Entwicklung eines Datenschutzkompetenzmodells

Alexander Hug[1], Rüdiger Grimm[2]

Abstract: Zur Beschreibung der Fähigkeit im Umgang mit (digitalen) Medien haben Six und Gimmler ein Medienkompetenzmodell veröffentlicht [SGG07]. Darin fehlen Punkte wie Risikobewertung und Vermeidungsstrategie, die unter dem Gesichtspunkt des Datenschutzes besonders zu beachten sind. Risikobewertungen können nach den Regeln der IT-Sicherheit vorgenommen und mithilfe des Vertrauensmodells von Mayer, Davis und Schoorman [MDS95] explizit gemacht werden. In diesem Artikel wird das Medienkompetenzmodell zu einem begründeten Datenschutzkompetenzmodell erweitert. Dabei erfolgt die Risikobewertung über ausgewählte Dimensionen des Medienkompetenzmodells. Ein derart erweitertes Modell liefert eine fachdidaktisch begründete Vorlage zur Messung der Risikobewertung bei Schülerinnen und Schülern in Bezug auf die Wahrung ihrer Privatsphäre.

Keywords: Datenschutz, Datenschutzkompetenzmodell, Medienkompetenzmodell, Vertrauensmodell, Referenzmodell IT-Sicherheitsanalyse

1 Internetnutzung als ein Zusammenspiel zwischen Selbstkontrolle und Vertrauen

Die Nutzung des Internets ist ohne eine Kooperation mit verschiedenen Parteien (Softwareherstellern, Providern, Dienstanbietern), denen man Vertrauen entgegenbringen muss, nicht möglich. In [GB15] wird Vertrauen definiert „als eine Bereitschaft des Trustors [des Vertrauensnehmers], eine riskante Handlung in einem Kontext zu unternehmen, die er nicht vollständig kontrolliert, in der Erwartung, dass der Trustee [der Vertrauensgeber] diesen kontrolliert und den Trustor darin schützt."

Das Zusammenspiel zwischen Trustor und Trustee wird durch das Modell von Mayer, Davis und Schoorman beschrieben [MDS95]. Der Nutzer (Trustor) schenkt den Anbietern (Trustees) aufgrund deren Kompetenz, deren Wohlwollen und deren Integrität sein Vertrauen. Liegt nun ein zu erwartendes Risiko vor, dann wird dieses in die Vertrauensbeziehung mit aufgenommen. Aufgrund der Wirkung der Ergebnisse dieser Vertrauensbeziehung wächst oder fällt mit der Zeit das Vertrauen, da die Ergebnisse wiederum die wahrgenommene Vertrauenswürdigkeit des Trustees darstellen. Dies stellt ein rückkoppelndes Element dar.

Handlungen, die im Zusammenhang mit der Internetnutzung vollzogen werden, sind risikobehaftet. Bevor der Nutzer den Trustees Vertrauen schenkt, muss er das Risiko

[1] Universität Koblenz-Landau, FB Informatik, Universitätsstr. 1, 56070 Koblenz, hug@uni-koblenz.de
[2] Universität Koblenz-Landau, FB Informatik, Universitätsstr. 1, 56070 Koblenz, grimm@uni-koblenz.de

wahrnehmen und bewerten. Mit Hilfe des Referenzmodells für ein Vorgehen bei der IT-Sicherheitsanalyse [Gr16] kann eine Bewertung vorgenommen werden. Es ist in erster Linie für die Entwickler von Sicherheitssystemen gedacht und kann in abgewandelter Form auch zur Einschätzung eines Nutzungsrisikos genutzt werden. Bei dieser Abwandlung werden nur die datenschutzrelevanten Aspekte und Kriterien des vierschrittigen Modells benutzt.

Im ersten Schritt, der sog. Ist-Analyse, sind die Güter in diesem Fall die persönlichen Daten. Als Akteure gelten der Nutzer, die Administratoren der Netzwerke, die Dienstanbieter und letztendlich auch die Personen, die unbefugt in den Prozess des Datenaustauschs eingreifen. Interessenkonflikte können in dem, was der Nutzer erwartet, und dem, was sich die anderen Kommunikationsteilnehmer wünschen, entstehen. Schwachstellen im System können durch eine falsche Konfiguration der Hard- und Software, durch Fehler in der Software, aber auch durch Missachtung von Verhaltensregeln entstehen.

Der zweite Schritt ist die Potenzial-Analyse. Bedrohungen als mögliche Folge von Angriffen (z. B. auf das Endgerät des Nutzers und auf den Kommunikationsprozess) sind z. B. eine Fremdsteuerung des eigenen Geräts, Datenverlust (etwa durch Diebstahl von Kreditkartendaten), das unbefugte Mitlesen von Kommunikation oder eine zweckfremde Nutzung von veröffentlichten Daten in sozialen Netzwerken. Dies bedeutet im letzten Fall konkret, dass aufgrund aggregierter Daten aus dem Profil, der Zeitleiste, den Chat-Verläufen, usw. entweder ein falsches Profil des Nutzers entstehen kann oder das Profil stimmig ist, aber der Nutzer aufgrund anschließender Einflussnahme des Betreibers unerwünschte Werbung, Spam-Mails o. Ä. erhält. Das Risiko ist daher immer in Bezug auf die schützenswerten Güter zu bemessen. Im Falle der personenbezogenen Daten ist ihr Bedrohungsrisiko je nach Datenart und nicht immer direkt monetär zu beziffern. Schwachstellen, die hier ausgenutzt werden können, sind zu leichte Zugänge zu den Servern (z. B. durch schwache Passwörter), unzureichend geschützte Zugänge zu den Daten (offene Netze) und das Nutzerverhalten (z. B. der Verzicht kryptografischer Verfahren). Die Anforderung eines Schutzes an Privatheit lässt sich so in folgende funktionale Sicherheitsanforderungen zerlegen: Vertraulichkeit und Zweckbindung der Daten, sowie Vertrauenswürdigkeit der anderen Parteien und eine funktionsintegre Verfügbarkeit der Daten.

Im nächsten Schritt wird ein Sicherheitskonzept entwickelt. Eine erste Sicherheitsmaßnahme ist die Nutzung von starken Passwörtern, von Verschlüsselung beim Mailen, Chatten und im Web. Ferner sollte der Nutzer durch Kenntnis der Datenschutzprinzipien darauf achten, dass er nur ausgewählte Inhalte kommuniziert und diese mit Bedacht weitergibt. Weiterhin sind Sicherheitseinstellungen vorzunehmen und Schutzmechanismen zu nutzen, etwa alternative Suchmaschinen oder das regelmäßige Löschen von Cookies und des Browserverlaufs.

Der letzte Schritt ist die Installation eines Sicherheitskonzepts. Es dient dem Internetnutzer, diejenigen Sicherheitsmechanismen des Selbstdatenschutzes

auszuwählen, die ihm ein adäquates Sicherheitsniveau bieten. Dabei muss er das verbleibende Restrisiko erkennen, akzeptieren und entscheiden, inwieweit er den Partnern, von denen er dann noch abhängt, vertraut. Hier ist die Handlungsfähigkeit in der Datenschutzkompetenz gefragt.

2 Von der Risikobewertung in einem Medienkompetenzmodell zu einem Datenschutzkompetenzmodell

In [SGG07] stellen Six und Gimmler ein Medienkompetenzmodell vor, das – wie Gimmler in [Gi12] schon zeigt – Datenschutzkompetenz in einem gewissen Maß zu beschreiben vermag. Aber eine Betrachtung des Risikos bei der Internetnutzung unterbleibt an dieser Stelle. Folgende Dimensionen aus dem Medienkompetenzmodell spielen bei der Risikobewertung eine Rolle:

Hintergrundwissen ist notwendig, da zur Abschätzung des Risikos der Internetnutzung die möglichen Schadensursachen und ihrer Gegenmittel ja bekannt sein müssen. Die Nutzung alternativer Softwareprodukte, z. B. alternativer Suchmaschinen und Verschlüsselungsmethoden, und die eigene Entscheidung über die Datenpreisgabe sind Datenschutzmaßnahmen, die der Nutzer ergreifen kann, wenn er sie kennt. Ferner zählen wir zu dieser Dimension auch das Wissen über die Prinzipien des Datenschutzes und deren Bedeutung und Anwendung.

Der Selbstdatenschutz verlangt Orientierungswissen, weil der Nutzer die Funktionen der Angebote verstehen muss. Er muss in der Lage sein, diese Funktionen in der Anwendungsumgebung, in der er sich befindet, sicher und wirkungsgemäß auszuführen.

Der Nutzer kennt die Angebote, kann die angemessenen auswählen und setzt sie aus dieser Orientierungssicherheit heraus situationsgerecht ein. Ferner kennt er Möglichkeiten, um sich weitere und neue Informationen zu erschließen.

Zur Urteilskompetenz zählt die Fähigkeit, die Angebote im Internet zu kennen und deren Wirkung zu beurteilen. Zusätzlich muss sich der Nutzer bei der Abwägung des Risikos ein Urteil über die Vertrauenswürdigkeit der anderen Kommunikationsteilnehmer bilden. Auf der Basis der Urteilsentscheidung nimmt der Nutzer das Angebot an oder lehnt es ab.

Durch die Auswahl- und Nutzungskompetenz kommt der Nutzer zu der „selbstbestimmten, zielorientierten und reflektierten Auswahl und Nutzung“ [Gi12] des Internetangebots. In risikobehafteten Situationen urteilt der Nutzer, ob er das Risiko eingehen wird oder nicht. Durch die passende Auswahl und Nutzung von Schutzmechanismen kann der Nutzer das Risiko minimieren.

Die Dimensionen des Medienkompetenzmodells sind nicht völlig unabhängig voneinander (bspw. Aspekte von Urteil und Orientierung), daher ist es hilfreich, einzelne Kompetenzaspekte mehrfach zuzuordnen. Die auf die ausgewählten Dimensionen des

Medienkompetenzmodells angewendete Risikointerpretation führt zu einer Erweiterung des Modells, welches als Datenschutzkompetenzmodell aufgefasst werden kann. Damit definieren wir Datenschutzkompetenz als den Zusammenschluss von Hintergrundwissen, Orientierungswissen, Urteilskompetenz, Handlungs- und Nutzungskompetenz, Risikobewertungskompetenz und die Anwendung von Handlungsmustern mit Bezug auf das schützenswerte Gut der persönlichen Daten.

3 Zusammenfassung und Ausblick

Eine datenschutzbewusste Internetnutzung ist gekennzeichnet durch die bewusste Ausübung des Selbstdatenschutzes im Rahmen des wahrgenommenen bestehenden Systemdatenschutzes und seiner Vertrauenswürdigkeit bei gleichzeitig kompetenter Abwägung des Restrisikos. Aufgrund des Medienkompetenzmodells von Six/Gimmler [SGG07], das Teilkompetenzen bzgl. des Datenschutzes aufzeigt, aber Risikobewertung außer Acht lässt, wurde das Modell zu einem Datenschutzkompetenzmodell erweitert. Die Validität dieses Modells soll im Rahmen einer weiteren Forschung untersucht werden. Auf Basis der Modellvorlage wird eine Schülerbefragung mit dem Schutz der Privatsphäre als Schwerpunkt durchgeführt, sodass aufgrund dieser Ergebnisse später konkrete Handlungsempfehlungen für Unterrichtsinhalte entwickelt werden.

4 Literaturverzeichnis

[GB15] Grimm, R.; Bräunlich, K.: Vertrauen und Privatheit. Anwendung des Referenzmodells für Vertrauen auf die Prinzipien des Datenschutzes. In Datenschutz und Datensicherheit - DuD, 2015, 39; S. 289–294.

[Gi12] Gimmler, R.: Medienkompetenz und Datenschutzkompetenz in der Schule. In Datenschutz und Datensicherheit - DuD, 2012, 36; S. 110–116.

[Gr16] Grimm, R. et al.: Referenzmodell für ein Vorgehen bei der IT-Sicherheitsanalyse. In Informatik-Spektrum, 2016, 39; S. 2–20.

[MDS95] Mayer, R. C.; Davis, J. H.; Schoorman, F. D.: An Integrative Model of Organizational Trust. In Academy of Management Review, 1995, 20; S. 709–734.

[SGG07] Six, U.; Gleich, U.; Gimmler, R. Hrsg.: Kommunikationspsychologie -- Medienpsychologie. Lehrbuch. BeltzPVU, Weinheim, 2007.