Bundesamt
für Sicherheit in der
Informationstechnik

Smartphones in Unternehmen und Behörden

–

Gefährdungen für die Informationssicherheit und Gegenmaßnahmen

Dr. Patrick Grete
Bundesamt für Sicherheit in der Informationstechnik
Referat B21 – Grundlagen der Informationssicherheit und IT-Grundschutz

GI SECMGT-Workshop: Praxisprobleme der Informationssicherheit
03.02.2012

Inhalt

- Einführung: Einige Zahlen zu Smartphones
- Typische Gefährdungen der Informationssicherheit durch Smartphones
- Weitere Gefährdungen durch „Consumerization“
- Smartphones und IT-Grundschutz
- Maßnahmen: Sicher(er) Betrieb von Smartphones

Cum grano salis: Einige Zahlen zu Smartphones (1/2)

- Junipers „Malicious Mobile Threats Report 2010/2011“:
  - 17% aller Smartphone-Trojaner senden Premium-SMS
- Pointsec Erhebung 2005: In 900 Chicago-Taxis: 85619 Handys, 21460 PDAs, 4425 Laptops in 6 Monaten „liegen gelassen“.
- BSI: 47% aller Smartphone-Nutzer haben noch nie das Smartphone gepatched

Cum grano salis: Einige Zahlen zu Smartphones (2/2)

- Steria Mummert Umfrage Juli 2011 (1000 Befragte)
  - 38% halten Datenverschlüsselung auf Smartphone für nötig
  - 60% benutzen Smartphone als PC, nur 15% sehen es als PC
  - 33% nutzen Smartphone für Finanztransaktionen
- McAfee Studie „Mobilität & Sicherheit 2011“ (1500 Befragte)
  - 40% meldeten Diebstahl an; 1/3 führte zu finanziellen Schäden
  - 20% lassen beliebige Smartphones am Arbeitsplatz zu

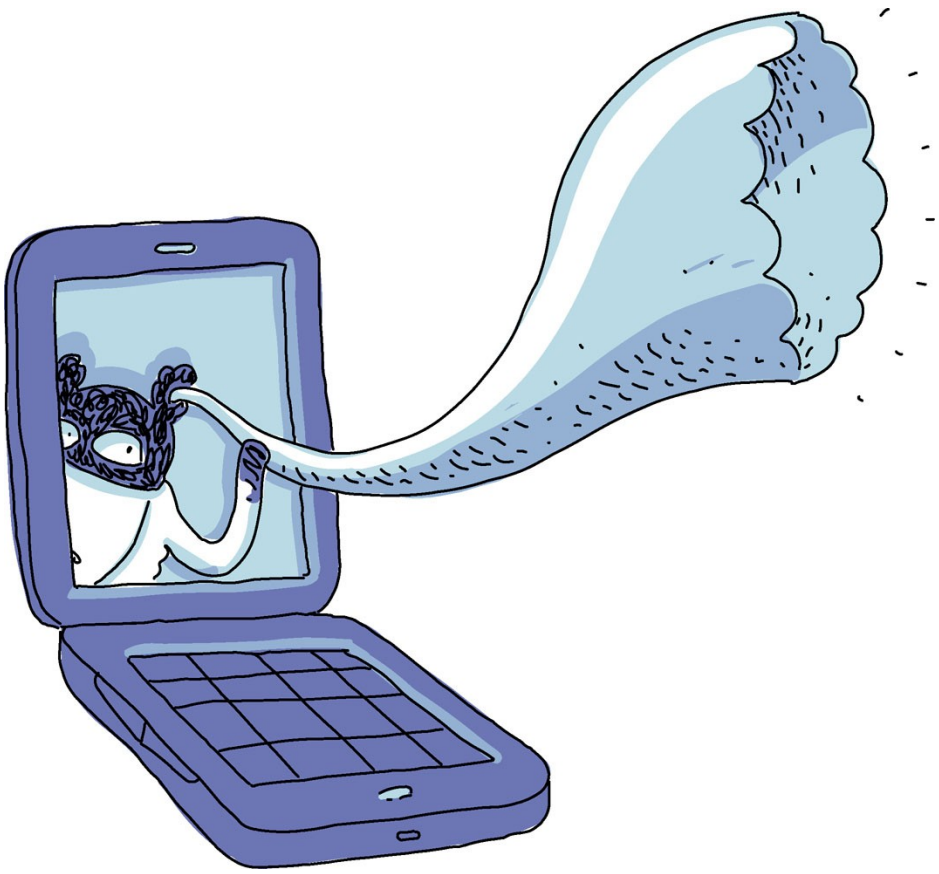
Gefährdung: Verlust/Diebstahl von Daten und Gerät

Gefährdung durch Einsatz in ungeschützter Umgebung

- Verlust von Vertraulichkeit durch
  - Neugierige Blicke
  - Gute Ohren
  - Unverschlüsselte Datenverbindung

Gefährdung durch Trojaner und Spionage-Apps

- FlexiSpy et al.
- 2009: iZombie für iPhone
- 2011: ZeuS-Trojaner stiehlt mTANs
- Auch ohne „Viren“: Rechtehungrige Apps
  - Taschenlampe ins Internet
  - Snake-Spiel mit Adressbuchzugang
  - Kochbuch will selbsttätig telefonieren
  - Einkaufszettel will GPS



Gefährdung: Bot-Netze und Dialer

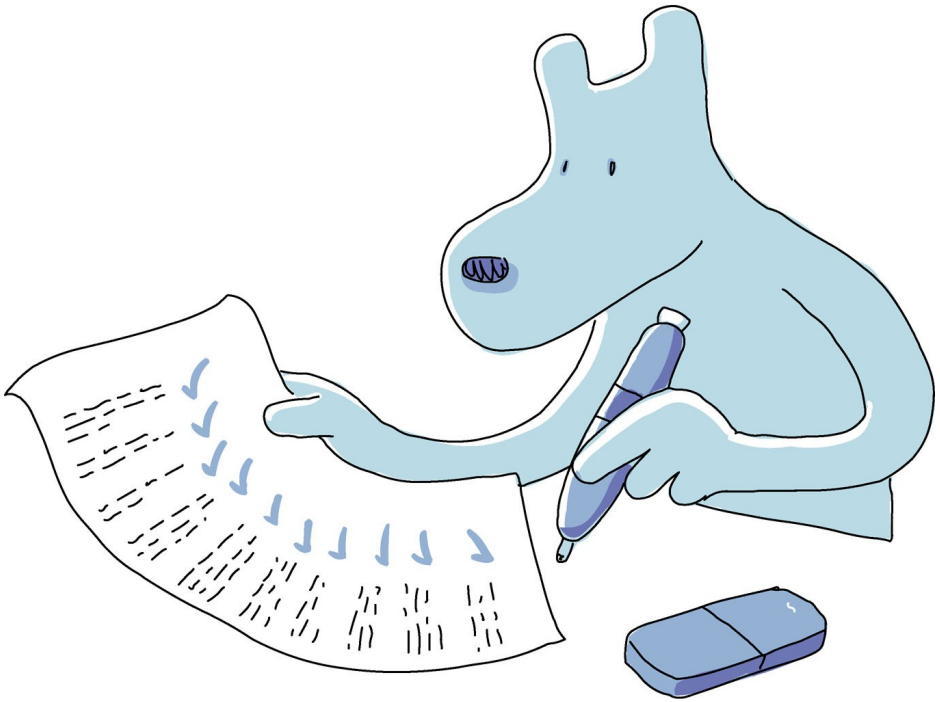
- 17% der Trojaner-Apps senden Premium-SMS
  („Malicious Mobile Threat Report 2010/2011“, Juniper Networks Global Threat Center)
- Trojaner-Apps versenden verseuchte Links über Twitter, Facebook & Co
- Trojaner-Apps klicken Werbung an
- Suchmaschinen Poisoning

Andere Einfallstore für Schadsoftware

- Verseuchte
  - E-Mails
  - SMS/MMS
  - Internetseiten
  - Dateiübertragung

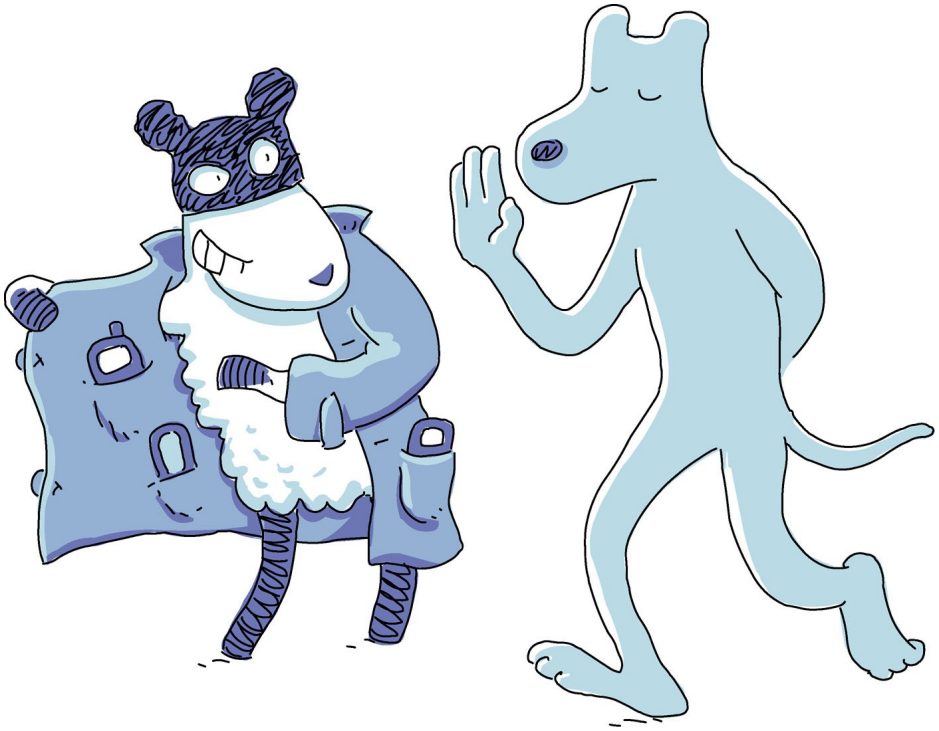
Gefährdung durch Unkenntnis oder Umgehung von Regelungen

- Allgemeine Richtlinien (Umgang, Datensicherung, Verlust, etc.)
- Passwortrichtlinien auf Smartphones
- Umgang mit Dateianhängen
- Trennung privat und dienstlich
- Mangelndes Problembewusstsein (20% halten jegliche Sicherheitsmaßnahmen für Smartphones für unnötig)(Steria Mummert Umfrage Juli 2011, „Mobile Geräte im Alltag“; 1000 Befragte)



Last but not least: Social Engineering

- Es muss nicht immer ein „Mission-Impossible“-Szenario sein
- Es reicht
  - Kurzer Zugriff auf Gerät
  - Anklicken eines Links
  - Öffnen einer Datei
- Generell: Je wertvoller das Ziel, desto höher der plausible Aufwand.



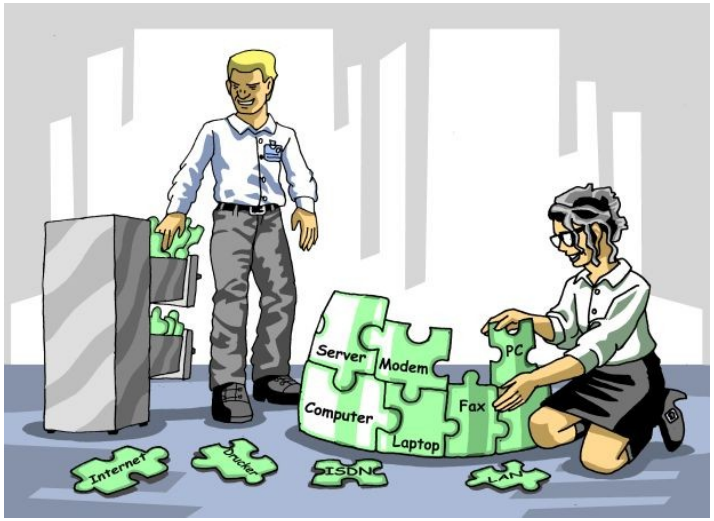
Zusätzliche Gefährdungen durch Consumerization

- Geräte sind nicht für professionellen Einsatz konzipiert
- Umsetzung der Sicherheitsleitlinien (Passwort, Patches, Datensicherung, etc.) ist bisweilen schwierig
- Zentrale Administration von privaten Geräten unerwünscht
- Zentrale Administration durch Vielzahl der Plattformen erschwert
- Ungeprüfte Apps im Netz der Institution
- Großes Problem Datenschutzkonformität: Fehlende Trennung zwischen dienstlicher und privater Nutzung

Maßnahmen für Informationssicherheit

„Wenn Sie denken, Technologie löst Ihre Probleme, verstehen Sie nicht die Technologie und Sie verstehen auch nicht Ihre Probleme.“ (Bruce Schneier)

IT-Grundschutz
Die Idee ...



- Typische Komponenten
- Typische Gefährdungen, Schwachstellen und Risiken
- Konkrete Umsetzungshinweise für das Sicherheitsmanagement
- Empfehlung geeigneter Bündel von Standard-Sicherheitsmaßnahmen
- Vorbildliche Lösungen aus der Praxis - „Best Practice“ - Ansätze

Ziel des IT-Grundschutzes

IT-Grundschutz verfolgt einen ganzheitlichen Ansatz. Infrastrukturelle, organisatorische, personelle und technische **Standard-Sicherheitsmaßnahmen** helfen, ein

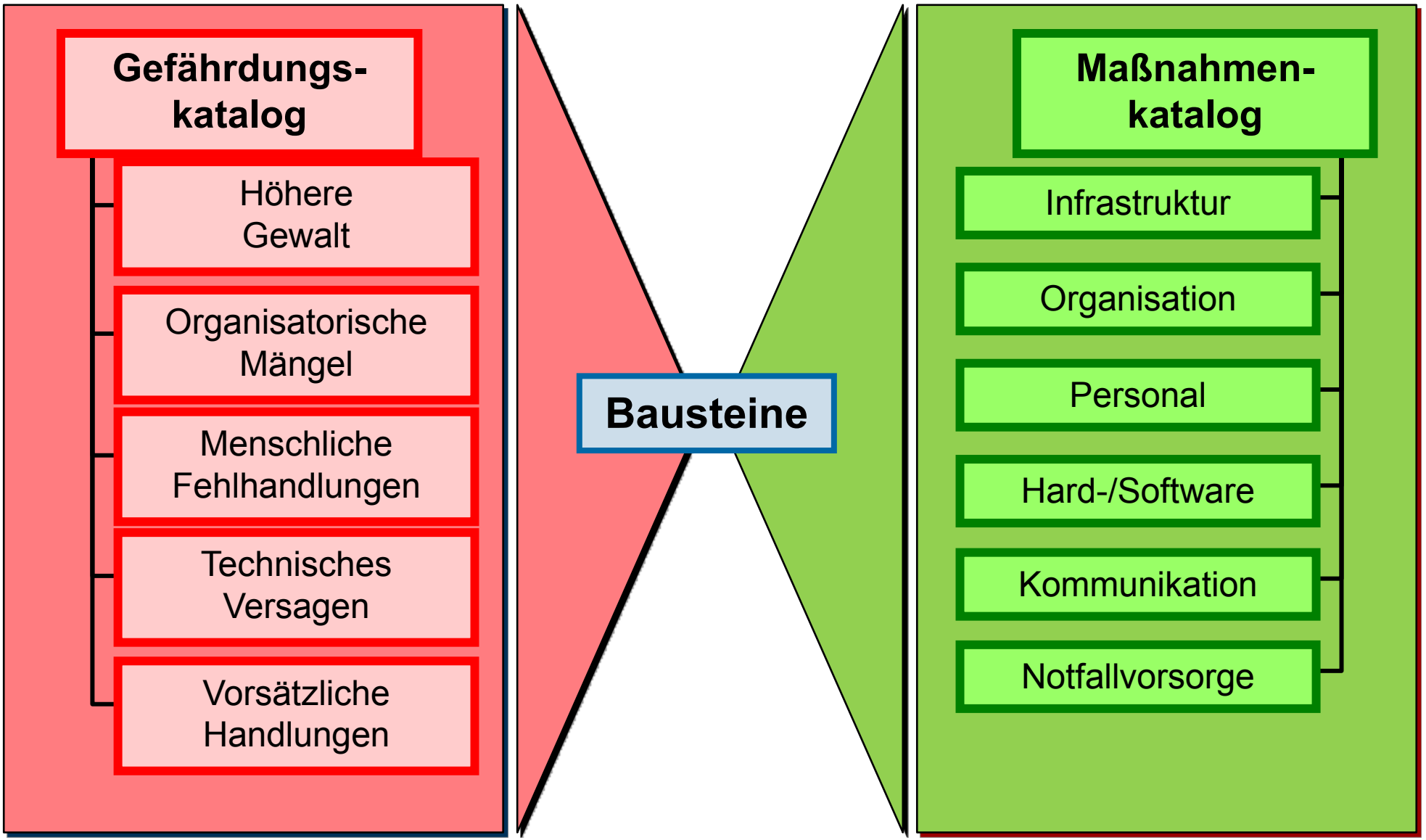
Standard-Sicherheitsniveau

aufzubauen, um geschäftsrelevante Informationen zu schützen.
An vielen Stellen werden bereits höherwertige Maßnahmen geliefert, die die Basis für sensiblere Bereiche sind.

IT-Grundschutz

BSI-Standards + **Loseblattsammlung**

Struktur der Bausteine



Bundesamt
für Sicherheit in der
Informationstechnik

Weil das länger dauert: IT-Grundschutz Überblickspapiere

Organisatorische Maßnahmen (1/2)

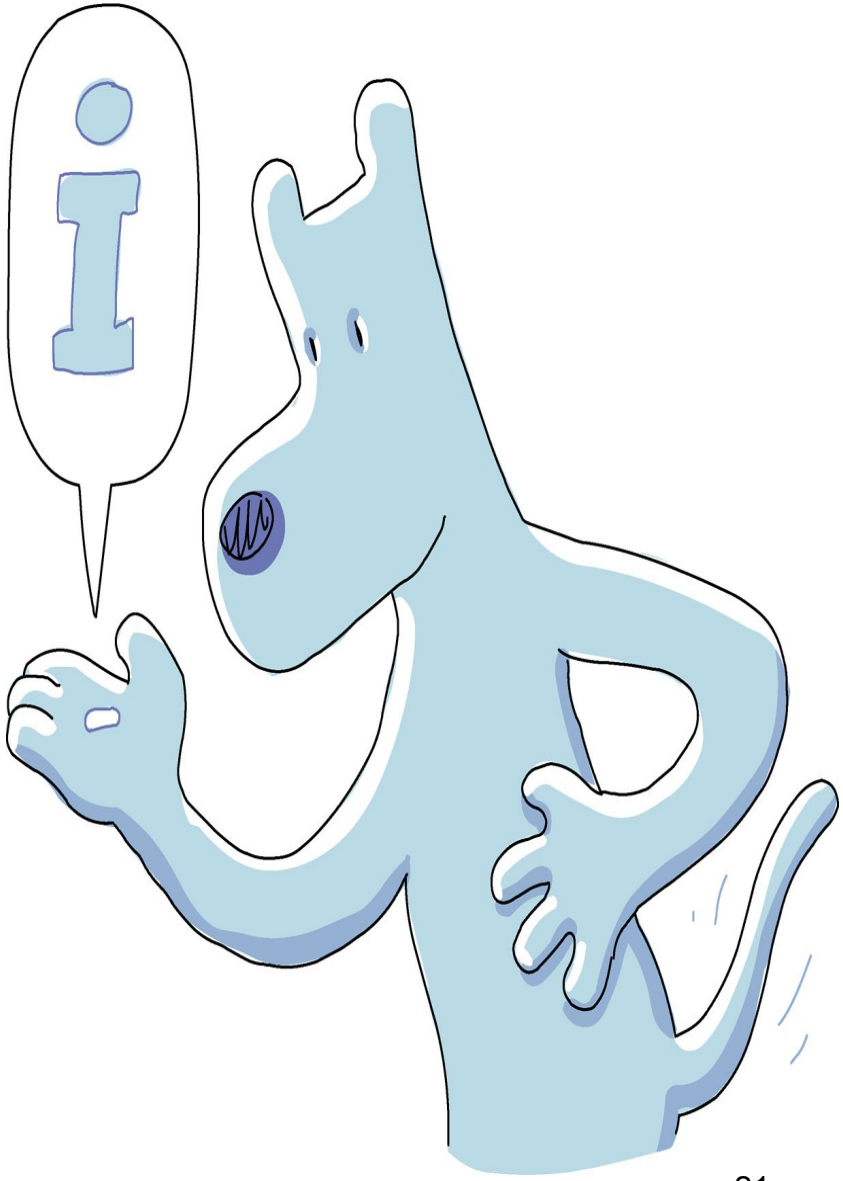
- Eingebettete Sicherheitsleitlinie für Smartphones
  - Was ist erlaubt, was nicht
  - Einsatz von privaten Apps klären; ggf. eigener App-Store
  - Verantwortung des Mitarbeiters und der Institution festlegen
  - Verfahren bei Ausfall und Verlust des Smartphones
  - Den gesamten Lebenszyklus (Planung, Beschaffung, Betrieb, Aussonderung, Notfallvorsorge) von Smartphones einbeziehen

Organisatorische Maßnahmen (2/2)

- Mitarbeiter schulen und sensibilisieren
  - Finanzieller Schaden durch Verlust/Diebstahl verdeutlichen
  - Sinn von Passwortrichtlinien verdeutlichen
  - Schadsoftware auf Smartphones
  - Rechtehungrige Apps
  - Sinn regelmäßiger Datensicherungen und Patches erläutern

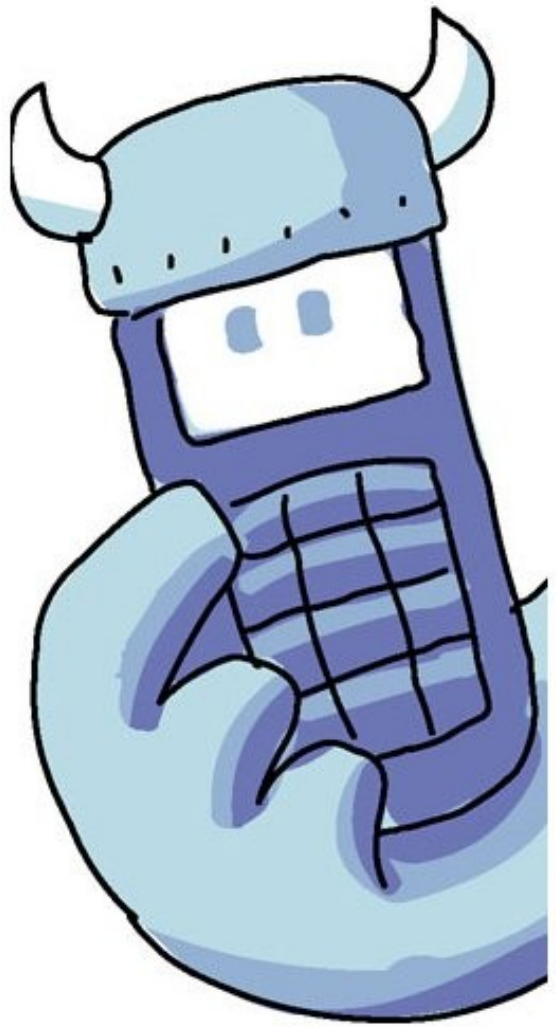
Technische Maßnahmen der Institution

- Zentrale Administration aller Smartphones
- Einhaltung der Sicherheitsleitlinie strikt prüfen
- Jailbreaking & Rooting detektieren
- Webverkehr durch Virenfilter leiten (zentral o. lokal)
- Datenschutz:
  - Smartphone als Thin-Client; alle Daten in der private Cloud
  - Virtualisierung → virtuelles privates und dienstliches Smartphone



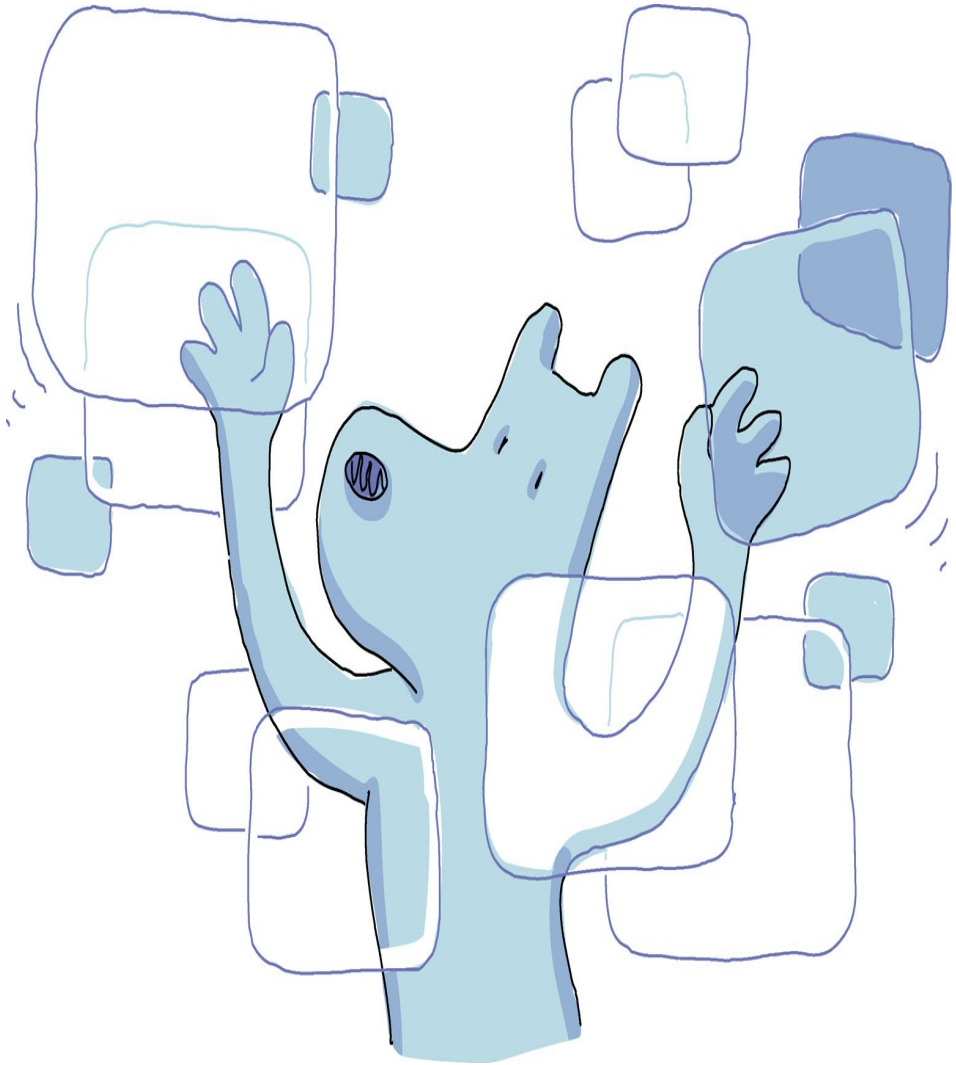
Maßnahmen am Smartphone

- Sichtschutzfolie für Smartphones
- Verschlüsselung aller Daten
- Umfassender Virenschutz
- Regelmäßige Datensicherung
- Regelmäßiges Patchen
- Fernlöschung und Lokalisierung
- Nur verschlüsselte Verbindung zum Netz der Institution
- Kein Jailbreaking oder Rooting
- Alle nicht benutzten Schnittstellen abschalten



Maßnahmen der Nutzer

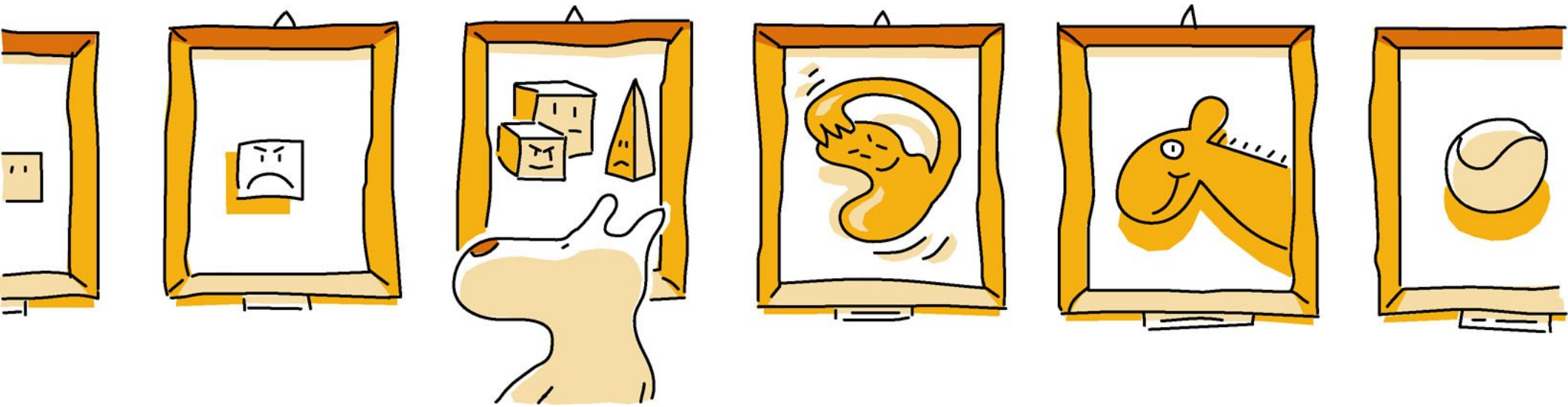
- Sicherheitsmaßnahmen nicht umgehen sondern umsetzen
- Virenschutz wie bei Laptop (E-Mail, Apps, Dateien, Surfen)
- Sparsamkeit: Diensten, Apps & Daten
- Gerät nicht aus der Hand geben oder liegen lassen
- Umsicht bei privaten Apps
- Vorsicht bei Web-Diensten



Fazit

- Smartphones sind ständig mit dem Internet verbundene Computer, aber nicht so sicher zu konfigurieren wie diese.
- Hauptgefährdungen sind Diebstahl, Datenverlust, Schadsoftware und fehlendes Problembewusstsein.
- Consumerization birgt weitergehende Gefährdungen.
- Technische Maßnahmen alleine greifen zu kurz
- Informationssicherheitsmanagement (ISM) mit Smartphones ist deutlich aufwendiger als bei PCs
- Sicherer Einsatz bedarf umfassendes ISM unter aktiver Beteiligung des Nutzers → IT-Grundschutz

Vielen Dank für die Aufmerksamkeit!
Fragen oder Anmerkungen?



Kontakt

Bundesamt für Sicherheit in der
Informationstechnik (BSI)

IT-Grundschutz
Godesberger Allee 195-198
53175 Bonn

Tel: +49 (0)22899-9582-5369
Fax: +49 (0)22899-9582-5405

grundschutz@bsi.bund.de
www.bsi.bund.de/grundschutz

IT-Grundschutz Gruppe im XING-Forum:
https://www.xing.com/net/itgrundschutz