Münchner Kreis: Arbeitskreis Security
Abstract zur Frage: Gesellschaftliche Diskussion anstoßen: Wo akzeptieren wir welche Überwachung? Oder: Wo müssen wir Daten wie schützen?

Herausforderung

Durch die Digitalisierung werden immer mehr Bereiche und Systeme, wie z.B. kritische Infrastrukturen, Straßenverkehr (autonomes Fahren), Smart Health, Industrieanlagen (Industrie 4.0) und Smart Home, zu IT-Systemen. Diese IT-Systeme sind dadurch gekennzeichnet dass sie eine Unmenge von Daten erfassen, austauschen und speichern, die mit der großen Rechenleistung von Cloud Systemen auch schnell (oft quasi in Echtzeit) und umfassend ausgewertet werden können. Dies eröffnet Chancen und Risiken, die gegeneinander abgewägt werden müssen:

- **Individuen** müssen entscheiden, ob sie neue Services nutzen wollen, oder ob sie den Verlust an Privatsphäre höher einstufen.
- **Produkthersteller** brauchen die Digitalisierung für neue Geschäfte müssen sich aber gegen Know-How Abfluss und Haftung bei Datenschutzverletzungen schützen.
- **Betreiber** kritischer Infrastrukturen können diese durch Digitalisierung optimieren (z.B. den Energieverbrauch oder die Betriebskosten reduzieren) müssen aber auch dafür sorgen, dass durch die verteilten Daten und Sensoren keine Betriebsrisiken entstehen.
- Der **Staat** muss den Schutz Seiner Bürger (Privatheit aber auch Sicherheit) gegenüber legitimen heutigen und zukünftigen Geschäftsinteressen, die durch Datenverarbeitung entstehen, abwägen.

Die neuen Möglichkeiten der Datenanalyse könnten so mächtig sein, dass es praktisch keinen Schutz gegen Informationsgewinnung mehr gibt. Dann stellt sich die Frage, ob IT-Sicherheit vielmehr auf die Verhinderung von Datenmanipulation reduziert werden kann. Dann stellt sich auch die Frage, welche solcher Methoden wir aus ethischen und gesellschaftspolitischen Gründen verbieten wollen.

Status Quo

Anhand von einigen Beispielen sollen die Themen und Fragestellungen für eine Fachkonferenz und ggf. einen politischen Abend motiviert werden.

Beispiel 1 - Autonomes Fahren. Verkehrsüberwachung, und die damit verbundenen Eingriffe in die Privatsphäre, ist akzeptiert und sogar gesellschaftlich gefordert als. Systeme wie E-Call oder das zukünftige autonome Fahren können jedoch eine weit umfassendere Überwachung ermöglichen. So ist folgendes Szenario vorstellbar: *In Zukunft kann jederzeit die Geschwindigkeit eines Fahrzeuges ermittelt, eine Überschreitung in Echtzeit festgestellt und eine automatische Abbuchung der Strafzahlung angestoßen werden. Bei starker Übertretung wird der elektronische Führerschein, der auf dem Handy gespeichert ist, automatisch eingezogen und das Fahrzeug automatisch an einem sicheren Ort abgestellt. Im Fahrzeug wird überwacht, wer das Fahrzeug fährt, um sicherzustellen, dass nur Lenker mit gültiger Fahrerlaubnis steuern, bzw. die Verantwortung für das autonom fahrende Auto tragen.*
Es sei hier anzumerken, dass dieses Szenario nicht zwangsläufig ist. Zum einen sind vollautomatisierte Entscheidungen (von Erkennung bis rechtskräftiger Bestrafung) rechtlich diskutiert worden und als nicht wünschenswert eingestuft worden. Die Einführung solcher Systeme erfordert also eine Neu-Bewertung im Rechtssystem. Weiterhin muss die technische Implementierung die rechtlichen Schranken auch durchsetzen helfen. Z.B. dadurch, dass das System Fahrzeuge nur bei

Regelverstößen deanonymisieren kann, da ansonsten Missbrauch (auch durch kriminelle) zu erwarten ist.

Beispiel 2- Exportkontrollen für Krypto-Produkte. Die aktuelle Diskussion über die Entsperrung des Iphones in USA zeigt den seit den 90er Jahren existierenden Konflikt zum Einsatz von Kryptographie. Macht es in einem internationalen Markt noch Sinn, Kryptographie als Exportkontrollierte Wahre zu definieren. Wie stark sind dadurch die Einschränkungen für den Einsatz insbesondere für KMU, die den Weltmarkt erschließen wollen? Warum können Firmen ihre Mitarbeiter nicht mit ihrem Firmen-Handy und -Laptop ins Ausland schicken? Schwächt die Forderung von Hintertüren bzw. der aktive Einbau von Hintertüren in kryptographische Standards, wie z.B. beim NIST Zufallszahlengenerator auf Basis elliptischer Kurven, nicht das ganze Internet und jedes digitalisierte Produkt, denn Hintertüren werden immer irgendwann entdeckt. Inwieweit behindert die aktuelle Einstellung der Behörden Hintertüren und Schwachstellen in Systemen lieber zu verheimlichen als an einer weltweit koordinierten Behebung zu arbeiten die Einführung neuer Technologien, wie z.B. Industrie4.0. Weiterhin haben die Exportkontrollen in den USA nachweislich die US IT-Sicherheitsindustrie wirtschaftlich geschädigt. In welchem Maße kann das auch europäische und deutsche Unternehmen treffen?

Jahrzehnte lange Beobachtungen aus dem Payment Bereich zeigen, dass es extrem schwierig ist, verteilte kritische Infrastrukturen gegen Missbrauch zu schützen. Kreditkartendaten werden wie billige Massenwahre im Internet gehandelt. PINs von Zugangskarten werden oft an Terminals gestohlen. Phishing und andere Angriffe auf die verteilten Eingabeterminals greifen die Transaktionen an, was zu einem starken Misstrauen gegen Homebanking führt. Andererseits sind Verbraucher und Betreiber aber auch nicht bereit, stärker in die Sicherheit zu investieren. So sind beispielsweise die leicht kopierbaren Magnetstreifen auch heute noch im Einsatz. Ähnliche Diskussion gibt es bei der Einführung des Smart Meters in Deutschland. Hier wurde eine Komponente einer sicheren Infrastruktur national standardisiert gegen großen Widerstand aus der Industrie und bei den Verbrauchern. Was muss man tun, um die Akzeptanz von IT-Sicherheitskosten zu erhöhen?

Heutzutage bilden Router das Tor zum Internet. Kunden beziehen von wenigen Herstellern diese Komponenten. Während die Netzwerkbetreiber davon betroffen sind, dass Geheimdienste die Geräte modifizieren, um abhören zu können, leiden Endkunden daran, dass die Geräte Schwachstellen haben. Diese meist SW-Schwachstellen in standardisierten Betriebssystemen, wie z.B. Linux werden zwar in der Anfangszeit noch gefixt, aber sobald die nächste Gerätegeneration am Markt ist, gibt es keine Wartung mehr. Das führt dazu, dass eine Menge Geräte mit alten Betriebssystemen am Markt ist, die eine Menge öffentlich bekannter Schwachstellen haben. Wie bringt man Produkthersteller dazu eine Wartung der Software von vernetzten Produkten über die gesamte Produktlebenszeit zu leisten. Wie schauen neue Geschäftsmodelle dafür aus? In wie weit betrifft dies auch die Rechte des Konsumenten/ Kunden (geplante Obsoleszenz, Einstellen der nötigen Netzinfrastruktur, wem „gehört“ das Gerät)?

Ziel / Nicht-Ziel

1. Welche Technologien können die Sicherheit in cyber-physikalischen Systemen erhöhen? Was ist einsatzbereit, was gibt es (und muss noch implementiert werden), was muss noch erforscht werden?

2. Möglichkeiten der Datenanalyse: Kann man Privatsphäre überhaupt noch schützen unter Berücksichtigung der Menge der erfassten Daten und der Data Analytics Möglichkeiten (Machine Learning, Deap Learning, Korrelationsanalysen, IBM Watson, Google, SAP Hana, …).
3. Was sind die Chancen, die sich durch die Verfügbarkeit der vielen Daten und Analysemöglichkeiten ergeben?
4. Regulierung: Wie und von wem sollten solche Technologien reguliert werden? In wie weit ist der Gesetzgeber verpflichtet den Bürger vor sich selbst zu schützen? Letzteres im Besonderen, wenn die Konsequenzen einer Technologie vom einzelnen nicht abschätzbar sein können. Grenzen: Welche Rechtsräume brauchen und akzeptieren wir?
5. Kryptographie versus legale Abhörmöglichkeiten oder wie können wir Strafverfolger auf die Herausforderungen die durch sichere ICT entstehen vorbereiten?
6. Auswertemöglichkeiten von Daten: Wo sind hier die Grenzen der Privatsphäre? (Erweiterung der Diskussion weg vom Abhören von Kommunikation)

Nicht Ziel: Generische Debatte über Datenschutz des Privatbürgers.

Umsetzung

Konferenz mit folgenden Themen:

- Themenblock Neue Anwendungen und technische Möglichkeiten von Datenanalyse
    - Vertreter von IBM Watson oder Google
    - Wissenschaftlicher Vertreter
    - Fraunhofer Industrial Data Space Initiative als Infrastruktur für den sicheren Datenhandel
- Themenblock Schutz des Individuums
    - Wie kann man Nutzer vor Datenmissbrauch schützen, bzw. ihnen die Risiken überhaupt bewusst machen. Beispiel könnte Facebook oder WhatsApp sein.
    - Welche Überwachung akzeptieren wir, z.B. diskutiert an der Verkehrsüberwachung.
- Themenblock staatliche Interessen
    - Schutz von Infrastruktur und kritischer Dienste
    - Abhörmöglichkeiten und Zivilschutz versus sichere Kryptographie
      Vertreter der ENISA (siehe Positionspapier); Vertreter des BKA, LKA oder Innenministeriums
    - Exportkontrolle die Kryptographie als „Waffe“ einstuft versus Schädigung der Industrie
        - Aufwände eines Unternehmens für die Exportkontrolle von IT-Sicherheitslösungen
        - Wirtschaftliche Risiken, z.B. IT Sicherheit, Exportkontrolle und Kryptographie aus Sicht eines KMU als Hindernis den Weltmarkt zu adressieren
- Themenblock Betreiber kritischer Infrastrukturen
    - Warum schafft es die Finanzbranche nicht, die Kundendaten zu schützen?
    - Welche Auswirkungen haben solche Datenschutzprobleme auf zukünftige Szenarien, wie z.B. das autonome Fahren, Smart Home Anwendungen oder Smart Health?
    - Wie kommen wir zu einer SW-Wartung über den gesamten Lebenszyklus aller vernetzen Produkte?