IT-SICHERHEIT UND MOBILE SECURITY

Grundlagen und Erfahrungen

Dr.-Ing. Rainer Ulrich, Gruppenleiter IT SECURITY

Fraunhofer IIS

Schäubles Handy bei Einbruch gestohlen

FrankfurterRundschau

Bei Wolfgang Schäuble ist eingebrochen worden. Die Diebe sollen in Schäubles Privathaus eingestiegen und mehrere persönliche Gegenstände mitgenommen haben – darunter auch das Handy des Finanzministers.

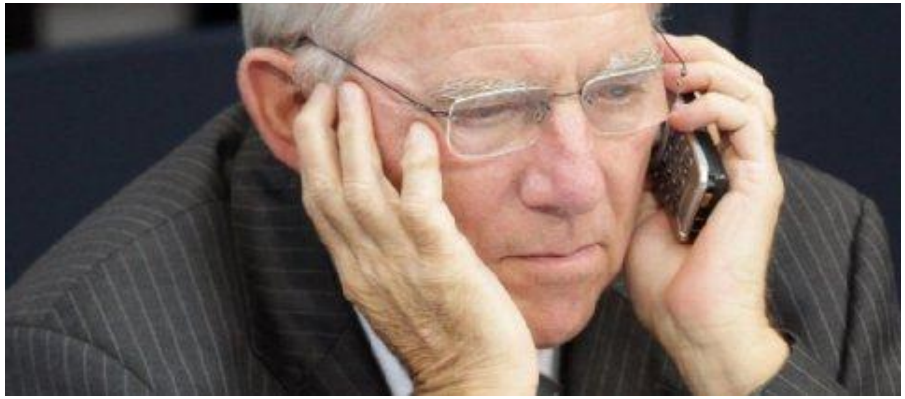


Foto: dpa

[…] Ob die Täter so an sensible Daten kommen könnten, ist unklar, das BKA nahm dazu keine Stellung.

Die »Berliner Morgenpost« zitiert einen ranghohen Polizeiführer, der den Einbruch als »eklatantes Sicherheitsproblem« bewertete. Schließlich seien in dem Handy »sicherlich nicht unwesentliche Telefonnummern« gespeichert gewesen.

Bedrohungsanalyse

- Ermittlung möglicher
  - Bedrohungen
  - Angreifer
- Bewertung des potenziellen Schadens
  - materiell
  - Imageschaden
- Wahrscheinlichkeit einer Bedrohung
- Die größte Gefahr für eine Firma ist nicht der Hacker aus dem Internet, sondern der nicht genügend geschulte Mitarbeiter!

BSI IT Grundschutz
Eine kurze Checkliste

- ☑ Serverraum sicher vor Feuer, Wasser, Spannungsausfall?
- ☑ Wichtige Geräte doppelt vorhanden?
- ☑ Regelmäßiges Backup aller Daten?
- ☑ Backup getrennt und sicher gelagert?
- ☑ Sichere Passwörter, Screensaver mit Passwortschutz?
- ☑ Stets aktueller Virenscanner?
- ☑ Sinnvoll konfigurierte Firewall?
- ☑ »Normales« Verhalten des Systems dokumentiert?
- ☑ Sensitive Daten sind verschlüsselt?
- ☑ Notfallpläne verfügbar?
- ☑ Regelmäßige Schulung der Mitarbeiter?
- ☑ Sicherheitskonzept wird regelmäßig überprüft?

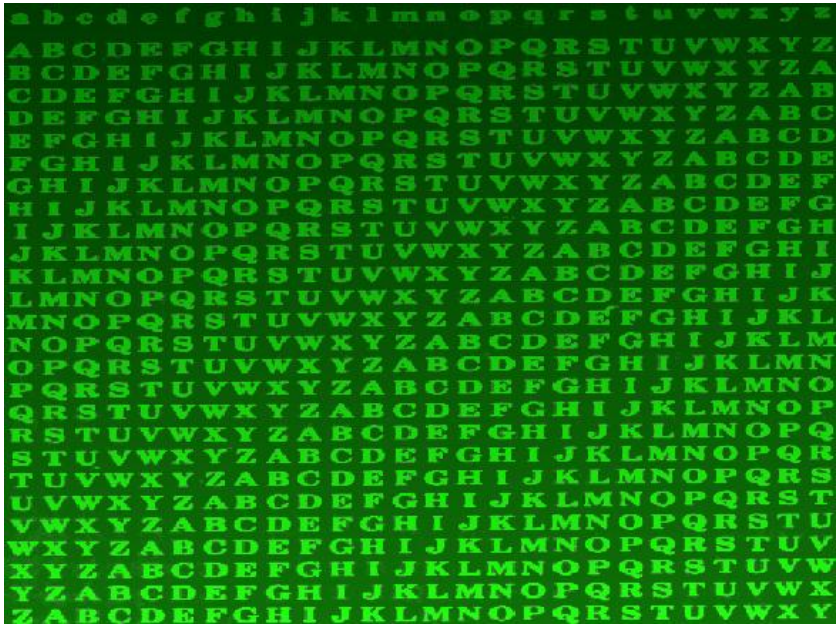
Authenifizierung

Identität kann bewiesen werden durch

- Besitz (z.B. Schlüssel)
- Ein gemeinsames Geheimnis (z.B. Passwort)
- Biometrische Merkmale

Verschlüsselung und Signatur

- Verschlüsselung zwingend bei vertraulichen und Personen bezogenen Informationen
- Mail: S/MIME oder PGP/GnuPG?
- Plattenverschlüsselung
- Verschlüsselung mobiler Speicher



Firewall und Virenscanner
Firewall

- Eine falsch konfigurierte Firewall ist genauso schlimm wie gar keine.
- Personal Firewall auf allen Rechnern mit direktem Internet-Zugang
  - schützt im öffentlichen WLAN
  - alleine nicht ausreichend
- Next-Generation-Firewalls?

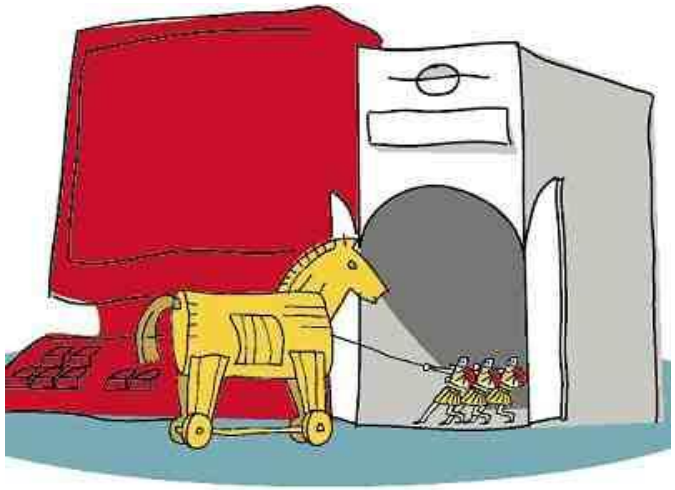
Firewall und Virenscanner

Virenscanner

- Aktueller Virenscanner auf jedem Rechner
- Externe Datenträger vor Benutzung scannen
- Email ist heute nicht mehr das Haupt-einfallstor für Viren!
- Keine Garantie, dass eine Mail virenfrei ist

Software regelmäßig aktualisieren

- Vorsicht bei Verwendung von Software aus unsicheren Quellen
- Keine Verwendung von Programmen, die unkontrollierbar Daten versenden: Browser-Toolbars, Internet-Optimierer, Screensaver,…
- Ständig Sicherheitspatches und Updates einspielen
  - Für das Betriebssystem
  - Für Virenscanner und Firewall



Angriffsziel Mitarbeiter

- »Verlorener« USB-Stick
- Heimliche Mitleser
- Diebstahl
- Telefonate in der Öffentlichkeit

Angriffsziel Mobile Devices: Diebstahl

- Smartphones enthalten oft mehr sensitive Daten als Laptops:
  - E-Mail
  - Kalender
  - Kontakte
  - Bilder
  - Dokumente
- Oft völlig ungeschützt

Bild: Kaspersky

Angriffsziel Mobile Devices: Phising, Malware

- Ein unbemerkt infiziertes Firmen-Handy ist ein ideales Spionagewerkzeug.
- Das Betriebssystem von Smartphones hat Lücken, die oft nicht geschlossen werden:
  Aktuelles OS nur mit neuem Smartphone.

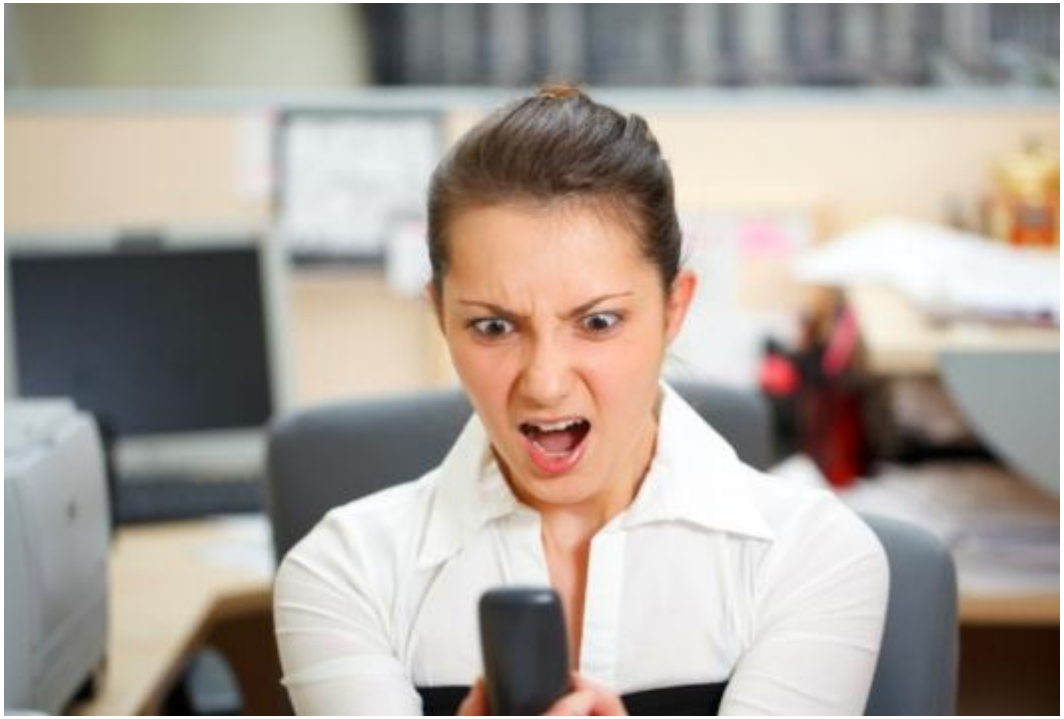


Bild: Kaspersky

Beispiele:

- PC-Welt 5/2011: 99 % aller Android-Smartphones geben die IDs ihrer Nutzer preis. Das Sicherheitsleck wurde erst mit der Version 2.3.4 gestopft. Die wird jedoch nur von 1 % aller Android-Kunden genutzt.
- Heise Security 28.9.2012: Die aktuelle Android-Version (4.1.x) ist erst auf 1,2 Prozent aller Android-Smartphones installiert – was vor allem daran liegen dürfte, dass es für die meisten Geräte kein Update gibt und auch nicht geben wird.
- Heise Security 6.11.2012: Android-Apps können dem Smartphone-Benutzer vorgaukeln, dass er eine SMS von einem beliebigen Absender erhalten hat […] Wann und mit welcher Android-Version die Lücke genau geschlossen wird, ist derzeit noch unklar. Wer ein Android-Smartphone besitzt, sollte sich jedoch keine allzu großen Hoffnungen machen, dass das Update sein bereits gekauften Gerät erreicht – die meisten Hersteller versorgen ihre Bestandskunden nur sehr mangelhaft mit OS-Updates.

Es gibt keine kostenlosen Apps:
Man bezahlt mit seinen Daten!

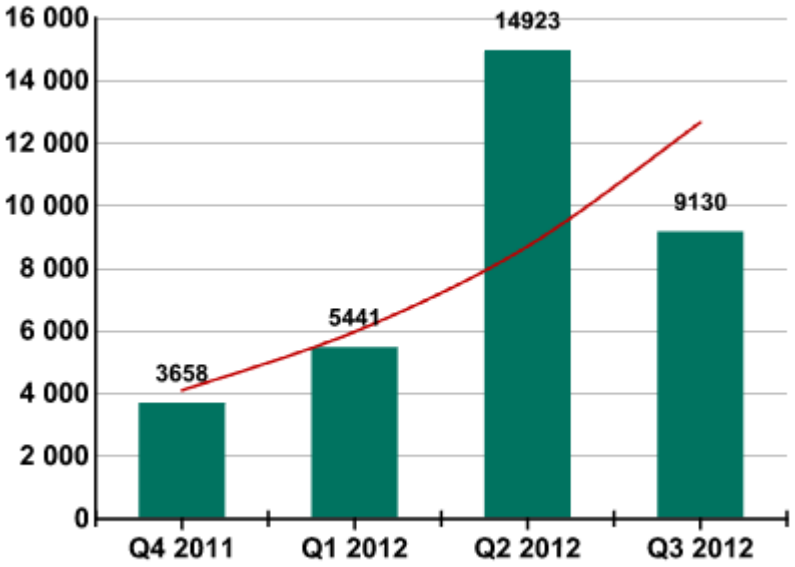
- Zugriff auf Positionsdaten
- Zugriff auf das Adressbuch
- Zugriff auf SMS
- Zugriff auf Kamera

…. und das oft ohne vorherige Erlaubnis

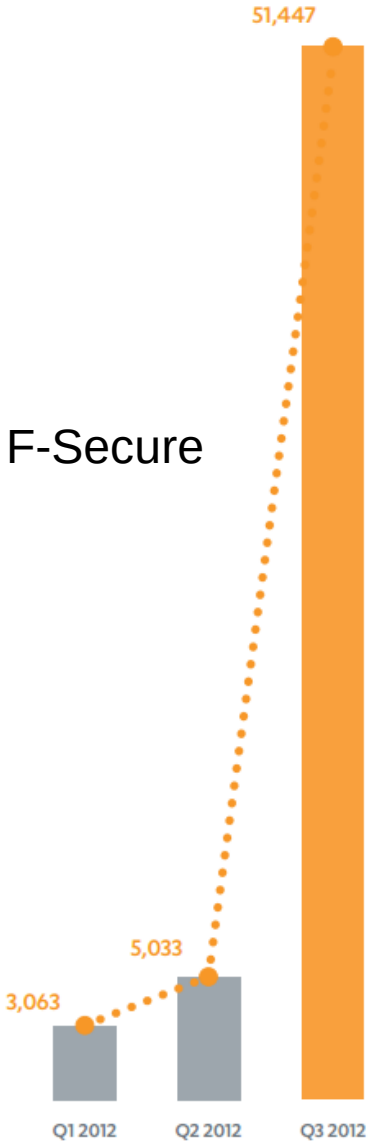
oder verklausuliert:
»Durchsuche deine Kontakte nach Leuten, die du bereits kennst«

Auftreten von Android-Malware:
Welcher Statistik kann man trauen?

Kaspersky



F-Secure



Fraunhofer IIS

Gegenmaßnahmen

- Diebstahl
  - Sperrung bei Kartenwechsel
  - Fernlöschen aller Inhalte
  - Alarm, GPS-Ortung
- Malware
  - App-Kontrolle
  - SMS-Filter
  - Firewall, Anti-Phising
  - Container
  - Verschlüsselung
  - Regelmäßige Updates

Bring Your Own Device (BYOD)

Smartphone gehört der Firma	■ Firma bezahlt und konfiguriert das Gerät ■ Wipe bei Missbrauch ■ Vertrauenswürdig	■ Sicherheitsrisiko
Smartphone gehört dem Mitarbeiter	■ Rechtlich problematisch	■ Gerät unter Kontrolle des Mitarbeiters ■ Kein Wipe durch die Firma möglich ■ Beschränkter Zugriff
	Managed	Unmanaged

Containerlösung für private Smartphones

- Firmendaten befinden sich in verschlüsseltem Container
- Container kann per Remote Wipe gelöscht werden
- Zugriff auf das Firmennetz nur über sichere Apps aus dem Container

Ihre Fragen, bitte!

Dr.-Ing. Rainer Ulrich

Fraunhofer-Institut für Integrierte Schaltungen IIS

Am Wolfsmantel 33, 91058 Erlangen

rainer.ulrich@iis.fraunhofer.de