Internet Security Europe

Gedanken Eines ITC – Insiders

Spätestens seitdem Edward Snowden der Öffentlichkeit ausführliche Informationen zur Arbeit der US-Sicherheitsbehörde NSA zugänglich gemacht hat, wird weltweit nicht mehr nur in Spezialistenkreisen über die Frage der Sicherheit von Daten im Allgemeinen und im Internet im Speziellen diskutiert.

Das Thema Datensicherheit ist mittlerweile in aller Munde.

Grob kann man die Diskutierenden in drei Kategorien einteilen**:**

- Diejenigen, denen die sichere Nutzung der elektronischen Medien am Herzen liegen.
- Diejenigen, die elektronische Medien zu ihrem eigenen Vorteil missbrauchen.
- Und schlussendlich diejenigen, die das „Hype"-Thema Datensicherheit lediglich zur eigenen Darstellung, bzw. als Sprungbrett, nutzen - ansonsten jedoch keinen brauchbaren Beitrag leisten.

Die letzte Gruppe wird erst dann relevant, wenn sie politischen und/oder rechtlichen Einfluss nimmt und aufgrund geringer Fachkenntnis oder fehlender Weitsicht zu Ergebnissen resp. Entscheidungen kommt, die dem Ziel Datensicherheit entgegenstehen.

Spricht man von Sicherheit, speziell von *Daten*sicherheit, so muss man sich vor Augen führen, dass dies ein äußerst komplexes Thema ist, mit dem sich Techniker, Informatiker, Analysten, Systemarchitekten oder Kryptographen auch Pädagogen, Verhaltenspsychologen, Zukunftsforscher und viele, viele mehr beschäftigen, die alle ihren Beitrag leisten, um eine größtmögliche

Sicherheit im Umgang mit den elektronischen Medien zu erreichen.

All dieses Wissen und Können ist auch notwendig, um die Komplexität rund um „die Sicherheit“ überhaupt zu erfassen, davon ausgehend, geeignete Technologien zu entwickeln, Nutzungstechniken abzuleiten und das richtige Userverhalten in dem technikgeprägten Umfeld zu lehren.

Selbst unterstellt, es gäbe den sicheren Computer, den sicheren Server oder „das“ sichere Netz, die schwächste Stelle, nämlich der Mensch, ist unberechenbar, und macht Fehler.

Da es aber nun mal keine absolut sicheren Computer gibt, oder sichere Server, oder „das“ sichere Netz, potenzieren sich die möglichen Schwachstellen durch die schier unermesslich großen Anzahl der beteiligten technischen und menschlichen Fehlerquellen, die wiederum von skrupellosen Kriminellen oder auch von offiziellen Stellen - natürlich in hehrer Absicht - ausgenutzt werden.

Ich möchte also keinesfalls bewerten, ob der Zweck die Mittel heiligt, oder nicht, wenn es um Terrorismus und das Leben Unschuldiger geht.

Sicherheit hat neben der rein technischen, auch politisch-kulturelle Aspekte. Die Unterschiede resultieren unter anderen aus den verschiedenen Rechtssystemen.

In Deutschland ist die Privatsphäre im Grundgesetz verbrieft, Datenschutzrecht und Telekommunikationsgesetz schützen sie. Während beispielsweise in den USA Internet-Unternehmen wie Google oder Facebook Milliarden dadurch verdienen, dass viele Daten gesammelt, ausgewertet und kommerziell verwertet werden.

Um also eine gemeinsame Basis zu erhalten, ist es notwendig, ein allerseits anerkanntes Regelwerk zu entwickeln, welches das Leben in der digitalen Welt ordnet.

Was benötigt wird, ist eine Angleichung der Spielregeln ohne Schlupflöcher, da sonst Konflikte vorprogrammiert sind, und ein gemeinsames Vorgehen gegen Verstöße so gut wie ausgeschlossen ist.

Die Vielfalt der Probleme lässt also auf die Frage „gibt es ein sicheres Internet?“ als Antwort nur ein „Nein“ zu.

Sicherheit hat viele Komponenten, und hier zeigt sich, dass nicht nur das schwächste Glied der Kette ausschlaggebend ist, sondern darüber hinaus die „Atmosphäre“ um diese “Internet-Kette“ gravierenden Einfluss auf die trügerische Stabilität (Sicherheit), hat.

Arne Petrowski, Bonn, 16.1.2014

High Level ITC / TC - Industries (Telekom)
EoE - Zeitzeuge und Essayist seit Juni 1998