CENTER FOR
ADVANCED
INTERNET STUDIES

Laura Kocksch

The Practice Turn in IT Security

CAIS Report

Veranstaltung
20.–21. Juli 2017

GEFÖRDERT DURCH

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen

The Practice Turn in IT Security

Interdisziplinärer Workshop zur Verfertigung von IT-Sicherheit

Mit der zunehmenden Vernetzung von Geräten im Alltag wird die Frage nach der Absicherung dieser Geräte und ihrer Verbindungen immer brisanter. Durch die Verbindung zum Smartphone werden Kühlschränke, Heizungen und Rollos angreifbar durch Hackerattacken. Der Preis einer Hackerattacke ist für Privatpersonen hoch, aber auch für staatliche Akteure, wie Medienberichte über Hacks von der Wahlsoftware bis zum Finanzmarkt zeigen. IT-Sicherheit wird seit einigen Jahren als wichtiger Faktor im Design und in der Anwendung von IT-Systemen gesehen. Zwar gibt es technisch immer neue Möglichkeiten, Computersysteme zu verschlüsseln und Netzwerke abzusichern, jedoch gelangen nur wenige davon zum Einsatz durch sowohl Nutzer*innen als auch Entwickler*innen.

Auf einem zweitägigen Workshop kamen Expert*innen der IT-Sicherheit mit einschlägigen Forscher*innen der Sozialwissenschaft zusammen, um über Fragestellungen an der Schnittstelle von Mensch und Technik zu diskutieren. Zwar ist die Beschäftigung mit dem ‚Faktor Mensch' in der IT-Sicherheit mittlerweile weit verbreitet, jedoch wird dabei oft von einzelnen, unabhängigen Nutzer*innen oder Entwickler*innen ausgegangen, die vermeintlich zu nachlässig oder zu unwissend seien, um Technologien sicher einzusetzen.

Langjährigen Erkenntnissen der Sozialwissenschaft zu organisatorischen, sozialen und situativ-praktischen Einbettungen menschlicher Handlungen wurde dabei bisher kaum Gehör geschenkt. Mit dem Zusammenkommen von Expert*innen auf den Gebieten der Sozialwissenschaft einerseits und der IT-Sicherheit andererseits konnten in dem Workshop Probleme mit der Sicherung von IT-Systemen vor dem Hintergrund sozialer Faktoren diskutiert werden.

Ergebnisse des Workshops

Der Workshop hat offengelegt, dass IT-Sicherheitsexpert*innen oft mit einer Problemorientierung an Sozialwissenschaftler*innen herantreten. Der Mensch wird als individuelle Fehlerquelle identifiziert und Ziel ist es, bessere Mechanismen zu entwickeln, um Nutzer*innen und Entwickler*innen zu schulen und so zu besserem Verhalten zu erziehen. Durch ein Gespräch über die Definitionen von Sicherheit und Unsicherheit während des Workshops stellte sich jedoch heraus, dass technische Definitionen hierbei Vorrang haben. Probleme sind demnach stets technisch definiert, weniger aus der Sicht von

Nutzer*innen oder Entwickler*innen. Betrachtet man zum Beispiel, wie Entwickler*innen arbeiten, sowie die organisatorische und soziale Einbettung ihrer Arbeit, tauchen plötzlich gänzlich andere Probleme auf und es wurden gute fachliche, organisatorische oder selbst emotionale Gründe für ‚schlechte' IT-Sicherheit deutlich. Wenn zum Beispiel Software gehackt wird, ermitteln IT-Fachleute zwar schnell die technischen Ursachen und identifizieren Verantwortliche für fehlerhaften Code. Allerdings wird selten nachgefragt, warum Entwickler*innen Sicherheit nicht in ihre Arbeitspraktiken integrieren können. Es fehlt ihnen zum Beispiel an Anerkennung von Sicherheitsthemen durch Kund*innen oder das Produktmanagement.

Der mit diesem Workshop angestoßene ‚Practice Turn' will IT-Sicherheitsprobleme nicht allein als ein Bündel technischer Probleme oder als einen Mangel an Verständnis oder Wissen seitens einzelner Nutzer*innen oder Entwickler*innen verstehen. Vielmehr werden mit ‚practices' situative Handlungen betrachtet, die eine Vielzahl von Akteuren involvieren und in unterschiedlichste Rahmenbedingungen eingebunden sind. Die Praktiken, durch die sich IT-Sicherheit vollzieht, sind verwoben mit verschiedenen technischen, sozialen und organisatorischen Aushandlungsprozessen. Wird IT-Sicherheit als Ergebnis von Praktiken verstanden, die zugleich technisch und sozial sind, kann Sicherheit als Design- und Management-Prozess verändert werden.

Der Ansatz, die Praktiken zu betrachten, in denen IT-Sicherheit hergestellt, aufrechterhalten oder umkämpft wird, macht deutlich, dass eine Vielzahl von Praktiken sicherheitsrelevant ist, die aber bisher nicht als Sicherheitspraktiken verstanden werden. Damit geht einher, dass Sicherheit nicht immer das Gleiche ist und das Gleiche tut — auch wenn IT-Sicherheit auf den ersten Blick ein scheinbar eindeutiges Konzept ist. Nur eine Betrachtung des einzelnen Falls, situativ und im jeweiligen Kontext, bringt die Vielzahl an ‚Sicherheiten', deren situative Anpassung und Sozialität zum Vorschein. Im Workshop wurden IT-Sicherheit und ihre Praktiken unter folgenden Kernfragen diskutiert:

- Ziel: Akteure definieren und Dezentralisierung von IT-Sicherheit nachvollziehen.
  – Welche Akteure sind am Design und der Aufrechterhaltung von IT-Sicherheit beteiligt?

- Ziel: Narrative und Techniken definieren, die an der Herstellung von Sicherheit beteiligt sind.
  – Welche Rolle spielen Artefakte bei der Aushandlung, was als sicher und unsicher gilt?
  – Warum funktionieren manche Sicherheitstools in der einen Umgebung, aber in einer anderen nicht?

- Ziel: Soziale Praktiken definieren, die an der Herstellung und Kontestierung von Sicherheit beteiligt sind.
  – Durch welche Praktiken wird IT-Sicherheit erreicht, aber auch riskiert?
  – Und zur Konkretisierung: Welche Werkzeuge und Modelling-Techniken werden hierfür eingesetzt?
  – Wie werden kollaborative Praktiken organisiert?
  – Welche sozialen und organisatorischen Grenzen müssen überbrückt und verhandelt werden, um etwas sicher zu machen?

Zur Klärung dieser Fragen ist es notwendig, technische Betrachtungen mit Beschreibungsmöglichkeiten des Sozialen zusammenzubringen, was wir durch die Zusammenstellung unserer Teilnehmer*innen erreichten.

Statements der Teilnehmer*innen

Die Teilnehmer*innen des Workshops wurden nach ihrem disziplinären Hintergrund und ihrer Erfahrung mit IT-Sicherheitsfragestellungen ausgewählt. Jede*r Teilnehmende wurde darum gebeten, ein Artefakt aus seiner*ihrer Arbeit mitzubringen und anhand dessen seinen*ihren Zugang zu IT-Sicherheit zu schildern. So wurde erreicht, dass ein interdisziplinärer Austausch stattfand, der für Sozialwissenschaftler*in-

nen einen Einstieg in das Thema IT-Sicherheit ermöglichte und dabei individuelle Praktiken, Probleme und Lösungen der IT-Sicherheitsexpert*innen thematisierte. So wurden nicht lehrbuchartige Beschreibungen der IT-Sicherheit diskutiert, sondern aktuelle Probleme oder Lösungsansätze. Alle Teilnehmer*innen äußerten ihren idiosynkratischen Blick auf IT-Sicherheit und zeigten dabei deutlich, dass Sicherheit nicht allgemeingültig oder abschließend definierbar ist. Hier ihre Standpunkte:

„Es gibt auch zu viel Sicherheit. [...] Was wir brauchen, ist die richtige Sicherheit."
Prof. Dr. Estrid Sørensen
Centre for Anthropological Knowledge in Scientific And Technological Cultures (CAST), Ruhr-Universität Bochum

„Sicher ist aber ein schlechter Begriff, sicher ist relativ zum Angreifer."
Prof. Dr. Alexander May
Lehrstuhl für Kryptologie und IT-Sicherheit, Horst Görtz Institut für IT-Sicherheit, Ruhr-Universität Bochum

„Sicherheit und Unsicherheit sind aus Praxisperspektive eine schlechte Dichotomie."
PD Dr. phil. Cornelius Schubert
Akademischer Rat für Innovationsforschung, Institut für Sozialwissenschaft, Universität Siegen

„Technik ist einfach. Das Problem ist der allgemeine Entwickler."
Dr. Martin Gilje Jaatun
Senior Research Scientist, Department of Software Engineering, Safety and Security SINTEF Digital, Norway

„Sicherheit kann man nicht herstellen, Sicherheit muss man verhandeln."
Helmut Rother
Senior Expert AXA Information Security

„Es gibt fast 100% Sicherheit."
Dr.-Ing. Peter Mayer
Research Group SECUSO – Security, Usability and Society
Technische Universität Darmstadt

„Ein Problem der ökonomischen Rationalität – Sicherheit steht im Widerstreit mit anderen Zielen."
M.Sc. Christopher Lentzsch
Lehrstuhl für Informations- und Technologiemanagement, Institut für Angewandte Arbeitswissenschaften, Ruhr-Universität Bochum

„Hacker möchten mit ihrer Arbeit Aufmerksamkeit für IT-Schwachstellen in einem breiten gesellschaftlichen Dialog schaffen. Softwareentwickler sollten dieses Selbstverständnis respektieren."
Dr. Matthias Korn
Collaborative Research Center 1187: Media of Cooperation

„Unsere Arbeit kann einen produktiven Austausch zwischen Akteuren, wie der Hacker-Gemeinschaft und Softwarefirmen, oder innerhalb von Firmen zwischen Softwareentwicklern und ihren Managern fördern."
Andreas Poller
Fraunhofer-Institut für Sichere Informationstechnologie SIT

„In der bisherigen IT-Sicherheit wird eine Soll-Welt gebaut; die Welt der eigentlichen Praktiken ist aber oft eine ganz andere Schiene."
Dr. Susann Wagenknecht
Institut für Sozialwissenschaft, Universität Siegen

„Sicherheit – oder eben Unsicherheit – ist das Ergebnis des vernetzten Verhandelns vieler Personen und Organisationen.“
Laura Kocksch, M.A.
Centre for Anthropological Knowledge in Scientific And Technological Cultures (CAST)/
NRW-Fortschrittskolleg SecHuman, Ruhr-Universität Bochum

Abbildungsverzeichnis

Foto Titelseite: CAIS, Matthias Begenat

Organisatorin

Laura Kocksch, M.A.
Research Associate
Cultural Psychology and Anthropology of Knowledge
RUSTlab - Ruhr University Science & Technology Studies
Bochum