Sicherheitskultur

für eine digitale Welt

Durch rein technische Maßnahmen lässt sich Sicherheit nicht gewährleisten, weil die Schutzziele untereinander konfligieren und in ihrer Priorisierung unter den Nutzern technischer Systeme ausgehandelt werden müssen. Das kulturelle Erfordernis zielt auf die Aufklärung der Nutzer sowie die Bereitstellung technischer Infrastrukturen, welche die hierfür notwendigen Informationen während der Mensch-System-Interaktion liefern und flexible Lösungen als Ergebnis der Aushandlungsprozesse erlauben.

A Culture of Security for a Digital World

Security can not only be guaranteed through technical devices for reasons of conflicting protection objectives, whose prioritization must be bargained by the users of technical systems. The cultural requirement aims at the education of users and at providing the technical infrastructure that generates the required information during the User-System-Interaction and enables flexible solutions as a result of the bargaining-process.

Christoph Hubig • Seit der neolithischen Revolution wurde in Ablösung der „Zufallstechnik“ (José Ortega y Gasset) der Jäger und Sammler die Planbarkeit des Handlungserfolgs dadurch sicher gestellt, dass den Gefahren der Natur durch den Aufbau technischer Systeme und Infrastrukturen begegnet wurde. Gefahren wurden transformiert in Risiken, die gestaltbar und wählbar wurden: Sicherheit als „Freiheit von unakzeptablen Risiken“ (ISO/IEC/TÜV). Wenn es ein Spezifikum der Technik gibt, so scheint dies Sicherheit als störungsfreie Wiederholbarkeit zu sein. Sicherheitsdefizite erscheinen als genuin technische Herausforderungen. Wozu bedarf es hier einer „Kultur“?

Sicherheitskonzepte

Sicherheit als „Schutz vor …“ und Sicherheit als „Sicherung des Gelingens zu …“ sind zu unterscheiden. Beides scheint durch Technik leistbar: Die immer komplexer werdenden technischen Systeme bis hin zu denjenigen einer „digitalen“ Welt dienen der Gefahrenabwehr und eröffnen neue Optionen gelingenden Handelns. Web 2.0 und Ubiquitious Computing, Smart Cards und elaborierte Telekommunikation erlauben die Minderung und Minimierung von Risiken (z. B. qua Vermeidung medizinischer Fehldiagnosen, Kompensation physischer und kognitiver Einschränkungen und Informationsdefiziten, Optimierung der Prävention) und erweitern unsere Handlungsräume (z. B. durch intelligente Seniorenwohnungen, Blindennavigation, smart factory, child finder, effektives Katastrophenmanagement). Assistenzsysteme sollen unser Leben leichter, angenehmer machen; Widerständigkeiten sollen abgebaut und die Lebensführungsumstände individueller und situationsadäquater anpassbar werden. Hierin liegen die Chancen durch die komplexen Systeme einer digitalen Welt. Gleichwohl besteht aus guten Gründen seit den 80er Jahren des letzten Jahrhunderts eine Diskussion um eine Sicherheit „vor“ den durch die Systeme ermöglichten Effekten. Man untersucht Risiken, die im Zuge der Nutzung der Systeme entstehen, und entwickelt Strategien ihrer Minderung. Hierbei zeigen sich ganz unterschiedliche Schutzziele und zahlreiche Binnenkonflikte zwischen den Beurteilungskriterien, bedingt durch unterschiedliche Interessen von Nutzern, Diensteanbietern und Betreibern. Neben „technikimmanenten“ Kriterien einer Safety wie Ausfallsicherheit/Zuverlässigkeit und Funktionssicherheit/Fehlertoleranz (für System und Systemnutzung), unter denen Versagens- und Betriebsrisiken minimiert werden, heben die Security-Schutzziele ab auf Vertraulichkeit, Integrität/Entdeckbarkeit von Fälschungen, Anonymität/Unbeobachtbarkeit/Unverkettbarkeit, Zurechenbarkeit/Authentizität sowie Verfügbarkeit.

Sicherheitskultur

Eine solchermaßen gefasste Sicherheit verweist auf die Notwendigkeit der Einbettung in eine Sicherheitskultur: Erstens bedarf es eines Abgleichs der zu vermeidenden Risiken, der Schutzziele einer Sicherheit vor systemischen Effekten (der Systeme selbst und/oder ihrer fehlerhaften oder missbräuchlichen Nutzung) mit den wahrzunehmenden Chancen einer „Sicherung zu …“. Zahlreiche Dienstleistungen erfordern eine Profilierung der Nutzerinnen und Nutzer, um adäquat vollzogen werden zu können. Sicherheitsstandards lassen sich in etlichen Fällen nur durch Überwachung erfüllen. Privacy konfligiert also mit Transparenz. Zweitens zeigen die Charakteristika einer Security, dass je nach Nutzerintentionen Vertraulichkeit, Integrität, Anonymität, Zurechenbarkeit und Verfügbarkeit bezüglich ihrer Gra-

Christoph Hubig

duierung und Priorisierung problemadäquat und flexibel auszuhandeln sind.
Die Frage eines umfassenden Diskussionsrahmens von Sicherheitskultur erscheint in ihrer Dringlichkeit.

Probleme und Forderungen

Angesichts der Missbrauchsmöglichkeiten (von der Überwachung bis hin zu Aktivitäten der „Cypher-Punks“ als „Piraten des 21. Jahrhunderts“ auf der Gegenseite) dürfen sich unaufgeklärte Nutzerinnen und Nutzer nicht mangels Wissen über die Leistungsfähigkeit der Schutzmechanismen in falscher Sicherheit wiegen oder überfordert werden angesichts technischer Optionen etwa der Verschlüsselung und Kryptographie. Ein naiver Optimismus bezüglich neuer Freiheiten universeller Informiertheit oder einer umfassenden Lebenserleichterung darf die Orientierung nicht vereinseitigen. Denn über den Verlust der Widerständigkeit im Zuge der Delegation von Leistungen an die Systeme verlieren wir in demselben Maße Kompetenzen (die wir bei Systemausfall vermissen), wie wir unsere Handlungsräume erweitern und unser Leben angenehmer machen.
Gewiss: Elaborierte Techniken des Datenschutzes sind bereitgestellt, z. B. zur Minimierung und systematischen Vermeidung von Datenspuren beim Web-Zugriff und Web-Kommunikation. Was nutzt dies jedoch, wenn die Nutzerinnen und Nutzer die elaborierten Techniken der Anonymisierung und Pseudonomysierung mangels technischem Know-how nicht nutzen (können), und aus derselben Liga der Informatik-Genies, die diese Entwicklungen vorantreiben, auch diejenigen stammen, die sie überwinden und missbrauchen können? Und was nutzen technische Optionen zur Herstellung von Transparenz, zur Bereitstellung von Ausstiegspunkten oder zur Integration in Netzwerke zwecks Lebenshilfe, Unterhaltung, Accident-Management oder Katastrophenschutz, wenn eine sorgfältige Analyse über die Notwendigkeit oder Zulässigkeit oder ein Verbot der Zusammenführung von Daten dem Einzelnen seine Rechte und Pflichten nicht problematisiert, sondern zugunsten eines diffusen Systemvertrauens außen vor bleibt? Was nutzt ein effizientes technisches Arsenal für den Katastrophenschutz, wenn das menschliche Engagement bei Systemversagen nicht mehr auf ursprüngliche Kompetenzen zurückgreifen kann? Oder zu ungunsten persönlicher Fürsorge die Verantwortung für die Alten an die intelligente Seniorenwohnung delegiert wird? Was erbringen Abwägungen über Zulässigkeit oder Unzulässigkeit der Kryptographie angesichts behördlicher Sicherheitsdesiderate, wenn im Falle der Prohibition gilt: „Dann haben eben nur die Verbrecher Kryptographie!“ Von einer Privatsphäre ganz zu schweigen, die angesichts der technischen Möglichkeiten nur noch derjenige für sich reklamieren kann, der uninteressant ist, analog der einzig noch durch Off-line-Betrieb zu realisierenden Sicherheit relevanter Rechner.

Lösungskonzepte

Fragen über Fragen. Patentrezepte zu ihrer Beantwortung stammen oft von gut meinenden Propagandisten, die angesichts der Deinstitutionalisierung des Netzbetriebs und eines individuell-adaptiven Ubiquitious Computing klassisches institutionelles Handeln des Verbraucherschutzes und der Überwachung („Zensur“) rehabilitieren wollen.
Konkrete Lösungen lassen sich m. E. nur durch Verfahren etablieren, die Mensch-System-Interaktionen kritisch zu begleiten erlauben. Interaktion beruht ja auf „Erwartungserwartungen“: Erwartungen der Nutzer über Erwartungen des Systems über deren Erwartungen und umgekehrt. Ein Abgleich solcher Erwartungen als notwendige Bedingung von Sicherheit sollte bei neuen Entwicklungen erstens im Vorfeld in Gestalt von organisierten Entwickler – Nutzer- Dialogen stattfinden. Zweitens muss parallel zur Nutzung eine Kommunikation über die Nutzung im Dialog zwischen (Assistenz-)System und Nutzer möglich sein: Herstellung von Transparenz on demand über Systemstrategien, Risiken, Bedingungen gelingender Nutzung, Gründe für Misserfolg, Verlautbarung und/oder Empfehlungen von Ausstiegspunkten. Drittens sollte ein institutionalisierter Erfahrungs-

Christoph Hubig ist seit 2010 Professor an der TU Darmstadt. Er leitet das Fachgebiet Philosophie der wissenschaftlich-technischen Kultur im Fachbereich Gesellschafts- und Geschichtswissenschaften.

austausch über die Nutzung in entsprechenden www-Foren stattfinden: Hier sollte die Einhaltung von Security-Kriterien bilanziert, Vereinseitigungen abwägend relativiert und Lernerfolge gezeitigt werden jenseits doktrinärer Aufklärung oder anonymer Vergemeinschaftung, hintergründiger Adaptivität der intelligenten Systeme oder einer Verwiesenheit auf individuelle, isolierte eigene Erfahrungen.
Medienkompetenz wird, wie alle Kompetenzen, nicht über Wissensvermittlung erreicht, sondern durch empfehlungsgeleitetes Training in Abarbeitung an Widerständigkeit. Sicherheit, die jegliche Widerständigkeit abzubauen sucht, zerstört Kompetenz und verhindert die Herausbildung neuer Kompetenzen. Mit Blick auf die biedermeierliche Empfehlungs- und Beratungskultur der Salons, Zirkel und Gesellschaften angesichts der Herausforderungen der ersten industriellen Revolution ist auch für uns eine Art neues „Biedermeier“ zu fordern, damit Systemvertrauen entstehen kann.

Institut für Philosophie
Prof. Dr. Christoph Hubig
Tel. 06151/16-64511
E-Mail: hubig@phil.tu-darmstadt.de
www.philosophie.tu-darmstadt.de