SICHERHEITSEMPFINDEN IN DER DIGITALITÄT

Anna Lena Fehlhaber
Leibniz University Hanover,
Faculty of Philosophy and Faculty of Computer Sciences Sociology, Information Technology,
Nettemannstr. 13, 30459 Hannover, Germany
e-mail: fehlhaberlena@gmail.com

Abstract

Trotz eines permanent hohen Forschungsbedarfs wurde sich der Thematik digitalen Sicherheitsempfindens bisher kaum angenommen. Zur Annäherung an das Sicherheitsempfindens im Digitalen, präziser noch im Internet, werden die verschiedenen Prozesse von Wirkung, Nutzung und Bewertung in der Digitalität analysiert. Dadurch kann das sich individuell konstituierende Sicherheitsgefühl wissenschaftlich-analytisch untersucht werden, und Einflussfaktoren auf dieses sichtbar gemacht werden.

Keywords

Sense of security; Digital world; Impact factors.

Einleitung

> *„Eine Garantie, dass du jetzt und hier gerade "sicher" (für dich angemessen) agierst kann dir niemand ausstellen.“*[1] – NealCaffrey

Dieses Zitat ist einer Unterhaltung in einem der zahlreichen Foren des sogenannten „Deep Web“ entnommen, dem Teil des Internets, welcher nicht von den großen Suchmaschinenanbietern indexiert[2] wird. Um auf das Deep Web zuzugreifen, muss der Nutzer die spezifische Adresse der Seite die er besuchen möchte also bereits kennen, technisches Grundwissen und Anonymität erschaffen in ihrem Zusammenspiel einen relativ sicheren digitalen Raum. Trotzdem weist der Nutzer ‚NealCaffrey‘ seine Gesprächspartner darauf hin, dass es keinerlei Sicherheitsgarantie im Internet geben kann, und Sicherheit von Individuen durchaus unterschiedlich empfunden wird.

Aber wie konstituiert sich das Sicherheitsempfinden im Internet (‚digitales Sicherheitsempfinden‘) für Individuen? Diese Frage soll in dem vorliegenden theoriegeleiteten Beitrag zum digitalen Sicherheitsempfinden zu beantworten versucht werden.

Für die digitale Sicherheit gibt es in den Sozialwissenschaften und benachbarten akademischen Disziplinen nur wenig Literatur, und dass, trotz eines „permanent […] hohe[n] […] Forschungsbedarf[es]“ [1, p. 6]. Durch eine im Folgenden näher beschriebene Prozessanalyse soll eine Annäherung an das digitale Sicherheitsempfinden versucht werden.

[1] Die geführte Diskussion über Sicherheit inklusive des Beitrags von dem Nutzer ‚NealCaffrey‘ kann über folgenden Link eingesehen werden: didwzweiypgcznon.onion/posts/list/162.page, Zugriff: 09.03.2018.

[2] Entsprechende Seiten des Deep Webs können dadurch nicht über eben solche Dienste und Anbieter durch- und gesucht werden, und erscheinen nicht als reguläre Suchergebnisse.

1 Das Sicherheitsempfinden im Internet

Das Medium Internet kann für die wissenschaftliche Analyse in fünf analytische Dimensionen aufgeteilt werden: Nutzung, Technik, Diffusion, Regulation und Bewertung [2, p. 1]. Das digitale Sicherheitsempfindens kann in dieser Einteilung in die Dimension ‚Bewertung', die gleichzeitig signifikant von der Nutzung abhängt, eingeordnet werden.

Die Wirkungsweisen, die dem Prozess der Bewertung vorausgehen, sind ebenso wie das Nutzungsverhalten vielfältig – so können auch bestimmte Nutzungsweisen abhängig vom Medium begünstigt oder limitiert werden [3, p. 325]. Durch die interdependente Beziehung von Wirkung und Nutzung entstehen bestimmte Rahmungen für die Wirkungsweisen. Die Verbindung von Nutzung und Wirkung wird beidseitig durch einen Bewertungsprozess hergestellt.

Diese Teilprozesse von Wirkung und Bewertung, sowie Nutzung und Bewertung bilden die Ausgangslage für die weiterführende Analyse.

2 Prozessanalyse: Wirkung und Bewertung

Das Internet zeichnet sich durch eine hohe Komplexität aus, die auf Seiten der Anwender schwierig nachzuvollziehen ist, und zu Überforderungen und Unsicherheitsgefühlen führen kann [3, p. 327].

> *"We simply benefit from technology advances without having to be know* [sic!] *much about them. With security, unfortunately, technology can be isolated from people only up to a certain point."* [4, p. 184]

Die Notwendigkeit, Informationstechnologie verstehen zu müssen um sie technisch sicherheitsunbedenklich anzuwenden, steht konträr zu Bestrebungen, Technologie für die Endanwender vereinfachen zu wollen. Der Wunsch, auf digitale Inhalte zuzugreifen ohne die technischen Wirkungsweisen verstehen zu müssen scheint für viele Nutzer im Vordergrund zu stehen [5]. Die individuelle Gewichtung von Datenschutz gegenüber Nutzerfreundlichkeit wird maßgeblich durch soziale Rollen und Positionsverortungen bestimmt [6].

Das Internet kann für Nutzer einerseits einen Kontrollzugewinn, andererseits einen Kontrollverlust bedeuten [2, p. 168], [3, p. 327]. Einige Beispiele zur Veranschaulichung werden in der folgenden Matrix (Tab. 1) offeriert:

Tab. 1: *Kontrollgewinn und -verlust im Kontext des Internets*

Kontrollgewinn	**Kontrollverlust**
Selbstpräsentation und -darstellung: • eine eigene Webseite • Profile in sozialen Medien oder auf anderen Dienstleistungsplattformen	Datenschutz und -sicherheit: • Speicherung von Daten auf fremden Servern durch automatisierte Kopiervorgänge, Zugriff oder eine Löschung dieser ist kaum mehr möglich • digitale Handlungen sind zu weiten Teilen irreversibel [3, p. 326]
Soziale Interaktionen: • digitale Beziehungspflege • social navigation: die Orientierung im digitalen, sozialen Raum [7, p. 7, p. 17]	Authentizität: • generelle Unüberprüfbarkeit von Aussagen im Internet • die Einfachheit, eine digitale Identität anzunehmen die nicht die eigene ist, und unter dieser zu agieren sind digitalspezifische Probleme

Quelle: Eigene Darstellung unter Hinzunahme bestehender Ausarbeitungen [3, p. 326] und [7, p. 7, p. 17]

Diese Dichotomie von Kontrollgewinn und -verlust schlägt sich ebenfalls in den heterogenen Resultaten von Nutzerbefragungen zu Wirkungsbewertung und Sicherheitsempfinden im Internet nieder [8].

Durch die strukturellen Gegebenheiten des Internets stellt sich die „Frage des Vertrauens ganz neu“ [3, p. 46], und an diese Bedingungen angepasste Vertrauensmechanismen vermögen das diffuse Gefühl von Unsicherheit einzugrenzen. Diese unterliegen jedoch häufig Fehlannahmen. Beispielsweise zeigen sich grundlegende Unterschiede in der Rezeptionsbereitschaft von weitergeleiteten Inhalten nach Anonymitätsgrad [7, p. 140]. Die digitale Identität scheint vertrauensstiftend zu wirken und wird nicht weiter hinterfragt, ist aus technischer Sicht jedoch einfach zu manipulieren [9]. Dadurch können weitere Unsicherheitserfahrungen entstehen, insbesondere dann, wenn die Abschätzung der technischen Möglichkeiten und Folgewirkungen sehr komplex ist.

3 Prozessanalyse: Nutzung und Bewertung

Der Mediennutzung gehen die Medienwahl und die Entscheidung für bestimmte Angebote, Plattformen und Diensten voraus. Diese kann durch rationale, normative und interpersonale Gründe, und durch deren Zusammenwirken erfolgen [2, p. 148]. Ein Beispiel wäre die Nutzung eines bestimmten E-Mail-Programms am Arbeitsplatz. Die rationale Motivation wäre hierbei, dass das Programm auf dem Rechner bereits vorinstalliert ist, und der Umgang mit dieser Software bereits sicher beherrscht wird. Normativ ist es die stillschweigende soziale Vereinbarung, dass über E-Mails kommuniziert wird, und dafür speziell dieses Programm verwendet werden soll. Auf interpersonaler Ebene könnte die Kommunikation beschränkt sein, wenn ein anderes, oder kein E-Mail-Programm genutzt wird.

Trotz der engen Verflechtung von Begründungen für oder wider eine Mediennutzung zeigt sich, dass insbesondere normative Motive einen erheblichen Anteil dazu beizutragen, welche konkreten Dienste im Internet genutzt werden: Die Wahl dieser erfolgt in enger Abstimmung an das soziale Umfeld [10]. Sicherheits- und Datenschutzrisiken scheinen bereitwillig eingegangen zu werden, wenn die Eingebundenheit in soziale Netzwerkstrukturen die Nutzung bestimmter Dienste vorgibt:

Dies zeigt sich zum Beispiel am Instant-Messenger Dienst ‚Whatsapp‘. Die Sicherheits- und Datenschutzprobleme wurden medienwirksam behandelt. Die unverschlüsselte Verbindung begünstigte den unerlaubten Zugriff auf die übertragenen Daten durch Fremde, und Datenschützer kritisierten den Zugriff der Applikation auf alle verfügbaren Kontakte des Smartphones, Juristen bezeichneten die Nutzung der App sogar als nach deutschem Recht illegal. Die Bewertungen der App im Google Play Store und im iTunes App Store waren während dieser Zeit von negativen Kommentaren geprägt, ein (vollständiger) Verzicht des Dienstes kommt für viele Kommentatoren dennoch nicht in Frage, wie auch die Zahlen zu Download- und Nutzungszahlen bestätigen.

Dieses Phänomen zeigt sich vor allem in modernen Gesellschaften: es herrscht ein hohes Problembewusstsein in Bezug auf Sicherheits- und Datenschutz, bei gleichzeitig fehlender Konsequenz, etwa der Vermeidung entsprechender Dienste und Plattformen [11, p. 358]. Erklärungsmöglichkeiten sind soziale Faktoren und Gruppenprozesse, die in diesem Kontext ein Gefühl der Sicherheit vermitteln können [12]. Dennoch kann sich die individuelle Nutzungsdauer bestimmter Dienste oder des Internets insgesamt verringern, wenn Nutzer Sicherheits- und Datenschutzbedenken haben [13].

Ausgeprägter bleibt jedoch die Anpassung der Nutzung an das Medium und dessen Systemeigenschaften, für interpersonale Kommunikationsprozesse im Internet wurde dies hinreichend theoretisch und empirisch belegt (vgl. Perspektive der social information

processing). Für Sicherheitsaspekte könnte dies ebenfalls zutreffen, allerdings werden naheliegende Bewältigungsstrategien, etwa das Beachten von Warnmeldungen im Internet, konsequent vermieden [14]. Dabei stellt sich die Frage, inwiefern das (fehlende) Wissen zur Vermeidung von Sicherheitsgefahren dazu beiträgt, dass unsichere Passwörter gewählt, Warnmeldungen ignoriert, und Updates nicht direkt durchgeführt werde[3], oder ob dies auf eine Anstrengungsvermeidung zurückzuführen ist.

4 Digitales Sicherheitsempfinden und Kompetenz

In der Literatur finden sich die Kenntnisse zur sicheren Handhabung von Informationstechnologie als digitale Kompetenz- und Fähigkeiten-Modelle (‚digital competence' und ‚digital skills') wieder. Diese digitalen Kompetenz- und Fähigkeiten-Modelle beinhalten das Wissen und die Reflektion des Umgangs mit dem Internet. Aus ihnen ergibt sich die digitale Befähigung oder auch Digitalkompetenz, die das Wissen, die Fähigkeiten und die Einstellungen in Bezug auf Informations- und Kommunikationstechnologie beschreibt [16, pp. 3–5].

Dabei ist zu beachten, dass das Wissen über Sicherheit und Sicherheitsbedrohungen allein einen Akteur nicht dazu veranlassen muss, entsprechende Maßnahmen einzuleiten und dieses Wissen zu beachten. Die zuvor erwähnten Anstrengungsvermeidungen können Ergebnis von vorangegangenen Kosten-Nutzen-Abwägungen sein. Letztgenannte rationale Motivationen bestimmen die Wahrscheinlichkeiten, welche Entscheidungen getroffen werden:

> *"Security does not come for free, and so it is necessary to look at the tradeoffs between costs and benefits."* [4, p. 183]

Diese konstituieren sich weitestgehend unabhängig von der digitalen Kompetenz und Befähigung. Sicherheitsrisiken und -bedrohungen werden in vielen Fällen bewusst akzeptiert, weil der Aufwand der Alternative oder der vollständigen Vermeidung zu hoch erscheint [17].

Unabhängig von der letztlichen Entscheidung für oder wider ein Risiko scheint sich die digitale Kompetenz- und Befähigung auf das generelle Sicherheitsgefühl auszuwirken [18]. Das bedeutet, dass auch wenn bewusst sicherheitskritische Entscheidungen getroffen wurden, die Nutzer sich nicht unsicher fühlen müssen. In qualitativen Interviews gaben die Befragten beispielsweise an, dass diese das Gefühl hätten, die Gefahr bewältigen zu können [18]. Auch möglich ist aber, dass die verfügbaren Informationen über Bedrohungen die Unsicherheitsgefühle situationsspezifisch verstärken, statt diese zu negieren [12].

Fazit

Das digitale Sicherheitsempfinden scheint sich auf individueller Ebene durch Prozesse von Wirkung, Nutzung und Bewertung zu manifestieren, und wird dabei maßgeblich von der Einschätzung der eigenen digitalen Fähigkeiten beeinflusst. Verschiedene Handlungsmotivationen scheinen in diesem Prozess gegeneinander abgewägt zu werden, wobei das soziale Umfeld und die Einschätzung der eigenen digitalen Kompetenz einen entscheidenden Einfluss auf die letztliche Entscheidung, und auch das Sicherheitsempfinden haben.

Literatur

[1] NEUGEBAUER, R.: (2018). *Digitalisierung*. Berlin, Heidelberg, New York: Springer-Verlag.

[3] Die genannten Instanzen werden in der Wissenschaftsliteratur als häufige menschliche Fehlerquelle für Sicherheitsrisiken benannt [15].

[2] DÖRING, N.: (2003). *Sozialpsychologie des Internet: die Bedeutung des Internet für Kommunikationsprozesse, Identitäten, soziale Beziehungen und Gruppen*. Göttingen: Hogrefe, Verlag für Psychologie. ISBN 3-8017-1466-7.

[3] PAPSDORF, C.: (2013). *Internet und Gesellschaft: Wie das Netz unsere Kommunikation verändert*. Frankfurt am Main: Campus Verlag.

[4] ODLYZKO, A. (2003). Economics, Psychology, and Sociology of Security. In: Wright R. N. (eds), *Financial Cryptography*. Lecture Notes in Computer Science, Vol. 2742. Springer, Berlin, Heidelberg, pp. 182–189. Print ISBN 978-3-540-40663-1. Online ISBN 978-3-540-45126-6. DOI: 10.1007/978-3-540-45126-6_13

[5] GERBER, P.; VOLKAMER, M.; RENAUD, K.: (2015). Usability versus privacy instead of usable privacy: Google's balancing act between usability and privacy. *ACM SIGCAS Computers and Society*. 45(1), pp. 16–21. DOI: 10.1145/2738210.2738214

[6] MARX, G. T.: (2015). Surveillance Studies and Utopian Texts. In: *Imagining Surveillance: Eutopian and Dystopian Literature and Film*. Edinburgh Scholarship Online. Print publication date 2015, Print ISBN-13: 9781474400190. DOI: 10.3366/edinburgh/9781474400190.003.0002

[7] HAUTZER, L.; LÜNICH, M.; RÖSSLER, P.: (2012). *Social Navigation: Neue Orientierungsmuster bei der Mediennutzung im Internet*. Baden-Baden: Nomos.

[8] IPSOS: (2017). *Jeder Zweite hat Angst, Opfer von Cyberkriminalität zu werden. Hamburg*. Available from WWW: https://www.ipsos.com/de-de/jeder-zweite-hat-angst-opfer-von-cyberkriminalitat-zu-werden

[9] DELL SecureWorks: (2016). *Underground Hacker Markets Annual Report–April 2016*. http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf

[10] OLTRAMARI, A.; HENSHEL, D. S.; CAINS, M.; HOFFMAN, B.: (2015). Towards a Human Factors Ontology for Cyber Security. In: *STIDS 2015* (Semantic Technologies in Intelligence, Defense, and Security). pp. 26–33. Available from WWW: https://dblp.org/db/conf/stids/stids2015.html

[11] KOBSA, A.; PATIL, S.; MEYER, B.: (2012). Privacy in Instant Messaging: An Impression Management Model. *Behaviour & Information Technology*. 31(4), pp. 355–370. DOI: 10.1080/01449291003611326

[12] HEIMER, C. A.: (1988). Social Structure, Psychology, and the Estimation of Risk. *Annual Review of Sociology*. Vol. 14, pp. 491–517. DOI: 10.1146/annurev.so.14.080188.002423

[13] AKHTER, S. H.: (2012). Who spends more online? The influence of time, usage variety, and privacy concern on online spending. *Journal of Retailing and Consumer Services*. 19(1), pp. 109–115. DOI: 10.1016/j.jretconser.2011.10.002

[14] SOTIRAKOPOULOS, A.; HAWKEY, K.; BEZNOSOV, K.: (2011). On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. In: *SOUPS '11* (Proceedings of the Seventh Symposium on Usable Privacy and Security). Article No. 3. DOI: 10.1145/2078827.2078831

[15] BOYCE, M. W.; DUMA, K. M.; HETTINGER, L. J.; MALONE, T. B.; WILSON, D. P.; LOCKETT-REYNOLDS, J.: (2011). Human Performance in Cybersecurity: A Research Agenda. In: *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting*. pp. 1115–1119.

[16] GALLARDO-ECHENIQUE, E. E.; OLIVEIRA, J. M.; MARQUÉS-MOLIAS, L.; ESTEVE-MON, F.: (2015). Digital Competence in the Knowledge Society. *Journal of Online Learning and Teaching*. 11(1), pp. 1–16.

[17] BYRNE, Z. S.; DVORAK, K. J.; PETERS, J. M.; RAY, I.; HOWE, A.; SANCHEZ, D.: (2016). From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet. *Computers in Human Behavior*. Vol. 59, pp. 456–468. DOI: 10.1016/j.chb.2016.02.024

[18] BRATINA, T.; KRAŠNA, M.: (2011). Students' attitude toward digital security. In: *INTED2011 Proceedings* (5th International Technology, Education and Development Conference). Valencia, Spain, pp. 2831–2839. ISBN 978-84-614-7423-3. ISSN 2340-1079.

POCIT BEZPEČÍ V DIGITÁLNÍM SVĚTĚ

Navzdory vysoké poptávce po výzkumu pocitu digitálního bezpečí a povědomí zůstává toto téma bez odezvy. Abychom analyzovali vývoj pocitu bezpečí v digitálním světě, přesněji na internetu, jsou zvažovány a zkoumány různé procesy dojmů, použití a hodnocení. Individuální povědomí a pocit bezpečí jako celek je analyticky zkoumán a jsou odhaleny faktory ovlivňující pocit bezpečí.

THE SENSE OF SECURITY IN THE DIGITAL WORLD

In spite of a high demand on research of digital security sense and awareness, the topic remains unattended. To analyse the development of the sense of security in the digital world, more precisely, on the Internet, the different processes of impression, usage and evaluation are considered and examined. Thereby, the whole constitution of individual security awareness and sense of security is analytically researched, and factors impacting on the sense of security are uncovered.

POCZUCIE BEZPIECZEŃSTWA W CYFROWYM ŚWIECIE

Wbrew dużemu popytowi na badania poczucia bezpieczeństwa cyfrowego i świadomości w tym zakresie, tej tematyce nie poświęca się zbytnio uwagi. By przeanalizować rozwój poczucia bezpieczeństwa w cyfrowym świecie, a ściślej w Internecie, rozważaniom i badaniom poddane są różne procesy wrażeń, wykorzystania i oceny. Indywidualna świadomość i poczucie bezpieczeństwa są jako całość przedmiotem analitycznych badań. Wskazane zostały czynniki wpływające na poczucie bezpieczeństwa.