BETRIEBLICHE KOOPERATIONSUNTERSTÜTZUNG BEI DYNAMISCHER VERTRAUENSBASIS - DATENSCHUTZANALYSE UND SOZIO-TECHNISCHE LÖSUNGSANSÄTZE

Schriftliche Prüfungsarbeit für die Master-Prüfung des Studiengangs Angewandte Informatik an der Ruhr-Universität Bochum

vorgelegt von
MARTIN DEGELING

Prof. Dr-Ing. Thomas Herrmann
Dr. Kai-Uwe Loser

Juni 2010

Martin Degeling: *Betriebliche Kooperationsunterstützung bei dynamischer Vertrauensbasis - Datenschutzanalyse und sozio-technische Lösungsansätze,* Juni 2010

LaTeX-Vorlage auf Basis von CLASSICTHESIS von Andrè Miede
http://www.ctan.org/tex-archive/macros/latex/contrib/classicthesis/

Dank an alle Korrekteur_innen, Hinweisgeber_innen, Lebensabschnitts-gefährt_innen, Erzeuger_innen, die Familie, Expert_innen, Professor_innen, Betreuer_innen, Freund_innen und alle anderen für den ganzen F.U.N.

ABSTRACT

This thesis deals with privacy problems in colaborative systems. The focus is on the usage of those systems, while respecting the dynamics of trust in small groups and their effect on the informational self-determination of the users. Three scenarios have been developed to describe these problems. In addition, possible solution have been discussed with privacy experts. The solutions are summarized in the categories *limited disclosure*, *access rights*, *usage context* and *user-centered actions* and offer socio-technical design options to strengthen the informational self-determination of the users.

ZUSAMMENFASSUNG

Diese Arbeit beschäftigt mit Datenschutzproblemen bei betrieblichen Kooperationssystemen, die die informationelle Selbstbestimmung der Mitarbeiter_innen negativ beeinflussen können. Der Fokus liegt dabei auf den wenig beachteten Problemen, die, bedingt durch dynamische Vertrauensverhältnisse in wenig strukturierten Gruppen, zwischen den Nutzer_innen auftreten. Zu diesem Zweck werden in dieser Arbeit Szenarien beschrieben, die in einem Workshop zum Thema erarbeitet wurden. Nach der Diskussion mit Datenschutzexpert_innen sind Maßnahmen in den Kategorien *Erhebungsbegrenzung, Zugriffsberechtigungen, Nutzungart* und *nutzer_innenzentrierte Maßnahmen* in Bezug auf die Szenarien diskutiert und evaluiert worden, die verschiedene Ansätze bieten die informationelle Selbstbestimmung der Nutzer_innen zu stärken.

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

ACRONYMS

ACL Access Control Liste

ACP Access Control Policy

BetrVG Betriebsverfassungsgesetz

BDSG Bundesdatenschutzgesetz

BSCW Basic Smart, Cooperate Worldwide

BSI Bundesamt für Sicherheit in der Informationstechnik

BVerfG Bundesverfassungsgericht

CAPTCHA Completely Automated Public Turing test to tell Computers and Humans Apart

CSCW Computer Support Cooperative Work

DLP Data Loss Prevention

DHP Data Handling Policy

DSB Datenschutzbeauftrage_r

DuD Datenschutz und Datensicherheit

ELICT Exploit Latent Information to Counter Insider Threats

EU Europäische Union

ILO International Labor Organisation

MCI Mensch Computer Interaktion

IDS Intrusion Detection System

IPS Intrusion Prevention System

IKT Informations- und Kommunikationstechnologien

ISMS Informationssicherheits-Managementsysteme

OTR Off-The-Record Messaging

PET Privacy Enhancing Technologies

RBAC Role-Based Access Control

SBD Scenario-based Design

TAIDA TRACK, ANALYSE, IMAGE, DECIDE, ACT

TMAC Team Based Access Control

TTP Trusted Third Party

VCS Version Control System

VoIP Voice over IP

XP Extreme Programming

1 EINLEITUNG

Diese Arbeit setzt sich mit Datenschutzproblemen auseinander, die mit der Nutzung von Kooperationssystemen in Unternehmen zusammenhängen.

In den letzten Jahren hat die Nutzung von elektronisch gestützten Kooperationssystemen stark zugenommen. Der Computer entwickelte sich vom Werkzeug zur Verarbeitung von Informationen über ein Kommunikationsmedium zum Allround-Gerät zur Kommunikation, Koordination und Kooperation. Schümmer and Lukosch (2007) beschreiben dies als den Wechsel von der *Mensch-Computer Interaktion* zur *Computervermittelten menschlichen Interaktion*. Gleichzeitig änderten und ändern sich die Arbeitsbedingungen. Von Wissensarbeiter_innen[1] wird nicht nur hohe fachliche, sondern auch soziale Kompetenz erwartet, die sich in Anforderungen wie Teamfähigkeit, Flexibilität und Integrität widerspiegeln und computervermittelt unterstützt werden sollen. In vielen Unternehmen ersetzt Projektarbeit in Gruppen mit flachen Hierachien das klassische Top-Down-Management. Agile Entwicklungsmethoden wie Extreme Programming (XP) oder *Scrum* in der IT-Branche sind konkrete Ausprägungen dieser Verhältnisse, aber nach Klotz (2009), noch nicht das Ende der Entwicklung.

Computervermittelte Zusammenarbeit im Arbeitsalltag immer wichtiger.

Die hohen Kooperations- und Kollaborationsanteile der Arbeit setzen voraus, dass (personenbezogene) Daten mittels der technischen Systeme mit den Kolleg_innen geteilt werden. Vertrauen zwischen den Beteiligten ist dazu zwingend notwendig. Da die internen Strukturen der Arbeitsgruppen aber meist nur geringen Formalisierungen unterworfen sind, ist auch die Vertrauensbasis dynamisch. Unstimmigkeiten und Missverständnisse lassen sich nicht vermeiden. Dass dabei die personenbezogenen Daten aus den Kooperationssystemen zu anderen Zwecken als den anfänglich geplanten genutzt werden können, ist eine Einschränkung der informationellen Selbstbestimmung der Betroffenen.

1.1 ANFORDERUNGEN AN DEN DATENSCHUTZ

Mit den beschriebenen Veränderungen wachsen auch die Anforderungen an den betrieblichen Datenschutz. In den benutzen Groupwaresystemen wird eine Vielzahl personenbezogener Daten gesammelt, von E-Mails über gemeinsam bearbeitete Dokumente hin zu gemeinsamen Terminkalendern. Bei guter Zusammenarbeit mit gegenseitigem Vertrauen ist der Zugriff auf die personenbezogen Informationen, die dazu geeignet sind, das Verhalten und die Persönlichkeit der Informationsherausgeber_innen zu beschreiben, nicht nur gestattet, sondern meist auch notwendig. Wandelt sich das Vertrauen, durch Konkurrenz oder Unzufriedenheit, in Misstrauen sind auch personenbezogene Daten nicht mehr nur Mittel zur Kooperationsunterstützung, sondern auch Quelle für die missbräuchliche Nutzung. Eine unterhaltsame E-Mail über das letzte Meeting mit einem kleinen Witz über die Krawatte

Wachsende Datensammlungen erfordern wachsende Anstrengungen beim betrieblichen Datenschutz

1 Wissenarbeiter_innen oder *Knowledge Worker* sind nach Davenport (2005) hoch ausgebildete Arbeiter_innen deren Arbeitsweise sich durch Einzelarbeit und kollaborative Phasen kennzeichnet und technisch Unterstütz wird.

des Chefs wird - an eben diesen weitergeleitet - ein Instrument zur Diffamierung und Bloßstellung.

1.2 BEISPIELE

Dass das Bewusstsein für diese Dynamik vorhanden ist, zeigt eine Studie von Brush et al. (2009). Sie berichtet, dass nur eine Minderheit der amerikanischen *Knowledge Worker* etwas dagegen hat, wenn ihre Stammdaten - also Name, Stellung und Kontaktdaten - im Inter- oder Intranet veröffentlicht werden. Genauso wenig Bedenken haben sie bei Terminen und dem Login-Status am Rechner. Sie sind sich über den Vorteil dieser Mechanismen zur besseren Koordinierung bewusst. Dass letztere Daten aber möglicherweise noch eine Woche nachdem sie ihre Aktualität verloren haben verfügbar und einsehbar sind, gefällt den Wenigsten.

Aus der Tagesspresse

EIN EXEMPLARISCHER FALL ereignete sich im Süden Deutschlands am Anfang des Jahres 2010: Ein Mitarbeiter der EDV-Abteilung eines Rathauses in einer kleinen Stadt in der Nähe von Augsburg war nach seinem Urlaub unzufrieden mit der Leistung seiner Urlaubsvertretung. Über Surf-Protokolle fand er heraus, dass seine Vertretung während der Arbeitszeit überwiegend privat im Internet unterwegs war. Eine Beschwerde darüber bei einer höheren Stelle führte zu einer Ermahnung des Surfers. Diese Strafe war dem Administrator aber nicht scharf genug. Nach einem länger andauernden internen Konflikt kündigte er und verschickte an alle Mitarbeiter_innen im Rathaus Auszüge aus Chat-Protokollen, sowie zu diesem Zeitpunkt bereits gelöschte E-Mails und Fotos des von ihm Beschuldigten, um seine Vorwürfe zu untermauern.[2]

IM APRIL 2010 ereignete sich ein weitere beispielhafter Fall kurz vor der Landtagswahl E-Mails an die Presse weitergeleitet worden, die einen Vertrauten des Ministerpräsidenten wegen dessen ausfallenden-den Bemerkungen über Dritte in Bedrängnis brachten.[3]

Cyber-Bullying nimmt seit Jahren zu

HANDLUNGSBEDARF sah auch 2007 die größte britische Gewerkschaft *Unite* mit dem Ministerium *business, innovation and skills*. Da die Anzahl der Fälle, in denen Kooperationssysteme missbräuchlich gegen Kollegin_innen eingesetzt werden, in den letzten Jahren gestiegen ist, hat sie die Kampagne Dignity at work ins Leben gerufen. Sie widmet sich der Aufklärung des Themas *Cyber-Bullying* - das Mobbing mittels Groupwaresystemen.[4]

1.3 ZIEL DIESER ARBEIT

Ziel dieser Arbeit ist es, die wenig betrachteten Implikationen von dynamischen Vertrauensverhältnissen im betrieblichen Kontext von Kooperationssystemen aus Datenschutzsicht zu beleuchten. Die Möglichkeiten bestehender Datenschutztechnologien und -maßnahmen werden

2 Eine rechtliche Prüfung der Vorgänge steht zwar noch aus, aber die lokalen Medien berichteten ausführlich über den Vorfall. Vergleiche u.a. Zeitungsberichte von Stölzle (2010) und Dirner (2010) abgerufen am 23.02.2010

3 Nachzulesen bei Blasius (2010) (abgerufen am 20.05.2010)

4 vgl. http://www.dignityatwork.org Abgerufen am 28.05.2010

vorgestellt und auf ihre Anwendbarkeit hinsichtlich der Themenstellung überprüft, sowie Vorschläge erarbeitet wie mit den Problemen umgegangen werden können, um missbräuchlich Nutzung zu verhindern und die informationelle Selbstbestimmung der Betroffenen zu gewährleisten.

IN KAPITEL 2 sind die Grundlagen von Groupwaresystemen zur Kooperations- und Kollaborationsunterstützung zusammengefasst, sowie datenschutzrechtliche Aspekte und verschiedene Arten von Vertrauen erläutert.

IN KAPITEL 3 werden Szenarien entwickelt, die die Probleme des Status Quo veranschaulichen. Diese Szenarien werden vorgestellt und mit Bezug auf den Kontext dieser Arbeit analysiert.

IN KAPITEL 4 werden technische und organisatorische Maßnahmen aus unterschiedlichen Bereichen kategorisiert und vorgestellt, die in Expert_innen-gesprächen diskutiert wurden, sowie ein Überblick über den Stand der Forschung gegeben.

IN KAPITEL 5 schließlich werden einzelne der im vorherigen Kapitel vorgestellten Maßnahmen auf die Szenarien angewendet und angepasst.

ZUM SCHLUSS fasse ich die Ergebnisse zusammen, zeige Mängel der bestehenden Möglichkeiten auf und gebe Empfehlungen, was getan werden kann um die Probleme zu lösen.

ABGRENZUNG Datenschutzfragen werden in vielen Forschungsrichtungen behandelt. Diese Arbeit beschäftigt sich nur am Rande mit den juristischen Kontexten, da angenommen wird, dass in die Nutzung betrieblicher Kooperationsunterstützungssysteme von den Mitarbeiter_innen eingewilligt wurde. Viele Quellen stammen aus dem Forschungsfeld des Computer Support Cooperative Work (CSCW), der Mensch Computer Interaktion (MCI) und IT-Sicherheit oder der Organisationspsycholgie. Da der Fokus auf der Datenschutzproblematik im Rahmen der eingesetzten technischen Systeme liegt, kann diese Arbeit in das erstgenannte Feld eingeordnet werden.

2 VERARBEITUNG PERSONENBEZOGENER DATEN IN UNTERNEHMEN

In diesem Kapitel werde ich näher auf die Datenverarbeitung in Unternehmen eingehen. Dabei werden Aspekte des Datenschutzes auf technischer und organisatorischer sowie (persönlichkeits-)rechtlicher Ebene betrachtet, die im betrieblichen Kontext mit der Verwendung von *sozio-technischen* Systemen relevant sind. Dabei will ich zuerst den theoretischen Hintergrund der informationellen Selbstbestimmung beschreiben und auf die Verhältnisse am Arbeitsplatz anwenden. Die organisationspsychologischen Einflussfaktoren des Vertrauens in Gruppen werden dann zum Ende dieses Kapitels mit den technischen Systemen und den darin verarbeiteten personenbezogenen Daten in Verbindung gesetzt.

2.1 GRUNDLAGEN DER INFORMATIONELLEN SELBSTBESTIMMUNG

Datenschutz dient der informationellen Selbstbestimmung. Man nimmt an, dass nur unter der Bedingung, dass eine Person die Möglichkeit hat zu wissen, was andere über sie wissen, diese ihre Persönlichkeit frei entfalten kann. Rössler (2001) beschreibt ausführlich in wie weit eine Verletzung der *informationellen Privatheit*[5] die Entwicklung einer Persönlichkeit beschränken können. Wird eine Person darüber getäuscht was andere über sie wissen, wird dadurch ihre informationelle Privatheit verletzt und ihre informationelle Selbstbestimmung eingeschränkt, was die Handlungsmöglichkeiten und damit die Autonomie eben jener Person einschränkt. In Gruppen bezeichnet man diese Vorgänge nach Goffman (1974) als *Kollusionen*.

informationelle Privatheit ist Voraussetzung für Autonomie

> Ein *kollusives Netz* oder eine *kollusive Gruppierung* ist eine Koalition mit dem Ziel einer speziellen Art von Kontrolle, nämlich der Kontrolle der Situationsdefinition der dritten Partei.[6]

Schätzt eine Person ihre Situationsdefinition, also ihre Annahmen darüber, was andere über sie wissen und denken, falsch ein, weil die Kollusoren sie absichtlich darüber täuschen, beruhen in der Folge alle Entscheidungen, die sie in diesem Rahmen trifft, auf falschen Annahmen. Ihre Entscheidungsfreiheit ist eingeschänkt, weil sie manche Entscheidungsmöglichkeiten auf Grund ihrer falschen Situationsdefintion, ihrer getäuschten Wahrnehmung der Verhältnisse, nicht sehen konnte.

EIN BEISPIEL Eine Mitarbeiterin namens Ann-Christin ist neues Mitglied einer Arbeitsgruppe, die schon länger besteht. Da sie mit den Aufgaben noch nicht so vertraut ist, lässt sie sich gerne anleiten und fragt,

5 Eine der bekannte Definitionen von Privatheit, auf die die Autorin verweist ist die von Westin (1967) *„the claim of individuals, groups or institutions to determine themselves when, how, and to what extent information about them is communicated to others"*. Informationelle Privatheit ist nach Rössler einer von drei Privatheitsaspekten. Daneben existiert *dezisionale Privatheit*, die sich auf Handlungs- und Entscheidungsspielräume bezieht, sowie die *lokale Privatheit*, die die räumliche Privatheit bezeichnet.

6 Goffman (1974) S. 438

wenn etwas erledigt ist, ob es den Ansprüchen (z.B. der Chefin oder der Gruppe) genügt. Eine Kollusion liegt dann vor, wenn die übrigen Gruppenmitglieder Ann-Christin täuschen, in dem sie beispielsweise eine schlechte Lösung gegenüber Ann-Christin als besonders gut loben und in ihrer Abwesenheit verbreiten, dass diese nicht in der Lage sei, die Aufgaben angemessen zu erfüllen. Sie geben also Ann-Christin andere Informationen über ihre Situation als der Umwelt. Stellt Ann-Christin zu einem späteren Zeitpunkt nun fest, dass sie getäuscht wurde - dabei kann der Grad der Täuschung auch nur ein leichter sein - ist doch ihre Selbstdefinition über ihren Status in der Gruppe hinfällig, da sie sich nicht darauf verlassen kann, dass andere Dinge, die ihr mitgeteilt wurden, der Wahrheit entsprechen und entsprochen haben.

Es ist nachvollziehbar, dass solche Verhaltensweisen massiv das Vertrauen zwischen den länger Beschäftigten (den Kollusoren) und Ann-Christin (der exkolludierten Person) stören. Da Vertrauen aber einer der wichtigsten Faktoren jeglicher - und im wesentlichen auch betrieblicher - Kooperation ist (vgl. Kapitel 3), ist eine gute Zusammenarbeit in dieser Konstellation nach der Störung des Vertrauensverhältnisses kaum vorstellbar.

2.2 DAS RECHT AUF INFORMATIONELLE SELBSTBESTIMMUNG

Die Aufnahme des Rechts auf informationelle Selbstbestimmung, dass der beschriebenen Notwendigkeit der Kontrolle über die eigene Situationsdefinition Rechnung trägt, in die Liste der Persönlichkeitsrechte erfolgte in Deutschland im Urteil des Bundesverfassungsgericht (BVerfG) zur Volkszählung 1983.[7] Es leitet dieses Recht aus dem ersten und zweiten Artikel des Grundgesetzes ab - dem Schutz der Menschenwürde und das Recht auf freie Entfaltung der Persönlichkeit. In dem Urteil stellten die Richter_innen fest, dass die Ungewissheit darüber, wer was in welcher Situation weiß und ob das eigene Verhalten dauerhaft protokolliert werden, den oder die Einzelne wesentlich in seiner oder ihrer Entfaltungschance beeinträchtige. Die Möglichkeiten zur freien, persönlichen Entfaltung seien aber sowohl für das Gemeinwohl als auch für das Funktionieren eines demokratischen Staates notwendig.

Im Volkszählungsurteil ist das Recht auf informationelle Selbstbestimmung gegründet

Das Recht auf informationelle Selbstbestimmung dient also einer Stärkung der informationellen Privatheit und soll so gewährleisten, dass der_die Einzelne über die korrekte Situationsdefintion verfügt.

Nun handelt es sich bei den Grundrechten um Schutzrechte des oder der Einzelnen vor den Eingriffen des Staates - im konkreten Fall gegenüber der geplanten Volkszählung - und nicht um Regelungen für Verhältnisse zwischen Privatpersonen. Trotzdem hat das Urteil des BVerfG und das Recht auf informationelle Selbstbestimmung wegen seiner Grundsätzlichkeit Einzug in andere Rechtsbereiche - so auch das Arbeitsrecht - gehalten. In einem Arbeitsverhältnis müssen zusätzlich die Interessen des_der Arbeitgebers_in, ein Unternehmen effizient zu gestalten, berücksichtigt werden und gegen die Rechte der Angestellten, die mit der_dem Arbeitgeber_in einen Vertrag eingegangen sind, abgewogen werden. *Das berechtige Informationsinteresse des Arbeitgebers [...] [ist] mit dem informationellen Selbstbestimmungsrecht der Beschäftigten [in] einen verhältnismäßigen Ausgleich zu bringen.*[8] Um dies zu gewährleisten wird den Arbeiternehmer_innenvertretungen ein Mit-

Es hat auch Gültigkeit im Arbeitslebne

7 vgl. BverfG 65
8 Däubler (2002) 3 Abs. 95

bestimmungsrecht eingeräumt bei der *Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen oder zu protokollieren* (§87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG))

Ähnliche Regelungen finden sich auch auf anderen juristischen Ebenen, etwa in der Datenschutzrichtlinie 95/46/EG[9] der Europäische Union (EU). Auf Grund dieser Richtlinie wurde 1995 die *Artikel-29-Datenschutzgruppe* als Beratungsgremium der EU-Kommission eingeführt. Diese formuliert folgenden Anspruch für den Arbeitnehmer_innen-Datenschutz:

> Arbeitnehmer geben ihr Recht auf Schutz der Privatsphäre und Datenschutz nicht allmorgendlich am Werkstor oder an der Bürotür ab. Sie haben eine berechtigte Erwartung, dass ihre Privatsphäre am Arbeitsplatz bis zu einem gewissen Grad gewahrt bleibt, da sie hier einen erheblichen Teil ihrer Beziehungen zu anderen Menschen entfalten. Dieses Recht muss jedoch gegen andere schutzwürdige Rechte und Interessen abgewogen werden. Dies gilt insbesondere für das Recht des Arbeitgebers, sein Geschäft bis zu einem gewissen Maß effektiv zu betreiben und vor allem für sein Recht, sich selbst vor der Haftung oder dem Schaden zu schützen, die das Verhalten seiner Arbeitnehmer verursachen kann. Diese Rechte und Interessen stellen einen legitimen Grund dar, der geeignete Maßnahmen zur Einschränkung des Rechts der Arbeitnehmer auf Schutz der Privatsphäre rechtfertigen kann. (vgl. Artikel-29-Datenschutzgruppe (2002))

2.3 DATENSCHUTZPRINZIPIEN

Sieben Datenschutzgrundregeln

Zur Gewährleistung der Rechte der Arbeitnehmer_innen sind international einige, aus den jeweiligen Datenschutz- bzw. Privacyrechten abgeleitete worden. Sie sind konkrete Gestaltungsprinzipien für den Einsatz von datenverarbeitenden Systemen und haben sich als Richtlinien bei der Überprüfung der Rechtskonformität bewährt.[10] Die folgende Liste nach Bizer (2007) bezieht sich auf das deutsche Recht und soll im Folgenden mit der Problemstellung in Verbindung gebracht werden.

RECHTMÄSSIGKEIT Für die Erhebung und Verarbeitung von personenbezogenen Daten gilt in Deutschland die *Verbotsvermutung mit Erlaubnisvorbehalt*. Einer öffentlichen Institution ist es damit nur erlaubt personenbezogene Daten zu erheben, wenn es eine gesetzliche Vorschrift erlaubt.[11] Für den nicht-öffentlichen Bereich, also die Privatwirtschaft, muss eine Einwilligung vorliegen. Für Angestellte gilt dabei meist der Arbeitsvertrag als initiale Einwilligung, bei Änderungen der Erhebung, z.B. durch Einführung einer neuen Software, werden zudem in Betriebsvereinbarungen mit

9 Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr EU-Parlament (1995)

10 Bizer (2007) fasst das Bundesdatenschutzgesetz (BDSG) zu einer griffigen Liste zusammen; Die europäische Kommission beschreibt ähnliches in der Richtlinie 95/46/EC Directive (1995) vgl. eine inhaltliche Auseinandersetzung damit in Elgesem (1999). In Amerika firmieren ähnliche Prinzipien unter dem Titel *Fair Information Practice Principes*, herausgegeben vom Verbraucherschutzministerium; vgl. dazu Brush et al. (2009)

11 Neben dem BDSG sind solche Erlaubnisse in diversen Einzelnormen vorhanden

den Betriebs- und Personalräten Regelungen ausgehandelt. Die Nutzung von Groupware widerspricht dieser Vorschrift in der Regel nicht, da ihr vordergründiges Ziel, die Unterstützung der Zusammenarbeit, auch Zustimmung bei den Betroffenen findet.

EINWILLIGUNG Eine Einwilligung muss stets informiert und freiwillig erfolgen. Die Betroffenen müssen ausreichend über den Zweck der Datenverarbeitung informiert sein. In Unternehmen wird diese Einwilligung durch den Arbeitsvertrag und entsprechende Betriebsvereinbarungen gegeben. Zusätzlich muss es die Möglichkeit zum Widerspruch geben, auch wenn dies meist nur in Form einer Kündigung möglich ist.

ZWECKBINDUNG Die erhobenen Daten dürfen nur für den Zweck, in den eingewilligt wurde, verarbeitet werden. Ändert sich der Zweck, ist eine erneute Einwilligung notwendig. Allerdings sind die Zwecke, gerade bei der Nutzung von Groupware, nur ungenau zu beschreiben, außerdem sind sie nicht immer vollständig absehbar. Angenommen werden kann aber, dass Kollusionen kein Zweck sind, in den eingewilligt wird und es sich hierbei um eine missbräuchliche Nutzung handelt.

ERFORDERLICHKEIT Die datenschutzkonforme Gestaltung von Informationtechnischen Systemen setzt voraus, dass alle erhobenen Daten auch für den Betrieb des Systems erforderlich sind. Dabei muss abgewogen werden zwischen einer absolut minimalen Datenerhebung (Datensparsamkeit) und einer größeren Menge an zusätzlichen Daten, die für den effektiveren Betrieb nützlich sind. Diese Abwägung ist nicht immer einfach, da von der geplanten Nutzung abhängig ist, welche Datenmenge die optimale Unterstützung gewährleistet. Zusätzlich kann nur schwer eingeschätzt werden wie sich die Nutzung über die Zeit ändert oder welche Rückschlüsse sich aus einer großen Datenmenge zusätzlich ziehen lassen, die vor der Einführung der Software noch nicht absehbar waren. Der Grundsatz der Erforderlichkeit schließt auch ein, dass Daten, die nicht mehr erforderlich sind, unverzüglich gelöscht werden

TRANSPARENZ Für den_die Betroffene_n muss transparent sein, wann personenbezogene Daten erhoben, verarbeitet oder weitergegeben werden. Darüber hinaus besteht ein Auskunftsrecht, d.h. es müssen Möglichkeiten geschaffen werden, eine Übersicht über die gespeicherten Daten zu bekommen. Dies dient (im Sinne der informationellen Selbstbestimmung) dazu, das eigene Selbstbild mit dem abzugleichen, das andere, mit Hilfe der Kenntnis der gespeicherten Informationen, erlangen können. Transparenz bedeutet in dem Fall aber nicht nur, eine listenförmige Übersicht über die gespeicherten Informationen zu bekommen, sondern im Idealfall auch Kenntnis darüber zu erlangen, welche zusätzlichen Informationen sich ableiten lassen und welche Gefahren von ihnen ausgehen. Die Komplexität der Informationen adäquat darzustellen, ohne die Transparenz für die Betroffenen durch Überforderung gleich wieder einzuschränken, ist eine Herausforderung.

DATENSICHERHEIT Datenschutz kann nur gewährleistet werden, wenn die gespeicherten Daten auch im Sinne der Datensicherheit ge-

schützt sind. Datensicherheitsprinzipien sind etwa VERTRAULICHKEIT - sicherzustellen, dass nur Berechtigte Zugriff auf die Daten bekommen -, VERFÜGBARKEIT - zu gewährleisten, dass die Daten verfügbar sind , wenn sie benötigt werden - und INTEGRITÄT - die Gewährleistung des Schutzes vor unerlaubten Veränderungen. Diese muss durch geeignete technische und organisatorische Maßnahmen, wie sie auch in dieser Arbeit vorgestellt werden, gewährleistet werden.

KONTROLLE Das BDSG sieht interne und externe Aufsichtsbehörden in Form von Datenschutzbeauftragten vor, die die Verarbeitung personenbezogener Daten kontrollieren sollen.

2.4 TECHNISCHE SYSTEME ZUR GRUPPENUNTERSTÜTZUNG

Wie bereits in der Einleitung beschrieben, werden in Unternehmen an vielen Stellen Daten über die Mitarbeiter_innen erhoben und gespeichert. Zusammen mit der Verbreitung des Computers als universales Kommunikations- und Kooperationsmedium sind auch die Möglichkeiten gewachsen, die Erhebung und Auswertung der gesammelten und produzierten Daten zu automatisieren. Diese Arbeit beschäftigt sich dabei vor allem mit Systemen, bei denen personenbezogene Daten im Rahmen der Nutzung der Systeme zur Organisation von Gruppen und zur technisch vermittelten Kommunikation und Zusammenarbeit anfallen. Personalinformationssysteme oder Überwachungssysteme, die Daten *über* Angestellte sammeln und Verwaltungs- und Abrechnungszwecken beziehungsweise der Leistungs- und Verhaltenskontrolle dienen, sind nicht Teil dieser Arbeit.[12] Die betrachteten Systeme werden im Folgenden unter dem Begriff GROUPWARE [13] zusammengefasst und lassen sich den Kategorien *Kommunikation*, *Koordination* oder *Kooperation* zuordnen, wobei ein Werkzeug nie eindeutig nur einer Kategorie zugeordnet werden kann (vgl. Abbildung 1). Überwiegend zur ersten Kategorie gehören beispielsweise Telefon- und E-Mail-Systeme, die vornehmlich der Kommunikation dienen, über die man sich aber auch mit den Kommunikationspartner_innen koordinieren kann. Expliziter dem Zweck der Koordination dienen Terminkalender oder Gruppenwerkzeuge zur Aufgabenverwaltung. Wissens- und Dokumentenmanagement-Systeme wie etwa Wikis oder Multi-User-Editoren haben ihren Schwerpunkt im Bereich der Kooperationsunterstüzung und erlauben die computergestützte Arbeit am gemeinsamen Material. Die Zusammenarbeit wiederum ist aber nicht möglich ohne Absprachen zwischen den Kooperationspartner_innen, so dass auch hier ein Maß an Koordination notwendig ist.[14]

Es geht Systeme zur Kommunikation, Koordination und Kooperation

12 vgl. dazu Däubler (2002) §2; Natürlich fallen in den betrachteten Systemen ebenfalls Daten zur Leistungs- und Verhaltenskontrolle an. Die damit mögliche Mitarbeiter_innenüberwachung ist aber nicht im Fokus dieser Arbeit.

13 In dieser Arbeit werden die Software-Systeme unter dem Begriff GROUPWARE zusammengefasst. Eine detaillierte Begriffsbestimmung wie etwa bei Prilla and Ritterskamp (2010) die für Software zur Gruppenunterstützung die drei Felder GROUPWARE, CSCW und WEB 2.0 ausmachen, erfolgt hier nicht. Die verschiedenen Bereiche weisen zudem erhebliche Schnittmengen auf. Da diese Arbeit sich aber um Werkzeuge im Unternehmenskontext dreht, sind nur wenige Elemente aus den Bereichen WEB 2.0 bzw. SOCIAL SOFTWARE (Richter and Koch (2007)) enthalten.

14 Eine detailliertere, dimensionale Untergliederung von Werkzeugen und ihren Funktionen ist Thema in Abschnitt 3.2.3.

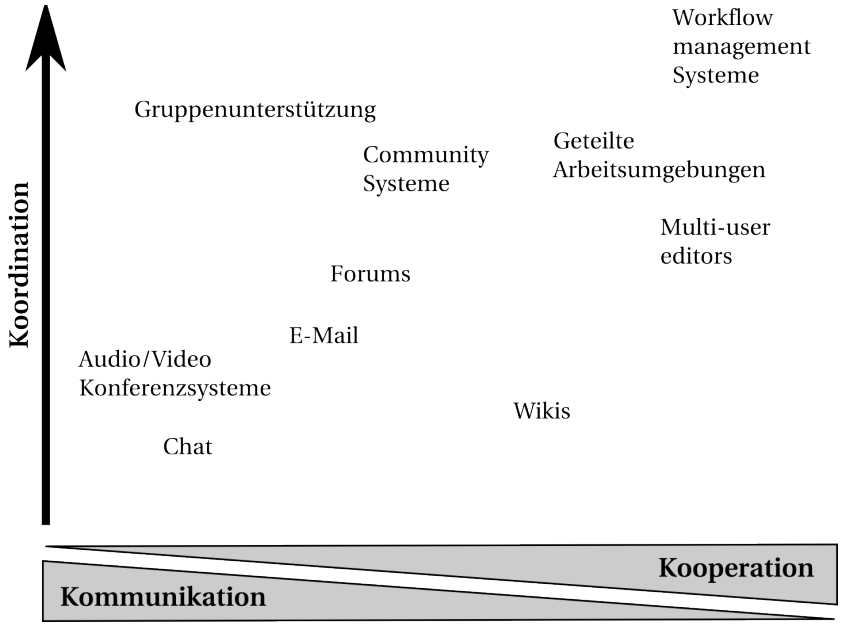


Abbildung 1: Funktionale Klassifikation von Groupwaresysteme nach Schümmer and Lukosch (2007) basierend auf Teufel et al. (1995)

2.5 DER EINFLUSS VON GROUPWARE AUF DIE INFORMATIONELLE SELBSTBESTIMMUNG

Zur Beschreibung des Einflusses von Groupware, und informationstechnischen Systemen generell, auf die informationelle Selbstbestimmung, ist das informationstheoretische Modell der ONTOLOGICAL FRICTION hilfreich. Floridi (2006) definiert persönliche Daten als Teil aller Informationen in der Infosphäre. In der Infosphäre sind alle Informationen vorhanden, aber ob und wie sehr sie denen, die die Informationen wahrnehmen, bekannt sind, hängt von der Reibung (FRICTION) innerhalb der Infosphäre ab. Neue Informations- und Kommunikationstechnologien (IKT), und dazu zählt auch Groupware, sind in den meisten Fällen vor allem dazu geeignet, die Reibung zu verringern und den Informationsfluss zu erhöhen und mehr Informationen der Infosphäre den Rezipient_innen zugänglich zu machen.

Als Vergleich dient eine Wohngemeinschaft, in der verschiedene Eigenschaften der Wohnung die Reibung in der Infosphäre beeinflussen. Die Tiefe und Festigkeit der Wände z.B. kann verhindern oder vereinfachen, dass Informationen aus Gesprächen aus dem einen in das andere Zimmer dringen. Genauso trägt auch das Material der Wände dazu bei; ob die Wände aus Stein oder aus Glas sind, macht für den Informationsfluss zwischen den Zusammenwohnenden einen wesentlichen Unterschied.

Groupware vereinfacht den Informationsfluss

Auf dieselbe Art trägt Groupware dazu bei, in Gruppen die Informationsflüsse zu vereinfachen und die Reibung zu verringern. Über die Statusanzeige eines Instant Messengers kann allen möglichen Kommunikationspartnern, unabhängig von deren Ort mitgeteilt werden, ob man gerade für ein Gespräch zur Verfügung steht oder nicht. Ein Gespräch kann zudem unabhängig vom Ort der Kommunizierenden geführt werden. Ohne diese Techniken, die die Reibung in der Infosphäre verringern, wäre es erforderlich, dass sich beide am selben Ort

treffen, um dann vielleicht festzustellen, dass einer der beiden keine Zeit für das Gespräch hat.

Die Vorteile der geringeren ONTOLOGICAL FRICTION führen aber gleichzeitig auch zu den oben beschriebenen Nachteilen in Bezug auf die informationelle Privatheit. Das IKT die Reibung verringern ist aber keinesfalls ein Automatismus. Sie können genauso dazu geeignet sein, die Verbreitung von Informationen, etwa personenbezogene, einzuschränken und die Reibung nur soweit zu verringern, dass ein Großteil der Vorteile, aber möglichst wenige Nachteile umgesetzt werden. Solche Technologien des technischen Datenschutzes werden unter dem Begriff der Privacy Enhancing Technologies (PET) zusammengefasst.

2.6 VERANTWORTUNG DER ARBEITGEBER_INNEN

Die Arbeitergeber_innen als VERANTWORTLICHE STELLE nach BDSG, als Betreiber_innen der Groupwaresysteme, sind für die Einhaltung der Datenschutzprinzipien bei der Nutzung von Groupwaresystemen verantwortlich. Zur ihrer Aufgabe zählt es damit auch für die Einhaltung des Zweckentfremdungsverbot zu sorgen.[15]

In den in Artikel-29-Datenschutzgruppe (2002) zitierten Verhaltenskodex der

International Labor Organisation (ILO) wird das wie folgt formuliert

Arbeitgeber_innen sind für die korrekte Nutzung der Daten verantwortlich

> Wenn personenbezogene Daten für andere Zwecke verarbeitet werden sollen als die, für die sie erhoben wurden, sollte der Arbeitgeber sicherstellen, dass sie nicht in einer mit dem ursprünglichen Zweck nicht zu vereinbarenden Weise verwendet werden. Er sollte die Maßnahmen treffen, die erforderlich sind, um jegliche Fehlinterpretation auf Grund eines geänderten Kontextes zu vermeiden.
>
> Personenbezogene Daten, die im Zusammenhang mit technischen oder organisatorischen Maßnahmen zur Gewährleistung der Sicherheit und des einwandfreien Funktionierens automatischer Informationssysteme erhoben werden, sollen nicht verwendet werden, um das Verhalten von Arbeitnehmern zu kontrollieren.

Zusätzlich stellt die Arbeitsgruppe fest

> Arbeitnehmer haben die berechtige Erwartung, dass ihre Privatssphäre am Arbeitsplatz gewahrt und nicht durch die Tatsache außer Kraft gesetzt wird, dass die Arbeitnehmer Kommunikationsgeräte oder andere geschäftliche Einrichtungen nutzen, die Eigentum des Arbeitgebers sind. (Artikel-29-Datenschutzgruppe, 2002, S. 9)

Die Nutzung der erhobenen Daten ist damit nicht nur für die Mitarbeiter_innenüberwachung untersagt, an denen die Arbeitergeber_innen möglicherweise selbst ein Interesse haben. Zusätzlich kann man aus diesen Aussagen auch die allgemeine Verantwortung der Arbeitgeber_innen ableiten, die informationelle Selbstbestimmung zu gewährleisten und damit auch die Zweckbindung der Daten für den Nutzungskontext selbst zu sichern. Zwar sind die Beziehungen zwischen den Mitarbeiter_innen nicht explizit Teil der beschriebenen Regelungen. Zu

15 vgl. §3 Abs. 129 in Däubler (2002)

verhindern, dass ein_e Mitarbeiter_in Daten benutzt, um einem_r Kollegen_in zu schaden, liegt, wenn er_sie dabei auf die Daten zugreift die von technischen Systemen für die Ziele des_der Arbeitgeber_in erhoben werden, damit auch im Verantwortungsbereich des_r Arbeitergeber_in.

2.7 VERTRAUEN IN ORGANISATIONEN

Die Probleme, die in dieser Arbeit behandelt werden, treten nach Einschätzung aller Befragten Expert_innen und Workshopbeteiligten vor allem in Gruppen[16] mit geringer Hierarchie auf. In solchen Konstellationen ist Vertrauen, so etwa Herrmann (2001) und Seifert and Pawlowsky (1998) ein wesentlicher Faktor, der die Koordinierung zwischen Mitgliedern der Gruppe erleichtert. Vertrauen fördert, wo stark formalisierte Strukturen fehlen, kooperatives und kommunikatives Verhalten und trägt so gerade bei Aufgaben mit einem hohen Anteil von Arbeitsteilung zum Erfolg eines Projektes bei. Vertrauen ist somit auch notwendig, um mittels Groupware effektiv kooperieren zu können.

Vertrauen ist Voraussetzung der Kooperation

Eine gute Zusammenfassung der Forschung zum Status des Vertrauens in Organisationen bietet Kramer (1999). Er beschreibt zwei verschiedene Modelle von Vertrauen. Die erste ist eine eher psychologische Beschreibung, die Vetrauen als Methode erklärt, wie Menschen in der Interaktion mit Unwägbarkeiten und Risiken umgehen. In Fällen, in denen man des Gegenüber bezüglich seiner Motive und Intentionen nicht einschätzen und somit keine Abschätzung treffen kann, wie er_sie sich verhalten könnte, ist Vertrauen notwendig. Vertrauen benötigt man dabei nicht nur in der direkten Interaktion, sondern auch im gesamtgesellschaftlichen Bezug, um funktionierende Institutionen und Systemen zu gewährleisten.

Es existieren verschiedene Erklärungsmodelle für Vertrauen

Ein anderes Modell erklärt Vertrauen ähnlich dem kalkulierten, wirtschaftlichen Tausch bei dem verschiedene Faktoren und Wissen über den_die Handelspartner_innen im Rahmen einer Kosten-Nutzen Rechnung zum Tausch führen. So kann beim Vertrauen jede_r Partner_in überlegen, ob es sich lohnt, das Vertrauen zu bestätigen. Dieses Modell wird aber stark kritisiert, da Untersuchungen zu dem Schluss gekommen sind, dass in der vertrauensbasierten Interaktion die Informationen fehlen oder die Kapazitäten nicht zu Verfügung stehen, um so zu kalkulieren.

VORTEILE VON VERTRAUEN Drei wesentliche Vorteile von Vertrauen unterscheidet Kramer (1999).

DIE TRANSAKTIONSKOSTEN und der -aufwand werden reduziert dadurch, dass nicht insofern ökonomisch gehandelt wird, als dass durch Auswertung der Situation günstige, sondern auf Grund von Vertrauen schnelle Entscheidungen getroffen werden können.

DIE SPONTANE „SOCIABILITY“ unter den Mitgliedern der Organisation werde erhöht. Der Erwartung an die Mitarbeiter_innen einer Organisation, dass sie ihre Zeit und Energie aufwenden, um ein gemeinsames Ziel zu erreichen oder zu kooperieren, ist wesentlich leichter nachzukommen, wenn sich die Mitglieder gegenseitig vertrauen.

16 Zur Definition einer Gruppe und Gruppenstrukturen siehe Chaum (1985).

VERTRAUEN UND FREIWILLIGE EINORDNUNG in eine Organisationsstruktur ist für die Beteiligten wesentlichen einfacher, wenn nicht alle Entscheidungen hinterfragt werden oder man ständig kontrolliert wird.

Dabei ist Vertrauen nicht nur in die Systeme selbst nötig,[17] um diese effektiv nutzen zu können, sondern auch in Gruppe und in deren korrekten Umgang mit dem System und den darin vorhanden Daten.[18] Andernfalls kann die Kooperation dadurch gestört werden, dass die Systeme nur so genutzt werden, dass sie ein möglichst gutes Bild des_der Nutzer_in vermitteln und nicht die tatsächliche Arbeit unterstützen.

ARTEN VON VETRAUEN Kramer (1999) beschreibt mehrere Arten von Vertrauen

VERANLAGTES VERTRAUEN resultiert aus der Sozialisation, sodass der_die Einzelne zu mehr oder weniger Vertrauenfähigkeit im Aufbau einer Beziehung veranlagt ist.

ERFAHRUNGSBASIERTES VERTRAUEN ist abhängig von früheren, vertrauensbasierten Interaktionen zwischen Personen oder Institutionen. Dadurch, dass Motive und Intentionen der an der Interaktion Beteiligten bekannt sind, lässt sich die Vertrauenswürdigkeit besser einschätzen. Ein Problem ist aber, dass in den meisten Organisationen nur wenig Möglichkeiten bestehen Vertrauen über Erfahrung aufzubauen, da die dafür erforderliche Zeit nicht zur Verfügung steht.

WEITERLEITUNG DES VERTRAUENS DURCH DRITTE ist daher eine übliche Form, die Vertrauenswürdigkeit einer bisher unbekannten Person einzuschätzen. Man verlässt sich dabei auf das Urteil einer Person, der man schon vertraut und der man zutraut, die Vertrauenswürdigkeit der unbekannten Person, deren Ruf, einzuschätzen. Ein Problem ist aber, dass die Dritten, auf deren Einschätzungen man sich verlässt, dazu neigen die Informationen so gefiltert weiterzugeben, wie sie glauben, dass sie der Meinung derjenigen, die etwas über den Ruf erfahren möchten, entsprechen.

AUF KATEGORIEN BASIERENDES VERTRAUEN ist solches, dass einem Menschen auf Grund der Tatsache entgegen gebracht wird, dass dieser einer bestimmten Gruppe angehört. Problematisch ist diese Art von Vertrauen vor allem dann, wenn der Gruppe eher Misstrauen entgegengebracht wird und es so zu keiner Vertrauensbildung auf Grund der tatsächlichen Vertrauenswürdigkeit der Person kommen kann.

ROLLENBASIERTES VERTRAUEN ergibt sich aus dem Vertrauen gegenüber der Organisation, die eine Person in eine Rolle eingesetzt hat. Das Vertrauen darin, dass die Mechanismen einer Organisation zur Vergabe von z.B. gehobenen Stellen funktionieren, resultiert in Vertrauen in die Rolle selbst.

REGELBASIERTES VERTRAUEN entsteht, wenn auf Grund von Regeln Vertrauen quasi formal vorausgesetzt wird. Kramer führt als

17 Vgl. dazu auch Iachello and Hong (2007) 3.3.9.
18 ebd. 3.4.4.

Beispiel ein IT-Unternehmen an, in dem es gestattet ist, Geräte mit nach Hause zu nehmen. Dieses, auf einer Regel beruhende, Vertrauen der Organisation gegenüber ihren Mitgliedern resultiert auch in Vertrauen zwischen den Mitarbeiter_innen.

Verdächtigungen schwächen Vertrauensbeziehungen

Wesentliche negative Einflussfaktoren auf Vertrauen sind Verdächtigungen und bestimmte Überwachungstechnologien. Verdächtigungen gegenüber Anderen resultieren häufig darin, dass Entscheidungen verlangsamt werden, da mehr Informationen zur Abschätzung der Vertrauenswürdigkeit hinzugezogen werden. Dabei kann auch der unbegründete Verdacht für beide Seiten letztlich negative Folgen haben, eben dadurch, dass die Transaktionskosten gesteigert werden. Vor allem Überwachungstechnologien sind gemäß verschiedener Studien vermutlich verantwortlich für sinkendes Vertrauen, da die intrinsische Motivation zu vertrauen durch das offensichtliche Misstrauen seitens der Überwacher_innen gestört wird. Verdächtigungen könnten folgen, auch wenn die Überwachungstechnologien nicht explizit gegen Einzelpersonen gerichtet sind.

2.8 GRUPPENPROZESSE

Wesentlichen Einfluss auf die Nutzung von Kooperationssystemen und das Vertrauen in die eingesetzten Systeme hat die Dynamik der Gruppenprozesse. In der Forschung existiert keine einheitliche Lesart, die die Prozesse in allen Gruppen ausreichend beschreibt. [19] Im folgenden gehe ich beispielhaft auf das Phasenmodell von Tuckman and Jensen (1977) ein, auf das sich auch die in 3.2.3 vorgestellten Patterns nach Schümmer and Lukosch (2007) beziehen.

In verschiedenen Gruppenprozessen sind personenbezogene Daten im Spiel

Camenish et al. haben aufbauend auf das Modell von Tuckman and Jensen ein Szenario beschrieben, das veranschaulicht, welche und wieviele personenbezogene Daten in den Gruppenphasen zur Zusammenarbeit und Vertrauensbildung benötigt werden, wenn die Arbeit computervermittelt abläuft.

FORMING referiert auf die Gründungsphase einer Gruppe, in der, am selben Thema Interessierte oder mit einer Aufgabe betraute, Personen sich zusammenfinden und eine Gruppe bilden. Computervermittelt kann dieser Prozess über ein soziales Online-Netzwerk ablaufen, indem sich Personen mit gleichen Interessen oder Aufgaben finden und bekannt machen können.

STORMING ist die Phase, in der eine Gruppe verschiedene Ideen diskutiert, wie man mit einem Thema oder einer Aufgabe umgehen kann. Diese Phase können jegliche Kommunikationswerkzeuge unterstützen. In dieser Phase werden zudem die Rollen in der Gruppe verteilt, was Konfliktpotential birgt, aber auch hilft Vertrauen aufzubauen.

NORMING bezeichnet den Teil der Gruppenarbeit, in der sich auf ein Vorgehen geeinigt und ein gemeinsames Ziel entworfen wird. Zur Koordination und besseren Zusammenarbeit ist hier stärkeres

19 Cosmar beschreibt vier große Modelle, die seit den 1950er Jahren entwickelt wurden und noch als gültig erachtet werden. Dazu existieren verschiedene Meta-Klassifizierungsmodelle, die im wesentlichen zwischen sequentiellen und nichtsequentiellen Gruppenentwicklungsmodellen unterscheiden.

Vertrauen, und damit meist die tiefere Kenntnis der personenbezogenen Daten, wie Awareness-Informationen, notwendig oder sogar unerlässlich. Auf Grund der unterschiedlichen Meinungen kann es hier aber auch zu Konflikten kommen.

PERFORMING bezeichnet anschließend eine Phase, in der das gemeinsam entwickelte Ziel ausgearbeitet wird. Hierbei ist es, auf Grund der erfolgten Aufgabenteilung, nicht zwingend notwendig, dass alle Gruppenmitglieder darüber Bescheid wissen, woran die jeweils anderen arbeiten. Die Kollaboration kann etwa durch ein Dokumentenmanagementsystem unterstützt werden.

ADJOURING ist die abschließende Phase in der anhand des gemeinsam genutzten Materials der vergangenen Arbeitsprozess reflektiert wird. Dazu kann auch der Zugriff auf die im Laufe der Zusammenarbeit angefallenen Informationen notwendig sein.

2.9 ZUSAMMENFASSUNG

In diesem Kapitel sind die Rahmenbedingungen dargestellt worden, unter denen Groupwaresysteme in Unternehmen eingesetzt werden. Dabei wurden sowohl die technischen als auch die sozialen und juristischen Aspekte dieser sozio-technischen Systeme beschrieben. Ein besonderes Gewicht liegt auf der informationellen Selbstbestimmung der Mitarbeiter_innen unter Berücksichtigung einer als dynamisch zu verstehenden Vertrauensbasis.

Vertrauen bildet die Grundlage effektiver Kooperation,[20] auch computervermittelter. Mangelndes Vertrauen erhöht dagegen den Aufwand, der bei Kooperationen betrieben werden muss. Die verschiedenen Einflussfaktoren zeigen aber, wie fragil Vertrauen sein kann. Vertrauen zu stärken bzw. Misstrauen zu verhindern trägt also zur besseren Kooperation von Mitarbeiter_innen bei.

Unter diesen Bedigungen ergeben sich einige Probleme. Die Nutzung der Systeme sind zur effektiven und effektiveren Zusammenarbeit nicht mehr wegzudenken. Eine eingeschränkte Nutzung für die Mitarbeiter_innen zu ermöglichen, die aus persönlichen Gründen an einem technischen System nicht teilnehmen wollen, ist dabei kaum möglich.[21]

Das liegt auch daran, dass sich Vertrauen vor allem in symmetrischen Beziehungen aufbaut, eine Nicht- oder nur teilweise Nutzung kann die Zusammenarbeit sogar behindern und verunmöglichen. Die Nutzung wiederum erfordert die Preisgabe von personenbezogenen Informationen, eine anonyme Nutzung ist gerade in Kleingruppen kaum möglich. Das hat einen erheblichen Einfluss auf die informationelle Selbstbestimmung. Für die Arbeitnehmer_innen wird es immer schwieriger nachzuvollziehen wer, was, wann über sie weiß und welche Folgen das haben kann.

In der Kooperationsunterstützung ist zudem die eindeutige Zuordnung von Datum zur Person schwierig, da das Wissen über eine Zusammenarbeit Aussagen über alle Beteiligten enthält und die Folgen einer Aggregation verschiedenster Daten nicht im vorhinein abschätzbar sind. Für die Arbeitergeber_innen folgt daraus ein Handlungsgebot,

20 Dies Einschätzung teilen auch Lewick and Bunker (1995) die dies inbesondere für Gruppen mit flachen Hierarchien feststellen

21 Oft beschrieben als das *Take it or leave it*-Problem. Entweder man nimmt vollständig Teil oder überhaupt nicht

da sie ein Interesse an der effektiven Zusammenarbeit haben, sowie die Pflicht, die informationelle Selbstbestimmung der Angestellten zu erhalten. Auf Grund der Komplexität der Systeme ist eine Einhaltung der Datenschutzprinzipien allerdings kompliziert. Diese sind, wie das auch die Rechtsgrundlagen darauf ausgerichtet die informationelle Selbstbestimmung der Betroffenen gegenüber den datenverarbeitenden Stellen zu gewährleisten und nicht gegenüber Kolleg_innen mit denen eine auf Vertrauen basierende Zusammenarbeit und Datenpreisgabe stattfindet. Diese Trennung ist aber nur schwer aufrecht zu erhalten, da die Kolleg_innen Teil der datenverarbeitenden Organisation sind.

Szenarien, in denen die Daten aus Groupwaresystemen missbräuchlich genutzt werden, werden im nächsten Kapitel entwickelt. In Kapitel vier werden anschließend Maßnahmen vorgestellt, die eine Zweckentfremdung verhindern können und helfen sollen, Systeme und Beziehungen transparenter zu gestalten.

3 SZENARIEN UND DATENSCHUTZANALYSE

Basierend auf den Prinzip des Scenario-based Design (SBD) von Rosson and Carroll (2002) werden im folgenden Kapitel Problemszenarien vorgestellt, die beispielhaft die Datenschutzprobleme in Kooperationssystemen bei dynamischen Vertrauensverhältnissen beschreiben.

Der szenariobasierte Ansatz eignet sich gut, weil mit den Szenarien die Komplexität der sozio-technischen Systeme und der verschiedenen involvierten Aspekte (vgl. Kapitel 2) dargestellt werden kann, bei denen sich die sozialen Rahmenbedingungen und die Möglichkeiten sowie der Einsatz der Technik gegenseitig beeinflussen. Die Szenarien dienen dazu, die Abhängigkeiten innerhalb einer Gruppe in Bezug auf die Technik beispielhaft darzustellen. Gleichzeitig enthalten sie Elemente, die sich auf andere Situationen übertragen lassen. Die Szenarien diene im weiteren Verlauf der Arbeit auch dazu die Lösungsansätze Kompatibilität mit den Szenarien hin zu untersuchen und zu evaluieren.

Die Arbeit mit Szenarien stammt aus der Zukunftsforschung und wurde in den 50er Jahren in Amerika entwickelt, um im militärischen Bereich verschiedene mögliche Entwicklungen darzustellen und Handlungsalternativen bewerten zu können. In den darauf folgenden Jahren hat sich die Planung und Entwicklung mit Szenarien auch in vielen anderen Bereichen bewährt.[22]

3.1 VORGEHEN

Szenario-based Design und TAIDA wurden zur Szenariokonstruktion eingesetzt

Da im SBD das Design neuer Software im Vordergrund steht, wurde das von Rosson and Carroll vorgeschlagene Framework um Elemente anderer szenarienbasierter Arbeiten erweitert. Im SBD erfolgt die Konstruktion der Szenarien vor allem auf Grundlage von Feldstudien und der -analyse von realen Prozessen und Artefakten aus Arbeitssituationen. Die in dieser Arbeit untersuchten Probleme sind allerdings Spezialfälle, die im Kontext bereits bestehender Systeme auftreten können, jedoch nicht determiniert sind. Gerade die dynamischen Vertrauenskomponenten können nicht vorhergesagt werden.

Basierend auf dem Vorgehen nach dem TRACK, ANALYSE, IMAGE, DECIDE, ACT (TAIDA) Ansatz zur Szenarienkonstruktion von Lindgren and Bandhold (2003) in Kombination mit der Erfahrung von thematisch ähnlichen Arbeiten,[23] diente folgende Liste als Richtlinie zur Konstruktion und Analyse der Szenarien.

TRACK Es wurde Material aus dem Bereich betrieblicher Datenschutz sowie Datenschutz in Kooperationssystemen rezipiert. Als Quellen dienten Forschungsprojekte und -arbeiten,[24] Informationen

22 So etwa bei der Planung von IT-Projekten nach Rosson and Carroll (2002)

23 Wright et al. (2008) beschäftigen sich in einem EU-Projekt mit den Auswirkungen des ubiquitären Computing auf Privacy-Fragestellungen und haben ihre Analysen ebenfalls an Szenarien fest gemacht. Szenarienbasiert arbeiten auch Perusco and Michael (2007) die sich auf die Analyse von *location-based Services* aus Privacy und Security Sicht konzentrieren.

24 Wright et al. (2008), Seifert and Pawlowsky (1998), eine Vielzahl von Artikel in der Datenschutz und Datensicherheit (DuD) z.B. Wiele (2009), Schild and Tinnefeld (2009) und **?**

zu arbeitsrechtlichen Themen,[25] Medienberichte [26] sowie die Patterns von Schümmer and Lukosch (2007) zur computergestützten Interaktion.

ANALYSE Die Analyse der Szenarien ist an das Schema von Wright et al. (2008) angelehnt.

1. Den *Kontext* herstellen: Fragestellung erläutern. Wer sind die Beteiligten, was passiert ihnen ,bzw. was tun sie. Wo findet das Szenario statt? Was sind die Kernannahmen?
2. Welche *Technologien* werden im Szenario angewendet?
3. Was sind die *Auslöser*, die Änderungen in den Vertrauensverhältnissen sowie für die Handlung im Szenario bewirken?
4. *Issues:* Welche Personen bzw. welche Daten über die Personen sind betroffen und warum?
5. Welche *Nutzung* ist entscheidend für den Verlauf des Szenarios? Wo sind die Schwachstellen der bisherigen Systeme? Inwieweit sind die Datenschutzprinzipien berücksichtigt?

IMAGE Ein Expertenworkshop diente dazu, die relevanten Elemente zu extrahieren und für die vorher nur grob skizzierten Szenarien zu detaillieren und auf ihre Nachvollziehbarkeit zu überprüfen (vgl.3.3).

DECIDE Um entscheiden zu können, welche die optimalen technischen und organisatorischen Maßnahmen sind, die für die Probleme angemessen sind, werden diverse Alternativen in Kapitel 4 beschrieben und bewertet.

ACT Eine Beschreibung von vorzunehmenden Änderungen findet dann in Kapitel 5 statt.

3.2 ELEMENTE DER SZENARIEN

Die Szenarien folgen alle dem selben Schema (vgl. Abb. 2) . In einer Gruppe wird eine Technik zur Kommunikations- und Kooperationsunterstützung eingesetzt. Die Gruppen bestehen nur aus wenigen Personen und sind in eine größere Organisation eingebettet. Die Zusammenarbeit zeichnet sich durch flache Hierachien aus. Die Aufgaben können im weitesten Sinne der Wissensarbeit zugeordnet werden. Sie erfordern die Kommunikation und Zusammenarbeit aller Beteiligten. Die Zuordnung der Verschiedenen Elemente zu den jeweiligen Szenarien ist in Abbildung 5 dargestellt.

3.2.1 *Auslöser*

In den seltensten Fällen nutzt ein_e Mitarbeiter_in grundlos personenbezogene Daten, um jemandem zu schaden. In der Regel gibt es innerhalb einer Gruppe Unstimmigkeiten, die das Verhalten bedingen. Diese sind entweder aus der Gruppendynamik entstanden, auf

25 Die Erläuterungen zum Arbeitnehmer_innen Datenschutz in Däubler (2002) enthalten eine Vielzahl von Urteilen und Beispielen zum Thema, in der Zeitschrift COMPUTER UND ARBEITE werden Informationen für Betriebsräte vorgestellt, z.B. bei Brandt (2008) oder Meier (2008)

26 vgl. Kapitel 1

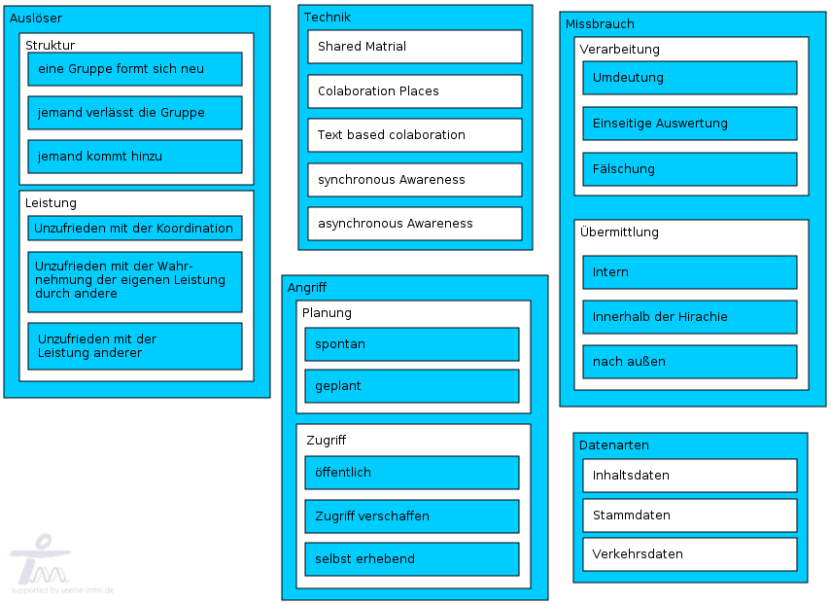


Abbildung 2: Elemente der Szenarien

den Inhalt und die Organisation der Gruppenarbeit bezogen, oder auf eine Änderung (dazu zählt auch die Konstituierung) der Gruppenstruktur zurückzuführen. Konfliktpotential bieten üblicherweise Fragen, die die Aufgaben- und Ressourcenverteilung betreffen, d.h. etwa wer welche Aufgabe bis wann erledigt haben soll, oder auch wenn eine Aufgabe nicht zur Zufriedenheit der Gruppe erledigt worden ist. Eine weitere mögliche Ursache wäre eine Person, die sich einer Aufgabe angenommen hat und sich innerhalb der Gruppe als benachteiligt empfindet. Konflikte mit Bezug zur Gruppenstruktur entstehen zum Beispiel, wenn jemand aus der Gruppe ausscheidet (freiwillig oder unfreiwillig) und/oder jemand weiteres zur Gruppe hinzu stößt. Bei solchen Veränderungen muss die Gruppenstruktur (s.o.) neu gebildet werden.[27]

3.2.2 *Datenaneignung*

Ein_e Angreifer_in nutzt nun das vorhandene Datenmaterial, um der oder den Streitgegner_innen Schaden zuzufügen. Dabei kann man unterscheiden zwischen

- einem geplanten Angriff, bei dem die Daten über längere Zeit gesammelt und ausgewertet wurden, bis zu dem Zeitpunkt, an welchem sie scheinbar genug Evidenz besitzen um veröffentlicht werden zu können - unter Umständen hat die angreifende Person bereits unberechtigt die Daten erhoben - und
- einen spontaner missbräuchlichen Nutzung der vorhandenen Daten aus einer Stimmung heraus.

Darüber hinaus kann der_die Angreifer_in unterschiedlich viel Aufwand aufbringen müssen, um an die Daten zu gelangen, je nachdem ob

27 Phase des Forming nach Tuckman and Jensen (1977).

- die Daten für die Person ohne großen Aufwand zu erreichen sind, z.B. wenn Informationen (Unternehmens-)öffentlich - etwa im Intranet - bereitstehen, oder ob die Daten aus dem Arbeitsbereich der Person stammen, auf den sie regulär Zugriff hat und sie für ihre Zwecke einsetzen kann.
- sie sich Zugriff verschafft, z.B. indem sie - eventuell mit Administratorberechtigung - Zugriffsperren umgeht oder sich über Umwege, durch das Ausnutzen einer Sicherheitslücke, die Daten beschafft.
- sie die Daten (im Fall der langfristigen Planung) selbst erhebt.

3.2.3 *Werkzeuge*

Schümmer and Lukosch (2007) haben eine umfangreiche Liste von *Patterns* identifiziert, die bei der computer-vermittelten Interaktion zum Tragen kommen können. Eine solche Interaktion zeichnet sich dadurch aus, dass zur Entwicklung vor allem sogenannte *wicked Problems* zu lösen sind, schließlich findet computervermittelte Interaktion in soziotechnischen Systemen statt, in denen sich die sozialen und technischen Komponenten gegenseitig stark beeinflussen.

Die Patterns sollen es Softwareentwickler_innen erleichtern, Groupware zu entwickeln und bekannte Fehler zu vermeiden. Patterns werden in der Softwareentwicklung eingesetzt, um regelmäßig auftretende Probleme und Lösungsansätze zu beschreiben. Dabei können sowohl die Patterns als auch die Lösungen von unterschiedlichem Abstraktionsniveau sein. Beispielsweise kann ein Pattern das Problem beschreiben, das zwei Kollaborateure sich oft nicht zur selben Zeit am selben Ort befinden. Das Pattern würden dann eine Möglichkeit darstellen, asynchron zu kommunizieren. Dabei wird keine Aussage darüber getroffen, ob nun E-Mail oder ein Anrufbeantworter geeigneter sind. Die Lösungsvorschläge bleiben mit Absicht unkonkret.

In der klassischen Softwareentwicklung werden Probleme in kleinere Einheiten zerlegt, die isoliert betrachtet und gelöst werden, mit dem Ziel diese Lösung (eine Routine oder Unterprogramm) beliebig oft wiederverwenden zu können. Demgegenüber bieten Patterns dazu nur unkonkrete Lösungen, die immer unter Berücksichtigung des jeweiligen Kontextes bei jedem Einsatz zu einer anderen Implementierung führen.

Pattern-Kategorien

Schümmer and Lukosch gliedern die Patterns in die Kategorien COMMUNITY SUPPORT, GROUP SUPPORT und BASE TECHNOLOGY. Für diese Arbeit wurden vor allem die GROUP SUPPORT Patterns genauer betrachtet und in die Szenarienentwicklung miteinbezogen. BASE TECHNOLOGIES sind im wesentlichen Patterns, die die grundsätzlichen Funktionalitäten beschreiben und Voraussetzungen für die Interaktion zwischen Benutzer_innen und dem technischen System bilden. COMMUNITY SUPPORT behandeln Patterns die zur Unterstützung WEB 2.0-ähnlicher Werkzeuge benötigt werden die in den hier beschriebenen betrieblichen Kontext keine Anwendung finden (siehe 2.4).

Die GROUP SUPPORT Patterns sind wiederum in mehrere Kategorien untergliedert. Eine detaillierte Beschreibung aller Patterns erfolgt hier aus Platz- und Redundanzgründen aber nicht, stattdessen werden nur die Kategorien kurz vorgestellt und im weiteren Verlauf auf diese verwiesen.

SHARED MATERIAL Patternsammlung, die die Bearbeitung, das Austauschen und den Zugriff auf gemeinsame Artefakte einer Gruppe beschreiben. Elemente dieser Patternkategorie sind zum Beispiel die Möglichkeit, eine Gruppe zu definieren, über Mechanismen zum Austauschen, Bearbeiten und Ansehen gemeinsamer Dokumente bis hin zu Abstimmungswerkzeugen, um in einer Gruppe eine Entscheidung zu treffen. Konkrete Bespiele: Konferenzsysteme, Versionskontrollsysteme (CVS, SVN), Dateiaustauschsystem (FTP, WebDAV, Google Docs), Desktop-Sharing (VNC, NetMeeting), Joint Editing (Shared Whiteboards).

COLLABORATION PLACES Möglichkeiten, einen Interaktionsraum zu gestalten, sind Patterns dieser Kategorie. Dazu gehören Patterns zur Definition eines *Raumes* in dem alle Kollaborationselemente gebündelt sind, verschiedene Wege für die Zusammenarbeit von Usern zu finden und Aufgaben und Aktivitäten zu verfolgen. Beispiele: Google Docs, Online-Konferenz-Systeme (NetMeeting), Spiele (MMOGs).

TEXT BASED COLLABORATION Pattern zur textbasierte Kollaboration, etwa über E-Mail, Chat, Foren oder Annotationen. Weitere Patterns dieser Kategorie erläutern Verfahren, um textbasierte Kommunikation zu strukturieren und zu vereinfachen. Beispiele: Google Docs, Social Networks, Foren, Usenet, E-Mail, Chat-Systeme, IMAP, TODO Messages, Points of interests.

SYNCHRONOUS GROUPWARE AWARENESS In dieser Kategorie sind Patterns gelistet, die Fragen beantworten wie: „Wer arbeitet gerade woran?“ „Was passiert als nächstes oder was soll als nächstes passieren?“ „Welche Möglichkeiten hat welche_r Nutzer_in, Artefakte zu sehen oder zu beeinflussen?“Beispiele: Social Networks, Chats, Spiele (MMOGs), Joint Editing Werkzeuge.

ASYNCHRONOUS GROUPWARE AWARENESS Patterns, die dazu dienen nach Phasen der Einzelarbeit den Usern wieder ein gemeinsames Niveau zu ermöglichen bzw. die Artefakte abzugleichen und Aufmerksamkeit auf das zu lenken, was von Anderen in der vergangenen Zeit bearbeitet wurde. Bespiele sind Versionskontrollsysteme, Foren, Dateiaustauschsysteme (BSCW, Google Docs), Social Networks und Chat.

Alle Patterns benötigen, um ihre unterstützende Wirkung entfalten zu können, Zugriff auf personenbezogene Daten der Benutzer_innen, um diese wiederum den anderen Beteiligten zur Verfügung stellen zu können. Diese können, wie im Falle der synchronen Awareness, eher flüchtig sein, aber auch, z.B. bei der Kommunikation über E-Mail oder Foren, dauerhaft gespeichert werden. Dabei lassen sich, je nach Datum, umfangreiche Rückschlüsse auf das Verhalten und die Leistung des_der Einzelnen ziehen.

3.2.4 *Datenarten*

Man verschiedene Arten personenbezogener Daten unterscheiden.

STAMMDATEN sind grundsätzlich Aussagen über eine Person, die nur geringer Veränderbarkeit unterliegen wie Name, Alter, Geschlecht oder Position.

Abbildung 3: Workshop-Situation

Als INHALTSDATEN bezeichnet man die Inhalte einer Kommunikation, also was jemand geäußert hat. Diese Daten lassen ebenfalls Rückschlüsse auf die Persönlichkeit zu.

Zuletzt liefern die VERKEHRSDATEN Informationen darüber, wer mit wem wann kommuniziert hat. Aus solchen Daten lassen sich Informationen über das soziale Netz und dessen Kommunikationsstrukturen, aber ebenso über die Kommunikationsfreudigkeit (innerhalb des kontrollierten Mediums) gewinnen.

3.2.5 *Missbräuchliche Nutzung*

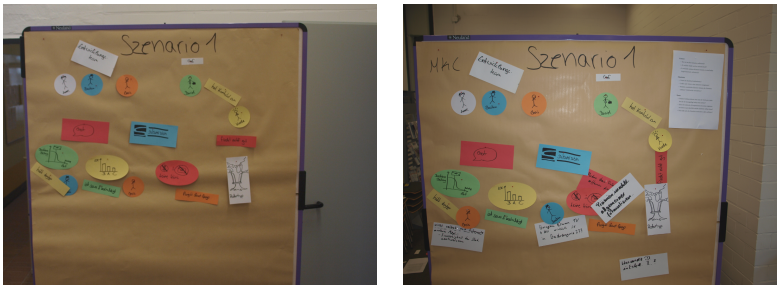
Die Analyse zu Missbräuchliche Nutzung beschäftigt sich mit der Frage, gegen welche Datenschutzprinzipien (vgl. 2.3) verstoßen wurde und wie. Daten können zweckentfremdet und dabei zu Ungunsten einer Person umgedeutet werden. Die einseitige Auswertung führt zu einem ähnlichen Ergebnis; hier wird aber Absicht unterstellt, d.h. Informationen, die bei der Auswertung ebenfalls vorliegen, werden unterschlagen. Darüber hinaus lassen sich Daten auch fälschen, um ein bestimmtes Ziel zu erreichen.

Alle Datenauswertungen haben aber nur einen geringen Effekt, wenn sie nicht an andere Beteiligte übermittelt, also veröffentlicht werden. Diesbezüglich werden in den Szenarien verschiedene Stufen beschrieben. Sowohl eine Verwendung innerhalb der Gruppe, als auch eine Weiterleitung an eine an den bisherigen Konflikten unbeteiligte Person, die sich aber im Hierarchiegefüge befindet, oder eine Weiterleitung an eine außenstehende Person, sind vorstellbar.

3.3 WORKSHOP

Nach der groben Ausarbeitung von drei Szenarien, die sich auf die vorangestellten Quellenanalyse stützen, wurden diese in einem zweiten Schritt im März 2010 innerhalb eines Workshops, der im Moderationslabor der Ruhr-Universität Bochum stattfand, in Kleingruppen diskutiert und detailliert ausgearbeitet. Dazu wurden neun Personen in drei gleich große Gruppen eingeteilt. Die Teilnehmer_innen waren Studierende und Mitarbeiter_innen der Ruhr-Universität die bereits Erfahrung mit

Neun Personen nahmen am Workshop teil



(a) vorher (b) nachher

Abbildung 4: Szenario 1 vor und nach der Bearbeitung durch eine Gruppe

Groupwaresystemen in unterschiedlichen professionellen und privaten Kontexten haben. Jede dieser Gruppen bekam eine Pinnwand zu Verfügung gestellt, auf der eines der Szenarien dargestellt wurde (vgl. Abbildung 3). Um die Diskussion und mögliche Veränderungen des Szenarios zu vereinfachen, wurde ein Modell erstellt, in dem Karten die Personen und Handlungselemente repräsentierten. Um Detailfragen vermerken zu können, lag das zu dem Zeitpunkt aktuelle Szenario auch zum Nachlesen vor. Die Leitfragen (siehe Anhang) sollten die Gruppe anregen, bestimmte Teilaspekte zu diskutieren. Während der Diskussionen waren die Teilnehmer_innen dazu angehalten, ihre Verbesserungsvorschläge und Kritikpunkte auf weiteren Karten oder direkt auf der Pinnwand festzuhalten. Im Anschluss an die halbstündige Diskussion hatten die Teilnehmer_innen zudem die Möglichkeit, weitere Anregungen und Kommentare auf einem Fragebogen festzuhalten, der im Stil einer Osborn-Checkliste[28] nach weiteren Änderungsmöglichkeiten und Situationsveränderungen fragte.

Dieser Ablauf wurde von jeder Gruppe für jedes Szenario durchgeführt. Zuletzt kamen alle zu einer Abschlussdiskussion zusammen, um generelle Anmerkungen und Anregungen für mögliche, aber bisher unbeachtete Situationen zu sammeln. Die Auswertung des Workshops erfolgte anhand von Fotos und den Fragebögen. Ließ sich aus diesen nicht rekonstruieren, was Gegenstand der Diskussion gewesen ist, standen zusätzlich Videoaufnahmen zur Verfügung. Auf diese wurde allerdings nur vereinzelt zurückgegriffen. Die Kameras im Raum haben zwar jeweils eine Gruppe aufgezeichnet, die Mikrofone allerdings jeweils synchron alle drei laufenden Diskussionen, so dass die Gespräche nur sehr mühsam nachvollzogen werden konnten.

ERGEBNISSE DES WORKSHOPS Erwartungsgemäß stellten viele Teilnehmer_innen heraus, dass meistens entweder die mangelnde Kommunikation oder soziale Konflikte innerhalb der fiktiven Situation für die Eskalation verantwortlich ist. Diese Beschreibungen waren beabsichtigt, denn ein Vertrauensbruch wird von - absichtlich oder unabsichtlich - mangelnder oder unzureichende Kommunikation ausgelöst. Dennoch wurde den Basis-Szenarien bestätigt, zum Großteil realitätsnah zu sein. Kritische Stellen wurden mehrfach angemerkt und mit Änderungsvorschlägen sowie Berichten aus der Erfahrung der Teilnehmer_innen ergänzt. Nachdem die Änderungen eingearbeitet worden waren, wurden die Szenarien eine Woche später noch ein weiteres Mal von jeweils

28 Die Checklisten nach Alex Osborn sind eine Kreativitätstechnik, um Fragestellungen noch einmal aus einer anderen Perspektive zu betrachten (vgl. Bayerl (2005))

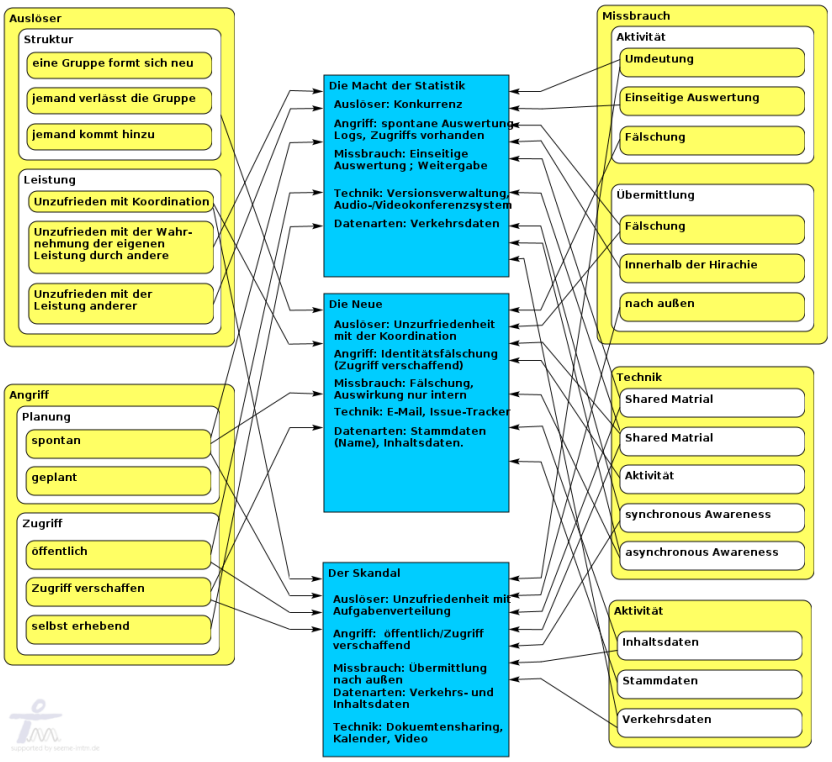


Abbildung 5: Elemente der Szenarien mit Relation zu ihrer Verwendung

einer Person begutachtet, die auch am Workshop teilgenommen hatte und letzte Unstimmigkeiten bereinigt.

3.4 SZENARIO 1: DIE MACHT DER STATISTIKEN

Kontext

Anne, Bastian und Chris arbeiten zusammen in einem Software-Entwicklungs-Projekt bei Andcompany. Ihre Aufgabe ist die Programmierung eines Lagerverwaltungssystems für eine lokale Backwarenkette zur Organisation der morgendlichen Lieferungen. Andcompany ist ein kleines, aufstrebendes IT-Unternehmen mit gegenwärtig knapp 20 Mitarbeiter_innen. Weil die Auftragslage in letzter Zeit gut ist, wurden fünf der zwanzig Angestellten erst vor wenigen Wochen eingestellt. Aus Skepsis, ob die gute Auftragslage anhalten wird, ist das Unternehmen noch nicht in größere Räumlichkeiten umgezogen, so dass akuter Platzmangel herrscht. Die Angestellten sind angehalten, an zwei von fünf Tagen in der Woche zu Hause zu arbeiten. Die drei Entwickler_innen organisieren ihre Arbeitszeiten so, dass sie mindestens einmal wöchentlich ein Meeting im Büro abhalten können. Daran nimmt grundsätzlich auch David teil, einer der Firmengründer, der bei dem auftraggebenden Unternehmen die Anforderungen an das zu entwickelnde Produkt erhebt und die Programmierer_innen anleitet.

Für die Entwicklungsgruppe ist das verteilte und asynchrone Arbeiten kein Problem, da sie zur Verwaltung des Programmcodes das Versionsverwaltungssystem Subversion[29] einsetzen, mit welchem sie von beliebigen Orten Zugriff auf den Quellcode haben und Änderungen schnell den Anderen verfügbar machen können. Tagsüber findet die Kommunikation meist über das Chat und Voice over IP (VoIP) Werk-

29 http://subversion.tigris.org

zeug Pidgin[30] statt, über das sie Video- und Audiokonferenzen abhalten können.

Situation

Zu Beginn des Projekts gestaltet sich die Arbeitsatmosphäre harmonisch und die Gruppe arbeitet produktiv. Die Anforderungen, die David an die Gruppe weiter gibt, verteilen die Drei ohne großen Planungsaufwand untereinander und setzen sie zügig um. Nach mehreren kurzen Entwicklungszyklen, die mit einer Filiale und der Zentrale getestet wurden, geht das Projekt in die Testphase, an der mehrere Filialen beteiligt sind. Unerwartet wachsen mit der Anzahl der teilnehmenden Testfilialen aber die Probleme. Lieferungen werden falschen Filialen zugeordnet und Mengenangaben sind nicht korrekt.

In der Entwicklungsgruppe wird es nun stressig. Als sich das Ende des Projekts weiter verzögert, muss Chris, auf Druck von David, seinen Urlaub absagen. Jede Verzögerung kostet Andcompany nun Geld und eigentlich waren die personellen Ressourcen schon für Nachfolgeprojekte eingeplant. Die Stimmung in der Gruppe ändert sich auch deshalb, weil in dem wachsenden Unternehmen neue Hierachiestufen geschaffen werden sollen. Sowohl Chris als auch Bastian interessieren sich für die Stelle eines Senior-Entwicklers, die für eines der Folgeprojekte eingerichtet werden soll.

erste Eskalation

In einer der Krisensitzungen, zu dem sich die Drei und David in den Räumen der Andcompany treffen, beginnt Bastian durch Sticheleien darauf hinzuweisen, dass die Verzögerung vor allem auf Chris' mangelndes Engagement zurückzuführen sei. Er habe eine Statistik vorbereitet, die, basierend auf den Informationen aus dem Versionsverwaltungssystem, das die Gruppe nutzt, belegen solle, dass Chris wesentlich weniger Codezeilen zum Programm beigetragen habe als die anderen beiden und auch generell ein schlechter Teamarbeiter sei. Chris bemüht sich darauf hinzuweisen, dass die Quantität der Codezeilen nichts über die Qualität aussage und er sich dafür mehr um die komplizierte Programmlogik gekümmert habe. Er ist dennoch sichtlich getroffen von dieser plötzlichen Beschuldigung. David versucht die Wogen zu glätten. Um das Projekt abschließen zu können ist schließlich eine gemeinsame Kraftanstrengung nötig, die nur im Team erbracht werden kann. Das entstandene Misstrauen kann er aber dennoch nicht mehr beseitigen.

zweite Eskalation

Trotz Davids Versuchen, Chris davon zu überzeugen, dass Bastians Vorwürfe nicht ernst zu nehmen seien und dieser nur ein impulsiver Mensch sei, sieht Chris seine Chancen auf die Beförderung schwinden. Der Ruf, ein Eigenbrödler zu sein, verfolgt ihn schon länger, er ist jedoch der Auffassung, sich gebessert zu haben. Um seine eigene Position zu stärken, schreibt er am Abend ein kleines Programm, das die Protokolle des Instant Messengers der letzten Wochen auswertet und präsentiert der Gruppe bei der nächsten Gelegenheit die Erkenntnis, dass er die meisten Kontakte zu den anderen beiden Entwickler_innen gehabt habe und auch die längste Zeit insgesamt online, also ansprechbar, gewesen sei. Dabei bemerkt er nebenbei, dass Bastians Kommunikationsbeteiligung am anderen Ende des Spektrums liege.

ZUSAMMENFASSUNG & KONTEXT Andcompany ist ein aktuell rasant wachsendes Unternehmen. Die gute Auftragslage führt dazu, dass

30 Pidgin ist ein Chat-Client der diverse Protokolle unterstützt. Im Zusammenspiel mit dem XMPP-Protokoll stehen diverse Kommunikationskanäle zur Verfügung http://www.pidgin.im/

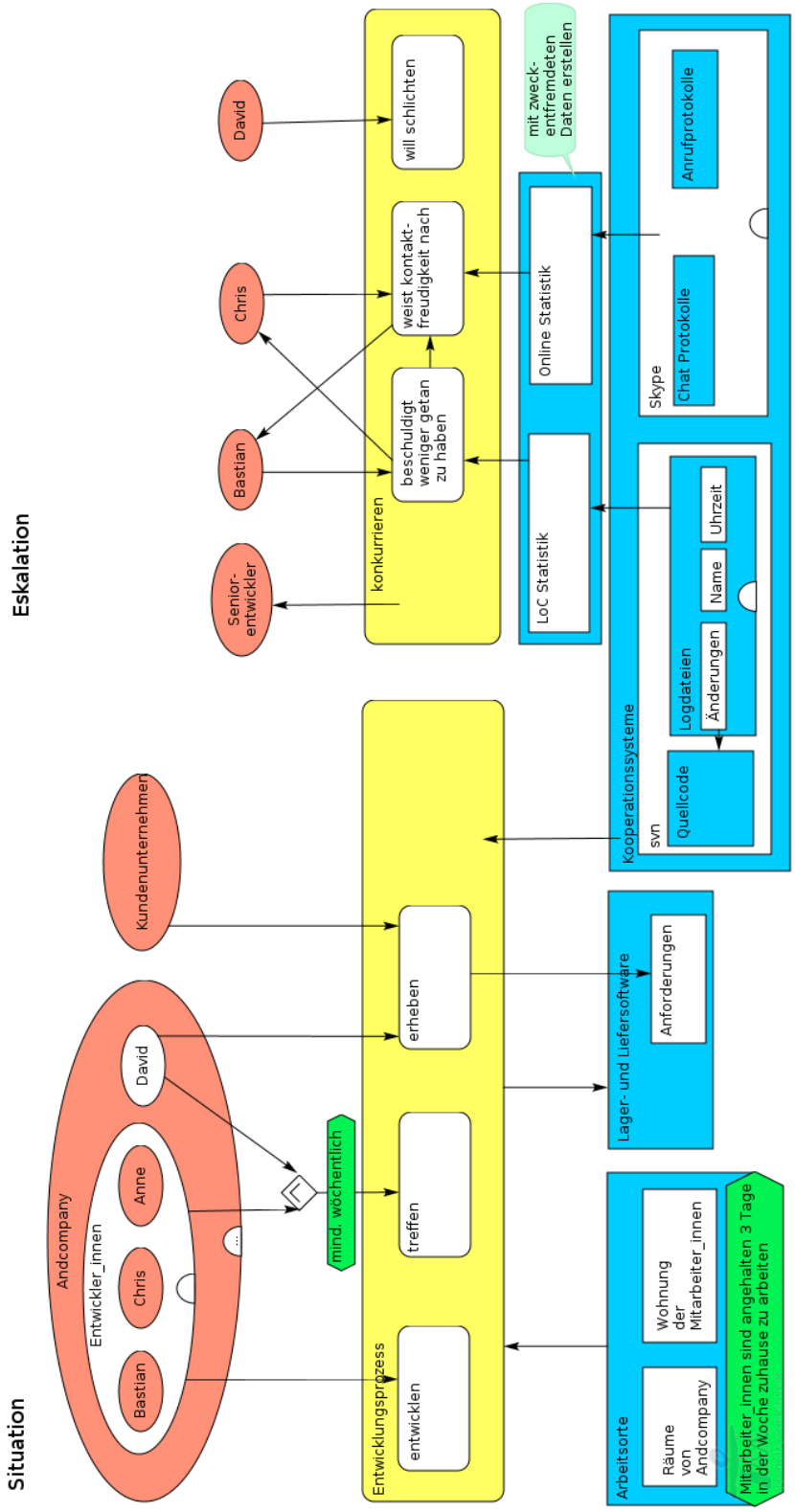


Abbildung 6: Modell „Die Macht der Statistik“

die Anzahl der Angestellten kurzfristig wächst. Allerdings sind weder die räumlichen Möglichkeiten noch die interne Struktur bisher darauf eingerichtet. Auf Grund von Raummangel sind die Angestellten angehalten, einen Teil ihrer Arbeit von zuhause zu erledigen. Damit sie trotzdem im Team arbeiten können, muss die Entwicklergruppe, um die es im Szenario geht, computervermittelt kommunizieren. Intern sollen neue Stellen und Hierarchiestufen geschaffen werden, um die Koordination zu verbessern. Ein_e Senior-Entwickler_in kann in Zukunft die Aufgabe der Anforderungserhebung von der Geschäftsführerung übernehmen, so dass diese sich um geeignete neue Räume kümmern kann.

In diesem Kontext arbeiten Anne, Bastian, Chris und David an einem Projekt. Die ersten drei übernehmen die Programmierung, während David zum größten Teil für die Anforderungsanalyse und die Kommunikation mit dem Kunden zuständig ist.

TECHNOLOGIEN & DATEN Die im ersten Szenario eingesetzten Werkzeuge gehören zum Handwerkszeug gegenwärtiger Softwareentwicklung. Subversion steht hier stellvertretend für eine Reihe von Versionsverwaltungsystemen.[31] Diese lassen sich der Patterngruppe SHARED MATERIAL zuordnen und bieten zudem mit Log-Dateien die Möglichkeit, die Änderungen am Quelltext zu verfolgen (ASYNCHRONOUS GROUPWARE AWARENESS). So lässt sich die Softwareentwicklung unabhängig von Ort und Zeit vollziehen. Im Szenario ermöglicht es dieses Feature auch, dass die Entwickler_innen nicht jeden Tag im Büro sein müssen, sondern von Zuhause arbeiten können.

Pidgin, im Zusammenspiel mit einem XMPP-Server, als Audio-/Video- und Chat-Konferenzsystem dient der synchronen Kommunikationsunterstüzung. Der Chat dient der TEXT BASED COLLABORATION, es lassen sich auch Dateien austauschen, Gruppen anlegen oder ein shared Whiteboard einrichten. Für das Szenario entscheidender sind die Funktionen zur SYNCHROUNOUS GROUPWARE AWARENESS. Sobald das Programm gestartet ist und man sich am Server angemeldet hat, wird allen Kontakten dies angezeigt. Der Status „Online"lässt sich dann noch präzisieren, in dem man anzeigt, dass man nicht gestört werden will oder abwesend ist.

AUSLÖSER Das Vertrauensverhältnis ändert sich durch die aufkommende Konkurrenz zwischen Bastian und Chris. Bastian sieht seine Chancen für eine Beförderung schwinden, da das Projekt wesentlich länger dauert als geplant. Er versucht sich zu profilieren, indem er Chris' Ruf negativ beeinflusst. Selbst als David eingreift, um die Situation zu entschärfen, möchte Chris die Anschuldigungen nicht auf sich sitzen lassen, da er ebenfalls auf eine Beförderung hofft.

ISSUES Chris wertet Daten aus den SVN-Logs aus, die Bastian betreffen. Es handelt sich um personenbezogene Informationen der Kategorien Verkehrs- und Metadaten über Bastian, die geeignet sind, seine Leistung und sein Verhalten zu bewerten. Chris beschränkt sich dabei auf die Zählung der Anzahl der Beiträge, die Bastian zum Code gemacht hat. Darüber hinaus enthalten die Logs auch Daten über die

31 Wikipedia listet im März 2010 14 solcher Programme. Davon gehört die Mehrheit zur Gruppe der verteilten Versionsverwaltung, bei der die Versionierung, und damit auch die Veränderungshistorie, auf jedem teilnehmenden Rechner verwaltet wird. Ein zentraler (sperrbarer) Server ist nicht notwendig.

exakte Uhrzeit, zu der Bastian die Codeveränderungen an den Server gesendet hat. Diese Informationen nutzt Chris jedoch nicht. Bastians Auswertung zielt darauf zu zeigen, wie lange er online war und wie oft er kommuniziert hat. Bei Ersterem handelt es sich um eine Information über ihn selbst. Zweiteres betrifft zwar auch ihn, aber im Szenario wertet er nicht nur aus, dass er kommuniziert hat, sondern auch mit wem. Dies ist eine Information, die für seinen Zweck nicht unbedingt nötig ist, ihm aber einen kleinen Seitenhieb gegen Chris erlaubt. Um der Leistungsbewertung von Chris über die SVN-Auswertung etwas entgegensetzen zu können, gibt er zusätzlich an, wieviele Stunden er seinen Status auf *Online* gestellt hatte.

NUTZUNG Chris und Bastian begründen ihre Anschuldigungen mit Daten aus den Groupware-Systemen, die sie nutzen. Chris wertet die Log-Dateien des Versionverwaltungsprogramms aus. Solche Logs werden in der Regel lange vorgehalten und dienen dazu spontan, oder auch noch nach längerer Zeit, den_die Urheber_in einer Veränderung am Code ausfindig machen zu können. Dieses Verhalten ist gewünscht. Es dient vor allen Dingen der Transparenz bei der Entwicklung und hilft beim Beheben von Fehlern oder um Kontakt aufzunehmen, wenn bei einer späteren Bearbeitung Unklarheiten auftauchen. In vielen Softwareprojekten ist die Dokumentation im Quellcode unzureichend, so dass Rückfragen an den_die Urheber_in notwendig werden können. Damit man auf die Daten zugreifen kann ist es in der Regel notwendig, einen eigenen User-Account zu besitzen.[32] Ist dieser vorhanden, bestehen keine weiteren Einschränkungen. Zur Leistungs- und Verhaltenskontrolle sind die Daten nicht gedacht. Um sie dazu zu nutzen ist, wie im Szenario beschrieben, eine zweckentfremdende Aggregation und Bewertung der Daten notwendig. Allerdings ist meist auch nicht festgelegt, wie lange die Daten nach Abschluss eines Projekts vorgehalten werden.

Bastian nutzt die Log-Dateien von Pidgin, weil er die genauen Zeitpunkte der Logins und Logouts feststellen und die Anzahl der Kontakte zu den anderen Gruppenmitgliedern darstellen will. Auch hier dienen die anfallenden Daten einem anderen Zweck, nämlich der Awareness über den Status der Arbeitskolleg_innen bzw. der späteren Nachverfolgbarkeit der Kommunikation.

3.5 SZENARIO 2: DIE NEUE

Kontext

Achim , Birgit und Carsten betreuen das Rechenzentrum eines Zulieferbetriebs aus der Automobilindustrie. Da die Fabrik 16 Stunden am Tag voll ausgelastet ist, muss in dieser Zeit im Rechenzentrum sichergestellt werden, dass alles funktioniert. Deswegen arbeiten die Administrator_innen im Schichtdienst zwischen 6 und 22 Uhr. In den frühen Morgenstunden ist nur eine Person anwesend, eine zweite unterstützt den Support zu den normalen Bürozeiten und wenn die Person aus der Frühschicht Feierabend hat, kommt die dritte Person zur Arbeit, die dann am späten Abend die Aufgaben alleine übernimmt.

Achim ist schon seit über 30 Jahren in dem Unternehmen angestellt, hat das Rechenzentrum mit aufgebaut und ist bis dato bemüht, die Technik auf dem neuesten Stand zu halten. Als Dienstältester steht er

32 In Gruppen mit flexibler Mitgliedschaft, z.B. Open-Source Projekten, sind die Daten oft auch anonym abrufbar, bzw. kann ein Nutzer_innenaccount ohne besondere Authentifizierung erstellt werden

aber nicht nur kurz vor dem Renteneintritt, sondern fällt wegen eines Rückenleidens unregelmäßig für wenige Tage bis mehrere Wochen aus. Deswegen wurde vor kurzer Zeit Daniela eingestellt, die das Team ergänzen soll, damit in Krankheitsfällen die anderen Beiden nicht zu stark belastet werden.

Weil die Anforderungen an die Server hoch sind, ist die Technik auf einem aktuellen Stand und regelmäßig werden neue Komponenten angeschafft. Im Regelbetrieb ist jeder der drei hauptverantwortlich für jeweils mehrere Komponenten wie Mailserver, Backups, Webserver oder Firewall. Trotzdem müssen in Notfällen alle in alle Systeme eingreifen können, sollte ein Fehler einen Ausfall produzieren. Achim ist dabei derjenige mit der besten Kenntnis über die gewachsene Struktur und kann mit seiner Erfahrung ausgleichen, dass es keine vollständige Dokumentation über die Funktionsweise aller Komponenten gibt, etwa jener, die nur selten gewartet werden müssen. Er hat insofern inoffiziell die Funktion des Teamleiters inne. Mit der Dokumentation hatte die Gruppe erst vor wenigen Monaten angefangen, als das Bewusstsein dafür wuchs, dass Achim sie in einiger Zeit verlassen werden würde.

Situation

In den ersten Tagen begleitet Daniela Achim in dessen Arbeitsalltag, weil sie schon einige Erfahrung mit Mailservern hat. Unglücklicherweise profitiert sie nur wenige Tage von Achims Kompetenz, da dessen Rückenleiden ihn unvorhergesehen wieder von der Arbeit abhält. Sie muss nun regulär in den Schichtdienst integriert werden und übernimmt in den darauffolgenden Wochen die Spätschicht. Nachmittags arbeitet sie parallel mit Carsten, der sie in das eingesetze Ticketing-System einweist. Mit diesem System lassen sich Fehler, Probleme und Anforderungen verwalten, Abhängigkeiten zwischen solchen definieren und Zuständigkeiten verteilen. Da im Schichtdienst nie alle drei gleichzeitig anwesend sind, existiert zur Kommunikation eine Mailingliste, die Daniela nun ebenfalls benutzt. Von dieser existiert auch ein sich automatisch erstellendes Archiv, aus dem sie zusätzliche Informationen über die diskutierten Themen der letzten Wochen gewinnen kann.

Eskalation

Birgit arbeitet zu dieser Zeit in der Frühschicht an der Integration einer neuen Software für die Verwaltungsabteilung in das System. Dazu ist es nötig, Änderungen an der Firewall vorzunehmen, um einen reibungslosen und dennoch sicheren Betriebsablauf gewährleisten zu können. Da Birgit das neue Ticketing-System noch nicht benutzt und sie Carsten zum Ende ihrer Schicht immer noch persönlich trifft, teilt sie ihm mündlich mit, was er als Verantwortlicher für die Firewall zu ändern hat. Da er die Installation des Ticketing-Systems vor nicht allzu langer Zeit vorgenommen und loggt er sich mit Birgits Account ein. Anschließend trägt er die Aufgaben ein und weist sie Daniela zu anstatt sich selbst. Im Anschluss erklärt er ihr, er und Birgit hätten entschieden, dass Daniela nun die Firewallbetreuung übernehmen müsse.

Daniela, die von Firewalls nur begrenzte Kenntnis hat, versucht nun über die rudimentäre Dokumentation und die Ticket-Einträge der letzten Wochen nachzuvollziehen, wie der Stand der Firewall ist und wie sie funktioniert, ob es schon ähnliche Fälle gab und wie sie vorgehen könnte. Dabei fällt ihr auf, dass bisher Carsten die firewallbezogenen Aufgaben erledigt hat, die nun sie zugewiesen bekommt. Aus den E-Mails erfährt sie dann, einhergehend mit den Fakten über die Funktionsweise der Firewall, dass Carsten sich dagegen gewehrt hatte, die Firewall als Hauptverantwortlicher zu betreuen, Achim aber am Ende ein Machtwort gesprochen hatte. Sie wird misstrauisch, erledigt als

Neue die Aufgaben vorerst trotzdem, weil sie sich nicht traut Carsten, darauf anzusprechen.

Als sich Achim nach einigen Wochen erholt hat und wieder in den Arbeitsbetrieb einsteigt, fragt Daniela ihn nach der ursprünglich geplanten Aufgabenverteilung. Immerhin war er schon früher mit Carstens Arbeitseinsatz unzufrieden, sodass er als Reaktion droht, sich bei einem Vorgesetzten für eine Abmahnung einzusetzen.

ZUSAMMENFASSUNG Die Gruppe der Administrator_innen befindet sich gegenwärtig in einer Neuorganisationsphase. Dadurch, dass Achim als inoffizieller Teamleiter aktuell regelmäßig und in Zukunft dauerhaft ausfällt, ist der Posten vakant. Anders als in *Die Macht der Stastik* folgt daraus aber keine offene Konkurrenzsituation zwischen denen, die Ansprüche auf den Posten erheben. Die Gruppenstruktur ändert sich dadurch, dass Daniela hinzukommt. Achim kann die Einweisung in die Systeme und die Arbeitsstruktur wegen einer Krankheit nicht abschließen, weshalb Daniela nicht vollständig vertraut mit ihrer neuen Arbeitsumgebung ist. Zu Beginn fühlt sich von den anderen beiden niemand dazu verpflichtet, Achims Rolle gegenüber Daniela auszufüllen, da durch Achims Abwesenheit keine unmittelbaren Probleme entstehen. Die Unsicherheit über die Form der Zusammenarbeit nutzt Carsten, damit er unliebsame Aufgaben loswerden kann, denn schließlich vertraut ihm Daniela zunächst und nimmt sich ihrer vermeintlichen Aufgaben an. Dabei betrügt Carsten Daniela, indem er ihr vortäuscht, es habe eine Absprache über die Aufgabenverteilung zwischen ihm und Birgit gegeben. Er übersieht dabei, dass Daniela auf den Betrug aufmerksam werden könnte und mit Achim darüber spricht.

TECHNOLOGIEN & DATEN Ticketing-Systeme weisen viele Merkmale der COLLABORATION PLACES-Patterns auf und schließen Funktionen der ASYNCHRONOUS GROUWARE AWARENESS ein. Aufgaben (Issues) lassen sich verwalten, Gruppen und Personen zuordnen, die so die übrigen Teilnehmer_innen über den Status der Lösung auf dem Laufenden halten können.

E-Mail ist die klassische Form der asynchronen TEXT BASED COLLABORATION, also eine einfache Text-Nachricht, die an eine_n oder mehrere Empfänger_innen addressiert sein kann. Mailinglisten[33] erweitern die Möglichkeiten leicht, indem sie es vereinfachen, an mehrere Personen zu senden. Die E-Mails laufen über einen Server, bei dem ein Postfach registriert ist, das eine empfangene E-Mail automatisch an die Adressen einer definierten Gruppe weiterleitet. Die E-Mail-Diskussionen werden meist zusätzlich auf dem Server gespeichert, damit ein zentrales Archiv zur Verfügung gestellt werden kann.

AUSLÖSER Achim ist als Dienstältester der akzeptierte Teamleiter, das heißt, dass seine Position auf dem Vertrauen der Anderen in seine Erfahrung beruht. Mit seinem kurzfristigen Ausfall und der Gewissheit darüber, dass er bald in Rente gehen wird, fällt für die Gruppe eine Koordinationsstelle weg. Die vorher klare Gruppenstruktur kann in dieser Form nicht aufrecht erhalten werden. Für Carsten stehen damit auch andere Teile der Gruppenorganisation, wie die der Aufgabenverteilung, zur Disposition. Er nutzt die Situation aus, um ihm unliebsame

33 Beispielsweise Majordomo, Mailman oder GoogleGroups

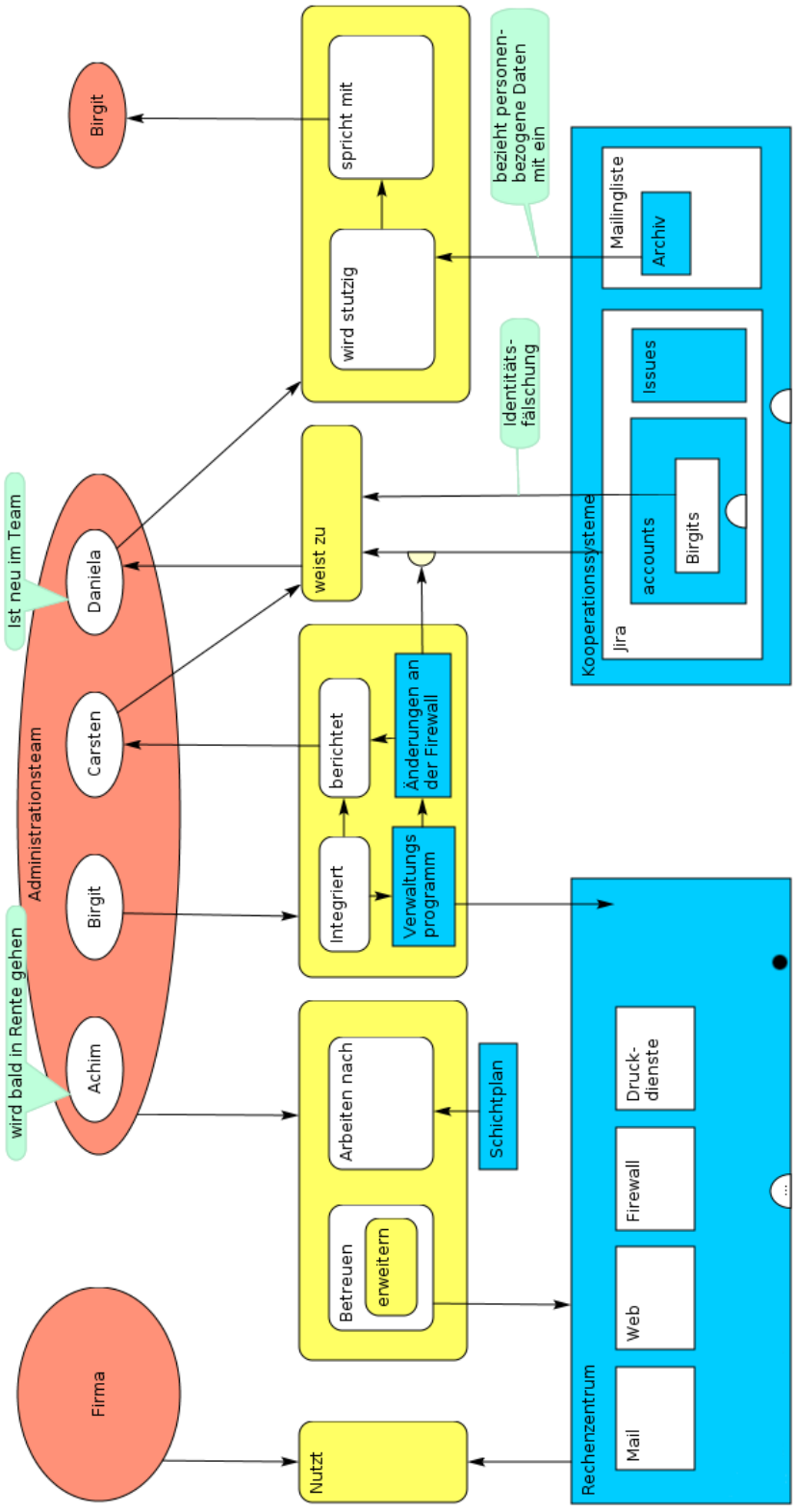


Abbildung 7: Modell „Die Neue“

Aufgaben abzugeben, für die er nur widerwillig und auf Druck von Achim Verantwortung übernommen hat. Er profitiert von Danielas Vertrauensvorschuss und entwirft dazu eine Kollusion. Der Vertrauensvorschuss resultiert aus Daniels role-based trust (vgl. 2.7). Birgit ist in sein Vorgehen nicht tatsächlich involviert, ihre Beteiligung wird von ihm nur simuliert.

Der Vertrauensvorschuss von Daniela ist aber nicht so groß wie von Carsten angenommen, einige kleine Hinweise aus alten E-Mails lassen sie schnell misstrauisch werden, so dass sie das Gespräch mit Achim sucht.

ISSUES Bei der Fälschung von Birgits Identität durch Carsten innerhalb des Ticketing-Systems sind kaum personenbezogene Daten von Birgit betroffen. Er nutzt ihre Identität im System, um Daten über sie zu produzieren. Diese gefälschten Daten enthalten dann wiederum vor allem VERKEHRSDATEN mit Personenbezug, nämlich solche, die belegen, dass Birgit Daniela die Behebung eines Fehlers zugewiesen hat. Daraus können auch noch Zusatzinformationen gewonnen werden, die aber im Szenario von niemandem genutzt werden, z.B., dass Birgit an etwas arbeitet, das die Arbeitsbereiche der anderen berührt.

Aus dem E-Mail-Archiv, auf das Daniela Zugriff gewährt wird, erhält sie Informationen über die Diskussion um die Zuständigkeitsbereiche. Das Archiv hält Informationen über alle bereit, die in dem Archivierungszeitraum an die Adresse der Liste eine E-Mail geschickt haben. Neben den bisherigen Administratoren können das auch Dritte, wie andere Mitarbeiter_innen des Unternehmens oder Ehemalige, sein. Weitere Informationen, genauso wie detaillierte VERKEHRSDATEN - wann wer eine E-Mail geschickt hat - werden von ihr in diesem Szenario nicht verwendet.

NUTZUNG Carsten missbraucht seine Zugriffsrechte, um über Birgits Account Einträge im System vorzunehmen. Dazu liegt ihm weder eine EINWILLIGUNG von Birgit vor, noch ist es für diese TRANPARENT. Da er Birgits Passwort kennt, scheint auch ein Problem bei der Datensicherheit vorzuliegen.

In Bezug auf die Mailingliste ist nicht bekannt, ob die Mitarbeiter_innen in eine Archivierung und mögliche Freigabe für Dritte eingewilligt haben. Schließlich ist die Archivierung, wie bei vielen Systemen, standardmäßig aktiviert, weshalb nicht davon ausgegangen werden kann, dass die Archivierung und Nutzung durch Daniela für die anderen transparent ist. Unklar ist zudem, ob das Archiv im Sinne der DATENVERMEIDUNG überhaupt angelegt werden muss, oder nicht Jira die Archivierungsfunktion übernimmt. Über eine Regelung der LÖSCHUNG ist ebenfalls nichts bekannt.[34] Bei der großen Informationsmenge, die potentiell aus den E-Mails gewonnen werden kann, ist es zudem schwierig, einen konkreten Zweck abseits dem der Kommunikation zu definieren.

3.6 SZENARIO 3: DER SKANDAL

Kontext

Alex und Dominique arbeiten seit längerem als wissenschaftliche Mitarbeiter_innen am Lehrstuhl von Professor Christoph an einer Universität

34 Als Beispiel: Mailman sieht keine Möglichkeit vor, die Speicherdauer des Archivs zu begrenzen

in Deutschland. Da unter den Wissenschaftler_innen ein offenes, kooperatives Klima herrscht, gemeinsam an Projekten gearbeitet wird, Rechercheergebnisse geteilt oder Termine organisiert werden, nutzen sie diverse Groupware-Systeme. Zur Unterstützung ihrer Zusammenarbeit organisieren sie ihren Dateiaustausch über ein webbasiertes System, in welches die Mitarbeiter_innen Dokumente einstellen, um gemeinsam an ihnen arbeiten zu können. Auch Kalenderdaten aller Personen sind dort gespeichert, damit sie gemeinsame Termine organisieren können. Sie verzichten dabei überwiegend auf eine genaue Zugriffssteuerung.

Situation

Vor wenigen Wochen wurde ein Forschungsantrag über *Marktstruktur von IT-Großprojekten* bewilligt an dem die Drei lange und ausführlich gearbeitet hatten. Das Projekt soll untersuchen, ob und in wie weit einzelne, große IT-Konzerne den Markt dominieren. An diesem Projekt, das *IT-WORLD* heißt, sind neben dem Lehrstuhl einige international tätige IT-Unternehmen beteiligt. Da aber noch andere Forschungsprojekte parallel laufen, können nur zwei der drei an dem neuen Projekt mitwirken. Christoph entscheidet sich dafür, sich mit Alex verstärkt um *IT-WORLD* zu kümmern. Dominique ist von dieser Entscheidung nur wenig begeistert, immerhin hält sie sich für fähiger als Alex, findet sich aber widerwillig damit ab.

Eskalation

In den kommenden Wochen sind Christoph und Alex viel international unterwegs, um verschiedene Produktionsstätten der Projektpartner zu besichtigen, IT-WORLD vorzustellen und sich mit den Kooperationspartnern zu organisieren. Dominique verfolgt die vielen Reisen mit etwas Neid, der noch dadurch verstärkt wird, dass die beiden Reisenden nur wenig von ihren Aktivitäten berichten und Dominique auf diese Weise noch deutlicher ausgrenzen. So haben sie zuletzt sogar den Zugriff auf einen Ordner im Dateiaustausch-System für sie gesperrt. Dieses in der Gruppe sehr ungewöhnliche und deswegen auffällige Verhalten hatten sie mit dem Hinweis auf Unternehmensinterna der Projektpartner, die nicht nach Außen gelangen dürften, gerechtfertigt.

Dominique wird danach misstrauisch und beobachtet das Verhalten der beiden genauer. Eines Morgens, während Christoph gerade für eine Woche auf einer Konferenz in der Schweiz ist, bemerkt sie, dass vor wenigen Stunden eine Änderung in dem Ordner vorgenommen wurde, deren Einsicht ihr nicht erlaubt ist. Sie kann allerdings einsehen, dass Christoph die Veränderung vorgenommen hat und das Programm zeigt auch die IP-Adresse an, über die Christoph eingeloggt war. Aus ihrem Studium ist ihr noch bekannt, das IP-Adressbereiche Weltregionen zugeordnet sind. Sie wird stutzig, denn die IP-Adresse scheint auf den ersten Blick nicht aus dem europäischen Raum zu stammen. Mittels eines Internetdienstes[35] kann sie Thailand zuordnen.

Dominique spricht daraufhin mit Alex darüber, die aber nur abwiegelt. Vermutlich sei Christoph über einen Anonymisierungsdienst ins Netz gegangen. Dominique ist nur wenig überzeugt, da Christoph so noch nie vorgegangen war und sie sowieso schon misstrauisch geworden ist. Als sie einige Zeit später zufällig an Alex geschlossener Bürotür vorbei läuft, hört sie, wie diese sich mit Christoph unterhält. Sie will die Sache direkt klären und betritt ungefragt den Raum. Mit Erstaunen sieht sie nun Christoph, der per Videochat zugeschaltet ist, im T-Shirt an einem sonnigen Ort, der nur wenig nach der zu dieser Jahreszeit überwiegend verschneiten Schweiz aussieht. Ziemlich perplex verlässt

35 solche Dienste bietet gratis z.B. http://www.hostip.info/ an

sie den Raum wieder. Ihr fällt wieder ein, dass vor einiger Zeit an einer anderen Uni ein Professor über eine Dienstreiseaffäre gestolpert ist.

Um Beweise für weitere Unregelmäßigkeiten zu finden, greift sie auf die Gruppenkalender zu, die sie gemeinsam nutzen, um Termine, die möglicherweise für alle relevant sind, zu verwalten. Sie findet dort allerdings kaum Einträge zu den vergangenen Monaten. Mithilfe von Sicherungsdateien, die sie wöchentlich von ihren lokalen Kopien automatisiert angelegt hat, kann sie aber ältere Kalenderdateien wiederherstellen, in denen Alex und Christoph Termine und Konferenzen eingetragen hatten, die, wie sie durch Internetrecherchen herausfindet, zu diesen Zeitpunkten nicht stattgefunden haben. Am darauf folgenden Tag wendet sie sich mit diesen Informationen an den Dekan ihrer Fakultät, um die Sache untersuchen zu lassen. Es stellt sich heraus, dass Christoph auf Kosten eines an dem Projekt beteiligten Unternehmens statt zu einer Konferenz nach Thailand geflogen ist, um sich dort eine Woche Urlaub zu gönnen. Alex ist eingeweiht gewesen und hat nachweislich bereits ähnliche Vorteile in Anspruch genommen.

ZUSAMMENFASSUNG Ein Gruppe von Wissenschaftler_innen startet ein neues Forschungsprojekt. Die Arbeitsteilung ist aber nicht zur Zufriedenheit aller Beteiligten, Dominique fühlt sich benachteiligt. Die Unzufriedenheit schlägt in Misstrauen um, was wiederum durch das Fehlverhalten der anderen bestärkt wird. Dominique nutzt die technische Infrastruktur, um ein Fehlverhalten zur persönlichen Bereicherung zu belegen und macht dieses schließlich öffentlich.

TECHNOLOGIEN & DATEN Die am Lehrstuhl eingesetzte Software dient der kollaborativen Zusammenarbeit (solche Funktionen bietet z.B. BSCW)genauso wie der Koordination (Kalender). Basic Smart, Cooperate Worldwide (BSCW) ist eine webbasierte Dokumentenmanagement-Lösung im Sinne eines SHARED MATERIAL. Mit diesem Werkzeug lassen sich Dateien in einer Ordnerstruktur verwalten und über ein Rechtemanagement anderen Benutzer(-gruppen) zugänglich machen. Zusätzlich werden viele Elemente der ASYNCHRONOUS GROUWARE AWARENESS angeboten, weshalb sich einsehen lässt, wer wann ein Dokument eingestellt hat, aber auch wer es wann gelesen hat.

Das ICS Kalenderformat bietet in Zusammenarbeit mit einer Serversoftware verschiedene Möglichkeiten zur Aufgaben- und Terminverwaltung. So lassen sich mehrere Kalender verwalten und sie für andere Benutzer zugänglich machen. Ein weiteres Feature erleichtert darüber hinaus das Finden von gemeinsamen Terminen. Wesentliche Patterns entsprechen der Kategorie der COLLABORATION PLACES.

AUSLÖSER Dominiques Unzufriedenheit mit der Koordination der Projekte, nämlich dass nicht sie, sondern Alex das Projekt durchführen darf, führt zu einem Vertrauensbruch. Dominique ist misstrauisch gegenüber Alex und Christoph und beobachtet deren Verhalten recht genau. Ihr Misstrauen wächst weiter, als sie feststellt, dass ihr auch nicht mehr getraut wird und ihr im BSCW der Zugang zu bestimmten Dokumenten verwehrt wird.

ISSUES Alex initiales Misstrauen beruht nicht auf Informationen, die sie aus den Systemen zieht, sondern rührt aus der Kenntniss darüber, dass das Vorgehen der anderen unüblich ist. Anders verhält es sich

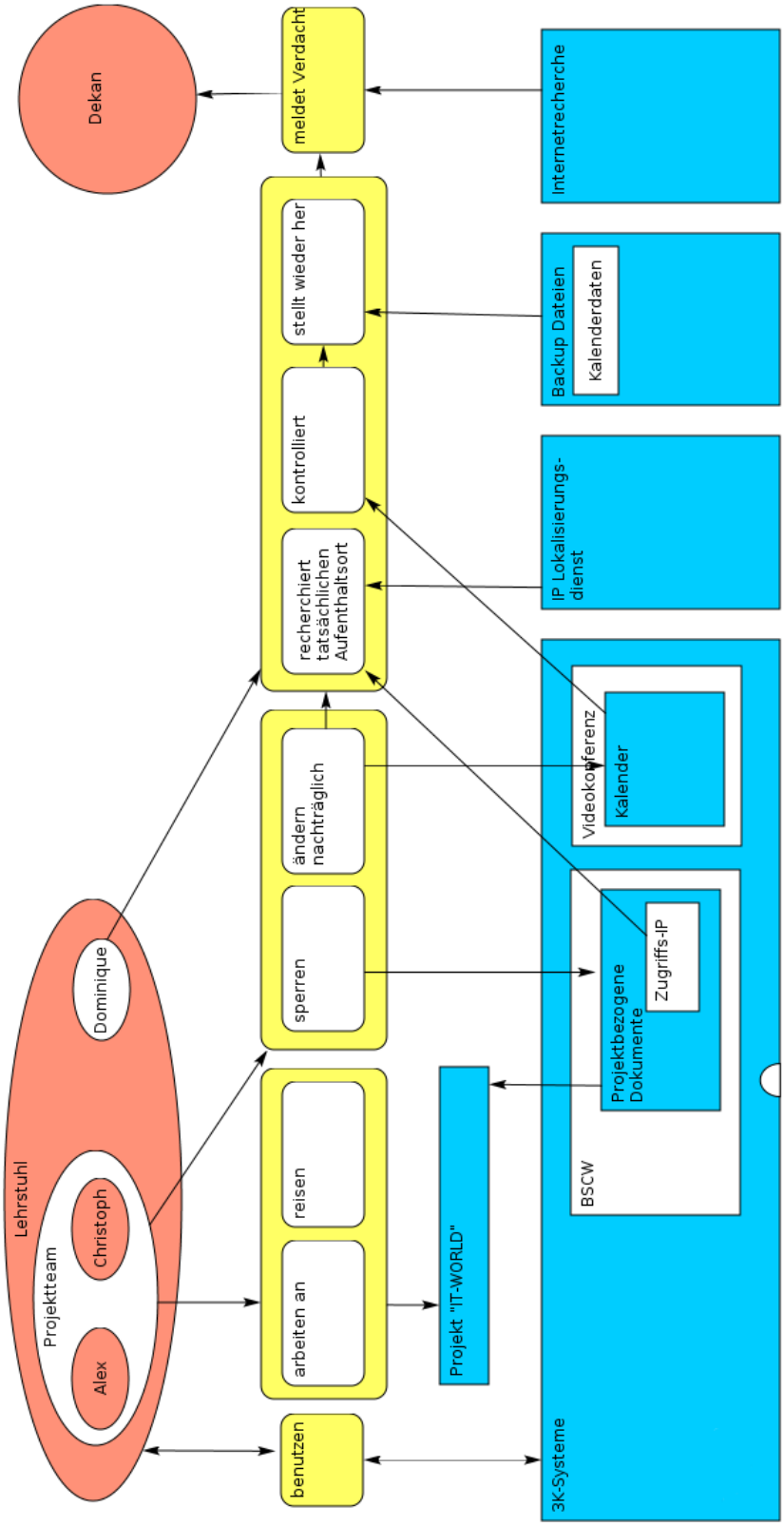


Abbildung 8: Modell „Der Skandal“

bei der Nutzung der IP-Adresse aus dem BSCW. Diese Information aus den VERKEHRSDATEN benutzt sie, um die Position von Christoph zu bestimmen.[36] Ihr Zugriff betrifft außerdem die INHALTSDATEN, die der Kalender bereithält, wobei hier nicht die Informationen über das Ziel der Reisen entscheidend ist, sondern die Information, dass die Einträge nachträglich geändert wurden.

NUTZUNG Dominique wird durch eine Information aus dem Dateisharing-Tool zufällig (spontan) auf die Unregelmäßigkeit aufmerksam. Die IP-Adresse, mit der Christoph eingeloggt war, konnte sie einem anderen Land zuordnen, als dem, in dem Christoph vorgab zu sein. Im vorliegenden Fall sind die Daten direkt einer Person (bzw. einem Benutzer_innennamen) zugeordnet, und lassen Rückschlüsse über den Aufenthaltsort ihres_r Besitzers_in zu. Die Preisgabe der IP-Adresse folgt aus einer Standardeinstellung des Systems, welches sie speichert. Es kann aber nicht davon ausgegangen werden, dass eine *Einwilligung* zur Veröffentlichung zum *Zweck* der Positionsbestimmung vorliegt. Da die Datenerhebung zur Standardeinstellung der meisten Webserver gehört, wird in der Regel auch darauf verzichtet, *Transparenz* über sie zu schaffen, obwohl eine *Datenvermeidung* dem Nutzen des Systems keinen Abbruch täte, denn die Benutzer_innen authentifizieren sich primär über den Login.

Etwas anders sieht es bei der Nutzung der Daten aus dem Kalender aus. In dessen Nutzung durch Kolleg_innen haben alle eingewilligt. Auch die Zweckbindung, nämlich feststellen zu können, zu welchem Zeitpunkt eine Person sich an welchem Ort aufhält, ist nicht verletzt. Allerdings ist die Überwachung der Kalender, wie Alex sie vornimmt, eine geplante Aktion, um für ein anfängliches Misstrauen Bestätigung zu finden. Diese Nutzung widerspricht dem eigentlichen Zweck des Kalendersystems, gemeinsame Termine zu finden und sich zu koordinieren.

3.7 ZUSAMMENFASSUNG

In den vorangegangenen Abschnitten dieses Kapitels werden drei Szenarien vorgestellt, die ein breites Spektrum an möglichen Konstellationen von Datenschutzproblemen bei dynamischen Vertrauensverhältnissen in IT-gestützten Kooperationssystemen widerspiegeln.

Die Varianz liegt dabei auf den Einsatzbereichen der genutzten Technologien in und zwischen den Kategorien Kommunikation, Kooperation und Koordination. Die Auslöser für Änderungen der dargestellen Vertrauensverhältnisse, die schließlich zum Missbrauch personenbezogener Daten führen, können spontan oder geplant sein. Der Aufwand der Datenaneignung liegt zwischen der Auswertung vorliegender bis zu expliziter Erhebung von Daten zur missbräuchlichen Nutzung. Die Daten stammen dabei aus den Kategorien Verkehrs-, Inhalts-, und Stammdaten; außerdem variieren in den Szenarien ebenfalls Mittel und Wege, mit denen die erhobenen Daten weitergegeben wurden.

Die drei Szenarien enthalten alle Elemente von sich ändernden Vertrauensverhältnissen. Dabei geht es nicht darum, dass diese Änderungen problematisch sind, unerwünscht oder von irgendeinem Nachteil. Im Gegenteil, Konkurrenzsituationen, wie in *Die Macht der Statistik*,

36 Solche Dienste lassen sich aber austricksen, indem man, wie Alex auch anmerkt, ein Proxy verwendet

sind in Unternehmen Teil des Alltags. Genauso sind Umbrüche, wie in *Die Neue*, nicht ungewöhnlich, wenn Angestellte ein Unternehmen verlassen und neue dazu kommen. Nicht zuletzt kann ein wenig Skepsis gegenüber auffälligem Verhalten, wie in *Der Skandal* unrechtes Verhalten aufdecken.

Der wesentliche Punkt ist, dass alle Änderungen in den Vertrauensverhältnissen initiiert, gestützt oder verstärkt werden durch personenbezogene Daten aus den informationstechnischen Systemen, die die Gruppen einsetzen. Wie in den an die Szenarien anschließenden Analysen herausgestellt wurde, widerspricht in vielen Fällen die Nutzung der Daten durch die Protagonisten den grundsätzlichen Datenschutzprinzipien. In *Die Macht der Statistik* ist durch den Datenmissbrauch eine Verschärfung zu beobachten, die in dieser Form bei datenschutzkonformem Verhalten nicht aufgetreten wäre. Die Tatsache, dass der Einsatz von computervermittelter Interaktion weiter steigt und damit auch die Menge und Qualität der Daten, macht vor dem Hintergrund des Szenarios deutlich, dass Strategien nötig sind, mit diesen Daten datenschutzfreundlich umzugehen.

Selbst wenn man die zweckentfremdende Nutzung der Daten in *Der Skandal* als angemessen einschätzen will, ist anzumerken, dass selbst für Alex und Christoph Datenschutz zu gelten hat.

Nach dieser ausführlichen Analyse ist der nächste Schritt nach TAIDA die Diskussion und Bewertung von Maßnahmen, die die vorgestellten Szenarien positiv, im Sinne des Datenschutzes, beeinflussen können.

4 MASSNAHMENBESCHREIBUNG

Im vierten Kapitel werden verschiedene technische und organisatorische Maßnahmen vorgestellt, die an unterschiedlichen Punkten der Szenarien deren Verlauf zu Gunsten des Datenschutzes beeinflussen können. Der Maßnahmenkatalog geht aus einer umfangreichen Recherche hervor, die den Bereichen Datenschutz und Datensicherheit insbesondere in der CSCW-Forschung und angrenzenden Gebieten entstammt.[37] Darüber hinaus wurden Gespräche mit 3 Datenschutzexpert_innen geführt. Die Ergebnisse aus Recherche und Gesprächen werden im folgenden vorgestellt. Der Maßnahmenkatalog ist organisiert nach den Kategorien ERHEBUNG (4.2), ZUGRIFFSSTEUERUNG (4.3), NUTZUNGSSTEUERUNG (4.4) und ORGANISATORISCHE REGELN (4.5), die an jeweils unterschiedlichen Punkten des Nutzungsprozesses ansetzen (vgl. 9). Die Kategorisierung stellt dabei vor allem eine Einschätzung dar, an welchen Stellen die Maßnahmen am sinnvollsten eingesetzt werden können. Allerdings sind die Kategorien nicht immer trennscharf, dienen aber dennoch in ihrer Konstruktion und Auswahl der Übersicht.

Die Maßnahmen unterscheiden sich zudem stark darin wie groß der mögliche Aufwand wäre, sie in die Szenarien einzubringen. In der Beschreibung wird darauf verzichtet Maßnahmen auszuschließen, nur weil die in den Szenarien eingesetzte Technik und nicht im Sinne der Maßnahmen anpassbar ist,[38] damit sie in zukünftigen Entwicklungen einfließen können und keine potentiellen Konstruktionen ausschließen.

4.1 EXKURS: EXPERT_INNEN-INTERVIEWS

Zur Evaluation der Szenarien und um geeignete und praxisnahe Maßnahmen zur Problembehebung erarbeiten zu können, wurden im Rahmen dieser Arbeit drei Interviews mit Datenschutzexpert_innen geführt.

Drei Expert_innen haben zur Thematik Stellung bezogen

Expert_innen-Interviews sind eine Methode der qualitativen Forschung.[39] Diese grenzt sich von der quantitativen Forschung, die sich auf möglichst große statistischen Datenmengen bezieht, dadurch ab, dass durch nicht standardisierte Interviews versucht wird, das Feld aus Sicht der Beteiligten zu erfahren. Während in der quantitativen Forschung durch gleichförmige Interviews oder Fragebögen versucht wird Hypothesen, die die Forscher_innen vor der Erhebung aufgestellt haben, zu ferifizieren oder zu falsifizieren, dient der qualitative Ansatz dazu, einen nicht vollständig erschlossenen oder erschliessbaren Forschungsgegenstand aus Sicht von Beteiligten erfassbar zu machen

Für diese Arbeit bietet sich dieses Vorgehen an, weil ich davon ausgehe, dass es keine objektiv richtige, vollständige und überprüfbare Lösung für die Probleme dynamischer Vertrauensverhältnisse am Arbeitsplatz gibt. Die Interviews bieten die Möglichkeit das Problem zu diskutieren und die aus der Expert_innensicht besten Maßnahmen,

37 Insbesondere in der Forschung zu ubiquitärem Computereinsatz werden ähnlich dynamische Probleme betrachtet

38 Das ist etwa bei proprietärer Software oft der Fall.

39 Das Vorgehen und die im folgenden erläuterte Methode richten sich nach Lamnek (2005)

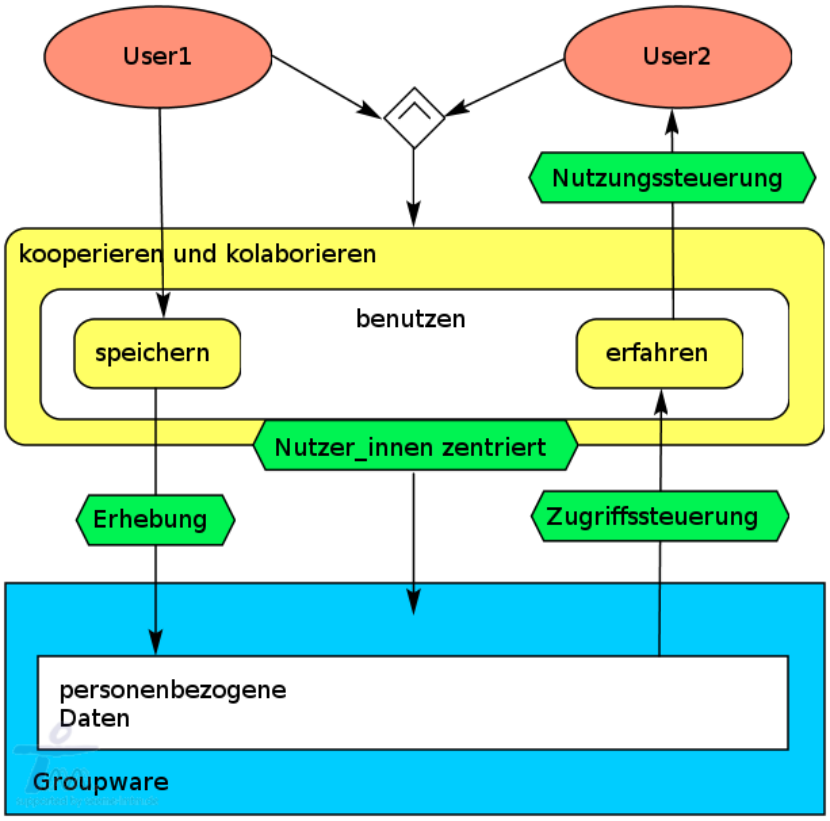


Abbildung 9: Maßnahmenkategorien

sowie Vor- und Nachteile verschiedener Verfahren zu erfahren und in meine Arbeit einfließen zu lassen.

Die Interviews bewegten sich dabei zwischen episodischen und fokussierten Interviews, in denen die Interviewten mit Hilfe der den Szenarien angeregt wurden vor dem Hintergrund ihrer Erfahrungen mögliche Lösungen zu durchdenken und zu artikulieren.

Die Auswertung erfolgte nach Meuser and Nagel (1991) in 5 Stufen

1. TRANSKRIPTION Die Interviews wurden aufgezeichnet und im Anschluss in transkibiert.
2. PARAPHRASIERUNG Im Anschluss wurden die Texte in thematische Blöcke unterteilt.
3. KODIERUNG Den verschiedenen Blöcken wiederum wurden Überschriften zugeordnet.
4. THEMATISCHER VERGLEICH Anhand dieser Überschriften wurden die verschiedenen Interviews in einen Zusammenhang mit den Ergebnissen der vorangegangenen Recherchen gebracht.
5. KONZEPTUALISIERUNG Zuletzt wurden die Inhalte der Interviews weiter abstrahiert und zu Thesen verdichtet.

Die Ergebnisse der ersten vier Schritte finden sich im Anhang A.2. Um einen Eindruck der Interviews zu vermitteln sind die wichtigsten Themen im folgenden hier zusammengefasst:

4.1.1 *Zusammenfassung von Interview 1*

Die Interviewte legt Wert darauf, dass ein klar definierter Prozess zur Einführung neuer Software eingehalten werden müsste. Dazu gehören insbesondere die Erarbeitung eines Berechtigungskonzept.

Berechtigungskonzepte

> bei den collaboration Tools [ist] deutlich zu bemerken ist, dass [..] alles so bunt ist und alle es so toll finden und deswegen der klassische der systematischen Dokumentation und Konzeptionieren von Berechtigungen unterbleibt, also dass der konzeptionelle Teil unterbleibt und das die Systeme häufig auch nicht in der Lage sind feingranulare Berechtigungen zu vergeben.

Ein gut durchdachtes Berechtigungskonzept würde dazu beitragen, dass viele der Probleme aus den Szenarien nicht entstehen. Dazu sei es nötig für eine strikte Einhaltung der Berechtigungen zu sorgen und auch Organisationsstrukturen einzuhalten.

> Ein Unternehmen, was ein Wiki erlaubt und ermöglicht muss dann aber umso mehr vorgeben, was die Grundregeln der Benutzung sind.

Zudem müssten für wesentliche Prozesse auch Verfahren definiert sein. Beispiel: Ein_ Mitarbeite_in scheidet aus dem Unternehmen aus:

> Definieren wir einen Workflow, in dem Moment in dem die Personalabteilung weiß da scheidet jemand aus, drückt sie auf einen Knopf und dann gibt es eine Benachrichtigungskette beispielsweise an die EDV. [..] Dann weiß die EDV „[dem müssen] wir zu dem Zeitpunkt eben also auf jeden Fall schon einmal die Netzwerkberechtigungen entziehen." Und dafür muss man überlegen [..] wie man den Workflow am besten definiert. Aber Ziel ist es natürlich, dass [..] der Abteilungsleiter dann auch eine Mail kriegt in der steht „Sie werden aufgefordert alle Berechtigungen die der Mensch hatte entweder zurückziehen zu lassen oder aber selbst zurückzunehmen."

Die Interviewte räumte zudem ein, dass gerade in kleinen Unternehmen und Gruppen ohne feste Hierachiestruktur, die vorherige Konzeption der Berechtigungen und Einhaltung der Prozesse, aus unterschiedlichsten Gründen nicht geleistet wird oder werden könne.

Verantwortung für eine geregelte Einführung und Einhaltung von Berechtigungskonzepten in kollaboration Software liege bei den Organisation.

Ein Problem sei aber, dass in vielen Softwarelösungen diese Aufgaben auf die Benutzer_innenebene verlagert worden seien, so dass diese

Entlastung der Angestellten

> neben ihrer Fachtätigkeit auch noch halbe Administratoren sind und wissen müssen sie bestimmte Dinge steuern und lenken müssen.

Die Organisationen würden teilweise die Verschiebungen auch gerne übernehmen, da dadurch die aufwendigen und kostspieligen Vorarbeiten verkürzt werden könnten.

Problematisch ist nach Meinung der Expertin bei Groupware zudem, dass oft mehrere verschiedene Lösungen eingesetzten werden, zwischen denen ein Datenaustausch stattfinde. Hier die Zweckdefinitionen

über die Schnittstellen hinweg aufrecht zu erhalten sei schwierig, Informationen die einmal elektronisch erhoben worden seien, seien nur noch schwer zu kontrollieren. Für Fotos in einer Webplattform müsse etwas gelten, dass

> sie einfach nicht exportiert [werden dürfen], [..] weil Wenn die Daten erst einmal raus diffundiert sind, wird es immer schwieriger, Weil das Verständnis dafür was erlaubt ist oder nicht, [..] mit jedem Schritt geringer [wird].

Ausreichende Schulung der Mitarbeiter_innen vor der Nutzung neuer Software zur Sensibilisierung auch für Datenschutzthematiken sei notwendig, *Schulung*

> weil man kann vieles durch Technik, vieles durch Organisation machen, man kann auch einiges durch Vorschriften machen, aber das ist keine Garantie. Wenn die Leute es nicht verstehen und wenn sie nicht willens sind oder das ganze in erster Linie als Arbeitsbehinderungsmaßnahme begreifen, dann hat man keine Chance, dass das sinnvoll eingesetzt und eingehalten wird, was da als Vorgaben erdacht wurde.

4.1.2 *Zusammenfassung von Interview 2*

Der zweite interviewte Experte berichtete vor allem aus seiner Erfahrung als externer Datenschutzbeauftragter. Auch er favorisiert vorbeugende Maßnahmen wie Minimierung und Berechtigungskonzepte um Datenschutzprobleme auf technischer Ebene zu verhindern. *Vorabkontrolle*

> Optimal wäre es natürlich wenn die Systeme dann, weil ich [als Datenschutzbeauftragter] rechtzeitig gefragt worden bin, so eingerichtet sind, dass z.B. was in den Szenarien dabei war, dass zu irgendwelche Kalendereinträge gelöschte Daten rekonstruiert werden können, dass so etwas erst gar nicht möglich ist von den normalen Mitarbeitern.

Er verweist dabei auf die Mitbestimmungsmöglichkeiten des Betriebsrates, Regelungen über Betriebsvereinbarungen treffen zu können und Rahmenrichtlinien zu erarbeiten, die auf unterschiedliche Systeme anwendbar sind.

> [..] dass es eine Rahmenregelung gibt, sei es mit oder ohne Betriebsrat, und das man dann für die einzelnen Werkzeuge nur noch, [..] gucken muss, wie wird diese zentrale Regelung [..] auf das abgebildet.

Allerdings sei dies von durch die Organisation von Unternehmen nicht immer möglich *Problem junger Unternemhen*

> Gerade so junge Unternehmen [..] ist es selten, dass es da einen Datenschutzbeauftragten gibt und Betriebsrat noch viel weniger.

Bei wesentlichen Konfigurationsänderungen sieht er das Vier-Augen-Prinzip bei dem mindestens zwei Personen, eine davon wenn möglich aus der Personalvertretung, als gutes Mittel um die korrekte Umsetzung von Anforderungen zu gewährleisten. *Vier-Augen-Prinzip*

> Ich brauch zwei Leute die müssen beide angemeldet sein und wenn dann ein Fenster aufgeht, dann können Änderungen durchgeführt werden, [..] weil dann sichergestellt ist, man muss wirklich den Betriebsrat fragen. Hat man keinen Betriebsrat wäre zumindest sicherzustellen, das es jemand aus der Personalabteilung ist.

Er benennt aber auch klar die Grenzen und verweist, insbesondere bei Problemen die aus einem gestörten Vertrauensverhältnis resultieren, wie in den vorliegenden Szenarien, auf die Verantwortung von Vorgesetzten und Projektleiter_innen diese frühzeitig zu erkennen und zu lösen.

Verantwortung der Vorgesetzten

> [..]solche Sachen treten weniger auf wenn Führungsqualität da ist oder Leitungsqualität. Wenn ein Gruppenleiter nicht mitkriegt, dass in seiner Gruppe was nicht stimmt, dann fehlt ihm eine Qualifikation.

Eine Möglichkeit solche Probleme generell zu verhindern sieht er nicht. Viel mehr sei eine regelmäßige Überprüfung des Nutzungsverhaltens sinnvoll um die Einhaltung der Zweckbindung sicherzustellen.

Zweckbindung organisatorisch festlegen

> Das geht dann tatsächlich nur über organisatorische Regelungen, zu den Zwecken dürfen sie verwendet werden, alle anderen Verwendungen sind unzulässig. Alle Arbeitsrechtlichen Schritte, die auf Grund unzulässig verarbeiteter Daten getätigt wurden sind per se nichtig

Zudem müsse das Bewusstsein für die Problematik geschärft werden

Sensibilisierung

> Wenn [die Nutzung] sehr dynamisch ist [..], dann ist tatsächlich Sensibilisierung, Rahmenregelung, viel mehr kann man dann auch kaum noch machen.

Inbesondere auch wenn mehrere Datensammlungen zusammengeführt werden sollte.

Schnittstellenproblem

> Denn es ist natürlich ganz wichtig, dass wenn die Daten von einem System ins andere System wandern, das klar ist, zu welchen Zwecken waren sie da, das man dann immer noch prüfen kann: jetzt haben wir einen neuen Zweck

4.1.3 *Zusammenfassung von Interview 3*

Der dritte Experte ist, wie auch die andere, der Meinung, dass eine stärkere Formalisierung, in Form von Berechtigungskonzepten und definierten Prozessen, die Probleme im wesentlichen verhindern könnten.

Formalisierung

> So ähnlich wie in einer Verwaltung die Akten-Kommunikation das führende System ist, es gibt keine andere Kommunikation die von Relevanz ist für eine Verwaltung, außer die, die in den Akten stattfindet. Und da kann man für Datenschutz sorgen.

Das Problem sei aber, dass gerade in kleinere oder sich gerade im Aufbau befindlichen Unternehmen diese Formalisierung (noch) nicht vorgenommen wird.

Unternehmensgröße

> Wir haben gute Revisionsmechanismen in den weltweit agierenden Banken, die haben gute Revisionen. Das haben kleine Unternehmen und auch kleinere Verwaltungen in dem Sinne so nicht.

Diese Aufgabe und auch die Verantwortung bei Problemen die durch mangelhafte Formalisierung entstehen, weist er den Unternehmen zu. Sie zu erfüllen sei aber auch eine Aufgabe für Experten, da, je nach Firmenkultur, eine zu starke Strukturierung kreative Potentiale einschränken könnte.

Ein weiterer Teil des Gespräches ging um die Frage ob Datenschutz bei den beschriebenen Problemen nicht an seine Grenzen stoße. Per Definition sei dieser für die Stärkung der informationellen Selbstbestimmung gegenüber Organisationen zuständig, etwa beim Verhältnis Kund_in ? Unternehmen oder Bürger_in ? Verwaltung.

Datenschutz und Interaktionssysteme

> Die Unterscheidung: Interaktionssysteme, Organisationssysteme und Funktionssysteme. Datenschutz guckt zwischen Organisations- und Funktionssystemen. Guckt nicht auf die Interaktionssysteme. Sie machen den Blick auf die Interaktionssysteme. E29

In Interkationssystemen müsse die informationelle Selbstbestimmung auch in dem Sinne gelte, dass andere bestimmen können was sie über mich wissen.

informationelle Selbstbestimmung

> wie andere über mich reden als Menschen usw., dass ist deren Recht auf informationelle Selbstbestimmung. Was ich aber beeinflussen kann ist, wie in Organisationen über mich eine Datenverarbeitung stattfindet. E12

Trotz allem sei die Fragen interessant, da die Interaktionssysteme in den beschriebenen Fällen Teil von, vom Datenschutz regulierten, Organisationen seien.

Generell sei aber eine Maßnahme, die momentan in der Entwicklung befindlich ist, die stärkere Nutzung von Policies.

Policies

> Das sind Frameworks, beispielsweise welche Anforderungen an das Sicherheitsniveau eines Zertifikats zu stellen sind. Oder was für Signaturen man brauch: Reichen fortgeschrittene oder müssen es qualifizierte sein. Dann gibt es ein ganzes Set an hierarchischen Abstufbarkeiten, und Erforderlichkeiten für bestimmte Transaktionen in der Kommunikation E26

Um Revisionsfest und Erwartungssicher einen gemanagten Prozess steuern zu können(E28) müsse die Überprüfung aller vorher definierten Anforderungen und die Zweckmäßigkeit der Nutzung automatisiert anhand von Metainformationen geschehen.

4.1.4 *Abgeleitete Thesen aus den Interviews*

Der Konzeptualisierungsschritt mündet in der Entwicklung von vier Kernaussagen, die hier kurz vorgestellt werden.

THESE 1: BERECHTIGUNGSKONZEPT Auf Grund der (gesetzlichen) Verantwortung der Unternehmen zum betrieblichen Datenschutz sollte vor Einführung eines technischen Systems unter Einbeziehung der Angestellten und eine_s Datenschutzbeauftragten ein Berechtigungskonzept erarbeitet werden. Dieses sollte so weit wie möglich technisch umgesetzt werden und durch organisatorische Regeln ergänzt werden. Im besten Fall existiert eine Rahmenstruktur, die auch mit den Dynamiken der Szenarien umgehen kann, um eine ganzheitliche Informationssicherheits-Managementsysteme (ISMS) Infrastruktur aufzubauen.

THESE 2: UNTERNEHMENSKULTUR Gerade in kleinen und/oder jungen und sehr dynamischen Unternehmen sind die Voraussetzungen zur Erarbeitung eines Berechtigungskonzeptes oft nicht vorhanden. Dabei kommt zusammen, dass eventuell keine offizielle Mitarbeiter_innen-Vertretung existiert, genausowenig wie ein_e DSB. Gleichzeitig ist die Nutzung verschiedener kollaborativer Werkzeuge mit hoher Komplexität sehr ausgeprägt, wobei deren Nutzung sich dynamisch ändert und vertrauensbasierte Regelungen vorherrschen.

THESE 3: SCHULUNG Sensiblisierung, Schulung und Ausbildung von Nutzungsregeln, die auch in soziale Normen übergehen können, sind essentiell zur Verhinderung der Probleme, die in den Szenarien beschrieben werden. Sie sollten vom Arbeitgeber angeboten werden. Nicht zuletzt gehört es dabei auch zu den Aufgaben von Vorgesetzten, die Probleme auf der sozialen Ebene früh zu erkennen und gegenzusteuern, sowie sich vorbildlich bei der Nutzung der Systeme zu zeigen.

THESE 4: NUTZUNGSKONTEXT Besonders bei der Nutzung von Schnittstellen zwischen mehreren Systemen enden die Möglichkeiten technischer Berechtigungskonzepte. Export oder die Verwendung der Daten aus einem System in einem anderen sind nur unzureichend regulierbar. Hier sind neue Verfahren notwendig, die die Einhaltung Datenschutzrechtlicher Regelungen über Schnittstellen und Systemänderungen hinweg gewährleisten.

Für die von den Expert_innen stets als wichtig betrachtete Prozessbeschreibung und die genaue Regelung der Benutzungssteuerung (These 1), existiert in der betrieblichen Praxis bereits ein breiter Katalog an Maßnahmen.[40] Daher wird im folgenden ein größerer Schwerpunkt auf dynamische und kontextsensitive Systeme gelegt, sowie auf Maßnahmen, die in kollaborative Umgebungen eingesetzt werden können.

4.2 ERHEBUNG

Eine der effektivsten Möglichkeiten die Zweckentfremdung personenbezogener Daten abzuwenden ist, ihre Erhebung zu verhindern oder zumindest einzuschränken. Datenminimierung ist daher auch eines der Datenschutzprinzipien 2.3. Allerdings steht die Option nicht bei jedem System in gleichem Maße zur Verfügung. Die Idee kommuni-

40 Am bekanntesten sind hier die Grundschutzkataloge, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben werden. Die Kataloge enthalten ausführliche Listen zur möglichen Gefährdungen von IT-Systemen und Gegenmaßnahmen zur Sicherung dieser und richten sich vor allen Dingen an Unternehmen.

NR.	FUNKTION	GESPRÄCHSDAUER
1	Datenschutzberatung	ca. 60 Min.
2	Datenschutzberatung	ca. 70 Min.
3	Datenschutzrechtler	ca. 30 Min.

Tabelle 1: Interviewübersicht

kationsunterstützender Software, wie E-Mail, ist es gerade, Daten und Informationen zwischen Personen in dem Maße zu vermitteln, wie sie von den Anwender_innen eingetragen werden. Sinnvoller kann es deswegen sein, den Personenbezug einzuschränken bzw. im Bestfall zu verhindern.

4.2.1 *Vorabkontrolle und Mitbestimmung*

Die Menge der personenbezogenen Daten ist auf diejenigen zu reduzieren die zur Nutzung des Systems erforderlich sind. Dies sicherzustellen sowie Nutzungszwecke und Löschfristen festzulegen, sind Aufgabe eines_r Datenschutzbeauftragten_r während der Vorabkontrolle. Die Vorabkontrolle ist im BDSG gesetzlich geregelt, genauso wie die Notwendigkeit eines_r Datenschutzbeauftrage_r (DSB) in jedem Unternehmen in denen *neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten*[41] beschäftigt sind.

Die Vorabkontrolle sollte vor der Einführung neuer Softwaresysteme stattfinden. Zudem ist der Betriebsrat eines Unternehmens in der Regel mit einzubeziehen.[42]

4.2.2 *Datenminimierung*

Datenminimierung ist eines der Grundprinzipien des Datenschutzes. Je geringer die Zahl der personenbezogener Daten ist, desto geringer ist das Missbrauchspotential. Wright et al. (2008) empfehlen deshalb, bereits bei der Entwicklung neuer technischer Systeme eine Selektion so früh wie möglich vorzunehmen, das heißt etwa bei eingebetteten Systemen die Hardware so herzustellen, dass nur benötigte Daten erhoben werden, genauso sollte bei der Software darauf geachtet werden das etwa bei Anmeldemasken nur so wenige Daten erfragt werden, wie unbedingt nötig sind. Sollten weitere Daten anfallen, weil sie etwa die für den Betrieb notwendig sind, sind sie vor der Weiterverwendung zu schützen und nur temporär, also auf einem nicht-persistenten Speichermedium, abzulegen. Gespeicherte Daten sollten zudem so früh wie möglich gelöscht werden.

Groupwaresysteme nutzen eine vielzahl personenbezogener Daten

In Groupwaresystemen, die meist personalisierte Dienste anbieten, lässt es sich nicht vermeiden, das einige Informationen über die Nutzer_innen erhoben werden. Eine zu rigorose Minimierung kann hingegen sogar dazu führen, dass wesentliche Funktionen nicht mehr den gewünschten Effekt erzielen und das Groupwaresystem als solches obsolet wird. Iachello and Hong (2007) verweisen etwa auf eine Stu-

41 § 4f Abs. 1. BDSG

42 Das BetrVG sieht die Beteiligung des Betriebsrates vor, wenn ein einzuführendes System dazu geeignet ist die Leistung und/oder das Verhalten von Mitarbeiter_innen zu kontrollieren. Bei Groupware-Systemen ist dies in der Regel immer der Fall.

die, die die Erwartung an Awareness-Information beschreibt. In einem Groupwaresystem wurde der Status *Do Not Disturb* durch *Offline* ersetzt, mit der Begründung, dasser die Mitteilung - der_die User_in ist in diesem Status nicht erreichbar - im Prinzip die selbe sei. Von anderen Nutzer_innen wurde hingegen daraufhin angenommen, dass entweder jemand tatsächlich abwesend sei - eben *Offline* - ist, oder es einen Defekt im System gebe. Den Status zu streichen hatte einen Verlust an Funktionalität zur Folge. Die regelmäßige Nutzung solcher Systeme lässt also auch Anforderungen auf Seiten der Nutzer_innen erwachsen, hinter die nicht ohne Effektivitätseinbußen zurückgekehrt werden kann.

Ein Problem besteht in der Praxis auch dadurch, dass in vielen Unternehmen kommerzielle Standardsoftware verwendet wird, welche - gerade wenn sie nicht quelloffen ist - kaum Minimierung erlaubt. Da bei der Entwicklung ein möglichst breiter Nutzungskontext berücksichtigt wird, sind meist Funktionen enthalten, die zwar nicht benötigt, aber auch nicht deaktivierbar sind. Diese Probleme können auch verstärkt werden, wenn Software zusätzlich von einem Hersteller stammt in dem, auf Grund des Herkunftslandes ein anderes Verhältnis zum Datenschutz - am Arbeitsplatz oder auch generell - herrscht.

4.2.3 *Anonymität*

Ein anonym nutzbares System ist eines, bei dem keinerlei personenbeziehbare Daten erhoben werden. Pfitzmann and Hansen (2009) definieren Anonymität wie folgt:

> Anonymity of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the anonymity set.

Praktisch bedeutet dies, dass ein Datensatz keiner bestimmten Person, aus einer Menge von bekannten Personen, mehr zuzuordnen ist. Voraussetzung für Anonymität ist also, dass sich die Person in einer Gruppe von Personen (ANONYMITY SET) befindet. Anonymität ist dann hergestellt, wenn eine_e Angreifer_in in diesem ANONYMITY SET keine einzelnen Personen identifizieren kann.[43] In Groupwaresystemen ist Anonymität aus mehreren Gründen nur schwer herzustellen.

1. Anonymität widerspricht einigen der Nutzungsideen von Groupwaresystemen.[44] Eine der wesentlichen Aufgaben ist es eine Handlung einer bestimmten Personen zuordnen zu können. Insbesondere die KOORDINATION und KOMMUNIKATION von Gruppen sind nur schwer ohne Personenbezug zu realisieren. Ein Kalender, dessen Einträge zwar einsehbar sind, der selbst aber keiner Person zugeordnet werden kann, hat für Koordinierungsaufgaben keinen

43 Pfitzmann and Hansen definieren darüber hinaus auch eine Maßeinheit für Veränderungen im Grad der Anonymität: das ANONYMITY DELTA. Dabei nehmen sie an, dass eine attackierende Person über den Zeitraum einer Attacke Daten observiert und damit möglicherweise ein negatives ANONYMITY DELTA erreichen kann, d.h. Personen könnten deanonymisiert werden. Sie legen dabei fest, dass ein ANONYMITY DELTA nur negativ, bestenfalls null, sein kann, da im Rahmen einer Observation stets Daten bestenfalls zur Deanonymisierung beitragen, nie aber die Anonymität stärken. Sieht man sich aber einen Datensatz unabhängig von einer aktuell laufenden Observation an, ist hingegen auch vorstellbar, dass das ANONYMITY DELTA einen positiven Wert annimmt, z.B. in dem Fall, dass Daten in bestimmten Zeitabständen unkenntlicher gemacht werden.

44 Zu den Vor- und Nachteilen von Anonymität in CSCW-Systemen siehe Gr\äslund and Krcmar (2001)

Wert.[45] Schwierig gestaltet sich auch die sinnvolle Nutzung eines anonymisierten Videochats, bei dem sowohl Bild als auch Ton verfremdet werden müssten.

Aufgaben die KOLLABORATIV gelöst werden, lassen sich dagegen in einigen Fällen anonym gestalten. Hierzu wurden bereits Mechanismen des *Reputationsmanagements* entwickelt, die dabei helfen anonyme Kollaborationspartner, anhand ihres bisherigen Verhaltens, einzuschätzen.[46]

2. Oft ist das ANONYMITY SET nicht groß genug. Wie Sweeney (2002) belegen und Machanavajjhala et al. (2007) fortführen, ist zu Herstellung von Anonymität ein ausreichend großes Set an Daten notwendig (K-ANONYMITY), in dem zusätzlich eine gewisse Vielfalt (L-DIVERSITY) die Identifizierung Einzelner verhindert. In den vorliegenden Szenarien gehen wir aber von Kleingruppen aus. Um hier Anonymität herzustellen, müsste eine wesentliche Anzahl von Daten gestrichen werden. Dies ist in den meisten Fällen nicht möglich ohne (siehe 1.) die Funktionalität wesentliche zu beeinträchtigen.

Zusatzwissen erleichtert Deanonymisierung

Eine komplett anonyme Nutzung ist also nicht nur nicht gewünscht, sondern auch nur schwer zu erreichen. In den Szenarien verfügen die Beteiligten nicht nur über die digital vorliegenden Informationen der Kooperationssysteme, sondern auch, abhängig davon wie stark das Vertrauen innerhalb der Gruppe ist, über Zusatzwissen, dass dabei helfen kann anonyme Daten einer Person zuzuordnen. Wer etwa weiß, an welchen Projekten ein_e Arbeitskolleg_in beteiligt ist, kann einen anonymisierten Kalender anhand der Termine zuordnen.

Da in fragilen Vertrauensverhältnissen bereits ein einzelnes, misstrauenerregendes Ereignis, basierend auf einer nicht anonymen Information, zum Problem führen kann, ist der Nutzen der Anonymisierung gering (vgl. *Die Neue*). Sind hingegen viele Datensätze notwendig (vgl. *Die Macht der Statistik*) können anonymisierte Daten Schutz bieten, da der manuelle Aufwand zu Deanonymisierung hoch ist.

4.2.4 *Pseudonymität*

Ein Pseudonym beschreiben Pfitzmann and Hansen (2009) wie folgt

> A pseudonym is an identifier of a subject other than one of the subject's real names.

Der Sinn von Pseudonymität zeigt sich besonders im Vergleich mit Anonymität. Bei einem Pseudonym lässt sich eine Zuordnung zu einer Identität herstellen, die bei Anonymität per Definition nicht möglich ist, gleichzeitig ist aber die reale Person hinter diese Identität nicht bekannt. So lässt sich etwa pseudonymisiert kommunizieren, was anonym bei mehr als zwei Beteiligten nicht möglich ist, da Beiträge nicht mehr einzelnen Kommunikationspartner_innen zugeordnet werden

45 Eine Ausnahme bilden Kalender, die Objekten zugeordnet sind, wie etwa Raumbelegungspläne, aber solche sind hier nicht gemeint.

46 Eine Übersicht findet sich bei Camenish et al. 3.2.4. Bekanntestes Beispiel ist die Bewertungsfunktion bei dem Online-Auktionshaus eBay bei der man nach abgeschlossener Transaktion den Partner für Zuverlässigkeit, Ehrlichkeit usw. in die Kategorie *gut, neutral, schlecht* einordnen kann

können. Gleichzeitig schützt ein Pseudonym aber vor der Identifizierung der realen Identität. Man unterscheidet verschiedene Arten von Pseudonymen

1. (1:1 Beziehung) Pseudonyme, die von einer einzelnen Person benutzt werden und sich dieser zuordnen lassen.
2. (1:n Beziehung) Eine Person kann mehrere Pseudonyme besitzen, wobei für jedes Pseudonym obige Regel gilt, aber nicht erkennbar ist, dass sie zu ein und derselben Person gehören.
3. (n:1 Beziehung) Ein einzelnes Pseudonym lässt sich auch von mehreren Einzelpersonen einer Gruppe nutzen.
4. (m:n Beziehung) Eine Gruppe von Personen kann mehrere Pseudonyme verwenden.

Die Einschränkungen für Pseudonyme sind in den Szenarien dieselben wie für die anonyme Nutzung. Über Zusatzinformationen kann es, gerade in Kleingruppen, böswillig Agierenden schnell gelingen, Pseudonyme der entsprechenden Person zuzuordnen. Wird z.B. in einem Chat mit einem Pseudonym kommuniziert, lässt sich in einer Gruppe von drei Personen, von denen bekannt ist wer sie sind, nur nicht welche Pseudonyme sie nutzen, schnell ermitteln, wer sich hinter einem bestimmten Pseudonym versteckt, wenn die der_die Angreifer_in ebenfalls Teil der Gruppe ist. Das Teilen eines oder mehrerer Pseudonyme wiederum steht oft, wie die anonyme Nutzung, im Widerspruch zum Zweck der Systeme.

Vorstellbar ist aber eine pseudonyme Nutzung von Kollaborationsaufgaben. In Fällen, in denen im Normalfall keine Identifizierung des_der Urheber_in nötig ist, es aber unter bestimmten Umständen notwendig sein kann, ließe sich mit zentralen Stelle arbeiten, die variable Pseudonyme zuordnet. Im Normalfall wären so für die Nutzer_innen nur die Pseudonyme sichtbar, unter bestimmten Bedingungen kann die zentrale Stelle allerdings die Zuordnung zu einer Person wieder herstellen. Eine genauere Beschreibung eines solchen Verfahrens erfolgt im Abschnitt 4.3.

4.2.5 *Veränderung*

Um die Aussagekraft von personenbezogenen Daten zu verringern z.B. für eine statistische Auswertung - wie in *Die Macht der Statistik* - können verschiedene Maßnahmen ergriffen werden.[47]

FILTERN UND LÖSCHEN von Einträgen, die nur vereinzelt auftauchen und eventuell Aussagen über singuläre Ereignisse zulassen, sind eine Maßnahme des datenschutzförderlichen Veränderns. Etwa in Statistiken oder auch wie in *Der Skandal* die außergewöhnliche IP-Adresse.

VERGRÖBERN und Verallgemeinern von Einträgen durch Entfernen von Details. Im Fall eines Version Control System (VCS) müssten etwa die sekundengenauen Zeitstempel, die belegen wann eine Änderung vorgenommen wurde, nicht angezeigt werden. Eventuell würden ab einem bestimmten Zeitpunkt auch die einfache Datumsangabe ausreichen.

47 vgl. Herrmann and Weber (1999) Abschnitt 5.1 für Maßnahmen zum *schützenden Verändern* von personenbezogenen Daten in statischen Auswertungen)

AGGREGIEREN von Informationen verhindert, dass Aussagen über einzelne Personen gemacht werden. Stattdessen enthalten die Daten nur noch einen Gruppenbezug.

Durch diese Maßnahmen können sowohl anonyme als auch personenbezogene Daten vor dem Durchsuchen nach auffälligen Einträgen geschützt werden.

4.3 ZUGRIFFSSTEUERUNG

In diesem Abschnitt sind Maßnahmen zusammengefasst, die den Zugriff auf bereits erhobene und gespeicherte Daten regulieren können.

4.3.1 *Zugriffsberechtigungen*

Zur Zugriffssteuerung über Benutzerrechte gibt es eine Vielzahl von Modellen die hier nur kurz umrissen werden. Viele der Mechanismen werden von Groupwaresystemen verwendet, auch wenn andere speziell zur Nutzung in kollaborativen Umgebungen schon vor einiger Zeit entwickelt wurden.

Allgemein definieren Pekárek and Pötzsch (2009) Zugriffsberechtigungen (englisch: Access Control Policy (ACP)) folgendermaßen

> An ACP protects access to an object by specifying which subjects should be granted which type of access to it. The object being protected can be a piece of data like a file, a database record, or a webpage, but it can also be a more abstract functionality like a service or a remote procedure call.

Es existieren viele verschiedene Zugriffskonzepte

Diese Anforderungen lassen sich sehr unterschiedlich umsetzen. Tolone et al. (2005) bieten einen Überblick über verschiedene ACP, bewerten sie nach ihren Möglichkeiten zum Einsatz in kollaborativen Umgebungen und für die Verwaltung gemeinsam bearbeiteter Dateien. In einer aktueller Studie von Hansen (2008) werden aus der Sicht des Identitätsmanagements verschiedene Systeme zur Zugriffssteuerung ausführlicher betrachtet und kategorisiert, bei denen der Fokus eher auf dem Management des Personenbezugs zur ACP liegt.[48] Einen groben Überblick über bietet die folgende Liste.

ACCESS MATRITZEN sind die einfachste Variante Rechte von Benutzer_innen auf Objekte (z.B. Dateien und Ordner) zu vergeben. Das ursprüngliche Konzept, wie es u.a. bei vielen Betriebssystemen noch eingesetzt wird erlaubt nur Unterteilung der Rechte zwischen dem_der Besitzer_in (Ownership) sowie Lese- und Schreibrechte für Benutzer_innen bzw. zu Gruppen zusammengefasste Benutzer_innen.[49]

Zur Vergabe von Zugriffsrechten bei komplexere Sachverhalten, wie mehrstufigen Berechtigungen oder Vererbung sind solche ACCESS MATRIZEN aber nur noch bedingt geeignet. Dewan and Shen

48 Neben ACP werden auch dort PRIVACY POLICIES näher betrachtet, die hier im nächsten Abschnitt unter Data Handling Policy (DHP) mitbehandelt werden.

49 Die Rechte werden in Form von Access Control Liste (ACL) - zu jedem_r User wird für jedes Objekt die Berechtigung gespeichert - oder "Capability Listen"(C-List) - für jedes Objekt werden jeweils die Rechte der einzelnen Nutzer_innen gespeichert - in das Dateisystem integriert.

(1998) haben deswegen ein komplexeres System für die Vergabe von Meta-Zugriffsrechten entworfen, die es erlaubt auch die Rechte, Rechte zu vergeben und zu ändern, in die Berechtigungsstrktur mit einschließt und sie nicht ausschließlich dem_der Benutzer_in zuschreibt, der_die als Besitzer_in eines Objektes vermerkt ist. Dies sind otwendige Erweiterung für kollaborative Systeme in denen mehrere Nutzer_innen an einem Objekt arbeiten. Dynamische Änderungen lasse sich aber in ZUGRIFFSMATRIZEN nicht abbilden. Trotz dieser Unzulänglichkeiten werden ACL meist als Standardberechtigungssystem eingesetzt.

ROLE BASED ACCESS CONTROL trennt die Rechte von dem konkreten User und macht sie abhängig von einer Rolle, die wiederum einem oder mehreren Usern zugewiesen werden kann. So sind Berechtigungen leichter übertragbar. Bisherige Implementierungen sind nach Tolone et al. (2005) aber nicht flexibel genug. Zwar seien Rollen auf Benutzerebene umgesetzt, die Berechtigungen aber an einzelne Objekte gebunden. Das Rollenkonzept konsequent gedacht, lege aber nahe Berechtigungen nicht an einzelne Objekte sondern mit Objekttypen zu verknüpfen. Zusätzlich sei ein aktives Berechtigungsmanagement notwendig, das eine Änderung der Rolle mit der ein_e Benutzer_in im System unterwegs ist, bemerken und Berechtigungsänderungen dann anwenden müsse.

Role-Based Access Control (RBAC) erleichtert es, den Zugriff auf bestimmte Daten für verschiedene Nutzer_innen einzuschränken, die in dem Moment nicht die entsprechenden Rollen ausfüllen. Auf der anderen Seite muss aus Datenschutzsicht aber sichergestellt sein, dass personenbezogene Daten möglichst in der Kontrolle der sie beschreibenden Person bleiben.

TASK BASED ACCESS CONTROL verbessern einige der Fehler in RBAC und gewähren Berechtigungen nach dem Schema eines Workflowmanagement Systems. Je nach Stand des Workflows werden an die Nutzer_innen unterschiedliche Rechte vergeben und andere entzogen. Allerdings lässt sich das Konzept nur schwer auf flexible kollaborative Kontexte übertragen, da dort die Aufgaben selten klar definiert und voneinander abgegrenzt sind.

CONTEX-AWARE ACCESS CONTROL erweitern RBAC um *Umgebungsrollen* die Rechte abhängig vom Kontext definieren. Diese Systeme wurden in ubiquitären Umgebungen getestet, so z.B. bei Zhang and Parashar (2004) die Zugriff auf Systeme abhängig von Kontextinformationen, dem Ort und der anfragenden Stelle und die aktuelle Uhrzeit, gewähren. Ein anderes Bespiel für kontextsensitive Berechtigungen liefert Langheinrich (2001) der die Nähe des_der Besitzer_in zu einem Aufzeichnungsgerät von dessen Funktionstüchtigkeit abhängig macht (PROXIMITY). Weitergedacht kann dies als die Notwendigkeit der räumlichen Nähe des_der Besitzer_in oder einer berechtigten zweiten Person zum Datenobjektes. Also eine Ortsabhängige Variante des Vier-Augen-Prinzips.

Bhatti et al. (2005) wiederum benutzen Kontextinformationen und verschiedene Attribute (siehe 4.3.3) nicht um abhängig von ihnen

> Zugriffsrechte zu gewähren, sondern weisen darüber eine Rolle zu an die wiederum bestimmte Berechtigungen geknüpft sind.[50]

Neben diesen generellen Überlegungen an welche Bedingungen Zugriffsrechte geknüpft sein können, ergeben sich weitere Anforderungen an eine gute Zugriffrechte-Verwaltung.

IDENTÄTS- UND BEZIEHUNGSMANAGEMENT Pekárek and Pötzsch (2009) erwarten von einem zuverlässigen Berechtigungssystem, dass es Möglichkeiten bietet Gruppen zu bilden und diesen Rechte zuzuweisen, dabei sollten die Gruppen möglichst gut differenzierbar sein und das Beziehungsgeflecht die Realität abbilden können.

SCHNITTSTELLEN Zugriffsschutz betrifft nicht nur die Daten innerhalb des Systems sondern insbesondere auch Exportmöglichkeit und andere Arten die Daten weiter zu verarbeiten. Die Berechtigungen sollten dabei nicht nur die Möglichkeit zum Export oder der Übermittlung eingrenzen sondern auch darüber hinaus wirksam sein.

KOMPLEXITÄT Berechtigungssysteme mit umfangreichen Möglichkeiten stehen aber vor dem Problem meist hoch komplex zu sein, da sie besonders hohen Anforderungen nach Flexibilität, Kontextsensitivität und dynamische/automatischer Anwendung genügen müssten. Dies ist gegen die Handhabung und Transparenz abzuwägen. Ein Beleg für diese Anforderung ist, dass theoretische Modelle in der Praxis aktuell kaum Anwendung finden. Auch keines der in den Szenarien genutzten Werkzeuge bietet eine komplexere Zugriffskontrolle, obwohl die Anforderungen dafür teilweise schon vor 20 Jahren erarbeitet wurden.[51]

FLEXIBILITÄT DURCH AUSHANDLUNG Ist ein System in der Lage die Struktur der Gruppe abzubilden, kann es sinnvoll sein, dass auch die Mitglieder Berechtigungen gemeinsam vergeben. Während normalerweise, wie oben schon beschrieben, vor Einführung eines Systems ein Berechtigungskonzept erstellt wird, kann dies in dynamischen Gruppen zu Problemen führen. Die Flexibilität der Gruppe, sowohl in der Struktur als auch in der Aufgabenverteilung lässt weder ein statisches Berechtigungskonzept zu, noch kann die Einhaltung gewährleistet werden. Als Lösung kann hier das von Herrmann (1995) vorgeschlagene Aushandlungssystem fungieren. Er schlägt ein System vor bei dem die Nutzer_innen entscheiden, wem welche Daten zur Verfügung stehen und hierzu, technisch unterstützt, Regelungen aushandeln. Diese nutzer_innengenerierten Systemanpassungen erfordern aber, dass sich eben diese damit auseinandersetzen. Gerade in kollaborativen Systemen wo Berechtigungen nicht zwischen zwei, sondern möglicherweise auch vielen Beteiligten ausgehandelt werden müssen, kann dies zu zusätzlichem Aufwand führen.

---

50 Tolone et al. (2005) stellen zusätzlich Team Based Access Control (TMAC) und SPATIAL ACCESS CONTROL als Zugriffskonzepte vor. Da sie allerdings keine weite Verbreitung erreicht haben und im vorliegenden Fall nicht anwendbar sind, seien sie nur kurz erwähnt. TMAC erweitert RBAC um die Bestimmung von Teams um gleiche Rollen in verschiedenen Teams zu behandeln. SPACIAL ACCESS CONTROL weist räumliche Zugriffsrechte in virtuellen 3D-Umgebungen zu, da diese aber relativ selten sind hat sich auch diese Zugriffsverwaltung nicht etablieren können.

51 vgl. u.a. Shen and Dewan (1992) und Pekárek and Pötzsch (2009) die ebenfalls eine ähnliche Liste an Anforderungen an ACP definiert haben.

KONTEXTSENSITIVITÄT Tolone et al. stellen heraus, dass die Kontextsensitivität von Berechtigungskonzepten in kollaborativen Umgebungen von besonderer Bedeutung ist, um den flexiblen Rahmenbedingungen gerecht zu werde. Allerdings sind die müssen dazu die Kontextvariablen genauer bestimmt werden. Bisherige Systeme (s.o.) reagieren meist nur auf Ort und Zeit des Zugriffsversuchs. Der Zugriff auf Informationen soll etwa nur während der Arbeitszeit und von einem bestimmten Arbeitsplatz aus, möglich sein. Dies wirkt auch verhaltensregulierend dadurch, dass die (örtliche) Anwesenheit von Kolleg_innen die Gefahr erhöht aufzufliegen.

Ist, wie im Fall von *Die Macht der Statistik* oder *Der Skandal*, verteiltes, asynchrones Arbeiten an unterschiedlichen Orten aber Teil des Arbeitsalltags ist eine Einschränkung des Zugriffs auf Basis dieser Variablen allerdings ungeeignet. In dem Szenario könnten stattdessen Kontextinformationen über den Status des Projekts (es gibt Verzögerungen) zur stärkeren Einschränkung des Zugriffs auf personenbezogene Daten führen.

Zur konkreteren Kontextbestimmung müssen allerdings auch wesentlich mehr Daten herangezogen werden. Das Problem wird im Abschnitt 4.4.2 an einem Beispiel beschrieben.

GLEICHBERECHTIGUNG Die Anforderung ist, dass eine_e Nutzer_in nur auf die Informationen anderen Gruppenmitgliedern zugreifen kann, die sie selbst den anderen ebenfalls zur Verfügung stellt. Im Falle einer Eskalation und einem damit einhergehenden Datenmissbrauch muss sich der_die Angreifer_in zumindest darüber bewusst sein, dass die gleiche Art der Informationen über sie ebenfalls genutzt werden könnten.

REGELMÄSSIGE ÜBERPRÜFUNG Gerade in dynamischen Gruppen ist es wichtig, dass auch das Berechtigungssystem reagiert. In den Werkzeugen, die in den Szenarien benutzt werden, sind meist nur einfache ACL implementiert, wenn eine explizite Rechtevergabe überhaupt möglich ist.[52] Es ist zusätzlich notwendig darüber hinaus zu überprüfen, ob die an eine Rolle vergebenen Rechte noch für die Situation passend sind. Solche Überprüfungen können sowohl in regelmäßigen zeitlichen Abständen, oder auch ereignisgesteuert erfolgen. So kann etwa das Ende eines Projektes oder das Ausscheiden eines_r Mitarbeiter_in eine erneute Aushandlung von gewährten Zugriffsberechtigungen anstoßen.

4.3.2 *Zugriff verhindern*

In den meisten Groupwaresysteme sind die in ihnen abgelegten Informationen durch Zugriffsberechtigungen geschützt. Welche Anforderungen an die Zugriffskonzepte geknüpft sind wurde im vorherigen Abschnitt erläutert. Ein Problem ist aber allen Systemen gemeinsam: Gelingt es eine_m Angreifer_in das Zugriffssystem zu umgehen, indem er_sie etwa von außerhalb des Systems auf die Daten zugreift, wie es Dominique in *Der Skandal* über die Backups gelingt, sind die Zugriffsberechtigungen unwirksam. Kryptografische Methoden und

52 In einem Chatprogramm beispielsweise ist, hat man einen Kontakt einmal bestätigt, diesem durch die dezentrale Struktur im Anschluss der Zugriff auf alle bei ihm eingegangenen Daten ohne weitere Einschränkungen möglich

andere Konzepte der *Informationssicherheit*[53] können stärkeren Zugriffsschutz gewährleisten und so die missbräuchliche Nutzung von Daten verhindern.

VERTRAULICHKEIT UND INTEGRITÄT sicherzustellen sind Grundziele der Informationssicherheit. Es sollen nur diejenigen Zugriff auf Daten haben, denen er explizit gewährt wurde und diese Daten sollten nicht versehentlich oder absichtlich, unbemerkt geändert werden können. Durch Verschlüsselung lassen sich diese Ziele in ausreichendem Maße erreichen. Man unterscheidet dabei zwischen *Leitungs-* und *Ende-Zu-Ende-Verschlüsselung*. Bei der Leitungsverschlüsselung werden die Daten zwischen den Kommunikationspartnern verschlüsselt übertragen, so dass Unbeteiligte sie nicht auslesen können. Allerdings wird auch bei der Kommunikation über mehrere Knoten nur zwischen den jeweiligen kommunizierenden Knoten verschlüsselt übertragen, bei der Verarbeitung auf den entsprechenden Knoten selbst allerdings unverschlüsselt verarbeitet. Hier besteht die Gefahr von Missbrauch oder Manipulation. Bei der Ende-Zu-Ende-Verschlüsselung wird der Inhalt einer Nachricht von der sendenden Seite verschlüsselt und erst bei dem_der Empfänger_in wieder entschlüsselt. Zwischenknoten, die die Nachrichten nur weiterleiten, haben so keinen Zugriff auf den Inhalt der Kommunikation.

symmetrische und asymmetrische Verschlüsselung

Weitere wichtige Kategorien kryptographischer Verfahren sind die symmetrischer und die asymmetrischer Verschlüsselung, da sie unterschiedliche Anwendungskonzepte unterstützen. Bei ersterem Verfahren[54] sind sendende und empfangende Stelle im Besitz des selben Schlüssels mit dem eine Nachricht sowohl ver- als auch entschlüsselt werden kann, ähnlich einem Schloss für das beide Seiten einen Schlüssel besitzen. Asymmetrische Verschlüsselung hingegen beruht auf dem Prinzip von öffentlichen und privaten Schlüsseln. Mithilfe des öffentlichen Schlüssels, der allen möglichen Sender_innen zugänglich gemacht werden kann, wird eine Nachricht verschlüsselt. Nachdem die Nachricht zum_zur Empfänger_in gelangt ist, kann nur diese_r dann mit dem privaten Schlüssel die originale Nachricht wieder herstellen. In der Schloss-Analogie bekommt die sendende Stelle ein Schloss von dem_der Empfänger_in, für das sie keinen Schlüssel besitzt. Mit diesem Schloss können Nachrichten für die empfangende Stelle verschlüsselt werden, die im alleinigen Besitz des Schlüssels ist. Weitere Verfahren sind notwendig, wenn der_die Empfänger_in die Identität des_der Absenders_in verifizieren möchte.

Zwei konkrete Implementierungen und Anwendungsszenarien, die im Rahmen von Groupware eingesetzt werden, sind

PRETTY GOOD PRIVACY (PGP)/S-MIME sind weit verbreitetes Verfahren zur verschlüsselten *Ende-Zu-Ende* Kommunikation und werden überwiegend im E-Mail Verkehr eingesetzt. Mittels *asymmetrischer* Verschlüsselung wird sichergestellt, dass nur die Person, die im Besitz des privaten Schlüssels ist, eine Nachricht entschlüsseln kann. Zusätzlich wird das Signieren von Nachrichten unterstützt um die Absender_innen-Identität für den_die Empfänger_in nachweisbar zu machen. Das Verfahren bietet sich zudem für asynchrone Anwendungen bei denen Daten verschlüsselt abgelegt oder

53 Im folgenden beziehe ich mich, wenn nicht anders angegeben auf Paar and Pelzl (2010)

54 Einsatzgebiete ist vor allem die Leitungsverschlüsselung wie etwas bei SSL-Verschlüsselter Client-Server-Kommunikation im Internet

versendet werden. In *Die Neue* hätten verschlüsselte E-Mails etwa verhindern können, dass Daniela Zugriff auf alle, per Mailingliste verschickten, E-Mails bekommt.

OFF-THE-RECORD MESSAGING (OTR) , wie es Borisov et al. (2004) konzipiert haben, wird eingesetzt um beim Instant-Messaging eine verschlüsselte *Ende-Zu-Ende* Kommunikation zu ermöglichen. Dabei wird für jede Sitzung ein *symmetrischer* Schlüssel generiert, der nach Ende der Sitzung vernichtet wird, so dass die Daten nicht mehr zu entschlüsseln sind, vorausgesetzt wird, dass nicht eine_r der beiden Kommunikationspartner die entschlüsselten Nachrichten mitschneidet. Das Verfahren ist insbesondere bei synchronem Daten- und Informationsaustausch einsetzbar.

AUTHENTIZITÄT ist das dritte Grundziel von Informationssicherheitsmaßnahmen. Authentizität zu gewährleisten bedeutet, Daten und Informationen vor dem Zugriff und der Manipulation durch dritte zu schützen. Die vorgestellten kryptografischen Verfahren leisten dies bereits auf der Ebene der Übertragung. Zusätzlich muss aber auch auf der Seite der Kommunikationsteilnehmer_innen sichergestellt werden, dass es keinen *unauthorisierten Zugriff* geben kann. Abhängig von der Sensibilität der Daten kann die einfachen Name/Passwort-Kombination etwa mittels einer kryptografischen Chip-Karte erweitert werden, um die Identität eines_r Nutzer_in zu verifizieren. So wäre es in *Die Neue* Carsten nicht ohne weiteres möglich Birgits Account zu nutzen.

4.3.3 *Erlaubten Zugriff einschränken*

Selbst wenn ein_e Nutzer_in die Zugriffsberechtigungen besitzt, um auf bestimmte Objekte zuzugreifen, kann es Gründe geben den Zugriff einzuschränken. In *Die Macht der Statistik* etwa soll es alle Beteiligten möglich sein auf die Log-Dateien zuzugreifen. Allerdings ist es in der Regel nicht notwendig, wie im Szenario, auf die komplette Sammlung zuzugreifen.

VERHINDERUNG MASSENHAFTER ODER AUTOMATISIERTER AUSWERTUNG Bei einer größeren Anzahl Daten ist eine Eingrenzung der Zugriffe, auch von Nutzer_innen mit den entsprechenden Zugriffsrechten, auf Basis verschiedener Attribute vorstellbar.

ANZAHL der Zugriffe pro Client. Bei den Log-Dateien im ersten Szenario kann etwa serverseitig die Anzahl der Zugriffe pro Nutzer_in und Tag begrenzt werden. Ein spontanes auslesen der gesamten Einträge kann so verhindert werden.

TIEFE der Recherche. Es kann sinnvoll sein, die Recherche, etwa in einem Kalender, auf einen bestimmten Zeitraum zu begrenzen und den Zugriff auf Einträge, die länger als drei Monate zurückliegen, nicht pauschal zu erlauben.

DETAILIERGRAD der Ergebnisse. Abhängig vom Zweck des Zugriff auf eine Datensammlung kann der Detailgrad der zurückgelieferten Daten auf das notwendige Minimum begrenzt werden. Bei einem Kalender könnte etwa in einem länger zurückliegenden Zeitraum der Titel des Termins ausgeblendet werden, so dass nicht sichtbar ist, um welchen konkreten Termin es sich gehandelt hat.

Abbildung 10: CAPTCHA. Quelle: http://www.wikimedia.org

Um die automatisierte Auswertung zu verhindern, können so genannten *Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA)* genutzt werden. Bei einer Abfrage wird der_die Nutzer_in aufgefordert, den Inhalt des CAPTCHA in ein Eingabefeld einzutragen. Bisher sind nur wenige Programme in der Lage die Bilderkennung zu automatisieren, so dass das automatisierte Abfrufen von großen Datenmengen (crawlen) verhindert werden kann.

TRUSTED THIRD PARTY Als Trusted Third Party (TTP) bezeichnet man in der IT-Sicherheit eine dritte Partei, die als vermittelnde Stelle die Kommunikation oder den Datenaustausch zwischen zwei, sich unbekannten Partnern, herzustellen hilft. Dabei kann die TTP Vertrauen vermitteln, indem es die Authentizität der Partner gegenseitig bestätigt. Dazu müssen beide sich vorher einmal gegenüber der TTP identifiziert haben, die dann auf Anfrage die Vertrauenswürdigkeit bestätigt. Vergleichbar ist das Konzept mit dem eines Personalausweises, dem zur Identifizierung einer Person mehr Vertrauen entgegengebracht wird, als einem mündlich mitgeteilten Namen. Die ausgebende Stelle, der jeweilige Staat, fungiert hier als TTP. Das Konzept kann so erweitert werden, dass die TTP nicht nur als vertrauensbildende Stelle genutzt wird, sondern auch Mittlerin der Information selbst wird. Dabei kann sie beobachten welche oder wieviele Informationen abgerufen werden.

Eine TTP dient als Mittler_in von Vertrauen

Eine TTP muss nicht Teil des Dienstes selbst sein - etwa ein VCS-Server der die Abrufe pro IP beschränkt - sondern kann, um die Sicherheit zu erhöhen, auch ausgelagert werden, so dass der Dienst bestimmte Informationen selbst nicht hat. Der VCS-Server könnte z.B. bei jedem Eintrag nur eine Einmal-Chiffre-Nummer, statt eines Namens speichern. Die Zuordnung von Chiffre-Nummer zum_r Urheber_in kann dann auf eine TTP ausgelagert werden, die im Anschluss bei jeder Abfrage regulierend eingreifen und den Zugriff auf die Zuordnung verwehren kann.

CREDENTIALS Berechtigungsnachweise (engl. CREDENTIALS[55]) lassen sich ebenfalls mittels einer TTP realisieren und ermöglichen bei einer Authentifzierung zur Datenminimierung beizutragen. Die TTP übermittelt im dem Fall nicht die gesamte Information (z.B. die Identität des_der Benutzer_in), sondern nur den relevanten Teil. Ist z.B. der Zugriff auf eine Datei oder Webseite Minderjährigen nicht gestattet, teilt die TTP nicht das Geburtsdatum mit, sondern nur die Information ob die Person älter als achtzehn Jahre ist oder nicht.

CREDENTIALS sind vor allem zur Zugriffssteuerung und Authentifizierung zwischen Client und Server im Einsatz. Vorstellbar ist aber auch ein Einsatz zu Vermittlung von Informationen in die andere Richtung. Je nach Zugriffsberechtigung können unterschiedliche detaillierte Informationen dem_der Nutzer_in angezeigt werden. So könnte etwa bei einem Kalendersystem die Einsicht so weiter eingeschränkt werden. Statt einen Zeitraum als belegt anzuzeigen, können Nutzer_innen auf

55 nach Chaum (1985) oder auch MINIMUM DISCLOSURE TOKENS Hansen (2008)

eine Terminanfrage nur mitgeteilt werden, ob zu diesem oder jenem Zeitpunkt eine Person verfügbar ist.

VIER-AUGEN-PRINZIP Das Vier-Augen-Prinzip soll verhindern, dass eine einzelne Person mit den ihr gewährten Berechtigungen missbräuchlich umgeht. Der Zugriff auf besonders geschützte Bereiche wird hier nur möglich, wenn eine zweite Person die Aktion authorisiert. Im einfachsten Fall bedeutet dies, dass ein nötiges Passwort zwischen zwei Personen geteilt wird und jede nur jeweils über eine Hälfte Kenntnis hat.[56] Zur Bestätigung müssen also immer beide anwesend sein. Technische Lösungen des Prinzips sehen vor, dass einer zweiten Person eine Anfrage zugesendet wird, die diese, mit ihrem Passwort oder Ähnlichem, bestätigen muss.

Geteilte Verantwortung

Statt pauschaler Berechtigunsfreigaben lässt sich so, etwa bei sensiblen personenbezogenen Informationen, ein System so konfigurieren, dass immer die Einwilligung des_der jeweiligen Besitzer_in der Information verlangt wird. Ein Nachteil ist, dass in Gruppen mit starken Hierarchien die Gefahr besteht, dass die Einwilligung unter sozialem Druck ungeprüft gegeben wird, oder, dass wenn zu häufig Anfragen genehmigt werden müssen, ein Gewöhnungseffekt eintritt und jegliche Anfragen ungeprüft genehmigt werden.

4.3.4 *Zugriff beenden*

Die bis hierhin beschriebenen Maßnahmen zur Zugriffssteuerung ermöglichen Zugriffsberechtigungen zu vergeben, den Zugriff für Unberechtigte zu verhindern und für diejenigen, denen Zugriff gewährt wurde, diesen einzuschränken. Eine Steigerung von letzteren Maßnahmen stellen die im Folgenden beschriebenen Möglichkeiten dar, die Einschränkungen dauerhaft zu machen und den Zugriff auf Daten irreversibel zu beenden.

LÖSCHUNG Sind Daten gelöscht und damit ein Zugriff nicht mehr möglich, ist auch eine missbräuchliche Nutzung ausgeschlossen. Die Frage ab wann Informationen gelöscht werden können, sollte im Normalfall während der Vorabkontrolle geklärt und festgelegt werden. Da aber oft der Zweck nicht endgültig bestimmt werden kann oder mit Absicht offen gehalten wird, kann auch kein Ende der Speicherung festgelegt werden. Werden etwa Daten für eine geplante Projektnachbesprechung aufgehoben, für die aber kein Zeitpunkt festgelegt wurde, kann auch eine Löschung der mit dem Ablauf nicht mehr benötigten Daten (etwa gespeicherte Zugriffe oder Daten zur Änderungsverfolgung) nicht definiert werden.

Doch selbst wenn Löschfristen bestimmt worden sind, sind diese nicht ohne weiteres durchzusetzen. In dezentralisierten Systemen, in den Szenarien sind dies zum Beispiel das Chat-System und das VCS, in denen jede_r einzelne Benutzer_in (erlaubt oder unerlaubt) eine lokale Kopie besitzt, ist die zentrale Kontrolle, ob nicht mehr notwendige Daten gelöscht wurden nur schwer möglich. Kompliziert kann es auch sein, Regelungen für das Löschen von Daten in Backups zu finden, wie sie in *Der Skandal* verwendet werden.[57]

56 Siehe dazu auch die Beispiele aus dem zweiten Experteninterview 4.1.2

57 Im Fällen in denen eine Löschung von Daten nicht möglich oder gewollt ist, wird oft auf die Möglichkeit der Sperrung zurückgegriffen. Gesperrte Daten sind zwar noch

VERFALL Um für die Fälle vorzusorgen in denen eine Löschung wegen dezentraler Speicherung nicht möglich ist, sind kryptografische Verfahren entwickelt worden, die einen automatisierten *Verfall* der Daten simulieren sollen. Während die Verfahren zur verschlüsselten Kommunikation (vgl. 4.3.2) zur Absicherung der Übertragung bereits seit einigen Jahren im Einsatz sind, werden Verfahren, die den Daten eine Art Verfallsdatum geben, und so den Zugriff nach einer gewissen Zeitraum verhindern, noch wenig genutzt.

Kryptographie um Daten nicht mehr verwendbar zu machen

VANISH wurde erstmals von Geambasu et al. (2009) vorgestellt. Das System basiert auf der Idee, dass der Schlüssel zu asymmetrisch verschlüsselten Daten in mehrere Teilschlüssel zerlegt und in Peer-to-Peer Netzwerken verteilt wird. Durch die Struktur der Netzwerke werden die Teilschlüssel nicht dauerhaft gespeichert. Der Verlust von Teilschlüsseln kann zwar einige Zeit durch mathematische Verfahren kompensiert und der Gesamtschlüssel wieder hergestellt werden, wenn aber eine bestimmte Menge an Teilschlüsseln aus dem Netzwerk entfernt ist, ist der Schlüssel verloren und die Nachricht nicht mehr wiederherstellbar. VANISH kommt ohne einen zentralen Server aus, da es sich bestehender Peer-To-Peer-Netzwerke bedient. Allerdings ist dadurch die Verfallsdauer nicht genau definierbar und liegt bei mehreren Stunden bis Tagen.

EPHEMERIZER beschrieben von Perlman (2005) geht einen ähnlichen Weg, bietet aber über einen zentralen Server genauere Steuerungsmöglichkeiten. Hier werden die Schlüssel an zentraler Stelle gespeichert und nach einem, von dem_der Ersteller_in definierten Zeitpunkt, gelöscht. Eine zweite Verschlüsselungsstufe stellt zudem sicher, dass nur der_die Empfänger_in die Nachricht entschlüsseln kann, so lange der erste Schlüssel noch auf dem Server einer TTP vorhanden ist.[58] Als Einsatzgebiet des EPHEMERIZER-Protokolls sehen die Autoren u.a. bei ausgelagerter Informationsverarbeitung, wie etwa beim CLOUD-COMPUTING. Das Prinzip lässt sich aber auch auf andere Szenarien anwenden.

Allen kryptografischen Methoden liegt allerdings die Annahme zu Grunde, dass sowohl sendende als auch empfangende Stelle keine böswilligen Absichten verfolgen und sich an die Protokolle halten. Die sehen vor, dass keine persistente Speicherung der entschlüsselten Informationen vorgenommen wird, die Klartexte also nur für begrenzte Zeit im Zwischenspeicher der Computer vorhanden sind. Für die Verfahren zur verschlüsselten Übertragung besteht zudem auch dann noch die Gefahr, dass sie nach einem Vertrauensbruch zweckentfremdet werden, da der_die Empfängerin unbegrenzt Zugriff hat. Die zuletzt vorgestellten Verfahren zum technisch provozierten *Verfall* sind nicht geeignet Missbrauch zu verhindern, der innerhalb des Verfügbarkeitszeitraums stattfindet. Allerdings lässt sich so verhindern, dass alle Daten, die seit Beginn der Kommunikation, evtl. über mehrere Jahre, angefallen sind, missbräuchlich genutzt werden können.

---

vorhanden, etwa weil ein Backup auf einem nicht änderbarem Medium wie einer CD abgelegt ist, an geeigneter Stelle ist aber hinterlegt, dass die Daten nicht verwendet werden dürfen.

58 Weiterentwicklungen wie die von Tang (2010) ergänzen die Struktur um eine weitere Serverinstanz um die Zeitlichkeit der Daten zu gewährleisten.

Die Verfahren können aber nicht vor einem geplanten Angriff schützen, bei dem ein Kommunikationspartner die Daten unverschlüsselt dauerhaft speichert um sie bei Gelegenheit auswerten zu können.

4.4 NUTZUNGSSTEUERUNG

Die vorgestellten Verfahren zur Zugriffssteuerung haben den Nachteil, dass im Missbrauchsfall ein einziger unerwünschter Zugriff auf die Daten genügt, um eine Kopie zu erstellen und die Daten ungehindert weiter verwenden zu können. In diesem Abschnitt werden deswegen Maßnahmen vorgestellt deren Ziel es ist, nicht den Zugriff sondern die Nutzung zu regulieren.

4.4.1 *Data Handling Policies*

Unter DHP versteht man ein Set an Eigenschaften, die einer Datei oder einer Information angehängt sind und die Aussagen darüber treffen, wie mit den Daten umgegangen werden soll (vgl. Ardagna et al. (2006)). Das Modell wurde inbesondere für den e-Commerce Bereich entwickelt. Der Unterschied zu ACL besteht in der Unterstützung von Übermittlung. Bei Zugriffssteuerung wird die Berechtigung der anfragende Stelle betrachtet und gegebenenfalls Zugriff gewährt. Ab diesem Moment wird ihr vertraut und sie kann die Daten prinzipiell auf beliebige Art weiterverarbeiten. Die Idee von DHP ist, dass sie die Übermittlung an die anfragende Stelle überdauern und die Zweckbindung auch noch nach der Übermittlung eingehalten, sowie Regeln definiert werden können, wie mit den Daten nach Abschluss der Verarbeitung, umgegangen werden muss.

DHP sollen über Schnittstellen hinweg verfügbar sein

Wesentliche Komponenten der DHP sind

RECIPIENTS Die Empfänger der personenbezogen Daten. Policies können abhängig von einem_r konkreten Empfänger_in (identity-based), der Kategorie von Empfänger_innen (category-based) oder von bestimmten Attributen (attribute-based) definiert werden.

ACTIONS Es können verschiedene Zugriffsaktionen gestattet werden. Vorgeschlagen sind von den Autor_innen *lesen*, *schreiben*, *übermitteln* und *ändern*.

PRIVACY PROFILE Die eigentlichen Daten, bestehen aus Tupeln <*attribute_name*, *attribute_value*> zusammen mit einem Hinweis auf die Identität oder ein Pseudonym des_der Besitzer_in. Die Profile können außerdem in Sub-Profile zerteilt sein für die wiederum unterschiedliche DHP gelten können.

RESTRICTIONS Einzuhaltende Nutzungs-Beschränkungen werden als RESTRICTIONS definiert. Die Autor_innen schlagen hier, für den eCommmerce, Einträge wie *Forschung* und *Abrechnung* vor. Dazu kommen Vorraussetzungen (*provisions*) und Pflichten (*obligations*) was im Anschluss an den Zugriff mit den Daten gemacht werden muss. Ersteres könnte z.B. eine gezahlte Gebühr sein, bzw. Benachrichtung über einen Zugriff.

Mit einem funktionierenden DHP-System ließe sich die Nutzung von personenbezogenen Daten bei der technischen Weiterverarbeitung stärker steuern. DHP eigenen sich dabei vor allem für STAMMDATEN und

VERKEHRSDATEN für die, anders als bei den INHALTSDATEN ein konkreter Verwendungszweck, der notwendig ist um die automatische Verarbeitung zu ermöglichen, definieren.

Nach Pekárek and Pötzsch (2009) sind DHP nicht weit verbreitet und sind vor allem in geschlossenen Systemen oder Einsatzumgebungen wie e-Commerce oder e-Government im Einsatz.[59]

Der Nutzung von DHP stehen allerdings einige Details entgegen. Zum ersten ist es, genauso wie bei einem Zugriffskonzept, notwendig, dass die Policies definiert werden. Das kann entweder im Rahmen der Vorabkontrolle passieren, was die bereits erwähnten Nachteile mit sich bringt, oder von den Nutzer_innen selbst flexibel angepasst werden. Dazu ist eine einfache Konfigurierbarkeit der DHP auch auf Ebene von Datenkategorien notwendig. Die Definition von Nutzungszwecken ist allerdings schwierig, da sie nicht zu allgemein aber auch nicht zu einschränkend sein dürfen. Gilt etwa für die INHALTSDATEN eine E-Mail mit vertraulichen Informationen, dass sie nicht weiterversendet werden dürfen, schließt dies auch aus, dass sie ausgedruckt werden, was aber möglicherweise notwendig ist, gleichzeitig aber das weiterversenden auf postalischem Wege ermöglicht.

Zum zweiten benötigen DHP eine technische Infrastruktur, die ihre Einhaltung gewährleistet. Sie bietem weitergehen Möglichkeiten Policies auch über Schnittstellen hinweg zu definieren, als dies bei Zugriffsberechtigungen der Fall ist. Das setzt aber voraus, dass sie auch korrekt interpretiert werden. Um dies sicherzustellen entwerfen Ardagna et al. (2006) eine zertifikatsbasierte Infrastruktur mit einer TTP die etwa Software und andere datenverarbeitende Stellen authentifiziert. Einen Schutz davor, dass Informationen in einen Texteditor kopiert und von dort weiterverarbeitet werden, bieten sie aber nicht.[60]

4.4.2 *Automatisierte Kontexterkennung*

Neben der manuellen Definition von Zugriffs- und Nutzungsberechtigungen ist auch eine automatisierte Erkennung denkbar. Wright et al. (2008) etwa forden intelligente Algorithmen, die, möglichst selbstlernend, den Kontext einer Datennutzung erkennen und im Interesse der Datenbesitzer_innen dynamisch entscheiden ob einem Zugriff bzw. einer Nutzung stattgegeben wird.

DATA LOSS PREVENTION Maloof and Stephens (2007) haben mit Exploit Latent Information to Counter Insider Threats (ELICT) ein Werkzeug entwickelt, dass eine Kontextbestimmung automatisch vornehmen soll. Das Ziel von ELICT ist allerdings nicht der Schutz von personenbezogenen Daten, sondern der von Unternehmensdaten. Dabei geht es nicht darum mögliche Angreifer von außen abzuwehren, sondern der Situation Herr zu werden, dass Mitarbeiter_innen unerlaubt vertrauliche Informationen kopieren und zum Beispiel zu einem neuen Arbeitgeber mitnehmen (Data Loss Prevention (DLP)). Da die Mitarbeiter_innen dazu häufig nicht einmal Sperren umgehen müssen und im

59 Konkrete Implementierungen gibt es vor allem auf Basis der Ausschreibungssprache XACML (vgl. u.a. Dürbeck et al. (2010) und für weitere Protokolle Hansen (2008); für den Einsatz von Policies bei Webservices Rost and Speck (2009)

60 Für einige Datentypen existieren seit geraumer Zeit Verfahren. Die sogenannten *Wasserzeichen* erzeugen und etwa Musik- und Filmdateien so zu ihrem Ursprung zumindest zurückverfolgen zu können.

Rahmen ihrer Tätigkeiten regulär Zugriff auf die Daten haben, helfen andere Sicherheitsmechanismen nur begrenzt weiter.

ELICT analysiert kontinuierlich den Netzwerkverkehr eines Unternehmens um verdächtiges Verhalten zu identifizieren

ELICT kann durch Analyse des Netzwerkverkehrs etwa detektieren, wenn ein_e Angestellte_er ein Dokument auf einem Drucker ausdruckt, der nicht der nächstgelegene oder der normalerweise verwendete ist. Dem liegt die Annahme zugrunde, dass die Wahl eines Druckers an einem abseits vom eigenen Büro gelegenen Standort darauf zurückzuführen ist, dass Kolleg_innen nicht mitbekommen sollen, wenn ein Dokument gedruckt wurde welches nichts mit dem eigentlichen Arbeitsgegenstand zu tun hat. Die Autoren entwickelten anhand der Analyse eines größeren Unternehmens und der Auswertung des Netzwerkverkehrs von fast einem Jahr 76 Symptome die auf unerwünschten Informationsabfluss hindeuten könnten. Ein Testlauf ergab eine korrekte Erkennung von 84 % der Angriffsszenarien, bei nur 1 % false-positives - also fehlerhafte Erkennungen.

Ein System ähnlich zu ELICT könnte sicherlich auch in den hier behandelten Szenarien Unregelmäßigkeiten bei dem Zugriff auf Datenbanken feststellen, allerdings sprechen mehrere Gründe gegen die Nutzung eines solchen Systems. Maloof and Stephens benutzen zum Aufbau ihrer statistischen Netzwerk unverhältnismäßig viele personenbezogene Daten der Mitarbeiter_innen des Unternehmens. Um Unregelmäßigkeiten aufzudecken wurde z.B. auf eine Datenbank zugegriffen in der allen Angestellten ein Tätigkeitsprofil zugewiesen wurde, mit Informationen über Projekten an denen er_sie arbeitet. Darüber hinaus muss für eine Analyse, wie die oben genannte Druckerwahl, der tatsächlich Einsatzort bekannt sein. Um außerdem noch verdächtige Kontakte zwischen Mitarbeiter_innen aufzudecken, wurde der gesamte E-Mail Verkehr analysiert und mittels des Vergleichs von Sender_innen und Empfänger_innen soziale Netzwerke ermittelt.

Zudem erforderte ELICT die Definition von Missbrauchsszenarien, deren Muster wiedererkannt werden sollen. Gerade die Dynamik und Vielfältigkeit der missbräuchlicher Nutzung zeichnet aber die Problemstellung dieser Arbeit aus.

Zum Schutz der Daten vor unberechtigtem Zugriff wäre es, angelehnt an ELICT vorstellbar, auf Ebene der ACP dynamisch Anpassungen vorzunehmen. Wenn man zum Beispiel annimmt, dass zum Zeitpunkt einer engen Zusammenarbeit auch ein reger Austausch von E-Mails und Zugriff auf gemeinsam erstellte Dateien erfolgt, wäre dies durch Netzwerkanalyse nachvollziehbar. Ist aber ein Projekt beendet sinkt das Kommunikationsaufkommen. Sinkt damit die messbare Kommunikationsrate unter einen bestimmten Wert könnte die ACP automatisch angepasst und etwa der Zugriff ältere Informationen eingeschränkt werden.

HONEY-POT-METHODE Ein anderes Werkzeug zur Detektierung von möglicherweise böswilligen Mitarbeiter_innen, dass weniger exzessiv auf andere Quellen zugreift, beschreiben Bowen et al. (2009). Ihr System basiert auf Köderdateien, die, wenn sie kopiert oder geöffnet werden, einen Alarm auslösen. Der Zugriff auf eine Köderdatei kann allerdings genauso auf Neugier zurückzuführen sein und, sollte es sich um personenbezogene Daten handeln mit denen eine Kolleg_in angeschwärzt werden könnte, höchstens einen Hinweis auf Probleme in der Vertrauensstruktur der Gruppe liefern.

4.4.3 *Restriktive Nutzungsregelungen*

Neben der Zugriffsbegrenzung auf Ebene von Objekten, Dateien und Ähnlichem kann auch restriktive Regulierung eines Netzwerks und der angeschlossenen Rechner Schutz vor ungewolltem Datenmissbrauch bieten. Ziegler (2010) stellt Software vor, auf den Rechnern der Nutzer_innen installiert, deren Verhalten überwacht und etwa das Anstecken von USB-Sticks genaus kritisch anmerkt wie den Versand von E-Mails mit möglicherweise sensiblem Inhalt an unternehmensexterne Adressen. Da Groupwaresysteme in der Regel ohne eine Netzwerkverbindung nicht auskommen, können auch restriktive Firewall bzw. Intrusion Prevention System (IPS)-Regelungen den Zugriff von nicht authorisierten Programmen, und damit die nicht authorisierte Nutzung, auf Datenbestände verhindern.

NACHTEILE DER ÜBERWACHUNTSTECHNOLOGIEN Für alle aktiv überwachenden Werkzeuge sei aber noch einmal darauf hingewiesen, dass die entstehenden Datensammlung auf Verdachtsbasis wiederum erhebliche Missbrauchspotentiale böten, abgesehen von der massiven Verhaltenskontrolle die damit möglich wäre.

4.5 NUTZER_INNENZENTRIERTE MASSNAHMEN

Eine letzte Kategorie von Maßnahmen versammelt solche, die nicht an einem bestimmten Punkt des Zugriffs oder der Nutzung technisch Einfluss nehmen, sondern sich an die Nutzer_innen richten und ihr Verhalten direkt beeinflussen sollen.

4.5.1 *Awareness*

Awareness-Funktionen,[61] konkreter die INTERPERSONELLE AWARENESS[62] ist nach Iachello and Hong (2007) einer der großen Vorteile von CSCW-Systemem. Sie vereinfacht die Kollaboration indem bei allen Beteiligten leichter ein Verständnis dafür entstehen kann welchen Stand die gemeinsame Arbeit hat, erleichtert aber auch die Koordination und Kommunikation indem z.B User u.a. einstellen können, wenn sie gerade nicht gestört werden wollen.

Die INTERPERSONELLE AWARENESS, wie in *Die Macht der Statistik* kann allerdings selbst ein Datenschutzproblem sein.[63] RECIPROCITY, von Schümmer and Lukosch (2007) auch als Pattern identifiziert, kann hier zumindest das Bewusstsein schärfen indem die Awarenesseinstellungen immer symmetrisch sind. Wenn z.B. in einem Instant Messaging System ein_e Benutzer_in darüber informiert werden möchte, wenn ein_e andere Benutzer_in online ist, müssen sie sich gegenseitig authorisieren. Danach wird aber immer beiden angezeigt, wenn der_die Gegenüber online ist.

Übertragen auf gespeicherte Daten kann es bedeuten, dass jeder Zugriff auf Informationen über eine Person, dieser Person mitgeteilt wird. In einige Sozialen Online Netzwerken wird diese Option angeboten.

61 Im Deutschen wird äquivalent der Begriff *Gewährtigkeit* genutzt, da er aber nicht so geläufig ist werde ich im folgenden von Awareness schreiben.

62 vgl. entspricht den Awareness Patterns (A-)SYNCHRONOUS GROUPWARE AWARENESS im Abschnitt 3.2.3

63 vgl. dazu auch Prinz (2001)

Nach Iachello and Hong (2007) können solche Funktionen durchaus erfolgreich sein und dazu führen, dass eine verdachtsunabhängige Durchforstung von Datensammlungen nicht ohne weiteres vorgenommen wird, da der_die Einsichtnehmende damit rechnen muss, dass die Einsicht dem Gegenüber bewusst wird, z.B. dadurch, dass ein Grund für die Überprüfung angegeben werden muss. Auf der anderen Seite versteht man unter PRIVACY AWARENESS eine Möglichkeit die informationelle Selbstbestimmung zu stärken.

> Privacy awareness is defined as a user's perception, cognition and attention on whether others receive or have received personal data, which personal data others receive or have received in detail, who receives or has received personal data, and how these personal data is or might be processed and used. (Pekárek and Pötzsch)

PRIVACY AWARENESS hat dabei nicht zum Ziel Nutzer_innen daran zu hindern personenbezogene Daten preiszugeben, sondern die Aufmerksamkeit zu schulen, welche, auch impliziten Daten, freigeben werden und welche Folgen daraus entstehen können. Ein Beispiel ist die Mailingliste in *Die Neue*. Sie hat sich als Kommunikationsmedium zwischen den Mitarbeiter_innen etabliert, asynchronen Kommunikation über die Schichtwechsel hinweg. Das Bewusstsein dafür, dass ein Archiv angelegt wird ist nicht zwangsläufig vorhanden, da alle die E-Mails auch in ihrem eigenen Postfach abgespeichert haben. Weil das Archiv nicht, oder nur in Einzelfällen genutzt wird, fehlt das Bewusstsein dafür, dass darüber auch Personen auf die E-Mails zugreifen können, die nicht explizit adressiert sind.

4.5.2 *Tranzparenz*

Eines der Probleme der informationellen Selbstbestimmung, nicht nur im betrieblichen Datenschutz, ist die mangelnde Transparenz der Datenerhebung und -verarbeitung. Die Komplexität der IT-Systeme macht es für Andwender_innen schwierig sie zur durchschauen. Vor der Nutzung ist unklar welche personenbezogenen Daten überhaupt erhoben werden, weil zum Beispiel nicht intuitiv erkennbar ist, dass die Uhrzeit der Nutzung aus Gründen der Systemstabilität mit Personenbezug gespeichert, diese aber gleichzeitg zur Verhaltenskontrolle genutzt werden kann. Genauso schwierig ist es aber auch, ist man sich über die Erhebung bewusst, abzuschätzen, welche Folgen die Erhebung haben kann. So können Änderungen die sich im Laufe der Zeit ergeben, wie etwa in *Die Neue*) nicht immer vorher erkannt werden. Während die Speicherung der personenbezogenen Daten, die bei der Nutzung der Mailingliste anfallen für das gruppeninterne Archiv möglicherweise beim Einrichten noch Zustimmung fanden, ist die Änderung, die sich dadurch ergibt, dass Daniela, die an der bisherigen Kommunikation unbeteiligt war, am Anfang nicht bedacht worden ist. Deswegen bescheiben Pekárek and Pötzsch die Notwendigkeit für Transparenz wie folgt

> Transparency of (personal) data flows contributes to privacy awareness of users. Technological means to provide transparency - so-called transparency tools - can give information on intended collection and storage of personal data

> (ex ante) or enable the user to access stored data (ex post) or even allow for counterprofiling in order to "guess"how user's data matches relevant group profiles.

Camenish et al. erwarten von transparenten Systemen, dass

- für die User erkennbar ist warum welche Informationen wo gespeichert werden.
- sie Nutzer_innen anzeigen welche Daten ganz konkret gespeichert sind und wie sie verarbeitet werden.
- schon vor der Speicherung angezeigt wird, welche Konsequenzen, z.B. im Bezug auf Profilbildung, zu erwarten sind, um die Risiken für den_die einzelne besser abschätzbar zu machen.

Die gespeicherten Daten und auch die Möglichkeiten verschiedener Mitarbeiter_innen auf sie zuzugreife,n unter anderem auch Administratoren, sollten also genauso einsehbar sein, wie eine Übersicht über das entstehende Profil.

4.5.3 *Prävention*

Artikel-29-Datenschutzgruppe (2002) verweisen zurecht darauf, dass es weniger aufwendig ist Prävention zu betreiben, als zu versuchen jeden Missbrauch aufzudecken. Darin waren sich auch die interviewten Expert_innen einig. Nicht zuletzt, weil nach einer missbräuchlichen Nutzung die Vertrauensbasis bereits gestört ist und diese wiederherzustellen kostet ebenfalls Zeit.

SENSIBILISIERUNG Zwar können die oben beschriebenen Awareness- und Tranzparenz-Informationen ein Bewusstsein dafür schaffen wie die Verarbeitung und Nutzung der personenbezogenen Daten abläuft, aber diese Informationen sind immer auch der Gefahr ausgesetzt, nicht wahrgenommen oder ignoriert zu werden.[64]

Im Rahmen von Schulungen zur Nutzung von neuen Systemen sollten die späteren Nutzer_innen deswegen immer auch auf die möglichen Konsequenzen aufmerksam gemacht werden. Dabei sollte insbesondere auf Techniken eingegangen werden, die den Usern die größten Freiheiten gewähren. E-Mails mit brisantem Inhalt sind immer wieder Ursache von Auseinandersetzungen.[65] Der Hinweis darauf, das bestimmte Informationen in einem andern Kontext verwendet und veröffentlicht möglicherweise das Gegenteil von dem Aussagen, was intendiert war, ist notwendig. *Schulungen*

Ziel einer Sensibilisierung kann es auch sein die von Artikel-29-Datenschutzgruppe (2002) vorgeschlagene Trennung von beruflich und privat, zumindest innerhalb der später noch nachvollziehbaren Kommunikation, zu erreichen. Die Autor_innen schlagen vor etwa verschiedene Postfächer für private und berufliche E-Mails zu nutzen oder auf Mailinglisten Privates außen vor gelassen wird.

64 Iachello and Hong (2007) führen Studien an, die nachweisen konnten das die meisten User Nutzungsbedingungen nicht lesen und auch warnende Pop-Ups in der Regel ignoriert werden.

65 Hier sei nochmal an das in der Einleitung erwähnte Beispiel verwiesen. *Think Before You Post* war auch der Titel des *Safer Internet Day 2010* `http://www.saferinternet.org/web/guest/safer-internet-day` (Abgerufen am 28.05.2010)

Um die Sensibilisierung im täglichen Arbeitsablauf aufrecht zu erhalten schlagen Ackerman and Cranor (1999) PRIVACY CRITICS vor. Das sind kurze, wechselnde Meldungen was an der aktuell genutzten Anwendung oder bei aktuell publizierten Daten problematisch sein könnte.

VERTRAUEN Ein starkes Vertrauen zwischen den Mitarbeiter_innen kann den Datenmissbrauch vorbeugend verhindern, ohne in den Prozess der Kollaboration direkt eingreifen zu müssen. Ist ausreichendes Vertrauen vorhanden, kann etwa Kritik offen geäußert und Probleme sachlich diskutiert werden.[66] Erfahrungsbasiertes Vertrauen (vgl. 2.7) kann etwa. durch stabile Gruppenkonstellationen oder offene Kommunikation erreicht werden. Das rollen- und regelbasierte Vertrauen wiederum kann durch klare Gruppenstrukturen und, wie auch in den Interviews angemerkt, engagierte und aufmerksame Vorgesetzte gestärkt werden.

Um Vertrauen aufbauen zu können in Systemen, in denen soziale Mechanismen nicht greifen können, existieren Systeme die zum REPUTATIONMANAGEMENT dienen.[67] Solche Situationen treten etwa auf, wenn nur einmalig computervermittelt interagiert und die nötigen Zusatzinformationen wie die Rolle in einer Organisation etc. nicht zur Verfügung stehen. Die Auktionsplattform eBay hat solche Systeme als eines der ersten Unternehmen eingesetzt um das Vertrauen zwischen Bieter_innen und Verk äufer_innen zu stärken. Die Reputation eine_s Verkäufer_in wird durch die Bewertungen vergangener Verkäufe bestimmt. Jede_r Käufer_in kann nach Abschluss einer Transaktion eine Bewertung über den Handel abgeben (Gut, Neutral, schlecht). Die Summe dieser Bewertungen werden allen zukünftigen Kund_innen angezeigt um diesen eine Entscheidungshilfe geben zu können ob einer_m Anbieter_in getraut werden kann.

4.5.4 *Organisation*

Nicht nur das Unternehmen ist in der Pflicht eine Infrastruktur bereit zu stellen, die den größt möglichen Schutz der Persönlichkeitsrechte der Angestellten bietet. Auch die Angstellten sind aufgefordet verantwortungsbewusst zu handeln, nicht nur gegenüber dem Unternehmen.

Es sollte die Norm sein, dass persönliche Daten nur in dem Rahmen verwendet werden, für den sie gedacht sind. Solche Prinzipien können zum Beispiel in interne Unternehmensrichtlinien festgeschrieben werden, um ihnen Nachdruck zu verleihen.

ARBEITSRECHTLICHE KONSEQUENZEN Es muss klar sein, dass ein Verstoß gegen die Zweckbindung der Daten, auch wenn diese ohne weiteres möglich ist, arbeitsrechtliche Konsequenzen haben kann. Je nach Art des Verstoßes kann auch eine Abmahnung die Folge sein. Dies muss unabhängig von den Schlussfolgerungen gelten, die ein_e Mitarbeiter_in aus den Daten ziehen kann. Auch wenn, wie im Fall *Der Skandal* tatsächlich ein Fehlverhalten vorliegt, dürfen die_der einzelne Mitarbeiter_in nicht selbst Nachforschungen anstellen, sondern sollten sich an die Personalabteilung wenden.

66 Das alle Probleme sachlich diskutiert werden müssten, statt sie über Interpretationen von der personenbezogenen Daten zu lösen, wurde auch im Workshop häufig angemerkt.

67 ausführlich in Camenish et al. S. 37f.

AUFSICHTSPFLICHT Genauso in der Verantwortung sind aber auch die jeweiligen Vorgesetzten. Sie tragen die Verantwortung für die Gruppe und müssen Zwischenfälle, je nach Hierachiestufe, auch nach oben rechtfertigen. Hier ist auch Sensibilität für die Gruppenstruktur und die einzelnen Angestellten gefragt um Konflikte erkennen zu können. Diese Art der Führungskompetenz hat insbesondere der zweite Interviewpartner betont.

AUDITS Eine regelmäßige Nachprüfung ist erforderlich um sich zu vergegenwärtigen welche Daten im Laufe der Nutzung des Systems zusätzlich angefallen sind. Da sich auch die Nutzung eines Systems über die Zeit ändert, wenn sie von den Nutzer_innen adaptiert wird, sind auch die die anfallenden personenbezogenen Daten möglicherweise nicht mehr vom ursprünglichen Zweck gedeckt. Regelmäßige Audits, in deren Rahmen auch eine Überarbeitung von Berechtigungskonzepten fallen kann, können, ähnlich der Vorabkontrolle, die Rahmenbedingungen zu Gunsten der informationellen Selbstbestimmung verändern.

ORGANISTATIONSSTRUKTUR Die Struktur einer Gruppe kann das gegenseitige Vertrauen maßgeblich beeinflussen. Gerade in kollaborativen Gruppen ist die Notwendigkeit von Kommunikation zur Koordination vorhanden, um auch Streitigkeiten wie etwa bei der Ressourcenverteilung beilegen zu können. Neben der Kommunikation, die über die verschiedenen Plattformen möglich ist, sind reale Treffen, in Face-To-Face-Kommunikationssituationen hilfreich um Konflikte, etwa für den_die Vorgesetzte sichtbar werden zu lassen und lösen zu können.

4.5.5 *Arbeitsplatz*

Gegen, die unbeabsichtigte, zufällige Preisgabe von Informationen (INCIDENTIAL DISCLOSURE) in *Der Skandal* existieren Maßnahmen die auf Ebene der Darstellung des Bildschirms Abhilfe schaffen.

Für Bildschirme, die in Büros mit Publikumsverkehr stehen oder für Reisende die z.B. während der Bahnfahrt ihren Monitor vor Blicken Dritter schützen möchten, gibt es bereits seit einigen Jahren so genannte Blickschutzfilter. Spezielle Folien verringern die Sichtwinkel in denen der Bildschirminhalt noch erkennbar ist auf einen so kleinen Bereich, dass nur die Person die direkt vor dem Bildschirm sitzt in der Lage ist alles zu erkennen.

Tarasewich and Campbell (2005) haben ein Firefox Werkzeug entwickelt, dass sensitve Daten - konkret beim Online-Banking - schwärzen und nur anzeigen, wenn sie mit der Maus markiert werden.

In Kombination mit einem Sensor wie ihn Neustaedter and Greenberg (2003) entwickelt haben lassen sich Video-Chat-Programme so konfigurieren, dass nur bei geschlossener Tür das Bild sichtbar ist.

4.6 ZUSAMMENFASSUNG DER MASSNAHMEN

In diesem Kapitel wurde eine Reihe von technischen und organisatorischen Maßnahmen vorgestellt, die die Zweckentfremdung personenbezogener Daten in Kooperationssystemen verhindern und die informationelle Selbstbestimmung der Nutzer_innen stärken können.

Eine Übersicht der Maßnahmen ist in Abbildung 11 zusammengestellt. Die Liste ist in mehrere Bereich gegliedert, die sich am Ablauf der

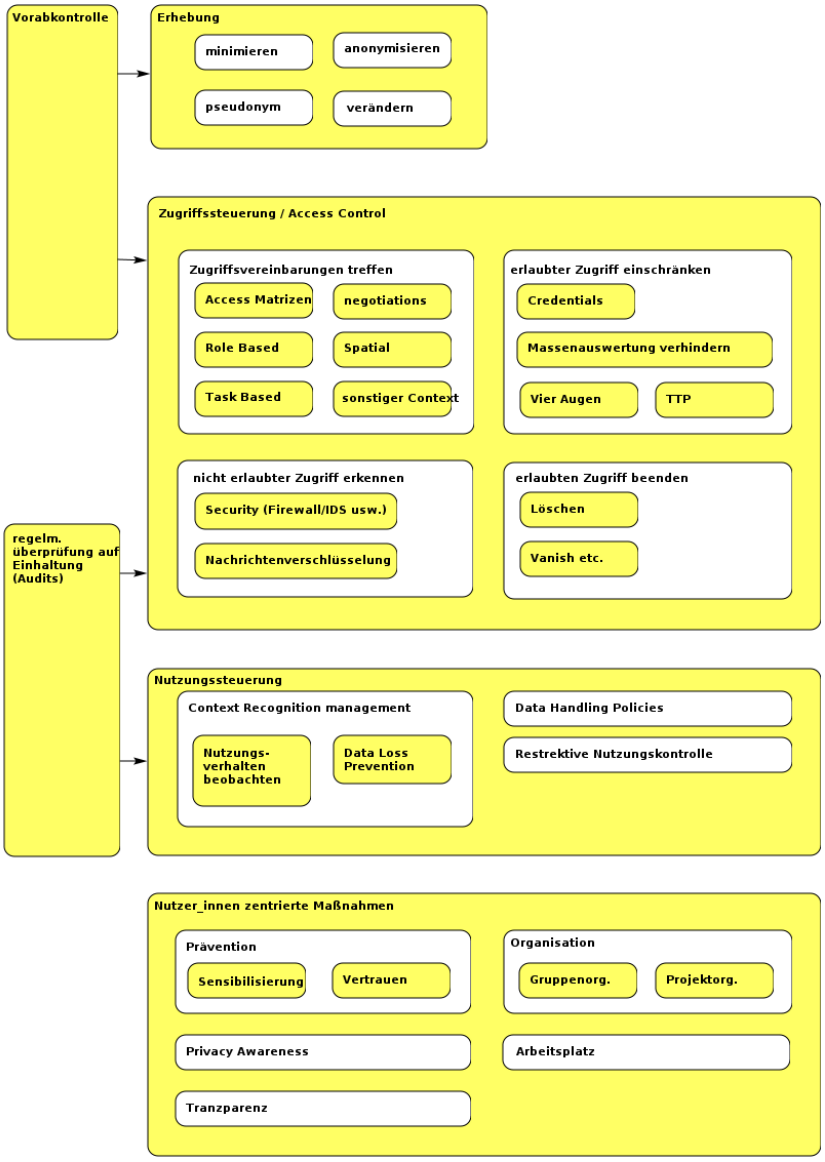


Abbildung 11: Maßnahmenübersicht

Nutzung von solchen Systemen orientieren. Viele Probleme lassen sich umgehen, in dem von Anfang an, z.B. im Rahmen einer Vorabkontrolle der unüberlegten Erhebung von Daten vorgebeugt (vgl. 4.2) und ein Berechtigungskonzept entwickelt wird, wer die Daten unter welchen Umständen verarbeiten darf (siehe 4.3). Einige Konzepte können auch zur Steuerung des Nutzungsverhaltens beitragen (vgl. 4.4). Nicht zu vernachlässigen sind aber auch die überwiegend organisatorischen Maßnahmen, die zentriert auf die Nutzer_innen, durch Sensibiliesierung für die mögliche Brisanz der bei der Nutzung entstehenden Daten und die Gruppenprozesse, präventiv wirken können (siehe Abschnitt 4.5).

5 LÖSUNGSENTWURF

In diesem Kapitel werden die im vorangegangenen Kapitel beschriebenen Maßnahmen konkretisiert und auf die unterschiedlichen Problemstellung der Szenarien, soweit möglich, angewendet. Da die Maßnahmen an sehr unterschiedlichen Punkten in der Nutzung ansetzen, werden keine optimierten Szenarien vorgeschlagen,[68] stattdessen werden die verschiedenen Möglichkeiten diskutiert und Empfehlungen gegeben, die so auch in ähnlichen Kontexten anwendbar sein sollen.

5.1 SZENARIO 1: DIE MACHT DER STATISTIK

Im ersten Szenario wurde der Alltag in dem wachsenden IT-Unternehmen *Andcompany* beschrieben. Als die Entwickler_innen in einem Projekt nicht wie geplant vorankommen und gleichzeitig Konkurrenz zwischen zwei der Beteiligten aufkeimt, eskaliert die Situation. Erst verwendet Carsten die Log-Dateien aus einem VCS, um seinem Konkurrenten Bastian Untätigkeit nachzuweisen. Im Gegenzug nutzt Bastian dann die Protokolle seines Chat-Clients, um sich selber zu profilieren.

5.1.1 *Logdateien eines VCS*

Carsten verwendet die Logdateien des VCS, um Bastian Beitrag zum Projekt quantitativ zu bewerten. Die Logdateien enthalten Informationen darüber wer, wann, welche Änderung am Quellcode eines Programms gemacht hat. Die Daten werden erhoben, um Konflikte zwischen verschiedenen Dateiversionen (automatisch) zu beheben, und um Änderungen eines_r Programmierer_in zurück verfolgen zu können, damit Rücksprache gehalten werden kann.

5.1.1.1 *Maßnahmen bei der Datenerhebung*

MINIMIEREN Um die Funktionalität eines VCS zu gewährleisten, speichern diese neben der Änderung selbst auch den Zeitpunkte zu denen eine Änderungen an den Server gesendet wird. Diese Änderungen werden einem Benutzernamen eine_r Entwickler_in zugeordnet. Die maximale Minimierung wäre an dieser Stelle möglich: eine Nutzung ohne Authentifizierung. Je nach Große der Entwickler_innengruppe und deren Arbeitsstruktur können aufkommende Fragen auch über andere Wege geklärt werden. Gibt es ein gemeinsames Büro könnte sie schlicht nachfragen, wenn Probleme auftauchen.

ANONYMISIERUNG Vollständig anonym wäre die Nutzung allerdings vermutlich nicht, da die Entwickler_innen sich absprechen, um möglichst effektiv an dem Programm arbeiten zu können, um doppelte Arbeit zu vermeiden oder Rücksicht auf die Stärken der Einzelnen

68 Wie auch von den Expert_innen in den Interviews einstimmig erklärt wurde, würde höchstwahrscheinlich eine detaillierte Erarbeitung, Anwendung und Durchsetzung eines von einer_m DSB erarbeiteten Regelwerk einen Großteil der Probleme lösen. Gerade die Gruppen- un Nutzungsdynamiken der Szenarien machen dies aber unrealistisch.

nehmen zu können, fällt eine Zuordnung einer Änderung zu einer bestimmten Person nicht schwer.

Wenn die Log-Dateien allerdings nur anonymisierte Informationen enthalten würden, wäre eine automatisierte Auswertung schwierig, da zuerst manuell und zeitaufwendig die Deanonymisierung vorgenommen werden müsste.

PSEUDONYME NUTZUNG Auf Grund des Zusatzwissens wäre ein einziges Pseudonym pro Person nutzlos. Vorstellbar wären dagegen automatisch generierte Pseudonyme, die bei jeder gesendet Änderung anders sein müssten. Eine TTP könnte die Zuordnung der Pseudonyme zu den realien Personen verwalten um in Einzelfällen eine Zuordnung vornehmen zu könne.

VERÄNDERN Maßnahmen wie etwa Vergröberung der Logging-Informationen über die Zeit sind denkbar. Sinnvoll erscheint zudem, das Löschen des Personenbezugs nach einem gewissen Zeitraum. Oft ist es selbst dem_der Urheber_in nach einer gewissen Zeit nicht mehr möglich, sich an den konkreten Anlass für eine Änderung und die Auswirkungen zu erinnern. Der Zweck kann also auch mit den gespeicherten Informationen nicht erreicht werden.

5.1.1.2 *Maßnahmen bei der Zugriffssteuerung*

ZUGRIFFSVEREINBARUNGEN Eine ACP ist nur rudimentär im Einsatz. Zugriff ist auf die Mitglieder des Entwicklungsteams beschränkt (RBAC). Ergänzend könnte die Steuerung kontextabhängig sein, indem der Zugriff z.B. auf das interne Firmennetz von Andcompany beschränkt oder nur tagsüber zu den üblichen Betriebszeiten möglich ist. So kann verhindert werden, dass sich nach Feierabend die aufgestaute Wut in der Suche nach verwertbarem Material entlädt.

Das VIER-AUGEN PRINZIP könnte zudem eine sinnvolle Ergänzung des Zugriffsschutzes darstellen. Eine etabliertes Verfahren in der agilen Softwareentwicklung, das Pair-Programming,[69] setzt voraus, dass immer zwei Entwickler_innen zusammen am Quellcode arbeiten. Diese Methode gilt nicht nur als effektivitätssteigernd, sondern würde auf organisatorischer Ebene bereits den Konflikt dadurch entschärfen, dass Änderungen am Quellcode nie nur einer Person zuzurechnen sind. Eine quantitative Bewertung der Arbeit von einzelnen Programmierer_innen wäre so ausgeschlossen.

Eine andere Form des VIER-AUGEN-PRINZIPS ist es, den Zugriff auf einen Eintrag in den Log-Dateien eines VCS abhängig zu machen von der Einwilligung einer zweiten Person. Die statistische Auswertung würde so zusätzlichen Aufwand, nicht nur bei dem_der Angreifer_in, erfordern, sondern auch bei denjenigen deren Einwilligung eingeholt werden muss.

ZUGRIFF EINSCHRÄNKEN Die Möglichkeiten die Daten statistische auszuwerten könnte dadurch eingeschränkt werden, dass eine TTP die Zugriffe auf die Log-Dateien reguliert. Wie oben beschrieben, kann die Nutzung von nur einmal genutzten Pseudonymen die massenhafte Abfrage über eine_n konkrete_n Urheber_in so verhindert werden.

69 Nach Beck and Andres (2001)

Die TTP kann außerdem dazu dienen, die Entscheidung über die Anfragen weiterzuleiten. Stellt ein_e Nutzer_in die oben genannte Anfrage, könnte die TTP den_die Urheber_in darüber informieren und selbst entscheiden lassen, ob er_sie diese Information freigeben möchte, oder möglicherweise direkt darauf reagiert, indem er_sie den_die Anfragende kontaktiert.

Soll der Zugriff auf die Log-Daten nicht auf diese Weise erschwert, sondern nur der im Szenario besprochene Missbrauch verhindert werden, böten Methoden, wie die Einbindung von CAPTCHAS, ausreichenden Schutz. Chris müsste erheblichen manuellen Mehraufwand leisten, um eine ausreichend große Datenbasis bekommen, wenn jeder Abruf von Log-Informationen durch ein CAPTCHA geschützt wäre.

Der Aufwand könnte auch dadurch vergrößert werden, dass die angeforderten Informationen dem_der Nutzer_in, statt in maschinenlesbarem Text, in ein Bild eingebettet angezeigt würden. So wäre das Kopieren und die Weiterverarbeitung in anderen Programmen erheblich erschwert.

ZUGRIFF VERHINDERN Ein Netzwerkanalysewerkzeug wie ein Intrusion Detection System (IDS), dass kontinuierlich den Nerzwerkverkehr beobachtet, kann dazu dienen ungewöhnliche Zugriffsmuster zu erkennen. Wenn etwa, statt einem einzelnen Eintrag aus den Log-Dateien, eine ganze Reihe abgerufen werden. Allerdings könnte dieses automatische System auch einige *Fehlalarme* erzeugen. Zusätzlich ist zu klären, wem die Alarmmeldungen mitgeteilt und welche, möglicherweise personenbezogenen Daten, dabei übermittelt werden sollen.

ZUGRIFF BEENDEN Wie oben bereits erwähnt, sind mit einigem Abstand die Zuordnungen von Änderungen zu Personen für den Zweck der Nachverfolgbarkeit kaum noch hilfreich. Deshalb sollte hierfür eine sinnvolle Löschfrist definiert werden. Eine Mindestanforderung ist, die Log-Informationen spätestens nach dem Ende des Projektes zu löschen.

5.1.1.3 *Maßnahmen zur Nutzungssteuerung*

DATA HANDLING POLICIES Um die Möglichkeiten von DHP ausnutzen zu können, bedarf es eines Systems, in das diese integriert sind. (vgl. Abschnitt 4.4). In der Programmierung werden oft spezielle Entwicklungsumgebungen eingesetzt, die diese Aufgabe übernehmen können. Über die DHP könnte so etwa die Speicherdauer auf den Client-Rechnern definiert werden, um lokale Datensammlungen zu verhindern. Die Verwendung in anderen Programmen sollte für Entwickler_innen nicht erlaubt sein, wenn notwendig, können bestimmten Rollen, wie der Projektleitung, Möglichkeiten zur Auswertung bereitgestellt werden.

RESTRIKTIVE REGELUNG Um die Nutzungssteuerung durchzusetzen muss dafür Sorge getragen werden, dass nur zertifizierte Software, die DHP unterstützt, eingesetzt wird. Andernfalls wäre es eventuell möglich die Daten wiederum zu exportieren und missbräuchlich zu nutzen.

CONTEXT RECOGNITION Ein System, ähnlich dem in Kaptitel vier vorgestelltem ELICT, wäre in der Lage zu bemerken, wenn Chris beginnt mehr Daten abzurufen als nur einzelne Änderungsinformationen. Genauso könnte detektiert werden, wenn er auf Projektdateien zugreift,

die nicht (mehr) in seinem Aufgabenbereich liegen. In dem Fall könnte eine entsprechende Meldung an David gehen. Die Daten ständen Chris zur Verfügung und seine Auswertung könnte er trotzdem erstellen, aber David hätte aber früher intervenieren können. Zudem werde es Chris möglicherweise von seinem Vorhaben abbringen, wenn die Überwachung für ihn transparent ist.

5.1.1.4 *Nutzer_innen zentrierte Maßnahmen*

TRANZPARENZ UND AWARENESS Es sollten diejenigen, deren Änderungen von Dritten eingesehen werden, darüber informiert werden. Neben dem Abschreckungseffekt auf Seiten von Chris böte dies Bastian die Möglichkeit sich direkt an Chris zu wenden, um zu erfahren was der Grund für die zahlreichen Informationsabrufe ist.

ORGANISATION Um die Zusammenarbeit in der Gruppe zu verbessern, ist auch eine geändertes Projektmanagement von Vorteil. In der Softwareentwicklung haben sich sogenannte *Agile Methoden* etabliert.[70] Durch das oben bereits beschriebene Pair-Programming wird nicht nur ein Vier-Augen-Prinzip eingeführt, sondern auch die Kommunikation in der Gruppe erhöht und durch die geteilte Verantwortung übermäßige Konkurrenz zwischen den Entwickler_innen im besten Fall verhindert. Projektmanagement mit Scrum erhöhet ebenfalls die Kommunikation und die Strukturierung der Arbeitsabläufe und würde Davids Rolle in der Gruppe stärken. Als Projektleiter sollte David generell mehr Verantwortung für die Mitarbeiter_innen übernehmen und auch auf die Einzelnen eingehen, um aufkeimende Konflikte frühzeitig zu erkennen.

5.1.2 *Logdateien eines Chat-Clients*

Nachdem Carsten Basti mit seinen Vorwürfen, basierend auf den VCS-Statistiken konfrontiert hat und Bastian sich bloßgestellt fühlt, möchte er sich verteidigen. Dazu wertet er wiederum die Protokolle seines Instant Messangers aus, der aufzeichnet wer, wann online ist, welchen Status er hat und mit wem kommuniziert wird.

5.1.2.1 *Maßnahmen bei der Datenerhebung*

MINIMIEREN Awareness Informationen sind wesentlicher Bestandteil von Groupwaresystemen. Die Anzahl der möglichen Stati kann dabei aber stark variieren. Üblich sind neben dem Status *Offline* die verschiedene Online-Stati *Verfügbar, Abwesend, Beschäftigt* und *Unsichtbar*. Letzterer zeigt nur ausgewählten Kontakten den *Online*-Status an. Eine weitere Reduktion der Stati verringert dabei aber eher den Nutzen der Information, als dass es aus Datenschutzssicht Vorteile brächte. Sinnvoller erscheint es eine dauerhafte Speicherung dieser Daten zu verhindern. Da sie, sobald sie durch einen neuen Awareness-Status ersetzt wurden, ihren Zweck erfüllt haben. Im vorliegenden Szenario ist das Problem, dass die Informationen von Bastian auf seinem lokalen Computer gesammelt werden und damit nicht mehr so leicht zentralen Löschfristen unterstellt werden können. Eine zentralisierte Konferenzlösung mit einem Client, der verhindert, dass die Daten lokal gespeichert werden können, wäre hier notwendig.

70 Zwei Methoden, neben anderen, sind XP nach Beck and Andres (2001) und *Scrum* nach Schwaber (2002).

ANONYMISIEREN/PSEUDONYMISIEREN Die Informationen über den Status eine_s Kollaborationspartner_in zu ano- oder pseudonymisieren, widerspricht dem Zweck dieser Information und ist daher nicht zu empfehlen.

VERÄNDERN Sollen die Informationen über vorangegangene Stati noch längere Zeit verfügbar sein, macht es Sinn sie für diesen Zweck vergröbert abzuspeichern. Je nach Zweck könnte die drei Online-Stati zu einem einzelnen aggregiert werdend zudem kann die konkrete Uhrzeit, zu der ein Status gewechselt wurde, abhängig vom Zweck, vergröbert werden.

5.1.2.2 *Maßnahmen bei der Zugriffssteuerung*

ZUGRIFFSVEREINBARUNGEN Die ACP des Chatprogramms sind kaum vorhanden. Die Authentifizierung erfolgt nur einmal durch eine Bestätigung als Kontakt. Dadurch wird die Berechtigung, den Status zu sehen, erteilt. Zudem sind die Informationen, auf Grund des eingesetzten Protokolls, direkt auf Bastians Rechner kopiert und entziehen sich damit einer zentralen Zugriffssteuerung. Um ein Zugriffskonzept zu etablieren, das auch spätere Berechtigungsänderungen noch nachträglich umsetzt, müsste die Kommunikation über eine zentrale Plattform, z.B. einer browser-basierten Lösung, laufen und nicht mehr auf den Client-Rechnern gespeichert werden.

ZUGRIFF EINSCHRÄNKEN Bastian könnte bei einer zentralisierten Lösung nur noch an eine Kopie der Daten gelangen, wenn er sie mutwillig über einen Crawler aus den Webseiten extrahieren würde.

ZUGRIFF BEENDEN Wie schon oben beschrieben, ist eine dauerhafte Speicherung von Statusinformationen in den wenigsten Fällen notwendig. Eine Speicherung könnte in der Client-Software untersagt und auch bei einer webbasierten Lösung verhindert werden.

ZUGRIFF VERHINDERN Um nicht Parteien, die an der Kommunikation nicht beteiligt sind, Zugriff auf die Inhalte zu geben, sollten diese verschlüsselt werden. Off-The-Record Messaging (OTR) bietet sich hier als Protokoll an. Damit können sowohl die Inhaltsdaten als auch die Statusinformationen verschleiert werden.

5.1.2.3 *Maßnahmen zur Nutzungssteuerung*

NUTZUNGSSTEUERUNG Die Kontrolle der Verwendung macht nur Sinn, wenn es nötig ist diese zu speichern. Die bisher vorgestellten Maßnahmen legen aber nahe dies nicht zuzulassen.

RESTRIKTION Wird weiterhin auf eine Client-seitige Software gesetzt, sollte hier vorgeschrieben sein, dass die Daten nicht speichern darf.

5.1.2.4 *Nutzer_innen zentrierte Maßnahmen*

Die zu Problem 1 vorgeschlagenen Maßnahmen sind zur Behebung beider Probleme geeignet.

5.2 SZENARIO 2: DIE NEUE

In *Die Neue* wird Daniela als Administratorin in einem kleinen Rechenzentrum angestellt. Sie soll auf Dauer die Aufgaben von Achim übernehmen, der in naher Zukunft in Rente gehen wird. Neben Achim sind noch Birgit und Carsten dort beschäftigt. Als Achim, der die Koordination der Gruppe innehat, wegen einem Rückenleiden für einige Zeit ausfällt, ist Danielas Einarbeitung abrupt beendet und sie muss reguläre Aufgaben im Schichtdienst übernehmen. Da die Administrator_innen nie alle parallel arbeiten, verwenden sie eine Mailingliste und einen Issue-Tracker zur Zusammenarbeit. Carsten nutzt die Gelegenheit und weist eine ihm unliebsame Aufgabe im Issue-Tracker Daniela zu. Um seine Spur zu verwischen, loggt er sich mit Birgits Benutzernamen ein. Daniela ist durch das Mailinglistenarchiv darüber informiert, dass es sich im Carstens Aufgabe handelt und stellt mit Birgit zusammen Carstens Betrug fest.

5.2.1 *Identitätsfälschung*

Carsten nutzt sein Wissen darüber, dass Birgit das System nicht nutzt, um mit ihrem Account Aufgaben für Daniela zu erstellen.

5.2.1.1 *Maßnahmen bei der Datenerhebung*

MINIMIEREN Im Issue-Tracking-System werden neben den Profilinformationen (Accountname u.ä.) mit Personenbezug nur die Aufgaben selbst gespeichert. Der Bezug zwischen einer Aufgabe und einer Person wird erst hergestellt, wenn die Aufgabe einem_r Administrator_in zugewiesen wird, damit diese_r sie bearbeitet.[71] Da diese Zuweisung Zweck des Systems ist, ist eine Minimierung hier nicht möglich ohne den Zweck des Systems zu stören.

ANONYMISIEREN / PSEUDONYMISIEREN Das Issue-Tracking-System dient der Koordination, indem Aufgaben bestimmten Personen zugeordnet werden. Dadurch, dass die Zuordnung einsehbar ist, kann verhindert werden, dass sich zum Beispiel zwei Personen um die Behbung des gleichen Problems kümmern. Es ist allerdings nicht in allen Fällen notwendig, dass auch bekannt ist, wer die Aufgabe eingetragen und zugewiesen hat. Dass diese Information mitangegeben wird, soll im Fall unklarer Formulierungen Rückfragen ermöglichen. Im beschriebenen Szenario könnte, auf Grund der geringen Gruppengröße und damit der potentiellen Urheber_innen eines Eintrags auch auf diese Information zu verzichten oder sie über Rollenpseudonyme[72] unzugänglich gemacht werden.. Im konkreten Fall könnte so verhindert werden, dass Daniela annehmen muss, Birgit hätte ihr die Aufgabe zugewiesen und eine Rückfrage an beide (über die Mailingliste) hätte Carstens Versuch, die lästige Aufgabe loszuwerden, früher auffallen lassen.

71 Weitere Rollen in dem Prozess sind zudem der_die *Reporter_in*, also die Person, die Aufgaben in das System einstellt, sowie eventuelle Kommentator_innen.

72 Diese könnten über einen Account *Reporter*, den alle Administratoren benutzen wenn sie einen Aufgabe eintragen, realisiert werden.

5.2.1.2 *Maßnahmen bei der Zugriffssteuerung*

ZUGRIFFSVEREINBARUNGEN Die Zugriffssteuerung der Benutzer innerhalb des Issue-Trackers funktioniert korrekt. Das Problem besteht nicht auf der Ebene der normalen Zugriffsrechte sondern auf dem der Administrationsrechte. Im Rahmen eines Zugriffskonzeptes darf es nicht passieren, dass Carsten Birgits Passwort kennt. Sie hätte es frühzeitig ändern müssen. Um zu verhindern, dass Carsten mit seinen Rechten als Administrator Birgits Passwort ändert, um so wieder Zugriff auf ihren Account zu bekommen wäre es notwendig, Carstens Administrationsrolle in dem System von seiner Rolle als Benutzer zu trennen. Änderungen an der Konfiguration durch die Adminstrationsrolle sollten dann durch eine weitere Person, etwa durch ein geteiltes Passwort, bestätigt werden.

ZUGRIFF EINSCHRÄNKEN Auf Grund der Arbeitsteilung in Aufgabengebiete ist es nicht notwendig, dass alle Nutzer_innen alle Aufgaben einsehen können. Denkbar wäre zudem, dass für eine_n Nutzer_in nur sichtbar ist welche Aufgaben ihm_ihr zugewiesen wurden, nicht von wem. Bei den Aufgaben, die anderen zugewiesen sind, reicht die Information, dass sie bearbeitet werden, von wem ist nicht zwingend notwendig zu wissen.

ZUGRIFF VERHINDERN Erschwert werden könnte die Identitätsfälschung durch zusätzliche Authentifizierungsmechanismen wie Smart-Cards oder Biometrische-Authentifizierung. Der Zugriff könnte pro Account auch an einen Rechner gebunden werden oder, außerhalb von den Arbeitszeiten der jeweiligen Peron, gesperrt sein.

ZUGRIFF BEENDEN Um Leistungs- und Verhaltensbewertungen wie in *Die Macht der Statistik* zu erschweren, sollte auch hier über Löschfristen nachgedacht werden, beziehungsweise Zeitpunkte zu denen die Aufgaben anonymisiert werden.

5.2.1.3 *Maßnahmen zur Nutzungssteuerung*

CONTEXT RECOGNITION UND DHP Da die personenbezogenen Daten nicht in anderen Systemen weiterverarbeitet oder übermittelt werden, bringen solche Maßnahmen für das konkrete Problem kein Vorteile.

AWARENESS UND TRANSPARENCY Birgit hat sich an die Benutzung des Systems noch nicht gewöhnt und bemerkt deswegen die Änderungen nicht. Um ihre Aufmerksamkeit für die Vorgänge im System zu erhöhen, könnte für eine Übergangszeit, eine E-Mail-Benachrichtigung aktiviert werden. Für Daniela wären Awareness-Informationen darüber, dass Birgit ihren Account nicht benutzt, etwa das sie selten eingeloggt ist, eine hilfreiche Information, die wiederum aber auch die Gefahr der Leistungs- und Verhaltenskontrolle mit sich bächte.

SCHULUNG Vor und während der Einführung des Systems sollten alle Beteiligten im Umgang damit geschult werden. Dabei hätte etwa auch jede_r sein_ihr Passwort festlegen können. Zudem wäre das Ziel einer Schulung, dass alle Administrator_innen das System auf ähnliche

Art nutzen und in ihren Arbeitsalltag integrieren, was die Situation entschärft hätte.

GRUPPENORGANISATION Da Achim schon mehrfach krank war, hätte auch in diesem Fall damit gerechnet werden können. Es sollte geregelt sein, wer seine Aufgaben im Fall einer Krankheit übernimmt, auch um den Betrieb des Rechenzentrums aufrecht erhalten zu können.

Eine klarere Strukturierung, wer die Leitung der Gruppe übernimmt und sich verantwortlich zeigt für die Einweisung von Daniela, hätte den Konflikt ebenfalls entschärft. Für Daniela wäre damit auch klarer gewesen, wessen Aussagen sie mehr vertrauen kann.

5.2.2 *Zugriff auf das Mailarchiv*

Eher durch Zufall stößt Daniela in der archivierten E-Mail-Kommunikation auf Hinweise, die vermuten lassen, dass die Aufgaben die ihr über den Issue-Tracker zugewiesen worden sind in Carstens Aufgabenbereich fallen.

5.2.2.1 *Maßnahmen bei der Datenerhebung*

MINIMIEREN Die Funktionsweise von E-Mail-Systemen ist stark standardisiert. Eine Minimierung der anfallenden Daten, würde die Nutzung eines anderen Kommunikationsmediums voraussetzen.[73] Allerdings stellt sich für das E-Mail-Archiv die Frage, ob es überhaupt angelegt werden muss oder die Archivierung der Aufgaben über den Issue-Tracker nicht ausreichend ist und die E-Mail Kommunikation eine unnötige Parallelstruktur darstellt.

ANONYMISIEREN Ist E-Mail-Archiv zur nachträglichen Dokumentation notwendig, kann versucht werden es zu anonymisieren. Allerdings würde das bedeuten, dass nicht nur die E-Mail-Adressen entfernt werden, sondern auch der Inhalt der E-Mails nach deanonymisierenden Anreden oder Signaturen durchsucht werden müssten.[74] Diese Maßnahme würde aber nur das zentral vorhandene Archiv betreffen. Die E-Mails in den Posteingängen der einzelnen Nutzer_innen blieben davon unberührt. Bei einem anonymisierten Archiv bliebe für Daniela die Möglichkeit erhalten vergangene Diskussionen nachzuvollziehen, die Zuordnung von Aussagen zu einzelnen Autor_innen wäre ihr aber nicht ohne weiteres möglich.

PSEUDONYMISIEREN Je nach Art der Nutzung der Mailingliste könnte auch eine Nutzung von rollenbezogenen (z.B. Frühschicht@[..], spätschicht@[..] usw.) E-Mail-Adressen den Personenbezug aufheben. Dabei ist aber zu beachten, dass im Inhaltsteil einer E-Mail (s.o.) oft Namen genannt werden, die einen direkten Bezug ermöglichen.

5.2.2.2 *Maßnahmen bei der Zugriffssteuerung*

ZUGRIFFSVEREINBARUNGEN Die Gruppe hat keine Regeln für den Zugriff auf das Archiv definiert, für den Fall, dass eine Person Zugriff

73 Es fallen neben Absender und Empfängeradresse z.B. auch die Uhrzeit und die Inhaltsdaten an.

74 Nicht zu vernachlässigen ist auch, dass möglicherweise individuelle Formulierungen und Schreibstile die Autor_innen identifizierbar machen können.

erlangen möchte, die bisher nicht an der Kommunikation beteiligt war. Diese Regel könnte sein, dass es einem Mitglied der Mailingliste nur möglich ist auf den Teil des Archiv zuzugreifen, der seit dem Beginn seiner Mitgliedschaft angelegt wurde.

ZUGRIFF EINSCHRÄNKEN Möglich wäre mit technischen Mitteln, wie sie schon für das VCS vorgeschlagen wurden, E-Mails pseudonymisiert anzuzeigen. Die Information über den_die Urheber_in kann, über ein zusätzliche Abfrage bei einer TTP, oder dem_der Urheber_in selbest, erfragt werden.

Sinnvoll wäre zudem, wenn Daniela bei der Dursicht des Archivs nicht allein bleiben würde. Eine weitere Person könnte nicht nur den Einblick auf das Notwendige beschränken, sondern gleichzeitig inhaltlich erläutern und so möglichen Missverständnisse vorbeugen, die durch Fehlinterpretationen von Daniela entstehen könnten.

ZUGRIFF VERHINDERN Hätten die drei Administrator_innen ihre E-Mails von Anfang an verschlüsselt, wären das Archiv vor Missbrauch geschützt und ständen nur ihnen selbst zur Verfügung.

ZUGRIFF BEENDEN Für das E-Mail Archiv sollten Löschfristen definiert sein. Wenn die Kommunikation zudem verschlüsselt stattfände, könnte der Einsatz von Systemen wie EPHEMERIZER zusätzlich verhindern, dass die E-Mails unbegrenzt in Kopie auf den Client-Rechnern gespeichert werden.

5.2.2.3 *Maßnahmen zur Nutzungssteuerung*

CONTEXT RECOGNITION UND DHP Wie bereits im Abschnitt 4.4 erläutert ist eine genaue Zweckbestimmung, gerade für E-Mails schwierig, dadurch, dass der Nachrichtenteil jede mögliche Information fassen kann. Ein Einsatz dieser Techniken würde hier deswegen keinen Vorteil bringen.

AWARENESS UND TRANSPARENZ Möglicherweise ist den drei Nutzer_innen der Mailingliste nicht bewusst, dass jede E-Mail archiviert wird. Gerade wenn das Archiv über einen längeren Zeitraum nicht genutzt wird, kann das Bewusstsein dafür schwinden. Möglich wäre über die Liste selbst regelmäßig einen Hinweis zu schicken, darüber, dass und welche Menge an E-Mails, in einem bestimmten Zeitraum, archiviert wurde.

Zusätzlich sollte es den Beteiligten möglich sein eigene Beiträge im Nachhinein zu löschen. Ein Vorfall etwa, bei dem ein Satz eventuell als Affront verstanden wurde, sollte nicht auf Dauer im Archiv gespeichert sein, wenn sich die Parteien geeinigt haben.

PRÄVENTION In vielen Unternehmen kommt es auf Grund von missverstandenen oder missverständlich formulierten E-Mail zu Problemen. Es ist deswegen notwendig eine Norm herauszubilden, in welchem Tonfall per E-Mail kommuniziert wird und bis zu welchem Grad sich in E-Mails persönliche und berufliche Informationen ausgetauscht werden. Sollte sich diese Norm in Richtung *'persönliches ist erlaubt'* entwickeln, sollte auch allen Beteiligten klar gemacht werden, dass die Informationen persönlich und nur für den_die direkten Empfänger_innen bestimmt sind. Ein teil-öffentliches Archiv wäre in dem Fall unangebracht.

5.3 SZENARIO 3: DER SKANDAL

In *Der Skandal* geht es um eine Gruppe von drei Universitätsangehörigen, von denen zwei (Christoph und Alex), an einem neuen Projekt arbeiten. Die dritte Person (Dominique) fühlt sich benachteiligt, weil sie an dem Projekt nicht beteiligt ist und wird misstrauisch, als sie an einer Änderung an einem Dokument in einer Webplattform nachvollziehen kann, dass diese von einem Computer am anderen Ende der Welt aus verändert wurde. Zufällig platzt sie dann wenig später in eine Videokonferenz der beiden von ihre Verdächtigten und sieht so, dass Christoph im T-Shirt vor der Kamera steht und offensichtlich nicht, wie angekündigt, in der Schweiz ist. Sie kontrolliert, nachdem der Betrug offensichtlich geworden ist, ihre Backup-Kopien alter Kalender und stellt fest, dass dort Konferenzen im Ausland eingetragen sind, die überhaupt nicht stattgefunden haben.

5.3.1 *Lokalisierung über die IP-Adresse*

Dominique kann die IP-Adresse, die als Quelle der letzten Änderung angegeben wird, erkenne, dass Christoph sich an einem anderen Ort aufhält als angenommen.

5.3.1.1 *Maßnahmen bei der Datenerhebung*

MINIMIEREN Die Erhebung der IP-Adresse des_der Zugreifenden ist für den Austausch von Dateien nicht zwingend erforderlich. Der Zweck der Erhebung geht aus dem Szenario nicht hervor. [75]

ANONYMISIEREN/PSEUDONYMISIEREN In einem Dateiaustauschsyste werden Zugriffsberechtigungen an bestimmte Nutzer_innen vergeben, so dass eine anonyme Nutzung ausgeschlossen ist.

VERÄNDERN Eine Vergröberung der IP-Adresse, zum Beispiel indem ein Teil der IP gekürzt wird, würde bis zu einem gewissen Grad Schutz bieten vor der Lokalisierung. Zuverlässig wäre aber einzig die IP-Adresse nicht zu erheben, da auch ein Teil der IP noch etwas über Aufenthaltsort des Rechners aussagen kann, von dem aus auf die Seite zugegriffen wurde.

5.3.1.2 *Maßnahmen bei der Zugriffssteuerung*

ZUGRIFFSVEREINBARUNGEN Die Zugriffssteuerung für die Inhaltsdaten werden von den Beteiligten genutzt. Was das System allerdings nicht anbietet, ist die Steuerung des Zugriffs auf die Verkehrsdaten, eben die IP-Adresse aber auch die Informationen über die letzte Änderungen. Ist der Zugriff auf den Inhalt einer Datei gesperrt, sollte gleichzeitig auch der Zugriff auf die Verkehrsdaten gesperrt sein. Zu klären ist, ob es notwendig ist, dass ein Ordner, für den keine Zugriffsberechtigungen existieren, überhaupt als existierend angezeigt werden muss.

75 In verschiedenen Internetbasierten Systemen wird die IP-Adresse zur einfachen Zugriffssteuerung verwendet. So ließe sich etwa der Zugriff auf das Datei-Sharing Programm auf einen IP-Adressbereich innerhalb eines bestimmten Netzwerkes (bspw. der Universität) beschränken.

ZUGRIFF EINSCHRÄNKEN Ist die Erhebung der IP notwendig, muss die Frage gestellt werden, ob sie allen zugänglich sein soll oder es ausreicht, wenn sie auf Serverebene gespeichert werden. Evtl. wird damit aber der Zugriff z.B. von externen Netzen gesperrt.

ZUGRIFF BEENDEN Sollte die IP aus bestimmten Gründen benötigt werden, sind Löschfristen (z.B. das Ende eines Projekts) einzuhalten.

5.3.1.3 *Maßnahmen zur Nutzungssteuerung*

DHP Ein Policy zur Nutzung der IP könnte den Server anweisen, diese zwar zu speichern, aber nur zu internen Zwecken (etwa zur Generierung von Nutzungsstatistiken etc.) zu verwenden. Die Policy sollte eine Weiterverwendung und Verbreitung, durch Veröffentlichung, auch durch den Administrator des Rechners, untersagen.

5.3.1.4 *Nutzer_innen zentrierte Maßnahmen*

AWARENESS UND TRANSPARENCY Für Christoph sollte transparent sein, dass seine IP Adresse gespeichert wird und sich daraus auch seine Position abgeleitet lässt. Sie könnte etwa neben seinem Logindaten angezeigt und mit einer Landesflagge versehen werden.

Um auch transparent zu machen welche Informationen am Ende für andere sichtbar sind, bieten ähnliche Systeme die Möglichkeit die Einträge aus der Sicht anderer User anzeigen zu lassen. Über diese Funktion wäre es für Christoph möglich zu erkennen, dass seine IP-Adresse auch für diejenigen sichtbar ist, die keinen Zugriff auf den Ordner haben.

5.3.2 *Zufällige Beobachtung einer Videokonferenz*

Dominique betritt Alex' Büro während diese ein Videotelefonat mit Christoph führt. Sie erkennt auf dem Videobild, dass Christoph offensichtlich nicht an dem Ort ist, an dem angegeben hat zu sein.

ERHEBUNG Die zufällige und unfreiwillige Offenbarung des Videobildes lässt sich durch veränderte Erhebung nicht beeinflussen, ohne dem Zweck der Videokonferenz zuwider zu laufen.

ZUGRIFF EINSCHRÄNKEN Am einfachsten ließe sich verhindern, dass Dominique das Bild von Christoph sieht, indem Alex Bildschirm so aufgestellt wird, dass er von der Tür aus nicht einsehbar ist. Zusätzlich gibt es für handelsübliche Bildschirme Klebefolien, die den Blinkwinkel in dem eine Einsicht möglich ist kann, einschränken.

5.3.2.1 *Maßnahmen zur Nutzungssteuerung*

5.3.2.2 *Nutzer_innen zentrierte Maßnahmen*

AWARENESS UND TRANSPARENZ In Einzelfällen sollte es für beide Seiten möglich sein ein Gespräch als vertraulich zu klassifizieren. In dem Fall müssten die Gesprächspartner_inne dafür Sorge tragen, das niemand unbefugtes im Raum ist oder auf andere Art mithören kann. Dies kann dem Gegenüber durch einen Schwenk durch den Raum angezeigt werden. Automatisieren ließen sich diese Funktion mit einem

zusätzlichen Raumsensor, der registriert wenn jemand den Raum betritt. Im Falle verletzter Vertraulichkeit wird das Gespräch dann sofort beendet.[76]

PRÄVENTION Da Alex nicht damit rechnet, dass Dominique spontan ihr Büro betritt, kann man annehmen, dass ihr verhalten unüblich ist. Es kann helfen soziale Normen wie das Anklopfen auch explizit zu formulieren, und so aufzufordern diese Regeln einzuhalten.

Darüber hinaus unterschätzt Christoph offensichtlich Dominiques Enttäuschung darüber, dass sie nicht an dem Projekt beteiligt ist. Etwas mehr Sensibilität für die Anliegen der Angestellten hätte vermutlich zu weniger Misstrauen auf ihrer Seite geführt.

Nicht zuletzt ist aber auch Christophs Vorgehen ein klarer Verstoß gegen die Dienstreiseregelungen der Universität. Es muss sichergestellt sein, dass dieser auch bemerkt wird. Damit die Angestellten aber nicht dazu angestiftet werden sich gegenseitig zu überwachen, könnte es eine Stelle in der Verwaltung geben, an die man sich, möglichst anonym, wenden kann, um einen Verdacht zu äußern.

5.3.3 *Gesammelte Informationen aus Backups*

Dominique stellt weitere Nachforschungen über die angeblichen Aufenthaltsorte von Christoph und Alex an und greift dazu auf ihre Sicherungsdateien zu, in denen sie verschiedene Version des Gruppenkalenders findet die noch Termin enthalten, die Christoph oder Alex in der aktuellen Version gelöscht hatten, um ihre Spuren zu verwischen.

5.3.3.1 *Maßnahmen bei der Datenerhebung*

MINIMIEREN Es ist zu hinterfragen, ob es notwendig ist, dass der Gruppenkalender mitgesichert wird. Wenn er nur an zentraler Stelle vorgehalten wird und auch dort gesichert wird, ist eine Sicherung durch alle, die darauf Zugriff haben, nicht notwendig.

ANONYMISIEREN/PSEUDONYMISIEREN Ein Gruppenkalender gewährleistet gegenüber Außenstehenden eine gewisse Pseudonymität, da Termine nicht einzelnen Personen zuordnet werden können. Dominique nutzt Zusatzwissen darüber wer an welchem Projekt beteiligt ist, um ihre Vorwürfe zu untermauern. Maßnahmen zur weiteren Anonymisierung können hier nicht greifen.

5.3.3.2 *Maßnahmen bei der Zugriffssteuerung*

ZUGRIFFSVEREINBARUNGEN Ein Zugriffsschutz kann hier nur wenig Hilfestellung bieten. Dadurch, dass auf den Gruppenkalender alle drei gleichermaßen Berechtigungen besitzen, ist auch Dominiques Backup und der Zugriff auf diese legitim. Sinnvoll wäre es die Kalender der einzelnen Mitarbeiter_innen voneinander zu trennen, so würde verhindert werden, dass sie, unbeabsichtigt, mit in ein Backup geraten.

ZUGRIFF EINSCHRÄNKEN Wie auch schon bei *Die Macht der Statistik* ist hier ein Problem, dass durch die dezentrale Backup-Lösung, Dominique vollen Zugriff auch auf alte Dateien hat. Problematisch ist, dass

76 So ein Sensor könnte etwa an der Tür befestigt sein wie ihn Neustaedter and Greenberg (2003) entwerfen.

so Änderungen im Zugriffsschutz umgangen werden können. Alex und Christoph als die jeweiligen Besitzer eines Termins haben nicht die Kontrolle über die Termine, die noch in Backups verbleiben.

ZUGRIFF BEENDEN Ein Programm nach dem Prinzip von EPHEMERIZER könnte hier den Zugriff auf die alten Kalender verhindern. Die Kalenderdateien sollten lokal nur verschlüsselt gesichert und auch beim Wiederherstellen aus alten Backups würde der Schlüssel wieder abgefragt werden. Wäre dieser nicht mehr vorhanden, wäre ein Zugriff für Dominique nicht möglich.

5.3.3.3 *Maßnahmen zur Nutzungssteuerung*

Bei einer zentralen Backup-Lösung könnte Dominiques Zugriff auf mehrere Backups registriert werden. Um daraus eine Alarmierung generieren zu können, müsste allerdings vorher dazu eine Regel definiert werden, was voraussetzt, dass es als Problem erkannt wurde.

Bei Einsatz eines DHP-Systems könnte dem Kalender auch der Hinweis anhaften, dass eine Kopie nicht gewünscht ist und von der Sicherung ausgeschlossen ist.

5.3.3.4 *Nutzer_innen zentrierte Maßnahmen*

NUTZUNGSREGELN Eine zentrales Backup-System, dass von einer zweiten Person, etwa einem Administrator, verwaltet wird, würde den Zugriff auf die Daten für Dominique erschweren.

AWARENESS UND TRANSPARENCY Alex und Christoph sind sich nicht bewusst darüber, dass Dominique Sicherungskopien des Kalenders anlegt und ihre Verschleierungsversuche so wirkungslos sind. Im Sinne der informationelle Selbstbestimmung müsste den beiden aber mitgeteilt werden, wenn und das der Kalender regelmäßig kopiert wird.

5.4 ZUSAMMENFASSUNG

Auf den vorangegangen Seiten wurde die im vorherigen Kapitel vorgestellten technischen und organisatorischen Maßnahmen auf ihre Anwendbarkeit hinsichtlich der einzelnen Problem in den Szenarien überprüft. Dabei ist immer eine Kombination von Maßnahmen notwendig. Für die Einzelnen Szenarien sind die grob

DIE MACHT DER STATISTIK Die Einsicht in die Log-Dateien sollte begrenzt und mit Einmal-Pseudonymen versehen werden. Die vollen Einträge sollten nur über den Umweg einer TTP oder direkter Einwilligung des_der Autor_in möglich sein. Das Konferenzsystem sollte entweder zentralisiert werden, so dass das Abgreifen der Statusmeldungen erschwert wird, oder die Clientsoftware vereinheitlicht werden auf ein Werkzeug, dass die später genutzten Daten nicht dauerhaft erhebt. Letzteres könnte durch eine DHP-Infrastruktur sichergestellt werden.

Auf der organisatorischen Ebene kann durch eine transparenter strukturierte Gruppenorganisation eine stärkere Zusammenarbeit unter den Programmierer_innen auf Basis von agilen Methoden

die Kommunikation und das Vertrauen gefördert werden. Zusätzlich sollte David als Gruppenleiter stärker für die sozialen Aspekte der Gruppe sensibilisiert werden.

DIE NEUE Da die Gruppe bereits über Schichtdienst und konkrete Aufgabenverteilung verfügt und die Systeme weniger der Kollaboration als der Kommunikation und Koordination dienen, scheint eine stärkere Strukturierung und Formalisierung, nicht von Nachteil zu sein. Eine organisatorische Lösung, wie mit dem Ausfall von Achim umzugehen ist und eine bessere Betreuung von Daniela, um ihre Einarbeitung abzuschließen, sind notwendig. Bei der Issue-Tracking Software sollte die Gruppe ihr Nutzungsverhalten vereinheitlichen, was auch zur besseren Koordination der Gruppe beitragen würde. Lösch- und Anonymisierungsfristen können zudem die Möglichkeiten zur missbräuchlichen Nutzung der Daten einschränken.

DER SKANDAL Die Dokumentenverwaltung sollte keine unnötigen Daten erheben bzw. transparenter machen, welche Informationen einsehbar sind. Darüber hinaus sollte es für Dominique nicht möglich sein das Gespräch zwischen Alex und Christoph zu stören. Entweder indem die Einsicht in den Bildschirm verhindert wird oder durch eine Sensorik, die das Gespräch unterbricht, sobald eine dritte Person den Raum betritt.

Im Bezug auf die Sicherungskopien sollten die Sicherung, z.B. über DHP, verhindert oder eine spätere Wiederherstellung durch Verschlüsselung verhindert werden.

Eine organisatorische Lösung wäre die zentralisierung des Backups. Für Dominique sollte die Möglichkeit bestehen sich innerhalb der Universität eine Stelle zu wenden, die Anonym ihren Verdacht aufnimmt und weiterverfolgt.

6 FAZIT

Diese Arbeit beschäftigt sich mit Datenschutzproblemen bei betrieblichen Kooperationssystemen, die die informationelle Selbstbestimmung der Mitarbeiter_innen negativ beeinflussen können. Der Fokus liegt dabei auf den Problemen, die, bedingt durch dynamische Vertrauensverhältnisse in wenig strukturierten Gruppen zwischen den Nutzer_innen auftreten. Zu diesem Zweck sind in Kapitel 3 Szenarien beschrieben, wie sie in einem Workshop zum Thema erarbeitet wurden. Nach der Diskussion mit Datenschutzexpert_innen sind in Kapitel 4 Maßnahmen zusammengefasst, die verschiedene Ansätze bieten die informationelle Selbstbestimmung der Nutzer_innen zu stärken. Im anschließenden 5. Kapitel sind diese technischen und organisatorischen Maßnahmen in Bezug auf die Szenarien diskutiert, evaluiert und zu einem angepassten, praxisbezogenen Konzept verdichtet worden.

6.1 DATENSCHUTZANFORDERUNGEN

Ich konnte in dieser Arbeit nachweisen, dass die Dynamik vertrauensbasierter Zusammenarbeit unter bestimmten Umständen die informationelle Selbstbestimmung der Betroffenen einschränken. Zum Problem wird dabei, dass bisher verwendete Datenschutzmaßnahmen nicht ausreichen, um in dynamischen Gruppen angemessenen Schutz zu gewährleisten. Die an den Datenschutzprinzipien orientierten technischen und organisatorischen Maßnahmen greifen vor allem, nach der von mir vorgestellte Katgorisierung (vgl. 9), bei der Regulierung der Erhebung von Daten und den Zugriffen darauf. Um der Dynamik gerecht zu werden, sollte zusätzlich verstärkt die Regulierung und Kontrolle der Nutzung auf ihre Zweckbestimmung mit in die datenschutzfreundliche Gestaltung von Groupware einbezogen werden. Hierzu sind Maßnahmen notwendig, die den Besonderheiten der Szenarien Rechnung tragen. Sie sollten mit der Flexibilität von kleinen Gruppen, deren Verhältnis durch nicht klar definierte Rollen und das hohe Vertrauen zwischen den Mitgliedern gekennzeichnet sind, umgehen können, beziehungsweise davon unabhängig sein. Daraus resultierende Änderungen im Nutzungsverhalten müssen dazu beobachtet und reguliert werden, um die informationelle Selbstbestimmung zu stärken, ohne dabei eine zu starke Formalisierung vorzunehmen. Zuletzt sollten solche Maßnahmen insbesondere die Schnittstellen zwischen mehreren Systemen und Services berücksichtigen und die Einhaltung definierter Regeln über diese Schnittstellen hinweg gewährleisten.

Datenschutzmaßnahmen müssen dynamische Vertrauensverhältnisse berücksichtigen

Ich habe in dieser Arbeit den Stand der Forschung zu Datenschutzmaßnahmen, die Zweckbindung der Nutzung von personenbezogenen Daten, vorgestellt und Vorschläge erarbeitet, wie diese Maßnahmen in Kooperationssystemen eingesetzt werden können. Daraus lassen sich allgemeine Anforderungen formulieren, die sich einerseits an die Entwickler_innen von Groupware richten und andererseits an die Organisationen, die diese einsetzen.

6.2 ANFORDERUNGEN AN DIE SOFTWARE

Generell ist *Datenschutz durch Technik*, die technische Umsetzung von Datenschutzanforderungen, organisatorischen Regelungen meist vorzuziehen. Wie bereits angemerkt, können nicht erhobene Daten nicht missbräuchlich genutzt werden. Die Datenschutzprinzipien sollten bei der Implementierung neuer Funktionalitäten immer berücksichtigt werden. Im speziellen sind bei der Entwicklung folgende Punkte zu beachten:

1. Die *Einhaltung von Berechtigungen und Zweckbindungen* muss über Schnittstellen hinweg gewährleistet werden. Schnittstellen sind dabei nicht nur die zwischen technischen Systemen, sondern auch Schnittstellen zwischen verschiedenen Gruppenprozessen und -strukturen.

2. Um den effektiven Einsatz der Berechtigungsfunktionen sicherzustellen, müssen diese flexibel *konfigurierbar* sein. Dabei ist von hoher Bedeutung, dass für die Fälle, in denen keine generellen Konzepte und Rahmenrichtlinien vorliegen, die Nutzer_innen selbst die Kontrolle über ihre personenbezogenen Daten bekommen, ohne durch die Komplexität der Problematik überfordert zu sein.

3. *Tranzparenz* über die erhobenen Daten und insbesondere *Awareness* über die Nutzung. Nicht nur durch Arbeitgeber_innen, sondern auch durch die anderen Nutzer_innen eines Systems. Hier sind Abwägungen nötig, da auch die informationelle Selbstbestimmung der andere Nutzer_innen eine Rolle spielt.

4. Für jedes Datum sollte überlegt werden, ob es zur Nutzung erforderlich ist oder zumindest zur Verbesserung der Möglichkeiten beiträgt. Dabei sollten Standardeinstellungen möglichst eine *Minimierung* vorsehen und geeignete *Löschfristen* vorgegeben sein. Sind in einem Unternehmen weder DSB noch Betriebsrat vorhanden und findet keine separate Vorabkontrolle statt, können gut gewählte Standardeinstellungen etwas Schutz bieten.

5. *Datensicherheit* bietet zuletzt effektive Möglichkeiten, um missbräuchliche Nutzung, bei der Systemgrenzen überwunden werden, zu erschweren. Es existieren eine Reihe ausgereifter kryptografischer Verfahren, die für den Einsatz in unterschiedlichsten Umgebungen geeignet sind.[77] In Groupwaresystemen kommen sie allerdings bisher nur selten zum Einsatz.

6.3 ANFORDERUNGEN AN DIE ORGANISATION

Da die beschriebenen Probleme ihre Ursachen in der Gruppen haben, die eine Software einsetzen, muss dies auch auf organisatorischer Ebene berücksichtigt werden. Allerdings sind einem organisatorischen Regelwerk enge Grenzen gesetzt, da es letztlich die Strukturen nicht zu sehr formalisieren darf und damit spontane, vertrauensbedingte Gruppenprozesse, die zu missbräuchlicher Nutzung führen, nie ausgeschlossen werden können.

77 Insbesondere der sinnvolle Einsatz von Verfahren wie VANISH und EPHEMERIZER in Groupwaresystemen ist noch wenig betrachtet.

1. Flexible Zusammenhänge erfordern mehr Vertrauen und Kommunikation. Dies kann durch mehr Strukturierung, etwa Rollenverteilung, erreicht werden. So kann neben dem erfahrungsbasierten Vertrauen gegenüber Einzelpersonen auch das Vertrauen in die Organisation und in die Rollen selbst gestärkt werden. Allerdings erfordert das die Reflektion der bisherigen Struktur, sowie die Annerkennung, dass es zu Problemen kommen könnte. Eine Gruppe kommt allerdings meist nicht direkt zu Beginn zu diesem Punkt der Reflektion, da diesem einige andere Gruppenprozesse vorausgehen.

2. Organisationsmodelle und -normen funktionieren nur, wenn sie für alle Beteiligten gültig sind und eingehalten werden. Um dies zu gewährleisten und das Bewusstsein zu schaffen sind Schulungen und Sensibilisierungsmaßnahmen notwendig.

Um Abwägungen treffen zu können muss man die Systeme gut kennen

Die richtige Balance zwischen Datenschutz und der notwendigen Offenheit der Systeme zu finden, ist keine leichte Aufgabe und kann nicht pauschal entschieden werden. Das Spannungsfeld zwischen Theorie und Praxis ist auch in Bezug auf unternehmerischen Datenschutz nicht auflösbar. Fachkundige Datenschutzbeauftragte können diese Expertise in Unternehmen einbringen.

6.4 ANSATZ FÜR WEITERE FORSCHUNGSARBEITEN

Notwendig ist die Anerkennung der besprochenen Problematik als Feld, in dem noch Verbesserungen notwendig sind. Die häufigste Vorschläge, dem Ruf nach stärkerer Professionalisierung und Strukturierung der Arbeit mit Groupware, verkennen, dass dies bereits der zweite Schritt ist. Datenschutzmaßnahmen müssen auch mit Blick auf wenig strukturierte, flexible und vertrauensabhängige Gruppen entwickelt werden.

Insbesondere im Feld der Nutzungssteuerung (4.4) sehe ich das Potential einen großen Teil der technischen Anforderungen erfüllen zu können. Es ist zu prüfen, in wie weit sich die Definition vom Nutzungszweck, wie für DHP nötig, formalisieren lassen, damit sie automatisiert zwischen Anwendungen ausgetauscht und ihre Einhaltung überprüft werden können, ohne dabei die Flexibilität der Nutzung einzuschränken.[78] In Kombination mit kryptografische Verfahren lässt sich so eine stärkere Bindung der Nutzung an Personen und Anwendungen herstellen.

Gleichzeitig sind weitere technische und organisatorische Maßnahmen erforderlich, die die Sensibilität für die Problematik bei allen Beteiligten erhöhen und ein Bewusstsein dafür schaffen, wie mit Respekt für die informationelle Selbstbestimmung mit den Daten aus und in Groupwaresystemen umgegangen werden darf.

78 Um diese Maßnahmen in der Praxis nutzen zu können sollten Spezifikationen erarbeitet werden wie sie etwa Dürbeck et al. (2010) vorgestellt haben oder Patterns wie von Schümmer and Lukosch (2007) mit dem Fokus auf Datenschutz, wie bei Romanosky et al. (2006)

ANHANG

A.1 WORKSHOP-FRAGEBOGEN

Folgenden Fragebogen sollten die Teilnehmer_innen des Workshops zum Ende ausfüllen, um, im Stile eine *Osborn-Checklikste*, zum kreativen Überdenken angeregt zu werden.

1. Welche anderen Kontexte kannst du dir noch vorstellen?
2. Wozu könnte man die Daten (in diesen oder anderen Kontexten) noch gebrauchen?
3. Wie ließe sich der Kontext anpassen, damit die Eskalation sich nicht entwickelt?
4. Wie ließe sich die Software anpassen, damit die Eskalation sich nicht entwickelt?
5. Welchen Einfluss könnte eine/mehrere weitere Person(en) haben?
6. Wie würde sich das Szenario entwickeln, wenn bei der Eskalation *Angreifer_in* und *Opfer* die Rollen vertauscht wären?
7. Welche Software kennst du noch, die ähnliche Möglichkeiten bietet?
8. Welche anderen Elemente (z.B. aus den anderen Szenarien) ließen noch verwenden.
9. Was noch?

A.2 INTERVIEWAUSWERTUNG

Die folgenden Tabelle stellen das Ergebnis der Paraphrasierung der Interviews mit den drei Expert_innen (vgl. Tabelle 1) und die Zuordnung der Aussagen zu den vier Hauptthesen (siehe 4.1.4) dar.

In den ersten Spalte der Tabellen sind jeweils die zugeordneten Stichworte aufgeführt. In Klammern steht die Nummer des Absatzes anhand derer sich die komplette Aussage in der Transkription wieder auffinden lässt. In der zweiten Spalte sind die zusammengefassten Aussagen mit einigen Zitaten (in kursiv) dokumentiert. In der dritten Spalte ist dann die Nummer der These (vgl. 4.1.4) aufgeführt, der die Aussage zugeordnet wurde.

STICHWORT	AUSSAGE	ZU THESE
Berechtigungskonzepte (E4)	Die Einführung von Kollaborationswerkzeugen sei oft nicht ausreichend geplant, so dass die *klassische oder systematische Dokumentation und Konzeptionierung von Berechtigungen unterbleibt*. Die hänge auch damit zusammen, dass *die Systeme häufig auch nicht in der Lage sind feingranulare Berechtigungen zu vergeben.*	1
verantwortliche Stelle (E5)	Es bleibe oft ungeklärt, wer für welche Daten verantwortlich sei, gerade auch wenn firmenübergreifend gearbeitet werde. *Durch diese Unschärfe und den mangelnden Willen, das zu beantworten bevor man loslegt, entstehen diese Situationen.*	2
Berechtigungskonzept (E5)	*[..] es sind eigentlich gar keine neue Forderungen, die man mit Kollaborationssoftware stellen muss. Die Forderungen sind die gleichen. [..] Nach einem technisch schönen, gut handhabbaren feingranular einstellbarem Berechtigungssystem.*	1
Datenarten (E5)	Berechtigungen müssten auch für Verkehrsdaten, also etwa Systemprotokolle, gelten. Das werde oft übersehen, so dass dort keine Regelung existiere.	1
Schnittstellen (E6)	Viele System böten Exportmöglichkeiten und Schnittstellen für Systeme von Dritt-Herstellern. *Wenn man dann über Berechtigungen nachdenkt, muss man auch darüber nachdenken, wer ist denn berechtigt diese Schnittstellen zu benutzen*	4
Berechtigungskonzept (E6)	Bei kollaborativer Software sei oft ein Mythos der Gleichheit im Hinterkopf der Beteiligten. *Davon darf man sich nicht blenden lassen. Wenn man so [eine Software] einsetzt dann muss man genauso die ordentlichen Arbeiten einer EDV-Abteilung durchführen*	1
Verantwortung der Organisation (E7)	Die Zwecke zu definieren und Benutzungsregeln zu bestimmen, gehöre zu den Aufgaben der Organisation vor der Einführung von kollaborativen Systemen.*Ein Unternehmen, was ein Wiki erlaubt und ermöglicht, muss dann aber umso mehr vorgeben, was die Grundregeln der Benutzung sind*	2
Löschfristen (E7)	*Löschfristen. Das ist eine ganz wichtige Sachen und wird immer gerne vergessen. [..] Die Datenbasis einfach klein zu halten und an der Erforderlichkeit streng ausrichten, dass ist wichtig.*	1
Umgang mit Dynamik (E8)	*Die Rahmenstrukturen müssen so sein, dass für diese Fälle [Dynamik in der Nutzung] auch vorgesorgt ist.*	1
Berechtigungskonzept (E8)	*Das hängt aber auch von der ordentlichen Strukturierung der Betriebsprozesse ab.* Auch für Verrentnerung, Urlaub und Ausscheiden von Mitarbeiter_innen *muss das die ganz normalen Berechtigungsvergabeprozess durchlaufen*	1
Berechtigungskonzept (E9)	Die Trennung von administrativen und normalen Berechtigungen sei notwendig. Wenn Mitarbeiter_innen ausscheiden, müssten dessen Berechtigugen z.B. an den_die Abteilungsleiter_in übergeben werden	1
Berechtigungskonzept (E10)	Allgemeine Prozessvorschriften seien von einer übergeordneter Stelle zu erlassen, so dass die nicht auf jeder Ebene neu verhandelt werden müssten. *Und wenn es einen Übergabeprozess gibt, dann ist das eine allgemeine Prozessvorschrift, die immer gilt.*	1
Berechtigungskonzept (E11)	Die Prozesse (z.B. für Urlaubsvertretung) müssten so sein, dass ein Umgehen nicht einfacher sei.*Das darf einfach nicht passieren, dass das Argument lautet: Es ist zu kompliziert, wenn ich das mache.*	1

Tabelle 2: Interview 1 Auswertung (Teil 1/2)

STICHWORT	AUSSAGE	ZU THESE
Zweckbindung (E12)	Zur Formulierung vom Datenverarbeitungszweck: *Wenn der Zweck zu allgemein formuliert ist, hab' ich nie eine Einschränkung, wenn er zu detailliert beschrieben ist, hab' ich das Problem, dass ich im Grund nur eine Verarbeitung durchführen darf und eine andere nicht.*	1
Berechtigungskonzept (E14)	*Berechtigungsmanagement ist eine sehr komplexe und eine sehr komplizierte Materie. Und das sollten Leute machen, die sich damit auskennen.*	1
Verantwortung, Berechtigungskonzept (E14)	Kollaborationssoftware wälze das Berechtigungsmanagement auf die Nutzer_innen ab, in dem diese alles selbst machen dürften. Dabei sei es Aufgabe der Organisation. *Es ist aber auch unfair, weil die Nutzer sind eigentlich die Angestellten oder Mitarbeiter der.*	1
Datenweitergabe(E18)	Ein häufiger Fehler sei, dass Empfänger_innenliste bei E-Mails für alle sichtbar seien. Das sei eine *Verletzung des Prinzips, dass man nicht Leuten, die nichts voneinander wissen, nichts miteinander zu tun haben, über die anderen Auskunft gibt.* Aber *beiden [Sender_in und Empfänger_in] obliegt es dann natürlich Sorgfalt walten zu lassen* und etwa nicht ungefragt E-Mails und Adressen weiterzugeben.	3
Kennzeichnung (E18)	Der Sender müsse zum Schutz *sichtbare Maßnahmen ergreifen, um den Inhalt der Mail tatsächlich geheim zu halten oder auch als vertraulich zu kennzeichnen.*	3
Kennzeichnung (E18)	Auch in Collaboration Software brauche man Klassifizierungsmöglichkeiten für Dokumente, wie sie beim ISMS üblich seien.	4
Regelung (E19)	*Man muss einfach Regeln etablieren, die allen Beteiligten klarmachen, wie sie Mails zu kennzeichnen haben*	3
Sensibilisierung/ Schulung (E20)	Um mit Regeln nicht zu sehr zu übertreiben, sei es notwendig, Sensibilität zu schaffen auch, um das *Alles-ist-bunt-und-schön-Paradigma* auszutreiben.	3
Schnittstelle (E23)	*Wie verhindere ich, dass jemand der eine Berechtigung auf irgendwas hat, diese Berechtigung weitergibt.* Das sei ein Problem von Kollaborationssoftware, weil es oft mehrere unabhängige Systeme gäbe.	4
Data Handling Policies (E23/24)	Beispiele: Fotos in einem Onlinenetzwerk könnten mit einem roten Punkt gekennzeichnet sein, der anzeige, dass diese nicht zum Herunterladen freigegeben seien.	4
Verantwortung, Data Handling Policies (E23)	Wer Daten nutzen wolle, müsse sich informieren, ob die Einwilligung vorläge. *Jeder, der ein Telefonbuch erstellt, muss sich daran halten, was derjenige [Anschlussinhaber_in] seinem Provider gegenüber erklärt hat.*	4
Berechtigungskonept (E24)	Man verliere schnell die Kontrolle über einmal preisgegebene Daten, deswegen müsse man *natürlich möglichst früh ansetzen mit Lösungen. Weil wenn die Daten erst einmal rausdiffundiert sind, wird es immer schwieriger.*	1
Verantwortliche Stelle (E24)	Die Verantwortung liege zu oft bei den Nutzer_innen, diese könnten damit aber evtl. gar nicht umgehen. Deswegen sei es notwendig ihnen die Verantwortung so früh wie möglich abzunehmen.	1
Verantwortung/ Schnittstelle (E24)	Die Hersteller würden sich für die Schnittstellenproblematik nicht verantwortlich fühlen. Noch weniger die Nutzer_innen. Wenn eine Funktion vorhanden sei, müsse man sie doch nutzen können.	2
Schnittstelle / Verantwortung (E24)	Wenn die Berechtigungen innerhalb eines Systems funktionierten, würde für einen Missbrauch der über eine Schnittstelle übertragenen Daten keine Verantwortung übernommen.	4
Verantwortung (E26)	*Aber es gibt eine Grenze wo man einfach sagen muss, das hätte nicht passieren müssen und dürfen und da trifft die Organisation eine Mitschuld, weil sie überhaupt nicht grundlegende Regeln aufgestellt hat, die man nicht verletzten sollte.*	2

Tabelle 3: Interview 1 Auswertung (Teil 2/2)

STICHWORT	AUSSAGE	ZU THESE
Betriebliche Mitbestimmung (E2)	Alle Tools, die (so gut wie immer) zentral eingeführt würden, unterlägen der Mittsbestimmungspflicht, weil sie immer zur Verhaltens- und meist auch zur Leistungskontrolle eingesetzt werden können,*sofern ein Betriebsrat da ist, ist der dann häufig mitbestimmungspflichtig, muss beteiligt werden.*	1
Gruppenprozesse/ Leitungsfähigkeit (E2)	*Wenn es dann zu Verwerfungen innerhalb der Gruppe kommt, ist dann ja eher ein soziologisches, oder ein Problem womit sich der Vorgesetzte beschäftigen muss.*	2
Unternehmensgröße/DSB (E2)	Gerade bei kleinen Unternehmen gäbe es keine Datenschutzbeauftragten, aber oft würden viele neue Tools eingesetzt. *Gerade so junge Unternehmen, wo alle es voll cool finden, ist es selten, dass es da einen Datenschutzbeauftragten gibt und Betriebsrat noch viel weniger.*	2
Vorabkontrolle (E2)	Eine Vorabkontrolle sei notwendig vor jeder Softwareeinführung.	1
Gruppenprozesse (E2)	Es sollte erst versucht werden die Probleme ohne die zusätzlichen Daten zu lösen. *Ich sehe es immer kritisch, persönlich, und versuche das auch in meine Beratungen einfließen zu lassen, wenn es technische Mittel, technische Möglichkeiten benutzt, um dann gruppeninterne Probleme oder Verwerfungen oder sonst etwas zu regulieren.*	
Aufgabentrennung (E2)	*Ob jetzt ein Mitarbeiter so etwas hätte herausfinden können oder eigentlich die Personalabteilung das hätte herausfinden können dürfen, das ist die datenschutzrechtliche Fragestellung.*	1
Prozesse (E3)	*Den Mitarbeitern sollten solche Dinge [Kalender rekonstruieren] [...] nicht möglich [sein]. Sondern, wenn es einen begründeten Verdacht gibt,[..] dass es dann über einen geregelten Weg, die Personalabteilung* geregelt wird.	1
Prozesse (E3)	*Optimal ist es wie gesagt, wenn es geordneten Wege und Regeln gibt.*	1
Berechtigungskonzept Administration (E4)	Wesentliche Änderungen sollten nur im Vier-Augen-Prinzip gemacht werden dürfen. Die IT-Abteilung in Kombination entweder mit dem Betriebsrat oder mit der Personalabteilung	1
Vorabkontrolle/ Prozesse (E5)	Er sei der Meinung, *dass [in den Szenarien] bei der Einführung eines Systems Fehler gemacht worden sind.* Da vor der Einführung geklärt werden müsste, was wofür genutzt würde.	1
Weitergabe (E5)	Er kenne Beispiele bei denen, *ein Abteilungsleiter den kurzen Dienstweg in Anspruch nimmt und sich direkt an die IT wendet und evtl. auch Antworten kriegt, die er eigentlich nicht kriegen sollte, selbst wenn es ein begründeter Verdacht ist.*	1
Berechtigungskonzept (E5)	*Der Endnutzer, wenn er es nicht für seine eigene Arbeit braucht, [..] sollte nur seine eigenen Einträge [in Logdateien] sehen können und nicht die aller anderen.*	1
Papierexport (E5)	Dass sich ein User Einträge aus Logs *natürlich jedesmal aufschreib[t], in einer Excel Tabelle oder auf Papier, das lässt sich kaum verhindern.*	4
Leitungsfähigkeit/ Gruppenprozesse (E5)	*Solche Sachen [wie in den Szenarien] treten weniger auf, wenn Führungsqualität da ist oder Leitungsqualität.* Oft solle die durch technische Überwachung ersetzt werden, das sei aber keine gute Option.	2
Zweckbindung/ org. Regeln (E6)	*Das geht dann tatsächlich nur über organisatorische Regelungen, zu den Zwecken dürfen sie verwendet werden, alle anderen Verwendungen sind unzulässig. Alle arbeitsrechtlichen Schritte, die auf Grund unzulässig verarbeiteter Daten getätigt wurden, sind per se nichtig.*	1
Gruppenprozesse (E6)	*Wenn sich rausstellt, dass vorher in der Gruppe gegenseitig Datensammlungen angelegt wurden, dann müsste man da wahrscheinlich auch schon mit einem Mediator in die Gruppe gehen.*	

Tabelle 4: Interview 2 Auswertung (Teil 1/2)

STICHWORT	AUSSAGE	ZU THESE
DSB/Betriebsrat (E6)	*Die Erfahrung ist leider, dass man als Datenschutzbeauftragter vielleicht vor der Einführung beteiligt wird, aber nach der Beschaffung.*	2
Privacy-By-Design(E7/E8)	Technische Regelungen seien organisatorischen vorzuziehen. *Nicht Datenschutz oder Technik, sondern Datenschutz durch Technik*	1
Schulung (E8)	Mit Schulungen sei es möglich auch dort, *wo die Leute kein hohes technisches Verständnis haben müssen, [..] solche Sachen wie Verschlüsselung und ähnliches zu installieren*	3
Sensibilisierung/DSB (E9)	*Das ist Sensibilisierung. Ein wichtiger Aspekt, der zu den Aufgaben des Datenschutzbeauftragte gehört, zu sensibilisieren. Den Leuten klar zu machen, wenn ihr so etwas ausdruckt, was ja manchmal für die Arbeit sinnvoll ist, ob es nun erforderlich ist mag dahingestellt sein* im Anschluss in den Aktenvernichter gehöre.	3
Vorbildfunktion (E9/10)	Es komme vor, *dass die Mitarbeiter zwar eine gute Sensibilisierung haben [..], aber die Unternehmensleitung sich dem Thema nicht entsprechend stellt.*	2
Berechtigungskonzept (E11)	*Erst wenn das Kind in den Brunnen gefallen ist, macht man sich dann Gedanken.*	1
Vorabkontrolle/ Komplexität (E12)	Bei komplexen Systemen sei eine vollständige Übersicht über alle möglichen Komponenten manchmal nicht möglich. Auch für den_die Arbeitgeber_in, *weil er vielleicht auch nicht weiß, dass es da noch andere Möglichkeiten gibt.*	1
DHP (E13)	DHP seien eine schöne Idee, funktionierten aber nur, wenn sichergestellt werden könne, dass die Informationen nicht entfernt werden.	4
Zweckbindung (E13)	*Wenn die Daten von einem System ins andere System wandern, dass klar ist, zu welchen Zwecken waren sie da, dass man dann immer noch prüfen kann: jetzt haben wir einen neuen Zweck.*	4
DSB (E14)	Er sage auch manchmal, wenn Dinge eigentlich nicht datenschutzkonform seien, aber die Firma das Risiko auf sich nehmen könne. *Nur ja/nein, schwarz/weiß funktioniert da nicht.* Er sehe sich da als *proaktiver* DSB und mache z.B. darauf aufmerksam, dass man bei der ersten Erhebung schon eine Einwilligung für irgendwas einholen könnte, was man zu Beginn vielleicht noch gar nicht geplant habe.	
Rahmenregelung (E16/E17)	*Sinnig ist es [..], dass es eine Rahmenregelung gibt, sei es mit oder ohne Betriebsrat, und das man dann für die einzelnen Werkzeuge nur noch [..] gucken muss, wie wird diese zentrale Regelung oder diese Rahmenvereinbarung, wie wird die auf das abgebildet.*	1
Unternehmensgröße/DSB (E16)	*Ist in mittelgroßen und größeren Betrieben gängige Praxis, mit einem Rahmen zu arbeiten und Detailregelungen. Wenn ich ein kleines Unternehmen habe [..], da wird das dann ein bisschen schwieriger. Gerade [bei] kleinen und kreativen und schnell agierenden Unternehmen, ist es natürlich schwierig.*	2
Gruppenprozesse (E17)	In Streifällen, *da sag ich dann als Datenschutzbeauftragter, damit hab ich eigentlich nichts zu tun, [..] da braucht ihr einen Mediator und nicht mich.*	
Dynamische Nutzungsentwicklung (E18)	*Eigenentwicklung in der Nutzung, das entwickelt sich fort. Man hat eine konkrete Idee, wie man es nutzen will und dann stellt man fest, das und das kann man auch noch damit machen und dann machen wir das.*	
Audits (E18/21)	*[Es] gibt Audit-Termine und im Rahmen der Audits würde dann auch immer mal wieder ein Wiki oder ein anderes solches Tool Thema sein und dann würde ich sagen, hier logge dich mal mit deinem Admin-Account ein und dann gucken wir mal uns ein paar Sachen an[..].*	4

Tabelle 5: Interview 2 Auswertung (Teil 2/2)

STICHWORT	AUSSAGE	ZU THESE
Randbereich des Datenschutz (E4)	Die Szenarien würden sich im Randbereich des Datenschutz bewegen, *[weil] es ja um die Kommunikation zwischen Menschen geht, und die beobachte ich professionell gar nicht. Das ist überhaupt nicht mein Fokus. Randbereich er ist aber deshalb, weil diese Kommunikation in Organisationen stattfindet.*	
Mitarbeiterdatenschutz (E4)	Da es sich um Kommunikation in Unternehmen handele, vermittelt durch IT, sei es aber doch Thema des Mitarbeiterdatenschutz. Aber: *Der Fokus von Datenschutz ist eigentlich immer Organisation - Klientel und nicht Menschen untereinander.*	
Randbereich des Datenschutz (E4)	Das beschriebene Problem gehöre in die Kategorie *Interaktionsysteme* und *da hat Datenschutz nicht viele Chancen.*	
Awareness (E5)	Damit Organisationen *leben* können, bräuchten sie einen gewissen Grad an nicht formalisierter Kommunikation. *Ich glaube, dass sie da mit dem klassischen Datenschutzhandwerk oder -methoden wahrscheinlich nicht sehr weit kommen. Da bleibt möglicherweise nur Awareness übrig.*	2
Zweckänderung (I/E 6)	Jede Zweckänderung müsse immer protokolliert werden.	1
Prozesse (E8)	Zugriff, Nutzung und Zweck eines Systems sollten vor Einsatz definiert sein.	1
Formale Kommunikation (E8)	*So ähnlich wie in einer Verwaltung, wo die Akten-Kommunikation das führende System ist, es gibt keine andere Kommunikation, die von Relevanz ist für eine Verwaltung, außer die, die in den Akten stattfindet. Und da kann man für Datenschutz sorgen.*	1
Löschung (E9)	E-Mails könnten nach dem Lesen gelöscht werden, um unerlaubte Weiterleitung zu verhindern.	1
Weitergabe (E8)	Eine Technik könnte überwachen (aufgesetzt auf E-Mail), dass diese nicht weitergeleitet wird.	4
Informationelle Selbstbestimmung (E10/12)	Bestimmte Informationen über einen selbst lägen ausschließlich in der Hand von anderen, die sich dabei wiederum auf ihre Informationelle Selbstbestimmung berufen könnten. *Dass heißt informationelle Selbstbestimmung, würde ich nie für mich beanspruchen, richtig, so im philosophischen Sinne, weil ich nicht genau weiß was damit gemeint ist.*	
Verantwortung (E14)	Die Organisation müsse dafür sorgen, dass alle nur Zugriff auf das haben, was sie etwas angehe.	1
Randbereich des Datenschutz (E14)	*Da wo Sozialverhältnisse über positives Recht reguliert sind auf Ethik zu verfallen, ist immer schon ein Zeichen von Schwäche sozusagen, oder auf Awareness der Menschen zu gehen oder einen Codex zu bauen, das tut man einfach nicht.*	
Informationsmonopol/ Datenntuzung (E15)	Um etwas bergleichbares wie das Gewaltmonopol des Staates auf Informationen umsetzen zu können (um z.B. Rufmord zu verhindern), wäre erheblicher Aufwand nötig.	
Berechtigungskonzept (E15)	*Beispiel Protokollierungsdaten: Die müssen immer verschlüsselt abgelegt werden. Es [darf] keinen anderen Modus als das verschlüsselte Ablegen von Protokollen [geben].*	1

Tabelle 6: Interview 3 Auswertung (Teil 1/2)

STICHWORT	AUSSAGE	ZU THESE
Nichtverkettbarkeit (E16)	Datenschutzpolicies böten Möglichkeiten, um *ganz spezifische Logdateien für ganz spezifische Services [zur Verfügung zu stellen]. Und es kommen nur Berechtige an diese Logdateien überhaupt ran.*	1
Berechtigungskonzept (E18)	Einen allwissenden Admin dürfe es nicht mehr geben. *Es ist im Grunde eine pathologische Organisationsstruktur, wenn es diesen Root noch gibt, und den gibt es zunehmend weniger.*	1
Gruppenprozesse (E20/21)	Am Anfang einer Organisation könnten flache Hierarchien und Offenheit noch sinnvoll sein, aber mit steigender Professionalisierung müsse auch die Formalisierung steigen. *Deswegen machen auch zwei Liebende oftmals einen Heiratsvertrag, weil es einfach sehr wahrscheinlich ist, dass auch ihre Liebe nicht ewig hält. Es ist einfach extrem unwahrscheinlich, dass es ewig hält.*	2
Unternehmensgröße (E20/21)	Mit der Größe steige die Formalisierung. *Wir haben gute Revisionsmechanismen in den weltweit agierenden Banken, die haben gute Revisionen. Das haben kleine Unternehmen und auch kleinere Verwaltungen in dem Sinne so nicht.*	1
Schnittstellen (IE21-23)	Es sei nicht nur schwierig die Zweckbindung zu gewährleisten, wenn Daten zwischen technischen Systemen ausgetauscht würden, sondern auch, wenn das Unternehmen in eine neue Organisationsform wechsele, weil es etwa wachse. *Und wenn man dann Informationen aus dem alten hat, um daraus was für die neue Struktur zu machen, das lässt sich, glaube ich, absolut nicht verhindern.*	4
Rechtskonformität (E24)	Rechtskonformität herzustellen sei das Ziel des Datenschutzes.	
Policies (I/E25-28)	Nutzungspolicies sollten im besten Fall aus Gesetzen direkt formalisiert werden. Zudem solle es eine zentralen Server, möglichst ebenfalls vom Gesetzgeber, geben der die Policies überwache. *Das sind Frameworks, beispielsweise welche Anforderungen an das Sicherheitsniveau eines Zertifikats zu stellen sind. Oder was für Signaturen man braucht: Reichen fortgeschrittene oder müssen es qualifizierte sein. Dann gibt es ein ganzes Set an hierarchischen Abstufbarkeiten, und Erforderlichkeiten für bestimmte Transaktionen in der Kommunikation.*	4
Randbereich des Datenschutz/Systeme/Schnittstelle (E29)	*Datenschutz guckt, ob die Differenz zwischen Funktions- und Organisationssystem funktioniert. Datenschutz guckt nicht, bislang nicht, aber vielleicht bringen sie mich jetzt auf die Idee, ob man das erweitern kann, auf Organisationssystem und Interaktionssystem, ob man auch da Datenschutz machen kann. Die Unterscheidung: Interaktionssysteme, Organisationssysteme und Funktionssysteme. Datenschutz guckt zwischen Organisations- und Funktionssystemen. Guckt nicht auf die Interaktionssysteme. Sie machen den Blick auf die Interaktionssysteme.*	

Tabelle 7: Interview3 Auswertung (Teil 2/2)

Mark S. Ackerman and Lorrie Cranor. Privacy critics: UI components to safeguard users' privacy. In *CHI '99 extended abstracts on Human factors in computing systems*, pages 258–259, Pittsburgh, Pennsylvania, 1999. ACM. ISBN 1-58113-158-5. doi: 10.1145/632716.632875. URL http://portal.acm.org/citation.cfm?id=632875. (Zitiert auf Seite 62.)

C. A. Ardagna, S De Capitani di Vimercati, and P Samarati. Enhancing User Privacy Through Data Handling Policies. In *Data and Applications Security XX*, volume 4127/2006 of *Lecture Notes in Computer Science*, pages 224–236. Springer Berlin / Heidelberg, July 2006. ISBN 978-3-540-36796-3. URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.96.932&rep=rep1&type=pdf. (Zitiert auf den Seiten 57 und 58.)

Artikel-29-Datenschutzgruppe. WP55 - Arbeitsdokument zur Überwachung der elektronischen ommunikation von Beschäftigten, May 2002. URL http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_de.pdf. (Zitiert auf den Seiten 6, 10 und 62.)

Claudia Maria Bayerl. *30 Minuten für Kreativitätstechniken*. GABAL Verlag GmbH, April 2005. ISBN 9783897495128. (Zitiert auf Seite 22.)

Kent Beck and Cynthia Andres. *Extreme Programming Explained: Embrace Change*. Addison-Wesley Professional, 2001. ISBN 0321278658. (Zitiert auf den Seiten 67 und 69.)

R. Bhatti, E. Bertino, and A. Ghafoor. A trust-based context-aware access control model for web-services. *Distributed and Parallel Databases*, 18(1):83–105, 2005. URL http://cobweb.ecn.purdue.edu/~iisrl/papers/ICWS_2004.pdf. (Zitiert auf Seite 49.)

Johann Bizer. Sieben Goldene Regeln des Datenschutzes. *Datenschutz und Datensicherheit - DuD*, 31(5):350–356, May 2007. doi: 10.1007/s11623-007-0133-x. URL http://johann-bizer.de/index.php?option=com_content&task=view&id=14&Itemid=32. (Zitiert auf Seite 6.)

Tobias Blasius. NRW-CDU startet Suche nach „Maulwurf" in ihrer Zentrale. *DerWesten*, March 2010. URL http://www.derwesten.de/nachrichten/NRW-CDU-startet-Suche-nach-Maulwurf-in-ihrer-Zentrale-id2667812.html. (Zitiert auf Seite 2.)

Nikita Borisov, Ian Goldberg, and Eric Brewer. Off-the-record communication, or, why not to use PGP. In *Proceedings of the 2004 ACM workshop on Privacy in the electronic society*, pages 77–84, Washington DC, USA, 2004. ACM. ISBN 1-58113-968-3. doi: 10.1145/1029179.1029200. URL http://portal.acm.org/citation.cfm?id=1029200. (Zitiert auf Seite 52.)

Brian Bowen, Malek Ben Salem, Shlomo Hershkop, Angelos Keromytis, and Salvatore Stolfo. Designing Host and Network Sensors to

Mitigate the Insider Threat. *IEEE Security and Privacy*, 7:22–29, 2009. ISSN 1540-7993. doi: http://doi.ieeecomputersociety.org/10.1109/MSP.2009.109. (Zitiert auf Seite 59.)

Jochen Brandt. Computerüberwachung und Persönlichkeitsrechte. *Computer und Arbeit*, 1/2008(1/2008):12–14, January 2008. (Zitiert auf Seite 17.)

A.J. Bernheim Brush, Brian R. Meyers, James Scott, and Gina Venolia. Exploring awareness needs and information display preferences between coworkers. In *Proceedings of the 27th international conference on Human factors in computing systems*, pages 2091–2094, Boston, MA, USA, 2009. ACM. ISBN 978-1-60558-246-7. doi: 10.1145/1518701.1519018. URL http://portal.acm.org/citation.cfm?doid=1518701.1519018. (Zitiert auf den Seiten 2 und 6.)

BverfG. Urteil vom 15. Dezember 1983, 1983. URL http://www.servat.unibe.ch/dfr/bv065001.html. (Zitiert auf Seite 5.)

Jan Camenish, Pierangela Samarati, Simone Fischer-Hübner, and Maren Raguse. First report on mechanisms. URL http://www.primelife.eu/images/stories/deliverables/d2.1.1-first_report_on_mechanisms-public.pdf. (Zitiert auf den Seiten 13, 46, 61 und 63.)

D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10): 1030–1044, 1985. URL https://www.cosic.esat.kuleuven.be/apes/papers/p1030-chaum.pdf.gz. (Zitiert auf den Seiten 11 und 54.)

D. Cosmar. Erarbeitung eines Konzeptes zur Computerunterst\ützung gruppendynamischer Prozesse in verteilt arbeitenden Gruppen. URL http://www.cosmar.de/wordpress/wp-content/belegarbeit_dirk_cosmar-erarbeitung_eines_konzeptes_zur_computerunterstuetzung_gruppendynamischer_prozesse_in_verteilt_arbeitenden_gruppen.pdf. (Zitiert auf Seite 13.)

Wolfgang Däubler. *Gläserne Belegschaften? Datenschutz in Betrieb und Dienststelle*. Bund-Verlag, Frankfurt am Main, vierte edition, 2002. ISBN 3766333879. (Zitiert auf den Seiten 5, 8, 10 und 17.)

T. H Davenport. *Thinking for a Living*. Harvard Business School Press Boston, 2005. (Zitiert auf Seite 1.)

Prasun Dewan and HongHai Shen. Flexible meta access-control for collaborative applications. In *Proceedings of the 1998 ACM conference on Computer supported cooperative work*, pages 247–256, Seattle, Washington, United States, 1998. ACM. ISBN 1-58113-009-0. doi: 10.1145/289444.289499. URL http://portal.acm.org/citation.cfm?id=289444.289499&type=series. (Zitiert auf Seite 48.)

E. U. Directive. 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data. *Official Journal of the EC*, 23, 1995. (Zitiert auf Seite 6.)

Niko Dirner. EDV-Mann in der Kritik. *Südwest Presse Online*, February 2010. URL http://www.swp.de/ulm/lokales/kreis_neu_ulm/art4333,353046. (Zitiert auf Seite 2.)

Stefan Dürbeck, Jan Kolter, Günther Pernul, and Rolf Schillinger. Eine verteilte Autorisierungsinfrastruktur unter Berücksichtigung von Datenschutzaspekten. *Informatik-Spektrum*, 33(03/2010):0, 2010. ISSN 0170-6012 (Print) 1432-122X (Online). doi: 10.1007/s00287-009-0411-0. URL http://dx.doi.org/10.1007/s00287-009-0411-0. (Zitiert auf den Seiten 58 und 82.)

Dag Elgesem. The structure of rights in Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and the free movement of such data. *Ethics and Information Technology*, 1(4):283–293, December 1999. doi: 10.1023/A:1010076422893. URL http://dx.doi.org/10.1023/A:1010076422893. (Zitiert auf Seite 6.)

EU-Parlament. Richtlinie 95/46/EG. *Amtsblatt*, (L 281):31–50, October 1995. URL http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html. Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. (Zitiert auf Seite 6.)

Luciano Floridi. The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, pages 185–200, May 2006. ISSN 1388-1957 (Print) 1572-8439 (Online). doi: 10.1007/s10676-006-0001-7. URL http://www.springerlink.com/content/u72834q5105m257n/. (Zitiert auf Seite 9.)

Roxana Geambasu, Tadayoshi Kohno, Amit Levy, and Henry M. Levy. Vanish: Increasing Data Privacy with Self-Destructing Data. In *Proc. of the 18th USENIX Security Symposium*, 2009. URL http://vanish.cs.washington.edu/pubs/usenixsec09-geambasu.txt. (Zitiert auf Seite 56.)

Erving Goffman. *Das Individuum im öffentlichen Austausch - Mikrostudien zur öffentlichen Ordnung*. Suhrkamp, Frankfurt am Main, 1 edition, 1974. ISBN 3-518-06386-3. (Zitiert auf Seite 4.)

K. Gr\äslund and H. Krcmar. Anonymit\ät. *CSCW Kompendium-Lehr-und Handbuch f\ür das computerunterst\ützte kooperative Arbeiten. Heidelberg: Springer*, 2001. (Zitiert auf Seite 45.)

M. Hansen. Study on protocols with respect to identity and. 2008. URL http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.8_Study_on_protocols_with_respect_to_identity_and_identification.pdf. (Zitiert auf den Seiten 48, 54 und 58.)

T. Herrmann. Workflow management systems: Ensuring organizational flexibility by possibilities of adaptation and negotiation. In *Proceedings of conference on Organizational computing systems*, page 94, 1995. URL http://www.sociotech-lit.de/Herr95-WMS.pdf. (Zitiert auf Seite 50.)

T. Herrmann. Kommunikation und Kooperation. *CSCW-Kompendium. Lehr-und Handbuch zum computerunterst\ützten kooperativen Arbeiten (S. 15-25). Berlin et al.: Springer*, 2001. (Zitiert auf Seite 11.)

T. Herrmann and H. Weber. Datenschutzkonzepte bei der Einf\ührung von Workflow-Management-Systemen. In A. W. Scheer and

T. Herrmann, editors, *Verbesserung von Geschäftsprozessen mit flexiblen Workflow-Management-Systemen*, volume 4, page 3–42. 1999. (Zitiert auf Seite 47.)

Giovanni Iachello and Jason Hong. End-user privacy in human-computer interaction. *Found. Trends Hum.-Comput. Interact.*, 1(1):1–137, 2007. ISSN 1551-3955. URL http://portal.acm.org/citation.cfm?id=1324103.1324104. (Zitiert auf den Seiten 12, 44, 60 und 62.)

Ulrich Klotz. Open-Source als Leitbild für die Arbeit 2.0. *FIfF-Kommunikation*, 26(3/2009):52–57, September 2009. ISSN 0938-3476. (Zitiert auf Seite 1.)

R. M Kramer. Trust and distrust in organizations: Emerging perspectives, enduring questions. *Annual review of psychology*, 50(1):569–598, 1999. (Zitiert auf den Seiten 11, 12 und 13.)

Siegfried Lamnek. *Qualitative Sozialforschung*. BeltzPVU, February 2005. ISBN 9783621275446. (Zitiert auf Seite 37.)

Marc Langheinrich. Privacy by Design — Principles of Privacy-Aware Ubiquitous Systems. In *Ubicomp 2001: Ubiquitous Computing*, volume 2201/2001 of *Lecture Notes In Computer Science*, pages 273–291. Springer Berlin / Heidelberg, 2001. URL http://dx.doi.org/10.1007/3-540-45427-6_23. (Zitiert auf Seite 49.)

R. Lewick and B. B Bunker. Developing and maintaining trust in work relationships. In *Trust in organizations: Frontiers of theory and research*, volume 1 of *Trust in organizations: Frontiers of theory and research*, page 114. 1995. (Zitiert auf Seite 14.)

M. Lindgren and H. Bandhold. *Scenario planning: the link between future and strategy*. Palgrave Macmillan, 2003. (Zitiert auf Seite 16.)

A. Machanavajjhala, J. Gehrke, D. Kifer, and M. Venkitasubramaniam. L-Diversity: privacy beyond k-Anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD)*, 1(1), 2007. (Zitiert auf Seite 46.)

M. A Maloof and G. D Stephens. ELICIT: A System for Detecting Insiders Who Violate Need-to-know. *Lecture Notes in Computer Science*, 4637:146, 2007. URL http://www.cs.georgetown.edu/~maloof/pubs/maloof-raid07.pdf. (Zitiert auf den Seiten 58 und 59.)

Joe Meier. Überwachung am PC-Arbeitsplatz - Nutzen und Gefahren. *Computer und Arbeit*, Jahrgan 17(1/2008):7–11, January 2008. (Zitiert auf Seite 17.)

M. Meuser and U. Nagel. ExpertInneninterviews–vielfach erprobt, wenig bedacht. *Qualitativ-empirische Sozialforschung. Konzepte, Methoden, Analysen. Opladen: Westdeutscher Verlag*, page 441–471, 1991. (Zitiert auf Seite 38.)

Carman Neustaedter and Saul Greenberg. The Design of a Context-Aware Home Media Space for Balancing Privacy and Awareness. In *UbiComp 2003: Ubiquitous Computing*, pages 297–314. 2003. URL http://www.springerlink.com/content/RE70Q1D4E7CDX46Y. (Zitiert auf den Seiten 64 und 77.)

C. Paar and J. Pelzl. *Understanding Cryptography: A Textbook for Students and Practitioners*. Springer-Verlag New York Inc, 2010. (Zitiert auf Seite 51.)

Martin Pekárek and Stefanie Pötzsch. Requirements and concepts for privacy-enhancing access control in social networks and collaborative workspaces, shorttitle = H1.2.5, July 2009. URL http://www.primelife.eu/results/documents. (Zitiert auf den Seiten 48, 50, 58 und 61.)

Radia Perlman. The ephemerizer: making data disappear. Technical report, Sun Microsystems, Inc., 2005. URL http://portal.acm.org/citation.cfm?id=1698176. (Zitiert auf Seite 56.)

L. Perusco and K. Michael. Control, trust, privacy, and security: evaluating location-based services. *IEEE Technology and Society Magazine*, 26 (1):4–16, 2007. (Zitiert auf Seite 16.)

Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management, December 2009. URL http://dud.inf.tu-dresden.de/Anon_Terminology.shtml. v0.32. (Zitiert auf den Seiten 45 und 46.)

Michael Prilla and Carsten Ritterskamp. The Interplay of Web 2.0 and Collaboration Support Systems: Leveraging Synergies. In *From CSCW to Web 2.0: European Developments in Collaborative Design*, number Part 3 in Computer Supported Cooperative Work, pages 193–218. Springer,, London ;;New York :, 2010. ISBN 9781848829657. URL http://www.sociotech-lit.de/PrRi10-IoW.pdf. (Zitiert auf Seite 8.)

W. Prinz. Awareness. *CSCW-Kompendium–Lehr-und Handbuch zur computerunterst\ützten Gruppenarbeit, Springer, Heidelberg et al*, 2001. (Zitiert auf Seite 60.)

A. Richter and M. Koch. *Social Software: Status Quo und Zukunft*. Fak. für Informatik, Univ. der Bundeswehr München, 2007. URL http://www.kooperationssysteme.de/docs/pubs/RichterKoch2007-bericht-socialsoftware.pdf. (Zitiert auf Seite 8.)

Sasha Romanosky, Alessandro Acquisti, Jason Hong, Lorrie Faith Cranor, and Batya Friedman. Privacy patterns for online interactions. In *Proceedings of the 2006 conference on Pattern languages of programs*, pages 1–9, Portland, Oregon, 2006. ACM. ISBN 978-1-60558-372-3. doi: 10.1145/1415472.1415486. URL http://portal.acm.org/citation.cfm?id=1415486. (Zitiert auf Seite 82.)

Beate Rössler. *Der Wert des Privaten*. Suhrkamp, Frankfurt, July 2001. ISBN 978-3-518-29130-6. URL http://www.suhrkamp.de/buecher/der_wert_des_privaten-beate_roessler_29130.html. (Zitiert auf Seite 4.)

Mary Beth Rosson and John M. Carroll. Scenario-Based Design. In J. Jacko and A. Sears, editors, *The Human-Computer Interaction Handbook*, pages 1032–1050. Lawrence Erlbaum Associates, 2002. URL http://ocw.tudelft.nl/fileadmin/ocw/courses/IntelligentUserExperienceEngineering/res00110/2_RossonCarrollSBDforHandbook2002.pdf. (Zitiert auf Seite 16.)

Martin Rost and Andreas Speck. Modellgestützte Validierung von WebService-Ketten. *Datenschutz und Datensicherheit*, 33 (6):359–363, 2009. doi: 10.1007/s11623-009-0073-8. URL http://www.springerlink.com/content/v05750286288012k/?p=0bf14e8c28f347a6b7e5864a8bd08a48&pi=0. (Zitiert auf Seite 58.)

Hans-Hermann Schild and Marie-Theres Tinnefeld. Entwicklungen im Arbeitnehmerdatenschutz. *Datenschutz und Datensicherheit - DuD*, 33(8):469–474, 2009. doi: 10.1007/s11623-009-0120-5. URL http://dx.doi.org/10.1007/s11623-009-0120-5. (Zitiert auf Seite 16.)

Till Schümmer and Stephan Lukosch. *Patterns for computer-mediated interaction*. John Wiley and Sons, 2007. ISBN 0470025611, 9780470025611. (Zitiert auf den Seiten 1, 9, 13, 17, 19, 60 und 82.)

Ken Schwaber. *Agile software development with Scrum*. Prentice Hall, Upper Saddle River NJ, 2002. ISBN 9780130676344. (Zitiert auf Seite 69.)

Matthias Seifert and Peter Pawlowsky. Innerbetriebliches Vertrauen als Verbreitungsgrenze atypischer Beschäftigungsformen. *Mitteilungen aus der Arbeitsmarkt- und Berufsforschung*, 31(3):599–311, 1998. URL http://213.241.152.197/mittab/1998/1998_3_MittAB_Seifert_Pawlowsky.pdf. (Zitiert auf den Seiten 11 und 16.)

HongHai Shen and Prasun Dewan. Access control for collaborative environments. In *Proceedings of the 1992 ACM conference on Computer-supported cooperative work*, pages 51–58, Toronto, Ontario, Canada, 1992. ACM. ISBN 0-89791-542-9. doi: 10.1145/143457.143461. URL http://portal.acm.org/citation.cfm?id=143461. (Zitiert auf Seite 50.)

Andrea Stölzle. Baiker: „Datenklau ist eine Straftat“. *Augsburger Allgemeine*, February 2010. URL http://www.augsburger-allgemeine.de/Home/Lokales/Neu-Ulm/Lokalnachrichten/Artikel,-Baiker-Datenklau-ist-eine-Straftat-_arid,2065932_regid,2_puid,2_pageid,4503.html. (Zitiert auf Seite 2.)

L. Sweeney. k-anonymity: a model for protecting privacy. *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, 10(5): 557–570, 2002. (Zitiert auf Seite 46.)

Q. Tang. From Ephemerizer to Timed-Ephemerizer: Achieve Assured Lifecycle Enforcement for Sensitive Data. Technical Report TR-CTIT-10-01, Centre for Telematics and Information Technology, University of Twente, Enschede, January 2010. URL http://eprints.eemcs.utwente.nl/17095/. (Zitiert auf Seite 56.)

Peter Tarasewich and Christopher Campbell. What Are You Looking At? In *Proceedings of SOUPS 2005*, Pittsburgh, PA, USA, 2005. ACM. URL about:blank. (Zitiert auf Seite 64.)

S. Teufel, C. Sauter, T. M\ühlherr, and K. Bauknecht. *Computerunterst\ützung f\ür die Gruppenarbeit*. Addison-Wesley, 1995. (Zitiert auf Seite 9.)

William Tolone, Gail-Joon Ahn, Tanusree Pai, and Seng-Phil Hong. Access control in collaborative systems. *ACM Comput. Surv.*, 37(1): 29–41, 2005. doi: 10.1145/1057977.1057979. URL http://portal.acm.

org/citation.cfm?id=1057977.1057979. (Zitiert auf den Seiten 48, 49 und 50.)

Bruce W. Tuckman and Mary Ann C. Jensen. Stages of Small-Group Development Revisited. *Group Organization Management*, 2(4):419–427, December 1977. doi: 10.1177/105960117700200404. URL http://gom.sagepub.com/cgi/content/abstract/2/4/419. (Zitiert auf den Seiten 13 und 18.)

Alan Westin. *Privacy and Freedom*. New Jork Atheneum, New York, 1967. (Zitiert auf Seite 4.)

Johannes Wiele. Mitarbeiterdatenschutz versus Sicherheit: Das Recht hilft nur mit Diplomatie. *Datenschutz und Datensicherheit*, Jahrgang 33(11/2009):685–689, 2009. (Zitiert auf Seite 16.)

David Wright, Serge Gutwirth, Michael Friedewald, Elena Vildjiounaite, and Yves Punie, editors. *Safeguards in a World of Ambient Intelligence*. Number 1 in The International Library of Ethics, Law and Technology. Springer, Springer Netherlands, 2008. ISBN 978-1-4020-6661-0. URL http://www.springerlink.de/content/v8k23l/?p=11d1416c0f964b7a90ce8301d7659bb2&pi=0&hl=u. (Zitiert auf den Seiten 16, 17, 44 und 58.)

G. Zhang and M. Parashar. Context-aware dynamic access control for pervasive applications. In *Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference*, page 21–30, 2004. URL http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.6.1258&rep=rep1&type=pdf. (Zitiert auf Seite 49.)

Max Ziegler. An die Kette - Werkzeuge gegen Datenklau. *c't - magazin für computer technik*, 27(3/2010):138–141, January 2010. URL http://www.heise.de/ct/inhalt/2010/03/138/. (Zitiert auf Seite 60.)

DOWNLOAD Die Bibliographie kann hier im BibTex Format heruntergeladen werden:
http://martin.degeling.de/masterarbeit/literatur.bib

EIGENSTÄNDIGKEITSERKLÄRUNG

Ich erkläre, dass das Thema dieser Arbeit nicht identisch ist mit dem Thema einer von mir bereits für ein anderes Examen eingereichten Arbeit. Ich erkläre weiterhin, dass ich die Arbeit nicht bereits an einer anderen Hochschule zur Erlangung eines akademischen Grades eingereicht habe.

Ich versichere, dass ich die Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen benutzt habe. Die Stellen der Arbeit, die anderen Werken dem Wortlaut oder dem Sinn nach entnommen sind, habe ich unter Angabe der Quellen der Entlehnung kenntlich gemacht. Dies gilt sinngemäß auch für Zeichnungen, Skizzen und bildliche Darstellungen und dergleichen.

Bochum, Juni 2010

Martin Degeling