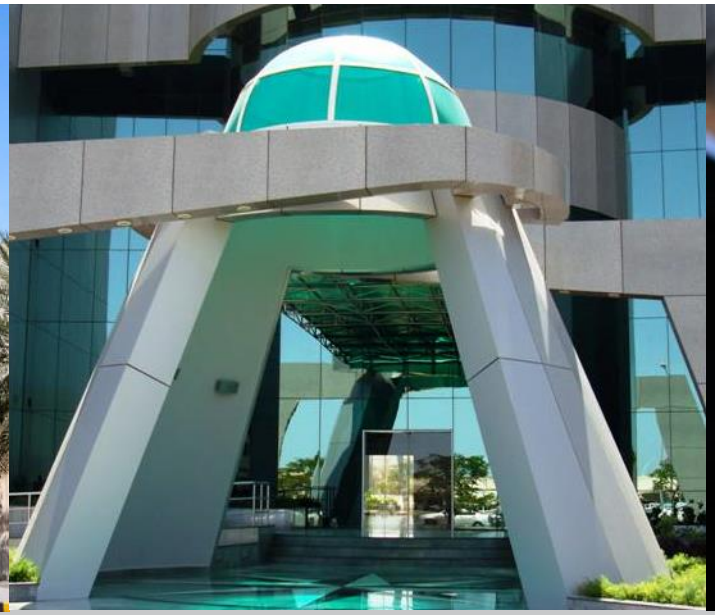
HAGELIN-CRYPTOS
CRYPTO AG


Crypto Secure Behaviour

How to protect your business data

Wolfgang Sidler, Senior Security Consultant

Steinhausen, 17. December 2007

Alles an den Haaren herbeigezogen ?

War die Festplatte verschlüsselt?

Mobility –
anytime, everywhere! Risk or Opportunity?

Angriffspunkt –
PC / Notebook / PDA / Speichermedien

Fakten

- Mobile Geräte und portable Speichermedien werden immer häufiger eingesetzt.
- Mitarbeitende tragen auf ihren mobilen Geräten vermehrt 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.

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

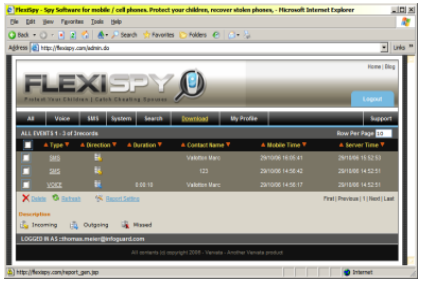
2004
- 63‘135 Handys
- 4‘973 Notebooks
- 5‘838 PDAs

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/

Angriffspunkt – Handyspion FlexiSpy –
– Server steht in Bangkok, Thailand

- 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



Speichergeräte - Risiken und Gefahren

- **Datenklau**
  - Schnelle (USB2.0 = bis zu 20MB/Sek.) Verbindungen, grosse Kapazitäten bis zu 8 GB (1GB ca. CHF 16.-)
  - Datenspeicher sind meist unverschlüsselt!
  - Klau-Programme (Trojaner) in verschiedenen Varianten
    - Einfaches kopieren (USBDump, iPodSlurp)
    - Versand via E-Mail im Hintergrund
    - Diebstahl von verschiedenen Informationen, wie Passwörter, Kreditkarten-Informationen etc.
- **Datenverlust**
  - Schnell kopiert, schnell verloren
  - Transport von Schad-Programmen (Trojaner, Malware)

Mobiles Arbeiten – Allgemeine Risiken und Bedrohungen 1

- Mobilität (Grösse/Gewicht/Funktionen) der Geräte
- Zunehmende Loslösung von den Kabeln
  - WLAN, Bluetooth, UMTS, EDGE etc.
- Synchronisation von Daten
  - PC zu Handy/SmartPhone/PDA
  - Netzwerk zu Notebook (Windows Offline Files)
- Zunehmende Komplexität der Lösungen und abnehmende Vorsicht der Benutzer – Bequemlichkeit ist unser grösster Feind!
- Immer und überall Zugang zu Firmennetz und Internet

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 Hacker-Tools
- Hohe Kommunikations-Kosten (Roaming, E-mail etc.)

Ungebetene Zuhörer

Macht der Behörden bzw. des Staates

- Telefonleitungen werden im Ausland vom Staat bzw. vom Nachritendienst abgehört
- Internet-Verbindungen werden protokolliert und gefiltert. (z.B. in UAE, Oman etc.)
- Skype bzw. VOIP ist in vielen Ländern (UAE und Oman) offiziell verboten und wird vom Provider gesperrt, wenn möglich.
- Für spezielle Kommunikations-Einrichtungen wie SAT, HF-Radio etc. benötigt man eine spezielle Einfuhr- und Betriebs-Lizenz.

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.)
- Verwenden Sie im Flugzeug oder im Zug einen speziellen Sichtschutzfilter (3M) für Ihren Notebook. Somit kann der Sitznachbar auf Ihrem Bildschirm nichts erkennen.

Tipps vom Sicherheits-Experten – Halten Sie vertrauliche Informationen einfach GEHEIM

- Schiessen Sie vertrauliche Unterlagen weg.
- Speichern Sie vertrauliche Daten auf mobilen Geräten immer verschlüsselt ab.
- Transportieren Sie vertrauliche Daten nur geschützt.
- Senden Sie vertrauliche e-Mails nur verschlüsselt.
- Wählen Sie ein komplexes Passwort von mind. 8 Zeichen. Machen Sie Passwörter einfach STARK.
- Keine sensiblen Dokumente und CD‘s ungeschreddert in den Papierkorb werfen.
- Keine Dokumente als DOC per E-Mail versenden. Senden Sie nur PDF-Dokumente als Attachment in einem E-Mail.

Tipps vom Sicherheits-Experten – Sind Sie einfach VORSICHTIG!

- Unbekannte Software nicht installieren/aktivieren. Vorsicht bei Freeware!
- Verwenden Sie WLAN und Bluetooth Verbindungen sparsam
- Schutz gegen Schädlinge installieren. Antivirus-Software auf dem aktuellen Stand halten. Auch auf dem PC zu Hause!
- Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihren Notebook/PC an (iPod-Slurp). Schliessen Sie Ihren USB-Stick nicht an einen fremden Notebook/PC an (USB-Dump).
- Legen Sie keine CD-Rom ein, von der Sie nicht wissen, woher sie stammt.
- Überprüfen Sie USB-Sticks und CD-Rom‘s nach Viren, bevor Sie sie verwenden.

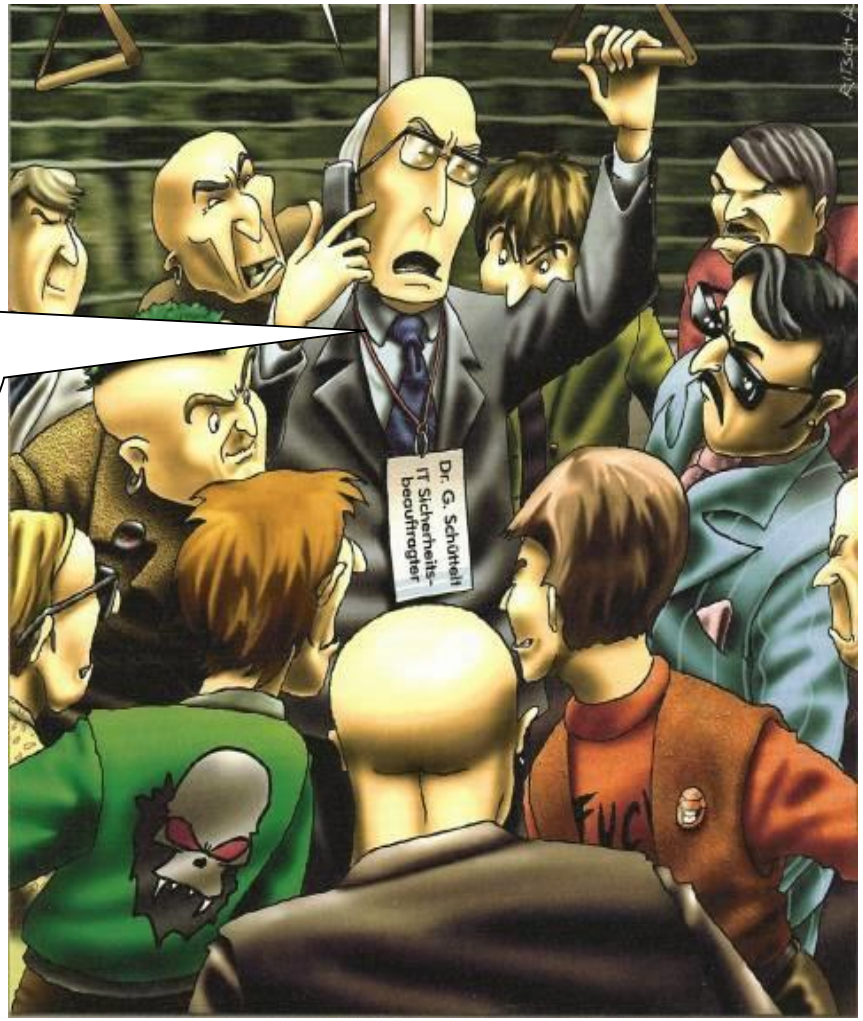
Social Engineering (SE) - Der Mensch als Tor zu sensiblen Informationen

- Informationen beschaffen
- Aufbauen eines vermeintlichen Vertrauens
- Gezielte Manipulation von Personen, um an die gewünschten Informationen zu gelangen
- Ausnutzen von menschlichen Eigenschaften, um das Opfer zu bestimmten Aktionen zu verleiten
- Angriffe auf IT-Systeme oder Diebstahl von Daten und Passwörtern über Menschen
- Personen ohne Fachwissen zu Sicherheitsgefährdenden Aktionen bewegen

Fazit: Ihr Nutzen …

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

Gesunder Menschenverstand



To Remain Sovereign

Thank you for your attention!

www.crypto.ch