Datenmissbrauch und Überwachungsstaat

V 1.0 20180815 - Jochim Selzer js@crypto.koeln - 6AA4 89F9 9E1F DCBA FF00 F291 8A97 4A5C 0970 E0CF

Von welcher Gefahr reden wir?

- Kriminelle (greifen direkt an)
- Ermittlungsbehörden (überwachen)
- Wirtschaft

Gewöhnliche Kriminelle

- Betreiben Phishing
- Installieren Trojanische Pferde
- Greifen Server an und saugen Nutzerdatenbanken ab
- Suchen Sicherheitslücken und verkaufen sie

Ermittlungsbehörden

- Greifen Daten an Knotenpunkten (DENIC) ab
- Werten Metadaten aus (Vorratsdatenspeicherung)
- Installieren Trojanische Pferde (Quellen-TKÜ)
- Installieren Trojanische Pferde (Onlinedurchsuchung)
- Kaufen Sicherheitslücken auf dem Schwarzmarkt

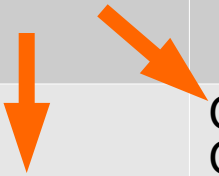
Privatwirtschaft

- Installiert Apps
- Wertet Metadaten aus
- Die Nutzer liefern die Daten freiwillig (unter anderem Metadaten)

Allgemein oder gezielt?

- Allgemein
  - Man nimmt, was man bekommt
  - Geringe Trefferquote, Erfolg durch Masse
  - Abwehr relativ leicht
- Gezielt
  - Genaues Wissen über das Ziel
  - Hoher Aufwand
  - Abwehr schwer bis unmöglich

	Kriminelle	Staat	Wirtschaft
allgemein	Phishing Scam Verseuchte Mailanhänge Drive-By-Downloads Passwortlisten Trojanische Pferde Viren Fake-Hotspots	Vorratsdatenspeicherung	Big-Data-Analysen
spezifisch	Social Engineering Belauschen von WLANs Auswerten von Social-Media-Profilen	Quellen-TKÜ Online-Durchsuchung	Apps Nutzerprofile



Klassische kriminelle Angriffe

- Schwache oder mehrfach verwendete Passworte
- Phishing
- Drive-by-Downloads
- Leichtfertig installierte Software

Was geht?

- Mobilfunkanbieter haben unsere Positionsdaten
- Google erfasst Suchbegriffe und Positionsdaten
- Facebook erfasst, wann wir reden, mit wem wir reden, worüber wir reden und wie wir reden
- Schufa-Scoring erfasst nicht nur die Zahlungsmoral, sondern auch scheinbar sinnlose Daten wie die Wohngegend
- Big-Data-Analysen finden Zusammenhänge in scheinbar sinnlosen Datenbergen
- Es gibt faktisch keine größeren anonymen Finanztransaktionen mehr

Was geht?

- Kommunikationsanbieter (Internet, Telefon) wissen, wann wir wo mit wem wie lange reden.
- Gratis-Apps liefern in der Summe ein Komplettprofil
- Payback liefert Kundenprofile
- Gesundheits-Apps liefern Patientenprofile
- PNR liefern detaillierte Fluggastdatenprofile, die teilweise über Jahrzehnte gespeichert werden.

Was geht nicht?

- Instagram und Facebook können zwar heimlich auf das Mikrofon zugreifen, aber es gibt keine belastbare Untersuchung, dass dies auch wirklich geschieht – im Gegenteil.
- Der auf einigen Smartphone-Akkus verbaute NFC-Chip ist kein verstecktes Mikrofon.

Polizeigesetz NRW

- Entwurf vom 11.4.
- Aus dem Begründungstext: „Einführung einer strafbewehrten präventiv-polizeilichen Rechtsgrundlage, um gegen **mutmaßliche Gefährder** orts- und gebietsbezogene Aufenthaltsanordnungen oder Kontaktverbotezu erlassen.“

Polizeigesetz NRW

- Entwurf vom 11.4.
- „Drohende Gefahr“ (§ 8)

„(4) Eine drohende Gefahr liegt vor, wenn im Einzelfall hinsichtlich einer Person **bestimmte Tatsachen** die Annahme rechtfertigen, dass die Person innerhalb eines **absehbaren Zeitraums** auf eine **zumindest ihrer Art nach konkretisierte Weise** eine Straftat von **erheblicher Bedeutung** begehen wird.“

Polizeigesetz NRW

Videoüberwachung des öffentlichen Raums (§ 15 a) wird ausgeweitet auf Orte bei denen „2. tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Straftaten von erheblicher Bedeutung **verabredet**, **vorbereitet** oder begangen werden.“

Polizeigesetz NRW

- Quellen-TKÜ (§ 20c)
  - Beim Verdächtigen selbst
  - Bei Mittelsleuten oder bei einer Person „bei der bestimmte Tatsachen die Annahme rechtfertigen, dass eine Person nach Nummer 1 deren Telekommunikationsanschluss oder Endgerät benutzen wird“
  - Zulässig, wenn „durch technische Maßnahmen sichergestellt ist, dass ausschließlich laufende Telekommunikation überwacht und aufgezeichnet wird“

Polizeigesetz NRW § 20c

- (3) Bei Maßnahmen nach Absatz 2 ist sicherzustellen, dass
  1. an dem informationstechnischen System nur Veränderungen vorgenommen werden, die für die Datenerhebung unerlässlich sind und
  2. die vorgenommenen Veränderungen bei Beendigung der Maßnahme, soweit technisch möglich, automatisiert rückgängig gemacht werden.
- Richtervorbehalt
- Keine **Aufzeichnung** des privaten Lebensbereichs

Polizeigesetz NRW

- Elektronische Fußfessel (§ 34 c)
- Unterbindungsgewahrsam bis zu einem Monat, zur Identitätsfeststellung bis zu sieben Tage (§ 38), allerdings Entscheidung eines Haftrichters spätestens am Ende des Tages nach Ergreifung
- Verdachtsunabhängige Kontrollen in bestimmten Gebieten bis zu 28 Tage mit Möglichkeit, um weitere 28 Tage zu verlängern (§ 12a „strategische Fahndung“)
- Neue Waffen „Distanzelektroimpulsgeräte“ (§ 58)

PolG NRW: Weitere Informationen

- Pro und Contra in der WZ
- Tobias Morsches: Quellen-TKÜ: Wenn Behörden in Computer einbrechen
- Christian Mertens: Das neue Polizeigesetz NRW

Was tun?

- Gute Passworte
- Festplatte verschlüsseln
- Backups
- Vorsicht bei unbekannter Software
- Vorsicht in offenen WLANs
- Weg von den großen Datensammlern, hin zu Unternehmen mit anderem Geschäftsmodell (z.B. Posteo als Mailanbieter)