. Nur ein Viertel der Senioren ab 65 Jahren nimmt es immer mit. „Dabei ist das Handy gerade für ältere Menschen ein Plus an Sicherheit, wenn etwa im Notfall ärztliche Hilfe benötigt wird“, so Scheer.

Quelle: BITKOM- Pressemeldung

Der Trend (II)

Bis 2012 steigt der Anteil der Smartphone-Intensivnutzer um 83%!

DIE ZEIT, die wir mit Medien verbringen, wird innerhalb der nächsten zwei bis drei Jahre um ungefähr eine Stunde täglich ansteigen, dabei nimmt der Anteil der Intensivnutzer zu. Der Anteil der Deutschen, die das stationäre Internet intensiv nutzen, wächst um 39 Prozent. Die Gruppe der Intensivnutzer von mobilem Internet über das Smartphone wird mit 83 Prozent den größten Zuwachs erfahren. Jeder zehnte Deutsche wird dann täglich das mobile Internet nutzen!

Quelle: GO SMART 2012, Studie zur Smartphone Nutzung 2012

Der Trend (III)



Quelle: BITKOM- Pressemitteilung

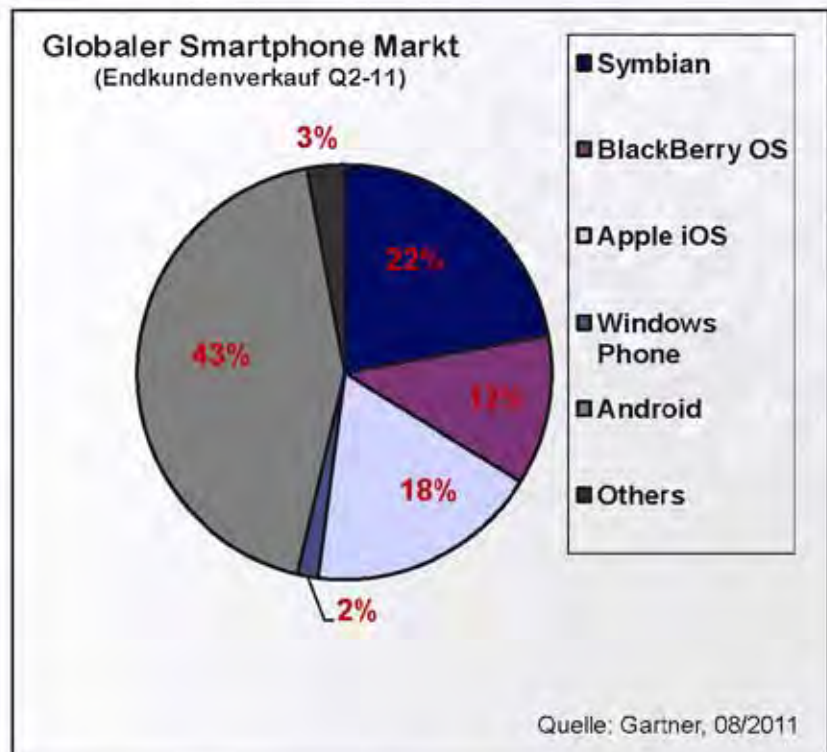
Smartphone Markt – weltweit

Der Smartphone Markt ist von Q2-10 zu Q2-11 um 74% gewachsen und entspricht derzeit 25% der gesamten verkauften Endgeräte weltweit.

Quelle: Gartner, 08/2011

Das Smartphone ist der Katalysator für die Erholung im weltweiten Handy-Markt in 2010

Quelle: IDC, Kevin Restivo, Senior Research Analyst



Ein Kommunikations-Multitalent



Typische Anwendungen - beruflich

- Mobile E-Mail, mobiler Zugang zu Terminkalendern
- Branchenlösungen und Individualsoftware
- ERP-Systeme:
 - Customer Relationship Management (Mobile CRM),
 - Supply Chain Management (Mobile SCM),
 - Mobile Procurement und
 - Mobile Business Intelligence
- Ach ja: Telefonie und SMS...

Typische Anwendungen - privat

- E-Mail, Kalender
- Internet Browsing
- Apps, Apps, Apps...
 - Social Media: z.B. Facebook, Twitter, Xing, Stayfriends
 - Informationsportale: z.B. Spiegel, Tagesschau, Sport
 - Spiele
 - Musik / Filme
 - Navigation
 - Online Banking
 - Online Shopping

- Ach ja: immer noch Telefonie und SMS...

Kontrollverlust durch „BYOD“?

CIOs kämpfen um Standardisierung, Konsolidierung und Sicherheit. Der Trend ByoD macht diese Arbeit nicht einfacher.

Fast vier von fünf IT-Verantwortlichen befürchten, durch den Trend "[Bring your own Device](#)" (ByoD) die Kontrolle über ihre Client-Landschaft zu verlieren. Ein Viertel stuft diese Gefahr sogar als "sehr groß" ein. Das hat eine exklusive Umfrage der COMPUTERWOCHE ergeben. Anfang April haben sich im Rahmen einer Online-Befragung fast 150 CIOs, [IT-Leiter](#), Administratoren sowie Support- und Sicherheitsverantwortliche dazu geäußert, wie sie die aktuellen Trends rund um die wachsende Consumerization der Unternehmens-IT und ByoD einschätzen und deren Folgen beurteilen.

Grundsätzlich überwiegt in den IT-Abteilungen die Skepsis, was die Nutzung privater Geräte wie [Smartphones und Tablets](#) in den Unternehmen anbelangt. Über 90 Prozent der Befragten gaben an, mit einer zunehmenden Zahl an persönlichen Devices erhöhe sich der Aufwand für das [Client-Management](#) und den Support. Jeder zweite IT-Verantwortliche charakterisierte die damit verbundenen Aufgaben als viel oder sogar sehr viel schwieriger. (Mit dem Thema "Achtung: Die Digital Natives kommen - was IT Manager und Digital Natives voneinander lernen können" beschäftigt sich auch die Veranstaltung "[IT Operations Day am 12. Mai in Berlin](#)")

Wie sicher sind Smartphones?



News Hintergrund Erste Hilfe

Security > Suche

Suche

heise Security Foren Preisvergleich

Smartphone

Security-Wissen ohne Umweg: Installieren Sie die Browser.

ungefähr 132 Treffer für **Smartphone**

HTC bestätigt Sicherheitsleck in Android-Smartphones

Der Hersteller hat einen Patch in Aussicht gestellt, der das am vergangenen Samstag gemeldete Problem lösen soll. Durch das Leck können Apps auf private Daten wie SMS, Telefonkontakte und GPS-Koordinaten zugreifen.
04.10.2011 – <http://www.heise.de/security/meldung/HTC-bestatigt>

Android-Trojaner per QR-Code

Das vor allem bei Android-Geräten verbreitete Verfahren, Software via QR-Code zu installieren, nutzen Angreifer für die Installation eines Trojaners aus. Die Schadsoftware sendet SMS an einen Premium-Dienst.
02.10.2011 – <http://www.heise.de/security/meldung/Android-Troja>

WLAN-MAC-Adressen: Google verspricht Opt-Out

Auf Druck europäischer Behörden will Google im Herbst ein Opt-Out-Verfahren für WLAN-MAC-Adressen vorstellen.
17.09.2011 – <http://www.heise.de/security/meldung/WLAN-MAC-Adre>

Weiterer Online-Banking-Trojaner für Android

Der sonst nur auf PCs und Symbian laufende Trojaner SpyEye wurde in einer Android-Version gesichtet. Zusammen mit Zeus gibt es nun zwei Schädlinge für diese Plattform, die das mTAN-Verfahren aushebeln.
15.09.2011 – <http://www.heise.de/security/meldung/Westerei-Online>

App-Stores als Hort der IT-Sicherheit

App-Stores können der europäischen IT-Sicherheitsbehörde ENISA zufolge einen wichtigen Beitrag gegen schädliche Apps leisten – vorausgesetzt, sie erfüllen ein anlässlich der Internet Security Days veröffentlichtes 5-Punkte-Programm.
14.09.2011 – <http://www.heise.de/security/meldung/App-Stores-als>

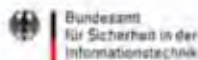
Update behebt kritische Sicherheitslücken in Smartphone-Messenger

Durch Manipulationen von WhatsApp für iPhone kann ein Angreifer beliebig Nachrichten fälschen und belauschen. Die neue Version schließt die Lücken.
08.09.2011 – <http://www.heise.de/security/meldung/Update-behebt>

Android vermehrt Ziel von Schadsoftware

Mit der zunehmenden Verbreitung des **Smartphone**-Betriebssystems

Wie sicher sind Smartphones? (forts.)



Presse

Kurzmitteilungen
Pressearchive
Informationen
Pressestelle
Presseverteiler

Suche

Startseite > Presse > Neue Schadsoftware liest mTAN-Nummern mit

Neue Schadsoftware liest mTAN-Nummern mit

Bonn, 04.03.2011

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) weist darauf hin, dass eine neue Schadsoftware-Variante Smartphones angreift, um mTAN-Nummern für das Online-Banking mitzulesen.

Der Angriffsweg führt zunächst über eine Infektion der PCs mit einer speziellen Schadsoftware. Ruft der Nutzer mit dem PC eine Online-Banking-Webseite auf, werden zusätzliche Felder oder Nachrichten eingeblendet. In der Optik der Webseits gehalten, fordern diese den Nutzer dazu auf, seine Mobilfunknummer sowie sein Handymodell oder die IMEI-Nummer (In Mobile Equipment Identity) einzugeben, um einen Link für ein angeblich notwendiges Zertifikats-Update zu erhalten. Mit dem der Nutzer daraufhin per SMS erhält, lädt er jedoch eine Schadsoftware auf sein Smartphone, die bei künftigen Online-Transaktionen die mTAN mitliest. So können Angreifer zum Beispiel Überweisungen manipulieren und auf fremde Konten

Angreifer nehmen mobile Endgeräte ins Visier

Grundsätzlich ist das mTAN-Verfahren, bei dem für jede Transaktion eine „mobile TAN“ per SMS an das Handy übermittelt wird, ein Sicherheitsgewinn im Vergleich zu herkömmlichen Verfahren, denn der Online-Banking-Vorgang und die Übermittlung der Daten auf verschiedenen Übertragungswegen. Die aktuelle Schadsoftware versucht, den Nutzer zur Eingabe der Handy-Daten zu bewegen, um damit diese Trennung auszuhebeln.

Quelle: Bundesamt für Sicherheit in der Informationstechnik - Pressemeldung

Typische Sicherheitsrisiken

- Datenverlust oder –diebstahl
 - Physischen Zugriff
 - Drahtloser Zugriff
 - Informationsübertragung

- Infektion mit Schadprogrammen
 - Email
 - Manipulierte Webseiten
 - Manipulierte Apps

- Ausfall bzw. Manipulation des Fernzugriffs
 - Unterbindung des Zugriffs auf Unternehmensdaten
 - Zugang zu Unternehmens-Infrastruktur

Vertrauen Sie Ihren Apps?

Live Demonstration



„Unbewusste“ Zugriffsrechte von Apps

Nur ein paar Beispiele...

- Liste der Telefonverbindungen
- Auslesen genutzter URLs (Internet Browser)
- Übersicht der App-Nutzung
- Mitlesen von SMS/MMS
- Bewegungsprofil über Cell-Informationen
- Zugriff auf Kalender-Einträge
- Zugriff auf Speicherkarte
- Mitschnitt von Kamerabildern und Videoaufnahmen
- Audio-Aufzeichnung

- SMS/MMS-Versand
- Aktivierung von Bluetooth-Verbindungen

Smartphone ist nicht gleich Smartphone

- Geschäftsmodelle und Philosophie der Hersteller

- Technische „Randbedingungen“

- Sicherheitsaspekte
 - technisch
 - im Umgang

BlackBerry OS (Research in Motion)

- Email-Kommunikation (neben Telefonie)
- Web-Browsing
- Adressbuch, Kalender, Aufgaben, etc.
- Optimierte Datenübertragung
- Gesonderte Tarifoption notwendig

- BlackBerry Enterprise Server (BES)
 - Daten-Synchronisation - annähernd in Echtzeit
 - Verschlüsselung der Kommunikation zum Gerät
 - Geräte und Dienstmanagement „over the air“
 - Umfangreiche Nutzerdatenkontrolle

Symbian (Nokia / Symbian Foundation)

- Variierendes Lizenzmodell
 - Symbian OS - Nokia
 - Symbian Plattform (quelloffen)
 - ab 2008 durch Symbian Foundation
 - ab 2010 durch Nokia

- Symbian Signed Process für Anwendungen von Drittanbietern zwingend erforderlich

- Vielzahl an Anwendungen und Diensten

- Firmware-Update direkt vom Endgerät, OVI-Suite oder PC Anwendung

Windows Mobile / Phone (Microsoft)

- Ursprung als tastaturloser PocketPC
- Mobile Nutzung klassischer Microsoft Anwendungen
 - Office (Kalender, Email, Aufgaben, Excel, Word)
 - Browser und Media Player
 - Freie Installation von Drittanbieter Lösungen
 - Unternehmenssoftware
- Datensynchronisation via ActiveSync
- Grundfunktionen für Geräte Sicherheit
- Individuelle Sicherheitslösungen

- Neues Konzept für Windows Phone

iOS (Apple)

- Anwendungen können grundsätzlich nur aus dem App-Store installiert werden
 - Prüfung von Funktionen und Datenversand
 - Keine individuelle (Unternehmens-) Anwendungen
- Restriktive Datenhaltung (z.B. keine Speicherkarten)
- Update-Management über iTunes
- Jail-Break per Click
 - Zugang zu offenen Stores (z.B. Cydia-Store)
 - Freie Installation von Drittanbieter Anwendungen
- Enterprise Solutions

Android (Google)

- Quelloffenes Betriebssystem
- Anwendungen können installiert werden aus
 - Android Market
 - direkt von Drittanbietern
wenn „Installation aus unsicherer Quelle“ auf dem Endgerät zugelassen wird
- Firmware-Updates werden Netzbetreiber abhängig angeboten. Installation direkt aus dem Endgerät oder über Hersteller spezifische Anwendung
- Funktion zur Remote-Löschung von Anwendungen durch Google

Aspekte zum Einsatz mobiler Endgeräte

- In welche Prozesse soll das Endgeräte eingebunden werden?
- Welche Daten werden wie auf dem Gerät gehalten?
- Wie soll das Gerät administriert werden?
- Welche Sicherheitsanwendungen werden benötigt?
- Welche Policies sind anzuwenden oder werden benötigt?

Auswahl der mobilen Plattform

Schritt 1: Welches Betriebssystem?

Schritt 2: Welcher Hersteller?

Erst dann
Schritt 3: Welches Modell?

Generelle Empfehlungen

- Zugangsdaten unter Verschluss halten und nur unter Sichtschutz gegenüber Dritten eingeben
- Wechseln Sie regelmäßig Ihre Passwörter
- Unbefugte Zugriffe und Manipulationen vermeiden
- Smartphone-Betriebssystem stets auf dem aktuellen Stand halten
- Installieren Sie Apps nur aus vertrauenswürdigen Quellen
- Installieren Sie nur Apps, die Sie regelmäßig nutzen
- Überprüfung von Einstellungen und Zugriffsrechten der Apps, falls möglich
- Unbenutzte drahtlose Schnittstellen (z.B. WLAN oder Bluetooth) deaktivieren
- Nutzung öffentlicher Hotspots mit erhöhter Vorsicht
- Umgehende Sperrung der SIM-Karte bei Verlust des Smartphones
- Nutzung der „Remote-Wipe“-Funktion Ihres Smartphones, falls vorhanden

Weitere Empfehlungen für berufliche Nutzung

- Verschlüsseln Sie sensible Daten wie E-Mails, Kontaktdaten und Zugangsdaten für das Firmennetz
- Das Telefonieren über GSM (Standard zur mobilen Sprach- und Datenübertragung) ist nicht abhörsicher
- Lassen Sie das Smartphone in Besprechungen mit vertraulichem Inhalt einfach mal draußen
- Bei Verlust bzw. Diebstahl des Smartphones umgehend den Systemadministrator Ihrer Firma informieren
- Beachten Sie die von Ihrer Firma vorgegebenen Sicherheitskonfigurationen für den Umgang mit Ihrem Smartphone
- Nutzen Sie sogenannte Krypto-Handys bei besonders hohem Schutzbedarf

Siehe: www.bsi-fuer-buerger.de

Anzeichen für mögliche Schadsoftware

- Akku-Verbrauch Ihres Smartphones ist ungewöhnlich hoch
- Smartphone schaltet sich unerwartet aus
- Smartphone versendet ungewollt persönliche Daten oder SMS
- PIN des Smartphones hat sich verändert
- Einzelverbindungsanzeige listet Verbindungen auf, die nicht zugeordnet werden können

Siehe: www.bsi-fuer-buerger.de

Weitergehende Informationen



www.bsi.de
www.bsi-fuer-buerger.de



<http://www.teletrust.de/>

Kontakt

OTARIS Interactive Services GmbH
Fahrenheitstraße 7
28359 Bremen

Fon +49 421 685 111 00
Fax +49 421 685 111 99

Frank Bittner
bittner@otaris.de

