Mobile Security

L. Aaron Kaplan

CERT.at

http://www.youtube.com/watch?v=Xs3SfNANtig

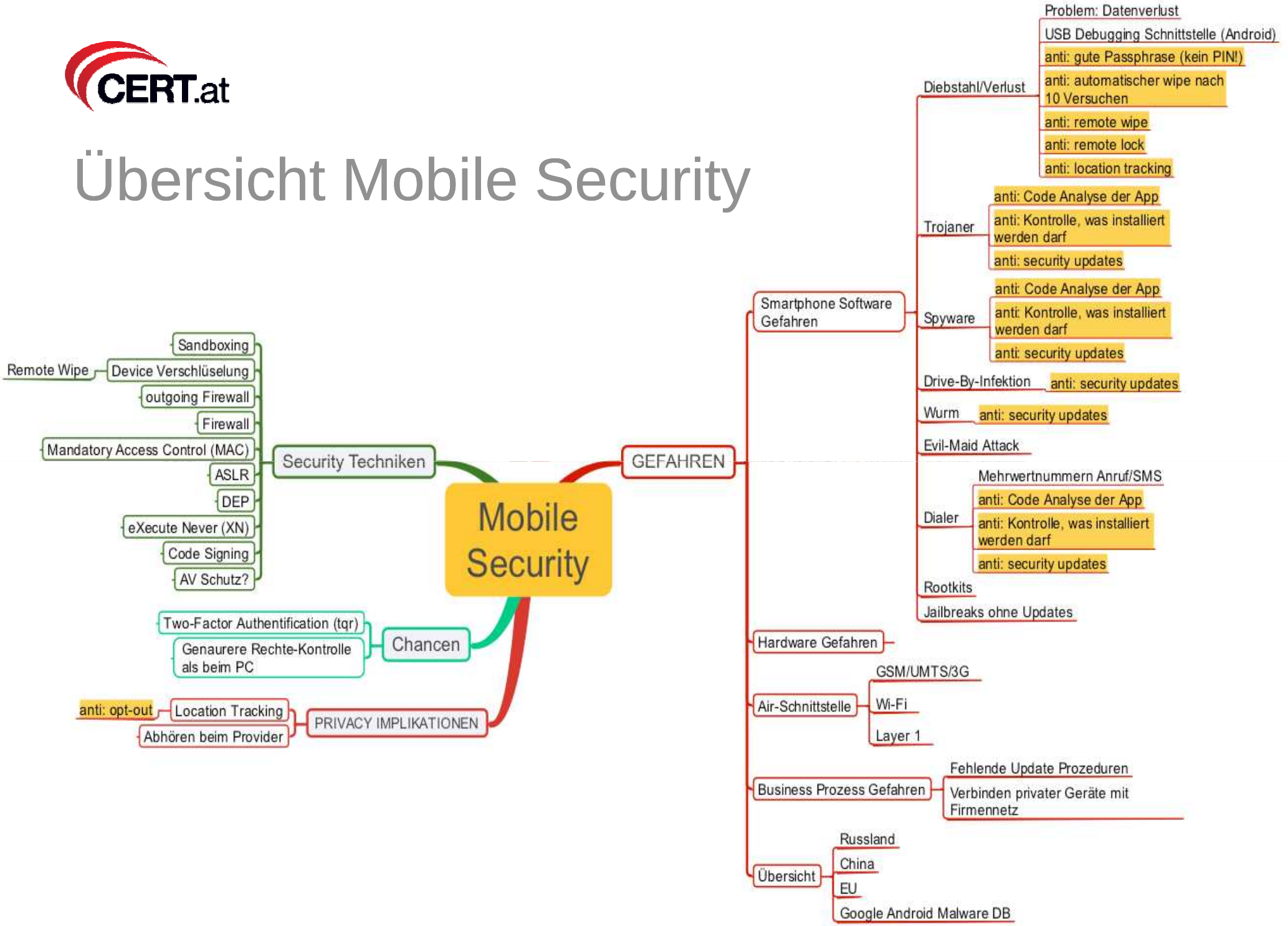
Die Geister die ich rief...

Überblick

- Übersicht Probleme
- Mobile Malware Varianten
- Infektionswege & Verbreitung
- Sicherheitstechniken von Smartphones
- Sicherheitsempfehlungen
- Smartphone als Securityhilfe?
- Air Interface
- Trends & Zusammenfassung

CERT.at

Übersicht Mobile Security

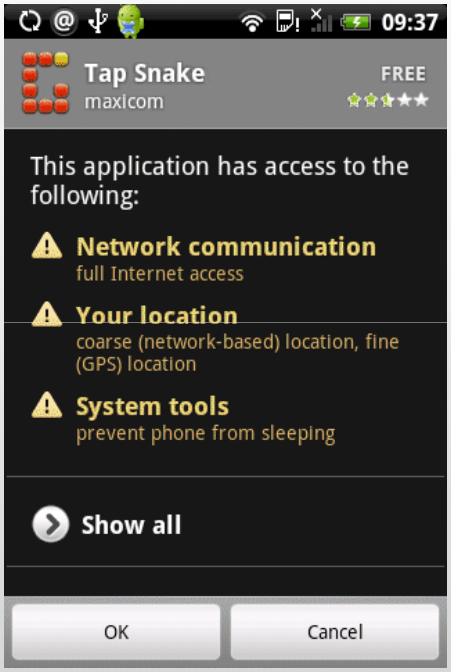


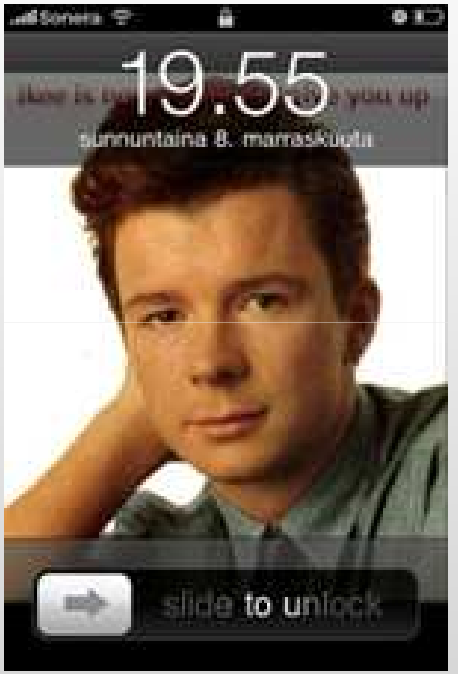
Mobile Malware Varianten

- Trojaner: „lustiges Spiel“ im Appstore
- Würmer: verbreitet sich selbständig
- Spyware: klaut Passwörter
- Ad-ware/Marketing-ware
- Fake Apps
- Drive-by-Infection („Dropper“): initialer Infektor
- Dialer / Mehrwert-SMS Versender

Beispiele erster Generation mobiler Malware

- iKee Wurm (iPhone)
- Tap Snake (Android)





Aktuelle mobiler Malware: Gingermaster (17.8.2011)

- Funktioniert auf Android 2.3 (Gingerbread)
- Root Exploit
- Trojaner, kommt mit existierenden Apps mit (zB Model Pictures)
- Installiert Service
- Verbindet sich zu C&C Server
- Wartet auf Commandos

http://www.cs.ncsu.edu/faculty/jiang/GingerMaster/

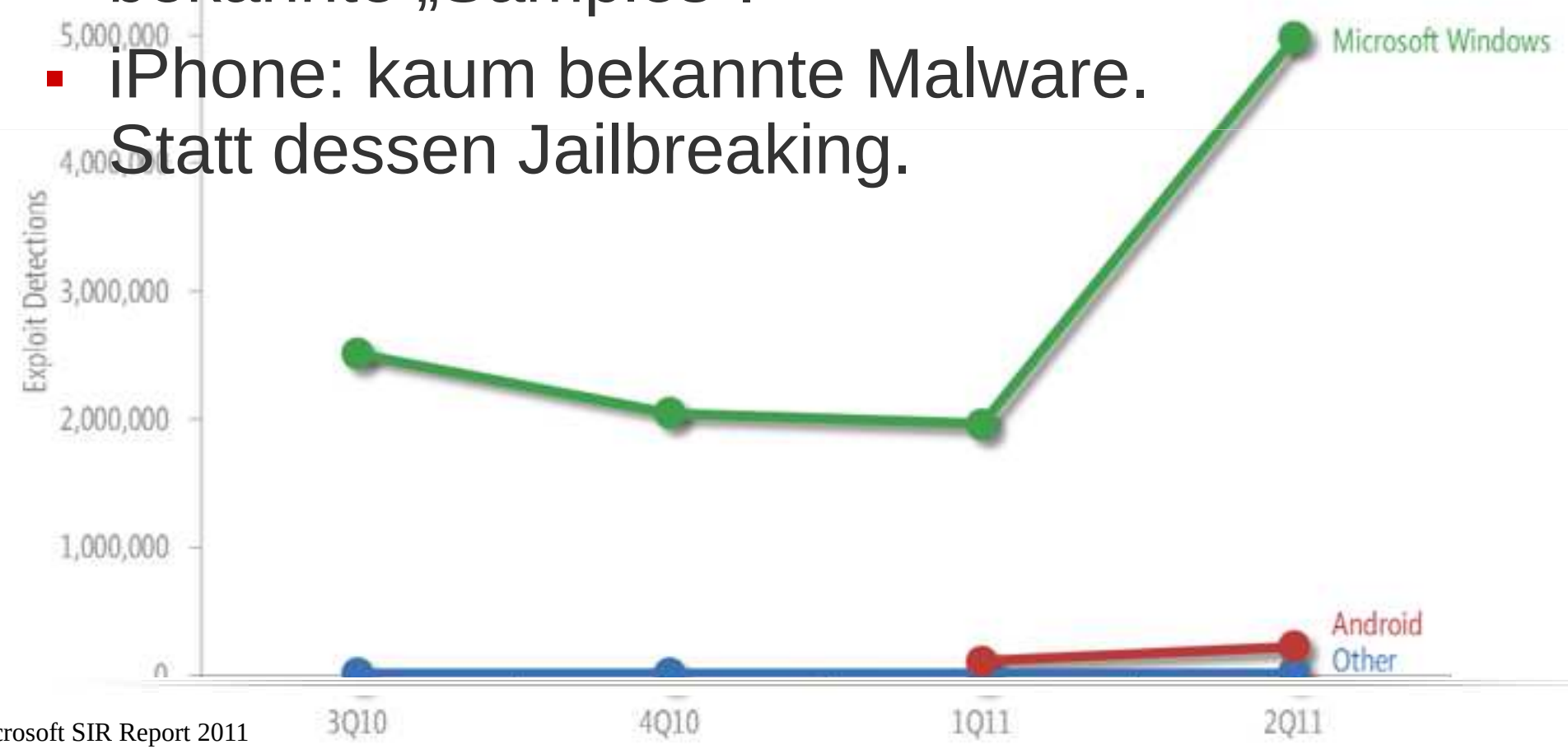
Infektion & Verbreitung

- Android: Appstore (Trojaner)
- iPhone: Appstore (Spyware, Trojaner)
- Alternative Downloads (Android)
- Symbian Malware: vor allem China (2600 Trojaner 1H 2011 [1])
- Russland: vor allem Dialer/Mehrwert-SMS

- [1] Quelle: http://english.peopledaily.com.cn/90780/7594669.html

Infektion & Verbreitung

- Android: Malware stark im Kommen. Mind. 80 bekannte „Samples“.
- iPhone: kaum bekannte Malware. Statt dessen Jailbreaking.



Microsoft SIR Report 2011

Sicherheitstechniken bei Smartphones

- Android:
  - Sandboxing++
  - Mandatory Access Control++, Rechtesystem
  - ASLR
- iPhone
  - eXecute Never (XN)++
  - Code Signing++
  - ASLR
  - Strikter Appstore
  - Verschlüsseltes Dateisystem

Schwachstellen

- Android:
  - Kein verschlüsseltes Dateisystem (→ Verlust)
  - Schwache checks im Appstore
  - Code Signing fehlt
- iPhone
  - War *doch* immer Jail-breakable
  - Verschlüsselung nicht ausreichend, bzw. PIN Code zu kurz
  - Verschlüsselung nicht konsequent
  - Fehlende outgoing Firewall
  - Rechtesystem nicht so raffiniert

Sicherheitsempfehlungen

1. Den Verlust vorausplanen: 3 x remote Lösung: remote wipe, remote lock, remote locating
2. Internet nur via VPN und über die Firma (dort dann firwallen, etc)
3. Strikte Richtlinien, was installiert werden darf
4. Trennung privates Smartphone vs. Firma
5. Absolut zeitnahe Systemupdates
6. > 6 stelliges Passwort (nicht nur Ziffern)
7. Zentrale Administration der Firmen-Smartphones

Verlust

- Android: SD Karten rausnehmen und kopieren → alle Daten
- iPhone: DFU Mode → neue Firmware einspielen → ssh server installieren → reinverbinden → Daten kopieren. Daten entschlüsseln

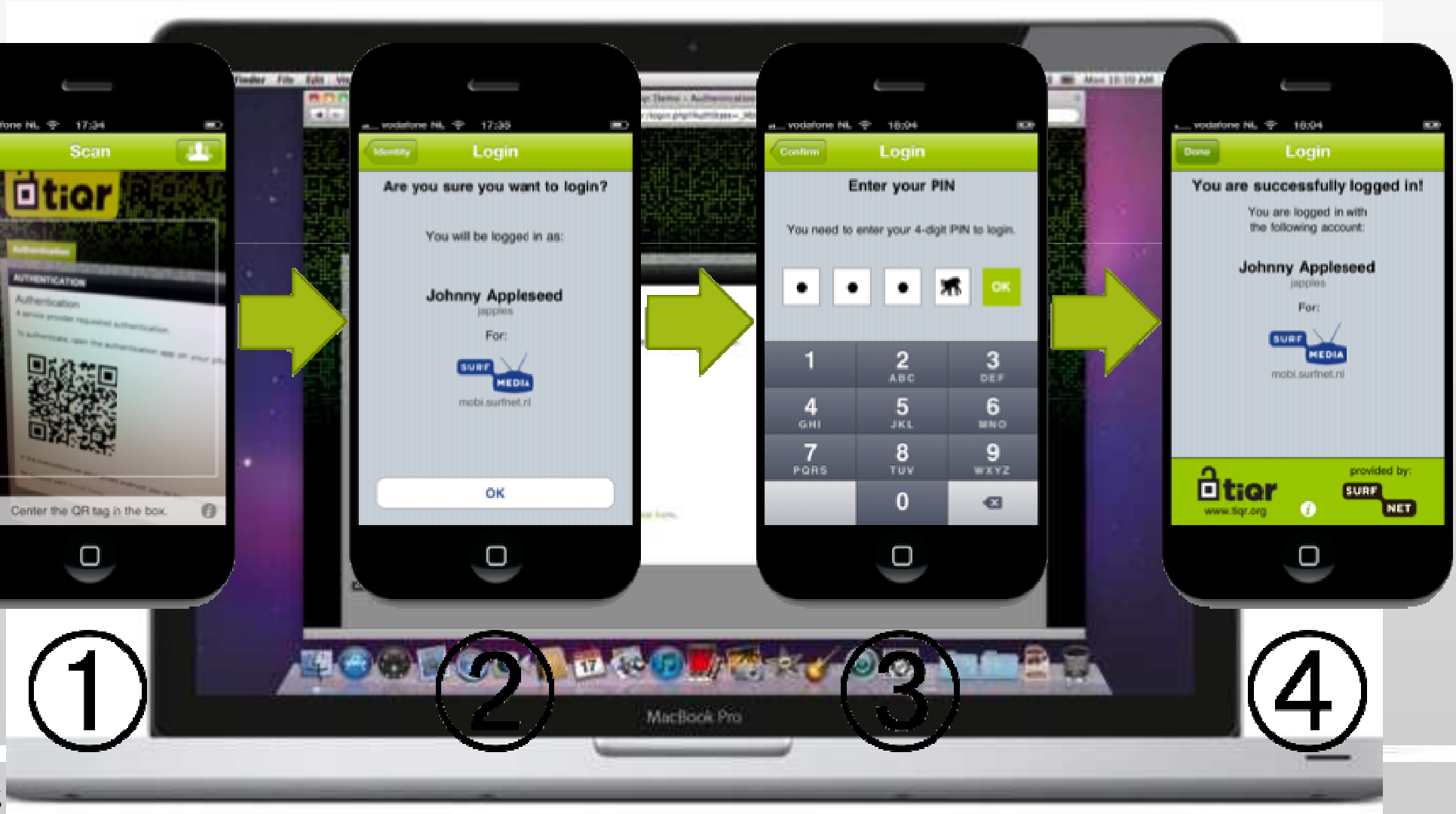
- **Nur ein remote wipe hilft (soferne die SIM Karte noch drinnen ist)**

Smartphone als Security Hilfe?

- Problem: Passwörter als Authentifizierung sind veraltet
- Idee: 2-Faktor Authentifizierung
- Google Authenticator
- QR-Codes via Smartphone

Google.com, Wikipedia „QR Code“

Smartphone als Security Hilfe?



Air Interface

- I
- F
  C
- C
- A
- U
  C
- E
- F
  (

Trends und Zusammenfassung

- Mobile Malware stark im kommen
- Bei weitem noch nicht so verbreitet wie Windows Malware
- Smartphone perfekte Zielscheibe
- Updaten, Updaten, Updaten
- Keine Panik, Mitarbeiter sensibilisieren und...

Jetzt vorplanen!

Danke!