Benutzbare Sicherheit für wirksame Berechtigungen in Organisationen*

Steffen Bartsch

CASED, TU Darmstadt
steffen.bartsch@cased.de

Abstract: Berechtigungen in Informationssystemen können die tägliche Arbeit behindern. Um ungewollte Behinderungen und daraus resultierende Sicherheitsprobleme zu minimieren, betrachtet diese Dissertation nicht nur die technischen Aspekte dieser Probleme. Stattdessen wurde umfassend aus verschiedenen Perspektiven analysiert, welche Ursachen und Konsequenzen diese Probleme in Organisationen haben. Es wurden dabei verschiedenste Probleme, von der unerlaubten Weitergabe von Passwörtern bis zur Unbenutzbarkeit der Verwaltungswerkzeuge, identifiziert. Um diese Probleme fundamental zu beheben, wurden acht Prinzipien für benutzbare Berechtigungen vorgeschlagen und anhand von fünf konkreten Artefakten, wie etwa flexiblen Berechtigungen, evaluiert. Insbesondere die Einbindung der verschiedenen Betroffenen, die Kombination von technischen mit nicht-technischen Maßnahmen und die präzise Anpassung auf die jeweilige Umgebung erweisen sich als wirksame Ansätze.

1 Ineffizienz und fehlende Sicherheit durch Berechtigungen

Berechtigungen und Restriktionen in Informationssystemen – Autorisierung – sind Eckpfeiler der Informationssicherheit und wurden und werden daher intensiv in Forschung und Praxis entwickelt. Umso mehr überrascht, dass – trotz der anzunehmenden technischen Reife von Berechtigungssystemen – weiterhin regelmäßig Probleme mit Berechtigungen auftreten. Häufig stören Berechtigungen die Arbeitsabläufe in Organisationen; beispielsweise, wenn eine Aufgabe wegen fehlender Berechtigungen nicht *effizient* bearbeitet werden kann. Probleme werden aber nicht nur durch restriktive Berechtigungen verursacht, sondern auch durch zu weitgehende, zum Beispiel, wenn Berechtigungen nach einem Positionswechsel zugewiesen bleiben. In diesem Fall ist die *Effektivität* der Sicherheitsmaßnahme beeinträchtigt, denn die Berechtigungen bietet nicht den erwarteten Schutz. Die Effektivität wird ebenfalls beeinträchtigt, wenn übermäßig restriktive Berechtigungen die Anwender dazu verleiten, die Autorisierung für ihre Aufgaben zu umgehen und beispielsweise ihre Passwörter weiterzugeben.

Diese Probleme betreffen vorrangig die Organisation selbst und die Anwender. Bei genauerer Betrachtung können aber weitere Personen innerhalb von Organisationen iden-

* Vollständiger Titel der Dissertation: "Broadening the Scope of Security Usability from the Individual to the Organizational: Participation and Interaction for Effective, Efficient, and Agile Authorization" [Bar12a]

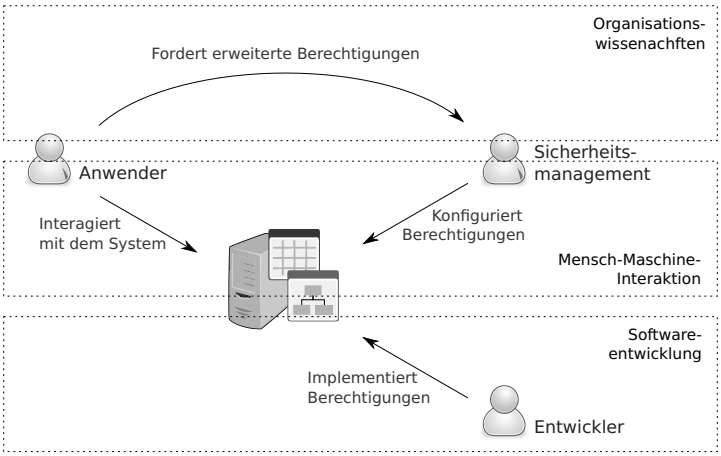

Abbildung 1: Perspektiven auf Berechtigungen und relevante Forschungsdisziplinen

tifiziert werden, die ebenfalls Probleme mit Berechtigungen haben, allerdings aus anderen Perspektiven (siehe Abbildung 1): etwa in der Verwaltung der Berechtigungen („Sicherheitsmanagement“). Beispielsweise müssen sich Anwender in vielen Organisationen an Verantwortliche wenden, wenn sie zusätzliche Berechtigungen benötigen. Als drittes müssen auch Entwickler mit einbezogen werden, denn diese implementieren die möglichen Beschränkungen erst in der Anwendung. Wenn diese Abläufe, Interaktionen und Aktivitäten im sozio-organisatorischen und -technischen Berechtigungssystem nicht harmonieren, werden Berechtigungen ihr Ziel, Sicherheit zu schaffen, wenn überhaupt, nur in Form einer übermäßigen Hürde erreichen. Die Produktivität der Organisation sinkt und Sicherheitsrisiken entstehen. *Rein technisch oder mit selektivem Blick auf eine einzelne Perspektive lassen sich die Probleme nicht bewältigen.* Abbildung 1 benennt einige der Disziplinen, die betrachtet werden müssen: Organisationswissenschaften, die Mensch-Maschine-Interaktion und die Softwareentwicklung.

Bisherige Arbeiten zu Berechtigungen bleiben dabei zumeist auf einer technischen Ebene, wie Siponen und Oinas-Kukkonen schreiben [SOK07]. Erst Zurko et al. [ZSS99] untersuchten die Benutzbarkeit von Berechtigungskonfigurationen und Brostoff et al. [BSC+05] wie verständlich die verwendeten Konzepte wie Rollen sind. Erst spät folgten einige – im Vergleich zur technischen Literatur zu Berechtigungen – wenige Studien zu den Praxisproblemen beim Setzen von Berechtigungen [WSC06, BCR+09, SG09]. Wie im vorhergehenden Absatz gesehen, greift allerdings eine selektive Betrachtung des Setzens von Berechtigungen zu kurz und übersieht etwa Probleme für den Anwender und die Auswirkungen für die Organisation. Damit bleibt dann für Entscheider unklar, warum sie diese Probleme angehen sollen.

Das Ziel der Dissertation [Bar12a] ist es deshalb, umfassende Lösungsansätze für die Probleme mit Berechtigungen in Organisationen zu entwickeln – also sich insbesondere nicht auf einzelne Perspektiven auf Berechtigungen zu beschränken. Dazu werden die Probleme systematisch und umfassend analysiert sowie die Bezüge zwischen den verschiede-

nen Perspektiven und deren Problemen hergestellt. Darauf aufbauend werden Ansätze zur grundsätzlichen Behebung der Probleme als acht Prinzipien entwickelt und anhand von fünf Artefakten evaluiert. Insbesondere die Einbindung der verschiedenen Betroffenen, die Kombination von technischen mit nicht-technischen Maßnahmen und die präzise Anpassung auf die jeweilige Umgebung erweisen sich als wirksame Ansätze.

2 Ganzheitliches Modell der Berechtigungsprobleme

Um die Probleme mit Berechtigungen umfassend zu erheben, wurden sie in einer großen qualitativen Studie – basierend auf Interviews mit 118 Mitarbeitern aus vielfältigen Umgebungen eines Großunternehmens – mittels des Grounded-Theory-Ansatzes [GS67] systematisch untersucht. Außerdem wurden die kausalen Zusammenhänge zwischen den Problemen identifiziert und mit den Organisationszielen in Bezug gesetzt. So zeigt sich etwa, dass Passwörter unter Mitarbeitern weitergegeben werden, weil die Prozesse für die Anforderung von Berechtigungen zum Teil zu lange („Monate“) dauern, aber die Arbeit erledigt werden muss. Aus diesen Ergebnissen in Verbindung mit den Problemen aus der Literatur ließ sich ein umfassendes Modell der Probleme und deren Abhängigkeiten entwickeln, basierend auf den verschiedenen Perspektiven von Benutzern auf Berechtigungen [BS13].

Zuoberst im Modell (dargestellt in Abbildung 2) befindet sich die Perspektive der *Entwickler*, die etwa das Berechtigungsmodell (also auch die möglichen Arten von Berechtigungen) und die Werkzeuge zum Setzen von Berechtigungen entwickeln. Diese Ebene beeinflusst unter anderem die nächsttiefer liegende Ebene der *Entscheidungen* zur Vergabe von Berechtigungen, die etwa, je nach Modell, feingranularer ausfallen können. Wie diese Entscheidungen erfolgen, gibt unter anderem den Rahmen für die *Prozesse* vor, denen Berechtigungsänderungen von der Beantragung bis zur Umsetzung folgen. Probleme sowohl mit Entscheidungen als auch mit den Prozessen können wiederum Auswirkungen auf die nächsttiefere Ebene der *Berechtigungen* selbst haben – beispielsweise, wenn Entscheidungen ohne ausreichendes Wissen gefällt werden oder Berechtigungen sich durch langlaufende Prozesse verzögern (wie im oberen Beispiel aus der Studie). Die Berechtigungen selbst beeinflussen dann die *primären Aufgaben der Anwender*; etwa wenn jeweils notwendige Berechtigungen fehlen. Letztlich haben Probleme in all diesen Ebenen Auswirkungen auf die *Ziele der Organisation*, also auf ihre Produktivität und die Wirksamkeit der Sicherheit.

Darüber hinaus konnte in der Studie anhand der Berechtigungssysteme in verschiedenen eingesetzten Systemen in dem Unternehmen gezeigt werden, dass das Auftreten der verschiedenen Typen von Problemen entscheidend von der Ausgestaltung des Berechtigungssystems abhängt. So traten Probleme mit den Prozessen zur Vergabe von Berechtigungen eher in Berechtigungssystemen mit zentralisierten und formalisierten Prozessen auf. Probleme mit Entscheidungen traten dagegen eher in Berechtigungssystemen mit dezentralen Strukturen auf. Daraus lässt sich schließen, dass die Probleme durch die richtige Gestaltung des Berechtigungssystem mit allen zugehörigen Komponenten (u.a. Werkzeugen, Prozessen und Entscheidungsstrukturen) adressiert werden können.

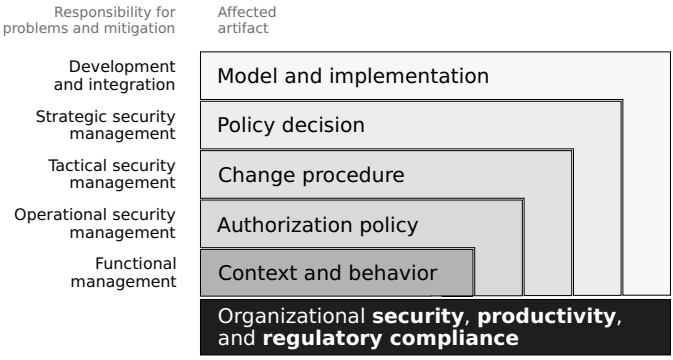

Abbildung 2: Empirisch identifizierte Ebenen der Berechtigungsprobleme

3 Acht Prinzipien für benutzbare Autorisierung

Für das Ziel, Ansätze zur Behebung der Probleme und zur Gestaltung von benutzbaren Berechtigungssystemen zu entwickeln, wurden acht Prinzipien für benutzbare Autorisierung entwickelt. Sie basieren auf etablierten und innovativen Forschungsansätzen aus der benutzbaren Sicherheit sowie praktischen Ansätzen aus der sicheren Agilen Software-Entwicklung:

Partizipation fördern Die Partizipation der verschiedenen Perspektiven und deren Austausch untereinander sollen gefördert, also etwa der betroffene Anwender stärker in die Entscheidungen einbezogen werden. Dadurch sollen dann zum Beispiel fehlende Berechtigungen aufgrund von fehlenden Informationen über deren Notwendigkeit beim Entscheider verhindert werden (vgl. Koordinierungsprozesse [Pal09]).

Belastung für den Einzelnen verringern Insbesondere wird dazu die Belastung für den Einzelnen verringert, also beispielsweise die Belastung, die ein Entscheider beim Ändern von Berechtigungen empfindet (vgl. [ZSS99]). Dadurch müssen unter anderem weniger Änderungen an Spezialisten, wie Administratoren, ausgelagert werden, was Missverständnisse vermeidet.

Interaktion konkretisieren Für eine leichtere Verständlichkeit wird angestrebt, das Abstrakte in den Benutzungsschnittstellen zu konkretisieren, so dass zum Beispiel von konkreten Anwendern und konkreten Berechtigungen und nicht von abstrakten Rollen gesprochen wird (vgl. [BCG08]).

Interdisziplinarität fördern Es sollen explizit Ansätze aus verschiedenen Disziplinen integriert werden, beispielsweise soziologische und organisatorische Herangehensweisen als Ergänzung der momentan vorherrschenden technischen.

Menschliches Verhalten einbeziehen Das menschliche Verhalten entsprechend der sozialen Umgebung soll berücksichtigt werden, also etwa, wann der Missbrauch einer Berechtigung zu erwarten ist (z.B. basierend auf Insider-Angreifer-Modellen

[Sch02]). Daraus kann dann etwa abgeleitet werden, ob Einschränkungen überhaupt notwendig sind.

Sicherheitsbewusstsein und Sicherheitsexpertise fördern Generell soll das Sicherheitsbewusstsein und die Sicherheitsexpertise gefördert werden [Bar11c], damit beispielsweise die Verwaltung von Berechtigungen näher zur eigentlichen Arbeit verlagert und zum Beispiel direkt im Team erledigt werden kann.

Auf Dynamik ausrichten Organisationen verändern sich. Um besser dieser Realität zu entsprechen, wird die Autorisierung als Maßnahme explizit auf Dynamik ausgerichtet. Wenn gar nicht davon ausgegangen wird, dass Berechtigungen statisch sind, sollten diese auch eher mit den realen Aufgaben und Bedürfnissen Schritt halten.

Auf die Umgebung anpassen Die Maßnahme soll generell eine Angemessenheit entsprechend der Umgebung in Bezug auf Prozesse (z.B. Formalität und Zentralisation der Organisation [Min89]) und Werkzeuge (notwendige Flexibilität, vorhandene Expertise) anstreben.

4 Entwicklung und Evaluierung von exemplarischen Lösungen

Die Autorisierungsprinzipien wurden evaluiert, indem fünf konkrete Artefakte entwickelt und jeweils empirisch evaluiert wurden. Die Artefakte zielen auf die Behebung verschiedener identifizierter Autorisierungsprobleme ab und sind so gewählt, dass sie jeweils primär eine der fünf Ebenen des Problemmodells abdecken.

4.1 Flexible Berechtigungen

Eines der entwickelten und evaluierten Artefakte betrifft die Ebene der Störungen im Arbeitsablauf der Anwender, die hier für Ausnahmesituationen adressiert werden. Die dahinterstehende Beobachtung ist, dass Berechtigungen häufig durch Weitergabe des Passwortes umgangen werden, um in Ausnahmesituationen kurzfristig wichtige Aufgaben zu erledigen, für die die Mitarbeiter im Normalfall nicht autorisiert sind. In Abbildung 3 sind diese Bedürfnisse gestrichelt dargestellt. Um Probleme in diesen Situationen zu vermeiden, werden flexible Berechtigungen umgesetzt, die es dem Anwender erlauben, kontrolliert die eigenen Berechtigungen temporär auszuweiten („Policy Override“). In Abbildung 3 sind diese Beschränkungen, die im Ausnahmemodus überschritten werden können, als „Soft Boundary“ eingezeichnet. Im Rahmen einer Fallstudie in einem mittelgroßen Unternehmen konnte die Machbarkeit des Ansatzes gezeigt sowie Faktoren für den Erfolg eines solchen Ansatzes identifiziert werden [Bar12b]. Insbesondere ist es wichtig, dass die flexiblen Berechtigungen in geeignete Prozesse eingebunden werden, damit reagiert werden kann, wenn der Ausnahmefall zur Regel wird.

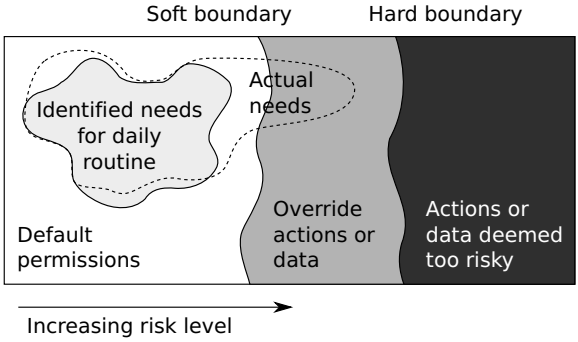

Abbildung 3: Schematische Darstellung normaler und Ausnahmeberechtigungen

4.2 Unterstützung für Berechtigungsänderungen

Ein weiteres Artefakt bietet eine Unterstützung für das Bearbeiten von komplexen Berechtigungen. Insbesondere bei rollenbasierten Berechtigungen kann es für Nicht-Experten schwierig sein, die technischen Änderungen an den Berechtigungen zu formulieren. Eine Änderungsunterstützung schlägt daher auf Basis von konkreten Änderungszielen (z.B. „Person A benötigt Berechtigung X, aber B soll sie nicht erhalten“) mögliche technische Änderungen vor. Dabei wurde ein effizienter KI-Algorithmus sowie eine Benutzerschnittstelle (dargestellt in Abbildung 4) implementiert [BSB09]. Auch hier zeigten sich in einer empirischen Evaluation mit Entscheidern und Administratoren aus verschiedenen organisatorischen Umgebungen die Vorteile des Ansatzes. Unter anderem berichteten Administratoren von einem erhöhten Sicherheitsgefühl beim Ändern von Berechtigungen, keine Fehler zu begehen. Darüber hinaus wurde in dieser Verwaltungsart eine verbesserte Basis für die Diskussion der Änderungsmöglichkeiten gesehen.

4.3 Entscheidungsunterstützung

Die Studie zu Problemen mit Berechtigungen zeigte auch, dass Entscheider mitunter überfordert sind, wenn sie entscheiden müssen, ob eine Person eine bestimmte Berechtigung bekommen sollte. Um diese Entscheidung zu unterstützen, wurde eine Entscheidungsunterstützung entwickelt, die Informationen zur Notwendigkeit von Berechtigungen und zu den potentiellen Risiken durch die Vergabe der Berechtigungen einbezieht [BS12]. Dazu werden verschiedene Betroffene – wie der Anwender und sein Vorgesetzter – in den Entscheidungsprozess einbezogen. Die Evaluation eines Prototypen des Werkzeugs (siehe Abbildung 5) mit Anwendern und Entscheidern aus unterschiedlichen Organisationen zeigte, dass ein solches Werkzeug zwar nicht in allen Umgebungen angemessen ist, aber einige Betroffene stark davon profitieren würden.

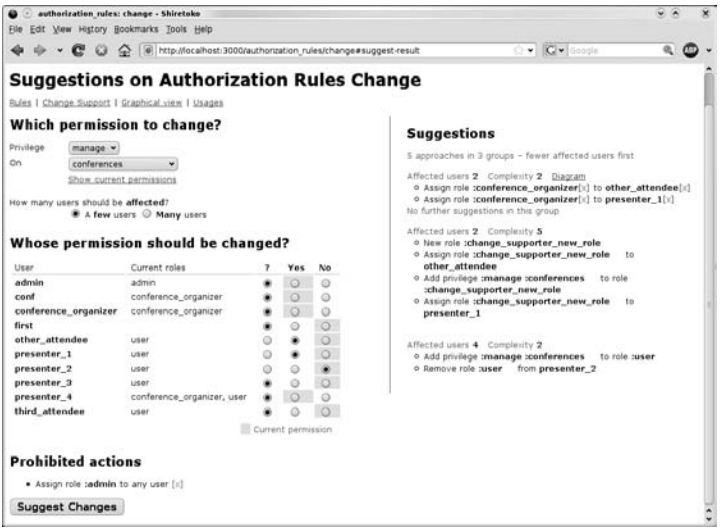

Abbildung 4: Benutzerschnittstelle für die Änderungsunterstützung

4.4 Angemessene Abläufe und Prozesse

Probleme mit Berechtigungen entstehen auch, wenn Anwendungen fortentwickelt werden, ohne bestehende oder durch neue Funktionen notwendige Berechtigungen zu beachten. Dann können Anwendern nach einem Update die benötigten Berechtigungen fehlen. Um diese Probleme anzugehen, wurde auf Basis der Literatur das integrative Prozessmodell INDUSE entwickelt, dass den Austausch zwischen Berechtigungsvergabe- und Entwicklungsprozessen explizit macht [Bar11b]. Dieses Modell wurde anhand von Interviews mit Entscheidern und Entwicklern in verschiedenen Umgebungen evaluiert. Dadurch konnten eine Reihe von informellen Prozessen und daraus resultierenden Probleme identifiziert werden.

4.5 Integration von Beschränkungen in Anwendungen

Die Probleme mit Berechtigungen, die ihren Ursprung in der Anwendungsentwicklung haben, hängen häufig mit fehlerhaftem Quelltext zur Durchsetzung der Berechtigungen zusammen – also etwa, wenn Berechtigungsabfragen fehlen. Je aufwendiger es ist, Durchsetzungen (z.B. Berechtigungsabfragen) in eine Anwendung zu integrieren und zu ändern, je wahrscheinlicher ist es, dass hieraus Probleme entstehen. Im Rahmen der Dissertation wurde daher eine Erweiterung für das Web-Entwicklungs-Frameworks *Ruby on Rails* entwickelt (*declarative_authorization*), deren Ansatz es ist, diese Aufwände zu minimieren [BSB09]. Die Open-Source-Erweiterung war zwischenzeitlich die beliebteste Ruby-on-Rails-Erweiterung für Berechtigungen. Um die Effekte der Erweiterung zu untersuchen,

	A	B	D	G
1	**Berechtigungsprofil**	Eigenschaften der Daten und Systeme		
2				
3	System	Auf welches System bezieht sich die Berechtigung?	[redacted]	
4	Datentyp	Welche Daten betreffen die Berechtigungen?	[redacted]	
5	Aktivität	Welche Aktivität wird erlaubt?	**Lesen**	z.B. Lesen, Ändern, Konfigurieren...
6				
10				
11	**Datensensibilität**			
12	Personenbezogene Daten	Sind personenbezogene Daten von den Berechtigungen betroffen?	N	Y: Yes, N: No
13	Mitarbeiterdaten	Mitarbeiterdaten?	N	Y: Yes, N: No
14	Sensible Daten	sensible personenbezogene Daten?	N	Y: Yes, N: No
16	Kommerzielle Sensibilität	Betreffen die Daten z.B. Verträge, das Risiko-Management oder externe Dritte?	Y	Y: Yes, N: No
17				
18	**Schäden**	(z.B. durch ungewollte Veröffentlichung, Änderungen...		
19		Stellen Sie sich vor, die Daten würden ungewollt veröffentlicht. Was wären die Konsequenzen für das Unternehmen?		1: vernachlässigbar, 2: gering, 3: merkbar, 4: kritisch, 5: katastrophal
21	Unternehmen	Wie schwer wären die Konsequenzen...		
22	Öffentlichkeitsarbeit	für die Öffentlichkeitsarbeit des Unternehmens?	2	1 – 5
23	Kommerzielle Schäden	für die kommerziellen Interessen oder die Produktivität?	4	1 – 5
25	Rechtliche Konsequenzen	aus vertraglichen oder gesetzlichen Verpflichtungen?	3	1 – 5
27	Persönliche Konsequenzen	Wie schwer wären die persönlichen Konsequenzen für den Verantwortlichen in Form von...		
28	(Straf-)Rechtlich	rechtlichen oder strafrechtlichen Ansprüchen?	1	1 – 5
29	Karriere, Arbeitsplatzsicherheit	Effekten auf die Karriere oder den Arbeitsplatz?	2	1 – 5
30				
31	**Bedrohungen**	für die Daten oder das System		
37	Vorsätzliche Bedrohungen	Wie wahrscheinlich ist es, dass einer der folgenden Akteure Interesse an der unerlaubten Veröffentlichung von Daten hat?		1: unwahrscheinlich, 2: entfernt, 3: gelegentlich, 4: möglich, 5: häufig
38	durch Konkurrenten	(z.B. um Kunden abzuwerben)	2	1 – 5
39	durch Lieferanten	(z.B. um höhere Preise zu erzielen oder Konkurrenten auszustechen)	1	1 – 5
40	durch Medien	(z.B. um eine interessante Geschichte zu veröffentlichen)	3	1 – 5
41	von eigenen Mitarbeitern	(z.B. um die Daten zu verkaufen oder weiterzugeben)	4	1 – 5
43	Unbeabsichtigte Bedrohungen			
...		Wie wahrscheinlich ist es, dass Daten unbeabsichtigt veröffentlicht		

Anfragender - Verwendung / Vorgesetzter - Zustimmung / Verantwortlicher - Rollenprofil / **Verantwortlicher - Berechtigungsprofil** / Verantwo

Abbildung 5: Prototyp der Entscheidungsunterstützung

wurde es in der Entwicklung einer realen Web-Anwendung für die Geschäftsprozesse eines mittelgroßen Unternehmens eingesetzt. In einer empirischen Auswertung des Entwicklungsverlaufs [Bar11a] ließ sich zeigen, dass die Entwickler tatsächlich Aufwände gespart hatten.

5 Leitlinien für effektive und effiziente Informationssicherheit

Das Anwenden der acht Prinzipien in den praktischen Artefakten und die damit verbundenen empirischen Evaluationen zeigen, dass die Prinzipien helfen, Autorisierung benutzbarer zu gestalten. Insbesondere die Partizipation aller Betroffenen an Entscheidungen zu Berechtigungen und die Kombination aus technischen Mechanismen zur Durchsetzung von Berechtigungen und nicht-technischen Maßnahmen (z.B. flexible Berechtigungen) verringern Produktivitätsverluste und Frustration. Weiterhin muss für alle Entscheidungen der Gestaltung der technischen und nicht-technischen Aspekte der Autorisierung die jeweilige Umgebung einbezogen werden. Genauso wie eine rein technische Lösung für die Berechtigungen nur in Ausnahmefällen zu optimalen Ergebnissen führt, gibt es bei der Vielzahl von sehr unterschiedlichen Kontexten von Autorisierung (vom Unternehmensumfeld über Berechtigungen für Nachrichten auf sozialen Netzwerken bis zu solchen für Anwendungen auf Smartphones) keine Standardlösung. Die Prinzipien bieten eine Leitlinie für die Entwicklung von angemessenen Berechtigungssystemen.

Die Lösungsansätze lassen sich auf weitere Gebiete der Informationssicherheit übertragen. Wie bei der Vergabe von Berechtigungen mangelt es auch hier häufig an dem notwendigen Wissen zu Risiken von bestimmten Entscheidungen (etwa: ob die Sicherheitswarnung des Web-Browsers ignoriert werden kann). Nicht zuletzt liegt es daran, dass die Kommunikation zwischen den sehr verschiedenen Gedankenmodellen von Entwicklern, Anwendern und Sicherheitsexperten fehlschlägt und damit z.B. Warnungen unverständlich und un-

verstanden bleiben. Die integrativen Methodik dieser Dissertation, also der Einbeziehung der verschiedenen Perspektiven von Betroffenen und der Multidisziplinarität, bietet einen vielversprechenden Ansatz für Forschung und Praxis, den genannten Herausforderungen zu begegnen: Durch das *Unterstützen einer „informierten Partizipation“* – also der Einbindung von Betroffenen in Entscheidungen [BDH93] – und durch die *Förderung der Interaktion zwischen den Betroffenen*. Dieser Ansatz bedeutet letztlich die Ausdehnung der Sichtweise vom Blick auf das Individuum in der benutzbaren Sicherheit (Wie kann der Einzelne mit dem Sicherheitsmechanismus umgehen?) auf das gesamte sozio-organisatorische Umfeld (Wie passt der Mechanismus in die realen Interaktionen und Abläufe im Umfeld? Wie können die Betroffenen eingebunden werden?). Der Ansatz erfordert allerdings auch eine noch größere Offenheit der Forschung für die Multidisziplinarität, um die Probleme mit der effektiven Sicherheit in Informationssystemen umfassend zu lösen und gleichzeitig ihre gesellschaftliche Akzeptanz zu fördern.

Literatur

[Bar11a] Steffen Bartsch. An Authorization Enforcement Usability Case Study. In *ESSoS 2011*. Springer, 2011.

[Bar11b] Steffen Bartsch. Exploring Twisted Paths: Analyzing Authorization Processes in Organizations. In *NSS '11: Proceedings of the 5th International Conference on Network and System Security*. IEEE Computer Society, 2011.

[Bar11c] Steffen Bartsch. Practitioners' Perspectives on Security in Agile Development. In *FARES '11: 6th International Workshop on Frontiers in Availability, Reliability and Security*. IEEE Computer Society, 2011.

[Bar12a] Steffen Bartsch. *Broadening the Scope of Security Usability from the Individual to the Organizational: Participation and Interaction for Effective, Efficient, and Agile Authorization*. Dissertation, Universität Bremen, 2012.

[Bar12b] Steffen Bartsch. Policy Override in Practice: Model, Evaluation, and Decision Support. *Security and Communication Networks*, 2012. In print.

[BCG08] Alan F. Blackwell, Luke Church und Thomas Green. The Abstract is 'an Enemy': Alternative Perspectives to Computational Thinking. *PPIG*, 2008.

[BCR+09] Lujo Bauer, Lorrie Faith Cranor, Robert W. Reeder, Michael K. Reiter und Kami Vaniea. Real life challenges in access-control management. In *CHI '09: Proceedings of the 27th international conference on Human factors in computing systems*, Seiten 899–908, New York, NY, USA, 2009. ACM.

[BDH93] John Seely Brown, Paul Duguid und Susan Haviland. Towards informed participation: Six scenarios in search of democracy in the electronic age. In *The Promise and Perils of Emerging Information Technologies*. The Aspen Institute, Queenstown, Maryland, USA, 1993.

[BS12] Steffen Bartsch und M. Angela Sasse. Guiding Decisions on Authorization Policies: A Participatory Approach to Decision Support. In *SAC '12: 27th ACM Symposium On Applied Computing*. ACM, 2012.

[BS13] Steffen Bartsch und M. Angela Sasse. How Users Bypass Access Control – and Why: The Impact of Authorization Problems on Individuals and the Organization. In *Proceedings for the 21st European Conference on Information Systems (ECIS 2013)*. AIS eLibrary, 2013. Accepted.

[BSB09] Steffen Bartsch, Karsten Sohr und Carsten Bormann. Supporting Agile Development of Authorization Rules for SME Applications. In *TrustCol '08: 3rd International Workshop on Trusted Collaboration*, Seiten 461–471, Berlin Heidelberg, 2009. Springer.

[BSC+05] Sacha Brostoff, Martina Angela Sasse, David W. Chadwick, James Cunningham, Uche M. Mbanaso und Sassa Otenko. 'R-What?' Development of a role-based access control policy-writing tool for e-Scientists. *Softw., Pract. Exper.*, 35(9):835–856, 2005.

[GS67] Barney G. Glaser und Anselm L. Strauss. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Aldine Transaction, 1967.

[Min89] Henry Mintzberg. *Mintzberg on management: inside our strange world of organizations*. Free Press, New York, NY, USA, 1989.

[Pal09] Frank Pallas. *Information Security Inside Organizations – A Positive Model and Some Normative Arguments Based on New Institutional Economics*. Dissertation, TU Berlin, 2009.

[Sch02] E. Eugene Schultz. A framework for understanding and predicting insider attacks. *Computers & Security*, 21(6):526–531, 2002.

[SG09] Diana K. Smetters und Nathan Good. How users use access control. In *SOUPS '09: Proceedings of the 5th Symposium on Usable Privacy and Security*, Seiten 1–12, New York, NY, USA, 2009. ACM.

[SOK07] Mikko T. Siponen und Harri Oinas-Kukkonen. A review of information security issues and respective research contributions. *SIGMIS Database*, 38:60–80, February 2007.

[WSC06] Tara Whalen, Diana K. Smetters und Elizabeth F. Churchill. User experiences with sharing and access control. In *CHI '06 extended abstracts on Human factors in computing systems*, Seiten 1517–1522, New York, NY, USA, 2006. ACM.

[ZSS99] Mary Ellen Zurko, Rich Simon und Tom Sanfilippo. A User-Centered, Modular Authorization Service Built on an RBAC Foundation. In *S&P '99: Proceedings of the 1999 IEEE Symposium on Security and Privacy*, Los Alamitos, CA, USA, 1999. IEEE Computer Society.

Steffen Bartsch wurde von der Universität Bremen im Juni 2012 mit einer Dissertation zum Thema benutzbare Sicherheit in organisatorischen Umgebungen promoviert. Seit Februar 2012 ist er Mitglied der Arbeitsgruppe SecUSo – Security, Usability and Society im CASED an der TU Darmstadt. Hier beschäftigt er sich mit der Unterstützung von sicherheitsrelevanten Entscheidungen, unter anderem durch die Verbesserung der Kommunikation zwischen den Verantwortlichen und Betroffenen. Zuvor forschte Steffen Bartsch seit Erhalt des Informatik-Diploms von der Universität Bremen 2007 im Technologie-Zentrum Informatik (TZI) der Universität Bremen.