

Helmut Reimer

# Vom Primat der Anwendungen

Die ‚Henne/Ei‘ Metapher ist wohl nie so häufig wie im Zusammenhang mit den fundamentalen IT-Entwicklungen der letzten 30 Jahre benutzt worden. Sie hinterfragt wiederholt die Proportionen zwischen technologischen, organisatorischen und regulativen Vorleistungen und darauf beruhenden nutzbringenden und akzeptierten Anwendungen. Ein akutes ‚Henne-Ei-Problem‘ liegt vor, wenn durch die Vorleistungen vorgedachte oder potentielle Anwendungen nicht stimuliert werden. Hier beginnt die jeweils spannendste Phase des weiteren Schicksals von Innovationen: im günstigen Fall als ein komplexer Vorgang zur Optimierung der gegenseitigen Anforderungen und Abläufe; andernfalls als Stagnation und letztlich Abschreibung der Vorleistungen.

Eigentlich ist es kein Geheimnis. Die Akzeptanz von IT-Technologie ist direkt an einen konkreten oder subjektiv empfundenen Nutzen und an ein gewinnträchtiges Geschäftsmodell gebunden. Auf diesen Grundlagen haben attraktive und nutzerfreundliche Anwendungen die großen Innovationsschübe bei Standardisierung, Infrastrukturentwicklung, Bereitstellung von Sicherheitswerkzeugen und -diensten bewirkt. Unter ständiger Risikobeobachtung durch die Beteiligten (und die Öffentlichkeit) ergibt sich eine fortlaufende Optimierung der Anwendungen und hinreichende Transparenz für die Notwendigkeit der Integration von technologischen Maßnahmen zur Verbesserung von Datenschutz und Datensicherheit, aber auch der Verbindlichkeit der Anwendungsziele. Typische Beispiele für diese Zusammenhänge sind die Entwicklungen rund um die E-Mail oder den Internet-Zahlungsverkehr. Sicher im juristischen Sinn sind diese Anwendungen nicht geworden, ihre Ergebnisse halten aber Plausibilitätsbewertungen aus und sind – mit Einschränkungen – als Anscheinsbeweise tauglich.

IT-Sicherheitsexperten, Technologieentwickler und Juristen kritisierten die geschilderten Abläufe ab Mitte der 1980iger Jahre zunehmend heftig. Ihre Vision lautete: die geschilderte Genese muss umgedreht werden. Zunächst ist eine hinreichend sichere Umgebung bereit zu stellen, die dann als Grundlage für Anwendungsentwicklungen dienen soll. Die Motivation ergab sich aus

- der schnell zunehmende zivilen Nutzung der Kryptographie;
- der zunächst überzeugenden These, das IT-Sicherheitstoken (z.B. SmartCards) einen entscheidenden Beitrag für eine sichere Anwendungsumgebung leisten können;
- der nachfolgend schnellen Verbreitung des Internet als offene Systemumgebung und ersten Standards für Infrastrukturen und Dienste;

- aber auch aus zunehmend kritischen Technologie-Folgenabschätzungen.

Sehr bald wurde die Komplexität der Vision sichtbar, insbesondere, dass die Aufgabenstellung nicht befriedigend im Rahmen der marktüblichen Hard- und Software mit ihren Schwachstellen und Fehlern gelöst werden konnte. Um Zielvorgaben für Forschung und Entwicklung zu bestimmen, und um zu Innovationen und Investitionen für IT-Sicherheit anzuregen, bedienten sich nationale Gesetzgeber nun häufig auch der Technikregulierung. Das bekannteste Beispiel für Irrungen und Wirrungen, die sich dabei ergeben, ist deutsche Signaturgesetzgebung. Die Umsetzung ist im Detail gründlich gelungen, Anwendungen, die mit der qualifizierten elektronischen Signatur ermöglicht werden, sind bis auf kleine Nischenlösungen aber bisher nicht entstanden. Trotzdem wurden – ohne Anwendungspraxis im Sinne von lebendiger Optimierung von Aufwand/Nutzen und subjektivem Erfolg – juristische Positionen und Grundsätze entwickelt, die dem Signaturkonzept a priori ein enges Korsett anlegen.

Die Bundesregierung wollte im Jahr 2005 mit einer eCard-Strategie neuen Schwung in die Verwertung von Potentialen der SmartCards und von IT-Sicherheitsdiensten bringen. Die Ziele dieser Strategie sind auch 8 Jahre später nicht erreicht:

- schnelle Einführung der Gesundheitskarte und vordringlich des elektronischen Heilberufsausweises mit einem Einsparungspotential von jährlich 1 Mrd EURO;
- Einführung des elektronischen Personalausweises, durch den im Bereich eGovernment, eBusiness und im elektronischen Rechtsverkehr flächendeckend eine sichere IT-Infrastruktur geschaffen wird;

Als vollständig untauglich für die Praxis haben sich später das JobCard-Verfahren (in der Folge ELENA) und die Ergänzung des ELSTER-Verfahrens durch die qualifizierte elektronische Signatur erwiesen.

Eine Erkenntnis lautet also: das *Wie von Anwendungen* und das *Was wird erreicht* lassen sich nicht politisch vorschreiben, technologische Abläufe ebenso wenig.

Zukünftige Erfolge werden sich nur dann einstellen, wenn nützliche Anwendungen wieder als entscheidende Triebkräfte für die Entwicklung von angemessen sicheren IT-Systemen betrachtet werden. Sie brauchen die ständige Anpassung an neue Hard- und Softwareentwicklungen, Standards und Schnittstellen sowie flexible Infrastrukturen und Sicherheitsdienste. Eine moderne Telematik im Gesundheitswesen sollte diesen Weg nachhaltig fördern.