KEY-NET Technologieseminar – Perlen 22. Juni 2007

Security für mobile Geräte

KEY NET
NETZWERK- UND KOMMUNIKATIONSLÖSUNGEN

Ihr Referent

Wolfgang Sidler
Senior Security Consultant
e-mail: wolfgang.sidler@infoguard.com
Tel: 041 749 19 67

Bei InfoGuard AG als Sicherheitsberater tätig.

- Master in Information Security, HSW Luzern
- Wirtschaftsinformatiker mit Eidg. Fachausweis
- BSI Certified ISO 27001 Lead Auditor
- Microsoft Certified Systems Engineer (MSCE)
- ITIL Certified

Berufserfahrung im Bereich ICT Security/Audit:

- 20 Jahre Informationstechnologie
- Seit mehr als 8 Jahren im Bereich Informationssicherheit tätig
- IT-Security Officer bei der renommierten Schweizer Privatbank Julius Bär
- Security Consultancy Manager Europe bei Zurich Financial Services
- Projektleiter im Ausland

Engagement

- Mitautor „Sicherheitshandbuch für die Praxis“ (ISBN 3-9521208-3-9)
- Prüfungsexperte für Informatik-Lehrlinge im Kanton Luzern

Page 2
© InfoGuard AG June 07

Angriffspunkt – PC / Notebook / PDA / Speichermedien

Fakten

- Mobile Geräte und portable Speichermedien werden häufig eingesetzt.
- Mitarbeitende tragen auf ihren mobilen Geräten vertrauliche Daten mit.
- Mobile Geräte gehen verloren oder werden gestohlen.

Risiko

- Ohne entsprechenden Schutz können diese Daten problemlos eingesehen und ausgelesen werden.

Der Hardware-Verlust ist in einem solchen Fall sekundär.

Page 3
© InfoGuard AG June 07

Menschliche Fehlhandlungen - Handys, PDAs, Notebooks und deren Weg …

Innert 6 Monaten verloren gegangene mobile Geräte in London:

2001
- 62'000 Handys (3 pro Taxi)
- 2'900 Notebooks
- 1'300 PDAs

2004
- 63'135 Handys
- 4'973 Notebooks
- 5'838 PDAs

2006
- 54'872 Handys
- 3'179 Notebooks
- 4'718 PDAs
- 923 Memory Sticks

Quellen:
http://www.theregister.co.uk/2001/08/31/62_000_mobiles_lost/
http://www.theregister.co.uk/2005/01/25/taxi_survey/

Page 4
© InfoGuard AG June 07

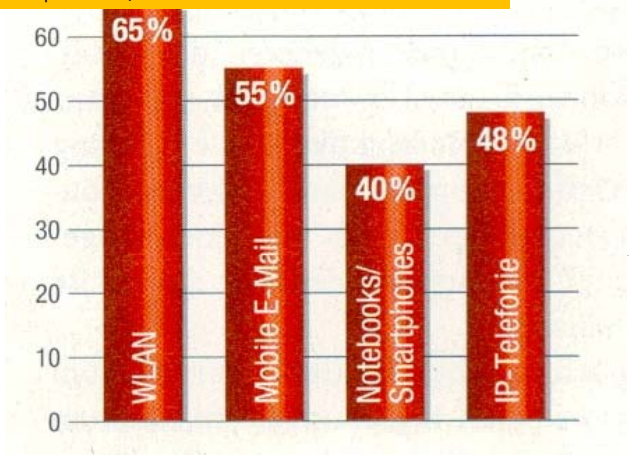
Alles an den Haaren herbeigezogen ?

War die Festplatte verschlüsselt?

Page 5
© InfoGuard AG June 07

Aktuelle Studien bestätigen dass ….

Mobilität der Mitarbeiter?
Eine Cisco Studie, 1'000 befragte Unternehmen,
Quelle: Computerworld, 1. Juni 2007



Page 6
© InfoGuard AG June 07

Angriffspunkt – Bluetooth

Fakt
Auf mobilen Geräten lassen sich sehr viele Informationen speichern und über Bluetooth austauschen/abgleichen.

Aber:
- Beliebige Dateien im Speicher können einfach ausgelesen oder gelöscht werden.
- Das Adressbuch und die Anrufprotokolle können eingesehen werden.
- SMS-Nachrichten können problemlos gelesen und (auf fremde Kosten) geschrieben werden.

Page 7
© InfoGuard AG June 07

Angriffspunkt – Handyspion FlexiSpy - ab 100.- Euro - Bangkok

- Überwacht Anrufe, E-Mail, Standort und SMS etc.
- Muss installiert & aktiviert werden
- Benötigt seit V2 physischen Zugang zum Telefon
- Einmal installiert und aktiviert, ist FlexiSpy ***vollkommen unsichtbar***
- Überwachung mittels Web-Zugang

Page 8
© InfoGuard AG June 07

Speichergeräte
Risiken und Gefahren

Datenklau

- Schnelle (USB2.0 = bis zu 20MB/Sek.) Verbindungen, grosse Kapazitäten (1GB ca. CHF 25.-)
- Datenspeicher unverschlüsselt
- Klau-Programme in verschiedenen Varianten
  - Einfaches kopieren
  - Versand via eMail im Hintergrund
  - Diebstahl von verschiedenen Informationen

- Datenverlust
  - Schnell kopiert, schnell verloren

- Transport von Schad-Programmen

Page 9
© InfoGuard AG June 07

Mobiles Arbeiten
Allgemeine Risiken und Bedrohungen 1

- Mobilität (Grösse/Gewicht) der Geräte

- Zunehmende Loslösung von den Kabeln
  - WLAN, Bluetooth, UMTS, EDGE etc.

- Synchronisation von Daten
  - Workstation zu SmartPhone/PDA
  - LAN zu Laptop (Windows Offline Files)

- Zunehmende Komplexität der Lösungen und abnehmende Vorsicht der Benutzer

- „Pervasive Computing“
  - Immer und überall Zugang zu Firmennetz und Internet

Page 10
© InfoGuard AG June 07

Mobiles Arbeiten
Allgemeine Risiken und Bedrohungen 2

- Zugänge zu privaten Netzen über unsichere Verbindungen
- Fehlende oder nicht aktuelle Datensicherungen
- Zunehmender Diebstahl
- Sorglosigkeit der Benutzer und keine Benutzer-Schulung
- Applikations-Fehler
- Attacken mit Forenesic-Tools
- Hohe Kommunkations-Kosten

Demo –
Notebook knacken

Notebook mit Windows NT/2000/XP (gefunden oder gestohlen).

System zeigt beim Start das Anmeldefenster mit (oder ohne) Benutzername.

Ziel:
- In kurzer Zeit Administrator-Zugang zum System, ohne das Passwort zu kennen
- Daten auf Disk auslesen
- Gelöschte Daten auf Disk finden
- Klau der Identität des Besitzers. Auslesen der IE-Passwörter (eMail Username und Passwort etc.)

Weitere Aktionen könnten sein: unsichtbarer Trojaner installieren und danach den Notebook anonym dem Besitzer zurückgeben.

Tipps vom Sicherheits-Experten
Halten Sie vertrauliche Informationen einfach GEHEIM

- Speichern Sie vertrauliche Daten auf mobilen Geräten immer verschlüsselt.
- Transportieren Sie vertrauliche Daten nur geschützt.
- Senden Sie vertrauliche eMails nur verschlüsselt.
- Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihren Computer an.
- Legen Sie keine CD ein, von der Sie nicht wissen, woher sie stammt.
- Überprüfen Sie USB-Sticks und CDs nach Viren, bevor Sie sie verwenden.
- Geräte nicht automatisch starten lassen (Windows Autorun Funktion).
- Daten auf sichere Art löschen; braucht zusätzliche Software.
- Verwenden Sie einen Display-Einsicht-Schutz (Privacy).
- Erstellen Sie ein Disk-Image und erstellen Sie regelmässig ein Backup (Daten-Synchronisation).

Tipps vom Sicherheits-Experten
Seien Sie einfach DISKRET

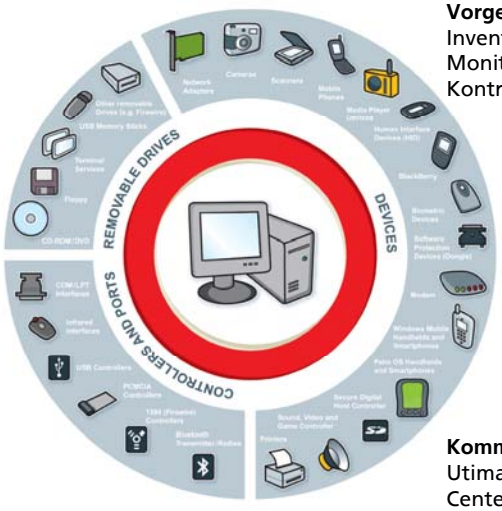
- Behandeln Sie geschäftliche Themen in der Öffentlichkeit vertraulich.
- Lassen Sie andere nicht mithören.
- Lassen Sie sich nicht aushorchen.
- Lassen Sie Notebook, Handy oder PDA nie unbeaufsichtigt, wenn, dann aktivieren Sie den Screen-Lock.
- Vermeiden Sie Ihr mobiles Gerät auf irgendeine Weise mit Ihrer Firma in Verbindung zu bringen (Logos, Kleber etc.).

Tipps vom Sicherheits-Experten
Sind Sie vorbereitet? Denken Sie in Szenarien!

- Risikoanalyse durchführen
- Regeln (Weisung) für die Nutzung von mobilen Geräten erstellen
  - Umgang, Was ist zu tun bei Verlust/Diebstahl, Verhalten auf Reisen etc.
- Den Benutzer in die korrekte Bedienung einführen.
- Keine privaten Geräte für geschäftliche Nutzung.
- Unbekannte Software nicht installieren/aktivieren.
  - Sensibilisierung der Benutzer
- Schutz gegen Schädlinge installieren.
  - Wenn möglich zentral verwalten
- Verschlüsselung der Daten auf dem mobilen Gerät sicherstellen.
  - Lösungen existieren (Symbian, Windows, PalmOS)
  - z.T. können Daten auch entfernt zerstört werden

Page 15
© InfoGuard AG June 07

Technische- und organisatorische Lösung - Device Control!



Vorgehen
Inventar, Weisung, Awareness, Monitoring, Device Management, Kontrolle

Kommerzielle Tools:
Utimaco, Santuary Device Control, Centennial, Device-Wall, ISM USB-Blocker Plus, Smartline Device-Lock, Safend Protector etc.

Page 16
© InfoGuard AG June 07

Fazit: Ihr Nutzen …

- Kein fahrlässiger Datenverlust!
- IT-Leiter hat keine schlaflosen Nächte mehr!
- Benutzer fühlt sich sicherer
- Interne Weisungen können so durchgesetzt werden
- Wettbewerbsvorteil -> Sicherheit = Vertrauen
- Fördert das „Sicherheitsbewusstsein" der Mitarbeiter
- Kein Image-Schaden und keine juristischen Konsequenzen

Page 17
© InfoGuard AG June 07

Vielen Dank für Ihre Mitarbeit

U make Sec_rity work!

Page 18
© InfoGuard AG June 07