Leitfaden – Sicherer Einsatz von Smartphones im Unternehmen

INSIDERS KNOWLEDGE

Security by Culture

AGENDA

SMARTPHONES IM UNTERNEHMENSNETZ

Endverbraucher Smartphones schwächeln im Unternehmensumfeld

Gartner berichtet in einer Studie im Februar 2012, dass über 25% aller im Jahr 2010 verkauften Mobiltelefone Smartphones waren. Die rasante Verbreitung dieser vielseitigen mobilen Endgeräte spiegelt sich auch im Einsatz in Unternehmen wieder:

- iPhones haben sich zur attraktiven Blackberry-Alternative entwickelt
- Die hohe Verbreitung von privaten Smartphones macht sog. "Bring your own device"-Strategien attraktiver. Bei diesen werden die privaten Geräte der Mitarbeiter im Unternehmen eingesetzt
- Viele Softwareanbieter (z.B. SAP, Salesforce, etc.) bieten vermehrt Apps an, die den Zugriff auf unternehmensinterne Informationsquellen ermöglichen

Endverbrauchergeräte sind aber häufig nicht für den Unternehmenseinsatz geeignet. Der Mangel an wichtigen Sicherheitsfeatures kann zum Verlust von sensiblen Informationen führen.

Die große Anbieter- und Plattformvielfalt stellt IT Abteilungen vor weitere Herausforderungen. Unterschiedliche Softwareversionen und inkompatible Sicherheitsfeatures können zu weiteren Gefährdungen führen.

➤ Smartphones im Unternehmen müssen in der Informationssicherheitsstrategie genauso berücksichtigt werden wie Computer und Notebooks.

WELCHE DATEN SIND GEFÄHRDET?

E-Mails, Kontaktinformationen und Apps beinhalten sensible Daten

E-Mails & Kontakte

Die auf dem Smartphone verfügbaren E-Mails und Kontaktinformationen sind für Angreifer wertvolle Informationen. Sie können nicht nur Geschäftsgeheimnisse beinhalten, es ist auch möglich, den E-Mail-Account auf meinem gehackten Smartphone zu nutzen, um E-Mails im Unternehmen zu verschicken. So können auch andere Computer innerhalb des Firmennetzwerks mit Hintertüren infiziert und ausspioniert werden.

Telefongespräche, SMS und Nachrichten

Es können auch andere Funktionen des Smartphones beeinträchtigt werden. Für Googles Android-Plattform ist mindestens eine Malware bekannt, mit der Angreifer alle Telefongespräche aufnehmen und belauschen können.

Smartphone-Apps für SAP und Co.

Erhält ein Angreifer Zugriff auf ein Smartphone, dann sind auch alle anderen unverschlüsselten Daten auf dem Gerät gefährdet. Apps, die den Zugriff auf CRM oder ERP System ermöglichen können in diesem Fall zum Verlust weiterer Informationen führen.

- Ein erfolgreicher Angriff auf ein Smartphone kann zum Verlust vertraulicher Informationen führen oder der Türöffner für weitere Angriffe sein

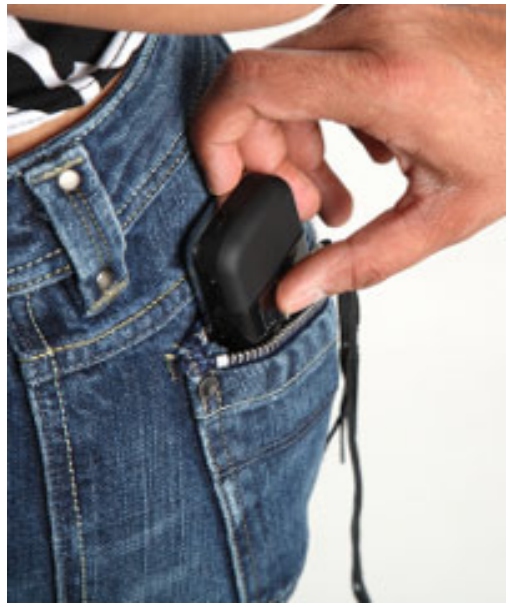
AGENDA

HÄUFIGE ANGRIFFSMETHODEN I

Schon heute existieren eine Vielzahl bekannter Angriffe auf Smartphones

Verlust oder Diebstahl

Gerade kleine Smartphones werden häufiger verloren als Notebooks und Aktentaschen. Besteht nach dem Verlust keine Möglichkeit die Daten auf dem Gerät aus der Ferne zu löschen, kann nicht sichergestellt werden, was mit den verlorenen Informationen geschieht.



Apps

Auch harmlos wirkende Apps können versteckte Funktionen beinhalten, mit denen Informationen von einem Smartphone entwendet werden können. Trotz strenger Kontrollen fielen im Februar 2012 mehre Apps in Apples AppStore auf, die ohne eine Benachrichtigung des Benutzers das komplette Adressbuch an den App-Anbieter übertrugen.

Available on the iPhone App Store

android market

BlackBerry App World™

HÄUFIGE ANGRIFFSMETHODEN II

Schon heute existieren eine Vielzahl bekannter Angriffe auf Smartphones

Drive-By Downloads

Schwächen im Web-Browser von Smartphones können zu sogenannte "Drive-By Download"-Infektionen mit Schadsoftware führen. Für den Anwender sieht es aus, als wäre lediglich der Web-Browser abgestürzt, während im Hintergrund jedoch Software installiert wurde.

Jailbreak

Nicht nur aus Sicherheits- sondern, auch aus Marketinggründen sind manche Funktionen auf vielen Smartphones eingeschränkt. Das bekannteste Beispiel ist der sog. Sim-Lock der ein Telefon auf das Netz eines bestimmten Anbieters beschränkt. Die Methode diese Einschränkungen zu beseitigen wird "Jailbreak" genannt und führt dazu, dass beliebige Drittsoftware auf dem Gerät installiert werden kann. Gleichzeitig werden jedoch auch viele Sicherheitsmechanismen deaktiviert, die Apps daran hindert auf die Daten von anderen Anwendungen zuzugreifen. Die Datensicherheit auf einem Smartphone kann daher nach einem Jailbreak nicht mehr gewährleistet werden.

Im Februar 2012 wurde eine Malware für Android-Telefone bekannt, die selbstständig einen Jailbreak ausführte, um vollen Zugriff auf das Telefon zu erlangen.

HÄUFIGE ANGRIFFSMETHODEN III

Schon heute existieren eine Vielzahl bekannter Angriffe auf Smartphones

Sicherheits- und Zollkontrollen

Aus China und Russland gibt es mehrere Berichte über Spionage-Tools die während einer Zollkontrolle auf Computern und Smartphones installiert wurden. Bei Reisen in diese Länder ist gesonderte Vorsicht geboten. In unserem Leitfaden "Reisen und Messen" gehen wir näher auf diese Gefahren ein.

Automatisches Update

Telekommunikationsprovider können Updates auf Blackberry-Telefonen in Ihrem Netz erzwingen. 2009 wurde bekannt, dass in den Vereinigten Arabischen Emiraten auf diesem Weg ein Software-Update verteilt wurde, dass Spionagesoftware enthielt, die den Zugriff auf E-Mails und Nachrichten ermöglichte. Betroffen waren hiervon nicht nur Einheimische, sondern auch Touristen und ausländische Geschäftsleute, die sich mit ihren Blackberry in diesem Netz eingesetzt haben.

BEKANNTE BEISPIELE AUS DER PRAXIS

Smartphones werden vermehrt für gezielte Angriffe und Spionage missbraucht

„We have been recently blogging about many Android malware as the threat landscape has been witnessing an increasing trend in targeting the mobile platforms and today we have received an Android package to our collection and observed that this piece of malware walks an additional mile by having a neat configuration and has a capability to record the telephonic conversation the infected victim makes."
- TotalDefense.com (01.08.2011)

„An update for Blackberry users in the United Arab Emirates could allow unauthorised access to private information and e-mails."
- BBC News (21.07.2009)

„Die iOS-App des sozialen Netzwerk Path überträgt ungefragt das gesamte Adressbuch des Nutzers an einen Server des Betreibers, wie der nicht mit dem Projekt in Verbindung stehende Entwickler Arun Thampi entdeckt hat. Der Anwender wird nicht darüber informiert."
- Heise Online (08.02.2012)

- Mangelnde Achtung des Datenschutzes und gezielte Angriffe haben bereits vermehrt zum Verlust von vertraulichen Informationen auf Smartphones geführt.

AGENDA

KOSTENERSPARNIS ODER RISIKO?

Lösen private Smartphones das Geschäftshandy ab?

Die Zahl der privaten Smartphones hat in den letzten Jahren rapide zugenommen. Wenn viele Mitarbeiter sich privat schon ein internetfähiges Smartphone zulegen, wäre es nicht sinnvoll, diese auch für geschäftliche E-Mails zu benutzen? Neu ist das Konzept „BYOD – Bring your own device“ nicht. Unternehmen könnten auf die Anschaffung teurer Hardware verzichten und stattdessen die privaten Geräte ihrer Mitarbeiter bezuschussen.

Eine solche Öffnung birgt jedoch informationssicherheitstechnische Risiken, vor Allem wenn viele unterschiedliche Geräte verschiedener Hersteller unterschützt werden sollen.

Bevor Apple 2007 das iPhone vorstellte, fand man diese Geräte fast ausschließlich im geschäftlichen Umfeld wieder. Research in Motion (RIM) galt lange als Platzhirsch in diesem Bereich. Neben den bekannten Blackberrys bietet RIM auch Softwarelösungen an, mit denen sich die Geräte im Netzwerk verwalten lassen. So können sicherheitsrelevante Optionen für alle Geräte im Netzwerk zentral festgelegt werden.

Diese Lösung ist nicht nur besonders komfortabel für die IT-Abteilungen, auch auf die Sicherung von Informationen wurde hier gesondert geachtet: E-Mails werden verschlüsselt übertragen, verlorene Blackberrys können aus der Ferne gelöscht und kritische Sicherheitsupdates erzwungen werden.

Solche Funktionen stehen bei dem Einsatz einer Vielzahl unterschiedlicher Endgeräte nicht mehr zur Verfügung.

- Der Einsatz von privaten Smartphones im Unternehmen stellt ein Risiko für die Sicherheit dar und erhöht den Wartungsaufwand enorm

AGENDA

GRUNDLAGEN FÜR DIE SICHERHEITSSTRATEGIE

Der sichere Einsatz von Smartphones muss gut organisiert sein

Anforderung an eine Sicherheitsstrategie für den Einsatz von Smartphones:

- Trainings – Ihre Mitarbeiter sind die erste Verteidigungslinie gegen Angriffe
- Kommunikation – Verdeutlichen Sie die Risiken, die durch den Umgang mit Smartphones entstehen und stellen sie sicher, dass Probleme kommuniziert werden
- Sensibilisierung – Verlust oder auch der Fremde Zugriff auf Messen und bei Reisen stellen einen Bruch der Vertraulichkeit dar
- Homogene, kontrollierte Plattform
  - Beschränken Sie Ihre Smartphone-Strategie auf Geräte eines Herstellers
  - Alle Geräte müssen Zentral gemanaged werden
- Folgende Sicherheitsfunktionen unterstützen eine sichere Smartphone Strategie
  - Beschränkung der installierbaren Apps um den Verlust vertraulicher Daten zu vermeiden
  - Verwenden Sie strenge Passwörter, vier Zahlen sind nicht genug
  - Entfernte Löschung und Sperrung der Geräte beugt wirksam dem Verlust oder Diebstahl der Geräte vor
  - Vollständige Verschlüsselung des E-Mail Zugriffs

➢ Der Einsatz von Smartphones ist notwendig, doch zur Wahrung der Sicherheit müssen Vorsichtsmaßnahmen getroffen werden

AGENDA

1 Smartphones enthalten sensible Daten
   - Smartphones im Unternehmenseinsatz
   - Welche Daten sind gefährdet?

2 Angriffe auf Smartphones in der Praxis
   - Häufige Angriffsmethoden
   - Bekannte Beispiele aus der Praxis

3 Private Smartphones im Unternehmen
   - Kostenersparnis oder Risiko?

4 Sicherer Einsatz von Smartphones
   - Grundlagen für die Sicherheitsstrategie

5 Ausblick und Fazit

6 Quellen und Referenzen

AUSBLICK UND FAZIT

Die Bedrohungen für mobile Geräte werden auch in der Zukunft zunehmen. Gleichzeitig werden die Folgen dieser Angriffe drastischer werden, da auf den Geräten mehr sensible Informationen abgefragt werden können.

Trotzdem bieten gut verwaltete Business Smartphones starke Sicherheitsfeatures und können wenn sie richtig eingesetzt werden einen guten Schutz von sensiblen Informationen an.

Die wichtigsten Funktionen für den sicheren Einsatz im Unternehmen sind:

- **Erzwungene Updates** - Keine Software ist fehlerfrei. Zügiges Einspielen von Sicherheitsupdates verringert das Risiko, dass bekannte Sicherheitslücken ausgenutzt werden
- **Fernlöschung** - Damit wird ein verlorenes oder gestohlenes Smartphone nicht zum Sicherheitsrisiko
- **Verschlüsselte E-Mail Kommunikation** - Bei der Kommunikation über öffentliche W-LANs kann sonst nicht sichergestellt werden, dass sensible Daten abgefangen oder verändert werden können
- **Beschränkung der Anwendungsinstallation** - Apps sollten auf ihre korrekte Funktion und die nötigen Datenschutzansprüche geprüft werden bevor sie eingesetzt werden dürfen
- **Blackberrys von RIM und Apples iPhones** stellen aktuell (Stand: März 2012) die sichersten Plattformen da – Android, Windows Mobile und Symbian Geräte sind noch nicht bereit für den Businesseinsatz

➤ Bleiben Sie sicher.

AGENDA

QUELLEN UND REFERENZEN

- „2011 Mobile Threats Report“, Juniper Networks, Februar 2012
  http://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2011-mobile-threats-report.pdf?utm_source=promo&utm_medium=right_promo&utm_campaign=mobile_threat_report_0212
- "Your address book is mine: Many iPhone apps take your data", VentureBeat, 14. Februar 2012
  http://venturebeat.com/2012/02/14/iphone-address-book/
- „Android.Counterclank Found in Official Android Market“, Symantec Connect, 27. Januar 2012
  http://www.symantec.com/connect/fr/blogs/androidcounterclank-found-official-android-market
- "Gartner Says Worldwide Smartphone Sales Soared in Fourth Quarter of 2011 With 47 Percent Growth", Gartner, 15. Februar, 2012
  http://www.gartner.com/it/page.jsp?id=1689814
- "Drive-by exploit slurps sensitive data from Android phones", The Register, 29. Januar 2011
  http://www.theregister.co.uk/2011/01/29/android_data_disclosure_bug/
- „ZeuS-in-the-Middle for Android“, SecureList by Kaspersky, 12. Juli 2011
  http://www.securelist.com/en/blog/208193029/ZeuS_in_the_Mobile_for_Android
- „A Trojan spying on your conversations“, Total Defense Blog, 01. August 2011
  http://totaldefense.com/blogs/security-advisor/2011/08/26/a-trojan-spying-on-your-conversations.aspx
- „Security Alert: New RootSmart Android Malware Utilizes the GingerBreak Root Exploit”, Xuxian Jiang, NC State University, 03. Februar 2012
  http://www.csc.ncsu.edu/faculty/jiang/RootSmart/
- „iPhone Rootkit? There‘s an App or that!“, Eric Monti, Trustwave Spiderlabs, Juni 2010
  http://reverse.put.as/wp-content/uploads/2011/06/iphonerootkittoorcon2010.pdf
- "BlackBerry's armor has cracks, security experts say", Reuters, 5. August 2010
  http://www.reuters.com/article/2010/08/05/us-blackberry-security-idUSTRE6745L820100805
- "UAE Blackberry update was spyware", BBC News, 21. Juli 2009
  http://news.bbc.co.uk/2/hi/8161190.stm
- “iOS-App verschickt Adressbuch an den Hersteller” Heise.de, 08. Februar 2012
  http://www.heise.de/newsticker/meldung/iOS-App-verschickt-Adressbuch-an-den-Hersteller-1430793.html

AGENDA

INSIDERS**KNOWLEDGE**

Security by Culture

Wir unterstützen kleine und mittelständische Unternehmen bei der Entwicklung von Informations-Sicherheitsbewusstsein in der Unternehmenskultur. Die Mitarbeiter unserer Klienten sind die erste Verteidigungslinie zum Schutz von Geschäftsgeheimnissen und vertraulichen Daten.

Wir bieten umfassende Sicherheitskonzepte an, die wir individuell an Ihr Unternehmen anpassen. Wir unterstützen Sie gerne bei:

- Managementstrategien zur Stärkung des Sicherheitsbewusstseins im Unternehmen
- Mitarbeitertrainings zur Identifikation von Angriffen und Wirtschaftsspionage
- Trainings für Ihre IT-Mitarbeiter zur Identifikation und Abwehr aktueller Angriffsmethoden
- Analyse und Beratung zur Sicherung bestehender IT-Infrastruktur
- Und allen anderen Fragen zum Thema Informationssicherheit

Für eine kostenlose Vorstellung unserer Beratungsleistungen können uns gerne über info@InsidersKnowledge.com kontaktieren.