Kommunikation und Privatsphäre

Eintrag ins Pflichtenheft von Politik und ITK - Wirtschaft

von Arne Petrowski

Kommunikation und Privatsphäre, klingt das nicht wie „das staubtrockene Wasser“ oder „die brütend kalte Hitze“? Lässt sich Kommunikation mit der Privatsphäre überhaupt vereinbaren? Schließlich sind mindestens zwei Parteien bei einer Kommunikation beteiligt! Gut – zwei Parteien, besser zwei Personen, können vielleicht noch eine Intimsphäre bewahren. Doch was ist mit drei oder mehr beteiligten Parteien? Lässt sich da noch von Privatsphäre sprechen?

Weiter: Was unterliegt der Privatsphäre? Ausschließlich das, was ich persönlich bereit bin, von mir preis zu geben? Was ist mit den Informationen, die in Teilen oder Gänze „zwangsveröffentlicht“ sind, wie z. B. mein Name, meine Anschrift, etc.? Hier gelten Regeln, die der „Gemeinschaftsphäre“ dienen, wie z.B. Meldepflicht, Steuerpflicht, u.v.m.! Oder ist dies eine andere Form der Privatsphäre? Eine Privatsphäre zweiter oder dritter Klasse, auf die ich „naturgemäß“ nur bedingt Einfluss habe?

Wer definiert „Privatsphäre“, und welche Definition ist schlussendlich die gültige? Und hält sich Jeder an die sich aus dieser Definition resultierenden Grenzen, Rücksichtsnahmen und Konsequenzen?

Zumindest auf die letzte Frage gibt es eine eindeutige Antwort: Nein, es hält sich nicht Jeder daran! Schließlich leben wir nicht im Paradies, sondern in einer unvollkommenen und sündhaften Welt, in der es in jeder Gesellschaft und in jeder Gesellschaftsschicht neben dem „Guten“ auch das „Böse“ gibt

Die vehement kontrovers geführte Diskussion zu Datensicherheit und Datenschutz lässt, ungeachtet der Umsetzung und des Umfangs, zumindest ein Resümee zu:

Datenschutz ist notwendig – so strikt wie möglich und so transparent wie nötig.

Ich möchte gar nicht auf die einzelnen Argumente der Befürworter oder der Gegner von Überwachungsmaßnahmen im Kommunikationsumfeld eingehen. Tatsache ist, dass ein Schutz vor Missbrauch jeglicher Art immer Hand in Hand mit mehr oder minder intensiven Einschränkungen für diejenigen, die den Schutz genießen, bedeutet. Dies liegt (leider) in der Natur der Sache und gilt ebenso für den Datenschutz und die Datensicherheit. Mit neuen Gesetzen, die lediglich national gelten, ist dem Datenmissbrauch nicht Einhalt zu gebieten. Selbst eine weltumspannend geltende Vereinbarung ist das Papier nicht wert, auf das sie geschrieben stünde, solange es wirtschaftliche und kriminelle Energien gibt, die ihre Vorteile aus (unrechtmäßigen) Datenauswertungen ziehen.

Das soll nun nicht dazu führen, dass sich Resignation breit macht und alles beim Alten belassen wird! Vielmehr gilt es umzudenken!

Beginnend bei den Nutzern von Kommunikationsmitteln, Plattformen und Netzwerken ist die notwendige Umsicht mit dem Umgang eigener Daten zu vermitteln. Damit kann gar nicht früh genug begonnen werden! Spätestens dann, wenn die erste vernunftbegabte Kommunikation außerhalb der eigenen Familie stattfindet, ist es Zeit, altersbezogen auf die Gefahren unreflektierter Weitergabe von Daten hinzuweisen. – Dies klingt tatsächlich nach den vielen Theoretikern, die weise den Finger heben und lautstark in den Chor der Warner und Unheilsverkünder einstimmen, jedoch bar der Realität keinerlei praktischen Ratschläge ihrer „Endzeitvisionen“ folgen lassen. – Gefahrenprävention von Kindesbeinen an … das klingt in der Tat weltfremd und überzogen!! Doch, ist es das wirklich?

Vor einiger Zeit erschien ein Artikel in der Zeitschrift C‘T mit dem Titel „Ein Netizen entdeckt den Wunsch nach Privatsphäre“ (nachzulesen im Archiv des Heise-Verlages 01/11). In diesem ist eindrucksvoll und erschreckend geschildert, welche Informationen aus dem unbedarften Umgang mit den eigenen Daten Jedermann zugänglich ist. Welche Informationen wären wohl *noch* zutage gefördert worden, oder was hätte mit den bereits ermittelten Informationen angestellt werden können, wenn es jemand darauf angelegt hätte, den Betroffenen schaden zu wollen? Weit hergeholt? Durchaus nicht!

Datenschutz und Datensicherheit beginnen bei demjenigen, dem die Daten gehören. Hier ist der allererste Ansatz zu suchen, nämlich die Sensibilität mit dem Umgang dieser Daten. Die für die heutige Zeit (leider) typischen exhibitionistischen Offenlegungen intimster Gedanken, Neigungen und Vorlieben bis hin zu augenblicklichen Stimmungszuständen und persönlichsten Angaben in so genannten sozialen Netzen und Chat-Umgebungen öffnen dem Missbrauch durch Unbefugte Tür und Tor. Privatsphäre wird plötzlich nebensächlich, Hauptsache man gehört dazu, ist Teil der Community, ist In! Privatsphäre wird erst dann wieder „wichtig“, wenn es „hehren Zielen“ dient, z.B. als Wahlkampfthema. Doch sonst … virtuelle Freunde sind wichtiger!

Der normale Nutzer ist gar nicht mehr in der Lage zu kontrollieren, was mit seinen Daten geschieht, wenn sie einmal in den Weiten des Internets verschwunden sind oder in den Fängen der diversen Anwendungen (neudeutsch: Apps) seines Smart Phones oder Laptops geraten. Sicherlich, diese Hilfsmittel einfach nicht mehr zu nutzen, ist unsinnig und widerspricht der technologischen Entwicklung. Ebenso unsinnig ist es, den Nutzer anzuhalten, seine Daten selbst so zu schützen, dass wirklich niemand unautorisiert darauf zugreifen kann. Schließlich handelt es sich um einen Nutzer und nicht um einen IT-Spezialisten oder Nerd! Also was tun?

Daten werden gesammelt, aus den verschiedensten Gründen. Teilweise sind die Gründe nachvollziehbar, teilweise nicht. Wenn Daten gesammelt wurden und der Zweck einsichtig und nachvollziehbar ist, wer hat dann Zugang zu diesen Informationen und wer hat wem die Kompetenz zur Einsichtnahme überantwortet? Wer ist in der Pflicht, diese Daten zu schützen? Was ist überhaupt schützenswert oder schützens-notwendig? Gut – die letzte Frage wird individuell sehr unterschiedlich beantwortet werden. Soll aber auch gar nicht in den Vordergrund gerückt werden, da die subjektive Einschätzung von „Wert“ für den Schutz dieses Wertes unerheblich ist. Was bleibt, ist die Frage: Wer schützt Informationen/Daten vor unbefugten Zugriff und wer führt darüber die Kontrolle aus?

Um es kurz zu machen: Wer Kommunikations- und/oder Speicher-Mittel zur Nutzung für Dritte zur Verfügung stellt, muss sich der Pflicht bewusst sein, den unbefugten Umgang mit diesen Mitteln zu unterbinden. Entweder durch Maßnahmen, die den Umgang selbst verhindern (was unrealistisch ist), oder dadurch, dass das Ergebnis des unbefugten Umgangs für den Unbefugten nicht nutzbar ist. Hierbei ist er durch die gewählten Vertreter der Nutzer (i.A. die Regierung) in jeder Hinsicht zu unterstützen, sowohl was die gesetzliche Basis betrifft, als auch die politische Rückendeckung.

Es sind also die Telekommunikations-, Informations- und Technologieunternehmen, die hier gefordert sind, Lösungen herbeizuführen. Lösungen gibt es bereits! Doch die sind teuer. Und – will wirklich jedes Unternehmen überhaupt sichere Daten zu jedem Preis?

Wenn anfänglich von einer „Erziehung“ des Nutzers im Umgang mit seinen persönlichen Daten die Rede war, so muss konsequenterweise auch das Umdenken derjenigen angemahnt werden, die diese Daten transportieren oder in Gewahrsam haben. Während die Einen die notwendige Sorgfalt mit der Streuung von Informationen (wieder) erlernen müssen, müssen die Anderen sich (endlich) der Pflicht stellen, die ihnen anvertrauten Informationen so zu schützen, dass sie nicht durch Unbefugte verwendbar sind - auch dies ist Zielsetzung des Eyes of Europe Programms: Nicht nur der Austausch von Wissen und die Weitergabe von Informationen, sondern auch das Bewusstmachen der Verantwortung für Privat- und „Gemeinschaftssphären“.

Arne Petrowski, 17.09.2013
High Level IT / TC - Industries