Technologiemix, Komplexität und der menschliche Faktor

Vor dem Vertrauen in Technik kommt das Vertrauen in Menschen

In dem Heise-Artikel

https://www.heise.de/news/Analyse-Warum-80-000-Arztpraxen-ihre-Verbindung-zur-Telematik-verloren-4842866.html

werden die Hintergründe des Ausfalls der Verbindung ausführlich beschrieben.

Es ist sicher ein Allgemeinplatz darauf hinzuweisen, dass der eingesetzte Technologiemix und die beteiligte Komplexität der Verschachtelungen der technischen Komponenten, der Systeme und Funktionen, zusammen mit dem menschlichen Faktor, jederzeit zu größeren Ausfällen führen können. Man sollte aber daran erinnern, dass unsere Gruppe der Kritiker in 2016 auf diese Faktoren und den vielfältigen Einsatz von XML, als Steuerungs- und Regelungsdateien, hingewiesen haben, mit der Ergänzung, dass im Vorfeld des größten IT-Projektes der Welt enorme, bzw. nie dagewesene Anstrengungen unternommen werden müssen um ein IT-System dieser Ausrichtung abzusichern.

Auch haben wir darauf hingewiesen, dass nirgends in den Projektbeschreibungen in einem ausreichenden und konkreten Maße erkennbar war, dass diese Anstrengungen und Maßnahmen unternommen worden sind. Dies hängt auch mit den offenen Beschreibung der Gesamtarchitektur zusammen auf einer höheren Abstraktionsebene, die nichts mit einer systemischen Beschreibung der verbundenen IT-Technologien zu tun hatte. Hier begründet sich auch die Schwierigkeit eine Datenfolgenabschätzung zu liefern, deren Voraussetzung eine äußerst feingrunalare Beschreibung des Systems und der Prozesse ist. Dabei ist es auch erforderlich jede Schnittstelle des IT-Systems, an der ein menschlicher Eingriff möglich ist, detailliert zu erfassen, zu beschreiben und mit einem Interaktions- und Kontrollprozess abzusichern.

Es geht hier um eine extrem mühselige Arbeit und ein sehr teures Unterfangen, im Gegensatz zum Aufbau des IT-Systems der Telematikinfrastruktur aus unzähligen fertigen Komponenten, die als Software- und Hardware-Bausteine zur Verfügung stehen. Es geht um ein durchdeklinieren aller beteiligten technischen und menschlichen Prozesse, der Funktionen und Schnittstellen und ihre Prüfung zur Absicherung während der Ausführung von Anweisungen.

Dies erfordert neuartige Ansätze, denn bisher gibt es zwar für viele Punkte der Programmierung und der informationellen Megasysteme Lösungsansätze für die Kontrolle, z.B. in Form von Rollbackverfahren, damit nach einer Änderung, im Falle von Fehlern, man jederzeit wieder zu einem funktionierenden Zustand zurückkehren kann, es existieren aber keine ganzheitlichen Verfahren und Lösungen für die Größenordnung der IT-Systeme, die sich jetzt etabliert haben.

Es muss noch viel Forschung betrieben und Ideen und Lösungen entwickelt werden, damit eine ausreichende Absicherung unserer sensiblesten Daten,die überhaupt existieren, erreicht werden könnte.

Auch zeichnet sich hier ab, dass diese Ziele, mit dem bestehenden Konzept der Vernetzung in der Telematikinfrastruktur, mit Mastersystemen und der globalen Öffnung der privaten Datenräume zu großen Institutionen hin, der falsche Ansatz ist.

Der noch größer gewordene Witz zum jetzigen Zeitpunkt ist, dass über einen sehr langen Zeitraum die Ausrichtung der Telematikinfrastuktur, ablenkend und verschleiernd als reines

Vernetzungsprojekt ohne zentrale Server beschrieben wurde. Immerhin konnte dadurch das Ziel erreicht werden die Bürger vor die vollendeten Tatsachen einer fremdbestimmten Verwertung ihrer Gesundheitsdaten zu stellen.

Jetzt ist Katze aus dem Sack, sowohl was die Realität laufender neuer Schwachstellen und Sicherheitlecks und die tatsächliche Dimension der Datenverarbeitung angeht, denen wir weiter ausgesetzt werden.

Mit Hilfe der eingesetzten Technologien will man Vertrauen herstellen, der Einsatz von Zertifikaten, den Zertifikatsketten und anderer Methoden soll Sicherheitsmechanismen zur Gewährleistung der Authentizität und Integrität der Daten erzeugen. Die digitalen Zertifikate dienen dem Zweck elektronische Daten zu signieren, damit der Nachweis der Echtheit von Daten und Kommunikation geführt werden kann. Dies ist ein überaus technischer Vorgang, doch hinter jeder Technik stehen die Eigner.

Die Zertifizierungsstelle (Certificate Authority, CA), also die Organisation, die das CA-Zertifikat bereitstellt und die Signatur von Zertifikatsanträgen übernimmt können wir nicht blindlinks vertrauen, man erwartet jedoch stets von uns der Technik im Allgemeinen und der Verkettung von Staat und Unternehmen zu vertrauen, die bis in die Zertifikatsverkettung der TI nachvollziehbar wird.

Im Falle der Telematikinfrastuktur hat es jedoch nie ausreichende demokratische Beteiligungsprozesse gegegeben, der das Vertrauen in die beteiligten Firmen, wie an Arvato, als höchste vertrauenswürdige Zertifizierungsstelle, rechtfertigt.

Hat es eine Volksentscheidung gegeben, die Telematikinfrastruktur so aufzubauen wie sie existiert?

Wir sind an dem Punkt angekommen unsere politische Infrastruktur wesentlich zu verbessern um damit zu neuen Lösungen zu gelangen, die nicht ausschließlich aus der Allianz von Staat und Unternehmen resultieren.

22.7.2020 Rolf D. Lenkewitz 87769 Oberrieden 0163170 68 09 www.rdlenkewitz.eu http://www.rdlenkewitz.eu/DSGVO/dsgvo.html