Gesellschaft für Informatik e.V. (GI)

publishes this series in order to make available to a broad public recent findings in informatics (i.e. computer science and information systems), to document conferences that are organized in cooperation with GI and to publish the annual GI Award dissertation.

Broken down into
• seminars
• proceedings
• dissertations
• thematics
current topics are dealt with from the vantage point of research and development, teaching and further training in theory and practice. The Editorial Committee uses an intensive review process in order to ensure high quality contributions.

The volumes are published in German or English.

Information: http://www.gi.de/service/publikationen/lni/

ISSN 1617-5468
ISBN 978-3-88579-297-0

The 5. DFN-Forum Communication Technologies 2012 is taking place in Regensburg, Germany, from May 21st to May 22nd.
This volume contains 12 papers selected for presentation at the conference.
To assure scientific quality, the selection was based on a strict and anonymous reviewing process.

P. Müller, B. Neumair, H. Reiser, G. Dreo Rodosek (Hrsg.): 5. DFN-Forum 2012

203

GI-Edition

Lecture Notes in Informatics

Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)

5. DFN-Forum Kommunikationstechnologien

Beiträge der Fachtagung

21.–22. Mai 2012
Regensburg

Proceedings

Paul Müller, Bernhard Neumair, Helmut Reiser,
Gabi Dreo Rodosek (Hrsg.)

5. DFN-Forum Kommunikationstechnologien

Verteilte Systeme im Wissenschaftsbereich

21.05. - 22.05.2012
in Regensburg

Gesellschaft für Informatik e.V. (GI)

Lecture Notes in Informatics (LNI) - Proceedings
Series of the Gesellschaft für Informatik (GI)

Volume P-203
ISBN 978-3-88579-297-0
ISSN 1617-5468

Volume Editors
Prof. Dr. Paul Müller (pmueller@informatik.uni-kl.de)
Technische Universität Kaiserslautern
Postfach 3049, 67653 Kaiserslautern
Prof. Dr. Bernhard Neumair (bernhard.neumair@kit.edu)
Karlsruher Institut für Technologie
Hermann-von-Helmholtz-Platz 1, 76344 Eggenstein-Leopoldshafen
PD Dr. Helmut Reiser (reiser@lrz.de)
Leibniz-Rechenzentrum
Boltzmanstraße 1, 85748 Garching
Prof. Dr. Gabi Dreo Rodosek (Gabi.Dreo@unibw.de)
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39, 85577 Neubiberg

printed by Köllen Druck+Verlag GmbH, Bonn

Vorwort

Der DFN-Verein ist seit seiner Gründung dafür bekannt, neueste Netztechnologien und innovative netznahe Systeme einzusetzen und damit die Leistungen für seine Mitglieder laufend zu erneuern und zu optimieren. Beispiele dafür sind die aktuelle Plattform des Wissenschaftsnetzes X-WiN und Dienstleistungen für Forschung und Lehre wie die DFN-PKI und DFN-AAI. Um diese Technologien einerseits selbst mit zu gestalten und andererseits frühzeitig die Forschungsergebnisse anderer Wissenschaftler kennenzulernen, veranstaltet der DFN-Verein seit vielen Jahren wissenschaftliche Tagungen zu Netztechnologien. Mit den Zentren für Kommunikation und Informationsverarbeitung in Forschung und Lehre e.V. (ZKI) und der Gesellschaft für Informatik e.V. (GI) gibt es in diesem Bereich eine langjährige und fruchtbare Zusammenarbeit.

Das 5. DFN-Forum Kommunikationstechnologien „Verteilte Systeme im Wissenschaftsbereich“ steht in dieser Tradition. Nach den sehr erfolgreichen Vorgängerveranstaltungen in Kaiserslautern, München, Konstanz und Bonn wird die diesjährige Tagung vom DFN-Verein und der Universität Regensburg gemeinsam mit dem ZKI e.V. und der GI am 21. und 22. Mai 2012 in Regensburg veranstaltet und soll eine Plattform zur Darstellung und Diskussion neuer Forschungs- und Entwicklungsergebnisse aus dem Bereich TK/IT darstellen. Das Forum dient dem Erfahrungsaustausch zwischen Wissenschaftlern und Praktikern aus Hochschulen, Großforschungseinrichtungen und Industrie.

Aus den eingereichten Beiträgen konnte ein hochwertiges und aktuelles Programm zusammengestellt werden, das neben künftigen Netztechnologien und Themen des „Future-Internet“ unter anderem auf IT-Sicherheit mit sicherem Grid- und Cloud-Computing und IT-Service- Management eingeht. Ergänzt wird es durch eine Podiumsdiskussion zu Datenschutz und Sicherheit im Cloud-Computing und durch eingeladene Beiträge zu Smart Grids sowie zur Wissenschafts-Cloud Helix-Nebula. Die Vielfalt und Qualität der für das Forum akzeptierten Beiträge zeigt, dass die Veröffentlichung sowohl im Rahmen der GI-Edition Lecture Notes in Informatics als auch mit Open Access für die Wissenschaftlerinnen und Wissenschaftler attraktiv ist.

Wir möchten uns bei den Autoren für alle eingereichten Beiträge, beim Programmkomitee für die Auswahl der Beiträge und die Zusammenstellung des Programms, bei den Mitarbeiterinnen und Mitarbeitern für die umfangreichen organisatorischen Arbeiten und beim Gastgeber für die Unterstützung des Forums sowie die Gastfreundschaft bedanken. Allen Teilnehmern wünschen wir für die Veranstaltung interessante Vorträge und fruchtbare Diskussionen.

Regensburg, Mai 2012

Paul Müller
Bernhard Neumair
Helmut Reiser
Gabi Dreo Rodosek

Programmkomitee

Rainer Bockholt, Universität Bonn
Alexander Clemm, Cisco
Gabi Dreo Rodosek (Co-Chair), Universität der Bundeswehr München
Thomas Eickermann, Forschungszentrum Jülich
Markus Fidler, Universität Hannover
Alfred Geiger, T-Systems SfR
Wolfgang Gentzsch, DEISA
Hannes Hartenstein, KIT
Dieter Hogrefe, Universität Göttingen
Eike Jessen, Technische Universität München
Ulrich Lang, Universität zu Köln
Paul Müller (Co-Chair), Technische Universität Kaiserslautern
Bernhard Neumair (Co-Chair), KIT
Gerhard Peter, Hochschule Heilbronn
Christa Radloff, Universität Rostock
Erwin P. Rathgeb, Universität Duisburg-Essen
Helmut Reiser (Co-Chair), LRZ München
Peter Schirmbacher, Humboldt-Universität zu Berlin
Uwe Schwiegelshohn, TU Dortmund
Manfred Seedig, Universität Kassel
Marcel Waldvogel, Universität Konstanz
René Wies, BMW Group
Martin Wimmer, Universität Regensburg

Inhaltsverzeichnis

Future-Internet und Netztechnik

Daniel Günther, Nathan Kerr, Paul Müller
Auswahl von Netzwerktransportangeboten in einer Future-Internet-Architektur basierend auf funktionalen Blöcken 1

Feng Liu, Patricia Marcu, David Schmitz, Mark Yampolskiy
Rethinking Multi-Layer Multi-Domain Network Monitoring 11

Paul Müller, Dennis Schwerdel
G-Lab - an Experimental Facility for Future Internet Research and its International Context 25

Uwe Hillmer
Exemplarisches Langzeitreporting von Netzverfügbarkeiten 37

Grid und Cloud Sicherheit

Nils gentschen Felde, Wolfgang Hommel, Jan Kohlrausch, Helmut Reiser, Christian Szongott, Felix von Eye
Das Datenschutzkonzept für das föderierte Frühwarnsystem im D-Grid und seine technische Umsetzung 53

Sebastian Graf, Jörg Eisele, Marcel Waldvogel, Marc Strittmatter
A Legal and Technical Perspective on Secure Cloud Storage 63

Gabi Dreo Rodosek, Mario Golling, Wolfgang Hommel, Alexander Reinhold
Inter-Clouds: Einsatzmöglichkeiten und Anforderungen an die IT-Sicherheit 73

IT-Service Management und Grids

Silvia Knittl, Achim Grindler, Karmela Vellguth
IT-Servicemanagement Rahmenwerke – wie sie sinnvoll in Universitäten einsetzbar sind – 85

Marek Dynowski, Michael Janczyk, Janne Schulz, Dirk von Suchodoletz, Sven Hermann
Das bwGRiD – "High Performance Compute Cluster" als flexible, verteilte Wissenschaftsinfrastruktur 95

IT-Sicherheit

Jan Potthoff
Beweiswerterhaltendes Datenmanagement im elektronischen Forschungsumfeld 109

Michael Simon, Marcel Waldvogel, Sven Schober, Saher Semaan, Martin Nussbaumer
bwIDM: Föderieren auch nicht-webbasierter Dienste auf Basis von SAML 119

Christian Paulsen
Die OCTAVE-Risikoanalysemethode als selbstgesteuerter Einstieg ins Informationssicherheitsmanagement 129

Future-Internet und Netztechnik

Auswahl von Netzwerktransport-angeboten in einer Future-Internet-Architektur basierend auf funktionalen Blöcken

Daniel Günther, Nathan Kerr, Paul Müller
AG Integrierte Kommunikationssysteme
Technische Universität Kaiserslautern
Gottlieb-Daimler-Straße 47
67663 Kaiserslautern
guenther, kerr, pmueller@informatik.uni-kl.de

Abstract: Verschiedene Ansätze im Forschungsfeld Future Internet beschäftigen sich mit der Problemstellung, die Flexibilität des Internets zu erhöhen. Um dieses Ziel zu erreichen, wurden bisher verschiedene Entwicklungsstufen durchlaufen. Ein verbreiteter Ansatz in diesem Forschungsfeld ist der flexible Zusammenbau von Netzwerkprotokollgraphen durch die Verbindung einzelner funktionaler Blöcke. Diese Methode erlaubt es, den Kommunikationsanforderungen der Anwendung mithilfe eines hierzu erstellten Netzwerktransportangebotes zu entsprechen. Aufgrund der hierdurch erreichten Flexibilität ist es möglich, dass mehrere Funktionskompositionen die gestellten Anforderungen – in unterschiedlicher Angebotsausprägung – erfüllen. Notwendig ist es nun, ein Angebot für die Kommunikation auszuwählen. Problematisch ist hierbei allerdings die Entscheidung, welches Angebot in Form eines Netzwerktransportangebotes verwendet werden soll. Unterschiedliche Optimierungskriterien erhöhen zusätzlich die Komplexität dieser Problemstellung. Der vorliegende Beitrag präsentiert eine Methode zur Auswahl eines geeigneten Angebotes basierend auf einem multikriteriellen Entscheidungsverfahren. Die dargestellte Vorgehensweise wird durch Simulation mehrerer Testfälle, Komplexitätsbetrachtung sowie Diskussion evaluiert.

1 Einleitung

Das Internet hat sich in den letzten Jahren stark entwickelt. Beginnend bei den Forschungsarbeiten in den 1960er Jahren, wobei hier hauptsächlich der einfache Datenaustausch zwischen Rechnersystemen im Vordergrund stand, bis hin zu aktuellen Einsatzbereichen wie Internet-Telefonie, Online-Banking und Live-Übertragungen kann ein stetiger Zuwachs der Anwendungsbereiche verzeichnet werden. Dennoch sind die Kernmechanismen im Wesentlichen unverändert. Dies bedeutet zum einen, dass existierende Methoden ursprünglich nicht für heutige Anforderungen konzipiert wurden und zum anderen, dass funktionale Kompositionen von Methoden zur Realisierung eines anforderungskonformen Datentransfers durch das relativ starre ISO/OSI-Modell vorgegeben werden. Die Lösung der hieraus resultierenden Schwierigkeit, sich an neue Anwendungsfälle bzw. erweiter-

te Einsatzbereiche flexibel anzupassen, ist eines der Kerngebiete der Future-Internet-Forschung. Ein verbreiteter Ansatz in diesem Forschungsfeld ist der flexible Zusammenbau von Netzwerkprotokollgraphen durch die Verbindung einzelner funktionaler Blöcke, welche die zur Realisierung des Kommunikationswunsches notwendigen Methoden implementieren [SGKM11]. Die funktionalen Blöcke sind dabei in einem Depot gespeichert und werden nach Anforderung für eine bestimmte Kommunikationsaufgabe unter Beachtung von zusätzlichen Kriterien und dem Netzwerkangebot zu einem Protokollgraphen komponiert. Die Abbildung 1 zeigt ein mögliches Beispielszenario einer solchen flexiblen Netzwerkarchitektur. Durch das neuartige Netzwerktransportangebot ist es möglich, den heutigen Kommunikationsanforderungen der Anwendungen in einem weit flexibleren Rahmen zu entsprechen, als es durch die bisherigen Strukturen im Internet realisierbar ist [MR08].

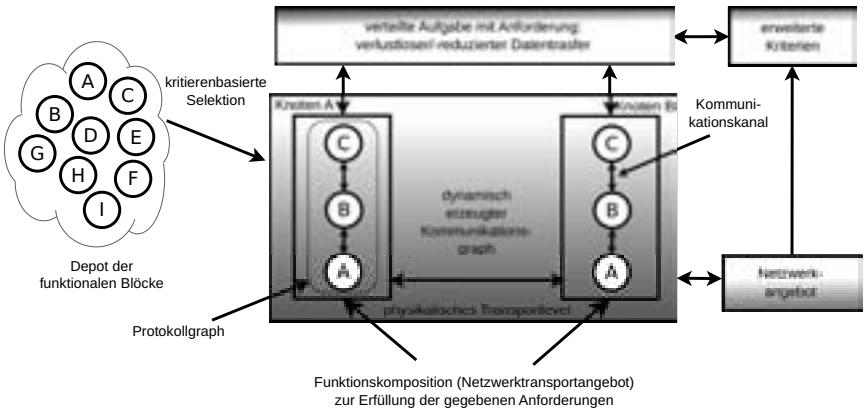


Abbildung 1: Future-Internet-Architektur basierend auf funktionalen Blöcken

2 Problemmotivation

Die Idee einer flexiblen Netzwerkarchitektur ist einer der Leitgedanken mehrerer Projekte im Bereich der Internetforschung. Dies sind beispielsweise Adaptive [SBS93], Da CaPo [VPPW93] sowie FCSS [Sti94]. Auch jüngere Forschungsprojekte wie 4WARD [VMK+08] und SONATE [MR08] verfolgen das Modell einer anforderungskonformen Kommunikationsarchitektur.

Der in diesem Beitrag einleitend skizzierte Lösungsansatz der Future-Internet-Forschung erlaubt sowohl eine einfache Integration neuer Funktionalitäten, als auch die Verwendung flexibler Funktionskompositionen. Es resultieren hieraus anforderungsangemessene Transportverbindungen mithilfe generierter Protokollgraphen. Die Verwendung solch flexibler Kompositionen löst einerseits das Problem der starren Kompositionsvorschrift des ISO/OSI-Modells, erzeugt aber gleichzeitig ein neues Problem: Eine Auswahl aus verschiedenen Netzwerktransportangeboten unter Beachtung mehrerer Eigenschaften und Optimierungswünsche muss getroffen werden.

Der einleitend beschriebene Ansatz gestattet unterschiedliche Lösungen, welche den gegebenen Anforderungen entsprechen können. Folgendes Szenario soll dies verdeutlichen. Die Komponenten des Protokollgraphen (die funktionalen Blöcke) können das gleiche Ziel anstreben – z.B. Paketverlustreduzierung – aber sie erreichen dies mit unterschiedlichen Methoden (Vorwärtsfehlerkorrektur oder automatische Wiederholungsanfrage). Hieraus kann geschlussfolgert werden, dass potenziell mehrere Protokollgraphen, die die Kommunikationsanforderungen erfüllen, existieren können.

Jedoch jeder funktionale Block selbst weist aufgrund der verwendeten Methode und jeder Protokollgraph aufgrund des unterschiedlichen Aufbaus verschiedene Charakteristiken auf, die dennoch in Summe alle gestellten Anforderungen an die Netzwerkkommunikation erfüllen können [GVM11]. In dem bereits aufgeführten Beispielszenario (Paketverlustreduzierung) könnte dies wie folgt der Fall sein. In der beschriebenen Kommunikationsarchitektur werden zwei Alternativen angeboten. Diese besitzen jeweils die Eigenschaften Datenrate und Paketverlustwahrscheinlichkeit. Bei der ersten Alternative sei die Datenrate $r = 100Kbit/s$ und die Paketverlustwahrscheinlichkeit $p = 0.0025$; bei der zweiten Alternative sei die Datenrate $r = 70Kbit/s$ und die Paketverlustwahrscheinlichkeit $p = 0.00125$. Für die Kommunikation wird allerdings $p < 0.03$ und $r > 64\,Kbit/s$ gefordert. Zusätzlich gibt es die Optimierungswünsche: r sei maximal, p sei minimal und die Optimierung von p besitze die höchste Priorität. Es ist offensichtlich, dass beide Angebote den Kommunikationswunsch erfüllen, allerdings in unterschiedlicher Ausprägung. Es muss also eine Entscheidung getroffen werden, welches Angebot auszuwählen ist, um das gezeigte Problem zu lösen.

Dieser Beitrag präsentiert eine Methode zur Auswahl von Netzwerktransportangeboten basierend auf einer multikriteriellen Entscheidungsmethode unter Beachtung priorisierter Optimierungskriterien. Dazu werden im Abschnitt 3 der Stand der Technik sowie verwandte Arbeiten aufgezeigt und diskutiert. Der darauf folgende Teil dieser Arbeit (Abschnitt 4) beschreibt den Lösungsansatz mithilfe einer generellen Problemmodellierung und der Darstellung des Entscheidungsprozesses. Die Evaluierung dieser Methode wird im Abschnitt 5 dargestellt und Abschnitt 6 fasst die Ergebnisse zusammen.

3 Stand der Technik

In der Literatur existieren verschiedene Methoden, um Entscheidungen treffen zu können. Hierbei gibt es Modelle mit probabilistischen Elementen [Wat86], Fuzzy-Methoden [Zim87], Simulationsansätzen [Geh92] und multikriteriellen Modellformulierungen. Dieser Beitrag geht davon aus, dass die zu lösende Aufgabe ein multikriterielles Entscheidungsproblem darstellt, d.h. mehrere Variablen – in unserem Fall sind es die Eigenschaften möglicher Alternativen sowie Optimierungskriterien – müssen berücksichtigt werden.

MacCrimmon K. teilt die multikriteriellen Entscheidungsmethoden in vier generelle Kategorien ein. Es handelt sich hierbei um Gewichtungs-, sequenzielle Eliminierungs-, mathematische Programmierungs- und Näherungsmethoden [Mac73]. Entgegen der intuitiven Annahme, dass aufgrund der Vielzahl von existierenden Lösungsmethoden und Model-

lierungsarten die Berechnung einer Entscheidung problematisch bzw. komplex ist, sieht Hanne T. das Hauptproblem bei multikriteriellen Entscheidungen in der Modellierung des Problems und der Wahl der Lösungsmethode [Han98]. Er zeigt weiter auf, dass die eigentliche Berechnung einer Lösung oft nur einen geringen Rechenaufwand bedeutet. Dennoch gilt, die Komplexität einer Entscheidungssituation wächst, wenn mehr Eigenschaften der zur Verfügung stehenden Alternativen zu beachten sind [EW03].

Der Annahme, dass die in diesem Papier aufgezeigte Problematik eine multikriterielle Problemsituation darstellt, folgt auch Khondoker R. in [KRS+10]. Seine Arbeit verwendet den von Saaty T. entwickelten *Analytic Hierarchy Process* (AHP) [Saa80], um funktionale Angebote zu selektieren. Er geht dabei von paarweisen Prioritäten zwischen den einzelnen Eigenschaften bzw. Kriterien aus. Die notwendigen Priorisierungsinformationen werden durch Interpolation bzw. Extrapolation der Werte der einzelnen Eigenschaften der Angebote ermittelt.

Völker L. untersuchte ebenso eine Auswahlproblematik in [VWZ08]. Auch hier müssen unterschiedliche Eigenschaften der zur Verfügung stehenden Alternativen (Sicherheitsprotokolle mit unterschiedlichen Kriterien) miteinander verglichen und letztlich eine Entscheidung für eine Auswahl getroffen werden. Auch er fasst diese Problemstellung als ein multikriterielles Problem auf. Als Lösungsansatz schlägt er die Anwendung der *Multi Attribute Utility Theory* (MAUT) [KRR79] vor. Grundlage dieses Lösungsansatzes ist eine Gewichtung der Eigenschaften bzw. der Kriterien.

Dieser Beitrag präsentiert nun eine Methode, welche eine Auswahl von Netzwerktransportalternativen mithilfe von geordneten Prioritäten (Entscheidungskriterien) realisiert.

4 Lösungsansatz

Die Lösung der in diesem Beitrag präsentierten Problemstellung basiert auf einer multikriteriellen Modellformulierung. Des Weiteren handelt es sich bei dieser Fragestellung um eine Entscheidung unter Sicherheit, d.h. es existieren keine subjektiven Wahrscheinlichkeiten [Doe07] im Entscheidungsprozess. Die für die Auswahl relevanten Eigenschaften bzw. Kriterien der zur Verfügung stehenden Alternativen sind generell unabhängig. Das bedeutet, wird eine Auswahl mit bestimmten Eigenschaften getroffen, so beeinflusst dies nicht die Qualität bzw. Ausprägung der Eigenschaften alternativer Wahlmöglichkeiten. Dennoch sind die einzelnen Eigenschaften der alternativen Angebote konjunktive Bedingungen und können als konkurrierende Ziele angesehen werden. D.h., wird ein Ziel – repräsentiert durch eine Eigenschaft – verfolgt, so beeinträchtigt dies möglicherweise die Erreichung eines anderen Zieles. Ein möglicher Zielkonflikt zwischen den Netzwerktransporteigenschaften Paketverlustwahrscheinlichkeit und Verzögerung möge hier als Beispiel dienen (Alternative 1: hohe Verzögerung, geringe Paketverlustwahrscheinlichkeit; Alternative 2: geringe Verzögerung, erhöhte Paketverlustwahrscheinlichkeit). Der hier beschriebene Lösungsansatz basiert auf den in [Mac73] vorgestellten Methoden der sequenziellen Eliminierung. Weiterhin gehen wir davon aus, dass die Angebote von funktionalen Kompositionen (Netzwerktransportangebote) für diesen Beitrag gegeben sind und den Anforderungen

in unterschiedlicher Ausprägung entsprechen. Im Folgenden wird das Problem generell modelliert, anschließend der vorgeschlagene Entscheidungsprozess dargestellt und an einem Beispielszenario die Arbeitsweise verdeutlicht.

4.1 Problemmodellierung

Die Lösung von multikriteriellen Problemen – *multiple criteria decision making* (MCDM) – basiert generell auf der Problemerkennung, -identifizierung und -strukturierung. Um dies zu erreichen, ist es notwendig, Alternativen und deren Ziel bzw. Eigenschaftsausprägungen sowie Optimierungskriterien zu definieren.

4.1.1 Definition und Strukturierung des MCDM

Ein MCDM ist ein Tupel (A, f), wobei A eine Menge von zur Verfügung stehender Alternativen und $f : A \rightarrow \mathbb{R}^q, q \geq 2$ eine Bewertungsfunktion ist. Durch f werden allen Alternativen Eigenschaftswerte $e \,\epsilon\, E$ zugewiesen, bezüglich derer optimiert werden kann. Die Anzahl der Eigenschaften bezeichnen wir mit q, die Anzahl der Alternativen mit n. Für jede Alternative $a \,\epsilon\, A$ stellen wir $f(a)$ folgendermaßen dar: $f(a) = (f_1(a), \ldots, f_q(a))$. Die Funktion f kann als eine Entscheidungsmatrix Z dargestellt werden. Abbildung 2 zeigt die Entscheidungsmatrix für die Problemstellung dieses Beitrags.

f	e_1	$\ldots$	e_q
a_1	$f_1(a_1)$	$\ldots$	$f_q(a_1)$
$\vdots$	$\vdots$		$\vdots$
a_n	$f_1(a_n)$	$\ldots$	$f_q(a_n)$

Abbildung 2: Entscheidungsmatrix Z

Wir definieren für dieses Lösungmodell weiterhin die notwendigen Optimierungskriterien $K = \{k_1, \ldots, k_m | \, k_i \epsilon O\}$. Wobei O die Menge der hier möglichen Ordnungsrelationen $O = \{\leq, \geq\}$ sei. Jedem e_i wird ein k_i zugeordnet.

4.2 Der Entscheidungsprozess

Ziel der hier vorgestellten sequenziellen Eliminierungsmethode ist es, eine Auswahlentscheidung für ein Netzwerktransportangebot zu treffen. Für diesen Prozess ist es erforderlich, dass die Eigenschaften e in eine strikte (lineare) Ordnung gebracht werden. Diese

Rangfolgebildung erfolgt durch lineare Priorisierung aller e. Beginnend bei der höchsten Priorität wird nun eine Sortierung nach der Ordungsrelation k der Alternativen in Z durchgeführt. Das bedeutet, wenn ein Optimierungskriterium $\leq$ ist, dann wird e_i aufsteigend und bei $\geq$ absteigend sortiert.

Beginnend bei einer Differenz zum optimalen Wert werden die folgenden Alternativen in Z eliminiert. Dieser Prozess wiederholt sich für alle gegebenen Eigenschaften e. Die Entscheidungsmatrix Z wird ausschließlich zeilenweise geordnet bzw. eliminiert, da die Eigenschaften $e_1 \ldots e_q$ in der dargestellten Problemstellung konjunktive Bedeutung haben. Algorithmus 1 verdeutlicht die einzelnen Arbeitsschritte der Entscheidungsmethode.

Algorithmus 1 Entscheidungsprozess

```
1: Rangfolgebildung der Eigenschaften e_1 ... e_q
2: while Es gibt noch nicht betrachtete Eigenschaften do
3:    if | A | = 1 then
4:       return Alternative a
5:    else
6:       e = nächste Eigenschaft
7:       k = Ordnung von e
8:       Sortierung der Alternativen in e bezüglich k
9:       Eliminiere in Z die nicht optimalen Alternativen
10:   end if
11: end while
```

Beendet wird der Entscheidungsprozess, wenn nur noch eine Alternative verwendbar ist oder alle möglichen Entscheidungskriterien geprüft wurden. Wird der Entscheidungsprozess nach Betrachtung aller Entscheidungskriterien beendet und sind noch mehrere Alternativen in Z, so sind alle Netzwerktransportangebote in jeder betrachteten Eigenschaft gleich. Zur Lösung der beschriebenen Problemstellung könnte daher jede Alternative gewählt werden. Wir wählen in diesem Fall die Erste.

4.3 Beispielszenario

Folgendes Szenario zeigt die Funktionsweise der präsentierten Entscheidungsmethode. Die einzelnen Werte der Entscheidungsmatrix Z sowie die Prioritäten der Eigenschaften sind im Rahmen dieses Beitrags gegeben (siehe Abbildungen 3 und 4). Ihre Berechnung erfolgte mithilfe des Mehrschrittprozessmodells aus [GKM12] und Annahmen über typische Erfordernisse einer *Voice-over-IP*-Kommunikationsverbindung.

	Eigenschaft	Ordnungsrelation (k_i)	Priorität
e_4	Framegröße in Byte	$\geq$ (maximieren)	4
e_3	Datenrate in Kbit/s	$\geq$ (maximieren)	3
e_1	Paketverlustwahrscheinlichkeit	$\leq$ (minimieren)	1
e_2	Verzögerung in ms	$\leq$ (minimieren)	2

Abbildung 3: Verwendete Entscheidungskriterien

Wie im Abschnitt 4.2 beschrieben, erfolgt zunächst eine Sortierung der Prioritäten nach ihrer Wichtigkeit (ordinale Reihenfolge wird erstellt, 1 = höchste Priorität). Nach erfolgter Neuordnung aller Eigenschaften, basierend auf den jeweils zugeordneten Prioritäten, permutieren die Zeilen in Z (siehe Abbildung 4).

	e_1	e_2	e_3	e_4
a_1	0.0025	204	99733.3	1496
a_2	0.000125	206	66488.9	1496
a_3	0.0025	206	99466.7	1492
a_4	0.000125	208	66311.1	1492
a_5	0.0025	206	99466.7	1492

$\rightarrow$

	e_1	e_2	...
a_4	0.000125	208	...
a_2	0.000125	206	...
a_1	0.0025	204	...
a_3	0.0025	206	...
a_5	0.0025	206	...

Abbildung 4: Z nach Ordnung der Eigenschaft mit der höchsten Priorität

Nach prioritätenkonformer Ordnung der Eigenschaften erfolgt die Eliminierung nicht optimaler Alternativen (siehe Abbildungen 5 und 6).

	e_1	e_2	e_3	e_4
a_4	0.000125	208	66311.1	1492
a_2	0.000125	206	66488.9	1496
a_1	0.0025	204	99733.3	1496
a_3	0.0025	206	99466.7	1492
a_5	0.0025	206	99466.7	1492

$\rightarrow$

	e_1	e_2	...
a_4	0.000125	208	...
a_2	0.000125	206	...
a_1	0.0025	204	...
a_3	0.0025	206	...
a_5	0.0025	206	...

Abbildung 5: Eliminierung nicht in e_1 optimaler Alternativen

	e_1	e_2	e_3	e_4
a_2	0.000125	206	66488.9	1496
a_4	0.000125	208	66311.1	1492

$\rightarrow$

	e_1	e_2	...
a_2	0.000125	206	...
a_4	0.000125	208	...

Abbildung 6: Ordnung und Eliminierung nicht in e_2 optimaler Alternativen

Weitere Schritte sind in diesem Szenario nicht notwendig, da bereits nur noch das Netzwerktransportangebot a_2 zur Auswahl steht.

5 Evaluation

Um den vorgestellten Lösungsansatz bewerten zu können, wurden mehrere Testszenarien simuliert und die Resultate analysiert. Zum Abschluss der Bewertung werden die Vor- und Nachteile des Entscheidungsprozesses diskutiert.

5.1 Testszenarien

In den folgenden Testszenarien werden ceteris paribus die Priorisierungen der Kriterien verändert, um die Auswirkung auf die Alternativenauswahl hinsichtlich der betrachteten und der optimalen Eigenschaften darzustellen. Die für diese Analyse zur Verfügung stehenden Alternativen haben die Eigenschaften wie in Abbildung 3 dargestellt. Die Prioritätenfestlegung der Eigenschaften für die durchgeführte Untersuchung wird in Tabelle 1 aufgezeigt.

e_1	e_2	e_3	e_4	a	Optimale Eigenschaften	Betrachtete Eigenschaften
1	2	3	4	a_2	e_1, e_4	$e_1,\ e_2$
2	1	3	4	a_1	e_2, e_3, e_4	e_2
2	3	1	4	a_1	e_2, e_3, e_4	e_3
2	3	4	1	a_2	e_1, e_4	e_4, e_1

Tabelle 1: Auswahl verwendeter Prioritäten für e_i der Testszenarien

Die 2. Spalte von rechts zeigt die Eigenschaften der gewählten Alternative, deren Wert optimal ist. Analog zur gewählten Alternative zeigt die 1. Spalte von rechts, welche Eigenschaften während des Entscheidungsprozesses betrachtet wurden.

Die durchgeführte Auswertung zeigt einerseits, dass immer ein optimales Ergebnis bei Anwendung dieser Entscheidungsmethode hinsichtlich der höchsten Priorität erfolgt. Andererseits kann abgeleitet werden, dass nicht in jedem Fall niederpriorisierte Eigenschaften beim Treffen der Entscheidung verwendet werden.

5.2 Komplexität

In dieser Arbeit wird festgestellt, dass die Einschätzung von Hanne T. – die Berechnung der Lösung des hier betrachteten Problems bedeutet oft nur einen geringen Rechenaufwand – bestätigt werden kann. Der bei Simulation der Testszenarien verwendete Sortieralgorithmus weist eine durchschnittliche Komplexität von $n \cdot log\, n$ auf [Net11]. Dieser Teilalgorithmus wird, wenn notwendig, q mal durchgeführt. Es ergibt sich hieraus also eine Laufzeitkomplexität von $O(n \cdot log\, n \cdot q)$.

5.3 Diskussion

Der präsentierte Entscheidungsprozess stellt die Ermittlung effizienter Alternativen sicher [Han98]. Ein wesentlicher Vorteil dieser Methode ist, dass die unterschiedlichen Eigenschaften des Netzwerktransportangebotes nicht direkt vergleichbar sein müssen. Ein solcher Fall könnte beispielsweise vorliegen, wenn es sich um eine Entscheidung zwischen Alternativen mit und ohne metrischen Werten handelt (Verschlüsselung, Verzögerung). Eine ordinale Eigenschaftsordnung ist hier ausreichend. Er ist deshalb geeignet, um in dem dargestellten Problemszenario eingesetzt zu werden. Ein weiterer Vorteil dieser Methode ist, dass Indifferenzen bei optimalen Werten innerhalb der gleichen Eigenschaft zu einer weiteren Betrachtung einer anderen Eigenschaft führen. Ein Nachteil des präsentierten Entscheidungsprozesses ist, dass Eigenschaften mit geringen Prioritäten in bestimmten Situationen, beispielsweise wenn mögliche Alternativen schon bei Betrachtung der höheren Prioriäten eliminiert wurden, nicht betrachtet werden. Dieses Verhalten hat allerdings keine signifikaten Auswirkungen, da die gewählte Alternative bereits effizient ist.

6 Zusammenfassung

Zusammenfassend kann festgehalten werden, dass die in diesem Beitrag beschriebene Problemstellung – Auswahl eines Angebotes mit verschiedenen Eigenschaften unter Beachtung ordinal priorisierter Optimierungskriterien – wie folgt gelöst wurde. Die Problemstellung wurde zunächst motiviert sowie durch Literatursichtung und Betrachtung verwandter Arbeiten in den Stand der Technik eingeordnet. Die präsentierte Methode ist ein multikriterielles Eliminierungsverfahren basierend auf geordneten Prioritäten und Eigenschaften. Sie führt zur Auswahl einer Alternative. Evaluiert wurde diese Methode durch Simulation, Komplexitätsbetrachtung und Diskussion. Das Ergebnis dieses Beitrags ist eine weitere Entwicklungsstufe innerhalb des Forschungsgebietes Future Internet.

Dieser Beitrag ist im Rahmen des Projekts “German-Lab” – gefördert durch das Bundesministerium für Bildung und Forschung (BMBF), Deutschland – entstanden. Für die konstruktiven und wertvollen Hinweise des Kollegiums fühlen sich die Autoren zu Dank verpflichtet.

Literatur

[Doe07] Doersam, P. *Grundlagen der Entscheidungstheorie anschaulich dargestellt*. PD-Verlag, 2007.

[EW03] Eisenführ, F. and Weber, M. *Rationales Entscheiden*. Springer Verlag, 2003.

[Geh92] Gehring, H. Simulation. In *Grundlagen des Operations Research 3*. Springer Berlin, 1992.

[GKM12] Günther, D., Kerr, N., and Müller, P. A Model to Select and Compose Functional Block Based Protocol Graphs. In *7th GI/ITG KuVS Workshop on Future Internet, Munich, Germany*, 2012.

[GVM11] Günther, D., Veith, E. MSP, and Müller, P. A Way to Identify Decision Criteria for Selecting Different Mechanisms which Provide Reliable Transmission in a Flexible Future Internet Architecture. In *7th Euro-NF Conference on Next Generation Internet, Kaiserslautern, Germany*, 2011.

[Han98] Hanne, T. *Multikriterielle Optimierung: Eine Übersicht*. Diskussionsbeitrag Nr. 251 der Wirtschaftswissenschaft der FernUniversität Hagen, 1998.

[KRR79] Keeney, R. L., Raiffa, H., and Rajala, D. W. Decisions with Multiple Objectives: Preferences and Value Trade-Offs. In *Proceedings of the IFIP TC6/WG6. 5 International Conference on Upper Layer Protocols, Architectures and Applications*, 1979.

[KRS+10] Khondoker, M. R., Reuther, B., Schwerdel, D., Siddiqui, A., and Müller, P. Describing and Selecting Communication Services in a Service Oriented Network Architecture. In *Proceedings of the ITU-T Kaleidoscope event, Pune, India*, 2010.

[Mac73] MacCrimmon, K. R. An Overwiew of Multiple Objective Decision Making. In *Multiple Criteria Decision Making*. University of South Carolina Press, 1973.

[MR08] Müller, P. and Reuther, B. Future Internet Architecture - A Service Oriented Approach. *it - Information Technology*, 50(6):383–389, 2008.

[Net11] The C++ Resourcess Network. STL Algorithms, 2011.

[Saa80] Saaty, T. L. *The Analytic Hierachy Process*. McGraw-Hill, New York, 1980.

[SBS93] Schmidt, D. C., Box, D. F., and Suda, T. Adaptive: A Dynamically Assembled Protocol Transformation, Integration and Evaluation Environment. *Concurrancy - Practice and Experience*, 1993.

[SGKM11] Schwerdel, D., Günther, D., Khondoker, M. R., and Müller, P. A Building Block Interaction Model for Flexible Future Internet Architectures. In *7th Euro-NF Conference on Next Generation Internet, Kaiserslautern, Germany*, 2011.

[Sti94] Stiller, B. Fukss: Ein funktionsbasiertes Kommunikationssubsystem zur flexiblen Konfiguration von Kommunikationsprotokollen. *GI/ITG-Fachgruppe Kommunikation und Verteilte Systeme*, 1994.

[VMK+08] Völker, L., Martin, D., Khayat, I. E., Werle, C., and Zitterbart, M. An Architecture for Concurrent Future Networks. In *2nd GI/ITG KuVS Workshop on the Future Internet*, 2008.

[VPPW93] Vogt, M., Plagemann, T., Plattner, B., and Walter, T. A Run-time Environment for Da CaPo. In *Proceedings of INET93 International Networking Conference of the Internet Society*, 1993.

[VWZ08] Völker, L., Werle, C., and Zitterbart, M. Decision Process for Automated Selection of Security Protocols. In *33rd IEEE Conference on Local Computer Networks (LCN 2008)*, 2008.

[Wat86] Waterman, D. A. *A Guide to Expert Systems*. Addison-Wesley, 1986.

[Zim87] Zimmermann, H. J. *Fuzzy Sets, Decision Making, and Experts Systems*. Kluwer, Boston, 1987.

Rethinking Multi-Layer Multi-Domain Network Monitoring

Feng Liu[1,2], Patricia Marcu[1,2], David Schmitz[1,2], and Mark Yampolskiy[1,3]

[1]Munich Network Management Team
[1]*{liufeng, marcu, schmitz, yampol}@mnm-team.org*
[2]Leibniz-Rechenzentrum (LRZ), 85748 Garching/München, Germany
[3]Vanderbilt Universtity, TN USA

Abstract: Accurate and efficient network fault localisation based on monitoring is obviously one of the vital but also formidable tasks for successful network operations. With proliferations of large-scale network services, e.g. Géant E2E links, monitoring and fault localisation across multiple domains with data obtained from different network layers are becoming unprecedentedly important. Many efforts have been invested to tackle the challenges posed by fault localisation, nevertheless, most approaches only suggest partial solutions to the problematics of multi-domain multi-layer aspects. Most importantly, a comprehensive view and deep understanding of the problem is still missing. In this paper, we intend to systematically discuss challenges and their implications posed by fault localisation with consideration on multi-domain and multi-layer monitoring data. The contributions of this paper are manifold: *first* we identify key research challenges regarding multiple layer monitoring for fault localisation across domains; *then* based on the identified multiple layer network patterns, we establish comprehensive problem dimensions in a systematic and structured way which holds key to the solution development; *finally* we propose a formal definitions on information model which captures essential characteristics of multiple network layers across domains.

Keywords: Multi-domain/Multi-layer Network Management, Network Monitoring, Network Fault Localization, Network Modeling, Formal Methods.

1 Introduction

Maintaining of well-functioning networks is one of the prerequisites for offering high quality networking services. This implies that network outages of any kind should be detected and localized the soonest possible so that impact to network can be reduced to its minimum. To facilitate high efficient network fault detection and localization processes, we need support from accurate and effective network monitoring approaches which allow network events to be registered and reported in a timely and precise manner. With proliferation of large scale network services across multiple domains, such as Géant end-to-end link services [YHL+10], monitoring mechanisms that are confined within a single administrative as well as technological domain are no longer suitable for performing monitoring tasks across several domains. Moreover, to increase the accuracy of the fault detection and

localization processes, monitoring data from multiple network layers need to be aggregated and correlated so that network faults could be precisely pin-pointed [Gop00, SS02]. We argue that to cope with today's network management problems, especially for fault detection and localization, monitoring approaches have to consider and combine the multi-domain and multi-layer aspects. Unfortunately, despite its importance, only little has been done in this research area. Research challenges and problematics regarding multi-domain multi-layer monitoring are neither well-understood nor thoroughly investigated.

To bridge this gap, in this seminal paper, we focus on several important issues as foundations for building a viable monitoring approach for the multi-domain and multi-layer networks. The goals of this paper are manifold: first we identify and articulate research problems and challenges. Then based on the problem statement, we establish a rather comprehensive problem dimensions based on network patterns that we identified. The given problem dimensions could be used as a reference for solution development and further research. Finally and most importantly, we propose a formally defined information model using set-theoretic notations, which we argue is a concise and flexible way to model network links and paths with consideration on multi-domain and multi-layer aspects.

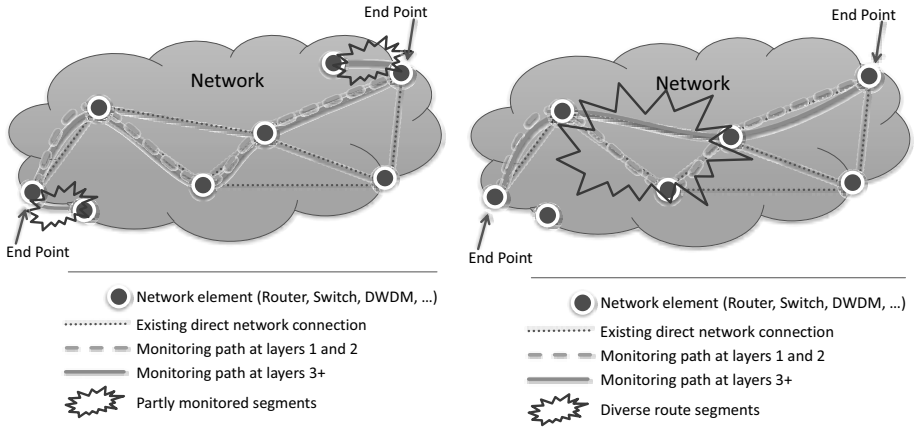
2 Problem Statement

In this section, we articulate research problems and challenges that are inherent to multi-domain multi-layer network monitoring approach. It is not our intention to provide an exhaustive list of problems, rather we try to identify and discuss some of the most important and fundamental ones.

Ideally all monitoring information that have to be correlated should be collected over the same infrastructure and at the same time. However, in the reality it is not always the case, we approach our problem statement with special focus on two main perspectives: *topology* and *time*.

For the matter of simplicity, for all examples in this section we assume that the monitoring information of ISO/OSI layers 1 and 2 should be correlated with the monitoring information obtained at ISO/OSI layer 3 and higher (noted as layer 3+ hereafter).

Topology: Measurement Points Regardless whether active or passive measurements are employed, monitoring should be performed between an actual pair of end-points (also known as measurement points) from which monitoring data are desired. Nevertheless, more than often, extra link segments lay between the measuring equipment and the actual measuring points, which is not only confusing but also may distort the monitoring results as well. The quality of network segment between actual measurement point and device to be measured can influence quality of results. Fig. 1(a) illustrates the discussed measurement points placement, in which equipment for ISO/OSI layer 3+ measurement is attached to two further components. To perform a multi-domain multi-layer monitoring operation, such scenarios must be considered.



(a) Monitoring between different end-points

(b) Monitoring different routes

Figure 1: Monitoring modes

Topology: Communication Path Even if the measurements are performed between an actual pair of end points, they are not always performed on the same monitoring subject. In Fig. 1(b) a typical situation of path diversity between ISO/OSI layer 1&2 and 3+ monitoring is depicted. In operations, the layer 1 and 2 monitoring is performed via access to the error counters at the installed network infrastructure. Usage of extra devices like Optical Time Domain Reflectometer (OTDR) is regarded as an expensive option. Consequently, monitoring at layers 1 and 2 can be seen as measurements over fixed path.

From ISO/OSI layer 3 upwards, a fixed path is not always guaranteed[1]. An network problem at layer 3 can force a router to switch to an alternative path. Such capability is overseen by almost every routing algorithms. This implies network problem at layer 2 cannot be detected if only layer 3 fault detection and localization is applied, since the self-repairing mechanism of routing algorithms mask such failure automatically. The alternative path may introduce extra network delay and it is a time-consuming process to find out the reason of network deterioration. A more advanced situation of route diversity is the route flipping, which means that there is no guarantee that the IP packets at layer 3 always routed through the same path. A direct consequence is that not only monitoring paths at different layers can differ but also the path difference can change over time. Further, this could also mean that the active probes for layer 3 monitoring can in worst case take a route which is completely different from the end user traffic. This in turn would lead to disagreements between monitoring data and end-user experience with the connection.

Time: Measurement Scheduling Even at ISO/OSI layer 3 along, different measurements can be performed. Due to its invasive nature, high-frequent usages of active measurements are not advisable. Less invasive approaches can be nevertheless applied fre-

[1]Even if such a fixed path can be enforced, e.g. via traffic engineering with MPLS.

quently, as it does not influence use traffic too much, for instance, the period of back-to-back packets sent for jitter measurements can be held quite short. The throughput measurements vice versa can be scheduled only occasionally as they directly influence the end-user service quality. Furthermore, some of the measurements can be barely performed at the same time. For instance, the mentioned throughput measurement would negatively influence measurements of delay variation.

Consequently, at different layers different permanent, periodical, and scheduled measurements are available for correlation. Further, also the measurements which have to be performed during some period of time can be scheduled for different time. This means that the monitoring information at different layers might be based on the measurements performed under different network conditions.

Time: Clock Synchronization Similar to the discussion about measurement scheduling, not synchronized clocks might cause the drift between the measurements at different layers. However, the application areas are different from those of scheduling. For instance, especially in the case of multi-domain network connections the monitoring measurements can be performed by different organizations. Further, the past monitoring data might have to be evaluated. This all requires that the measurements provided by different monitoring infrastructure and organizations have to be correlated for the exact time period. This in turn requires that either the clocks between all monitoring infrastructures are synchronized during measurements or the clock deviation is known so that it can be taken in account during post-processing.

In addition to the aforementioned technical problems, a non-technical barrier worth mentioning is that various management policies reign among the participating domains. For example, a domain may be reluctant to share its information regarding network connectivities for security reasons, thus it may pose a very restrictive information-sharing policy towards external entities. Consequently lacking essential monitoring information, even the most sophisticated fault localization algorithm cannot produce expected results. To this end, fault localization approaches have been investigated based on partial network information. Inference techniques based on Bayesian theory, neural networks and decision trees, etc. have been applied to cope with incomplete network information.

3 Scenario Dimensions

For a better delimitation of the main problems concerning multi-layer multi-domain monitoring three scenario dimensions have been identified:

- Multi-layer: concerned with the influence the network layering has on monitoring. As on each network layer other metrics or parameters are needed, an overview of these layers and their interconnections is taken into account. Multi-layer is a vertical dimension.
- Multiple technical domains: this is only one part of the multi-domain dimension.

	QoS-Param	Topology	Time	Functionalities
Multi-layer	ML-Q	ML-To	ML-T	ML-F
Multiple technical domains	MT-Q	MT-To	MT-T	MT-F
Multiple organizational domains	MO-Q	MO-To	MO-T	MO-F

Table 1: The dimension matix

Monitoring a multi-domain network it is a challenge to bring together information from different technical domains, so domains that uses different techniques (Ethernet, MPLS, SDH etc.). This is a horizontal dimension.

- Multiple organizational domains: the second part of the multi-domain dimension. There is a difference between this and the former one, as there could be the same technique used in two different organizational domains as well as two different techniques within one organizational domain.

For the given dimensions following network properties are relevant in the different specificity:

- QoS-Parameter: as the most important quantifiable parameter for the network monitoring
- Topology: representing the real and logical components and their connection on all layers of the network.
- Time: challenges as measurement scheduling and clock synchronization are directly connected with the parameter of time.
- Functionalities (management and usage): generally represents what the network offers in terms of usage (connectivity, IP services etc.) and how this is managed.

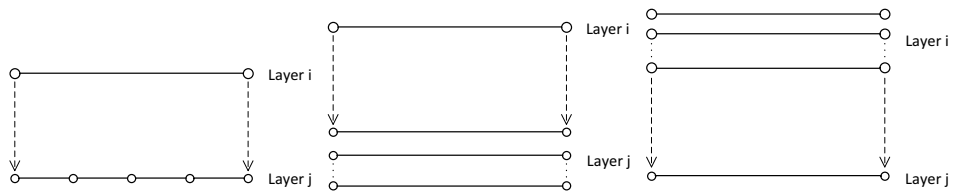
The dimension matrix (see Table 1) results from the combination between the different dimensions on the vertical(left) and the properties horizontal (on top).

In the following the fields of the dimension matrix will be explained. Not each of these fields have the same importance. We will begin with the multi-layer/topology (ML-To) field as the most complex of them. This is also the basic problem space on which all other are based on. Therefore we propose for ML-To item three different patterns (see Figure 2). In all of these we compare two general layers (i and j) of the network.

- Simplified Segmented Layering: For this pattern (see Figure 2(a)) we assume that for a link on layer i a segmented link on a lower layer (layer j) exists. The „margins" of the link on the upper layer correspond to some other nodes in the layer below. In the layer j as the name suggests more link segments are given which realize on this layer the pre-requisite for the functionality of the link on the upper layer.

- Bundling: In this case on layer i (upper) exists a link which is realized by bundling some links on a lower layer j. So here we have a projection of a layer i „margin" on more „margins" of all of the links in the bundle on layer j (see Figure 2(b))
- Link Sharing: In the last pattern proposed (see Figure 2(c)) on layer i there are a bunch of links realized all though one link on the lower layer j. As all these links on the upper layer use that one link on the lower layer, this has been named link sharing.

Although we present these three patterns, it could be possible that other patterns exist. These chosen patterns are that ones which bring for our multi-layer, multi-domain monitoring approach the most essential and needed information content.



(a) Simplified Segmented Layering (b) Bundling (c) Link Sharing

Figure 2: Multi-Layer/Topology Patterns

As stated before the ML-To field of the dimension matrix is the basis for all other. We will not detail here all of them, we only highlight some connections between them. Multi-layer/QoS-Parameter (ML-Q) is based on ML-To as all the QoS-Parameter are specific for each network layer respectively network topology. ML-T (multi-layer/time) is also strongly related on ML-To as synchronization and scheduling of measurements for a proper monitoring result have to be related to the multiple-layer/topology issue. Same problematic for ML-F (multi-layer/functionalities) as different functionalities can be delivered on different layers and naturally for different topologies. Also for each network layer/topology different management functionalities are assigned.

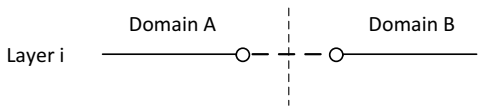


Figure 3: Multi-domain: intra-/inter-domain links per layer

The second row in the dimension matrix is dealing with the multiple technical domains in relation with the different parameters. All four fields are directly related to the upper one as each technical domain is organized as a multi-layer network. So MT-To (multiple technical domains/topology) is directly based on ML-To so the patterns described above meet at their margins other technical domains (see Figure 3). For the third row of the dimension matrix multiple organizational domains apply the same consideration as for the second row.

4 Solution Building Blocks

As presented in the precious sections, designing a comprehensive fault localization approach across multiple layers and multiple domains is a challenging task. The fact that, not only technical issues but also organizational, even political reasons contribute to the complexity, further deteriorates the problematic. Therefore, instead of offering a complete solution, as core contribution of this paper we rather intend to discuss the essential generic building blocks that must be considered and observed in a development of such an approach. The presented models could be used as templates or guidelines by designing specific network monitoring approaches across domains and layers. We argue that a set of clearly presented solution models are more crucial and provide piece-meal solutions.

We believe that a comprehensive solution must be designed with four different model-based views, including: *Information Model, Communication Model, Organisational Model* and *Functional Model*, as it is methodologically suggested in [HAN99]. However, concentration will be given to the information model at this stage, detailed discussion regarding other models will be provided in our series of paper in future.

4.1 Information Model

We use a formal model to clearly define and describe the essential elements and corresponding structural patterns introduced in Section 2. In addition to simplicity and conciseness, using mathematical model allows utilizing well-defined mathematical operations to manipulate the model. For later applications, the model can be simply mapped to data structure, in a selected programming language. We approach the modeling operation in two phases: first we provide a definition of a basic link model which can be regarded as the very elementary building block; then, based on the basic model, we describe formally the network patterns as we identified in the previous section.

4.1.1 Basic Definitions

In order to formally define the ML-To patterns it is necessary to introduce some general definitions borrowed from graph theory. This can be divided into two categories: the general/layer-independent and the layer-dependent definitions for link and path.

Definition 1. *Link*

*A **link** is defined as an edge $e \in E$ from **start node** v_{start} to **end node** v_{end}, with $v_{start}, v_{end} \in V$, with E the set of all potential links (edges) and V the set of all potential nodes.*

Following functions for edge/node relationships are defined:

$\texttt{start} : E \rightarrow V$ *with start node* $\texttt{start}(e) = v_{start}$ *and*
$\texttt{end} : E \rightarrow V$, *with end node* $\texttt{end}(e) = v_{end}$.

Definition 2. *Path*

*A **path** p from **start node** v_{start} to **end node** v_{end} is a (ordered) sequence of links $[e_1, e_2, \ldots, e_n]$, with $e_1, e_2, \ldots, e_n \in E$, $v_{start} = \texttt{start}(e_1)$, $\texttt{end}(e_{i-1}) = \texttt{start}(e_i)$, for $i = 2, \ldots, n$, and $v_{end} = \texttt{end}(e_n)$*

Following functions for path/node relationships (using same names as for edge/node relationships, i.e. overloading the function names) are defined:

$\texttt{start} : P \to V$ *with start node* $\texttt{start}(p) = v_{start}$ *and*
$\texttt{end} : P \to V$ *with end node* $\texttt{end}(p) = v_{end}$.

The set of all such paths is denoted by P. In order to define the ML-To patters we need an additional description in the above given definitions to differentiate between the links and path on the different network layers. Therefore a refinement per layer – nodes, links, (and consequently paths) pertain to one particular layer $i \in I$ only and are connected only within the same layer – is needed. These is the layer-dependent definition for layer $i \in I$:

Definition 3. *Node, link, path layer-dependent definition*

In the layer-independent definition for link, node and path above replace E with E^i (links on layer i), V with V^i (links on layer i), and P with P^i (paths on layer i), with $i \in I$.

4.1.2 Formalising the ML-To Patterns

Having the basic link model defined, we further provide formal descriptions of network patterns as discussed in Section 2. The description uses the basic model as an elementary building block.

Definition 4. *Basic Path Mapping*

*Given 2 paths $p^i \in P^i$ and $p^j \in P^j$ on layer i and j, respectively, with $i > j$, the **basic path mapping** between p^i and p^j is the element (p^i, p^j) of the full relation $P^i \times P^j$.*

In detail, it describes the relationship $p^i \mapsto p^j$ between the two paths
$p^i = [e^i_1, e^i_2, \ldots, e^i_n]$ *from* $\texttt{start}(p^i) = \texttt{start}(e^i_1)$ *to* $\texttt{end}(p^i) = \texttt{end}(e^i_n)$ *and*
$p^j = [e^j_1, e^j_2, \ldots, e^j_m]$ *from* $\texttt{start}(p^j) = \texttt{start}(e^j_1)$ *to* $\texttt{end}(p^j) = \texttt{end}(e^j_m)$,
i.e. especially the start/end nodes are mapped correspondingly: $\texttt{start}(p^i) \mapsto \texttt{start}(p^j)$ *and* $\texttt{end}(p^i) \mapsto \texttt{end}(p^j)$.

Definition 5. *Set-theoretic notation for link segmentation pattern*

A single basic path mapping can be directly used to represent a link segmentation pattern: a link segmentation $p^i = [e^i_1, e^i_2] \mapsto p^j = [e^j_1, e^j_2, \ldots, e^j_n]$ (compare Figure 2(a)) with $i > j$, is represented by (p^i, p^j) or more general by the singleton $\{(p^i, p^j)\} \subset P^i \times P^j$ (to make it compatible with the following notations for the other two patterns).

Definition 6. *Set-theoretic notation for link bundling pattern*

A link bundling is denoted by a set of related basic path mappings:
given a path $p^i \in P^i$ on layer i and n bundled paths $p^j_1, p^j_2, \ldots, p^j_n \in P^j$ on layer j with $i > j$, $\texttt{start}(p^j_k) = v^j_{start} = \texttt{const}$ *, and* $\texttt{end}(p^j_k) = v^j_{end} = \texttt{const}$ *($k = 1, \ldots, n$),*

the subset $\{(p^i, p_1^j), (p^i, p_2^j), \ldots, (p^i, p_n^j)\}$ *of* $P^i \times P^j$ *represents the corresponding link bundling* $p^i \mapsto p_1^j, p_2^j, \ldots, p_n^j$ *(compare Figure 2(b)).*

Definition 7. *Set-theoretic notation for link sharing pattern*

A link sharing is also denoted by a set of related basic path mappings:
given n *(multiplexed) paths* $p_1^i, p_2^i, \ldots, p_n^i \in P^i$ *on layer* i *and the shared path* $p^j \in P^j$ *on layer* j *with* $i > j$, $\texttt{start}(p_k^i) = v_{start}^i = \texttt{const}$ *, and* $\texttt{end}(p_k^i) = v_{end}^i = \texttt{const}$ *(*$k = 1, \ldots, n$*), the subset* $\{(p_1^i, p^j), (p_2^i, p^j), \ldots, (p_n^i, p^j)\}$ *of* $P^i \times P^j$ *represents the corresponding link sharing* $p_1^i, p_2^i, \ldots, p_n^i \mapsto p^j$ *(compare Figure 2(c)).*

We described here the way the ML-To patterns proposed in Section 3 can be formalized: so each of the three link topology patterns (for layers $i > j \in I$) is represented as a relation between P^i and P^j (i.e. a subset of $P^i \times P^j$)

Nevertheless as we cannot find in real systems a pure form of these patterns the capacity to combine them essential. This has also to be formalized as well:

The combination of segmentation pattern with either bundling or sharing is already subsumed in the respective notations for bundling/sharing, as both are based on the definition of a basic link mapping (which subsumes segmentation as a particularization, compare above definition 5)

So it is left to show that the combination of bundling + sharing can be represented using these definitions.

A combination of n multiplexed links sharing on layer i a bundling of m links on layer j (with $i > j$) $p_1^i, p_2^i, \ldots, p_n^i \mapsto p_1^j, p_2^j, \ldots, p_m^j$ with
$\texttt{start}(p_k^i) = v_{start}^i = \texttt{const}$, $\texttt{end}(p_k^i) = v_{end}^i = \texttt{const}$ ($k = 1, \ldots, n$),
$\texttt{start}(p_k^j) = v_{start}^j = \texttt{const}$, and $\texttt{end}(p_k^j) = v_{end}^j = \texttt{const}$ ($k = 1, \ldots, m$),
can be represented by the relation

$\{(p_1^i, p_1^j), (p_1^i, p_2^j), \ldots, (p_1^i, p_m^j), (p_2^i, p_1^j), (p_2^i, p_2^j), \ldots, (p_2^i, p_m^j),$
$\ldots$
$(p_n^i, p_1^j), (p_n^i, p_2^j), \ldots, (p_n^i, p_m^j)\} \subset P^i \times P^j$

4.1.3 Extension for multi-domain

To support the distinction of different domains (technical and/or organizational ones, see the scenario dimension in Table 1), the set-theoretic notation for the ML-To patterns are extended:

For any layer $i \in I$ the pertaining to a particular technical/organizational is an characteristic of the nodes V^i. Therefore two functions $dom_{tech}^i : V^i \to D_{tech}$ and $dom_{org}^i : V^i \to D_{org}$ with D_{tech} and D_{org} being the sets of all potential technical and organizational domains, respectively, are introduced to model this characteristic.

Links on any layer whose start and end node pertain to the same technical resp. organizational domain, are technical resp. organizational intra-domain links, all others being technical resp. organizational inter-domain links.

This extension can be used with any combination of the notations defined for the ML-To patterns.

In Figure 4.1.3 an illustration for an example of combination with link bundling is given. For a short notation a node $v^i \in V^i$ for $i \in I$ which pertains to (technical or organizational) domain d is denoted by $v^{i,d}$. Similarly an intra-domain link $e^i \in E^i$ within domain d is denoted by $e^{i,d}$, while an inter-domain links e^i is denoted generally by $e^{i,inter}$. In the example the inter-domain path $[e^{i,inter}]$ (= $[e^i]$ with e^i being inter-domain) on layer i is based on the bundling of the two inter-domain paths $[e_1^{j,d_1}, e_2^{j,d_1}, \ldots, e_{n-1}^{j,d_1}, e_n^{j,inter}, e_{n+1}^{j,d_2}, \ldots, e_{n+m}^{j,d_2}]$ and $[f_1^{j,d_1}, f_2^{j,d_1}, \ldots, f_{k-1}^{j,d_1}, f_k^{j,inter}, f_{k+1}^{j,d_2}, \ldots, f_{k+l}^{j,d_2}]$ on layer j (the nodes of e^i being denoted by v_{start}^i and v_{end}^i, the nodes of e_x^j being denoted by $v_{x,start}^j$ and $v_{x,end}^j$ for $x = 1, \ldots, n+m$, and the nodes of f_x^j being denoted by $w_{x,start}^j$ and $w_{x,end}^j$ for $x = 1, \ldots, k+l$).

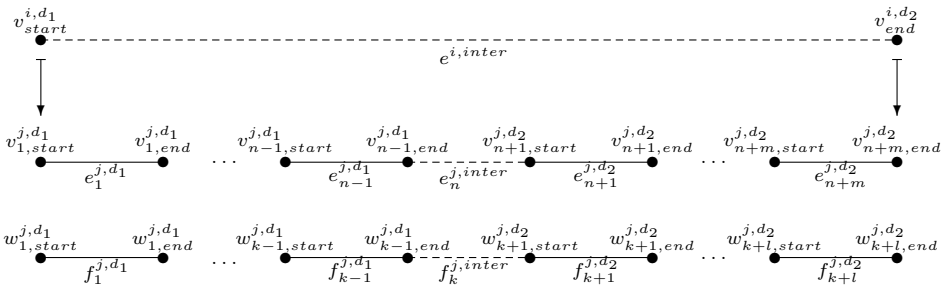


Figure 4: Example illustration of multi-domain mapping, combined with link bundling

4.2 Other Model-based Perspectives

In the former section the information model as base for multi-domain/multi-layer monitoring has been described. In order to fulfill the management architecture some more components should be described. These are not a main part of this paper but for the sake of completeness this will be here mentioned only. The *functional model* has to underline the most important functionalities concerning multi-domain/multi-layer monitoring based on the information model. The *organizational model* should reveal the roles and responsibilities in intra-/inter-organizational environments that are required in order to conduct efficient the multi-domain/multi-layer monitoring. Last but not least the *communication model* should deliver the required information communication exchange measures and procedures.

5 Existing Approaches

Given the importance of ensuring network stability and robustness, a plethora of researches have been done in the area of network monitoring. One of the ultimate goals of the invested efforts, above all, is to perform better network fault management based on the monitoring information in terms of time and accuracy. Nevertheless, the importance of the aforementioned cross-layer and cross-domain aspects in real-world network operation scenarios has been unfortunately understated. As revealed by our survey of related works, much effort has resulted in *partial solutions*, which means those solutions are specially tailored for some aspects of network monitoring and fault localization challenges as posed previously.

A survey from Sethi et al. [S+04] documents fault localization techniques which covers AI techniques, model traversing and fault propagation models. Most of the surveyed approaches are limited to academic discussions based on relatively simple network models. A special attention has been given to approaches based on inference techniques such as neural networks, decision trees and Bayesian networks, etc. Among others, issues concerning multi-layer fault localization and temporal correlations are regarded as open problems, thus no solution is presented. Challenges regarding network monitoring and fault localization across multiple domains are not discussed at all. IETF RFC 3386 [LMB+02] provides a solid groundwork and a useful reference for the further discussion of network monitoring across layers and domains. Even if the discussion focuses on the hierarchy and multi-layer *survivability*, however, terminology and concepts posed in the work can be directly applied in our discussion. Mas et al. [MT00] propose an algorithm for locating soft and hard network failures in WDM networks. Their approach mainly concentrate on the fault localization of WDM networks (ISO/OSI layer 1). Kompella et al. [KYGS05, Kom07] present a risk-modeling based method to facilitate fault localization in IP backbone network, in the meanwhile, it is also possible to detect and locate silent failures (so-called *network blackhole*). The suggested approach is mainly focused on locating faults at IP level. Also the inter-domain aspect is not considered as well. Pal et al. [PPM+08] show in their work a scheme for detecting and locating multiple failures in WDM optical networks. Their approach is confined to layer 1. The work from Dhamdhere et al. [DTDD07] proposes an algorithm called NetDiagnoser to identify fault locations with the ability to perform multi-AS network troubleshooting. The approach is based on an extend Boolean tomography approach. However, the proposed algorithm works sheerly based on layer 3 network links. Xie et al. [XFY09] approach the challenge of cross-domain fault localization by applying the graph-digest based methods, including isolated inference, full disclosure and privacy preserving collaboration. Their proposed approaches considers different degree of information sharing between domains, ranging from totally uninformed inference to full collaborative data-sharing. The issues regarding collaborations throughout vertical network layers remains unanswered in their suggested approaches. Marcu [Mar11] proposes an architecture concept for inter-organizational fault management. It is designed to facilitate collaborations between organizations with regard to life cycle of faults of networked services. Such an architecture can be extended and applied as a information interchange platform for the cross-layer, cross-domain fault localization. In the context of management of future Internet, Liu [Liu11, Liu09] pro-

poses to apply AI-based planning technique as a viable method to compose management action plans automatically. With a slight modification of the planning knowledge, such an approach can be used to encode fault localization procedural knowledge which is otherwise impossible. Based on the formalized planning knowledge, the planning engine then can make context-based decisions and compose one or several fault localization action plans. Event correlation for fault diagnosis is treated in the work of Hanemann [Han07], in which he proposes a framework to perform fault diagnosis using a hybrid approach involving event correlation and case-based reasoning techniques. Valta [Val90] proposes a formal description method for heterogeneous networks, which relies on graph-theoretical based approach called *layered attributed graph* to model networks. This work lays a solid foundation, on which we build our approach by integrating the inter-domain perspective and more detailed link patterns (as illustrated in Figure 2).

6 Conclusion and Future Work

With proliferation of large scale network services with high requirement on link qualities, network monitoring for fault localization across different domains becomes unprecedentedly important for the network management operations. To perform accurate fault localization, aggregation of monitoring data from different network layers also plays a decisive role, by which fault data could be correlated to precisely pinpoint the fault locations. Thus a precise and effective monitoring approach for fault localization of large scale network service should consider not only the multi-domain aspect, but also multiple data obtained from different participating domains. Despite of its importance and many invested efforts, multi-layer monitoring across domains boundaries has not been fully understood and the corresponding problematics are not throughly defined.

To fill-in this gap, in this paper we systematically analyzed and discussed network monitoring with consideration on the multi-layer and multi-domain aspects. We approach the problematic with a rather detailed deliberation and observation on the research challenges. We then establish a comprehensive problem dimension room which captures the essential factors as references for providing a solution. The problem dimension room is built based on the multi-layer/topology patterns we identified. Finally we provided a formally defined information model based on the set-theoretical principle. Additionally to its conciseness and clarity, a mathematically well-formulated model has the advantage of flexibility, by which mathematical operations could be performed to manipulate and operate on data. Having the information model formalized, one of our future work will discuss a set of mathematical operations that can be performed to extract relevant informations. Those operations could be then mapped to the programming languages by implementations of the information model. Since our work in this seminal paper currently concentrates on the information modeling, in our further work, we will give a detailed treatments on the other crucial aspects which include organizational model, communication model and functional model. Furthermore, our effort will be also dedicated to the adaptation of the presented information model to real-world scenarios, such as management of E2E links provided in Géant.

Acknowledgment

The authors wish to thank the members of the Munich Network Management Team (MNM-Team) for helpful discussions and valuable comments on previous versions of this paper. The MNM Team directed by Prof. Dr. Dieter Kranzlmüller and Prof. Dr. Heinz-Gerd Hegering is a group of researchers at Ludwig-Maximilians-Universität München, Technische Universität München, the University of the Federal Armed Forces and the Leibniz Supercomputing Centre of the Bavarian Academy of Sciences and Humanities. See http://www.mnm-team.org/

References

[DTDD07] A. Dhamdhere, R. Teixeira, C. Dovrolis, and C. Diot. NetDiagnoser: Troubleshooting network unreachabilities using end-to-end probes and routing data. In *Proceedings of the 2007 ACM CoNEXT conference*, page 18. ACM, 2007.

[Gop00] R. Gopal. Layered model for supporting fault isolation and recovery. In *Network Operations and Management Symposium, 2000. NOMS 2000. 2000 IEEE/IFIP*, pages 729–742. IEEE, 2000.

[HAN99] H.-G. Hegering, S. Abeck, and B. Neumair. *Integrated Management of Networked Systems – Concepts, Architectures and their Operational Application*. Morgan Kaufmann Publishers, ISBN 1-55860-571-1, 1999.

[Han07] A. Hanemann. *Automated IT Service Fault Diagnosis Based on Event Correlation Techniques*. PhD thesis, Ludwig-Maximilians Universität München, 2007.

[Kom07] R.R. Kompella. *Fault localization in backbone networks*. PhD thesis, University of California, San Diego, 2007.

[KYGS05] R.R. Kompella, J. Yates, A. Greenberg, and A.C. Snoeren. IP fault localization via risk modeling. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2*, pages 57–70. USENIX Association, 2005.

[Liu09] F. Liu. The role of AI planning in the management of future Internet. In *Integrated Network Management-Workshops, 2009. IM'09. IFIP/IEEE International Symposium on*, pages 147–148. IEEE, 2009.

[Liu11] F. Liu. *Supporting IT Service Fault Recovery with an Automated Planning Method*. PhD thesis, Ludwig-Maximilians Universität München, 2011.

[LMB+02] W. Lai, D. McDysan, J. Boyle, M. Carlzon, R. Coltun, T. Griffin, E. Kern, and T. Reddington. Network hierarchy and multilayer survivability. Technical report, RFC 3386, November, 2002.

[Mar11] P. Marcu. *Architekturkonzepte für interogranisationales Fehlermanagement*. PhD thesis, Ludwig-Maximilians Universität München, 2011.

[MT00] C. Mas and P. Thiran. An efficient algorithm for locating soft and hard failures in WDM networks. *Selected Areas in Communications, IEEE Journal on*, 18(10):1900–1911, 2000.

[PPM+08] A. Pal, A. Paul, A. Mukherjee, M. Naskar, and M. Nasipuri. Fault detection and localization scheme for multiple failures in optical network. *Distributed Computing and Networking*, pages 464–470, 2008.

[S+04] A.S. Sethi et al. A survey of fault localization techniques in computer networks. *Science of Computer Programming*, 53(2):165–194, 2004.

[SS02] M. Steinder and A.S. Sethi. End-to-end service failure diagnosis using belief networks. In *Network Operations and Management Symposium, 2002. NOMS 2002. 2002 IEEE/IFIP*, pages 375–390. IEEE, 2002.

[Val90] R. Valta. *Entwicklung einer Methodik zur Beschreibung von offenen Rechnernetzen als Grundlage für integrieretes betrieberorientiertes Netzmanagement*. PhD thesis, Technische Universität München, 1990.

[XFY09] G.G. Xie, W.D. Fischer, and J.D. Young. Is Cross-Domain Fault Localization Feasible, 2009.

[YHL+10] M. Yampolskiy, W. Hommel, B. Lichtinger, W. Fritz, and M.K. Hamm. Multi-domain End-to-End (E2E) Routing with Multiple QoS Parameters-Considering Real World User Requirements and Service Provider Constraints. In *Evolving Internet (INTERNET), 2010 Second International Conference on*, pages 9–18. IEEE, 2010.

G-Lab - an Experimental Facility for Future Internet Research and its International Context

Paul Müller, Dennis Schwerdel
Integrated Communication Systems Lab
University of Kaiserslautern
Paul-Ehrlich-Straße, Gebäude 34
67663 Kaiserslautern
pmueller, schwerdel@informatik.uni-kl.de

Abstract: The G-Lab project aims to investigate new networking paradigms and algorithms for a future internetworking architecture in an experimental manner. Thus the G-Lab project consists of a spiral process of two major fields of activities: research studies of future network components and their experimental design within an experimental facility. Both activities are controlled by the same community to ensure that the experimental facility fits to the demand of researchers. Researchers gain access to virtualized resources or may also gain exclusive access to resources if necessary. This paper presents the current setup of the G-Lab experimental facility, and puts the platform into an international context.

1 Introduction

Today's Internet has a large economic influence but is based on mechanisms and algorithms from the 70ies and 80ies. The ever changing requirements of applications and capabilities of the transport technologies demands for changes even of the core technologies of the Internet. Thus several research efforts worldwide currently investigate concepts and technologies for new future internetworking architectures [RM08]. The goal of the G-Lab project is to foster experimentally driven research in this field.

The G-Lab project[1] has started in 2008 as a BMBF[2] funded distributed joint research and experimentation project for Future Internet studies and development between six German universities: Würzburg, Kaiserslautern, Berlin, München, Karlsruhe, and Darmstadt. G-Lab can be divided in two major interacting tasks, the Future Internet research projects and the experimental facility. That means that the G-Lab project is not limited to explore only theoretical possibilities and novel ideas but also to use experimental approaches to verify the derived results while using the experimental facility. To investigate the functional aspects of novel internetworking architecture approaches (like routing, addressing, control, monitoring & management) and their interaction with each other is such an intricate task that could not be validated only in an analytical way.

[1] http://www.german-lab.de
[2] German Federal Ministry of Education and Research, "Bundesministerium für Bildung und Forschung"

The project itself is composed in diverse working groups that are dedicated to different aspects of future Internet research, ranging from architecture to mobility and management. A special working group deals with a distributed experimental facility consisting of wired and wireless hardware with over 185 nodes, which are fully controllable by the G-Lab partners. This infrastructure provides the experimental facility to the G-Lab working groups to test their proposed approaches and ideas for the future Internet architecture. The whole network of the platform is distributed into individual clusters at the six different locations within Germany with Kaiserslautern as the main site. The first version of platform was available in March 2009 and first experiments took place at the commencement of April.

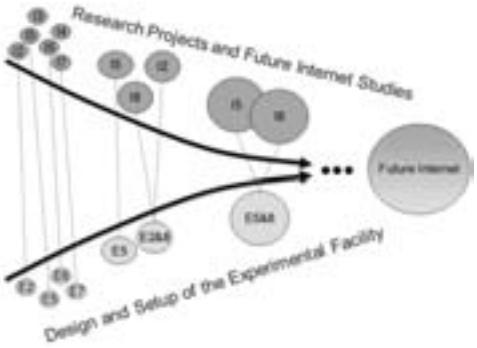


Figure 1: German-Lab philosophy

The overall goal of the G-Lab project is that theoretical research and the experimental facility will converge into a new future internetworking architecture as depicted in Figure 1. Thus it is important that the experimental facility is flexible enough to adapt to the needs of the experiments and ultimately become a research field in itself. With this interwoven approach G-Lab avoids the situation that the platform providers offer their services but nobody is going to use it.

2 Experimental Facility Design

In the design of the G-Lab experimental facility [SGH+10] it has been an important point to use existing solutions, adapt them if needed and integrate them. Thus it was possible to build up a running testbed very quickly. The usage of free and mostly open source software solutions allowed to use the full budget for hardware equipment and also makes it easy to adapt the used software.

2.1 Hardware Layout

The hardware equipment consists of three types of nodes and one switch per site. The nodes can be classified in the following category types:

NormalNode: This is the standard type of node, which can be used to run networking tests and computations. These nodes contain two Xeon Quadcore Processors with 16 GB of RAM, 500 GB of HDD and four gigabit Ethernet interfaces.

NetworkNode: The second node type is designated for special networking tests requir-

ing more network interfaces. To facilitate Emulab-like experiments, the network nodes differ from the normal nodes in the sense that there are eight gigabit Ethernet interfaces.

HeadNode: The last type is acting as a head node and manages the local site. This node differs from the other types by a faster CPU and much more disk space.

After vigorous scrutiny, Sun Microsystems and Cisco Systems have been chosen as hardware providers for the facility. All the nodes include a dedicated service processor, i.e. a small computer that allows controlling and monitoring the hardware remotely with a special management network interface. Each site has one head node, two network nodes and a variable amount of normal nodes. The networking equipment consists of a layer-3 switch from Cisco Systems (Catalyst 4500 E Series).

2.2 Network Setup

All nodes of a site are located in one network segment interconnected by the switch, which has been split into two virtual switches using VLANs. The public part contains all interfaces of the normal and network nodes and all except one interface of the head node. The private part contains all management interfaces of the service processors and one normal interface of the head node. Both networks are completely separated and only the public network has an uplink to the Internet. With this separation the access to the service processors can be controlled by the head node.

Public IP addresses are needed for all interfaces of each node (except management interface). The addresses are distributed by the head node using DHCP. Global DNS records are managed by the main site (Kaiserslautern), a site-specific zone is delegated to each site to allow decentralized DNS management.

Some sites have policies denying externally controlled nodes with IP addresses in the address range of that site, because some access rules are based on IP ranges. In this situation special firewall rules have been set up that blocks all communication between the nodes and the rest of the site except a few defined proxy hosts.

2.3 Headnode Structure

In the initial design of the experimental facility the head node has an operating system running directly on the hardware, which has early been recognized as being inflexible. Now the head node has been virtualized and separated in a couple of virtual machines. This has some major advantages:

- Different functionality can be separated into different virtual machines. This even allows for different operating systems (e.g. Fedora Linux and Debian Linux) running on these machines.

- Virtual machines allow easy backups with snapshots of running machines.
- Virtual machines can be cloned and the clone can then be used for development and testing purposes, it can even be sent to other sites.
- The virtualization host provides a remote control (e.g. console login) over the virtual machines which are an additional way of access in case a virtual machine is not working properly.

As a virtualization solution Proxmox VE is being used but other solutions like VMWare, Xen [BDF+03] and VirtualBox[3] are also being examined. Currently the head node in Kaiserslautern (main site) has virtual machines for monitoring (section 2.6), PlanetLab Central (section 2.5), website, user database, a file server, the head node software and various machines for testing purposes.

The headnode software manages and controls all local nodes at a site. It provides the following services:

- Administration of the local network segment using DHCP.
- Provision of boot images for the associated nodes using PXE netboot (see section 2.4).
- Administration of access to the management interfaces of the local nodes via VPN.
- Proxy for monitoring that allows the central monitoring server to monitor the management interfaces (see section 2.6).

This system is provided as a set of Debian packages. So, all sites have the same base system consisting of software from a shared repository.

2.4 Flexible Software Deployment

The headnode software of the local site provides boot images for the nodes via PXE[4] Netboot. Thus any boot image can be booted on any node. In the context of German-Lab we define three categories of boot images:

1. PlanetLab boot image (described in section 2.5): This allows a node to boot the PlanetLab software which is the default. This boot image contains a part that is specific to each node.
2. Virtualization boot image: This kind of boot image provides virtualization with access for all German-Lab users. Thus users can use nodes booted with this image to run custom software images by means of the used virtualization technology. The

[3] http://www.virtualbox.org
[4] Preboot Execution Environment

default virtualization boot image is Proxmox VE. which provides both OpenVZ virtualization and and KVM[5].

3. Custom boot images: This kind of boot image contains a system designed by a user and only allows access to a limited user group specified by the system itself.

There is a clear trade-off between access for more users and more privileges for users. PlanetLab provides a very good virtualization when measured in the number of concurrent users that it allows, but it is very limited in the hardware access it provides (e.g. only TCP and UDP sockets, no raw sockets). Custom boot images can provide full hardware access and also allow for kernel modifications but restrict the number of users that can access the node.

The German-Lab experimental facility allows both, access for all users to almost all nodes (PlanetLab software is the default) and full access to a few nodes if needed. A central management platform for distributing boot images and assigning them to the nodes called "Boot Image Management" (BIM) has been developed.

2.5 PlanetLab Infrastructure within G-Lab

PlanetLab [PBFM06, Fiu06, PR06] is a software environment, that allows to virtualize nodes using the VServer technology and which provides a central managing and control platform. There is also a testbed called PlanetLab (for which the software has been designed) with which we do not currently share resources.

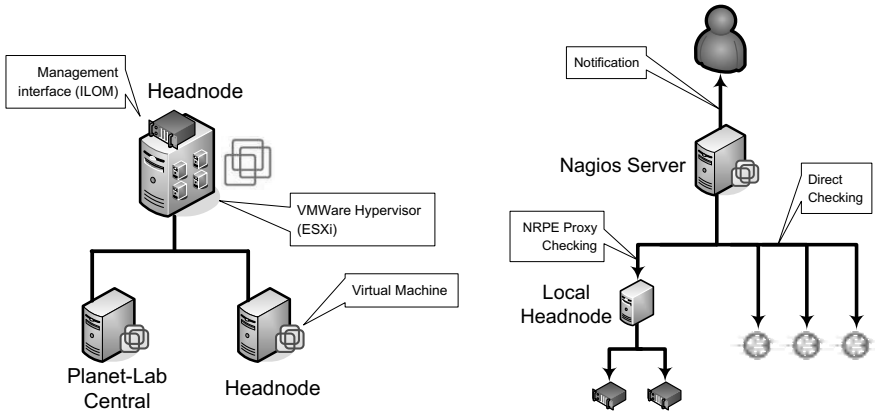
The PlanetLab software consists of a central server called PlanetLab Central (PLC) and a boot image for all nodes. On the PLC all sites, users and nodes can be configured and a custom boot image for each node can be generated.

In German-Lab the PLC runs in a virtual machine on the head node in Kaiserslautern. In the PlanetLab testbed the boot image is booted from a CD or a USB device but in German-Lab that has been modified to be used as a PXE boot image that is provided by the head node software at each site. Figure 2a shows how the PlanetLab software is used in German-Lab. Administrators configure the node on the PLC, which then provides a custom boot image. This boot image is used on the local headnode to boot the node via PXE. Once the node is booted, the node only communicates with the PLC and the users.

2.6 Central Monitoring

The monitoring of the entire infrastructure is also part of the goal. A dedicated virtual server in Kaiserslautern is used for the monitoring infrastructure. The software Nagios[6] is being used to collect monitoring data of individual hosts and services and notify adminis-

[5] http://www.linux-kvm.org
[6] http://www.nagios.org



(a) Planet-Lab usage

(b) Monitoring of the G-Lab Platform

Figure 2: German-Lab Structure

trators by e-mail when problems occur. Information that is currently monitored is:

- Resource usage (CPU, memory, disk, etc.) on all virtual machines
- Hardware health of all nodes (using the service processors)
- Availability of all nodes and service processors

Some of this information is not visible for the monitoring server like resource usage on distant hosts and information of hosts that are not visible from the server like the service processors. To allow the monitoring of these hosts and services the Nagios Remote Plugin Executor (NRPE) software is being used as a proxy. NRPE is a server that allows specified hosts (i.e. the G-Lab monitoring server, see figure 2b) to execute preconfigured commands. With this proxy both internal data and hidden hosts can be checked.

To configure the data for the Nagios software (e.g. hosts, services, check commands, users), Nagios Administrator[7] is used. The monitoring information can be visualized in two ways:

1. A structure diagram gives the current state of each host or host group with green, yellow or red lights. The NagVis[8] software is used for this purpose.
2. Using PNP4Nagios[9] the history of monitored values can be visualized in a time-line graph for each host and each service.

[7] http://www.nagiosadmin.de
[8] http://www.nagvis.org
[9] http://www.pnp4nagios.org

The web-frontends of Nagios, the Nagios Administrator and both visualization tools have been combined in a central website[10]. Of course all monitoring information is also being stored in log files so that future visualization or analysis can work on the history too. The G-Lab monitoring architecture has been valuable since it was deployed and helps to detect and solve problems quickly. Problems that can be fixed without hardware change have frequently been solved within a few hours.

2.7 Design Support for Experiments

A lot of software for experimental facilities has been developed and each one works at a certain level of realism, concurrency and repeatability. The German-Lab experimental facility allows its researchers to choose from various experimental facilities software tools. Within the G-Lab project special software tool for designing and deploying experiments to the experimental facility was developed. This software tool is called Topology Management Tool (ToMaTo)[SHG+11, SRM11b]. ToMaTo allows researchers to create virtual network topologies populated by virtual nodes running standard software. It is a design goal of ToMaTo to overcome limitations found in experimental facility software so that the user has maximal flexibility for his experiments. ToMaTo allows its users to configure and use multiple concurrent network topologies. It also aims to allow lightweight virtualization and full operating system access for the experiments .

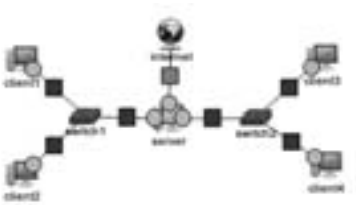


Figure 3: An example topology

The goal of ToMaTo is to enable users to create and use network topologies for their experiments. A network topology consists of two types of components. Devices are active components like computers that run the software of the experiment and are the only sources and sinks of data. Connectors are network components that connect devices and transport their data exhibiting certain configurable characteristics. Figure 3 shows a topology with four client devices, one server device, two switch connectors and one Internet connector.

Figure 4: ToMaTo graphical front end

[10] http://nagios.german-lab.de

ToMaTo uses virtualization technologies to allow experiments to run concurrently in isolated environments spanning parts of the experimental facility. ToMaTo consists of three modules, the host system, the central back-end and the web-based front-end (http://tomato.german-lab.de) as shown in figure 4. The host system runs on all hosts of the experimental facility and offers virtualized resources to be controlled by the central back-end. The host hypervisor consists of a Linux operating system with the following additional components installed:

- PROXMOX VE[11] as virtualization tool for virtual machines
- Tinc[12] as virtualization tool for virtual networks
- TC/Netem as a link emulation tool

2.8 Experiment example

A lot of experiments used or still use the German-Lab experimental facility to develop, test, analyze or evaluate different aspects in the field of future networking. One experiment [SRM11a] that has been run on the experimental facility demonstrates[13] the usage and benefits of ToMaTo in protocol analysis with the scenario of malware analysis. Malware poses a huge security thread on Internet users as it has access to all data on the computer, can record user actions without the knowledge of the user and send this data over the Internet. The most common kind of malware allows the attacker to control the computer remotely and use it to launch other attacks and send spam mails. This way malware is currently responsible for most attacks and spam mails in the Internet.

An analysis of the communication protocol between the malware on the victims computer and the attacker can lead to methods to detect infected computers and quarantine them. Flaws in the communication protocol might offer a way to destroy the overlay network of the infected computers and thus break the control of the attacker. Although only a disinfection of the infected computer can completely remove the malware containment and attacks on the communication infrastructure of the malware network can prevent the disclosure of private user data as well of attacks and spam mails sent by the infected computer.

In this experiment, the communication between the malware instance and its control server could be captured in a secure way. The analysis revieled information like the address of the control server and the protocol that is used to communicate.

[11] PROXMOX VE is a product of Proxmox Server Solutions GmbH, see http://pve.proxmox.com
[12] Tinc is a VPN software project by Tilburg university, see http://tinc-vpn.org
[13] http://dswd.github.com/ToMaTo/presentations/malware_euroview2011.html

2.9 Identity Management

The user management is an important part of the experimental facility and the project because G-Lab is a closed environment in contrast to comparable infrastructures like PlanetLab. While PlanetLab is open to everyone who joins the project with at least two systems, G-Lab is only open to registered users of the G-Lab project. Especially the organization of the identity of a user and his access rights is a critical issue in public available experimental facility design. In case of the G-Lab project the user management is necessary in two different areas, the infrastructure services, and the testbed platform itself.

The infrastructure services consist of the internal and external project documentation area, mailing lists, help desk, and software management. The testbed itself can be divided into a management and experimenter view. The experimenter requires access to the nodes and testbed resources on several layers. As standard software in G-Lab, the PlanetLab environment is used, also for the management of access rights. For deploying and operating specialized images a central account management is provided.

The administration of the users and system resources is done by a distributed administration team organized as a subproject of the overall G-Lab project. Each site might have some equipment, but at least users for the facility equipment. The approach distributes the responsibilities for the users assigned to a specific site to a representative of this site. This procedure requires additional role and access rights assignments for an extended group of identities. For example the headnodes, the node management and monitoring, and the private PlanetLab node administration are typical tasks, which are delegated to site representatives. Also a site representative has to organize the experiments and the resource usage of that site.

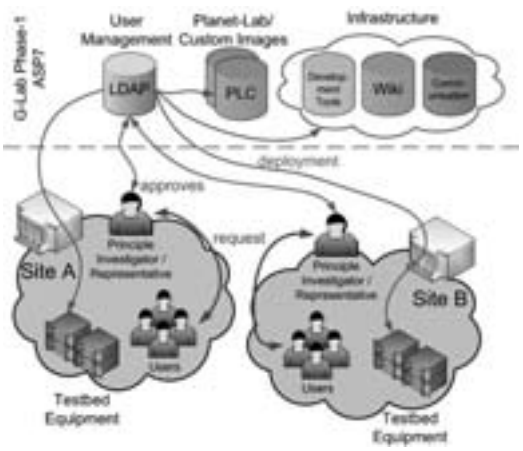


Figure 5: ToMaTo graphical front end

Figure 4 shows an architectural overview of the technical structure of the G-Lab identity and role dependency management. In general a central LDAP server stores the user's identities in a separate subtree, which is suborganized in subtrees containing the users of a specific site. A basic rule is that an identity is not associated with any access rights. This is organized in a separate tree, the so called group tree. Each service is represented by a unique group, which grants its members access to this server. A third separate subtree organizes virtual identities on machine level, so that each site has its own system level access user. This enables a fine grained and easy manageable environment on site level, even in case of changes. For services like the private PlanetLab installation account synchronization will be realized, so that the central LDAP database serves as master environment.

This can easily be extended to future services, if required. The management of the central database is done by a set of scripts, which respect a set of defined default roles for specific tasks. Also these scripts verify the integrity of the stored user data.

3 International Approaches

As mentioned above, the future of the Internet is a global issue which is tackled by activities around the world, for example PlanetLab, GENI (Global Environment for Network Innovations, US) and JGN2plus (Advanced Testbed Network for R & D, Japan), just to name a few. On a European scale, there are several national initiatives and projects which have similar or complementary objectives as G-Lab has. There are projects in France RNRT (French Research Network for Technological Innovation), ICT SHOK (Finnish Future Internet Research Programme), Ambient Sweden, Internet del Futuro (Spain).

But also under the umbrella of the European Commission within the 'Cooperation' program theme Information and Communication Technologies (ICT) of the 7th Framework Programme FP7 (2007 – 2013) of the European Community the "Future Internet Research & Experimentation" FIRE program was launched[14]. The FIRE initiative creates an open research environment, which facilitates strategic research and development on new Internet concepts giving researchers an instrument to carry out large-scale experimentation on new paradigms, across all levels and layers. It is the aim of the FIRE Facility to support Future Internet research in Europe, in a sustainable demand-driven way, which is independent from the program, the research is funded under. The Projects PanLab and OneLab, as well as their successors (OneLab2 and PII) are investigating possible organizational and business models for such a facility. As a result, FIRE will strengthen the competitive position of European research and industry in the important domain of Internet technologies and services. Figure 5 gives an overview about projects under the FIRE umbrella.

Starting from summer 2010, a second wave of projects with a budget of 50 million Euro is significantly expanding the scope of FIRE, moving it in new directions taking on technologies such as sensor networks, clouds and also high level service architectures. A more detailed description of some FIRE projects can be found in [FM10].

Another important project which must be mentioned here is the GENI[15] (Global Environment for Network Innovations) project which is a unique virtual laboratory for at-scale networking experimentation across the US under the auspices of the NSF (National Science Foundation). The GENI mission is to:

open the way for transformative research at the frontiers of network science and engineering; and inspire and accelerate the potential for groundbreaking innovations of significant socio-economic impact.

This project which is more or less an infrastructure oriented project comparable to the FIRE program is accompanied by a more research oriented program from NSF called

[14] http://cordis.europa.eu/fp7/ict/fire/fire-fp7_en.html
[15] http://www.geni.net/

NeTS[16] (Networking Technology and Systems). While GENI is comparable with FIRE and the experimental facility part of G-Lab the NeTS-projects can be compared with the more future internetworking architecture part of G-Lab.

While in the past all these projects were more or less focused on infrastructure and the core mechanisms of the Internet there are recent signs of a focus shift towards applications. In the European context a PPP[17] (public private partnership) program was launched last year (2011) which follows an industry-driven approach and works on research and development in network infrastructures, devices, software, service and media technologies. In parallel, it promotes its own experimentation and validation platform, bringing together demand and supply and involving users early in the research lifecycle. The new platform will thus be used by range of actors, in particular SMEs and Public Administrations, to validate the technologies in the context of smart applications and their ability to support user driven innovation schemes.

Comparable to the European PPP program the NSF started the US-IGNITE[18] program which is a Public-Private Partnership for the development of gigabit applications and services in areas of national priority[19] based on ultra-high speed (>100 Mbps symmetric) networks and deeply programmable (allowing new internet architectures and protocols), and sliceable (allowing isolated experiments or services running in parallel) network testbeds.

Last but not least, the AKARI[20] Architecture and Design Project in Japan should be mentioned. The goal of this project is to implement the basic technology of a new generation network by 2015, developing a network architecture and creating a network design based on that architecture. The overall philosophy is to develop an ideal solution by researching new network architectures from a clean slate without being impeded by existing constraints. Based on these new architectural ideas a new network will be designed and a migration path from today's conditions will be considered using these design principles. The overall goal is to create an overarching design of what the entire future network should be. To accomplish this vision of a future network embedded as part of societal infrastructure, each fundamental technology or sub-architecture must be selected and the overall design simplified through integration.

4 Conclusion & Future Work

On a technical level the German-Lab platform can currently be used to run different algorithms either using the PlanetLab software, in a virtualized system or in a custom system directly on the hardware. This provides maximal flexibility for experimenters and thus increases the usage of the platform. In the future the components of the platform will be integrated even more. Currently some efforts are under way to ensure the sustainability

[16] http://www.nsf.gov/funding/pgm_summ.jsp?pims_id=503307

[17] http://www.fi-ppp.eu/

[18] http://www.nsf.gov/cise/usignite/

[19] advanced manufacturing, health, education, energy, economic development, transportation, and public safety/emergency

[20] http://akari-project.nict.go.jp/eng/index2.htm

of the experimental facility which is more than generating some money to keep paying hardware, software and personal expenses. Long-term, organizational sustainability involves four main dimensions, including strategic, programs, personnel and finances. So for the near future we first take attention to the first three dimensions of sustainability, then financial sustainability is much more likely to occur – and much easier to accomplish.

In the past months there were several discussions, especially with industrial partners, in order to clarify whether such a platform could be used under commercial terms and conditions. It has been experienced that manufacturers are interested and forced by quality control services to test and verify their products in a "real" environment before bringing it into the market. This gives G-Lab as a developed platform extra importance in commercial market besides many infrastructure providers also shown the interest to test their product in a "post-IP" environment.

References

[BDF+03] Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T. L., Ho, A., Neugebauer, R., Pratt, I., and Warfield, A. Xen and the art of virtualization. In Scott, M. L. and Peterson, L. L., editors, *SOSP*, pages 164–177. ACM, 2003.

[Fiu06] Fiuczynski, M. E. PlanetLab: overview, history, and future directions. *Operating Systems Review*, 40(1):6–10, 2006.

[FM10] Fischer, S. and Müller, P. Experimentalforschung für das Future Internet - deutsche und europäische Initiativen. In *Springer Verlag*, February 2010.

[PBFM06] Peterson, L. L., Bavier, A. C., Fiuczynski, M. E., and Muir, S. Experiences Building PlanetLab. In *OSDI*, pages 351–366. USENIX Association, 2006.

[PR06] Peterson, L. L. and Roscoe, T. The design principles of PlanetLab. *Operating Systems Review*, 40(1):11–16, 2006.

[RM08] Reuther, B. and Müller, P. Future Internet Architecture - A Service Oriented Approach. In *In it - Information Technology, Volume 50, Number 6, 2008, Oldenbourg Verlag, Munich*, 2008.

[SGH+10] Schwerdel, D., Günther, D., Henjes, R., Reuther, B., and Müller, P. German-Lab Experimental Facility. In *Future Internet - FIS 2010*, 2010.

[SHG+11] Schwerdel, D., Hock, D., Günther, D., Reuther, B., Tran-Gia, P., and Müller, P. ToMaTo - a network experimentation tool. In *7th International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities (TridentCom 2011)*, April 2011.

[SRM11a] Schwerdel, D., Reuther, B., and Müller, P. Malware Analysis in the ToMaTo Testbed. In *Proceedings of EuroView2011*, 2011.

[SRM11b] Schwerdel, D., Reuther, B., and Müller, P. The Topology Management Tool - A demonstration. In *Next Generation Internet (NGI), 2011 7th EURO-NGI Conference on*, pages 1 –2, june 2011.

Exemplarisches Langzeitreporting von Netzverfügbarkeiten

Uwe Hillmer
Regionales Rechenzentrum Erlangen (RRZE)
Martensstrasse 1, 91058 Erlangen
uwe.hillmer@rrze.uni-erlangen.de

Zusammenfassung: So wie das Datennetzwerk (ISO/OSI-Ebenen 1-3) zur Abwicklung IT-gestützter Kommunikationsvorgänge von fundamentaler Bedeutung ist, stellt dessen Verfügbarkeit einen bedeutenden Parameter der Dienstqualität dar. Dies gilt insbesondere im Umfeld eines Universitätsklinikums, das nicht mehr "nur" durch Verwaltungsvorgänge geprägt ist, sondern längst auch Elemente unmittelbarer Patientenversorgung enthält (z.B. "Vernetzte Medizinprodukte"). Allerdings lässt sich die Netzverfügbarkeit auf Grund von Vielschichtigkeit (Netzkomponenten, Schnittstellen, Pfade, usw.) und unterschiedlichen Sichtweisen (Netzbetreiber, Systembetreuer, Endnutzer) schwer allgemeingültig fassen, entsprechend ermitteln und kompakt darstellen. Das RRZE (Regionales Rechenzentrum Erlangen) hat dazu als langjähriger Betreiber des Datennetzes des Universitätsklinikums (UK-Erlangen) einen pragmatischen Ansatz gewählt, danach Netzverfügbarkeiten bestimmt und den Nutzern zur Ansicht bereitgestellt. In diesem Kontext werden allgemeine Problematik, angewandte Methodik und Reporting behandelt, sowie Resultate im Gesamtverlauf von 10 Jahren betrachtet.

1 Einleitung

Je mehr die Datennetze von Institutionen, wie dem Universitätsklinikum Erlangen, die Rolle einer generellen Kommunikationsinfrastruktur einnehmen, desto bedeutender für das Unternehmen sind stabil funktionierender Betrieb und dessen Beleg. Grundlage eines zuverlässigen Betriebes bilden Netzwerkdesign und konkrete Gestaltung gemäß den lokal spezifischen Anforderungen und Gegebenheiten. Für ein medizinisches Umfeld hat der Hersteller Cisco (Marktführer im Bereich Netzwerkkomponenten) Konzepte und Richtlinien beschrieben, die eine allgemeingültige Orientierung auf aktuellem technologischem Stand darstellen, auch wenn sie sich in konkreten Umsetzungen hauptsächlich auf eigene Produkte beziehen („Medical Grade Network“, [MGN]). Zum Thema Verfügbarkeit werden vor allem redundante Konstrukte behandelt, so wie Verfahren erläutert, die für besonders kritische Anwendungen (Datacenter) automatische Problemerkennung und unterbrechungsfreies Umschalten ermöglichen sollen. Durchdachte Architekturen und besondere Vorkehrungen sind zwar

Voraussetzungen zur Erlangung „hoher“ Verfügbarkeiten, lösen aber nicht die Problematik begrifflicher Definition und praktischer Verifikation.

Zur allgemeinen Beschreibung von Verfügbarkeit in Netzen und deren Bestimmung findet man in der Literatur verschiedene Ansätze. Für Hersteller von Netzkomponenten und Hardware bedeutet Netzverfügbarkeit im Allgemeinen die Verfügbarkeit von Hardware, d.h. die Netzverfügbarkeit ist dann gegeben, wenn die Geräte ohne Ausfall ihre Funktionen erfüllen. Bei dieser Betrachtungsweise von Netzverfügbarkeit sind daher meist die Metriken Mittlerer Fehlerabstand (MTBF: „Mean Time Between Failure“, und Mittlere Reparaturzeit (MTTR: „Mean Time to Repair“) ausschlaggebend. Für eine einzelne Netzkomponente lässt sich damit die Verfügbarkeit gemäss unten angeführter Formel (I) definieren. Daraus kann eine Netzverfügbarkeit abgeleitet werden, in dem sie als Produkt der Einzelverfügbarkeiten berechnet wird [NTR, CIS]. Dies impliziert allerdings, dass das Netz nur dann als verfügbar gilt, wenn alle seine Komponenten verfügbar und Einzelausfälle statistisch voneinander unabhängig sind. Diese Betrachtungsgweise lässt zudem ausser Acht, dass ein Netz auch dann nicht verfügbar sein kann, wenn etwa durch Ausfall einer Leitung Verbindungen zwischen den Komponenten gestört sind. Für den User stellt sich ein Netzausfall dar, egal ob dieser Ausfall an einem z.B. durch einen Bagger verursachten Kabelbruch oder an einer Fehlfunktion an einem Switch liegt, d.h. es muss auch die Verfügbarkeit der Verbindungen mit in die Betrachtung einfliessen [ZAH, GRE]. Darüber hinaus gibt es weitere Möglichkeiten, die Verfügbarkeit bzw. Die Nicht-Verfügbarkeit eines Netzes zu definieren: Zahemszky et al. lassen z.B. in ihre Defintion mit einfliessen, dass nicht alle Netzverbindungen gleich wichtig sind und untersuchen gewichtete Verfügbarkeiten der Verbindungen. Gleichzeitig ziehen sie weitere Faktoren wie Prozentsatz der betroffenen Nutzer, Dauer der Störung und Paketverlust mit ein. So gilt in ihrem Fall ein Netz als nicht verfügbar, wenn mindestens 20% Nutzer betroffen sind, die Störung 10s oder länger dauert und mindestens 5% der IP Pakete verloren gegangen sind bzw. keine Verbindung möglich ist. In [CIS], [GRE] und [ZOU] werden diese Ansätze gleichermassen diskutiert, allerdings fliessen hier noch zusätzlich Redundanzbetrachtungen in die Netzverfügbarkeitsbeschreibung mit ein.

Vor dem Hintergrund des hier zunächst im prinzipiellen Aufbau skizzierten Netzwerkes des Universitätsklinikums Erlangen (2 Netzwerk) wird die Verfügbarkeitsproblematik genauer erläutert (3 Netzverfügbarkeit). Als Beschreibung konkreter Praxis des Netzbetreibers RRZE werden angewandte Methodik (4 Messverfahren und Reporting) beschrieben, sowie zusammenfassende Messdaten über Verläufe von 10 Jahren dargestellt und besprochen (5 Langzeitverlauf). Schliesslich regen verschiedene Punkte zur Weiterentwicklung an, nach denen Netzverfügbarkeiten noch genauer und zielgerichteter bestimmt werden könnten (6 Ausblick).

2 Netzwerk

Das hier betrachtete Datennetz des Universitätsklinikums Erlangen bildet die Infrastruktur IT-gestützter Kommunikation, also die Grundlage zum Transfer von Daten zwischen angeschlossenen Endsystemen (Server, Workstations, Drucker, Spezialgeräte, usw.). Es behandelt die untersten drei Ebenen des ISO/OSI-Referenzmodelles, die sich in der Umsetzung durch die Begriffe „Strukturierte Verkabelung“ (physikalische Ebene 1), „Virtuelle Ethernet-LANs“ (Link-Ebene 2) und „Internet-Protokoll“ (Netzprotokoll Ebene 3) beschreiben lassen. In der Realsierung besteht das Netzwerk aus untereinander über die Verkabelung verbundenen Switchen/Routern (IP-Vermittlung, LAN-Switching) und LAN-Switchen (LAN-Switching, Anschlussports). Die Architektur des Netzes folgt einem hierarchischen Modell, das in Core (Vermittlung zwischen Bereichen), Distribution (Bereichsversorgung) und Access (Zugangspunkte für Endsysteme) gegliedert ist. Core- und Distribution Komponenten sind doppelt ausgelegt (Redundanz). Abbildung 1 stellt die Netzstruktur im prinzipiellen Aufbau schematisch dar.

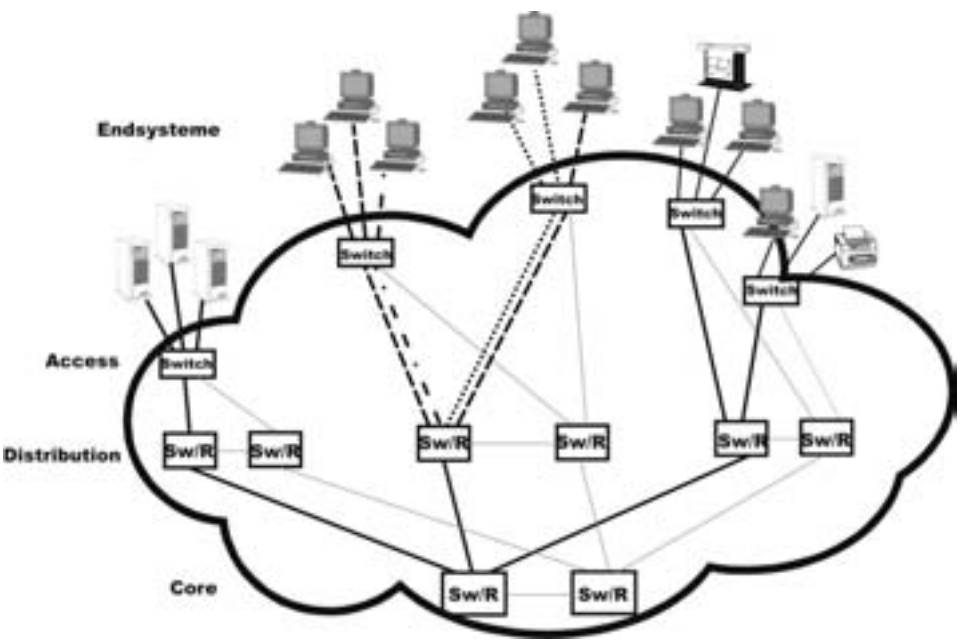


Abbildung 1: Aufbau des Netzwerkes mit hierarchischer Struktur

Entsprechend dem inneren Aufbau des Netzwerkes gliedern sich auch die Schnittstellen zu den Endsystemen in die drei unteren ISO/OSI-Ebenen, grob skizziert durch die Verbindung des betreffenden Endgerätes zum Zugangsport eines Access-Switches (Ebene 1, Link, einschlieslich zuführender Verkabelung), dem zugehörigen lokalen Netz (Ebene 2, VLAN) und einer IP-Schnittstelle für LAN-übergreifende Kommunikation (Ebene 3, IP-Defaultroute). Auch wenn das Netzwerk „einfach" strukturiert und bezüglich seiner Art aus „wenigen" Grundkomponenten zusammengesetzt ist, stellt es ein komplexes, vielschichtiges und umfangreiches Gebilde dar, dessen Verhalten und Eigenschaften in Gesamtsicht allenfalls näherungsweise zu fassen und numerisch auszudrücken sind.

Im Ausbaustand 2010 bestand das Netz aus 14 Switchen/Routern („Sw/R"), 350 LAN Switchen („Switch") mit 18300 Anschlussports zur Versorgung von 14000 registrierten Endsystemen in 380 Subnetzen (siehe dazu auch [HILL]).

3 Netzverfügbarkeit

Ein Datennetz kann als verfügbar bezeichnet werden, wenn alle seine Komponenten im Betrieb ordnungsgemäß funktionieren und die Kommunikationsanforderungen seiner Teilnehmer erfolgreich vermittelt und abgewickelt werden. Mit dieser allgemeinen Formulierung ist allerdings die Verfügbarkeit in Bezug auf ein gegebenes Netzwerk nur ansatzweise beschrieben. Für den Anwendungsfall sind u.a. konkret zu beschreiben, welche Art von Aussagen gewonnen werden sollen (Zweck, Zielvorstellung), worauf sich Aussagen genau beziehen sollen (Komponenten, Netzebenen), wie Funktionalitäten zu prüfen sind (Messmethodik) oder Ergebnisse kompakt darzustellen sind (Verfügbarkeitszahl).

Die damit verbundene vielschichtige und mehrdimensionale Problematik wird in folgenden Punkten kurz skizziert:

- **Herangehensweise (Netzbetreiber, Endnutzer)**
  Während der Netzbetreiber sich der Verfügbarkeit eher über die Betriebsbereitschaft der Geräte nähert, interessiert den Endnutzer vorrangig, ob er die gewünschten Kommunikationsbeziehungen aufbauen kann, z.B. von seiner Arbeitsplatzstation zu zentralen Servern.
- **Zu prüfende Objekte, Objektklassen, Operationen**
  Potentielle Testobjekte sind z.B. einzelne, „reale" Geräte (z.B. Router, Switche), ihre Interfaces, Links (Verbindungen untereinander), aber auch „virtuelle" Objekte und Schnittstellen (VLANs, Defaultroutes), so wie Funktionen im Zusammenwirken (Routing, Kommunikationspfade).
- **Einzel- und summarische Aussagen (Bewertung, Zusammenfassung)**
  Sowohl für komplexe Objekte (z.B. Router), als auch erst recht für ein gesamtes Netzwerk stellt sich die Frage, welche Bedeutung ermittelte Verfügbarkeiten

einzelner Elemente oder Teilbereiche für das jeweils übergeordnete Gebilde haben.

- **Definition und Bestimmung von Verfügbarkeiten bzw. Ausfällen**
  Je komplexer einzelne Objekte oder Funktionen sind, desto erforderlicher ist es festzulegen, wann sie als verfügbar bzw. ausgefallen (nichtverfügbar) gelten und mit welchen Methoden dies zu ermitteln ist.
- **Definition von Betriebszeiten (100%), Berücksichtigung von Ausfallursachen**
  Am nächsten liegt der pauschale Ansatz für die Betriebszeit (Sollzeit der Verfügbarkeit, 100%-Bezug) von 24 Stunden an allen Tagen. Er könnte aber z.B. für einzelne Netzteile oder Komponenten individuell modifiziert werden, wenn sie vorübergehend gezielt aus dem Betrieb genommen werden (geplante Unterbrechungen, Umbau/Wartung). In diesen Fällen wäre es auch vertretbar, entsprechende Ausfälle nicht als solche zu bewerten, also zur Beurteilung von Verfügbarkeit nicht zu berücksichtigen. Dies gilt für einen Netzbetreiber in gewissem Masse auch für Ausfälle, deren Ursachen außerhalb seines Einflussbereiches liegen (externe Ursachen, Stromausfälle, Störungen durch Nutzerfehlverhalten).
- **Zielsetzung, Aufwand, Werkzeuge**
  Ausgerichtet an Zielvorstellungen sind im konkreten Fall Begriffe, Parameter und Methodik zu definieren. Dabei sind erforderlicher Aufwand, verwendbare Werkzeuge, sowie personelle und technische Möglichkeiten zu berücksichtigen, d.h. unter Gesichtspunkten von Kosten/Nutzen zu bewerten.

Zur Berechnung von Verfügbarkeitszahlen gibt es verschiedene formale Ansätze. So orientiert sich zum Beispiel Formel (I) an einem Modell, in dem Betriebsstörungen als Fehler einzelner Komponenten (Geräte) erkannt, identifiziert, behoben werden und darüber entsprechend Buch geführt wird.
Sie lautet

$$Verfügbarkeit = \frac{Mittlerer\ Fehlerabstand}{(Mittlerer\ Fehlerabstand + Mittlere\ Reparaturzeit)} \qquad (I)$$

Dabei stehen der mittlere Fehlerabstand (englisch: Mean Time Between Failures) für Zeiten ohne Fehler und die mittlere Reparaturzeit (englisch: Mean Time To Repair) für Ausfallzeiten. Es wird also ausfallfreie Zeit in Bezug zur Summe aus ausfallfreier und Ausfallzeit gesetzt (Prozentwert ergibt sich aus Multiplikation des Quotienten mit 100).

Das gilt auch für einen etwas „offeneren“ Ansatz, bei dem Betriebs- und Ausfallzeiten direkt in die Berechnung eingehen, also z.B. ohne vorherige Mittelung:

$$Verfügbarkeit = \frac{(Betriebszeit - Ausfallzeit)}{Betriebszeit} \qquad (II)$$

(*Ausfallzeit* steht für die Summe aller Ausfälle eines betrachteten Zeitraums).

Beide Ansätze führen bei entsprechender Interpretation zu gleichen Resultaten, lassen aber für die Anwendung offen, auf welche Objekte oder Objektmengen sich die Formeln genau beziehen und wie die eingehenden Parameter konkret definiert und ermittelbar sind. Dies ist in Bearbeitung oben beschriebener Problematik in der Praxis spezifisch festzulegen. Daraus ergibt sich auch, dass resultierende Angaben, Auswertungen und Darstellungen immer im jeweiligen Kontext zu betrachten und nur sehr bedingt allgemein vergleichbar sind. So erfordern z.B. „garantierte" Jahresverfügbarkeiten von 99,999 % und höher (max. 5 Min. Ausfall im Jahr) nicht nur gezielte Maßnahmen der Gestaltung von Betrieb und Netzwerk, sondern auch spezifische Methoden für ihren Nachweis, abgesehen davon, dass ein solcher Wert zwar generell anzustreben, aber allenfalls in sehr speziellem Kontext tatsächlich sinnvoll anzufordern ist.

4 Messverfahren und Reporting

Das RRZE verwendet zur Gewinnung von Aussagen über Netzverfügbarkeiten einen pragmatischen, ohne großen dedizierten Aufwand umzusetzenden Ansatz mit dem zentralen Netzwerkmanagement (NMS) bzw. seiner Statusüberwachung als Ausgangsbasis. Er lässt sich wie folgt beschreiben:

- **Zweck**
  Ermittlung, Reporting und Dokumentation von Verfügbarkeitsdaten für Netzbetreiber und Nutzer(gruppen) als ein wesentlicher Aspekt der Dienstgüte.
- **Beobachtete Objekte**
  Die behandelten Objekte gliedern sich in zwei Gruppen:
  - „reale" Netzgeräte (Router und Switche) und
  - „virtuelle" Netzschnittstellen (IP-Defaultrouten von Subnetzen).
- **Einzelverfügbarkeit**
  Verfügbarkeit wird in Prozent pro Objekt berechnet nach der Formel

$$Verfügbarkeit_{Obj} = \left(\frac{Betriebszeit - Ausfallzeit_{Obj}}{Betriebszeit}\right) * 100 \qquad (III)$$

  Diese Formel, die dem oben beschriebenen Ansatz (II) entspricht, dient der monatlichen und jährlichen Berechnung prozentualer Verfügbarkeiten.
- **Parameter Betriebszeit**
  Als Betriebszeit gelten pauschal für alle Objekte 24 Stunden an allen Tagen eines Monats bzw. Jahres.
- **Parameter Ausfallzeit**
  Ausfallzeiten werden pro Objekt über die zentrale Statusüberwachung bestimmt, sie sind jeweils als die Summe aller Abschnitte zwischen „down" und „up" definiert.
- **Statusermittlung**
  Ein Objekt hat den Status „up", wenn es vom zentralen Management (NMS) erfolgreich angesprochen werden kann (über Protokolle SNMP, Ping), den

Status „down“, wenn dies nicht der Fall ist. Die Abfragezyklen liegen in der Regel zwischen 60 und 180 Sekunden.

- **Statusbedeutung**
  Der Status beurteilt neben der Funktionsfähigkeit eines Objektes auch den jeweiligen Kommunikationspfad durch das Netz (vom NMS zum Objekt) und damit auch allgemeine Grundfunktionalitäten des Netzes.
- **Anmerkung**
  Ausfallzeiten gehen unabhängig von ihren Ursachen (extern/intern, geplant/ungeplant) in die Berechnung ein. (Dagegen rechnen manche Netzprovider wie der DFN angekündigte geplante Unterbrechungen aus den Ausfallzeiten heraus).
- **Reporting**
  Die monatlich/jährlich ermittelten Einzelverfügbarkeiten werden für die Nutzer aufbereitet und über ein WEB-Interface („WEB-NMS“) zur Ansicht bereitgestellt (Reporting). Dabei sind zu jeder (der beiden) Gruppen die Objekte aufsteigend nach Verfügbarkeitswerten gelistet und „längere“ Ausfallzeiten in Kommentaren textlich erläutert und bewertet (Ursachen, Auswirkungen, Behebungen, u.s.w.)
- **Summarische Verfügbarkeit**
  In den zusammenfassenden Auswertungen werden Durchschnitts- und Minimalwerte betrachtet.

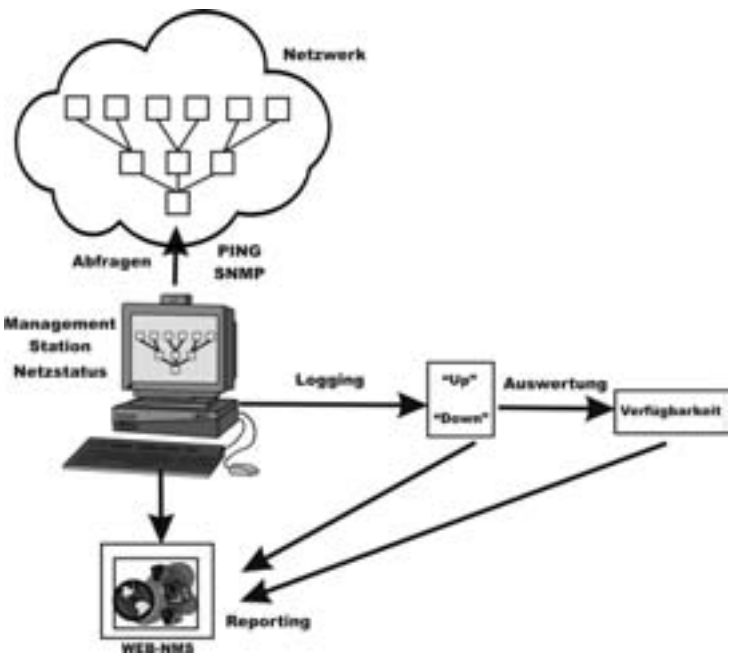


Abbildung 2: Netzwerkmanagement und Verfügbarkeitsbestimmung

In Abbildung 2 sind die Statusermittlung durch eine zentrale Managementstation, Auswertung des Loggings zur Bestimmung von Verfügbarkeiten und das Reporting der Resultate über ein für Nutzer zugängliches WEB-Interface skizziert.

5 Langzeitverlauf

Das RRZE hat nach der beschriebenen Methode ab dem Jahr 2000 Verfügbarkeiten systematisch bestimmt und dokumentiert. Bei Betrachtung und Vergleich der Resultate ist zu beachten, dass sich der Aufbau des Netzwerks im Laufe der Zeit auf Basis technologischen Fortschritts und finanzieller Möglichkeiten verändert hat und die oben beschriebene Struktur migrativ entstanden ist. Die verschiedenen Ausbau- und Entwicklungsstufen des Klinikumsnetzes sind in einem zusammenfassendem Bericht des RRZE näher beschrieben [HILL].

5.1 Verfügbarkeit von Netzgeräten (Router, Switche)

Die Verlaufsgrafik in Abbildung 3 stellt die Verfügbarkeiten aller Netzkomponenten, d.h. der Router und (zentral betreuten) LAN-Switche dar, unabhängig von ihrer Relevanz für den gesamten Klinikbetrieb. Angezeigt sind pro Jahr der jeweils minimale („Min“) und maximale (“Max“) Wert, sowie der Durchschnitt („Mittel“) über alle der erfassten Geräte. In einer 2. Minima-Kurve („Min2“) sind extreme Ereignisse mit sehr geringer Bedeutung für den Gesamtbetrieb ausser Acht gelassen, wie z.B. eine von der betreffenden Nutzergruppe initiierte lokale Stromabschaltung über die Osterfeiertage (in „kleinem“ Einzelgebäude, 2008) oder Abschaltungen im Rahmen genereller, baulicher Renovierungsmassnahmen in der Rechtsmedizin (ohne unmittelbar klinische Versorgung, 2009).

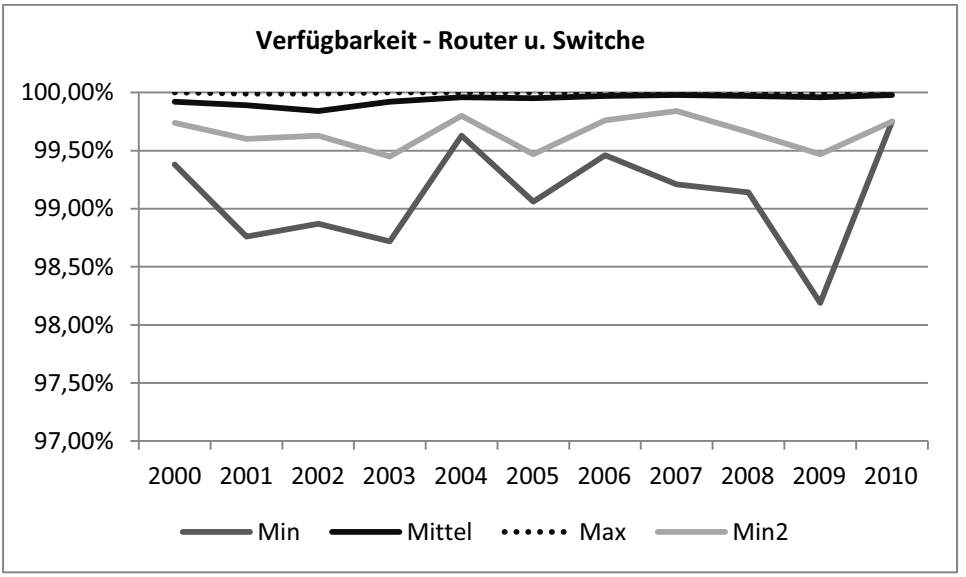


Abbildung 3: Jahresverfügbarkeiten der Netzkomponenten (Router+Switche)

Die Abstände der Verlaufskurven lassen darauf schließen, dass „relativ schlechte" Verfügbarkeiten weitgehend Einzellfällen zuzuordnen sind. „Min2" deutet an, wie durch genaue Betrachtung und Bewertung von Fehlersituatienen ein differenzierteres Gesamtbild gezeichnet werden kann.
Das Netz hatte bezüglich seiner Netzkomponenten in der Gesamtheit unabhängig von Störungsursachen, d.h. unter Einschluss extremer Sonderfälle, über die angezeigten 11 Jahre eine mittlere Verfügbarkeit von 99,93% und war in den letzten 5 Jahren im Mittel zu 99,97% verfügbar. Das entspricht einer durchschnittlichen Ausfallzeit von 6 bzw. 2,5 Stunden pro Jahr. Dabei sei nochmal angemerkt, dass diese Verfügbarkeiten verschiedene Funktionalitäten und Konnektivitäten der Komponenten beinhalten, also z.B. nicht auf reine (aktive) Standzeiten („SysUpTime") der Geräte beschränkt sind.
Unter den Netzkomponenten spielen die Router als LAN-Verteiler und Vermittler zwischen verschiedenen IP-Netzen eine fundamentale Rolle. Ihre Verfügbarkeiten werden deshalb herausgehoben und in Abbildung 4 gesondert dargestellt. Im Redundanzkonzept des Netzes werden primäre („Normalbetrieb") und sekundäre Router („Standbybetrieb") unterschieden. In zusammenfassender Auswertung sind bezüglich aller, jeweils betriebenen Router die minimalen („R-Min"), durchschnittlichen („R-Mittel") Jahreswerte dargestellt, ergänzt durch eine nur über die primären Router bestimmte Minimakurve („R-Min-P"). Desweiteren enthält die Grafik drei individuelle Kurven, die die Verfügbarkeiten des primären Routers eines Bereiches darstellen. In diesem Sinne gilt dabei eine eindeutige Zuordnung, obwohl die Router je nach Entwicklungsphase des Netzes für unterschiedliche „reale" Geräte(typen) stehen können.

Die schlechtesten Verfügbarkeiten („R-Min“: 2001, 2003) gehören zu sekundären Routern und sind daher nur mit sehr bedingtem Einfluss auf den Betrieb. Dazu ist z.B. in der originalen Jahresstatistik 2001 kommentiert („romulus“ gehört zum Bereich „sued“):

„Backup-Router romulus :
Ausfaelle auf Grund von Instabilitaeten und Tests (vornehmlich Mai und Oktober) ohne gravierende Auswirkungen auf den Betrieb.“

Der kleinste Wert eines primären Routers („R-Min-P“: 2002) fällt in die Aufbauphase eines neuen Bereiches („noz“, Neubau „Nicht Operatives Zentrum“) und steht damit für einen noch nicht voll eingeführten Regelbetrieb. Sonst liegen die Werte in jüngerer Vergangenheit tendenziell oberhalb von 99,95. In den Kurven zu den Anfangsjahren spiegelt sich wieder, wie steigende Nutzung die wenigen Router zunehmend an ihren Leistungsgrenzen belastet und zu gelegentlichen Verklemmungen geführt hat. Ihre Entlastung durch Ausbau und Einsatz von Geräten neuerer Technologie (Schnittstellen > 622 mbps statt 155 mbps, „Routing in Hardware“ statt über „CPU-Verarbeitung“) sind an jeweils deutlich verbesserten Werten abzulesen. Sie liegen ab 2004 im jeweiligen Jahresmittel oberhalb von 99,98% bzw. 1 Std. 45 Min pro Jahr.

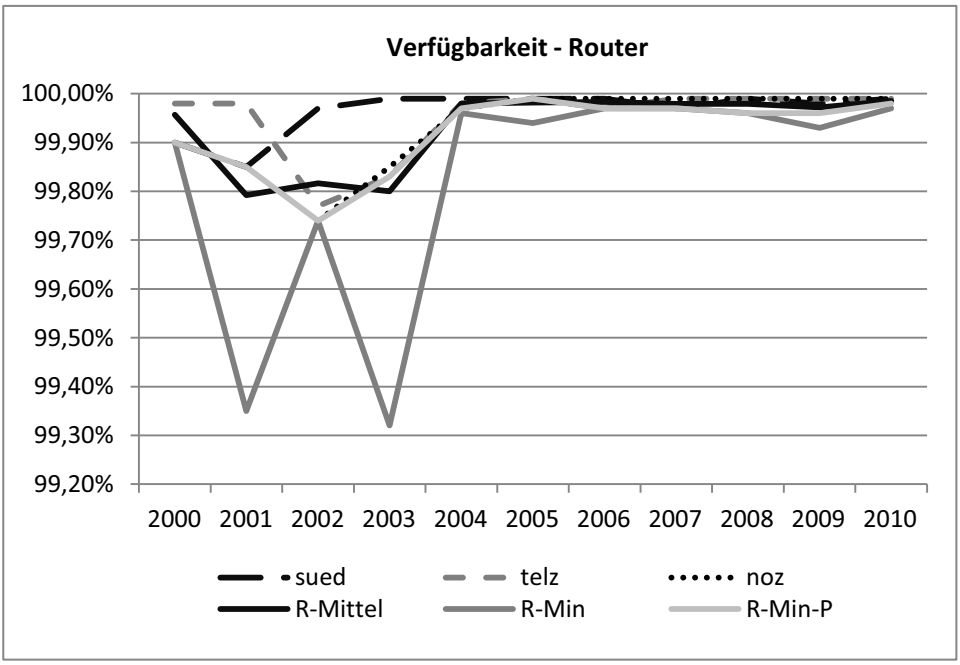


Abbildung 4: Summarische und exemplarische Jahresverfügbarkeiten der Router

5.2 Verfügbarkeit logischer Netzschnittstellen

Für Nutzer bzw. Endgeräte sind auf IP-Ebene sobezeichnete „Defaultroutes“ die nächsten Schnittstellen zur Kommunikation mit Systemen ausserhalb des eigenen VLANs bzw. IP-Subnetzes. Diese stellen sich im hier betrachteten Netzwerk als logische, virtuelle IP-Hostadressen dar, die in Redundanz jeweils einem von zwei Routern zugeordnet sind. Dabei erfüllt einer der Router die Schnittstellenfunktion im Standardbetrieb („primärer Router“), während der zweite dessen Aufgaben in Ausfallsituationen automatisch übernimmt („Standby-Router“). Dementsprechend sind in der Regel die Verfügbarkeiten der IP-Schnittstellen höher, als die einzelner Router. Es kann aber durchaus auch Ausnahmen geben, in denen der Betrieb einzelner Subnetze gestört ist, während die betreffende Router erreichbar und funktionsfähig sind. Beispiele dafür können etwa partielle Verklemmungen (unter Einschluss des Redundanzbetriebes) oder Ausfälle im Betrieb der zugehörigen virtuellen LANs sein.

In Abbildung 5 sind die Verfügbarkeiten verschiedener, als Repräsentanten (regionaler) Bereiche ausgewählter Netze, sowie Minimum („Min“) und Durchschnitt („Mittel“) bezüglich aller erfassten Subnetze dargestellt.

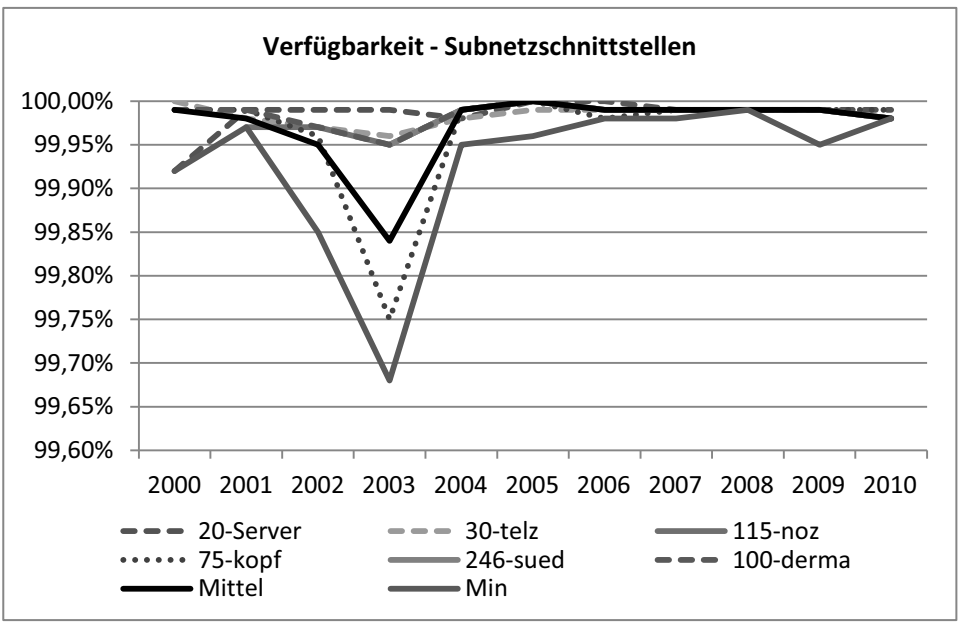


Abbildung 5: Summarische und exemplarische Jahresverfügbarkeiten von Nutzerschnittstellen (IP-Defaultroutes)

Auch hier ist der Effekt steigender Last in Bezug auf die „klassischen“, „CPU-gesteuerten“ Router zu erkennen. Über die Jahre 2004 – 2010 lag die aggregierte Verfügbarkeit über alle Subnetze bei 99,99%, d.h. die entsprechende Ausfallzeit betrug pro Jahr eine knappe Stunde (53 Min.).

6 Ausblick

Die dargestellte Methodik zur Erfassung und Auswertung von Verfügbarkeitsdaten bietet verschiedener Ansätze zur Verbesserung und zur Erhöhung der Aussagekraft. Dazu gehören folgende Punkte:

- **Erhöhung der Genauigkeit von Erfassung und Auswertung**
  Je mehr sich die Verfügbarkeitszahlen oberhalb von 99,95 % bewegen, desto stärker erscheint es angebracht, die Genauigkeit durch kürzere Abfragezeiten (kleiner 60 bzw. 180 sec) und exaktere Berechnungen (etwa auf drei Dezimalstellen) zu erhöhen.
- **Klassifizierung von Ausfallzeiten und zugeordneter Berechnungen**
  Durch Einteilung von Ausfallzeiten in geplante / ungeplante oder intern / extern verursachte Unterbrechungen können entsprechend zusammengefasste Auswertungen diese Unterscheidungen auch zahlenmäßig ausdrücken (statt nur in textlich kommentierter Form).

- **Berücksichtigung der Bedeutung getesteter Objekte**
  Das Netzwerk ist als Kommunikationsinfrastruktur darauf ausgelegt, möglichst gleichförmige Bedingungen zu schaffen. Dennoch gibt es aber Unterschiede einzelner Komponenten oder Standorte in der Bedeutung für den gesamten Netz- und Klinikbetrieb. Entsprechend können Störungen als mehr oder weniger gravierend beurteilt werden. Dies könnte in zusammenfassenden Berechnungen etwa durch gewichtete Durchschnittsbildung entsprechend berücksichtigt werden.
- **Ausweitung der Tests auf weitere Objekttypen**
  Technisch wäre z.B. die Einbeziehung von Endsystemen in die Verfügbarkeitstest überhaupt kein Problem. Um dabei Aussagen über das Netzverhalten zu gewinnen, müssten die Endsysteme allerdings selbst eine „sehr hohe“ Verfügbarkeit aufweisen bzw. eigene Ausfälle klar diagnostizierbar und damit rausrechenbar sein. Entsprechend geeignete Testsysteme (Probes) könnten dann als Referenzen verschiedener Netzbereiche dienen.
- **Dedizierte Testszenarien**
  Für besonders hohe Verfügbarkeitsanforderungen etwa von zentralen Servern oder kritischen Apparaturen lassen sich spezielle Testszenarien entwickeln, die die Einhaltung von Vorgaben überprüfen. Die Systeme selbst und gezielt platzierte Probes könnten Teil solcher Szenarien sein.

Darüber hinaus gibt es natürlich auch Ansätze, die nur mit ergänzender oder alternativer Anwendung weiterer Werkzeuge zu verfolgen sind. Als Beispiel dafür seien der Einsatz mehrerer Abfragestationen und entsprechend übergreifender Auswertungen genannt, was sich etwa mit Cisco-IP-SLA (Netzkomponenten als Testquellen) oder aber mit verteilten Managementsystemen realisieren ließ.

Die vom RRZE geübte Praxis hat über einen für IT-Verhältnisse langen Zeitraum nützliche Grundaussagen über die Netzverfügbarkeit geliefert. Die Offenlegung der Resultate und deren grobe Zusammenfassungen kann bei „naiver" Betrachtung zwar auch zu Fehlinterpretationen führen, sind aber bedeutender Bestandteil eines transparenten Netzbetriebes. Sie geben Betreibern und Nutzern Basis zur Abschätzung eines für Netzgestaltung und Anwendungen wichtigen Dienstgüteparameters. Aus dieser Sicht machen Fortführung und Weiterentwicklung unter Beachtung vertretbaren Aufwandes weiter Sinn.

Literaturverzeichnis

[CIS] Cisco System Inc.: "Availability Measurement", Networkers 2004, Session NMS-2201, verfügbar am 03.20.2012 unter http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6550/prod_presentation0900aecd80310695.pdf.

[GRE] Green, H., Hant J., Lanzinger, D.: "Calculating Network Availability", Aerosp. Corp., Los Angeles, CA, Aerospace conference, 2009 IEEE, verfügbar am 03.02.2012 unter http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4839386.

[HILL] Hillmer, U.: "Das Datennetz im Universitätsklinikum, Entwicklung von 1994 – 2011", RRZE-IFB 8, Dezember 2011, https://www.portal.uni-erlangen.de/get/file/1136.

[MGN] Cisco Medical-Grade Network (MGN) 2.0 Campus Architecture, last updated March 31, 2011, http://www.cisco.com/en/US/docs/solutions/Verticals/Healthcare/MGN_Campus.pdf.

[NTR] N-Tron Corporation: "Network Availability", www.n-tron.com/pdf/network_availability.pdf, verfügbar am 03.02.2012.

[ZAH] Zahemszky, A., Tapolcai, J., Császár, A., Mihály, A.: "Novel Availability Metrics for Network Topologies", High Speed Networks Laboratory, Budapest University of Technology and Economics, http://hsnlab.tmit.bme.hu, Sept. 30, 2009, verfügbar am 03.02.2012 von http://www.networks2008.org/data/upload/file/-Technical/C1_3_Zahemszky_Tapolcai_Csaszar_Mihaly.pdf.

[ZOU] Zou, W., Janic M., Kooij, R., Kuipers, F.: "On the Availability of Networks", Broadband Europe, Antwerp, Belgien, 3.-6. Dezember 2007, verfügbar am 03.02.2012 unter http://www.nas.ewi.tudelft.nl/publications/2007/bbeurope07.pdf.

Grid und Cloud Sicherheit

Das Datenschutzkonzept für das föderierte Frühwarnsystem im D-Grid und seine technische Umsetzung

Nils gentschen Felde[1], Wolfgang Hommel[1], Jan Kohlrausch[2],
Helmut Reiser[1], Christian Szongott[3], Felix von Eye[1]
[1]Leibniz-Rechenzentrum, [2]DFN-CERT, [3]Regionales Rechenzentrum Niedersachsen
felde@nm.ifi.lmu.de, wolfgang.hommel@lrz.de, kohlrausch@dfn-cert.de,
helmut.reiser@lrz.de, szongott@rrzn.uni-hannover.de, felix.voneye@lrz.de

Abstract: Im Projekt GIDS wird ein föderiertes Intrusion Detection System für das D-Grid konzipiert, implementiert, evaluiert und produktiv geführt. Dabei müssen zur D-Grid-weiten Erkennung von Angriffen auf Grid-Ressourcen lokale Alarmmeldungen der einzelnen Ressourcenanbieter organisationsübergreifend ausgetauscht, korreliert und u. a. zur Anzeige in einem zentralen Benutzerportal aufbereitet werden. Die dafür technisch vorhandenen Möglichkeiten werden praktisch sowohl durch restriktive *Information-Sharing-Policies* der beteiligten Organisationen als auch durch rechtliche und datenschutzrechtliche Randbedingungen eingeschränkt. In diesem Artikel werden das GIDS-Datenschutzkonzept und seine technische Umsetzung vorgestellt.

1 Ausgangssitutation und Herausforderungen

In einem organisationsübergreifenden Verbund muss die Informationssicherheit nicht nur jeweils organisationsintern, sondern auch für den Verbund als Ganzes betrachtet werden. Zu diesem Zweck müssen präventive, detektierende und reaktive Maßnahmen konzipiert und implementiert werden, die explizite Schnittstellen zwischen den beteiligten Organisationen vorsehen. In [gJMT06, HKK+11] wurde gezeigt, dass durch den Einsatz föderierter bzw. kooperativer Sicherheitsmechanismen ein verbessertes Sicherheitsniveau großer organisationsübergreifender IT-Infrastrukturen erzielt werden kann. Zentrale Herausforderungen für solche Sicherheitssysteme sind die potentiellen Kollisionen mit Datenschutzvorschriften und zum Teil sehr restriktiven organisations- und fachspezifischen Leitlinien zur Heraus- bzw. Weitergabe von IT-sicherheitsspezifischen Informationen an Dritte.

Die Idee eines föderierten, D-Grid-weiten Angriffserkennungssystems, die im Projekt GIDS (ein Grid-basiertes, föderiertes Intrusion Detection System zur Sicherung der D-Grid Infrastruktur) umgesetzt wird, ist in [Hgv+10c] beschrieben. Die Soll-Erkennungsleistung und die daraus resultierenden technischen Anforderungen wurden in [Rgv+10] analysiert. Auf dieser Basis wurde eine verteilte Architektur erarbeitet, die eine lose Kopplung der am D-Grid bzw. an GIDS beteiligten Ressourcenanbieter vorsieht, um die im Grid-Umfeld gewünschte organisatorische, administrative und technische Unabhängigkeit und Autonomie zu berücksichtigen.

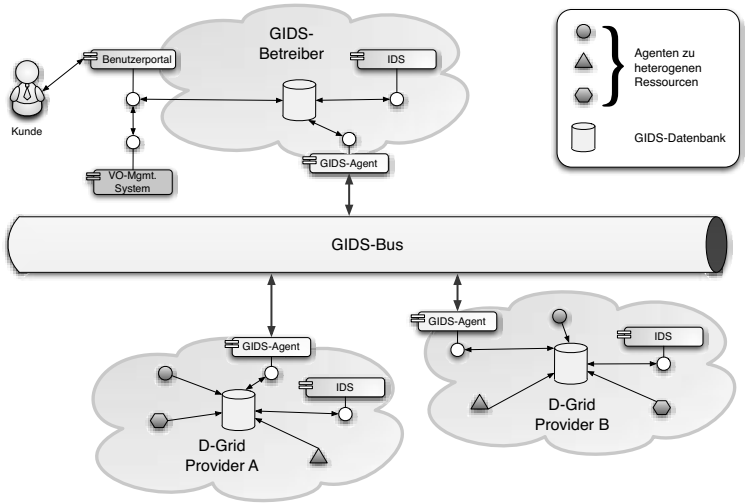


Abbildung 1: Architekturidee von GIDS nach [Hgv+10c] und [Hgv+10a]

Abbildung 1 gibt einen Überblick über den Architekturentwurf von GIDS. Die (lokalen) IDS-Instanzen basieren auf *Prelude* (`http://git.lrz.de/prelude/`), das nativ zu einer Vielzahl anderer IDS kompatibel ist und zudem die ausgereifte Bibliothek *libprelude* bereitstellt. Um die Idee der Föderation bestehender sicherheitsrelevanter Komponenten zu realisieren, bedarf es einer Kommunikationsinfrastruktur, die durch einen Nachrichten-Bus (*GIDS-Bus*) realisiert wird. Er basiert auf einer organisationsübergreifenden und Multicast-fähigen VPN-Infrastruktur. Als VPN-Lösung kommt die freie Software *OpenVPN* (`http://www.openvpn.net`) zum Einsatz und stellt einen SSL-geschützten Tunnel zwischen allen Ressourcenanbietern bereit. Über den GIDS-Bus können alle an GIDS beteiligten Ressourcenanbieter unter Wahrung der Integrität, Authentizität und Vertraulichkeit der übermittelten Informationen Daten über erkannte Angriffe austauschen. Es ist jedoch zu beachten, dass jede über den Bus gesendete Nachricht von allen an den Bus angeschlossenen Parteien gelesen werden kann.

Da solche Nachrichten personenbezogene Daten wie beispielsweise Benutzerkonten oder IP-Adressen enthalten, sind die Vorgaben des Bundesdatenschutzgesetzes (BDSG) zu berücksichtigen, das die Weitergabe stark einschränkt. Allerdings sind diese Daten oftmals für eine Angriffserkennung und die Einleitung von Gegenmaßnahmen notwendig. Um im GIDS einen effektiven Betrieb realisieren zu können, wurde ein Datenschutzkonzept entwickelt, das technische und juristische Mittel anwendet, um eine föderierte Erkennung von Angriffen zu ermöglichen ohne die rechtlichen Rahmenbedingungen zu verletzen.

Um auf Seiten der Ressourcenanbieter erhobene, für GIDS relevante Daten (dies können z. B. Log-Daten von Firewalls, Berichte von lokalen IDS-Instanzen o. ä. sein) GIDS-weit austauschen und automatisiert verarbeiten zu können, bedarf es gemeinsamer Datenformate und Protokolle. Die Übersetzung der vorliegenden Daten und die Verbreitung der

Informationen über den GIDS-Bus nehmen Agenten vor, die von den jeweiligen Ressourcenanbietern selbst betrieben und konfiguriert werden, so dass die volle Kontrolle und Unabhängigkeit der Ressourcenanbieter gewährleistet bleibt.

Als Grundlage für das in GIDS verwendete Datenaustauschformat dient das XML-basierte *Intrusion Detection Message Exchange Format* (IDMEF [DCF07]). Neben `Heartbeat`-Nachrichten sind `Alert`-Nachrichten der entscheidende Teil zur Übermittlung von Alarminformationen. Hier können neben Informationen über die Quelle und das Ziel eines Angriffs vielfältige weitere Daten aufgenommen werden. Insbesondere sind eine Klassifizierung und eigene Erweiterungen im IDMEF-Standard vorgesehen.

Dieser Artikel beschreibt ausgewählte Aspekte des Datenschutzes beim Einsatz eines föderierten Frühwarnsystems im D-Grid und die praktische Umsetzung. Abschnitt 2 skizziert das GIDS zugrundeliegende Datenschutzkonzept. Abschnitt 3 widmet sich der technischen Umsetzung des Datenschutzkonzepts. Abschnitt 4 fasst die Ergebnisse zusammen und gibt einen Ausblick auf anstehende Weiterentwicklungen.

2 Ein Datenschutzkonzept zur Verwendung innerhalb von GIDS

Im Rahmen von GIDS werden Daten über Angriffe auf Grid-Systeme erhoben und verarbeitet. Die Daten werden von verschiedenen Sensoren aufgezeichnet und betreffen detaillierte Informationen über Angriffe, die z. B. Quelle und Ziel des Angriffs beinhalten. Da ein Teil dieser Daten den Bezug zu Personen zulässt – dies können z. B. kompromittierte Benutzerkonten sein – fallen diese mindestens unter den Schutz des Bundesdatenschutzgesetzes (BDSG), das die Erhebung, Verwendung und Weitergabe dieser Daten stark einschränkt. Des Weiteren können diese Daten kritische Sicherheitslücken auf der Seite der beteiligten Partner offenlegen. Deshalb sind Sicherheitsanforderungen der beteiligten Partner zu berücksichtigen, die die Verarbeitung, Verbreitung und den Zugriff auf diese Daten betreffen.

Das GIDS-Datenschutzkonzept muss diese Anforderungen in sich vereinen: Neben allgemein gültigen rechtlichen Regelungen des BDSG müssen die technischen Spezifika und die Anforderungen der beteiligten Organisationen berücksichtigt werden. Wir fassen im Folgenden kurz die Grundlagen zusammen, die zu einem Datenschutzkonzept [Hgv+10b] geführt haben, und gehen anschließend auf praktische Aspekte seiner Umsetzung ein. Zwar wird die Erhebung, Verwendung und Weitergabe personenbezogener Daten durch das BDSG stark eingeschränkt, jedoch sieht der Gesetzgeber auch Mittel vor, die eine Weitergabe unter bestimmten Bedingungen ermöglichen. So erlaubt beispielsweise das Telekommunikationsgesetz die Nutzung personenbezogener Daten zur Beseitigung von Störungen in IT-Anlagen.

Grundaspekte des Datenschutzkonzepts Für den nachhaltigen Betrieb von GIDS sind verschiedene Aspekte zu berücksichtigen, die den Schutz und die Verwendung der Angriffs- und Betriebsdaten betreffen:

Technische Anforderungen. Im Datenschutzkonzept muss berücksichtigt werden, dass der Zweck erhobener und verarbeiteter Daten die Absicherung von Grid-Systemen ist. Angriffe müssen sowohl lokal als auch im Grid als Ganzes effektiv erkannt werden. Zudem muss rasch und möglichst weitgehend automatisiert reagiert werden können, um auch die von einem Angriff noch nicht betroffenen Systeme besser schützen zu können.

Sicherheitsaspekte bei Erhebung, Transport und Speicherung der Daten. Da im Rahmen von GIDS sicherheitskritische Informationen verarbeitet werden, müssen die grundlegenden Sicherheitsaspekte Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit gewährleistet sein. Dies betrifft insbesondere Daten, die auf der Seite der Betreiber von Grid-Ressourcen erhoben werden und deren Kenntnis sich möglicherweise für Angriffe ausnutzen lassen würden. Weiterhin kann potentieller Missbrauch durch Anwendung des „*least privilege*"-Prinzips minimiert werden.

Sicherheitsanforderungen der beteiligten Organisationen. Neben Angaben zu Angriffen sind bei verteilten IDS häufig weitere Informationen über Interna der beteiligten Organisationen zu verarbeiten. Dies umfasst einerseits Informationen der Betreiber über die Position ihrer Sensoren und die interne Struktur ihrer Netze. Andererseits liefern die Sensordaten indirekt auch Informationen über die Verwundbarkeit und den Zustand der überwachten Netze. Damit diese Daten nicht an Unbefugte weitergegeben werden, ist eine genaue Festlegung der Verwendungszwecke der Daten notwendig, der alle beteiligten Organisationen zustimmen müssen.

Rechtliche Regelungen. Der Betrieb eines verteilten, in Deutschland eingesetzten IDS unterliegt rechtlichen Regelungen, beispielsweise dem Datenschutzgesetz und dem Telekommunikationsgesetz; die entsprechenden Vorgaben bezüglich der Erhebung, Verarbeitung und Speicherung personenbezogener Daten müssen zwingend eingehalten werden.

2.1 Verwandte Arbeiten

Die für das GIDS-Datenschutzkonzept relevanten Vorarbeiten lassen sich in mehrere Bereiche aufteilen. Zuerst gibt es verwandte Arbeiten im Grid-Umfeld, die analog zu GIDS die rechtlichen Rahmenbedingungen im produktiven Betrieb berücksichtigen. So wurde vom D-Grid-Projekt „PneumoGrid" ein eigenes Datenschutzkonzept erstellt und veröffentlicht [KC09]. Zwar fokussiert dieses Konzept auf die datenschutz- und arzneimittelrechtlichen Vorgaben, die durch Pseudonymisierung personenbezogener Daten erfüllt werden, jedoch wird auch auf den Schutz der Daten im Benutzerportal eingegangen.

Des Weiteren sind viele Ansätze vorgeschlagen worden, um IDS-Daten rechtlich konform zu erheben und zu verarbeiten, wie beispielsweise in [BF00]. Der Schwerpunkt dieser Arbeiten liegt aber auf einem Konzept für die Pseudonymisierung der IDS-Daten.

Einen Schritt weiter gehen Flegel et al. in [FHM10] mit dem Ziel, eine Kooperation in einem zentralen Frühwarnsystem zu etablieren. Hier werden neben den gesetzlichen Bestim-

mungen zusätzlich die Anforderungen der beteiligten Partner an die Vertraulichkeit der übertragenden Daten berücksichtigt. Jedoch bildet auch dieser Ansatz die Anforderungen an das Datenschutzkonzept des GIDS nur teilweise ab. So müssen im GIDS die Anforderungen der föderierten, autonom agierenden Partner berücksichtigt werden. Dies beinhaltet zum Beispiel, dass die Partner entscheiden können, welche Daten weitergegeben werden können und welche herausgefiltert werden. Im Gegensatz zu [FHM10] basiert GIDS auf einer dezentralen Struktur und sieht auch die Verarbeitung von Daten vor, die nicht direkt im Zusammenhang mit Angriffen stehen, sondern Betriebsdaten der Grids sind. Ein weiterer Unterschied ist die Datenquelle, die beim GIDS beliebige IDS-Sensoren sind. Neben der Anwendung des Datenschutzkonzepts auf IDS-Daten sind also zusätzliche Anforderungen zu berücksichtigen, die die Erstellung eines eigenen GIDS-Datenschutzkonzepts notwendig machen.

2.2 Ansätze zur rechtlich-konformen Umsetzung des Datenschutzkonzepts

Das in [Hgv+10b] vorgelegte GIDS-Datenschutzkonzept dient zunächst als rechtlich fundierte Grundlage für die Verarbeitung von Angriffsdaten in GIDS. Seine praktische Umsetzung, also die technische Implementierung der organisatorischen und rechtlichen Vorgaben, ist ein wichtiger Schritt, der von allen an GIDS teilnehmenden Organisationen durchlaufen werden muss.

Der Gesetzgeber bietet die Möglichkeit durch das Telekommunikationsgesetz (TKG), Verkehrsdaten im Allgemeinen oder IDS-Angriffsdaten im Speziellen für die Erkennung und Beseitigung von Störungen zu erheben. Allerdings ist die Erhebung an diesen Anlass gebunden und es gelten strikte Einschränkungen für die Verwendung und Weitergabe. Grundlegend ist die Verwendung auf die Beseitigung der Störung beschränkt (Zweckbindung) und die Weitergabe an Dritte untersagt. Die Weitergabe der Daten im Rahmen des GIDS kann aber durch eine geeignete vertragliche Bindung zwischen den Nutzern und Betreibern des GIDS ermöglicht werden.

Der gesetzliche Schutz bezieht sich auf personenbezogene Daten. Fehlt dieser Bezug, entfallen Einschränkungen bezüglich der Erhebung und Weitergabe. Deshalb ist es eine wirkungsvolle technische Maßnahme, personenbezogene Daten vor der Weitergabe zu anonymisieren oder zu pseudonymisieren. Ein Vorteil der Pseudonymisierung ist, dass der Bezug zu den ursprünglich erhobenen Daten rekonstruiert werden kann und die Korrelation von Daten ohne Einschränkungen möglich ist. Da allerdings eine Zuordnung zu einer Person zumindest noch in der Theorie existiert, ist nicht unumstritten, in welchem Umfang die Einschränkungen für personenbezogene Daten entfallen. Im Zweifelsfall ist eine Anonymisierung der Daten zu bevorzugen, durch die der Bezug vollständig vermieden wird.

Als Beispiel eines Datums mit Personenbezug gilt bereits eine IPv4-Adresse. Hier reicht es im Regelfall beispielsweise, das letzte Byte einer IPv4-Adresse zu löschen, um einen Personenbezug im juristischen Sinne aufzuheben. Im Gegenzug müssen aufgrund des damit verbundenen Informationsverlusts möglicherweise Einschränkungen bei der Erkennungs- und Korrelationsleistung in Kauf genommen werden.

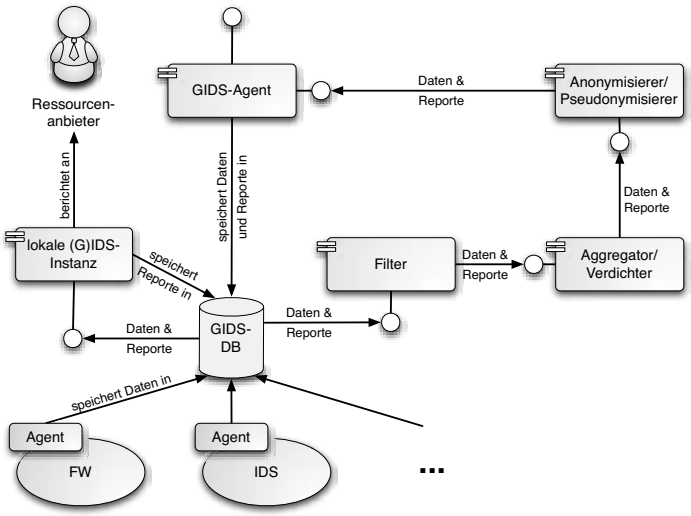


Abbildung 2: GIDS-Architektur auf Seite einer teilnehmenden Organisation nach [Hgv+10a]

3 Technische Umsetzung des Datenschutzkonzepts

Um das Datenschutzkonzept vor dem Übergang der Informationen auf den GIDS-Bus technisch realisieren zu können, wurden in einem ersten Schritt alle Attribute und XML-Knoten von IDMEF auf ihre datenschutzrechtliche Bedeutung geprüft. Da die Semantik der Attribute und Knoten durch den Standard [DCF07] festgelegt ist, ist eine für die Ressourcenanbieter zuverlässige Zuordnung der datenschutzrechtlich und sicherheitspolitisch relevanten Teile einer IDMEF-Meldungen möglich.

Abbildung 2 stellt den dreistufigen Vorverarbeitungsprozess dar, den eine IDMEF-Nachricht durchlaufen muss, bevor sie über den GIDS-Bus verteilt wird. Fällt an einer Informationsquelle (hier beispielhaft eine Firewall oder eine lokale IDS-Instanz) eine Nachricht an, so wird diese von einem für das jeweilige System entwickelten Agenten ins IDMEF-Format übersetzt und in eine lokale Datenbank geschrieben. Alle neuen Nachrichten in dieser Datenbank durchlaufen zur Veröffentlichung anschließend zuerst eine Filterung, die die Umsetzung lokaler Datenschutzrichtlinien unterstützt. Danach findet eine Korrelation/Aggregation der Daten statt, die die Skalierbarkeit des Systems sicherstellt, bevor vor der Weitergabe der IDMEF-Nachrichten an Dritte schlussendlich noch eine Anonymisierung oder Pseudonymisierung personenbezogener Daten vorgenommen wird, um den rechtlichen Anforderungen genüge zu tun.

Die Reihenfolge der Schritte ist so gewählt, damit Datensätze, die die Domänengrenzen nicht überschreiten dürfen, als erstes aussortiert werden, danach eine Aggregation auf den komplett vorhandenen Datensätzen durchgeführt werden kann und erst im letzten Schritt eine Anonymisierung der (aggregierten) Datensätze stattfindet. Damit erreicht man eine

maximale Erkennungsleistung bei gleichzeitiger Umsetzung des Datenschutzkonzeptes. Die Umsetzung der drei letztgenannten Komponenten und ihr Bezug zum gesamten Datenschutzkonzept ist im Folgenden beschrieben.

Nachrichtenfilterung Zunächst werden Meldungen, die nicht für die Weitergabe an die anderen Teilnehmer des GIDS bestimmt sind, ausgefiltert. Dies hat den praktischen Grund, dass Sicherheitsmechanismen, die bei den beteiligten Ressourcenanbietern installiert sind, in der Regel mehr als nur die am D-Grid angeschlossenen Ressourcen zu überwachen haben. Somit kommt es laufend vor, dass Alarmmeldungen nur organisationsintern verarbeitet werden, aber nicht an die anderen GIDS-Teilnehmer versendet werden sollen. Das GIDS-System bietet die Möglichkeit, solche Nachrichten komplett auszufiltern. Somit dient diese Maßnahme nicht primär den rechtlichen Anforderungen, sondern in erster Linie der Erfüllung lokaler Sicherheitsrichtlinien. Dabei ist es möglich, die Nachrichten, die ausgefiltert werden sollen, über reguläre Ausdrücke zu identifizieren. Ein praktischer Nebeneffekt der Filterung ist das frühzeitige Entfernen ungewünschter bzw. unnötiger Daten, was direkt zur Ressourcenschonung und somit Skalierbarkeit des Gesamtsystems positiv beiträgt.

Datenverdichtung durch Korrelation und Aggregation Bei der Datenverdichtung geht es in erster Linie darum, das über den GIDS-Bus zu übermittelnde Datenvolumen zur Sicherstellung der Skalierbarkeit zu minimieren, indem mehrere Meldungen Site-lokal zu einer Meldung zusammengefasst werden, so dass das Datenschutzkonzept hier nur am Rande von Bedeutung ist. Eine nähere Betrachtung im Rahmen dieser Arbeit bleibt außen vor.

Anonymisierung und/oder Pseudonymisierung Im letzten Schritt kann jede Nachricht anonymisiert oder pseudonymisiert werden. In diesem Fall kann man einzelne Attribute oder XML-Knoten, die datenschutzrechtlich relevant sind, auswählen, damit sie anonymisiert oder pseudonymisiert werden. Dies ist der zentrale Schritt, in dem die Einhaltung der rechtlichen Randbedingungen, speziell der Datenschutzgesetze, realisiert wird.

Im praktischen Einsatz ergeben sich jedoch eine Reihe von Herausforderungen. Zum einen ist der Umfang einer IDMEF-Nachricht im Wesentlichen eine Kompromisslösung, um verschiedenartige Alarmmeldungen u. a. von Logfile-Analyzern, Firewalls oder Intrusion Detection Systemen abzubilden. Somit werden viele, für eine tiefere Analyse wichtige Daten, in das Feld `AdditionalData` ausgelagert, dessen genaue Verwendung im IDMEF-RFC bewusst nicht spezifiziert wurde, um die Möglichkeiten zur Erweiterung des XML-Schemas nicht einzuschränken. Da jedoch die Semantik der darin enthaltenen Daten nicht a priori festgelegt ist, sind diese Felder im Sinne einer strengen Auslegung des Datenschutzgesetzes vollständig zu löschen. Ansonsten kann beispielsweise nicht ausgeschlossen werden, dass personenbezogene Daten (ggf. in binärer Form) enthalten sind. An dieser Stelle wäre eine standardisierte Erweiterung von IDMEF hilfreich, die mehr Felder bereit stellen könnte, deren Semantik a priori bekannt ist.

3.1 Erweiterungen des IDMEF-Formates mit datenschutzrechtlichem Bezug

In Abbildung 1 ist als Schnittstelle zwischen den Kunden und dem GIDS ein Benutzerportal dargestellt. Dieses dient der Information bzw. Alarmierung von Grid-Benutzern und Site-Administratoren. Benutzer müssen sich authentifizieren und werden Rollen zugeordnet, um nur die für sie relevanten Meldungen einsehen zu können.

Bei der Löschung von z. B. IP-Adressen aus Alarmmeldungen oder einer zu starken Anonymisierung wird jedoch auch die eindeutige Zuordnung eines Alarms zu einer Ressource erschwert oder gänzlich unmöglich gemacht. Dabei ergeben sich Probleme, um beispielsweise die Zugriffsregelungen im Portal eindeutig durchsetzen zu können.

Dieses Problem lässt sich jedoch mit Mitteln lösen, die im D-Grid bereits vorhandenen sind. Im *Grid Ressource Registry Service* (GRRS) existiert für jede Ressource eine Zuordnung zu einem Ressourcenanbieter, dem eine *Short-ID* zugeordnet ist, also ein Kurztitel. Jeder IDMEF-Nachricht wird daher ein zusätzlicher XML-Knoten vom Typ `AdditionalData` hinzugefügt, in dem die Short-ID des GIDS-Teilnehmers, der die Nachricht erstellt hat, vermerkt ist. Damit ist auch nach einer vollständigen Anonymisierung der Nachrichten eine eindeutige Zuordnung zu den Ressourcen und den dazugehörigen VO-Nutzern möglich. Dies eröffnet zwar potentiell neue Datenschutzrisiken, vor allem wenn es sich bei den Short-IDs um Grid-Ressourcen bestehend aus einer einzelnen Maschine handelt, auf der immer nur ein Nutzer Grid-Jobs rechnet. Es unterliegt jedoch den Ressourcenanbietern, Alarmmeldungen, die einen solchen eindeutigen Nutzerbezug haben, mit den oben genannten Anonymisierungs- oder Filterfunktionen datenschutzkonform vorzubereiten.

Ein ähnlicher Weg wird für die Durchsetzung lokaler Datenschutzrichtlinien bei von anderen Domänen empfangenen Alarmmeldungen gegangen. Da es unwahrscheinlich ist, dass bei allen Ressourcenanbietern die anfallenden Daten nach der gleichen Anzahl von Tagen gelöscht werden, ist es nötig, ein System zu entwickeln, das garantiert, dass die Daten, die die Domänengrenzen überschreiten, trotzdem nach den Richtlinien der ursprünglichen Domäne behandelt werden. Auch hier wird wieder ein weiterer XML-Knoten vom Typ `AdditionalData` hinzugefügt, dessen Inhalt ein Ablaufdatum für die Nachricht ist. Sobald das hier definierte Datum erreicht ist, muss die Nachricht auch bei den anderen GIDS-Teilnehmern komplett gelöscht werden. Für die Löschung „abgelaufener“ Daten sind regelmäßig auszuführende Automatismen verantwortlich, zu denen sich alle an GIDS beteiligten Ressourcenanbieter a priori verpflichten.

3.2 Erfahrungen im Praxiseinsatz

Im Projekt werden derzeit verschiedene Anonymisierungs- und Pseudonymisierungsstufen evaluiert. In einem ersten Schritt wurde die strengste Auslegung des Datenschutzes erprobt. Diese führt dazu, dass alle Attribute bzw. XML-Knoten, die personenbezogene Daten enthalten können, komplett aus der Nachricht gelöscht werden. Damit wird ein Personenbezug vollständig ausgeschlossen. Dies geht jedoch zu Lasten der theoretisch

möglichen und praktisch erzielten Erkennungsleistung: In diesem Fall ist keine ordentliche Korrelation von Meldungen über Domänengrenzen hinweg mehr möglich. Daher wird schrittweise empirisch ermittelt, welche und wie viele Teilinformationen beispielsweise über die Ziel- und Quelladressen eines Angriffs nötig sind, um angriffsspezifische Korrelationen durchzuführen, die die Grid-globale Erkennungsleistung verbessern.

Ein parallel verfolgter Ansatz nutzt Pseudonymisierungswerkzeuge wie z. B. Crypto-PAn. Dabei werden „kritische“ Teile einer Nachricht kryptographisch verschlüsselt und somit für Außenstehende nicht mehr erkennbar gemacht. Bisher wurde in der D-Grid-Praxis von dieser Möglichkeit noch kein Gebrauch gemacht. Dies hat zwei Gründe: Zum einen ist es juristisch noch umstritten, ob eine Pseudonymisierung den Auflagen der Datenschutzgesetze genügt, da ein Personenbezug, wenn auch mit Aufwand, immer noch herstellbar ist. Zum anderen ist für ein solches Verfahren ein wirkungsvolles Krypto-Schlüsselmanagement zu integrieren, da der verwendete Schlüssel regelmäßig erneuert werden muss, um die Vertraulichkeit der verschlüsselten Daten langfristig gewährleisten zu können.

4 Zusammenfassung und Ausblick

Föderierte Frühwarnsysteme, wie sie im Rahmen von GIDS für das D-Grid aufgebaut werden, unterliegen Einschränkungen, die organisationsinterne Intrusion Detection Systeme nicht haben: Zum einen ist die uneingeschränkte Weitergabe von Informationen über Angriffe an externe Dritte oftmals unerwünscht und zum anderen müssen gesetzliche Auflagen, insbesondere mit Bezug auf den Datenschutz, umgesetzt werden.

In diesem Artikel wurden das GIDS-Datenschutzkonzept und seine technische Umsetzung vorgestellt: Von einer Organisation intern erzeugte Alarmmeldungen werden zunächst gefiltert, verdichtet und anonymisiert bzw. pseudonymisiert, bevor sie über eine VPN-geschützte Multicast-Bus-Infrastruktur an die anderen beteiligten Organisationen weitergegeben und zur Anzeige im GIDS-Webportal aufbereitet werden. Als Transportformat wird das weit verbreitete IDMEF eingesetzt, für das präzise definiert wurde, welche Attribute und XML-Knoten potenziell kritische bzw. personenbezogene Daten enthalten können. Eine aktuell laufende Evaluation analysiert die Korrelations- und Erkennungsleistung des Grid-weiten Frühwarnsystems in Abhängigkeit vom Informationsverlust, der durch Anonymisierung eintritt.

Neben der Produktivführung des erarbeiteten Systems, die sich an die Evaluation anschließen wird, ist geplant, das Konzept der so genannten *sticky policies* in GIDS zu integrieren. Momentan werden Angriffsmeldungen, die an andere an GIDS beteiligte Sites weitergegeben werden, nur mit einem Soll-Ablaufdatum versehen. Die Empfänger dieser Meldungen verpflichten sich organisatorisch bzw. vertraglich dazu, diese Ablaufdaten zu honorieren und die entsprechenden Meldungen rechtzeitig wieder bei sich zu löschen. *Sticky policies* verknüpfen die ausgetauschten Daten hingegen untrennbar mit fein granulierten Regelungen, die neben der maximalen Aufbewahrungsdauer beispielsweise auch eine genaue Zweckbindung und weitere Auflagen umfassen können. Sie sind eine wichtige Voraussetzung für die Akzeptanz des GIDS aufgrund der sehr heterogenen Information-Sharing-

Policies der D-Grid-Ressourcenanbieter.

In GIDS wurden auch einige Erweiterungen des IDMEF-Formats vorgenommen. Diese nutzen zwar die bereits vorhandenen Schnittstellen, stellen zunächst jedoch eine D-Grid-proprietäre Entwicklung dar. Um die Übertragbarkeit der Ergebnisse auf andere Grids und unternehmensübergreifende Verbünde sicherzustellen, soll mit den IDMEF-RFC-Autoren diskutiert werden, wie eine Standardisierung erreicht werden kann.

Literatur

[BF00] Joachim Biskup und Ulrich Flegel. On Pseudonymization of Audit Data for Intrusion Detection. In Hannes Federrath, Herausgeber, *Designing Privacy Enhancing Technologies*, number 2009 in Lecture Notes in Computer Science, Berkeley, California, USA, Juli 2000. Springer, Heidelberg.

[DCF07] Herve Debar, David A. Curry und Benjamin S. Feinstein. The Intrusion Detection Message Exchange Format (IDMEF), 2007. IETF RFC 4765.

[FHM10] Ulrich Flegel, Johannes Hoffmann und Michael Meier. Cooperation enablement for centralistic early warning systems. In Sung Y. Shin und Sascha Ossowski, Herausgeber, *Proceedings of the 25th International ACM Symposium on Applied Computing (SAC 2010)*, Sierre, Schweiz, März 2010. ACM Press.

[gJMT06] Nils gentschen Felde, Marko Jahnke, Peter Martini und Jens Tölle. Impact of Sanitized Message Flows in a Cooperative Intrusion Warning System. In *Proceedings of the 25th Military Communications Conference (MILCOM 2006)*, Washington, DC, USA, Oktober 2006.

[Hgv+10a] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. Architekturkonzept für ein Grid-basiertes IDS. Technical report, D-Grid, Oktober 2010.

[Hgv+10b] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. Datenschutzmodell für ein Grid-basiertes IDS. Technical report, D-Grid, Juli 2010.

[Hgv+10c] Wolfgang Hommel, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. Grobskizze einer Architektur. Technical report, D-Grid, April 2010.

[HKK+11] Wolfgang Hommel, Jan Kohlrausch, Jan Köcher, Christian Szongott, Nils gentschen Felde und Felix von Eye. Ein föderiertes Intrusion Detection System für das D–Grid. In *18. DFN Workshop „Sicherheit in vernetzten Systemen“*, Hamburg, Deutschland, Februar 2011. DFN-CERT GmbH.

[KC09] Dagmar Krefting und Sebastian Canisius. Anforderungen in PneumoGrid an Sicherheit und Nutzerfreundlichkeit. Grid Security Workshop in Göttingen, Oktober 2009.

[Rgv+10] Helmut Reiser, Nils gentschen Felde, Felix von Eye, Jan Kohlrausch und Christian Szongott. Anforderungs- und Kritierienkatalog (MS 6). Technical report, D-Grid, Januar 2010.

A Legal and Technical Perspective on Secure Cloud Storage

Sebastian Graf, Jörg Eisele and Marcel Waldvogel, University of Konstanz*
Marc Strittmatter, University of Applied Sciences, Konstanz+

*(firstname.lastname)@uni-konstanz.de
+(firstname.lastname)@htwg-konstanz.de

Abstract: Public cloud infrastructures represent alluring storage platforms supporting easy and flexible, location-independent access to the hosted information without any hassle for maintaining own infrastructures.

Already widely established and utilized by end-users as well as by institutions, the hosting of data on untrusted platforms, containing private and confidential information, generates concerns about the security. Technical measures establishing security rely thereby on the technical applicability. As a consequence, legal regulations must be applied to cover those measures even beyond this technical applicability.

This paper provides an evaluation of technical measures combined with legal aspects representing a guideline for secure cloud storage for end-users as well as for institutions. Based upon current approaches providing secure data storage on a technical level, german laws are applied and discussed to give an overview about correct treatment of even confidential data stored securely in the cloud.

As a result, a set of technical possibilities applied on fixed defined security requirements is presented and discussed. These technical measures are extended by legal aspects which must be provided from the side of the hosting Cloud Service Provider.

The presented combination of the technical and the legal perspective on secure cloud storage enables end-users as well as hosting institutions to store their data securely in the cloud in an accountable and transparent way.

1 Introduction

Internet Services such as Flickr, Dropbox, Wuala as well as Amazon S3 and Google Cloud Storage provide comfortable and ubiquitous storage and sharing for a wide class of data. These services relieve the user from hardware purchases, software bug fixes, and infrastructure maintenance, at the cost of the users implicitly granting the Cloud Service Provider and their administrators full access to all their sensitive data, including secret business data when used by a company or institution.

The world-wide accessibility of these public services not only supports external attackers to gain access to the data: It must be assumed that within these public clouds, the hosting companies like Amazon, Google and Yahoo use the data, representing an alluring mass of confidential information, for user-analysis and advertising. The different attack-models, ongoing with the geographical distribution of the data over different countries, make the identification of necessary security measures ongoing with corresponding legal aspects hard to accomplish.

This paper maps common security requirements to the peculiarities of cloud-based storage. Since security is only guaranteed by the satisfaction of all security requirements, a combination of different measures is discussed and extended by corresponding legal aspects.

The proposed set of techniques, guarding the data on a technical base extended by suitable regulations, represents a guideline for secure storage on public cloud infrastructures for end-users as well as for institutions.

2 Applying security measures to cloud-based storage

Public cloud infrastructures offer different Cloud Service levels of utilization defined as "Software as a Service" (SaaS), "Platform as a Service" (PaaS) and "Infrastructure as a Service " (Iaas) [MG09].

Applications are commonly deployed on one of the defined Cloud Service levels. Figure 1 maps these levels on the ability of technical control: Each service deployed in the cloud relies on an execution stack consisting of Services, Applications, Platforms, Operating Systems and Hardware. The ability to influence the application for a customer e.g. for establishing security bases on the cloud level utilized for deployment. As a consequence, the responsibility for ensuring trust is shared between the customer and the Cloud Service Provider. Within SaaS-infrastructures, the customer has only the ability to control the service itself without having influence on the lower levels, while in PaaS-infrastructures, the customer can control the service and the representing application. For the lower levels, only the Cloud Service Provider has technical control and is therefore responsible for providing security. This transition of responsibility based on the denoted application-stack is called *Threshold of Technical Control* within Fig. 1 and the rest of the paper. Consequently, technical security measures can only be applied by the customer on her side of the *Threshold of Technical Control* depending on the deployed level, while security on the side of the Cloud Service Provider must be covered by legal regulations to provide throughout security in the cloud.

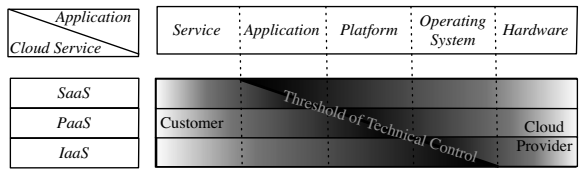


Figure 1: Point of interference

Cloud storage systems commonly fit the SaaS- and PaaS-levels: Security measures applied on native clients (like e.g. provided by Wuala [GMSW06] and Dropbox) as well as on common web services (like e.g. REST [Fie00] accessing Google Cloud Storage or the Amazon S3 system) therefore ensure security on the Service as well as on the Application level depending on the concrete system. For all lower levels down to the Hardware level, the Cloud Service Provider is responsible for guaranteeing secure data storage. This responsibility increases since cloud services are often stacked resulting in cloud-service

supply chains[1].

Based upon the *Threshold of Technical Control*, the concrete kinds of established security measures depends on the level of control namely the kind of service which is utilized for storage: Enabling storage on untrusted public infrastructures thereby fit two main kinds: User-centric cloud storage and application-centric cloud storage.

2.1 User-centric cloud storage

Figure 2 shows a schema of an user-centric cloud storage.

Clients, which are under user-control and therefore trusted denoted by the lockers, use the cloud to store the data directly. The cloud itself consists of abstraction layers mirroring the data world-wide. Since the storage is represented by a direct accessible service, it is utilized as SaaS. Consequently, technical measures to provide security must be applied on the client-side before the data is sent into the cloud. Each client accesses the storage directly, applying optional rules for sharing. Nevertheless, these access rights are only recognized by other clients while internal access is not technically restricted by default. Practical examples of this scenario include Dropbox and Wuala where native applications care about the synchronization between the clients and the cloud.

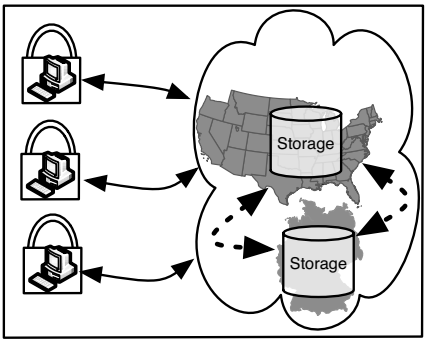


Figure 2: User-centric Cloud Storage

2.2 Application-centric cloud storage

Figure 3 shows a different schema of an application-centric cloud storage.

Institutions for example rely on trusted centralized components and therefore access the cloud in a centralized way. Again, the cloud represents an abstraction of services and storages opaque for the users: The concrete location of the data is unaware even though many Cloud Service Providers offer regional storage options in this scenario. The storage is often utilized as PaaS where either own defined applications care about the data handling in the cloud or the storage is accessed with the help of web services. This access is performed by trusted centralized applications denoted as “Internal Service” in Fig. 3. Access rights as well as technical security measures are administrated over this service whereas

[1] Dropbox for example utilizes Amazon S3 as storage backend.

the cloud has no deeper semantic knowledge about the data. Examples of this scenario are the Google App Engine, Microsoft Azure, Amazon S3 as well as the Google Cloud Storage.

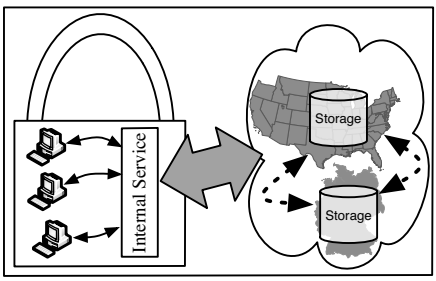


Figure 3: Application-centric Cloud Storage

In both scenarios, techniques to provide security must be established either on the clients or within the centralized "Internal Service". Legal regulations must extend those techniques from the side of the Cloud Service Provider while the *Threshold of Technical Control* is represented by the transfer of the data into the cloud.

3 Defining a secure cloud storage

Before discussing technical measures as well as legal regulations, common security requirements [Sto01, Sch00, Lam01] must be mapped to the use case of secure cloud storage. Based on this mapping, technical approaches as well as concerned regulations are discussed.

- **Confidentiality in the cloud:**
  Confidentiality definitely represents a major security concern within the cloud. The question "Who can read my data?" is not only related to companies or institutions hosting third-party data. Internal malicious accessors as well as external attackers leverage from the world-wide accessibility and hosting of the data. Besides these attack scenarios, the inlying information represents an alluring mass of information for the Cloud Service Providers answering questions about the generosity of their often free offers.

- **Availability in the cloud:**
  "How can I ensure everlasting access to my data?" is one driving question behind putting data in the cloud extended by the wish for easy sharing. Since the physical control of the data is obscured by the *Threshold of Technical Control*, users have only the possibility to trust the Cloud Service Providers regarding their "number of nine's"[2] and their promises not to harm any data.

- **Integrity in the cloud:**
  Consistence is a major issue often only applied on the transfer of the data. The question "Is my data still intact in the cloud?" demands the integrity. Guarding integrity

[2]The "number of nines" represent the exact percentage of availability of the services (e.g. 99.99 % related to Amazon in 2007 [Gar07]).

represents a major security challenge since integrity-checks as well as restoration of data are less reliable when performed directly in the cloud.

- **Accountability in the cloud:**
  The traceability of actions on the data is covered by the question "What actions occurred on my data?". Accountability defines the ability to trace any kind of access as fine-granular as possible. Tracing read access is thereby hardly realizable in the cloud due to the physical abstraction of the storage and the various possibilities of access. Accountability applied to secure cloud storage thereby focusses on modifications on the data including procedural approaches.

- **Assurance on the cloud:**
  Assurance is the overall trust even beyond the applied security measures. Applied to cloud storage, it is formulated as the question "How secure is my data in the cloud?". The answer to this question is a combination of all applied security techniques combined with regulations and policies. Assurance thereby includes legal aspects as well, since a fixed definition of reliances is mandatory to provide security even beyond the *Threshold of Technical Control*.

To store data "securely" in the cloud, a combination of measures to satisfy all denoted security requirements becomes necessary. The *Threshold of Technical Control* defines the possible field of the appliance of technical measures whereas the aspects must not only adhere the characteristics of cloud-based storage, namely its high availability, the mistrustfulness of the hosting infrastructure, the distant location from the data as well as the loss of physical possession of the data. Furthermore, technical approaches should neither hamper collaboration and sharing nor complicate synchronization of data between different locations. All security measures must, based on the *Threshold of Technical Control*, be applicable on the trusted components only, even though the denoted benefits of the cloud should be utilized.

3.1 Technical approaches

All technical measures, applied on the trusted side of cloud-storage architectures, must adhere the defined security requirements.

3.1.1 Confidential data handling

Confidentiality represents the most obvious security requirement to be satisfied in the cloud. Straight-forward encryption ensures confidentiality of the data, yet synchronization mechanisms necessary for pushing data efficiently in the cloud should respect the modifications in an encrypted way. Based on diff-algorithms, transferring only deltas between two versions enables performant synchronization. Encrypting the data while not respecting the underlaying versioning thereby results in the transmission of entire versions instead of the transmission of (encrypted) deltas only. Besides the awareness of the deltas,

a suitable key management must be established to provide secure data sharing. Since sharing and collaboration represent main use cases for cloud storage, this functionality should no be hampered by establishing confidentiality. Confidentiality-awareness in the cloud is as a consequence less a question of encryption but more a field of encryption-aware synchronization and key management enabling efficient access on encrypted data for disjunct clients.

3.1.2 Keeping the data available

Besides the necessity for confidentiality without reducing cloud-based functionalities, the availability of cloud-based data must be guaranteed as well. The high availability of cloud services leads to the perception that data stored in the cloud will remain accessible forever. As a consequence, users often do not backup their data when pushed into the cloud. Nevertheless, errors in cloud infrastructures occur[3]. Besides disturbances within the cloud infrastructure itself, the access to the cloud represents not only a bottleneck related to data transfer rates but also a vulnerability related to the access.

Current approaches provide redundancy by storing data on multiple clouds, namely in a cloud-of-clouds like DepSky [BCQ+11]. Besides the utilization of multiple clouds, local caching of the data buffers possible network disturbances.

3.1.3 Consistency checks of the data

Erasure codes like provided within DepSky guard furthermore the integrity of the data. Due to the physical loss of control, such checks become necessary to be aware about the status of the data. Based upon at least local partial caching, out-of-the-box integrity checks like provided by Amazon can be utilized even though the main purpose of those checks is the awareness of transmission errors.

Specialized approaches like HAIL [BJO09] try to fill this gap based upon replication and checking of blocks utilizing signatures and checksums. Since the data at rest in the cloud stays behind the *Threshold of Technical Control*, integrity-checks in the cloud rely on the trust against the hosting provider resulting in the necessity for suitable regulations established between the customer and the Cloud Service Provider.

3.1.4 Tracing actions on the data

Accountability describes the ability to trace actions on single entities within the data. A straight forward approach represents logging and auditing as well as establishing policies and regulations for the access. Since we rely on data storage only, sophisticated versioning of the data represents a straight-forward mechanism to ensure accountability. Such a versioning must be robust against the damage of single versions to offer easy reconstruction of any version. Due to the distance to the storage, the deltas between consecutive

[3]The Amazon EC2 cloud crashed at the beginning of 2011 generating some data lost without any possibility of reconstruction.

modifications must be balanced and encryption-aware to ensure efficient transfer of the data.

3.1.5 Combining measure to assure data security

Violating one security requirement results in a vulnerable cloud storage. As a consequence, confidentiality, availability, integrity as well as accountability must be applied synchronously to gain assurance.

Fig. 4 recapitulates the proposed measures. Some of these techniques thereby satisfy more than one security requirement. Erasure codes ensuring availability within DepSky for example guard the integrity utilizing the computation they are based on. Checksums and signatures, guarding mainly the consistence of the data, play an important role for providing accountability as well: Combined with versioning of the data, higher level security goals like non-repudiation can be established.

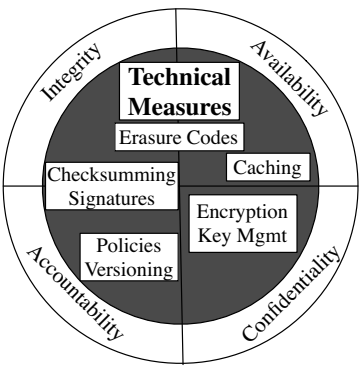


Figure 4: Technical measures

Since the measures can only be applied on the customer side of the *Threshold of Technical Control*, legal implications ensuring secure cloud storage on the Cloud Service Provider side become necessary to provide throughout assurance.

3.2 Legal implications

Legal concepts applied on security do not depart from the classification of security requirements like technical measures because of the various legal disciplines which are touched e.g. data protection law, torts law, contracts and criminal law. Applying acts to cloud storage is in practice thereby not as easy as it seems: First, the geographical distribution of services make the application of mandatory law, relying on the border of countries, often hard to determine. Data stored in a cloud while uploaded from e.g. Germany might be illegal in other countries. Within this paper, we mainly focus on the application of German statutory laws based on Sec. 9 I StGB which relies on the place of action (namely the initial push of the data into the cloud). Sec. 7 I StGB furthermore defines the application of repressive measures if the action is unlawful in other countries as well.

Technical undefined terms in statues like “notable” and “necessary” make an interpretation of law even more complicated. We will therefore evaluate the implications of security to cloud storage based upon different scenarios:

3.2.1 Unauthorized access

Even though from a technical point of view there is an immense difference how to establish confidentiality by encrypting or by just blocking the access, from a legal point of view Sec. 202a StGB and Sec. 202b StGB prevent any unauthorized access. Only accessing restricted content in an unauthorized manner is sufficient to harm those statutes regardless if the accessor attacks from outside or is represented by an internal person. It is important to know that even the preparation of unauthorized data access is indictable by Sec. 202c StGB.

3.2.2 Harming data

Unauthorized modifications or deletions of data are covered by Sec. 303a StGB. Any unexpected status of the data is not only harming the integrity but also the availability. If a copy of the unauthorized removed/modified data exists, this act might not be impinged. The preparation to make data inaccessible in an unauthorized way is covered by Sec. 202c StGB as well. Similar to possible unauthorized access to the data, it is unimportant if the attack harming the data occurs from outside or inside the cloud.

3.2.3 Data privacy

Data privacy is a huge field within cloud infrastructure utilization. The storage of information in untrusted infrastructures not only harms confidentiality, it touches, from a legal point of view, all security requirements. German law about data privacy is rather strict when personal information is stored. From an EU perspective, any stored personal information must be handled in a way that the user keeps control over the data, directly or indirectly by installing a contractual data controller-data processor relationship while restricting data processing to countries with acceptable levels of data security. Harming the related German statute Sec. 43 II BDSG thereby can be based upon unauthorized modifications (mapping the confidentiality and integrity) as well as the accountability since the user has the ability to order a reconstruction of all actions taking place on the data. Data privacy is handled differently within different countries which complicates related user-requests. European harmonization has installed a minimum level of protection. Current 2011 ECJ (European Court of Justice) decisions have triggered legal discussions of the need for a maximum protection level by EU law overruling more protective country laws (such as German BDSG). These discussions include the appliance of technical security measures and their impact on the appliance of relevant privacy statues. As an example, it is at the moment unclear from a legal point of view if data privacy statutes must be applied on encrypted data stored in the cloud.

3.2.4 Author's rights

The ease of collaboration brings concerns about authors right into the focus of security. Unauthorized access thereby not only covers the field of confidentiality, it furthermore

harms the accountability. Unauthorized copies of data are harming authors rights especially when the attackers intent is to make unlawful profit. Related statues harmed in such scenarios are Sec. 106 and 108 UrG.

3.2.5 Contracts

It should be noted that the contractual definition of "confidentiality" and "security" is typically subject to the parties appraisal. Depending on the applicable law (typically freely eligible by merchant parties to contracts, with some restrictions also by parties of contracts where one party is an end-consumer) the definition of what the parties accept as "secure" or define as "confidential" has a large gamut of variances. At times, the Cloud Service Provider even tie the minimum level of security to the one of its contractual partner[4]. Jurisdictions which rely on statutory, codified law (esp. Continental) do have less leniency in the interpretation of legal concepts than the common law ones (Anglo-Saxon). In essence, there is a considerable need to trigger a discussion around standardized legal concepts which are intended to be used for multi-jurisdictional relationships.

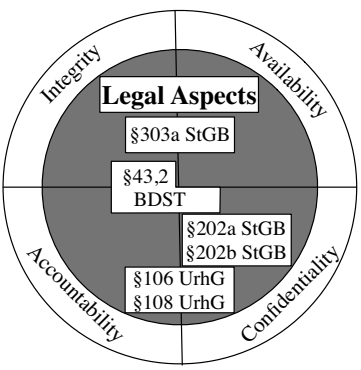


Figure 5: Legal measures

Fig. 5 summarizes the denoted regulations mapping the different security requirements. Similar to the technical measures, many regulations match multiple security requirements: Privacy law for example guards all security requirements since the data must handled in a way like a physical possession is present. Criminal law focus mainly on the availability and the integrity of the data as well as on the access. Further regulations are possible depending on concrete cases they could be applied on. Contract-based policies are excluded in Fig. 5 since they represent such a special case applicable only between the participating parties.

4 Conclusion and outlook

Secure cloud storage can neither be guaranteed by satisfying single security requirements like confidentiality or integrity only, nor by taking technical measures without suitable legal interpretations into account. Technical measures satisfying even multiple security requirements, must be established within trusted components up to the *Threshold of Technical Control*. Beyond this threshold, legal regulations must be established to guarantee throughout security. The corresponding legal applications cover thereby multiple disjunct

[4] e.g. by regulations like "You will take all reasonable measures to avoid disclosure, dissemination or unauthorized use of XY Confidential Information, including, at a minimum, those measures you take to protect your own confidential information of a similar nature."

areas of law science and heavily depend on the locality of the applied law. Nevertheless, it is mandatory that institutions and end-users are aware of the security requirements and the resulting mapping of at least the local regulations since they guard the stored data even beyond technical possibilities.

We will continue our work in three directions: The first direction, the technical side, is represented by the ongoing development of a client called Treetank [S.11, GKW11] combining the proposed technical measures to satisfy security upon the *Threshold of Technical Control*. Second, we will continue our evaluation on corresponding legal aspects and apply our findings so far to international statues as well, satisfying the global-aware nature of cloud infrastructures. Finally, we work on an in-depth evaluation of the interaction of the proposed technical measures with legal implications e.g. the impact of encrypted data in the cloud to privacy law.

References

[BCQ+11] Bessani, A., Correia, M., Quaresma, B., André, F., and Sousa, P. DepSky: dependable and secure storage in a cloud-of-clouds. In *Proceedings of the sixth conference on Computer systems*, EuroSys '11, 2011.

[BJO09] Bowers, K., Juels, A., and Oprea, A. HAIL: a high-availability and integrity layer for cloud storage. In *Proceedings of the 16th ACM conference on Computer and communications security*, CCS '09, 2009.

[Fie00] R. Fielding. *Architectural styles and the design of network-based software architectures*. PhD thesis, University of California, Irvine, 2000.

[Gar07] S. Garfinkel. An Evaluation of Amazons Grid Computing Services: EC2, S3, and SQS. Technical report, Harvard University, 2007.

[GKW11] Graf, S., Kramis M., and Waldvogel M. Treetank: Designing a Versioned XML Storage. In *XMLPrague'11*, 2011.

[GMSW06] Grolimund D., Meisser L., Schmid S., and Wattenhofer R. Cryptree: A Folder Tree Structure for Cryptographic File Systems. In *25th IEEE Symposium on Reliable Distributed Systems (SRDS)*, 2006.

[Lam01] P. Lamsal. Understanding Trust and Security. Technical report, University of Helsinki, 2001.

[MG09] Mell, P. and Grance, T. The NIST definition of cloud computing. *National Institute of Standards and Technology*, 53(6), 2009.

[S.11] Graf S. A secure cloud gateway based upon XML and web services. In *PhD Symposium, ECOWS'11*, 2011.

[Sch00] B. Schneier. *Secrets and lies: digital security in a networked world*. John Wiley, 2000.

[Sto01] G. Stoneburner. Underlaying Technical Models for Information Technology Security. *National Institute of Standards and Technology*, 2001.

Inter-Clouds: Einsatzmöglichkeiten und Anforderungen an die IT-Sicherheit

Gabi Dreo Rodosek[1], Mario Golling[1], Wolfgang Hommel[2],
Alexander Reinhold[1]

[1] Universität der Bundeswehr München, MNM-Team, Neubiberg
{gabi.dreo, mario.golling, alexander.reinhold}@unibw.de

[2] Leibniz-Rechenzentrum, MNM-Team, Garching
wolfgang.hommel@lrz.de

Abstract: Trotz der wirtschaftlichen Attraktivität und des unbestrittenen Marktpotentials gestaltet sich der Einsatz von Cloud-Computing in Deutschland weiterhin schwierig. Während auf der einen Seite gerade der Zusammenschluss von isolierten Cloud-Inseln zu Inter-Clouds („Cloud of Clouds“) verspricht, die unbestrittenen Vorteile des Cloud-Computing wie geringe Kosten durch effiziente, bedarfsgerechte Bereitstellung von Ressourcen noch weiter nach vorn zu treiben, sind Öffentlichkeit und Industrie durch die Vielzahl an Sicherheitsvorfällen der letzten Zeit für die Sicherheitsproblematik sensibilisiert worden. Dadurch rücken auch Sicherheitsfragen und -probleme beim Einsatz von Cloud-Computing stärker in den Fokus. Um daher den Unternehmen die sichere Nutzung der Inter-Clouds zu ermöglichen und nicht gegen den in Deutschland gültigen Datenschutz zu verstoßen, müssen zentrale Fragen wie Integrität, Vertraulichkeit, Nichtabstreitbarkeit, Transparenz, Authentizität und Verfügbarkeit adressiert werden. Als Basis für die Entwicklung geeigneter Sicherheitskonzepte, -methoden und -werkzeuge wird im Rahmen dieses Artikels ein Überblick über die Einsatzmöglichkeiten von Inter-Clouds sowie daraus resultierende Anforderungen an die IT-Sicherheit gegeben.

1 Einführung

Cloud-Computing verändert die Informations- und Kommunikationstechnologie (IKT) Landschaft zusehends. Die Vorteile des Cloud-Computing sind unbestritten. Neben dem flexiblen Zugriff auf Ressourcen (insbesondere bei Lastspitzen) ermöglicht Cloud-Computing auch eine schnellere Entwicklung neuartiger Anwendungen, Dienste und Lösungen, die besser an die Kundenwünsche angepasst sind. Gegen den breiteren Einsatz von Cloud-Computing spricht derzeit jedoch die mangelnde IT-Sicherheit. Ferner fordern die rechtlichen Bestimmungen hinsichtlich des Datenschutzes in Deutschland die Entwicklung neuer, eigener Cloud-basierter Lösungen.

Dadurch rücken die Sicherheitsfragen und -probleme beim Einsatz von Cloud-Computing besonders in den Fokus. Obligatorisch wird in diesem Themenkreis auch immer die Sicherheit der eigenen Unternehmensdaten genannt. Auch das Bundesdatenschutzgesetz (BDSG)

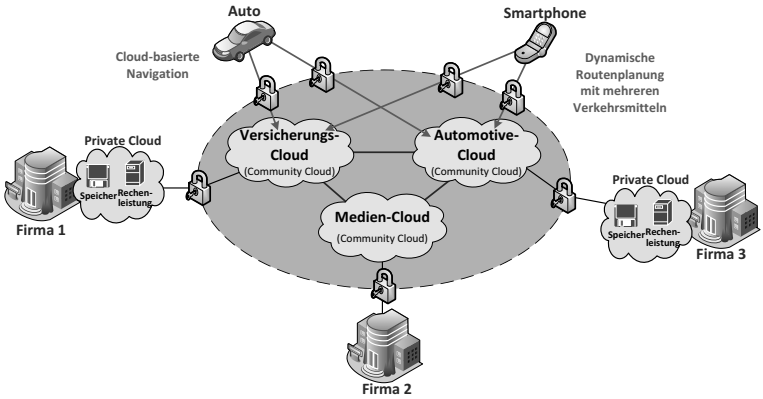


Abbildung 1: Sicherer Zusammenschluss von Clouds zu Inter-Clouds

in Deutschland stellt eine Hürde für den Einsatz von aktuellen Cloud-Computing Lösungen dar. Die großen Cloud-Computing Anbieter haben ihren Firmensitz ausschließlich in den USA und unterliegen damit dort geltenden Gesetzen, wie z. B. dem PATRIOT Act. Dieser erlaubt US-Behörden Zugriffe auf die bei den Cloud-Computing Anbietern gespeicherten Daten, ohne dass die betroffenen Kunden, d. h. die Eigentümer der Daten, informiert werden. Aus diesem Grund können deutsche Unternehmen solche Anbieter nur sehr eingeschränkt nutzen, ohne gegen die in Deutschland geltenden Datenschutzauflagen zu verstoßen.

Vint Cerf, der „Vater des Internets“, vergleicht das derzeitige Cloud-Computing mit der Zeit vor dem Internet, als versucht wurde, das ARPANET mit anderen Netzen zu verbinden (siehe auch: *Cloud-Computing and the Internet* von Vint Cerf[1]). Ähnlich wie das *Internet* der Zusammenschluss verschiedener Netze ist, ist auch die *Inter-Cloud* der Zusammenschluss verschiedener Clouds. Wie Abbildung 1 zeigt, bringt gerade der Zusammenschluss von Clouds zu Inter-Clouds den eigentlichen Mehrwert gegenüber isolierten Cloud-Inseln. Beispiele von Community Clouds sind die *Automotive-*, die *Versicherungs-*, die *Behörden-* oder die *Medien*-Cloud. Die Vernetzung von Community-Clouds ermöglicht es, Dienste und Daten aus einzelnen Community Clouds übergreifend zu innovativen Mehrwertdiensten zusammenzuführen sowie Cloud-übergreifend Ressourcen zu nutzen.

Die Voraussetzung für die sichere Vernetzung von Clouds in Inter-Clouds ist die Entwicklung einer IT-Sicherheitsarchitektur sowie die Entwicklung neuartiger Konzepte für die Datensicherheit. In diesem Beitrag werden die Einsatzmöglichkeiten und Anforderungen an die IT-Sicherheit in einer Inter-Cloud-Umgebung im Einklang mit der deutschen Rechtsprechung heraus gearbeitet.

[1] `http://googleresearch.blogspot.com/2009/04/cloud-computing-and-internet.html`

2 Terminologie

Um die Idee von Inter-Clouds veranschaulichen zu können, ist eine allgemeingültige Begriffsdefinition notwendig. Durch das National Institute for Standards and Technology (NIST) wurden im Bereich Cloud-Computing verschiedene Einsatzmodelle und Servicemodelle spezifiziert [MG11].

Die Einsatzmodelle *Public Cloud*, *Private Cloud* und *Community Cloud* unterscheiden sich hauptsächlich in der Art des Nutzerkreises der jeweilige Cloud. Bei einer Public Cloud ist der Nutzerkreis unbeschränkt, bei einer Private Cloud ist er auf ein einziges Unternehmen begrenzt. Community Clouds stellen eine zwischen verschiedenen Organisationen, die gemeinsame Interessen oder Vorgaben haben, geteilte Cloud-Infrastruktur dar.

Die Servicemodelle *Infrastructure as a Service (IaaS)*, *Platform as a Service (PaaS)* und *Software as a Service (SaaS)* variieren in der Art der angebotenen Dienste. IaaS-Dienste stellen dem Kunden selbst steuerbare hardwarenahe Ressourcen, wie z. B. Rechenkapazität und Speicherplatz, zur Verfügung, auf der er seine einige Software aufspielen und nutzen kann. PaaS-Dienste ermöglichen hingegen keine Kontrolle über die Cloud Infrastruktur, jedoch auf die Applikationsumgebung, wie z. B. dem Betriebssystem. Über die vom Provider angebotenen SaaS-Dienste können einzelne Applikationen genutzt werden; eine eigenständige Kontrolle der Cloud Infrastruktur oder eine Erweiterung um eigene Applikationen ist dabei nicht möglich.

3 Anwendungsbeispiele

In diesem Abschnitt wird die Notwendigkeit von Inter-Clouds anhand verschiedener Anwendungsfälle dargestellt. Sie wurden in enger Abstimmung mit Partnern aus der Wirtschaft erstellt und erheben somit einen Anspruch auf Realitätsnähe und Relevanz.

3.1 Inter-Cloud-basierte Navigation

Navigationsgeräte in Fahrzeugen sind weit verbreitet und führen Fahrer gut ans Ziel, indem sie das vorhandene Kartenmaterial und Eigenschaften von Verkehrswegen, z. B. Stau-Neigungen zu gewissen Uhrzeiten, auswerten und so eine möglichst gute Route vorschlagen. Aktuelle Informationen über die aktuelle Route betreffende Vorfälle können über Mobilfunk und auch per Traffic Message Channel (TMC) in die Planung aufgenommen werden, sind allerdings in ihrem Umfang limitiert. Auf Basis der Verknüpfung von Daten unterschiedlicher Quellen (bspw. intelligente Verkehrsführung, Unfallschwerpunkte, Baustellen, angemeldete Schwerlasttransporte und Straßenabsperrungen - siehe Abbildung 2) können noch komplexere Sachverhalte für Simulationen genutzt werden, die eine Berechnung von Strategien erlauben, um Staus noch effektiver zu verhindern oder abzumildern, Routen für Einsatzfahrzeuge frei zu machen oder das Risiko für Unfälle zu senken. Durch die Komplexität der notwendigen Berechnungen wird es aber erforderlich, Rechenkapazität

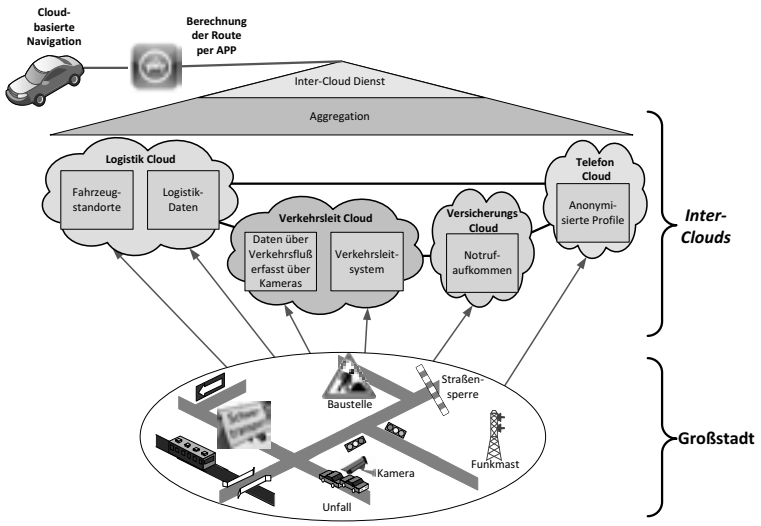


Abbildung 2: Zusammenführung von Daten unterschiedlicher Clouds zur Inter-Cloud-basierten Navigation

aus der Inter-Cloud zu nutzen, um eine zeitnahe Anpassung der Strategie erreichen zu können. So kann z. B. diese Anwendung einem sich im Stau befindenden Pendler den Weg zum nächsten Park-and-Ride-Parkplatz weisen und ihn über die öffentlichen Verkehrsmittel zu seinem Ziel lotsen, oder einen Studenten über eine Stellwerksstörung informieren und ihn zum nächsten Leihfahrrad führen.

3.2 Inter-Cloud in der öffentlichen Verwaltung

Cloud-Computing ist für die kommunale Verwaltung eine attraktive Lösung, um einfach Infrastruktur-Ressourcen (IaaS) bei Lastspitzen zuzuschalten oder Anwendungsdienste (SaaS) mit anderen Kommunen zu teilen. Während für die reine Datenspeicherung Verschlüsselungslösungen existieren, muss die Verarbeitung der Daten bis auf absehbare Zeit noch unverschlüsselt erfolgen und ist damit prinzipiell unsicher. Mit einer Klassifizierung von Daten und der Möglichkeit der Weiterverarbeitung in der Inter-Cloud können Ressourcen, die nur bei Spitzenlast gebraucht werden, aus der Inter-Cloud bezogen werden. Sensible Daten müssen hierzu pseudonymisiert werden.

Dazu muss ein generischer Dienst zur Verfügung gestellt werden, der es erlaubt, Informationen unter Berücksichtigung der Bedürfnisse der Anwender mittels Pseudonymisierung in der Inter-Cloud zu verarbeiten, wobei die zu verarbeitenden Daten unterschiedlichen Schutzbedarf haben können. Abhängig davon können bspw. Daten ausschließlich in einer Private Cloud, in einer Inter Community Cloud eines vertrauenswürdigen Partners oder in einer Public Cloud verarbeitet werden. Die vertraulichen Daten der Anwender werden

dabei stets ausschließlich in der Datenbank der Behörde gespeichert und verlassen deren Private Cloud nicht.

3.3 Inter-Cloud in der Gebäudeautomatisierung

In modernen Gebäudeautomatisierungssystemen werden permanent Sensordaten unterschiedlicher Betreiber produziert, die auf geeignete Weise ausgewertet, korreliert, protokolliert und gespeichert werden müssen, etwa Bildmaterial in Videoüberwachungssystemen, Raumluftparameter wie Temperatur und Rauchkonzentration in Brandmeldesystemen, oder Daten von Bewegungsmeldern einer Einbruchsmeldeanlage. In traditionellen Systemen werden die entstehenden Daten direkt auf den Geräten bzw. auf Zentraleinheiten im Gebäude verarbeitet und gespeichert. Durch zunehmende Netz- und Internetfähigkeit der Geräte wird es möglich, Funktionalität und Speicherkapazität nicht mehr ausschließlich lokal vorzuhalten, sondern selektiv auszulagern. Solche Systeme sind insbesondere in kleinen und mittelständischen Unternehmen (etwa Tankstellen, Bekleidungseinzelhandel, Cafés) attraktiv, weil sich so Funktionen kostengünstig bereitstellen lassen und die Fähigkeiten mit den Anforderungen dynamisch wachsen können.

Inter-Cloud-Dienste können dabei für die Analyse von Sensordaten, etwa zur Erkennung von Alarmfällen (Feueralarm, Einbruchsalarm), zur Optimierung von Heizungs-, Belüftungs- und Beleuchtungssystemen, oder zur Unterstützung von Business Analytics (z. B. Reduzierung von Wartezeiten an Kassen und Beratungspunkten) genutzt werden.

4 Anforderungsanalyse

Bereits aus den drei oben stehenden Anwendungsszenarien ergeben sich eine Vielzahl offensichtlicher Anforderungen. Vor allem die gesetzlichen Vorgaben des BDSG beeinflussen diese stark. Durch die Kumulation der Daten könnten Cloud-Anwendungen die Erstellung von personifizierten Bewegungs- und Nutzungsprofilen forcieren. Um die Persönlichkeitsrechte jedes Einzelnen zu wahren, sind Methoden zu bewerten und zu entwickeln, die die Daten soweit möglich in anonymisierter bzw. pseudonymisierter Form verarbeiten. Speziell bei der Zusammenführung von Datenbeständen unterschiedlicher Behörden stellt dies eine große Herausforderung dar, da hier unter Umständen der Personenbezug bestehen bleiben muss. Durch technische Maßnahmen muss in solchen Fällen die Verarbeitung personenbezogener Daten unter Einhaltung geltenden (deutschen) Rechts gewährleistet sein.

Zudem ist die Datensicherheit bei der Nutzung einer Inter-Cloud speziell für sensible Daten zu garantieren. Die technische Umsetzung hat sowohl die sichere Datenspeicherung und -verarbeitung als auch den sicheren Datentransport zu umfassen. Anhand von zu spezifizierenden Datenschutzklassen kann das Sicherheitsniveau für Daten festgelegt werden. In Abhängigkeit der Schutzklassen kommen unterschiedlich ausgeprägte Sicherheitsmechanismen zur Anwendung. Existierende Protokolle im Bereich Cloud-Computing können als Basis dienen und sind um die Zuordnung von Daten zu bestimmten Schutzklassen zu erwei-

tern. Die Robustheit und Verfügbarkeit von Daten und Diensten sind durch vorzuhaltende Mechanismen auch im Katastrophenfall sicherzustellen.

Der Verbund einzelner Clouds miteinander setzt gegenseitiges, verifizierbares Vertrauen der Kooperationspartner und somit ein Trust Management System voraus. Anhand von festzulegenden, objektiven Kennzahlen ist eine Klassifizierung von den beteiligten Providern als auch von den einzelnen Cloud Diensteanbietern vorzunehmen. In Abhängigkeit von den unterstützten Verfahren zur Gewährleistung der Sicherheit (Authentifizierungsverfahren, Verschlüsselungsmechanismen, Verfügbarkeit, Integrität etc.) und auf Basis der Reputation kann z. B. eine Klassifizierung vorgenommen werden.

Der sichere, organisationsübergreifende Ansatz, Daten über eine Inter-Cloud-basierte Infrastruktur miteinander auszutauschen und diese gemeinsam zu nutzen, erfordert eine organisationsübergreifende Authentifizierungs- und Autorisierungsinfrastruktur (AAI). Daraus ergibt sich zudem die Notwendigkeit eines föderierten Identitätsmanagements (FIM) für Inter-Cloud-Umgebungen.

Inter-Clouds beherbergen zum einen eine hohe Anzahl an nutzbaren, ggf. äußerst sensiblen und personifizierten Daten, zum anderen stellen sie ein hohes Maß an verteilten Ressourcen bereit. Allein durch die beiden Punkte ergeben sich neue Angriffsvektoren und Missbrauchsmöglichkeiten, die es genauer zu identifizieren gilt. Nach einhergehender Analyse und Bewertung dieser Bedrohungen sind entsprechende Verfahren zu entwickeln bzw. existierende in das Cloud Umfeld zu portieren. Dies können z. B. speziell ausgelegte, organisationsübergreifende Intrusion Detection Systeme sein.

Für alle Mechanismen, Verfahren und Prozesse für die Speicherung, Verarbeitung und für den Transport der Daten im Inter-Cloud Umfeld gilt, dass sie auditier- und verifizierbar sein müssen, um ein hohes Maß an Sicherheit und Vertrauen zu gewährleisten.

5 Analyse des Stands der Wissenschaft und Technik

Durch seine grundlegende Bedeutung für den Einsatz von Rechen- und Speicherressourcen und durch das große Marktpotenzial bedingt wird Cloud-Computing derzeit im Rahmen vieler industrieller Gremien, wissenschaftlicher Arbeiten, Studien und Projekte unter verschiedensten Blickwinkeln untersucht. Im Folgenden fassen wir eine Analyse ausgewählter Cloud-Sicherheitseigenschaften im Kontext von Inter-Clouds zusammen, um die aktuellen Möglichkeiten und Grenzen des Stands von Wissenschaft und Technik aufzuzeigen. Hierzu betrachten wir im Folgenden zunächst die aktuelle Literatur zu diesem Thema und zeigen im Anschluss eine Gegenüberstellung aktueller deutscher Cloud-Projekte.

5.1 Studien und wissenschaftliche Beiträge zur Cloud-Sicherheit

Zu den bekanntesten europäischen Studien zum Cloud-Computing gehören diejenigen der ENISA [CH09] und des Fraunhofer AISEC [SR09]. Sie betrachten die Thematik primär aus

Perspektive der Cloud-Computing-Nutzer. In den Arbeiten des BSI [Bun11] wurden komplementär dazu die Mindestsicherheitsanforderungen an Cloud-Computing-Dienstleister erarbeitet. Dabei wurden Technologien und Prozesse spezifiziert, die von Cloud-Computing-Dienstleistern umzusetzen sind. Auch das US-amerikanische NIST verfolgt das Ziel intensiv, gemeinsam mit der Industrie neue Standards zu entwickeln und Lösungen u. a. für Cloud-Interoperabilität, Portabilität und Sicherheit zu erforschen. Ferner definiert auch die Cloud Security Aliance mit der Cloud Security Alliance Cloud Controls Matrix (CCM, [Clo]) u. a. die Sicherheitsgrundsätze für Cloud-Dienstleister, um Sicherheitsrisiken besser abschätzen zu können. Die CCM bietet hierzu einen Rahmen für ein detailliertes Verständnis von Sicherheitskonzepten und Grundsätzen für Cloud-Security-Standards und zeigt die Beziehungen zu anderen Sicherheitsstandards, Vorschriften und Kontroll-Frameworks (u. a. ISO 27001, COBIT) auf. Das Global Inter-Cloud Technology Forum (GICTF) fördert die weltweite Standardisierung von Inter-Cloud-Systemschnittstellen zur Gewährleistung der Interoperabilität; ein Schwerpunkt ist die garantierte Verfügbarkeit von Diensten bei partiellem Systemausfall innerhalb einer Inter-Cloud-Umgebung [Glo10].

Diverse auch für Inter-Clouds relevante Sicherheitsprobleme sind schon in anderen Zusammenhängen umfassend behandelt worden, wie beispielsweise der sichere Datentransfer [KS05] und das sichere Datenbackup mit Hilfe von Verschlüsselung. Mehrere Forschungsvorhaben, z. B. [RTSS09], beschäftigen sich mit der Sicherheit der eingesetzten Virtualisierungstechniken. Ferner beschäftigen sich die Trusted Cloud Initiative der Cloud Security Alliance OASIS [OAS] und die Open Identity Exchange Initiative mit der sicheren Identitäts- und Rechteverwaltung im Rahmen des Cloud-Computing. In diesem Zusammenhang richten die wissenschaftlichen Arbeiten von Bertino et al. [BPFS09] und Huang et al. [HZH09] besonderes Augenmerk auf den Schutz der personenbezogenen Daten der Nutzer von Cloud Services. Celesti et al. spezifizieren die Referenzarchitektur ICIMI (InterCloud Identity Management Infrastructure), die das Problem des Identitätsmanagements in Inter-Clouds angeht [CTVP10].

5.2 Gegenüberstellung aktueller deutscher Cloud-Projekte unter Sicherheitsgesichtspunkten

Eine inzwischen recht große Zahl deutscher, zum Teil geförderter Projekte thematisiert Cloud-Computing und setzt sich dabei überwiegend explizit mit Sicherheitsaspekten auseinander. Im Folgenden konzentrieren wir uns aus Platzgründen auf solche Projekte, die mehrere Aspekte der Cloud-Sicherheit parallel in Angriff nehmen; darüber hinaus existieren zahlreiche weitere Projekte, die sich mit ausgewählten Basistechnologien wie dem Identity Management im Cloud-Umfeld auseinandersetzen.

Zu den hier betrachteten Projekten gehören im Rahmen des BMWi-Programms Trusted Cloud die Projekte CloudCycle, Value4Cloud, Sealed Cloud, SkIDentity, MIA, Cloud4E, Peer Energy Cloud, Sensor Cloud und goBerlin. Das Projekt Mimo Secco thematisiert Cloud Security im Kontext mobiler Dienstnutzung. Sec2 vertieft den Anwendungsfall Ad-hoc On Demand Virtual Private Storage. Die CollabCloud legt ihren Schwerpunkt auf Dokumentenmanagement und kombiniert Data Mining und Semantic Computing mit

Clouds. Frankfurt und Berlin haben eigene städtespezifische Cloud-Projekte; während in Berlin das Ziel Open Data im Vordergrund steht, spezialisiert sich die Frankfurt Cloud auf die Unterstützung rechen- und datenintensiver Forschungsvorhaben. Die deutsche Anteil der Eurocloud wird vom Verband der deutschen Cloud-Computing-Industrie betrieben; eine Kompetenzgruppe Recht und Compliance setzt sich dabei mit Regelungen um Datenlokationen, Archivierungsvorgaben, Abrechnungsverfahren und Eigentumsverhältnissen auseinander.

Im Rahmen des Projekts mOSAIC werden Vermittlungsdienste auf Basis einer Open Source API entwickelt. BonFIRE bietet hingegen eine kommerziell angebotete Cloud-Infrastruktur, die insbesondere räumlich verteilte Ressourcen zu einem Ganzen bündeln kann. Im Projekt VENUS-C wird eine Plattform für die Entwicklung und Forschung rund um Cloud-Services erarbeitet; StratusLab fokussiert IaaS-Plattformen auf Open-Source-Basis und erarbeitet Methoden zur einfachen Integration weiterer Ressourcen. Die Deutsche Wolke ist schließlich eine Initiative zum Aufbau einer föderierten Cloud-Infrastruktur in Deutschland auf Basis offener Standards und Open Source.

Die sicherheitsspezifischen Gemeinsamkeiten und Unterschiede dieser Projekte sind in Abbildung 3 dargestellt. Betrachtet werden dabei zum einen Datenschutzaspekte, d.h. ob personenbezogene Daten verarbeitet werden, ob bewusst Nutzungsprofile erstellt werden, ob Geheimhaltungsvereinbarungen im Rahmen industrieller Anwendungen vorgesehen sind, ob die Konformität mit dem Bundesdatenschutzgesetz explizit thematisiert wird und inwiefern eine anonymisierte Datenverarbeitung vorgesehen ist. Ferner wird betrachtet, ob die Nutzung standardisierter Protokolle vorgesehen ist und ob explizite Konzepte für die Authentifizierung, Autorisierung und das Trust Level Management existieren. Neben der einfachen Erweiterbarkeit um neue Dienste und die Berücksichtigung betriebswirtschaftlicher und rechtlicher Anforderungen werden auch die praktische Umsetzung, z. B. in Form eines Demonstrators, betrachtet.

Insgesamt zeigt sich, dass Aspekte wie die Definition und forcierte Umsetzung von Schutzklassen für Daten, die Berücksichtigung benutzerfreundlicher Sicherheitsmechanismen z. B. durch Single Sign-On, explizites Cloud-Risikomanagement, der Einsatz quantifizierender Sicherheitskennzahlen und die Zusammenarbeit mit Standardisierungsgremien noch verstärkt angegangen werden müssen. Auch die Aktivitäten im Inter-Cloud-Bereich müssen noch deutlich ausgebaut werden.

6 Zusammenfassung

Um den Unternehmen in Deutschland die sichere Nutzung des Cloud/Inter-Cloud-Computing bei gleichzeitiger Wahrung der wirtschaftlichen Vorteile desselben zu ermöglichen, bedarf es insbesondere einer ganzheitlichen IT-Sicherheitsarchitektur, die im Idealfall bereits zum Zeitpunkt des Designs integraler Bestandteil des Gesamtkonzepts ist („Security by Design"). Diese hohe Bedeutung der IT-Sicherheit für das Thema Cloud-Computing verdeutlichen u. a. die zahlreichen Förderprojekte auf nationaler und Internationaler Ebene, wie das Aktionsprogramm Cloud-Computing, die Hightech-Strategie 2020 für Deutschland

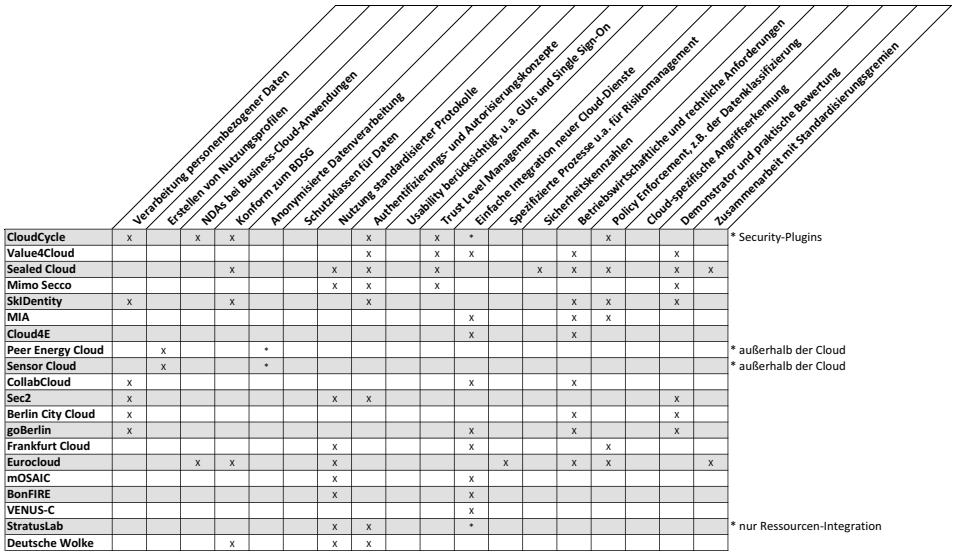


Abbildung 3: Gegenüberstellung laufender deutscher Cloud-Projekte unter Sicherheitsaspekten

oder die EU-Strategie zum Cloud-Computing.

Mit dem Ziel, Anforderungen an eine sichere Inter-Cloud-Lösung abzuleiten, wurden im Rahmen dieses Artikels in enger Kooperation mit Anwendern wie BMW, Allianz und der Landeshauptstadt München unterschiedliche Anwendungsfälle und Szenarien erarbeitet, aus denen Anforderungen an eine sichere Inter-Cloud-Lösung abgeleitet wurden. Um als Ziel diese innovativen, sicheren Inter-Cloud-basierten Mehrwertdienste in einer sicheren und vertrauenswürdigen Umgebung zu realisieren, bedarf es darauf aufbauender IT-Sicherheitskonzepte, -methoden, -prozesse und -werkzeuge, die es ermöglichen, Inter-Clouds in der gewünschten Weise sicher zu nutzen. Dazu müssen u. a. Antworten auf folgende Problemfelder gefunden werden:

- Festlegung einer Sicherheitstaxonomie
- Definition einer sicheren Inter-Cloud-Kommunikation
- Inter-Cloud Identity Management
- Angriffserkennung in einer Inter-Cloud-Umgebung
- Spezifikation von Sicherheitsmangementprozessen

In weiterführenden Forschungsarbeiten werden wir zunächst den Fokus auf die Aspekte der Datenkorrelation und Verdichtung sowie der Angriffserkennung in Inter-Clouds legen.

Danksagung

Die Autoren danken dem Munich Network Management Team (LMU, LRZ, UniBwM), den Mitarbeitern von Fraunhofer AISEC sowie Mitarbeitern von Bosch Sicherheitssysteme, Giesecke&Devrient, Infineon, SpaceNet AG, EURO-LOG, SSP Europe, Telefonica, Oracle, BMW, Allianz und der Landeshauptstadt München für wertvolle Hinweise und Diskussionen.

Literatur

[BPFS09] E. Bertino, F. Paci, R. Ferrini und N. Shang. Privacy preserving digital identity management for Cloud-Computing. *IEEE Data Eng. Bull.*, 32(1):21–27, 2009.

[Bun11] Bundesamt für Sicherheit in der Informationstechnik. *Sicherheitsempfehlungen für Cloud Computing Anbieter (Mindestsicherheitsanforderungen in der Informationssicherheit)*. Bundesamt für Sicherheit in der Informationstechnik, 2011.

[CH09] D. Catteddu und G. Hogben, Herausgeber. *Cloud Computing – Benefits, risks and recommendations for information security*. The European Network and Information Security Agency (ENISA), 2009.

[Clo] Cloud Security Alliance. Cloud Controls Matrix V1.1. `https://cloudsecurityalliance.org/research/initiatives/cloud-controls-matrix/`.

[CTVP10] A. Celesti, F. Tusa, M. Villari und A. Puliafito. Security and Cloud Computing: Inter-Cloud Identity Management Infrastructure. In *Enabling Technologies: Infrastructures for Collaborative Enterprises (WETICE)*, pages 263 –265, june 2010.

[Glo10] Global Inter-Cloud Technology Forum. Use Cases and Functional Requirements for Inter-Cloud Computing. `http://www.gictf.jp/doc/GICTF_Whitepaper_20100809.pdf`, 2010.

[HZH09] X. Huang, T. Zhang und Y. Hou. ID management among clouds. *First International Conference on Future Information Networks (ICFIN)*, pages 241–273, 2009.

[KS05] S. Kent und K. Seo. Security Architecture for the Internet Protocol. *Network Working Group, Request for Comments: 4301*, 2005.

[MG11] P. Mell und T. Grance. The NIST Definition of Cloud Computing - Recommendations of the National Institute of Standards and Technology. *Nist Special Publication*, 800-145:7, 2011.

[OAS] OASIS. OASIS Identity in the Cloud TC. `http://www.oasis-open.org/committees/tc_home.php`.

[RTSS09] T. Ristenpart, E. Tromer, H. Shacham und S. Savage. Hey, you, get off of my cloud: Exploring Information Leakage In Thirdparty Compute Clouds. *CCS '09: Proceedings of the 16th ACM conference on Computer and communications security*, pages 199–212, 2009.

[SR09] W. Streitberger und A. Ruppel. *Cloud Computing Sicherheit – Schutzziele. Taxonomie. Markübersicht.* Fraunhofer SIT, 2009.

IT-Service Management und Grids

IT-Servicemanagement Rahmenwerke – wie sie sinnvoll in Universitäten einsetzbar sind –

Silvia Knittl, Institut für Informatik
Ludwig-Maximilians-Universität München (LMU)
Achim Grindler, IT-Security und Service-Management
Karlsruher Institut für Technologie (KIT)
Karmela Vellguth, IT-Service-Desk
Technische Universität München (TUM)
knittl@nm.ifi.lmu.de, achim.grindler@kit.edu, vellguth@tum.de

Abstract: Unter IT-Servicemanagement (ITSM) versteht man Methoden und Verfahren zur Sicherstellung der optimalen Unterstützung der Geschäftsziele eines Unternehmens durch die Informationstechnologie (IT). Hierfür haben sich Standardregelwerke etabliert. Sie geben einen Rahmen vor, wie in Organisationen ITSM umgesetzt, betrieben und verbessert werden kann, indem verschiedene Prozesse festgeschrieben werden, die sich in der Praxis bewährt haben. Auf universitäre Umgebungen sind solche Vorgaben jedoch nicht ohne weiteres übertragbar. In diesem Artikel betrachten wir die besonderen organisatorischen Gegebenheiten von Universitäten und zeigen auf, welche Konsequenzen diese auf die Umsetzung von ITSM-Rahmenwerke haben. Es werden mögliche Lösungsansätze aufgezeigt, die sich in verschiedenen Universitäten bereits bewährt haben und somit auch auf andere Hochschulen übertragen werden können.

1 Motivation

Das IT-Servicemanagement (ITSM) hat zum Ziel, die Informations- und Kommunikationstechnologie (IuK) einer Organisation so zu gestalten, dass die IuK optimal die Erfordernisse der Organisation unterstützt. In der Praxis bewährte Methoden, sog. *Best Practices* haben zur Etablierung von ITSM-Rahmenwerken geführt, welche konkrete Handlungsanweisungen für das Management und das IT-Betriebspersonal darstellen. Das bekannteste Beispiel ist die IT Infrastructure Library (ITIL) [[OG07]. ITIL Version 2 bildet die Grundlage für die Norm ISO/IEC 20000.

ITSM-Rahmenwerke sind in der Regel so strukturiert, dass möglichst alle Managementaspekte eines IT-Dienstlebenszyklus berücksichtigt werden. Die aktuelle ITIL Version 3 unterteilt fünf Domänen: Servicestrategie, -entwurf, -übergang, -betrieb und kontinuierliche Serviceverbesserung. Alle empfohlenen ITSM-Prozesse werden in diesen Service Life Cycle eingebunden. Beispiele sind etwa das Serviceportfolio Management (SPM) in der Domäne Servicestrategie, der Prozess des Servicekatalog- oder Kapazitäts-Managements im Bereich des Serviceentwurfs oder das Incident Management (IM) im Bereich des operativen Servicebetriebs. Für jeden dieser Prozesse werden Ziele definiert und die zur Ziel-

erreichung notwendigen und sinnvollen Aktivitäten vorgeschlagen. Für diese Aktivitäten werden weiterhin Inputs und Outputs beschrieben, klare Rollenmodelle vorgegeben und dedizierte Leistungskennzahlen zur Prozesskontrolle und -steuerung (KPI) benannt. Auch wenn sich manche Bezeichnungen in den verschiedenen Versionen der ITSM-Rahmenwerke und die Strukturierung etwas unterscheiden, haben doch alle den gemeinsamen Anspruch, ein generisches Rahmenwerk zu liefern, das in unterschiedlichen Organisationen und Branchen seine Anwendung finden kann.

Wir zeigen in diesem Beitrag, dass sich dieser Anspruch auf Generalität in Universitäten aufgrund besonderer organisatorischer Merkmale nicht widerspiegelt. Zur Verdeutlichung beschreiben wir im folgenden Abschnitt 2 die prinzipiellen organisatorischen Merkmale, wie sie sich in vielen Universitäten im deutschsprachigen Raum wiederfinden und zeigen am Beispiel des IM die daraus resultierenden Schwierigkeiten bei der Einführung und Anpassung von ITSM auf. Im Abschnitt 3 stellen wir Ansätze für Best Practices bei der Umsetzung von ITSM dar, die sich bereits in drei verschiedenen Organisationen erfolgreich bewährt haben. Sie können nach unserer Einschätzung auch als Grundlage für die Einführung von ITSM in anderen Hochschulen dienen.

2 Organisationsspezifische Charakteristiken von Hochschulen

Nachfolgend werden die typische Aufbauorganisation von Universitäten, eine Ablauforganisation am Beispiel des IM und daraus resultierenden Herausforderungen beschrieben.

2.1 Organisatorische Gliederung

Viele Universitäten im deutschsprachigen Raum folgen der in Abbildung 1 dargestellten Gliederung. Die Leitung einer Hochschule erfolgt i. d. R. durch ein Präsidium, dem ein Präsident und eine unterschiedliche Anzahl von Vizepräsidenten vorstehen. Dieses Präsidium übernimmt meistens auch Leitungsfunktionen von wichtigen Gremien, wie etwa einer erweiterten Hochschulleitung und von zentralen Einrichtungen, wie etwa der zentralen Verwaltung. An der Ludwig-Maximilians-Universität (LMU) besteht dieses Präsidium aktuell aus einem Präsidenten und fünf Vizepräsidenten, denen jeweils thematische Schwerpunkte wie der Bereich Studium oder Berufungen zugeordnet sind. Das Präsidium des Karlsruher Instituts für Technologie (KIT) hat zwei Präsidenten und vier Vizepräsidenten mit thematischer Ausrichtung. Auch wenn diese Struktur eine hierarchische Gliederung vermuten lässt, sind die Fakultäten bzw. Fachbereiche und ihre angegliederten Lehrstühle bezüglich Mittel- und Personaleinsatz weitgehend eigenständige Organisationseinheiten (OE). Artikel 5 Absatz 3 des Grundgesetzes garantiert die Freiheit von Wissenschaft, Forschung und Lehre. Dieser Freiheitsbegriff wird instituts- und fakultätsbezogen verstanden. Die hochschulweite Koordination der OE erfolgt über die genannten Gremien. Laut [Cla83] resultiert insbesondere bei auf Gremien bzw. Lehrstühlen basierenden Organisationen eine Sammlung von „small monopolies of thousands of parts“. Dies führt nach

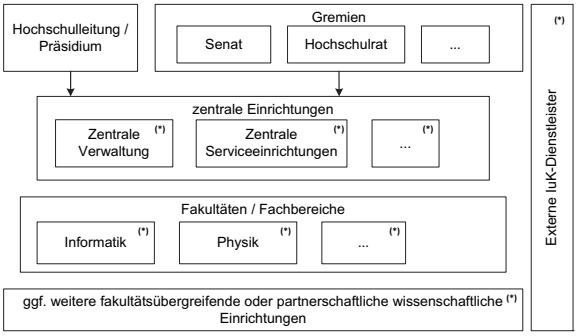


Abbildung 1: Generische Organisationsstruktur von Hochschulen [(*) = IuK-Dienstleister]

[CMO72] zu einem eher zufälligen Entscheidungsfindungsprozess, da der Zusammenfluss der Ströme „Probleme, Lösungen, Teilnehmer und Entscheidungsgelegenheiten“ zu wenig koordiniert geschieht. Wie Abbildung 1 zeigt, folgt die Struktur des IT-Betriebs und der IuK-Bereitstellung der OE-Gliederung. Die zentrale Verwaltung ist in der Regel auch für den IT-Dienst *Studentenverwaltungssystem* zuständig und Bibliothekssysteme o. ä. werden oft in zentralen Serviceeinrichtungen verantwortet. Zudem haben sich weitere dezentrale aber auch externe IuK-Dienstleister etabliert. So sind im Rahmen des Computer-Investitions-Programm (CIP) Rechnerpools für die Studierendenausbildung entstanden. Der Betrieb dieser Pools erfolgt häufig dezentral unter Verantwortung der jeweiligen OE. An der LMU gibt es derzeit ca. 20 verschiedene Rechnerpools mit teils unterschiedlichen Nutzerrichtlinien und Zugangsvoraussetzungen.[1] IuK-Dienste werden zum Teil direkt an den Lehrstühlen den verschiedenen Benutzergruppen einer Hochschule bereitgestellt. An der Technischen Universität München (TUM) wurden diverse E-Mailsysteme sowohl auf Lehrstuhl- als auch auf Fakultätsebene betrieben, bevor das Angebot zentraler E-Maildienste verfügbar war [BB10].

2.2 Prozessorientiertes ITSM an Hochschulen

Incident Management allgemein Das IM hat das prinzipielle Ziel, den (vertraglich) vereinbarten Dienstbetrieb bei Störungen schnellstmöglich wiederherzustellen. Dazu laufen im Service Desk (SD), der einen Single Point of Contact (SPOC) darstellt, alle Störungsmeldungen von Anwendern, des technischen Betriebspersonals oder von Monitoringsystemen zusammen. Anwender sind hierbei diejenigen Personen, die die IuK-Dienste tatsächlich verwenden, während derjenige, der die IT-Dienstleistung finanziert, als Kunde bezeichnet wird. Die Störungsmeldungen werden dann vom SD-Personal identifiziert, dokumentiert und einer Kategorie und Priorität zugeordnet. Sollten die SD-Mitarbeiter selbst nicht in der Lage sein, eine Störung zu beheben, werden Spezialisten beauftragt. Dieser Vorgang wird als funktionale Eskalation bezeichnet. Eine hierarchische Eskalation, d. h.

[1] `http://www.uni-muenchen.de/einrichtungen/itzentren/cip/index.html`

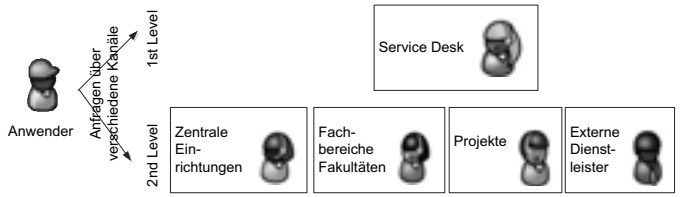


Abbildung 2: Funktionale Eskalation im Support

das Einbeziehen höherer Managementebenen, erfolgt, wenn Prozesse, Antwortzeiten o. ä. nicht mehr den definierten Vorgaben (Service Level) entsprechen. Typische KPI zur IM-Prozesssteuerung sind z. B. die durchschnittliche Lösungszeit, die Erstlösungsrate des SD oder die Anzahl der bearbeiteten Anfragen je Mitarbeiter.

Incident Management an Hochschulen An vielen Universitäten wurden ein IM mit SD nach ITIL-Vorgaben etabliert. Abbildung 2 zeigt eine funktionale Aufteilung in einen 1st- und einen 2nd-Level Support. Diese beziehen sich auf die oben beschriebenen OE der Dienstbetreiber. Weitere vorhandene Unterteilungen sowohl der Support-Level als auch der IT-Dienstleister werden aus Übersichtsgründen nicht dargestellt. So erfolgt die Benutzerunterstützung i. d. R. direkt durch die jeweiligen Dienstbetreiber, welche meistens zentrale Einrichtungen, aber auch Fachbereiche, Fakultäten, Lehrstühle, externe Dienstleister oder im Rahmen von Drittmitteln finanzierte IT-Projekte sind. Für die Benutzer ergeben sich somit vielfältige Kanäle zur Inanspruchnahme von Supportleistungen. Aufgrund der gestiegenen Ansprüche der Anwender an die Funktion und Qualität der IT-Dienste ist das Bewusstsein, dass eine (Re-)Zentralisierung der Strukturen und Prozesse vorteilhaft sein kann, gewachsen. Am KIT wurden vorrangig die durch die Fusion des Forschungszentrums und der Universität Karlsruhe geführten IT-Projekte, wie das campusweite Identitätsmanagement oder die Migration von Systemen und Diensten in die neue KIT.EDU-Domäne, hauptsächlich durch zentrale Dienstleister begleitet und umgesetzt. Die Zentralisierungserfolge an der TUM im Rahmen des Projektes IntegraTUM, das „zum Ziel die Schaffung einer benutzerfreundlichen und nahtlosen Infrastruktur für (..) (IuK) an der TUM “ hatte [BB10], schufen die Grundlage für eine weitere Prozessorientierung. So wurde ein SD eingeführt, der sich zuerst auf die Anfragen innerhalb des IntegraTUM-Dienstangebots konzentrierte. Die Benutzer nahmen dieses Angebot über ein SPOC dankbar an. Damit ein Anwender bei Fragen oder Problemen zu IT-Diensten die zuständige Stelle findet, war es oft notwendig mehrere Ansprechpartner zu kontaktieren. Dies machte den Supportprozess umständlich und langwierig. In den meisten Fällen handelte es sich bei diesen Ansprechpartnern um Mitarbeiter verschiedener Fakultäten, die ihre Rolle des IT-Supporters unfreiwillig annehmen mussten. Der neue SPOC erleichterte die Behebung der Probleme und Störungen (Incidents) deutlich. Auch am KIT führte die Einführung eines gemeinsamen IM mit SD im fusionierten Rechenzentrum, Steinbuch Centre for Computing (SCC), zu merklichen Verbesserungen bei der Störungsmeldung und -behebung. Der Fokus lag auf intern erbrachten Diensten. Wie die Abbildung 2 verdeutlicht, gibt es jedoch zwischen den vorhandenen Supportstufen, dem SD und den Supporteinheiten der

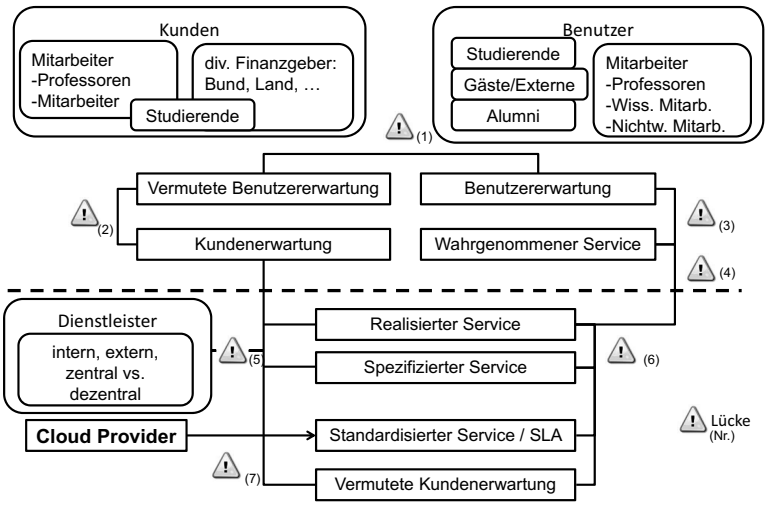


Abbildung 3: Gap-Modell nach [HBS06] mit eigenen Erweiterungen

verschiedenen OE keine direkten Kompetenz- bzw. Zuständigkeitsregelungen. Die daraus resultierenden Probleme werden im folgenden Abschnitt beschrieben.

2.3 Folgen: Struktur und Prozess folgen nicht denselben Hierarchien

Will man ITSM-Prozesse in einer traditionell sektoral gegliederten Hochschule einführen, müssen die notwendigen Prozessaktivitäten nun quer durch die verschiedenen OE ablaufen. Dies macht eine enge Koordination zwischen den verschiedenen Prozessbeteiligten erforderlich. Erläutert wurde dieser Sachverhalt am Beispiel des IM, kann aber ebenso in anderen ITSM-Disziplinen, wie z. B. dem Change Management beobachtet werden. Wie eingangs dargestellt, trennen die ITSM-Rahmenwerke klar zwischen den Rollen Anwender und Kunde, wobei letzterer für die Beauftragung und Finanzierung von IuK zuständig ist. Das GAP-Modell ist eine weitverbreitete Methode zur Einschätzung der Dienstqualität von Organisationen. Es stellt dazu systematisch die Leistungserwartungen der Kunden und Anwender den von den Dienstleistern erbrachten Leistungen gegenüber. Abbildung 3 zeigt diese Einteilung im Kontext von Hochschulen. Die organisatorische Aufteilung von Hochschulen ergibt ein klares Rollenmodell für die Abbildung der Kernprozesse Forschung, Lehre und Innovation mit den dafür typischen Rollen wie Student, Mitarbeiter oder Lehrbeauftragter. Eine entsprechende Rollenverteilung zur Abbildung von ITSM-Prozessen kann jedoch nicht unmittelbar aus dem Organigramm abgeleitet werden. Die grundlegende Finanzierung von Hochschulen und damit auch die von IuK-Diensten bzw. teils von IuK-Personal erfolgt aus einer Kombination von: a) staatlichen Mitteln (Land, Bund), b) Drittmitteln, die häufig auf Ebene der dezentralen OE eingeworben werden und sowohl von staatlichen als auch im Rahmen von Industriekooperationen bereit gestellt werden, c)

Einnahmen durch Studiengebühren, d) Spenden von z. B. Alumni- oder Fördervereinen. Will man den Kundenbegriff von ITIL direkt auf Hochschulen adaptieren, müssen Gruppen von Stakeholdern als potentielle Kunden identifiziert werden. Dies verkompliziert das von den ITSM-Rahmenwerken geforderte Ausrichten der IuK an den Kundenbedürfnissen (Lücke 1-3). Aufgrund der komplexen Stakeholderstruktur ist es auch für einen internen IT-Dienstleister oft unklar, wer was beauftragen kann bzw. darf. Diese komplexen Strukturen führen häufig dazu, dass sich die Anwender in der Rolle des Kunden wähnen, oder der IT-Dienstleister eigenmächtig Vorgaben für eine IT-Strategie definiert. Der Bezug externer IT-Leistungen führt bei fehlender Anpassungsmöglichkeit zu weiterem Vermittlungs- bzw. Integrationsbedarf zwischen IT und Kunde/Anwender (Lücke Nr. 6,7). Insbesondere trifft das Problem bei Cloud-Diensten zu, bei denen es sich um hoch standardisierte Dienste mit entsprechend standardisierten AGBs handelt.

ITSM-Rahmenwerke geben hinsichtlich verteilter ITSM-Prozesse wenig Gestaltungshinweise. Als Lösung werden vertragliche Leistungsvereinbarungen durch sogenannte Operational Level Agreements (OLA) mit internen oder Underpinning Contracts (UC) mit externen Leistungserbringern empfohlen. Diese Art vertraglicher Leistungsvereinbarungen ist in Hochschulumgebungen kaum durchsetzbar. Gründe dafür sind u. a. ein nicht durchgängig definiertes und kommuniziertes Dienstangebot, mangelnde Transparenz bzgl. der Zuständigkeiten, aber auch eine oft fehlende oder unzureichende Leistungsverrechnung von IT-Diensten. Hinzu kommt die besondere Personalsituation an Hochschulen: IuK-Mitarbeiter sind oft in befristeten (wissenschaftlichen) (Projekt-)Stellen beschäftigt. Die dadurch entstehende hohe Fluktuation und der damit verbundene Know-how-Verlust erschwert es dem IT-Management, längerfristige und verbindliche Zusagen für IT-Dienstgüteparameter abzuschließen. Zudem erschwert die Einbettung in die Tarifstruktur des öffentlichen Dienstes die Umsetzung von z. B. Bereitschaftszeiten für den IT-Betrieb. Im Münchner Hochschulumfeld führt das dazu, dass selbst der primäre IT-Dienstleister, das LRZ, lediglich „best-effort“ als Dienstqualität garantieren kann.[2] Den Ansprüchen der Anwender nach einer besseren Dienstqualität kann auf Seiten des IT-Dienstleisters nur mit technischer Redundanz begegnet werden.

Die Prozessorganisation an der TUM gestaltet sich innerhalb des IM-Prozesses aufgrund der mangelnden Weisungsbefugnis für die SD-Leitung zu einer echten Herausforderung. Die prozessorientierte Aufteilung des IM in verschiedene Stufen (1st-Level, 2nd-Level, ...) folgt nicht der organisatorischen Zuständigkeit innerhalb der angefragten IT-Themen- und -Aufgabenbereiche. So ist eine durchgreifende Lösung der Probleme für die SD-Leitung nur begrenzt möglich, etwa wenn Anfragen langsam oder in Extremfällen sogar überhaupt nicht bearbeitet werden.

Die in den ITSM-Rahmenwerken vorgeschlagenen Kennzahlensysteme zur effizienten Steuerung der ITSM-Prozesse fehlen an Universitäten oder sind aufgrund der organisatorischen Gegebenheiten nur schwer umsetzbar. Leistungskennzahlen (KPI), wie etwa die der bearbeiteten Anfragen je Mitarbeiter könnten sowohl zur Kontrolle der Prozessleistung als auch zur Kontrolle der Mitarbeiter verwendet werden. Deshalb ist laut Betriebsverfassungsgesetz die Mitbestimmung des Betriebs- oder Personalrates erforderlich. Dieser Umstand kann zu einer größeren Hürde innerhalb des Einführungsprozesses von ITSM

[2] `http://www.lrz.de/wir/regelwerk/dienstleistungskatalog.pdf`

führen und muss daher sorgfältig und rechtzeitig betrachtet werden. Ein weiterer Aspekt ist der hohe Aufwand, der bei der Einführung von über Kennzahlen kontrollierten Prozessen entsteht, vor allem dann, wenn die ITSM-Prozesse verteilt und ohne integrierte Werkzeugunterstützung gelebt werden sollen.

3 ITSM-Empfehlungen für Universitäten

ITSM-Leitfäden werden hier vorgestellt, um eine effizientere Unterstützung der Erfordernisse eines modernen Hochschulbetriebs durch die IuK zu ermöglichen. Sie haben sich bereits an Universitäten bewährt und beziehen sich auf eine gesamtheitliche Struktur der IT-Governance. Diese umfasst hierbei die Führung, Organisationsstruktur und Prozesse. Die Studie in [Sch10] ergab eine derzeit wenig ausgeprägte Reife der IT-Governance im deutschen Hochschulumfeld. Wir zeigen die Vorteile der Einführung einer IT-Governance-Struktur für die Anwendung von ITSM-Rahmenwerken in Universitäten und welche der oben aufgezeigten Kommunikationslücken sich dadurch reduzieren lassen.

3.1 Führung und Organisationsstruktur

Eine an den Benutzerbedürfnissen orientierte IuK stellt auch an Hochschulen einen wichtigen Erfolgsfaktor dar. Deshalb muss die IuK-Strategie auch als Führungsaufgabe wahrgenommen werden und nicht wie oben dargestellt, Ergebnis oft zufälliger Entscheidungsprozesse sein. Bewährt hat sich hierbei die Etablierung einer dedizierten IuK-Führungsstruktur. An der TUM und am KIT wurden dazu die Rolle eines Chief Information Officers (CIO) eingeführt. Die etablierte Autonomie der Organisationseinheiten wird hierbei nicht in Frage gestellt. Der CIO steht einem Gremium vor, welches gemeinsam die IuK-Strategie prägt. Dieses ist an der TUM mit je einem Information Officer (IO) aus jeder Fakultät besetzt. Mit steigender Reife der IT-Governance kann die Rolle eines CIO auch immer mehr an Weisungsbefugnissen erhalten. Auch am KIT ist der CIO hochschulweit für die gesamten IuK-Aktivitäten zuständig und mit den erforderlichen Entscheidungskompetenzen ausgestattet. Bewährt haben sich innerhalb dieser Struktur auch fachspezifische Gremien, die gültige Regelungen z. B. zum Arbeitsschutz, IT-Nutzung, IT-Sicherheit oder Recht ausarbeiten. Somit kann der CIO bzw. das CIO/IO-Gremium den Servicebedarf mit den Anwendern identifizieren und definieren und dadurch klare Aufträge an die IT-Dienstleister stellen. Durch diese zentrale Koordination von IuK-Fragen wird die vorher aufgezeigte Lücke zwischen Dienstleister und Kunde geschlossen.

Neben der Etablierung einer klaren IuK-Führungsstruktur haben sich weitere organisatorische Anpassungen bewährt. Es sind neben der Rolle des CIO noch weitere an die ITSM-Rahmenwerke angelehnte Rollen notwendig und in der Organisationsstruktur abzubilden und zu kommunizieren. So sind die Mitglieder eines Change Advisory Boards (CAB) so festzulegen, dass darin die zuständigen Entscheidungsträger vertreten sind. Am KIT wird das CAB flexibel zusammengestellt und besteht aus Vertretern der Leitung, Mit-

gliedern der Fakultäten und Instituten, sowie den Dienstleistungseinheiten. Gemeinsam werden Anforderungen an Dienste spezifiziert und Pilotservices aufgesetzt. Die Rolle des Change-Managers ist am SCC des KIT transparent. Die Kommunikation von Änderungen bzw. Wartungen zwischen der IT und den Anwendern erfolgt über festgelegte Kommunikationskanäle. An der TUM erfolgen diese Aufgaben im Rahmen der neu gegründeten Gremien IT-Koordinierungskreis und IT-Steuerkreis mit ähnlicher Zusammensetzung und Aufgabenaufteilung wie am KIT. Diese Gremien vereinfachen und verbessern die Kommunikation mit und innerhalb der IuK-OE deutlich, wodurch sich die oben aufgezeigte Lücke zwischen den verschiedenen IT-Dienstleistern und den Kunden wiederum schließt. Zur Verringerung der Kommunikations- und Koordinationslücke zwischen den Anwendern und deren Erwartungshaltung bzgl. der IT-Dienste hat es sich bewährt, sog. Stakeholder-Foren einzuführen (vgl. S. 35ff, in: [BB10]). Am SCC des KIT wurde die Rolle des Servicemanagers etabliert und kommuniziert. Anwender haben somit die Möglichkeit direkt an dieser Stelle Anregungen, Kritik und Lob einzubringen.

3.2 Prozesse

Die in den ITSM-Rahmenwerken geforderte Prozessorientierung kann auch an Hochschulen erfolgreich etabliert werden. Hierzu sind aber eigene Anpassungen aufgrund der dargestellten Dezentralität notwendig. Eine ITIL-Orientierung unterstützt dabei die Schaffung einer einheitlichen Begriffswelt und eines gemeinsamen Verständnisses der ITSM-Prozesse. Bei der Umsetzung von ITSM sind gemäß der Rahmenwerke Prozesse, Rollen und Werkzeuge einzuführen. Nach unserer Einschätzung empfehlen wir, mit dem Service Portfolio Management (SPM) und dem Incident Management (IM) zu beginnen. Diese beiden Prozesse verringern die oben dargestellten Lücken. Auch die Kommunikation zwischen Kunden und IT (SPM) bzw. zwischen Anwender und IT (IM/SD) wird verbessert.

Service Portfolio Management Ziel des SPM ist die auf die Vorhaben und Ziele der Kunden ausgerichtete Definition, Gestaltung und Zusammenstellung der zu erbringenden IT-Services. Hierbei ist auf ein angemessenes Investitionsniveau zu achten. Ein umfassend dokumentierter Dienstleistungskatalog (ITSK), in dem alle IuK-Dienste samt Zuständigkeiten, Abhängigkeiten und Nutzungsvoraussetzungen erfasst sind, schafft die notwendige Transparenz nach innen und nach außen. Er dient außerdem als Diskussions- und Kommunikationsgrundlage mit den Stakeholdern. Am KIT ist die Aufgabe des SPM auf mehrere Rollen verteilt (Servicemanager, Serviceverantwortliche und IT-Teams). An der TUM wird der ITSK auch verwendet, um u. a. neu gegründeten Organisationseinheiten einen Überblick über das IuK-Angebot zu verschaffen und damit die Kommunikation mit dem TUM-IT-Management zu fördern.

Incident Management Auch ohne direkte Weisungsbefugnis kann ein IM mit (integriertem) SD für Anfragen aller Anwender an Hochschulen erfolgreich etabliert werden. Der Vorteil ist die unmittelbare Vereinfachung des Anwenderzugangs zu IT-Diensten und eine

verbesserte Kommunikation durch den SD als „Information Hub“ zwischen IT, Anwender und IT-Management. Am KIT werden Anfragen über ein zentrales Ticketsystem erfasst und bearbeitet. Betriebliche Meldungen werden über eine einheitliche Meldeseite kommuniziert. An der TUM übernimmt der SD die eingehenden Anfragen und koordiniert die funktionale Eskalation an die Fachbereiche. Der Vorteil einer einzigen Benutzerschnittstelle wurde auch von den dezentralen IT-Dienstleistern und IT-Beauftragten erkannt und wird mittlerweile von ca. 250 Supportmitarbeitern aus den verschiedenen OE genutzt. Die Einführung von SPM und IM und ihre hochschulinterne Anpassung empfiehlt sich als erstes bei der ITSM-Orientierung. Erst mit steigendem Reifegrad ist die Einführung anderer ITSM-Prozesse sinnvoll. Am SCC des KIT erfolgte etwa die Einführung eines Change- und Configuration-Managements. Auch hierfür wurden Rollen festgelegt und Prozesse definiert. Weiterhin wird auch eine geeignetere Werkzeugunterstützung evaluiert.

Werkzeugunterstützung Ein integriertes, prozessorientiertes ITSM und dessen Steuerung und Kontrolle in einer über verschiedene hierarchische Strukturen verteilten Hochschule erfordert eine geeignete Werkzeugunterstützung. Die Verwendung von E-Mail hat sich hierbei als denkbar ungeeignet erwiesen. Kollaboratives Arbeiten und Möglichkeit einer zentralen Auswertung sind so nicht gegeben. Eine hohe Mitarbeiterfluktuation führt ebenso zu Problemen, da bestehende Inhalte der bisher geführten Kommunikation für andere nicht mehr zugreifbar sind. Die Verwendung von Shared-Mailboxen ist aufgrund mangelnder globaler Auswertbarkeit und unübersichtlicher Bedienbarkeit (vor allem bei großen Anwendergruppen) nicht ratsam. Es sollte deshalb ein integriertes ITSM-Werkzeug zum Einsatz kommen, das an den etablierten bzw. geplanten Reifegrad der Prozesse angepasst werden kann. Dem aktuellen Reifegrad entsprechend wird deshalb sowohl an der TUM als auch an der LMU das open-source-Werkzeug otrs (Open Ticket Request System) als Ticketsystem verwendet. Am KIT bildet eine integrierte Dokumentationsplattform die Servicekonfigurationsdaten strukturiert ab und verknüpft sie mit weiteren Prozessen (Definition der Zuständigkeiten und Abhängigkeiten bzgl. der IT-Services, Veröffentlichung im Online-Servicekatalog und Meldungswebseite). Diese Konfigurationsdaten werden auch für das zentrale Ticketsystem, das Incident und das Change Management genutzt und stellen die Grundlage für das ITSM dar.

Kennzahlen Zur belastbaren Darstellung der Effektivität der IT-Dienste bedient sich die IuK-Führung geeigneter Kennzahlen (KPI). Diese sind individuell entsprechend der erwarteten und vereinbarten Leistungsziele der Geschäftsprozesse festzulegen und zu kommunizieren. So können sie durch die Leitung und die Serviceverantwortlichen qualitativ und quantitativ verfolgt werden. Da, wie oben dargestellt, nicht alle in den ITSM-Rahmenwerken vorgeschlagenen KPI im Hochschulumfeld sinnvoll anwendbar sind, ist eine an den jeweiligen Reifegrad angepasste Auswahl zu treffen. Eine Grundlage kann etwa die in [SUB08] vorgeschlagene Balanced Scorecard liefern, bei der die verschiedenen Perspektiven der Stakeholdergruppen bzgl. ihrer Erwartungen in Beziehung gebracht werden kann. Die Etablierung von Kennzahlensystemen zur Steuerung und Kontrolle von ITSM-Prozessen ermöglicht dann die bessere Vergleichbarkeit auch zwischen Hochschul-IuK, wie sie etwa im amerikanischen Raum längst gegeben ist (vgl. [DCA04]).

4 Zusammenfassung und Ausblick

Die Professionalisierung der IuK gewinnt auch an Universitäten immer mehr an Bedeutung und führt zur Einführung von ITSM-Rahmenwerken. Diese setzen implizit organisatorische Merkmale, wie hierarchische oder vertragsbedingte Weisungsbefugnis und Koordination voraus, die aber an Universitäten meist nicht gegeben und umsetzbar sind. Deshalb sind neue, angepasste „Best Practices“ notwendig. Aus unserer praktischen Erfahrung sind einige von ITIL empfohlene Prozesse und Funktionen einsetzbar. Hierzu zählen die Prozesse Incident, Change, Service Portfolio und Configuration Management. Kontrollmöglichkeiten der Prozessumsetzung wie z. B. KPI und Leistungsmessung sind anfangs nicht anwendbar. Bewährt hat sich dagegen die Etablierung einer dedizierten IT-Governancestruktur, welche u. a. Rollenmodelle zur besseren Abstimmung der IuK-Strategie (CIO/IO, Servicemanager, SD, ...) definiert und somit vorhande Kommunikations- und Koordinationslücken weitgehend schließt. Die Einführung eines SD als SPOC vereinfacht für den Anwender den Kontakt zu seiner IT und beschleunigt die Vorfallsbearbeitung durch das zentral vorgehaltene Know-How und einen definierten Supportprozess. Weitere Rezentralisierungs- und Konsolidierungsbemühungen in der IuK und die Einführung von Cloud-Diensten unterstützen die Konzentration auf eine IT-Governance, erfordern aber eine stärkere Kommunikation mit den betroffenen Stakeholdern. Ein Stakeholderprinzip, wie es am KIT gelebt wird, kann hierbei als vorbildliche Praxis auch von anderen Hochschulen übernommen werden.

Literatur

[BB10] Bode, A. und Borgeest, R., Herausgeber. *Informationsmanagement in Hochschulen*. Springer Berlin Heidelberg, März 2010.

[Cla83] Clark, B. R. *The higher education system: Academic organization in cross-national perspective*. University of California Press, 1983.

[CMO72] Cohen, M., March, J. und Olsen, J. A Garbage Can Model of Organizational Choice. *Administrative Science Quarterly*, 17:1 – 25, 1972.

[DCA04] Dowling Dougherty, J., Clebsch, W. und Anderson, G. Management by Fact: Benchmarking University IT Services. *EDUCAUSE Quarterly*, 27(1), 2004.

[HBS06] Huppertz, P. G., Bause, M. und Swidlowski, S. *IT-Service - Der Kern des Ganzen*. Serview GmbH, 2006.

[[OG07] [OGC]. *ITIL V3 complete suite - Lifecycle Publication Suite*. The Stationery Office Ltd, 2007.

[Sch10] Schwabe, G. IT-Governance an Universitäten in Deutschland, Schweiz und Österreich. In *ZKI-Herbsttagung 2010 - IT-Governance und IT-Infrastrukturmanagement in europäischer Ausprägung*, September 2010.

[SUB08] Schulz, V., Uebernickel, F. und Brenner, W. Erfolgsmessgrössen bei IT Shared Service Organisationen. In Bichler, M. et al., Herausgeber, *Multikonferenz Wirtschaftsinformatik*. GITO-Verlag, Berlin, 2008.

Das bwGRiD – „High Performance Compute Cluster“ als flexible, verteilte Wissenschaftsinfrastruktur

Marek Dynowski[a], Michael Janczyk[a], Janne Schulz[a], Dirk von Suchodoletz[a]
Sven Hermann[b]

[a] Technische Fakultät / Rechenzentrum
Albert-Ludwigs Universität Freiburg
[b] Steinbuch Centre for Computing
Karlsruher Institut für Technologie (KIT)

marek.dynowski@rz.uni-freiburg.de
michael.janczyk@rz.uni-freiburg.de
janne.schulz@rz.uni-freiburg.de
dirk.von.suchodoletz@rz.uni-freiburg.de
sven.hermann@kit.edu

Abstract: Das bwGRiD-Projekt startet 2008 an acht Universitäten in Baden-Württemberg, um Wissenschaftlern aller Fachrichtungen Ressourcen im Bereich des High Performance Computings effizient und hochverfügbar zur Verfügung zu stellen. Im Vordergrund steht der Aufbau einer dezentralen Grid-Struktur, bei der homogene Parallelrechner-Cluster transparent zu einem Grid-Verbund gekoppelt werden. Das Projekt soll die Machbarkeit und den Nutzen von Grid-Konzepten für die Wissenschaft nachweisen und bisherige Organisations- und Sicherheitsproblematiken überwinden. Die Grid-Struktur ermöglicht eine Spezialisierung der einzelnen Rechenzentren im Anwendungs und Hardwarebereich, sowie die Entwicklung neuer Cluster- und Softwarewerkzeuge. Die durch diese Struktur entstehende Lizenzproblematik für proprietäre Software soll im Rahmen dieses Projektes gelöst werden. Durch den kontinuierlichen Ausbau der lokalen bwGRiD-Cluster und die Integration neuer Standorte kommt es zu einer wachsenden Heterogenität, welche durch die stetige Weiterentwicklung von Software und Konzepten überwunden werden muss, um eine maximale Kompatibilität zwischen den Standorten zu gewährleisten. Die Hardware des Projektes wurde vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen der D-Grid-Initiative und die Personalstellen vom Ministerium für Wissenschaft, Forschung und Kunst (MWK) Baden-Württemberg finanziert. In diesem Artikel werden Konzepte, Erfahrungen und Resultate des bisherigen bwGRiD-Projektes vorgestellt.

1 Das bwGRiD – ein Community-Grid im Südwesten

Die Konzepte der Compute- und Daten-Cloud werden im Zusammenhang mit wissenschaftlichem Rechnen zunehmend diskutiert und umgesetzt. Die hierbei formulierten Ziele wie Resource-On-Demand, schnelles Deployment, flexible Anpassung an bestimmte Nutzerwünsche, Virtualisierung von Ressourcen und geographische Verteilung sind oft

gar nicht so neu und vielfach bereits Realität [BK10]. Das bwGRiD ist Teil der D-Grid-Initiative [Gen06] der Bundesregierung und wurde mithilfe einer Infrastrukturförderung des BMBF und mit zusätzlicher finanzieller Unterstützung des Landes Baden-Württemberg auf Basis des Landeshochschulnetzes BelWue realisiert. Der gewählte Ansatz ist eine dezentrale Struktur, bei der die über das Land verteilten Cluster mit Hochgeschwindigkeitsdatenleitungen vernetzt werden.

Die Gründungsmitglieder des bwGRiD-Projektes sind, zunächst unter Federführung des Stuttgarter Höchstleistungsrechenzentrums (HLRS), die Universitäten Freiburg, Heidelberg, Karlsruhe, Konstanz, Mannheim, Tübingen und Ulm. Später schließt sich Esslingen als erste Hochschule dem Projekt an [RV10]. Das Ziel des Projektes ist die Untersuchung von „High Performance Computing"-Grids (HPC) im Hochschulumfeld hinsichtlich ihres Nutzens, sowie die Identifikation der verschiedenen Anforderungen an solche Umgebungen [Mic06]. Zu diesem Zweck werden die lokalen HPC-Cluster für die Nutzer transparent zu einem Verbund zusammengeschlossen. Diese Struktur soll sicherstellen, dass verfügbare Computing-Ressourcen für die akademische Forschung standortunabhängig und hochverfügbar bereitstehen. Geprägt wird diese Infrastruktur durch gemeinsame Standards beim Zugriff auf die Ressourcen, Authentifizierung und der Verteilung der Jobs. Dabei wird keine durchgehend einheitliche Hardware gefordert, jedoch wurden zu Projektbeginn identische Komponenten gemeinsam beschafft, um die Vorteile eines solchen Vorgehens zu evaluieren. Dieser Ansatz löst das klassische, zentralisierte HPC ab. Nicht einzelne Forschungseinrichtungen oder Arbeitsgruppen mit Bedarf an Rechenleistung beschaffen und betreiben ihre eigenen Cluster. Stattdessen werden die Aufwendungen in einen gemeinsamen Pool überführt, um diese in Summe effektiver einsetzen zu können. Das Konzept erlaubt neben einem verbesserten Support durch eine größere Anzahl von Administratoren und Entwicklern auch die HPC-Versorgung mit unterschiedlicher Hard- und Software, was auch die Bildung von untereinander vernetzten lokalen Kompetenzzentren für wissenschaftliche Fachbereiche ermöglicht. Dadurch kann gezielter auf die Erfordernisse der verschiedenen Wissenschaftsdisziplinen und Forschergruppen eingegangen werden und die daraus resultierenden Aufgaben lassen sich zwischen den Projektpartnern aufteilen. Ferner wird eine höhere Effizienz der Ressourcennutzung durch optimale Auslastung über den gesamten Lebenszyklus der Cluster-Hardware erzielt.

Eine entscheidende Rolle spielt das Betriebskonzept, das auf der einen Seite den Benutzern eine stabile und performante Umgebung sicherstellt, auf der anderen Seite jedoch flexibel auf neue Anforderungen, wie Erweiterungen der Hardwarebasis oder Modifikationen der Softwareausstattung, reagieren muss. Die Projektpartner im bwGRiD entwickeln und prüfen entsprechende Konzepte hinsichtlich einer gemeinsamen Sicherheitsstruktur zwischen den Rechenzentren zur Lösung von Organisations- und Sicherheitsproblematiken. Weitere zentrale Herausforderungen sind zudem der Aufbau einer performanten, verteilten Datenhaltung sowie die Integration unterschiedlicher Nutzerverwaltungen der jeweiligen Standorte. Die Koordination gemeinsamer Beschaffungen der im Projekt vorgesehen Soft- und Hardware soll die Anschaffungskosten für alle Beteiligten senken, Wartungsverträge optimieren und den gegenseitigen Support zwischen den Rechenzentren erleichtern. Ein weiteres erklärtes Ziel des Projektes liegt in der Unterstützung vielfältiger Forschungsfelder, weshalb dezidiert Mittel für Lizenzen kostenpflichtiger Software bereitgestellt wur-

den. Hierbei wird auch die Lizenzproblematik für den Grid-Verbund analysiert und evaluiert. Des Weiteren werden die zur Verfügung stehenden Ressourcen für eine Optimierung von Grid-Konzepten für Forschergruppen die bereits im HPC-Bereich aktiv sind genutzt. Auch hat in den letzten Jahren das Hochleistungsrechnen in vielen nicht-klassischen HPC-Disziplinen erheblich an Bedeutung gewonnen. Daher kommt dem Heranführen solcher Forschergruppen an „High Performance"- und Grid-Computing, durch innovative und speziell für diese Gruppen entwickelte Werkzeuge, Hilfestellungen und Dokumentationen, eine außerordentliche Bedeutung in dem Projekt zu.

2 Verteilte Hardware – verteilte Systeme

Das bwGRiD, zunächst als ein dezentrales Grid homogener Cluster geplant und beschafft, wurde im Laufe der Zeit aufgrund von Nutzeranforderungen und Investitionen von Arbeitsgruppen an einigen Standorten heterogen ausgebaut (siehe Abbildung 1). Die Hauptinvestition bestand zunächst aus 101 Bladecentern des Typs H von IBM, die jeweils 14 Blades des Typs HS21 XM[1] fassen. Im Primärausbau des bwGRiDs entspricht das einer Gesamtzahl von 11312 Kernen und 22624 GByte RAM. Um die Rechenleistung des Clusters vollständig nutzen zu können, sind die Rechenknoten an den Standorten mit einem 20 Gbit/s-InfiniBand-Netzwerk verbunden.[2] Untereinander sind die Cluster über das BelWue-Netz mit 10 Gbit/s angeschlossen. Dies ermöglicht einen schnellen Datentransfer und gewährleistet dem Nutzer eine hohe Flexibilität bei der Auswahl des jeweiligen Standortes.

Die 101 Bladecenter wurden, mit Ausnahme von Stuttgart, gleichmäßig an alle teilnehmenden Standorte verteilt (Stuttgart erhielt 31 Bladecenter). Die restlichen Standorte wurden mit je 10 Bladecentern ausgestattet, wobei der Cluster in Konstanz mit dem Cluster am Standort Ulm vereint wurde. Die Heidelberger und Mannheimer Cluster wurden 2009 über eine InfiniBand-Glasfaser-Kopplung miteinander verbunden [RHKK10]. Esslingen investierte 2009 in 180 Appro-Bladeserver gB222X[3] von NEC. Damit wuchs das bwGRiD auf eine Gesamtzahl von 1594 Rechenknoten mit 12752 Kernen und 26944 GByte RAM an.

Im HPC-Bereich ist eine effiziente Nutzung der Ressourcen unerlässlich. Neue Hardware muss zeitnah eingegliedert werden, da mehrere Faktoren wie Garantie, Abschreibung und Auftraggeber auf eine möglichst schnelle Nutzung der Ressource hin drängen. Hierbei hat sich eine zentrale Installation, die über das Netzwerk verteilt wird, bewährt [SvW+11]: Änderungen am Betriebssystem können zentral eingepflegt und in kürzester Zeit an alle Maschinen verteilt werden. Außerdem können alternative Linux-Betriebssysteme angeboten werden, sodass schnell zwischen den Umgebungen gewechselt werden kann. Als Betriebssystem lief zunächst ein Scientific Linux Version 5.0, das im Laufe der Zeit auf die Version 5.5 aktualisiert wurde.[4] Ein Upgrade des Betriebsystems auf Version 6.x wird

[1] Zwei Vierkern-CPUs Intel Harpertown Xeon E5440 (2.83 GHz) und 16 GByte RAM.

[2] Die Knoten sind mit einer Mezzanine-Karte ConnectX von Mellanox ausgestattet. Verbunden sind sie über einen InfiniBand-Switch Voltaire Grid Director ISR 2012.

[3] Zwei Intel CPUs Gainestown Xeon E5520 bzw. X5560 und 24 GByte RAM.

[4] Ein RHEL-Derivat. Projektseite: `http://www.scientificlinux.org/`

derzeit evaluiert.

Zur Verbesserung der Performance wurden an den meisten Standorten Festplatten für temporäre Daten nachgerüstet. Für große Datenmengen steht ein paralleles Netzwerkdateisystem zur Verfügung. Die Ausschreibung gewann eine HP-Speicherlösung, die auf Lustre 1.8.3 aufsetzt[5] und auf hohe Redundanz ausgelegt ist. Stuttgart, Ulm und Tübingen wurden mit je 64 TByte Speicherplatz, die anderen Standorte mit je 32 TByte Speicherplatz ausgestattet. In Esslingen wurde 36 TByte LustreFS-Speicher der Firma NEC beschafft. Der parallele Lustre-Speicher ist über InfiniBand mit den Knoten verbunden. Untereinander sind die Server, welche die Festplatten ansprechen, über 10 Gbit/s FibreChannel vernetzt.

Der Zugang zum Grid und die Jobsubmission erfolgen über die Globus-Middleware.[6] Jedoch können Jobs auch lokal am Cluster abgeschickt werden. Der Login an einem Cluster erfolgt für Grid-Nutzer über `GSISSH`[7] und für lokale Nutzer via `SSH`.

3 Geschäftsmodell und Organisation

Das bwGRiD soll ein möglichst breites Spektrum an Anwendern und Anwendergruppen ansprechen. Die Nachteile, die durch die Beschaffung und den Betrieb von HPC-Ressourcen durch einzelne Arbeitsgruppen oder im Zuge einzelner kleiner Projekte entstehen, sollen dadurch vermieden werden. Synergieeffekte durch die gemeinsame Beschaffung von identischer Hardware führen zu einer effizienteren Nutzung monetärer Mittel. So war es unter anderem möglich, günstigere Großkundenkonditionen zu erhalten, was sich neben der Beschaffung auch auf die Konditionen von Wartungsverträgen positiv auswirkt. Weiterhin erleichtert eine homogene Basisausstattung die Administration der Systeme, da im Verbund Probleme gelöst und Erfahrungen ausgetauscht werden können. Die Wartung und Konfiguration der Systeme, wie auch das Scheduling werden unproblematischer, da häufig Hilfestellung durch andere Standorte angeboten werden kann. Außerdem wird eine gemeinsame Beschaffung Hardware-spezifischer Software (z.B. Compiler) ermöglicht.

Im Rahmen des Projektes wurden fachspezifische Kompetenzzentren an den jeweiligen Standorten gebildet. Durch die starke Vernetzung der Wissens-Cluster kann eine optimale Nutzerunterstützung koordiniert und gewährleistet werden. Mitarbeiter eines Standortes können Gruppenprofile präziser abschätzen und bieten den Nutzern über lokale und damit kurze Kommunikationswege einen idealen Support. Verschiedene Aufgaben und Verantwortungsbereiche wurden an einzelne Standorte übertragen: So übernahm Karlsruhe im Jahr 2010 die Projektleitung von Stuttgart und Konstanz ist für den Betrieb und die Gestaltung der Projektseite *www.bw-grid.de* zuständig, die Informationen zum Projekt, die an den jeweiligen Standorten installierte Software, die Zugangsinformationen zu den Clustern und Beschreibungen der auf dem Grid gerechneten Projekte, anbietet. Die interne

[5] Derzeitiger Stand: Lustre Server Version 1.8.4, Lustre Client Version 1.8.5 (`www.lustre.org/`)

[6] Derzeitige Version: 4.0.8. (`http://www.globus.org/`)

[7] Ein auf GSI (Grid Security Infrastructure) basierender SSH-Client (`http://grid.ncsa.illinois.edu/ssh/`)

Abstimmung der Projektpartner und der Unterprojekte erfolgt über eine E-Mail-Liste, die von Ulm betreut wird, und durch eine zweiwöchentlich stattfindende Videokonferenz mit allen Projektpartnern. Gemeinsame Dokumente werden über die BSCW-Groupware[8] zur Teamarbeit, die in Stuttgart verwaltet wird, organisiert.

3.1 Einheitliche Softwareausstattung

Um eine möglichst homogene Softwareausstattung im bwGRiD zu gewährleisten, ist eine klare Softwarestruktur zwingend erforderlich. Das Softwarepaket `modules`[9] wird hierbei genutzt, um eine temporäre Benutzerumgebung für ein bestimmtes Programm durch setzen der entsprechenden Umgebungsvariablen der Linux-Shell, zu erzeugen. Dadurch können mehrere Versionen eines Programms parallel installiert und bei Bedarf von den Anwendern geladen und genutzt werden. Eine einheitliche Benennung der Module ist unabdingbar, um Nutzern das Abschicken ihrer Jobs auf jedem Cluster des bwGRiDs ohne vorherige Anpassung ihrer Skripte zu ermöglichen. Daher wurde ein Standard für die Namensgebung der Modulnamen entwickelt. Weiterhin wurde die Verantwortlichkeit für Entwicklung, Nutzersupport und Pflege der Module auf die einzelnen Standorte ihren Schwerpunkten entsprechend aufgeteilt. Um die Organisation und Nutzung der Module zu vereinfachen, wurden diese in Klassen eingeteilt.[10] Die mit `mandatory` gekennzeichneten Pakete müssen an allen Standorten installiert sein. Bei Software aus dieser Klasse können sich die Nutzer ohne vorherige Überprüfung darauf verlassen, dass diese auf jedem Cluster installiert ist. Andernfalls obliegt es den Nutzern zu prüfen, ob die erforderlichen Module am gewünschten Standort verfügbar sind.[11] Angaben zu den Paketen wie Modulname, Softwareversion, verantwortlicher Standort und Klasse werden zurzeit zentral in einer Tabelle gespeichert und die Module zum Download über einen Repository-Server in Freiburg angeboten.

Da sich die Grid-weite Bereitstellung standardisierter Softwaremodule als kritischer Punkt erwiesen hat, wurde im Rahmen der *Ergänzenden Maßnahmen* zum bwGRiD-Projekt die Stelle des Softwarekoordinators geschaffen. Dieser entwickelt Konzepte für eine Qualitätskontrolle der von den Standorten bereitgestellen Softwaremodule.

3.2 Lizenzproblematik

Der Erfolg der bwGRiD-weiten Beschaffung von Softwarelizenzen ist stark von den Anbietern abhängig. Das AMBER-Projekt erkannte das bwGRiD als eine Institution an, wo-

[8] Web-Präsenz: `http://www.bscw.de/`

[9] Projektseite: `http://modules.sourceforge.net/`

[10] `mandatory` – garantierte Verfügbarkeit an allen Standorten, `optional` – Installation optional, `local` – Lizenzpflichtige Programme, die nur an bestimmten Standorten verfügbar sind, `private` – kann von interessierten Standorten installiert werden und `on_request` – werden auf Nutzeranfrage zur Verfügung gestellt.

[11] Web-Maske mit Suchfunktion: `http://www.bw-grid.de/benutzerinformation/software/software-suchen/`

durch eine Lizenz für das gesamte Grid erworben werden konnte. Somit kann die Software ohne Einschränkung an jedem Standort des Grids installiert und genutzt werden. Auch die Anbieter der „Schrödinger Molecular Modeling Suite “ und der „ANSYS Computer Aided Engineering und Multiphysik“-Software erlauben die Nutzung im bwGRiD durch dynamisch abrufbare Lizenztokens.[12] Entsprechende Lizenzserver werden an den Standorten Tübingen (Schrödinger) und Karlsruhe (ANSYS) betrieben. Insbesondere für Arbeitsgruppen, die eine bestimmte Software nicht permanent nutzen, ist dies ein erheblicher Vorteil. Administrativ ergibt sich allerdings ein signifikanter Mehraufwand durch das Betreiben der Lizenzserver, da diese nicht nur eingerichtet werden, sondern auch permanent mit hoher Verfügbarkeit erreichbar sein müssen.

Probleme mit diesem Lizenzmodell ergeben sich auch in Verbindung mit dem verwendeten Batchsystem.[13] Es ist nicht auszuschließen, dass ein Job startet, obwohl nicht genügend freie Lizenzen vorhanden sind, was zu einem Jobabbruch führt. In diesem Bereich besteht noch erheblicher Handlungsbedarf, da die Lizenzproblematik vom Scheduler derzeit nicht berücksichtigt wird. Für die Intel Compiler Suite wurde ein Preis für alle Standorte ausgehandelt, jedoch handelt es sich um lokale Standortlizenzen, sodass auch die Lizenzserver an den Standorten betrieben werden müssen. Weiterhin gibt es Lizenzvereinbarungen, die auf einen Standort beschränkt sind, aber von allen Nutzern des bwGRiDs genutzt werden können. Mit dem Anbieter der Computerchemie-Software Gaussian konnte trotz intensiver Verhandlungen keine angemessene Grid-weite Lizenz ausgehandelt werden. Letztendlich bleibt zu vermerken, dass lediglich bwGRiD-Lizenzen, wie sie von AMBER bereitgestellt werden, eine Alternative zu Open Source Software darstellen.

3.3 Entwicklung des bwGRiDs

Das Bestreben eines Anbieters von HPC-Diensten ist die permanente Bereitstellung leistungsstarker Hardware für Anwender. Daher wurden die bwGRiD-Cluster an verschiedenen Standorten stetig ausgebaut (Abbildung 1). Gerade kleineren Standorten bietet das bwGRiD eine potente Basis für eine stete Erweiterung ihrer HPC-Ressourcen. Ferner können dadurch auch Kompetenzzentren im Hardwarebereich aufgebaut werden, was die Attraktivität des jeweiligen Standorts und des gesamten bwGRiDs für Anwender erhöht. Insbesondere in Freiburg und Tübingen wurden die bwGRiD-Cluster durch Betreiber- und Anwender-finanzierte Hardware kontinuierlich erweitert. Teilweise ist es gelungen, bestimmte Hardware dem gesamten Grid zur gemeinsamen Nutzung zur Verfügung zu stellen. Im Gegenzug profitieren die Arbeitsgruppen von der fachkundigen Administration ihrer Systeme durch die bwGRiD-Betreiber und dem Know-How der anderen Grid-Standorte sowie von der teilweisen Übernahme der Kosten für den Betrieb. Aktuell können Anwender von Arbeitsgruppen mit eigener Hardware bei Bedarf mit höherer Priorität versehen werden, sodass der Zugriff auf die eigenen Ressourcen jederzeit gewährleistet ist. Durch dieses Modell können auch andere Grid-Nutzer von der zusätzlichen Hardware pro-

[12] Web-Präsenz AMBER `http://ambermd.org/`, Schrödinger `http://www.schrodinger.com/`, ANSYS `http://www.ansys.com/`, Gaussian `http://www.gaussian.com/`

[13] TORQUE und Moab (`http://www.adaptivecomputing.com/`)

Integration neuer Ressourcen			
Standorte	**# Knoten**	**CPU/GPU**	**RAM (GByte)**
Freiburg	16	Intel Xeon X5550, 2.67GHz (2x4 Kerne)	24
	8	Intel Xeon X5650X5550, 2.66GHz (2X6 Kerne) / Nvidia Tesla M2090** (1x512 Kerne)	
	4	Intel Xeon E5520, 2.27GHz (2x4 Kerne) / Nvidia Tesla C1060* (2x240 Kerne)	
Stuttgart	1	AMD Opteron 8360 SE, 2.44GHz (8x4 Kerne)	512
		AMD Opteron 8384, 2.64GHz (8x4 Kerne)	256
	8	Intel Xeon 5472, 3.00GHz (2x4 Kerne) / Nvidia Quadro FX 5800 (240 Kerne)	8
Tübingen	24	Intel Xeon L5530, 2.4GHz (2x4 Kerne)	72
	18	AMD Opteron 6172, 2.1GHz (2x12 Kerne)	32
	16	Intel Xeon 5150, 2.66GHz (2x2 Kerne)	
	8	Intel Xeon 5355, 2.66GHz (2x4 Kerne)	
		Intel Xeon 5150, 2.66GHz (2x2 Kerne)	16
	1	Intel Xeon E7-4830, 2.13GHz (4x8 Kerne) / 6,5 TByte Storage	512

* 2x Tesla S1070 mit je 4x C1060 (2x4 GByte RAM) | ** intern verbaut (6 GByte RAM)

Abbildung 1: **Hardware des bwGRiDs** (Stand: 02.04.2012)

fitieren, wenn die Auslastung durch die priorisierten Nutzer gering ist. In diesem Zusammenhang wird aktuell an weiteren Betriebs-Modellen intensiv gearbeitet.

3.4 Nutzungsrichtlinien

Der Zugang zu den bwGRiD-Clustern erfolgt grundsätzlich über die im D-Grid verwendete Globus-Middleware. Globus unterstützt die Authentifizierung mithilfe von X.509-Zertifikaten. Daher haben alle Standorte des bwGRiDs eine Registration Authority für DFN-Gridzertifikate eingerichtet. Außerdem wurde innerhalb des Projektes beschlossen, dass neben den üblichen Grid-CAs[14] auch eigene CAs der beteiligten Einrichtungen gegenseitig akzeptiert werden. Grundsätzlich können alle Mitglieder der Hochschulen in Baden-Württemberg und deren Projektpartner Mitglied der VO bwGRiD werden. Zusätzlich steht das bwGRiD auch Mitgliedern anderer D-Grid-VOs zur Verfügung. Für die Nutzung der Ressourcen ist lediglich eine Zustimmung zur D-Grid-Einverständniserklärung[15] obligatorisch. In diesem Dokument sind die Rechte und Pflichten der Nutzer von D-Grid-Ressourcen geregelt, insbesondere die Voraussetzungen für das Erlangen eines Grid-Nutzerzertifikats. Zusätzlich kann jeder Standort seinen lokalen Nutzern den Zugang zum jeweiligen Cluster erlauben. Jedoch stehen diesen dann nur die Ressourcen des Standortes zur Verfügung. Die Administratoren des bwGRiDs sind angehalten den Betrieb auf den HPC-Clustern zu überwachen und bei Verstößen gegen die Einverständniserklärung entsprechende Maßnahmen gegen die Nutzer zu ergreifen.

[14] Certificate Authorities: Grid-CA des DFN-Vereins, GridKa-CA des Forschungszentrums Karlsruhe

[15] Einverständniserklärung: `http://www.fz-juelich.de/dgrid/AUP/D-Grid-User-AUP.pdf`

3.5 Hilfswerkzeuge zur Unterstützung der Nutzer

Die effiziente Nutzung verteilter Rechenumgebungen wie die des bwGRiDs erfordert, dass Anwendern und insbesondere Einsteigern adäquate Lehrmaterialien und Softwarewerkzeuge zur Verfügung gestellt werden. Zunächst muss eine umfassende Dokumentation der jeweiligen HPC-Cluster erfolgen. Dabei sollte nicht nur der unterschiedliche Kenntnisstand der Benutzer berücksichtigt werden, sondern auch ausführlich auf die Unterschiede bei der Benutzung der einzelnen Standorte, die es trotz aller internen Abstimmungen immer noch gibt, eingegangen werden. Deshalb werden im bwGRiD entsprechende Materialien derzeit noch dezentral auf den Webseiten der Standorte bereitgestellt. Zusätzlich wird gegenwärtig ein Benutzerhandbuch für das bwGRiD entwickelt, das sowohl in elektronischer als auch in gedruckter Form verfügbar sein wird. Es enthält neben standortspezifischen Besonderheiten auch Informationen und Beispiele für verschiedenste Benutzergruppen. Weitere Softwarewerkzeuge für die Nutzung des bwGRiDs wurden von den Projektteilnehmern entwickelt und verteilt. Dazu gehört eine vorkonfigurierte virtuelle Maschine (bwGRiD-VM) auf Basis von Ubuntu 10.04LTS. Diese stellt bereits eine vollständige Globus-Installation, sowie zahlreiche Skripte für die Konfiguration und Nutzung des bwGRiDs zur Verfügung. Außerdem wurden mittlerweile zwei Informationsflyer mit generellen und technischen Informationen über das Grid erstellt und veröffentlicht.

Im April 2010 startete das bwGRiD-Portal-Projekt.[16] Es richtet sich vor allem an Forschungsgruppen, deren Mitglieder wenig Erfahrung im Umgang mit HPC-Ressourcen haben und soll ihnen einen einfachen Zugang zum Grid-Computing[17] ermöglichen. Insbesondere der teils komplizierte Umgang mit der Kommandozeile soll durch das Webportal ersetzt und die Verwaltung und Überwachung von eigenen Jobs und Daten vereinfacht werden. Anwendungsspezifische Komponenten (Portlets) bieten hierbei die Möglichkeit zum Erstellen beziehungsweise Hochladen von Eingabedaten und zum Abschicken der Jobs. Die Portlets werden an verschiedenen Standorten in enger Zusammenarbeit mit den jeweiligen Anwendern entwickelt. Zurzeit ist nur die Grid-Anbindung via Globus (4.0.8 WS-GRAM) realisiert. Der Zugriff auf das Portal erfolgt über Grid-Nutzerzertifikate (siehe Abschnitt 3.4). Im Rahmen des Projektes wurde das Firefox-Addon „Grid Proxy Manager“ entwickelt, welches das Erstellen und Hochladen von MyProxy-Zertifikaten [NTW01] für die Nutzeridentifikation innerhalb des Grids erheblich erleichtert.[18]

4 Resultate

Die erfolgreiche Entwicklung des bwGRiD-Projektes lässt sich an der kontinuierlichen Zunahme der Publikationen ablesen. Wurden im Jahr 2008 sieben Publikationen, die das

[16] Technisch basiert das bwGRiD-Portal auf dem Portlet-Framework GridSphere und dem Servlet-Container Apache Tomcat

[17] Die Kommunikation mit den Grid-Komponenten erfolgt über das Grid Application Tookit (GAT) und Gatlet.

[18] Projekt-Webseiten: `http://www.gridsphere.org/gridsphere/gridsphere`, `https://gforge.cs.vu.nl/gf/project/javagat`, `http://gatlet.scc.kit.edu/`, `https://addons.mozilla.org/de/firefox/addon/grid-proxy-manager/`

bwGRiD referenzieren, veröffentlicht, waren es im Jahr 2011 schon 101 Veröffentlichungen (Abbildung 2a). Insgesamt sind bislang 220 Publikationen oder Konferenzbeiträge eingereicht und akzeptiert worden.[19]

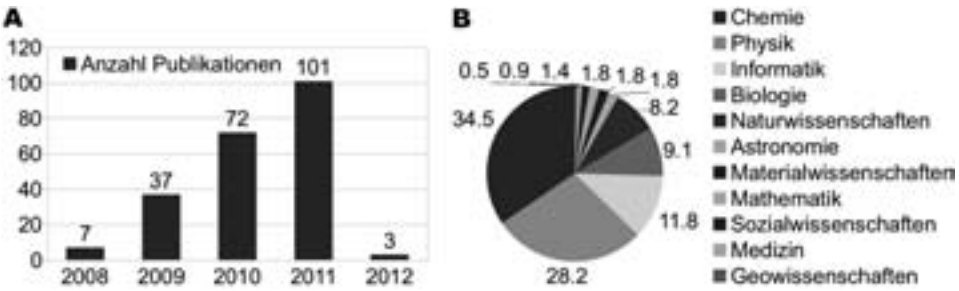


Abbildung 2: **Publikationen im bwGRiD** (Stand: 28.03.2011)
(A) Anzahl der Publikationen in denen Berechnungen auf dem bwGRiD durchgeführt wurden.
(B) Prozentualer Anteil der Schlagworte an Gesamtzahl der Publikationen.

Die Aufschlüsselung der mithilfe des bwGRiDs erzeugten Publikationen nach Fachrichtungen zeigt, dass der Großteil der derzeitigen Anwender aus dem naturwissenschaftlichen Bereich kommt. So machen Veröffentlichungen in den Bereichen Chemie, Physik, (Bio-) Informatik, Biologie und weiteren naturwissenschaftlichen Feldern zusammen einen Anteil von über 90 Prozent an allen Veröffentlichungen aus. Auf die restlichen rund acht Prozent verteilen sich Veröffentlichungen in den Gebieten Astronomie (1,8%), Materialwissenschaften (1,8%), Mathematik (1,8%), Sozialwissenschaften (1,4%), Medizin (0,9%) und Geowissenschaften (0,5%). Aus der Analyse der Publikationen lassen sich zwei Schwerpunkte für die weitere Entwicklung des bwGRiDs ableiten. Zum einen die Stärkung des Anteils von nicht-klassischen Disziplinen durch verstärkte Werbung und den Abbau der Einstiegshürden für das Grid-Computing. Zum anderen die Optimierung des bestehenden Angebotes, um die Fachbereiche, die bereits die Dienstleistungen des bwGRiDs nutzen, noch besser zu unterstützen.

5 Fazit und Ausblick

Schnelle Netze erlauben neuartige Betriebsmodelle für HPC-Cluster. Die überregionale Vernetzung der Cluster über Hochgeschwindigkeits-Weitverkehrsnetze erhöht die Redundanz erheblich und führt zu einer Hochverfügbarkeit der HPC-Ressourcen für Anwender. Ein Ausfall oder die Wartung eines Standortes können durch andere Standorte kompensiert werden. Single-Point-of-Failures werden somit minimiert. Dadurch nähert man sich dem aktuellen Cloud-Paradigma, das Community-Grids und Nachhaltigkeit fordert, weiter an. Das heißt, die für die jeweilige Berechnung am besten geeigneten Maschinen und der optimale Ort für die konkrete Ausführung verschiedener Jobs mit unterschiedlichen Anforderungen lassen sich dynamisch über große geografische Entfernungen zusammenfügen.

[19] Publikationsliste bwGRiD (Stand: 28.03.2011): `http://www.bw-grid.de/publikationen/`

Dabei erleichtert eine geeignete Job-Klassifikation den Grid-Nutzern sinnvolle Vorschläge zur optimalen Rechenumgebung, beziehungsweise zum Ausführungsort zu unterbreiten. Grundlage dafür sind neben einer ausreichend hohen Netzwerkbandbreite auch das Setzen gemeinsamer Standards sowie das Treffen und Einhalten gemeinsamer Absprachen. Ein bedeutender Vorteil des bwGRiD-Modells ist die Möglichkeit einer Spezialisierung innerhalb der Grid-Community, in dem sich verschiedene, verteilte Gruppen um unterschiedliche Aspekte des Cluster-Betriebs kümmern.

Durch den Verzicht einzelner Projektpartner auf ein gewisses Maß an Souveränität zugunsten eines gemeinsam abgestimmten Vorgehens bei der Beschaffung und dem Betrieb des bwGRiDs konnte der akademischen Forschung in Baden-Württemberg, und über das Bundesland hinaus, eine flexible und hochverfügbare HPC-Umgebung zur Verfügung gestellt werden. Das bwGRiD bietet HPC-erfahrenen Arbeitsgruppen und Neueinsteigern eine wertvolle Plattform für die Spitzenforschung im Land. Dies lässt sich auch an der konstant hohen Auslastung der bwGRiD-Ressourcen erkennen, welche ein auf dem bwGRiD basierendes Folgeprojekt notwendig macht.

Zuvor werden jedoch noch folgende Fragestellungen in den nächsten zwei Jahren behandelt. Zum einen wird eine Möglichkeit eines einfachen Cluster-übergreifenden Meta-Schedulings im Rahmen der *Ergänzenden Maßnahmen* untersucht. Dabei liegt die eigentliche Schwierigkeit in der Bereitstellung der Daten, einer Abschätzung der Übermittlungszeit dieser und der Wartezeit in der Schlange, sowie der Bereitstellung der eventuell angefragten Lizenztokens. Des Weiteren wird eine einfache Authentifizierung und Autorisierung gegenüber dem bwGRiD-Projekt mithilfe von Shibboleth untersucht. Es finden zudem Bestrebungen zur Entwicklung einer zentralen Datenbank und eines Software-Repositories statt, die für eine schnellere Verteilung der Software auf alle Standorte sorgen und damit die Administration erleichtern, sowie den Nutzern möglichst homogene Softwareumgebungen bieten sollen. Das bwGRiD-Portal wird gerade vom Portlet-Framework GridSphere auf das leistungsstärkere Liferay[20] portiert und eine Migration von Globus 4 auf Globus 5 ist ebenfalls in Planung.

Das bwGRiD hat sich im Laufe der Zeit zu einem erfolgreichen und unverzichtbaren Werkzeug für eine Vielzahl von Wissenschaftlern aus den verschiedensten Disziplinen entwickelt und wird auch in Zukunft eine bedeutende Rolle für die Forschung spielen.

Literatur

[BK10] C. Baun und M. Kunze. Aufbau einer Computing Cloud am KIT – Betrachtung von Leistungsaspekten. *Praxis der Informationsverarbeitung und Kommunikation (PIK)*, pages 26–35, 2010.

[Gen06] W. Gentzsch. Das Verbundprojekt D-Grid. *Praxis der Informationsverarbeitung und Kommunikation (PIK)*, pages 132–139, 2006.

[20] Projektseite Liferay: `http://www.liferay.com/`

[Mic06] K.-P. Mickel. Erfahrungen mit Produktionsgrids am Beispiel des LHC-Computing-Grid (LCG). *Praxis der Informationsverarbeitung und Kommunikation (PIK)*, pages 140 – 145, 2006.

[NTW01] J. Novotny, S. Tuecke und V. Welch. An Online Credential Repository for the Grid: MyProxy. In *Proceedings of the 10th IEEE International Symposium on High Performance Distributed Computing*, pages 104–, Washington, DC, USA, 2001. IEEE Computer Society.

[RHKK10] S. Richling, S. Hau, H. Kredel und H.-G. Kruse. Operating Two InfiniBand Grid Clusters over 28 km Distance. *P2P, Parallel, Grid, Cloud, and Internet Computing, International Conference on*, 0:16–23, 2010.

[RV10] A. Reber und P. Väterlein. Computer aus der Steckdose Hochschule Esslingen wird Teil des bwGRiD. *Horizonte*, 36(ISSN: 1432-9174):70, 2010.

[SvW+11] S. Schmelzer, D. von Suchodoletz, D. Weingaertner, L. C. De Bona, G. Schneider und C. Carvalho. Universal Remote Boot and Administration Service. In *7th Latin American Network Operations and Management Symposium*, number ISBN 978-1-4577-1791-8, 2011.

IT-Sicherheit

Beweiswerterhaltendes Datenmanagement im elektronischen Forschungsumfeld

Jan Potthoff

Steinbuch Centre for Computing (SCC)
Karlsruher Institut für Technologie (KIT)
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen
jan.potthoff@kit.edu

Abstract: Sowohl durch den Einsatz des Computers als auch von Messgeräten mit digitalem Output entstehen im Forschungsprozess im zunehmenden Maße digitale Daten. Um einerseits diese Datenmengen geeignet zu verwalten und andererseits den Forschungsprozess nachvollziehbar zu dokumentieren, werden Anwendungen eingesetzt, die für diesen Zweck entworfen wurden. Neben der nachvollziehbaren Dokumentation wird nach den Regeln der guten wissenschaftlichen Praxis auch der langfristige Erhalt der Datenintegrität und -authentizität gefordert. Der im Rahmen des BeLab-Projekts entworfene Prototyp kann unter anderem dazu genutzt werden, den Beweiswert übergebener Daten zu bestimmen, um anschließend diese Daten beweiswerterhaltend zu archivieren. Da das System generisch entworfen wurde, kann grundsätzlich jede Art von Anwendung, die im Forschungsumfeld genutzt wird, den BeLab-Prototypen verwenden. Entworfen wurde das Konzept jedoch für elektronische Laborbuch-Entwicklungen. Sind die eingesetzten Systeme untereinander abgestimmt und auf den Arbeitsablauf des Wissenschaftlers ausgelegt, können Effizienzsteigerungen erzielt, die Nachvollziehbarkeit gewährt und durch den Einsatz des BeLab-Prototypen die Integrität und Authentizität der archivierten Forschungsdaten gesichert werden.

1 Elektronische Verarbeitung von Forschungsdaten

Der experimentelle Forschungsprozess lässt sich beispielsweise grob in fünf Phasen unterteilen [PR+11]: In der Planungsphase erfolgt eine Literaturrecherche, das Experiment wird geplant und Parameter werden festgelegt. In der Durchführungsphase werden die Experimente ausgeführt und die Ergebnisse in den zwei darauf anschließenden Phasen aufbereitet und ausgewertet. Diese Phasen erfolgen abhängig von der Forschungsrichtung und dem jeweiligen Forschungsvorhaben. Je nach Ergebnis werden die Phasen iterativ ein- bis mehrmals durchlaufen. Dabei werden Ergebnisse der Experimente verglichen oder Parametereinstellungen angepasst oder verbessert. In der nächsten Phase werden die gewonnenen Erkenntnisse und Ergebnisse des Forschungsprozesses veröffentlicht und so der Forschungscommunity zur Verfügung gestellt.

Abschließend erfolgt die Archivierung der im Forschungsprozess angefallenen Daten. So stehen diese für eine Nachnutzung weiterhin zur Verfügung. In diesem Zusammenhang kann vom „Scientific Data Lifecycle“ gesprochen werden.

1.1 Die gute wissenschaftliche Praxis

Die Archivierung der im Scientific Data Lifecycle angefallenen Daten ist nicht nur für eine Nachnutzung, sondern auch im Rahmen der guten wissenschaftlichen Praxis (GWP), wie sie beispielsweise die Deutsche Forschungsgemeinschaft (DFG) verlangt [DFG98], von Bedeutung. Danach sollen Forschungsdaten (Primärdaten), die zu einer Veröffentlichung geführt haben, für mindestens 10 Jahre archiviert werden. Dabei soll auf eine langfristige Interpretierbarkeit geachtet werden. Um Forschungsergebnisse nachvollziehbar zu archivieren, soll der Forschungsprozess entsprechend dokumentiert werden. Dazu gehören auch alle Daten und Erkenntnisse, die im Prozess gewonnen werden. Auch Universitäten und Forschungseinrichtungen ([MPG00], [KIT]) haben Grundsätze zur Sicherung der GWP verabschiedet, die sich teilweise auf die Empfehlungen der DFG beziehen. Sie verfolgen das Ziel, die Qualität der Forschung und der Ausbildung des wissenschaftlichen Nachwuchses sicherzustellen und Betrug oder Fälschung im Wissenschaftsbetrieb zu verhindern.

Die Dokumentation erfolgt üblicherweise mithilfe eines Laborbuchs, das auch heute noch teilweise in Papierform geführt wird [PJ11]. Auch wenn Aussehen und konkrete Inhalte stark variieren können, besteht Einigkeit über die Form der Dokumentationsweise [UOl], [Prov]. So werden beispielsweise Seiten des festgebundenen Laborbuchs durchnummeriert, um die Vollständigkeit zu belegen. Jede Seite wird mit einer Unterschrift und jeder Eintrag mit einem Datum versehen. Änderungen erfolgen nicht durch ein Unkenntlich machen, sondern durch das Streichen des entsprechenden Eintrags. Auch dieser Vorgang wird mit einer Unterschrift des Forschenden bestätigt [EB+06]. Durch diese Maßnahmen wird die Integrität und Authentizität der Einträge innerhalb des Laborbuchs gewährleistet.

1.2 Datenmanagement im Scientific Data Lifecycle

In den einzelnen Phasen des Scientific Data Lifecycle entstehen Daten, die abhängig vom Forschungsbereich in Art und Umfang stark variieren und im zunehmenden Maße in digitaler Form vorliegen [HJ+11]. Die digitalen Daten entstehen durch den Einsatz unterschiedlichster Messgeräte mit digitalem Output, aber auch durch eine Vielzahl unterschiedlicher Applikationen, die in allen Phasen des Scientific Data Lifecycle eingesetzt werden. Zur Datenerhebung werden beispielsweise spezielle Softwareentwicklungen verwendet, die vom Hersteller des entsprechenden Messgeräts bereitgestellt werden. Die Software, die zur Auswertung oder weiteren Bearbeitung der Ergebnisse genutzt wird, ist fach- oder versuchsspezifisch. So werden z. B. auch selbstentwickelte Programme verwendet, die speziell für den Anwendungsfall programmiert wurden. In der Regel gibt es keine Vorgabe vom Institut oder der Abteilung bezüglich der zu verwendenden Software [PJ11].

In Versuchsreihen mit kleineren Mengen digitaler Daten können die Daten beispielsweise durch einen Ausdruck mit in das papiergebundene Laborbuch aufgenommen werden. In anderen Fällen ist dies aufgrund der Art, wie die Daten in einer dreidimensionalen Darstellung oder der Menge an digitalen Daten, nicht möglich. In diesem Fall werden die digitalen Daten separat verwaltet. So entstehen hybride Laborbücher, die die Gefahr von Datenverlusten aufkommen lassen [HJ+11]. Aus diesem Grund existieren Softwarelösungen, die speziell für die Dokumentation des Forschungsprozesses entwickelt wurden und damit eine zentrale Datenpflege erlauben. Sie werden als elektronisches Laborbuch (eLab), Datenmanagementsystem oder Laborinformation und Managementsystem (LIMS) bezeichnet. Auch andere Anwendungen, wie beispielsweise Wiki-Systeme oder Microsoft Office Anwendungen, werden zur Dokumentation des Forschungsprozesses zweckentfremdet [PJ11].

Um Daten zu verwalten und wieder auffinden zu können, werden Metadaten verwendet. Die Pflege von Metadaten ist von System zu System sehr unterschiedlich realisiert. So können zum Beispiel mittels der Applikation DataFinder des Deutschen Zentrums für Luft- und Raumfahrt (DLR) benutzerdefinierte (Meta-)Datenstrukturen angegeben werden [DLR]. Das System lässt sich durch zwei getrennte Clientanwendungen bedienen. Mithilfe des Administrator-Clients können Strukturen vorgegeben werden, die vom Benutzer-Client genutzt werden. Daten, die mithilfe dieser Struktur verwaltet werden, können über das System auf unterschiedlichen Datenspeichern, wie z. B. WebDAV Server, File Server oder Tivoli Storage Server, abgelegt werden. Durch die Suchfunktion, die Hauptfunktionalität der Anwendung, können gewünschte Daten entsprechend aufgefunden werden. Eine andere Lösung, die speziell für den Arbeitsablauf eines Chemikers ausgelegt ist und so zu einer gezielten Effizienzsteigerung im eingesetzten Arbeitsbereich führt, ist open enventory [AKGo]. Das System bietet, neben der Verwaltung von Chemikalien, die Möglichkeit der Pflege eines eLab, in das Ansätze und Ergebnisse eingetragen werden können. Zusätzlich können über vorgegebene Eingabemasken Metadaten eingegeben und gepflegt werden. Eine Erweiterung der Metadaten durch den Benutzer ist nicht vorgesehen. Durch eine integrierte Benutzerverwaltung ist eine Kollaboration zwischen mehreren Forschern möglich. Die Daten werden in diesem Fall in einer Datenbank abgelegt.

Die Form der Integritäts- und Authentizitätssicherung, die im papiergebundenen Laborbuch Verwendung findet (siehe Abschnitt 1.1), ist auf die elektronische Dokumentationsweise nicht direkt übertragbar. Des Weiteren sind gesonderte Sicherheitsmaßnahmen zu treffen, um die Daten vor ungewollten Zugriffen oder Veränderungen zu schützen [Be10]. Zwar ist auch die papiergebundene Dokumentation nicht per se davor geschützt, aber durch den technischen Fortschritt sind Manipulationen an digitalen Daten im größeren Stil leichter zu realisieren. Des Weiteren lassen sich diese Manipulationen ohne getroffene Maßnahmen schwieriger bis gar nicht nachweisen.

1.3 Datenintegrität, Datenauthentizität und Datenschutz

Auch vor Gericht gilt ein elektronisches Dokument als leicht manipulierbar [Fi06]. Daher wird dem elektronischen Dokument eine geringere Beweiskraft zugesprochen und ist nach § 371 Absatz 1 Satz 2 Zivilprozessordnung (ZPO) nur Beweis des Augenscheins. Um für ein Dokument in Papierform die Beweiskraft einer Privaturkunde zu erlangen, muss diese nach § 416 ZPO vom Aussteller oder einem mittels notariell beglaubigten Handzeichens unterzeichnet sein. Um Vergleichbares für elektronische Dokumente zu erzielen können nach dem Signaturgesetz qualifizierte elektronische Signaturen verwendet werden. Denn sind elektronische Dokumente mit einer qualifizierten Signatur versehen, werden sie nach § 371a ZPO auch als Urkunde gewertet.

Elektronische Signatur können mithilfe des Public-Key-Algorithmus[1] umgesetzt werden. Im ersten Schritt wird aus Gründen der Effizienz der Hashwert des Dokuments gebildet. Dazu wird eine öffentlich bekannte Einweg-Hash-Funktion verwendet. Im zweiten Schritt erfolgt die Verschlüsselung des Hashwertes mithilfe des privaten Schlüssels. Zum Überprüfen der Signatur wird der Hashwert unter der Verwendung des öffentlichen Schlüssels entschlüsselt und mit dem erneut berechneten Hashwert verglichen. Sind beide Werte gleich, ist nachgewiesen, dass das Dokument unverändert, d. h. die Datenintegrität gewahrt ist [Er07]. Durch elektronische Signaturen kann zwar der Nachweis geführt werden, dass ein digitales Dokument verändert wurde, eine Veränderung kann damit jedoch nicht verhindert werden. Der Zugriff auf ein eLab oder ein anderes genutztes System muss daher geregelt und unter der Annahme, dass das System von mehreren Forschern genutzt wird, Zugriffskonzepte definiert werden [Be10].

2 Beweiswerterhaltung und Zugriffskontrolle

Möglichkeiten, die Form der Dokumentation in papiergebundenen Laborbüchern zum Zweck der Datenintegrität und –authentizität auf die elektronische Dokumentation zu übertragen und neue Verfahren zu entwerfen, ist Ziel des Forschungsprojekts „Beweissicheres elektronisches Laborbuch (BeLab)“.[2] Das von der DFG geförderte Verbundprojekt wird gemeinsam durch die Universität Kassel, die Physikalisch-Technische Bundesanstalt (PTB) in Braunschweig und das Karlsruher Institut für Technologie (KIT) bearbeitet. Ziel ist der Entwurf eines Konzepts und eine prototypische Implementierung, mit der eine beweiswerterhaltende Langzeitarchivierung von digitalen Forschungsprimärdaten erreicht werden kann. Sowie die Vollständigkeit, die Integrität und Authentizität der Daten als auch die Nachvollziehbarkeit sollen dabei langfristig gewahrt bleiben.

---

[1] Die Idee der Public-Key-Kryptographie ist, dass eine Nachricht mit einem öffentlichen (bekannten) Schlüssel verschlüsselt wird, das Entschlüsseln jedoch nur noch mit dem dazugehörigen privaten (geheimen) Schlüssel möglich ist. Elektronische Signaturen nutzen dieses Verfahren im umgekehrten Sinne [Er07].

[2] Siehe http://www.belab-forschung.de.

2.1 Integrität und Authentizität im elektronischen Laborbuch

Aufgrund der im Abschnitt 1.2 beschriebenen Vielfalt an Applikationen, die zur elektronischen Dokumentation des Forschungsprozesses und zur Verwaltung der Daten genutzt werden, wurde das im Rahmen des BeLab-Projekts entworfene Konzept mit einem generischen Ansatz verfolgt [Be11]. Konkret kann ein Web Service durch das eLab-System genutzt werden, um Daten, die beweiswerterhaltend archiviert werden sollen, zu übergeben. Das Zusammenspiel der Anwendungen eLab, BeLab (als Black-Box) und Archivsystem ist in Abbildung 1 dargestellt.

Bevor Daten durch das BeLab-System angenommen werden, wird das Datenformat überprüft. Nur bei dem erwarteten universellen Objektformat (UOF) werden die Daten angenommen. Dabei handelt es sich um ein Format, das auf den Ergebnissen des Projekts „kopal“[3] beruht. Danach werden entsprechende Dateien in einem TAR- oder ZIP-Archiv zusammengefasst. Zusätzlich wird dem Archiv (im Folgenden UOF-Objekt genannt) eine Datei (mets.xml) hinzugefügt, die die Metadaten zu den Dateien enthält. Die Struktur der Datei basiert auf dem Metadata Encoding & Transmisson Standard (METS). Mit ihm wurde ein Konzept entworfen, das mithilfe von Metadaten die Verwaltung und den Austausch von digitalen Objekten ermöglichen soll [Di10]. Der Nutzer des BeLab-Systems muss mindestens für jede Datei den entsprechenden Pfad in der Archiv-Datei und den Hashwert der Datei den Metadaten hinzufügen.

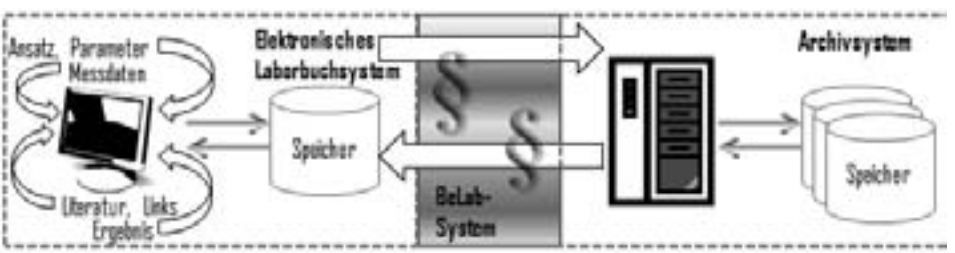


Abbildung 1: Kombination von eLab-, BeLab- und Archivsystem

Die Daten werden vor der Archivierung durch Datenüberprüfungsmodule des BeLab-Systems analysiert. Basierend auf dem Dateityp, der in einem ersten Schritt durch ein gesondertes Modul ermittelt wird, werden die entsprechenden Module geladen. Realisiert sind beispielsweise Module, die die Gültigkeit von internen oder externen Signaturen überprüfen. Die Module protokollieren die Ergebnisse in einem Log, der anschließend der Klassifizierung übergeben wird. Neben der Überprüfung einzelner Dateien erfolgt eine Analyse des gesamten übergebenen Archivs. Hier wird beispielsweise das Archiv auf mögliche Folgen von Dateien geprüft. Wird bei mehreren Dateien ein Muster im Dateinamen erkannt, erfolgt eine Prüfung auf Vollständigkeit, d. h. es wird betrachtet, ob (hier) eine Zahlenfolge Lücken aufweist [El11].

[3] Siehe http://kopal.langzeitarchivierung.de.

Die Vollständigkeit der Daten lässt auf eine gesicherte Datenerhebung schließen. Ein weiteres, stärkeres Indiz für eine gesicherte Datenerhebung ist die Nutzung von elektronisch signierenden Messgeräten. Diese sichern während der Datenerzeugung deren Integrität und Authentizität [PR+11]. Nach der Aufbereitung der Daten, kann die Integrität und Authentizität durch eine erneute Signatur gewährleistet werden. So geben eine vorhandene elektronische Signatur und die Gültigkeit der Signatur Rückschlüsse auf die Beweiskraft der Datei. Im Rahmen der im BeLab-System durchgeführten Klassifizierung werden diese Faktoren betrachtet. Ein weiterer Aspekt ist die Tauglichkeit des Dateityps zur Langzeitarchivierung. Hier werden durch die Klassifizierung Empfehlungen ausgegeben, wie geeignet oder ungeeignet ein Dateiformat bezüglich der Langzeitarchivierung ist [Be11].

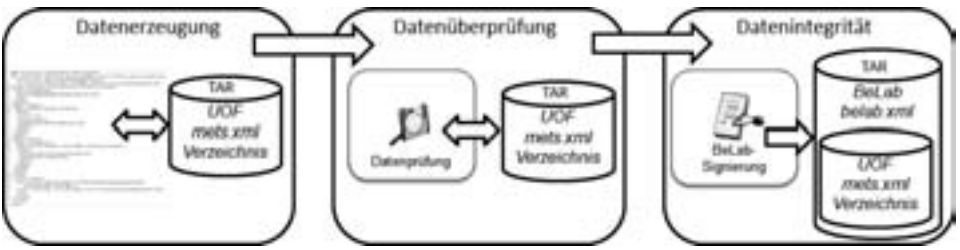


Abbildung 2: Verarbeitungsstufen zum Erhalt der Beweiskraft von Dateien

Bevor die Annahme der Daten durch das BeLab-System bestätigt werden kann, muss überprüft werden, ob die Integrität und Authentizität gewährleistet ist. Vorhandene elektronische Signaturen wurden bereits in der Datenüberprüfungsphase verifiziert. Es bleibt zu prüfen, ob jede in der mets.xml eingetragene Datei auch wirklich in der Archiv-Datei vorhanden ist. Andersherum muss geprüft werden, ob für jede Datei auch ein Eintrag in der mets.xml existiert. Ist dies der Fall, wird von jeder Datei der Hashwert erneut gebildet und mit dem in der mets.xml eingetragenen Wert verglichen. War dieser Vorgang erfolgreich, kann die mets.xml durch das BeLab-System signiert werden. Damit ist die Integrität der Archiv-Datei und der Metadaten gewährleistet. Die Verarbeitungsstufen der zu archivierenden Daten, beginnend bei der Datenerzeugung durch den Anwender, ist in Abbildung 2 dargestellt. Auf der Grundlage des vom Nutzer übergebenen UOF-Objekts werden die Datenprüfungen durch das BeLab-System durchgeführt. Die Ergebnisse werden sowohl in einem Log-Objekt als auch in den Metadaten protokolliert. Des Weiteren werden die Ergebnisse der anschließenden Klassifizierung mit in die Metadaten aufgenommen. Um die Integrität der übergebenen Metadaten zu schützen, werden die durch das BeLab-System zusätzlich erzeugten Metadaten in einer Kopie (belab.xml) erfasst. Diese Kopie wird im letzten Prozessschritt des Systems signiert und gemeinsam mit dem UOF-Objekt an das Archivsystem übergeben. Durch die Verwendung des BeLab Web Services kann der Forschende, der zur Dokumentation ein eLab verwendet, die im Scientific Data Lifecycle anfallenden und über das eLab-System gepflegten Daten beweiswerterhaltend archivieren. Über das Klassifizierungssystem wird dem Nutzer ein Maß zur Verfügung gestellt, mit dem die Beweiskraft, die Langzeitarchivierungstauglichkeit der Daten und die Art der Datenerzeugung bewertet werden kann.

2.2 Verwendung des BeLab Web Services

Um den im vorherigen Abschnitt beschriebenen Web Service nutzen zu können, muss sich der Nutzer im ersten Schritt erfolgreich authentifizieren. Dies kann mithilfe eines Benutzernamens und dem zugehörigen Passwort oder einem Client-Zertifikat geschehen [Be10]. Die Funktionen, die durch den Web Service zur Verfügung gestellt werden, dienen zur Datenübergabe, zum Datenabruf, zum Aktualisieren der Daten und zum Stornieren der Daten. Bei der Datenübergabe und der Aktualisierung werden die im vorherigen Abschnitt genannten Prüfungsmodule ausgeführt. Darauf basierend erfolgt die Klassifizierung. Bei einer Aktualisierung der Daten werden ältere Versionen mit einer entsprechenden Versionsnummer markiert. Die bei der Datenübertragung zurückgegebene Daten-ID wird dazu genutzt, um zugehörige Daten wieder abzurufen. Um den Einsatz des Archivierungssystems flexibel zu gestalten, wurde auch bei der Output-Schnittstelle des BeLab-Systems ein generischer Ansatz verfolgt. So ist es möglich mehrere Archivsysteme zu definieren, an die die Forschungsdaten übergeben werden. Bei der Datenübergabe werden die Daten in alle zuvor definierten Archive gespeichert. Beim Auslesen der Daten erfolgt ein Abgleich der Hashwerte der Daten aus jedem Archiv. Wurde in keinem Archiv eine Veränderung der Daten festgestellt, werden die Daten zurückgegeben.

Um das „Beschönigen“ von Messreihen zu verhindern, können Daten über das BeLab-System nicht gelöscht werden [Be11]. Stattdessen werden die Daten als „storniert“ gekennzeichnet. Beim Zugriff auf entsprechende Daten erfolgt ein Hinweis, dass die Daten bereits storniert wurden. Der Zugriff auf die Daten ist in diesem Fall nur über den Administrator des Systems möglich. Sind Daten nicht storniert und besitzt der Nutzer entsprechende Rechte, werden die archivierten Daten ausgegeben. Zusätzlich steht eine Funktion zur Verfügung, mit der die Metadaten zum Datenobjekt separat abgerufen werden können, so dass beispielsweise bei einer Metadaten-Recherche nicht alle Daten abgerufen werden müssen. Zurückgegeben werden die vom Benutzer übergebenen inklusive der vom BeLab-System erzeugten Metadaten.

Daten werden im BeLab-System auf unterschiedlichen Ebenen verwaltet. Unterschieden werden das eLab-System, die Projektzugehörigkeit der Daten und die Zuordnung der Daten zu einem benutzerdefinierten Container. Der Container kann beispielsweise für Forschungsdaten einzelner Forscher, die nur durch den entsprechenden Forscher eingesehen werden dürfen, oder als gemeinsam genutzter Datenbereich verwendet werden. Um den Zugriff auf die Funktionen nur berechtigten Personen zu erlauben, wird nach der erfolgreichen Authentifizierung eine Autorisierung durchgeführt. Dabei werden die drei genannten Datenebenen und die für den Benutzer zur Verfügung gestellten Funktionen berücksichtigt. Die Definition der Zugriffsregeln wurde über eine XML-Struktur realisiert. Für jeden Nutzer wird darin der Benutzername, die erlaubten Funktionen und die eLab-IDs, Projekt-IDs und Container-IDs für die der Zugriff erlaubt sein soll, festgehalten. Um Datenzugriffe und die Art des Zugriffs eines BeLab-Nutzers zu dokumentieren, werden bei jeder erfolgreichen Authentifizierung und Autorisierung Benutzername und gewünschte/ausgeführte Funktion durch das BeLab-System protokolliert. Dabei werden die entsprechenden Datenbereiche (eLab, Projekt, Container) mit aufgenommen.

Die im Abschnitt 1.2 vorgestellten Systeme DataFinder und open enventory nutzen den BeLab Web Service für eine beweiswerterhaltende Archivierung der im System gepflegten Daten. Das eLab-System open enventory bietet dazu dem Nutzer einen Button, mit dem die Übergabe der Daten an das BeLab-System angestoßen werden kann [Ru11]. Jedem Forscher steht es damit frei, die beweiswerterhaltende Archivierung zu einem gewünschten Zeitpunkt durchzuführen. Zur Übergabe der Daten werden die Daten aus dem eLab in Form eines Prüfberichts zusammengestellt. Vor der Integration des BeLab Web Services wurden diese Berichte ausgedruckt, vom Forscher unterschrieben und in einem gesammelten Buch archiviert. So wurde sowohl die Integrität und Authentizität als auch der Schutz vor unbefugtem Zugriff auf Forschungsergebnisse gewährleistet. Um den Archivierungsprozess zu vereinfachen, werden nun diese Prüfberichte als PDF erzeugt und im UOF, das durch das BeLab-System vorgegeben wird (siehe Abschnitt 2.1), an den Web Service übertragen. Jeder Nutzer des open enventory Systems, der sich erfolgreich am System angemeldet hat, kann über die Archivierungsfunktion den BeLab Web Service nutzen. Zur Authentifizierung und Autorisierung am BeLab-System wird bei dessen Installation ein Benutzer definiert, für den die gewünschten Rechte (hier: Datenübergabe und Datenaktualisierung) festgelegt werden. Da der Datenabruf und das Stornieren von Daten im Regelfall nicht abgedeckt sein müssen, werden diese Funktionen gesondert integriert. Die Autorisierung wird auf den Datenbereich des eLab-Systems eingeschränkt. Dazu wird die entsprechende eLab-ID für den definierten Benutzer eingetragen.

Auch in der Datenmanagement-Anwendung DataFinder wird der Archivierungsprozess durch den Nutzer des Systems veranlasst [Sc11]. Dazu wählt der Benutzer den entsprechenden Eintrag aus einem Kontextmenü, um die gewünschten Daten an den BeLab Web Service zu übergeben. Daten, die mithilfe des BeLab-Systems beweiswerterhaltend archiviert werden sollen, werden in einem dafür vorgesehenen Datenbereich gesammelt. Startet der Forscher den Archivierungsprozess, werden diese Daten in das Objektformat des BeLab-Systems umgewandelt und an die BeLab-Schnittstelle übergeben. Wie auch im vorherigen Beispiel, kann jeder Benutzer, der sich erfolgreich gegenüber dem System authentifiziert hat, die Übertragung veranlassen. So erfolgt auch in diesem Fall die Authentifizierung und Autorisierung am BeLab-System über einen zuvor definierten Nutzer, für den entsprechende Rechte festgelegt werden.

Durch den generischen Ansatz des BeLab-Systems können auch zur Archivierung der Daten unterschiedliche Archivsysteme eingebunden werden. Für jedes Modul wird eine entsprechende Schnittstelle entwickelt, die die notwendigen Funktionen zur Verfügung stellt. Die Authentifizierung und Autorisierung des BeLab-Systems gegenüber den Archivsystemen wird über einen dafür im Archivsystem definierten Nutzer realisiert. Die Zugangsdaten werden für das entsprechende Modul in der Systemkonfiguration eingetragen. Dem im Archivsystem definierten Benutzer müssen alle Funktionen, die durch das BeLab-System zur Verfügung gestellt werden, zugewiesen werden. Damit ist es dem eLab-Nutzer möglich alle Funktionen, die im BeLab-Konzept entworfen wurden [Be11], zu nutzen oder durch die Definition eines BeLab-Nutzers mit eingeschränkten Rechten zu kontrollieren.

3 Fazit und Ausblick

eLab-Systeme, LIMS und Datenmanagementsysteme dienen zur Verwaltung der Forschungsdaten und zur Dokumentation des Forschungsprozesses. Des Weiteren werden in der Forschung auch andere Anwendungen, die nicht für den Dokumentationsprozess entworfen wurden, dazu verwendet. Darüber hinaus werden Applikation im gesamten Scientific Data Lifecycle zur Auswertung und Verarbeitung der Daten eingesetzt. Durch die Integration des BeLab Web Service in diese Anwendungen, im speziellen in eLab-Systeme, kann zusätzlich der Beweiswert der Daten für den Anwender erkenntlich bestimmt und die Daten anschließend beweiswerterhaltend archiviert werden. Der Prozess der Archivierung kann dabei, wie in den im letzten Abschnitt beschriebenen Anwendungen, vom Forschenden in den Arbeitsprozess integriert werden. Andere Lösungen, wie die automatisierte Archivierung von Forschungsdaten zu einer vorgegebenen Zeit, sind des Weiteren denkbar und können je nach Wunsch umgesetzt werden. Durch den Zusammenschluss der Anwendungen (eLab-, BeLab- und Archivsystem) kann der Forschungsprozess zentral durch den Wissenschaftler gesteuert werden. Dabei bekommt der Benutzer durch das BeLab-System unterstützende Hinweise, wie beispielsweise über die Tauglichkeit der Daten zur Langzeitarchivierung.

Durch Autorisierungskonzepte werden Kollaborationen zwischen Forschern oder die Geheimhaltung von Daten realisiert. Im einfachsten Fall dient die Abfrage eines Benutzernamens und eines Passworts als Zugriffsschutz auf entsprechende Forschungsdaten. Diese Definitionen der Rechte variieren mit der Zahl der im Forschungsprozess eingesetzten Anwendungen. Beim Zusammenschluss der eLab-, BeLab- und Archivsysteme sind bereits drei Rollenkonzepte zu berücksichtigen. Die Pflege unterschiedlicher Rechtedefinitionen birgt die Gefahr der Fehlkonfiguration, so dass durch den Zusammenschluss der Systeme Rechte eventuell verletzt und die Geheimhaltung von Daten gefährdet wird. Ziel soll es daher sein, die Rechteverwaltung möglichst einheitlich und standardisiert, z. B. durch die eXtensible Access Control Markup Language (XACML)[4] zu pflegen. Es muss berücksichtigt werden, dass in der Regel eLab- und Archivsystem getrennt durch unterschiedliche Firmen oder Organisationen realisiert werden. So ist die Nutzung einer zentralen, gemeinsamen Autorisierungseinheit, Policy Decision Point (PDP) genannt, nur durch Kooperationen oder einer gesondert zu entwickelnden Einheit, Policy Enforcement Point (PEP) genannt, realisierbar.

Des Weiteren sind die Geheimhaltung von Daten, z. B. in einem Archivsystem, und der Verlust von Daten zu berücksichtigen. Werden z. B. Daten eines Forschenden durch gesonderte Zugriffsrechte oder eine Verschlüsselung geschützt, können diese Daten, durch das Ausscheiden des Forschers aus dem Unternehmen, verloren gehen. Daher müssen neben dem Zugriffsschutz Maßnahmen für Datenzugriffe in diesem Spezialfall im Rollenkonzept, z. B. durch ein Vier-Augen-Prinzip, berücksichtigt werden.

---

[4] OASIS eXtensible Access Control Markup Language (XACML) TC, http://oasis-open.org/committees/xacml/.

Literaturverzeichnis

[AKGo] AK Gooßen: open enventory, http://www.open-enventory.de/ - Stand 04.04.2012.

[Be10] Projektgruppe Beweissicheres elektronisches Laborbuch (BeLab): Anforderungspapier V.1.1, 2010, http://www.belab-forschung.de/belab/fileadmin/templates/mm_dam_fe/Anforderungspapier_V1.1_19.11.10.pdf - Stand 04.04.2012.

[Be11] Projektgruppe Beweissicheres elektronisches Laborbuch (BeLab): Schnittstellenpapier V.1.2, 2011, http://www.belab-forschung.de/belab/fileadmin/BeLabSchnittstellenpapierV1.2.pdf - Stand 04.04.2012.

[DFG98] DFG: Vorschläge zur Sicherung guter wissenschaftlicher Praxis: Empfehlungen der Kommission „Selbstkontrolle in der Wissenschaft, Wiley-VCH 1998.

[Di10] Digital Library Federation: <METS> Metadata Encoding and Transmission Standard: Primer and Reference Manual, Version 1.6 Revised, 2010, http://www.loc.gov/standards/mets/METSPrimerRevised.pdf - Stand 04.04.2012.

[DLR] Deutsches Zentrum für Luft- und Raumfahrt (DLR): DataFinder, http://datafinder.sourceforge.net/ - Stand 04.04.2012.

[EB+06] Ebel, H.F., Bliefert, C. und Greulich, W. Schreiben und Publizieren in den Naturwissenschaften. Wiley-VCH, Weinheim, 2006.

[El11] Ellmer, F. Automatische Metadatenanalyse zur beweiswerterhaltenden Langzeitarchivierung im Forschungsprozess. Karlsruher Institut für Technologie, Steinbuch Centre for Computing, Bachelorarbeit, 2011.

[Er07] Ertel, W. Angewandte Kryptographie. HANSER, München, 2007.

[Fi06] Fischer-Diskau, S. Das elektronisch signierte Dokument als Mittel zur Beweissicherung. Nomos, Baden-Baden, 2006.

[HJ+11] Hackel, S., Johannes, P.C., Potthoff, J., Madiesh, M. und Rieger, S. Scientific Data Lifecycle - Beweiswerterhaltung und Techniken. In BSI (Hrsg.): Sicher in die digitale Welt von morgen - Tagungsband zum 12. Deutschen IT-Sicherheitskongress, SecuMedia, Ingelheim, 2011.

[KIT] Karlsruher Institut für Technologie: Regeln zur Sicherung guter wissenschaftlicher Praxis im Karlsruher Institut für Technologie (KIT), http://www.kit.edu/downloads/K_OBP_XX_RI_01_05-10.pdf - Stand 04.04.2012.

[MPG00] MPG: Regeln zur Sicherung guter wissenschaftlicher Praxis – beschlossen vom Senat der Max-Planck-Gesellschaft am 24. November 2000, http://www.mpip-mainz.mpg.de/~pleiner/ombuds/regeln.pdf - Stand 04.04.2012.

[PJ11] Potthoff, J. und Johannes, P.C. Beweissicherheit und Archivierung von Forschungsdaten in der MPG. In A. Oberreuter, S. Vollmar und A. Weiße (Hrsg.): 27. DV-Treffen der Max-Planck-Institute, GWDG Bericht Nr. 77, GWDG, Göttingen, 2011.

[PR+11] Potthoff, J., Rieger, S., Johannes P.C. und Madiesh, M. Elektronisch signierende Endgeräte im Forschungsprozess. In: P. Schartner und J. Taeger (Hrsg.): D-A-CH Security 2011 - Tagungsband zur Konferenz D-A-CH Security 2011, syssec, Klagenfurt, 2011.

[Prov] Provendis GmbH: Laborbücher richtig geführt – Hinweise für den Wissenschaftler, http://www.provendis.info/fileadmin/provendis/downloads/Provendis-Website/Publikationen/Anleitung_Laborbuecher_091009x.pdf - Stand 04.04.2012.

[Ru11] Rudolphi, F. (Max-Planck-Institut für Kohlenforschung): Vortrag „open enventory“, 5. BeLab Workshop, 24.11.2011, Karlsruher Institut für Technologie.

[Sc11] Schreiber, A. (Deutsches Zentrum für Luft- und Raumfahrt): Vortrag „DataFinder“, 5. BeLab Workshop, 24.11.2011, Karlsruher Institut für Technologie.

[UOl] Zentrale Studienberatung der Universität Oldenburg: Das Laborbuch, http://www.studium.uni-oldenburg.de/cman/dateien/Lernwerkstatt/textsorten/Laborbuch.pdf - Stand 04.04.2012.

bwIDM: Föderieren auch nicht-webbasierter Dienste auf Basis von SAML

Michael Simon, Marcel Waldvogel, Sven Schober, Saher Semaan, Martin Nussbaumer

simon@kit.edu, marcel.waldvogel@uni-konstanz.de,
sven.schober@uni-ulm.de, semaan@uni-freiburg.de, nussbaumer@kit.edu

Abstract: Zur organisationsübergreifenden Nutzung von IT-Diensten werden Dienst-Föderationen gebildet. Dabei kann das Nutzerkonto der sogenannten Heimateinrichtung auch zum Zugriff auf nicht-lokale Dienste genutzt werden, d.h. Dienste, die von Dritten innerhalb der Dienst-Föderation angeboten werden. Während die Integration webbasierter Dienste in Föderationen mit SAML und beispielsweise Shibboleth mittlerweile in vielen Anwendungsbereichen allgegenwärtig ist, fällt die Integration nicht-webbasierter IT-Dienste (z.B. Dienste mit SSH-Zugängen) schwer. Existierende Ansätze, mit denen sich prinzipiell auch nicht-webbasierte Dienste integrieren lassen, erfüllen essentielle Anforderungen nicht und/oder sind nach ihrem heutigen Entwicklungsstand noch nicht betriebsfähig. In diesem Papier werden zwei Verfahren für nicht-webbasierte, föderative Dienstzugriffe (Moonshot und PAM/ECP) evaluiert und notwendige Erweiterungen zur Sicherstellung der Betriebsfähigkeit vorgestellt. Ein implementierter Proof-of-Concept zeigt die Umsetzbarkeit der Lösung.

1 Einleitung

Die zunehmende organisationsübergreifende Nutzung von IT-Diensten ist heutzutage nicht nur in der Forschungsgemeinschaft ein deutlich erkennbarer Trend. Zur effizienten und effektiven Arbeit ist die Nutzung von Diensten, die nicht lokal in der eigenen Organisation zur Verfügung stehen oder gestellt werden können, oft unabdingbar. Sind diese Dienste über einen Browser - demnach webbasiert - erreichbar, stellt dies für den Nutzer kaum noch besondere Hürden dar, obwohl oft ein Registrierungsschritt und die Preisgabe diverser personenbezogener Daten notwendig sind, um Zugang zum gewünschten Dienst zu erhalten. Insbesondere im Umfeld der wissenschaftlichen Dienstnutzung werden diese lokal beim Dienst implementierten Registriervorgänge und damit auch Dienst-lokale Nutzerverwaltungen bereits immer häufiger durch die für den Nutzer wesentlich komfortableren SAML[1]-basierten Implementierungen, wie zum Beispiel Shibboleth[2] oder SimpleSAMLphp[3], ersetzt. Diese Verfahren ermöglichen es, ein Nutzerkonto, das die eigene Organisation für den Nutzer verwaltet, zur Nutzung von Diensten Dritter einzusetzen.

Durch den Einsatz solch föderativer Verfahren zur Authentifikation (AuthN) und Autori-

[1] SAML: Security Assertion Markup Language, http://saml.xml.org/saml-specifications
[2] http://shibboleth.internet2.edu/
[3] http://simplesamlphp.org/

sierung (AuthZ) wird Nutzern ein größtmöglicher Komfort geboten, indem die Lokalität eines Dienstes weitestgehend verborgen wird und keine zusätzlichen Nutzerkonten zum Zugriff notwendig sind. Ferner ist dadurch in der Regel Single Sign-on (SSO) zwischen den in einer Föderation beteiligten Diensten möglich. Im Folgenden werden Mechanismen als *föderative Verfahren (FV)* bezeichnet, bei denen Nutzer dasjenige Konto für den Zugriff auf Dienste Dritter nutzen können, das ihre sogenannte Heimateinrichtung verwaltet.

Werden - kontrastierend zu webbasierten Diensten - nun die Dienste betrachtet, zu denen keine Möglichkeiten des webbasierten Zugriffs existieren, ist eine deutlich schlechtere Nutzerunterstützung in Form von FV feststellbar. High Performance Computing- (HPC), Grid- oder Cloud-Dienste sowie großskalige Datendienste bedürfen Dienst-lokale Nutzerkonten. Dies wird aus technischen Gründen auch in Zukunft nicht vermeidbar sein, jedoch lassen sich Dienst-lokale Konten durch FV vor einem Nutzer verbergen, indem das föderative Konto auf ein z.B. ad-hoc eingerichtetes Dienst-lokales Konto abgebildet wird. Obwohl Nutzern zusätzliche initiale Aufwände zur Dienstnutzung und oft auch ungewollte Hürden aufgebürdet werden, setzen Dienstbetreiber heute zumeist Personen und/oder umständliche Registriervorgänge zur Einrichtung Dienst-lokaler Konten ein. Begründet ist dies dadurch, dass bereits implementierte FV derzeit nur mit sehr viel Aufwand auf nicht-webbasierte Zugänge, wie zum Beispiel SSH-Zugänge, adaptierbar sind.

In diesem Papier werden zwei Ansätze vorgestellt, mit denen sich FV für nicht-webbasierte Dienste implementieren lassen, und im Hinblick auf ihre Tauglichkeit im produktiven Einsatz untersucht. Als Basis dafür dient ein im Folgenden vorgestellter Anforderungskatalog. Darauf aufbauend werden die Anforderungen identifiziert, denen durch die beiden föderativen Verfahren derzeit nicht nachgekommen werden kann: Dies betrifft insbesondere die Provisionierung und Deprovisionierung sowie Möglichkeiten zur Implementierung von Zustimmungsverfahren. Ein Ansatz für eine Kombination aus einem dieser Verfahren und notwendigen Erweiterungen wird vorgestellt. Ein standortübergreifend implementierter Proof-of-Concept (PoC) mit SSH-basierten Dienstzugängen zeigt die Umsetzbarkeit des Konzepts. Zusammenfassend sind die folgenden Beiträge Inhalt dieser Arbeit:

- Aufstellung eines Anforderungskatalogs zur Bewertung von FV
- Evaluation zweier existierender bzw. im Aufbau befindlicher FV
- Konzept zur Implementierung eines den Anforderungen entsprechenden Verfahrens
- *Proof-of-Concept* zur Verdeutlichung der Betriebsfähigkeit des Konzepts

Die hier vorgestellten Ergebnisse entstammen dem vom Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK) unterstützten Landesprojekt bwIDM[4].

Das Papier ist folgendermaßen strukturiert: Kapitel 2 gibt einen Überblick über den Stand der Technik in Bezug auf ausgewählte Komponenten und Mechanismen, die bei FV zum Einsatz kommen. In Kapitel 3 werden die Anforderungen an ein Verfahren für föderative und nicht-webbasierte Dienstzugänge zusammengetragen, bevor in Kapitel 4 zwei existierende bzw. im Aufbau befindliche Verfahren auf Basis dieser Anforderungen evaluiert

[4] www.bw-grid.de/bwservices/bwidm/

werden. Kapitel 5 beschäftigt sich mit den notwendigen Erweiterungen eines dieser Verfahren und Kapitel 6 fasst das Papier abschließend zusammen und gibt einen Ausblick auf die nächsten Schritte im Aufbau eines betriebsfähigen, föderativen Verfahrens.

2 Stand der Technik

FV müssen die Delegation der AuthN von Nutzern an Identitäts-Provider (IdP) unterstützen sowie die Möglichkeit bieten, AuthZ-Merkmale an einen Dienst zu liefern. Dies erfordert etablierte Vertrauensstellungen zwischen den Föderationspartnern. Im Folgenden werden ausgewählte System-APIs sowie zwei FV kurz vorgestellt.

2.1 Ausgewählte System-APIs zur Authentifikation

Eine Integration nicht-webbasierter Dienste in FV ist nicht trivial. Es bietet sich an, dafür Komponenten zu verwenden, die eine einheitliche AuthN-Schnittstelle bieten. Im Folgenden werden bekannte Schnittstellen unixoider Systeme vorgestellt.

Pluggable Authentication Modules (PAM) [Sam96] ist eine von Samar und Lai entwickelte Schnittstelle, die es ermöglicht eine zentrale AuthN bereit zu stellen. Sie stellt ferner grundlegende Funktionen zum Account-, Passwort- und Session-Handling zur Verfügung. PAM wird heute in nahezu allen unixoiden Systemen verwendet und kann aufgrund seiner Modularität erweitert werden.

Das **Generic Security Service Application Program Interface (GSS-API)** [Lin93] stellt eine Abstraktionsebene für Dienste bereit, die verschiedene Protokolle Betriebssystemunabhängig kapselt. Mittels GSS lassen sich AuthN-Mechanismen nutzen, ohne diese selbst zu implementieren. Ein Beispiel hierfür ist die Nutzung von Kerberos [NYHR05] über GSS-API [Lin96] (Implementierungen: MIT [NYHR05] oder Heimdal [DW98]).

2.2 Ausgewählte föderative Implementierungen

Eduroam (Education Roaming) [MRW+08] (gefördert durch GÉANT2-Projekt) ist ein Verfahren, das es Nutzern ermöglicht, eine WLAN-Infrastruktur mit den Zugangsdaten ihrer Heimateinrichtung zu verwenden. Basis dafür bildet das Extensible Authentication Protocol (EAP), durch welches das Ergebnis der AuthN an den Access Point vor Ort gelangt [ABV+04]. Die Föderation wird durch eine baumartige RADIUS-Server-Hierarchie aufgespannt [RWRS00]. Eine robuste RADIUS-Implementierung stellt Radiator dar, die Weiterleitungen von Nachrichten über gesicherte Verbindungen mit definierten Vertrauensstellungen unterstützt [WMVW11]. Eine Adaption weiterer Dienste - neben WLAN - ist beispielsweise im Rahmen des eduGAIN-Projektes geplant [HVS10].

Die SAML-basierte **Shibboleth**-Software wurde von der Internet2 Middleware Initiati-

ve entwickelt und erlaubt die Umsetzung einer *Authentication and Authorization Infrastructure* (AAI). Die AAI des Deutschen Forschungsnetz (DFN-AAI) verwaltet SAML-basierte Föderationen für die deutschen Hochschulen. Bei einem Dienstzugriff innerhalb einer AAI delegiert ein Dienst (Service Provider, SP) die AuthN des Nutzers an einen IdP. Darüber hinaus unterstützt SAML den verschlüsselten Austausch von Attributen zwischen IdP und SP zur AuthZ des Nutzers. Neben Shibboleth existieren weitere SAML-Implementierungen, wie beispielsweise SimpleSAMLphp.

3 bwIDM-Anforderungskatalog für föderative Verfahren

Die Auswahl einer technischen Grundlage für die AuthN/AuthZ für nicht-webbasierte IT-Dienste richtet sich nach den Anforderungen anzubindender Dienste. Im Rahmen von bwIDM wird auf Cloud-Speicherdienste und damit Protokolle wie CIFS oder NFS sowie insbesondere Computing-Dienste (HPC, Grid etc.) mit SSH-Zugängen fokussiert.

Neben Anforderungen an die AuthN müssen AuthZ-Merkmale an IT-Dienste übermittelt werden können *(Anforderungsblock A-1)*. Dazu gehören beispielsweise Attribute wie Name, E-Mail-Adresse oder die Institutionszugehörigkeit im Sinne der Landeshochschulgesetze (siehe auch eduPerson-Schema des DFN-Vereins[5]). Die Übertragung soll gemäß den Schutzzielen der IT-Sicherheit erfolgen (vgl. [Eck09], Kapitel 1.2). Ferner stellen bestehende Datenschutzgesetze (z.B. BDSG) Anforderungen an die Lösung. Es gilt insbesondere der datenschutzrechtliche Grundsatz der Datensparsamkeit. Werden die Attribute an Dritte übertragen, sind darüber hinaus Einverständniserklärungen der Nutzer sowie ggf. Zustimmungen zu Nutzungsrichtlinien (engl.: Acceptable Use Policies, AUP) notwendig.

Werden Attribute zum Dienst übertragen, müssen diese Daten aktuell gehalten beziehungsweise widerrufen werden können. Demnach sind die Provisionierung und Deprovisionierung für FV inhärente Anforderungen *(Anforderungsblock A-2)*. Bei einer erstmaligen Anmeldung an einen Dienst über ein FV werden ggf. Attribute als Grundlage für eine Zugriffsentscheidung übermittelt. Die Aktualität dieser Attribute ist insbesondere dann wichtig, wenn diese für weitere Prozessschritte im Anschluss an die eigentliche Dienstnutzung Verwendung finden. Dies kann zum Beispiel bei einem Bibliotheksdienst der Fall sein, bei dem Ausleihen getätigt wurden und ein Mahnverfahren notwendig wird. Beispiele für eine notwendige Deprovisionierung sind Dienst-lokale Konten sowie die Reservierung von persistent adressierbaren Ressourcen bei Computing-Diensten. Verliert ein Nutzer die Zugriffsberechtigung, bedarf es entsprechender Richtlinien und technischer Verfahren.

Einen dritten Anforderungsblock *(A-3)* bilden Merkmale, die ausschlaggebend für die Betriebsfähigkeit des Ansatzes sind. Hierzu gehört die Vermeidung zentraler Komponenten, wenn deren Funktionalität in dezentralen Komponenten abgebildet werden kann, um Wartungsaufwände und Abhängigkeiten gering zu halten. Ferner soll das FV absehbar zukunftssicher sein. Kriterien für die Abschätzung der Zukunftssicherheit sind die Art der Fortentwicklung eines FV und die Möglichkeit dieses in bestehende föderative Verbände - wie beispielsweise die DFN-AAI - zu integrieren. Ferner sollen die Aufwände zur Im-

[5] https://www.aai.dfn.de/der-dienst/attribute/

plementierung und zum Betrieb möglichst gering gehalten werden (Lizenz-/Hardware/ Wartungskosten und Nutzer-Support). Beispielsweise steigt der Aufwand für den Nutzer-Support, wenn Anmeldevorgänge nicht selbsterklärend sind oder wenn Nutzer-lokale Anpassungen erforderlich werden. Letztendlich muss das Verfahren skalierbar im Hinblick auf die Anzahl der Nutzer, Dienste und teilnehmenden Einrichtungen sein.

4 Evaluation föderativer Verfahren

Im Folgenden werden zwei Ansätze zur Implementierung von FV vorgestellt, jeweils hinsichtlich der in Kapitel 3 vorgestellten Anforderungen evaluiert und die Betriebsfähigkeit nach aktuellem Entwicklungsstand diskutiert. In die Evaluation fließen insbesondere auch die Erfahrungen aus einer jeweiligen Test-Implementierung beider Ansätze ein.

4.1 Moonshot-Ansatz

Im Projekt *Moonshot*[6] (gefördert von JANET (UK) und GÉANT) werden Anpassungen und Kombinationen von Standard-Software-Komponenten gängiger Betriebssysteme für FV entwickelt. Kern des Ansatzes bildet die Kombination der GSS-API und EAP (vgl. Kapitel 2) sowie die Integration in RADIUS-Infrastrukturen. Des Weiteren soll zur Übermittlung von AuthZ-Attributen SAML eingesetzt werden. Im Fokus der Entwicklung stehen nicht nur unixoide Systeme, die durch Anpassung der GSS-API integriert werden, sondern auch Windows-Systeme. Moonshot strebt an, Anpassungen von Standardkomponenten zukünftig zu vermeiden, indem veränderte Mechanismen in Form von RfCs dokumentiert und in die Distributionen der einzelnen Betriebssysteme integriert werden.

Moonshot lehnt sich technologisch sehr stark an die bereits etablierten Mechanismen an, die im Rahmen von eduroam zum Einsatz kommen. Ein Nutzer wird hierbei ausschließlich direkt gegenüber seiner Heimateinrichtung authentifiziert, so dass die Anmeldedaten sowohl im Sinne des Datenschutzes als auch der IT-Sicherheit ausreichend geschützt sind. Bislang ist noch offen, wie Merkmale des Nutzers von der Heimateinrichtung an den Dienst übertragen werden, die etwa zur AuthZ benötigt werden; gerade dies ist aber im Rahmen von bwIDM eine zentrale Anforderung *(Anforderungsblock A-1)*.

Des Weiteren wird der Bereich der Provisionierung und Deprovisionierung von Nutzerkonten durch Moonshot bislang nicht betrachtet. Jedoch sind diese elementaren Prozesse eines FV Anforderungen im Rahmen von bwIDM *(Anforderungsblock A-2)*.

Schließlich setzt Moonshot voraus, dass beim Rechner des Nutzers angepasste Programme beziehungsweise Bibliotheken vorliegen. Dies ist derzeit im Allgemeinen nicht der Fall und auch frühestens mittelfristig zu erwarten, so dass zunächst auf jedem Client zusätzliche Software installiert werden muss. Dies bedeutet einen nicht unerheblichen Wartungs- und Supportaufwand *(Anforderungsblock A-3)*.

[6] http://project-moonshot.org/

4.2 PAM/ECP

Enhanced Client or Proxy (ECP) ist ein SAML-Profil [HCH+05], das - im Gegensatz zum sonst oft üblichen WebSSO-Profil - für nicht-webbasierte Zugangssysteme Verwendung finden kann. Dabei wird entweder ein erweiterter *Client* benötigt, der dieses Profil nativ unterstützt, oder ein *Proxy*, der die Funktionalität vor dem Client verbergen kann.

Der SAML-Standard spezifiziert *Assertions* zur Übertragung von Attributen, um den Diensten AuthZ-Merkmale bereit zu stellen *(Anforderungsblock A-1)*. Bezüglich der Datensicherheit sollte bei der Übertragung der Attribute jedoch auf einen sicheren Kanal geachtet werden. Dies ist bei SAML nicht verpflichtend, wird aber empfohlen und üblicherweise durch HTTPS als Übertragungsstandard umgesetzt. Bei gängigen SAML-Implementierungen - wie etwa Shibboleth - kann festgelegt werden, welchem Dienst welche Attribute übermittelt werden*(Anforderungsblock A-1)*. Dadurch werden die Anforderungen bzgl. der Datensparsamkeit erfüllt. Derzeit ist jedoch das Einholen einer expliziten Erlaubnis zur Übermittlung von personenbezogenen Daten innerhalb eines PAM-Moduls nicht möglich. Es können auch keine Änderungen an personenbezogenen Daten ohne erneute Interaktion des Nutzers übermittelt werden *(Anforderungsblock A-2)*. Zusätzlich ist bei der einfachsten Variante von PAM ein Vertrauen gegenüber dem Dienst notwendig, da dieser in seiner Funktion als Proxy Kenntnis der Zugangsdaten bekommen kann.

Ferner unterstützt die aktuelle Shibboleth-Implementierung eines Identity Provider ECP „nur“ mit der sogenannten *HTTP Basic Authentication*. Das Anmelden ist demnach jedoch wie gefordert mit einer Nutzername-/Passwort-Kombination möglich. Durch die Verwendung von PAM werden zudem nachgelagerte oder vorausgehende AuthN-Mechanismen eines Dienstes nicht beschränkt. Effektiv kann also bei einem SSH-Dienst weiterhin zusätzlich eine Public-/Private-Key-AuthN vom SSH-Server direkt vorgenommen werden, wie es dem heutigen Vorgehen entspricht. Grundsätzlich wird die Kombination von PAM und ECP implizit von allen SAML-Föderationen mitgetragen. Bei SAML handelt es sich ferner um einen etablierten Standard, den bereits viele Hochschulen beispielsweise im Rahmen der Teilnahme an der DFN-AAI unterstützen. Wird bei den Institutionen ein Shibboleth IdP in einer neueren Version verwendet, ist ECP durch eine Änderung der Konfiguration aktivierbar. *(Anforderungsblock A-3)*

5 Notwendige Erweiterungen: Konzept und Implementierung

Wie in den vorangegangenen Abschnitten erläutert wurde, kann mit Hilfe von PAM/ECP auch auf unixoiden Systemen die AuthN von Nutzern über Shibboleth-Mechanismen erfolgen. Allerdings werden hierbei weitere Fragen und Probleme aufgeworfen, die nicht unmittelbar die AuthN als solche betreffen. Da für die Nutzung eines unixoiden Systems ein Eintrag in einer Name Switching Service-Datenbank (NSS) notwendig ist, kann auf einen Registriervorgang nicht verzichtet werden. Dieser Registriervorgang kann in einer Webanwendung realisiert werden. Dort ist es möglich das Einverständnis des Nutzers zur Datenübermittlung einzuholen. Da die aktuellen Daten bei jedem weiteren Login übermittelt

werden, besteht die Möglichkeit, dass personenbezogene Daten, die sich geändert haben, ohne erneutes Einverständnis des Nutzers an den Service Provider gemeldet werden. Konkret handelt es sich hier demnach um die vor- beziehungsweise nachgelagerten notwendigen Vorgänge, also die Provisionierung und Deprovisionierung von Dienst-lokalen Nutzerkonten. Zusätzlich ist es möglich und wünschenswert, eine explizite Bestätigung der Kenntnisnahme der Acceptable Use Policy (AUP) durch den Nutzer zu fordern. Diese drei Aspekte erfordern zusätzliche Infrastruktur, wie in den folgenden Abschnitten erläutert wird. Im Rahmen von bwIDM wurden diese Ergänzungen in Form eines Prototypen implementiert.

5.1 Provisionierung von Nutzern durch einmaliges „Registrieren“ (Web)

Einer der Vorteile einer dezentralen AuthN, wie sie mit Shibboleth zur Verfügung gestellt wird, besteht darin, dass neue Nutzer mit relativ wenig Aufwand angelegt werden können. Es ist nicht notwendig, alle potentiell betroffenen Systeme von dieser Änderung in Kenntnis zu setzen; vielmehr ist es ausreichend, dem zuständigen Identity Provider gegenüber die Daten des neuen Nutzers bekannt zu geben. Dies hat aber andererseits zur Folge, dass ein Dienst, der Shibboleth zur AuthN von Nutzern verwendet, per definitionem keine A-priori-Kenntnis haben kann, welcher Nutzer potentiell den Dienst in Anspruch nehmen wird. Dementsprechend ist es dem Dienst unmöglich, von sich aus etwaig notwendige Vorbereitungen zu treffen, um jedem potentiellen Nutzer Zugang zum Dienst zu gewähren.

Um beispielsweise auf einem Linux-Rechner, der als Dienst oder Dienstzugang genutzt wird, sinnvoll arbeiten zu können, ist es häufig notwendig, dass der Nutzer über ein lokales Nutzerkonto verfügt, das über längere Zeit hinweg unverändert zur Verfügung steht. Insbesondere sind eine wohldefinierte Unix-UID und ein wohldefiniertes Home-Verzeichnis notwendig, wenn nicht bei jedem Zugriff auf den Dienst alle notwendigen Daten erneut auf die Linux-Maschine kopiert und nach erfolgter Benutzung des Dienstes alle Ergebnisdaten wieder auf einen anderen, permanenten Speicher zurückkopiert werden sollen. Genau dieses Modell findet beispielsweise im Grid-Umfeld Anwendung und erlaubt es mangels der Notwendigkeit, Daten für längere Zeit aufzubewahren, Dienstnutzer für die Dauer der einzelnen Nutzung dynamisch auf einen im Prinzip beliebigen lokalen Account abzubilden. Die damit verbundenen Nachteile sollen jedoch im Projekt bwIDM vermieden werden, so dass es insbesondere notwendig ist, für jeden Dienstnutzer ein permanentes (oder wenigstens mittelfristig stabiles) lokales Nutzerkonto einzurichten.

Dies erfolgt im vorgestellten Prototyp mit Hilfe eines webbasierten Selbstbedienungsportals, das der Nutzer einmalig vor dem allerersten Dienst-Zugriff besuchen muss. Das Webportal erlaubt es dem Anwender, nach erfolgter Shibboleth-Webauthentifikation auf „Knopfdruck“ ein lokales Nutzerkonto erzeugen zu lassen, das mit seiner Shibboleth-Identität verknüpft wird. Durch diese „Registrierung“ des Nutzers wird Dienst-seitig eine (aus Nutzersicht zunächst zufällige) UID gewählt und damit ein lokales Konto eingerichtet sowie das zugehörige Home-Verzeichnis angelegt. Nach dieser Registrierung steht das Konto permanent und stabil zur Verfügung, so dass der Nutzer einen „normalen“ SSH-Zugang zum Dienst bereitgestellt bekommt. Insbesondere können aus technischer Sicht

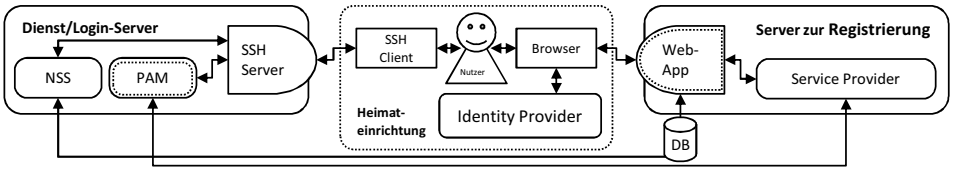


Abbildung 1: Proof-of-Concept: PAM/ECP-Ansatz mit Erweiterung (WebApp und PAM)

beispielsweise SSH-Schlüssel in das Home-Verzeichnis abgelegt werden, so dass sich der Zugang aus Nutzersicht wie jeder andere SSH-Zugang verhält.

5.2 AUP-Unterstützung durch getrennten Provisionierungsschritt (Web)

Als weiteren Vorteil der im vorigen Abschnitt beschriebenen Registrierung mittels eines Webportals erweist es sich, dass durch diese Dienstaktivierung durch den Nutzer eine direkte Interaktionsmöglichkeit hergestellt wird. An dieser Stelle ist es beispielsweise möglich, der Registrierung eine Anerkennung der für den konkreten Dienst gültigen AUP voranzustellen, ohne die keine Aktivierung des Dienstzugangs erfolgt. In ähnlicher Weise kann auch eine erneute Anerkennung der AUP durch den Nutzer erzwungen werden, indem das lokale Nutzerkonto mit einem entsprechenden Hinweis deaktiviert wird, der den Nutzer auffordert, sich erneut zu registrieren. Dies ist beispielsweise dann wünschenswert beziehungsweise notwendig, wenn sich die AUP seit der letzten Zustimmung des Nutzers geändert haben und dies dem Nutzer explizit zur Kenntnis gegeben werden soll.

5.3 Realisierung als Proof-of-Concept

Um diese Thematik weiter zu evaluieren, wurde ein PoC erstellt (vgl. Abbildung 1). Teil des PoC ist ein PAM, das als Enhanced Proxy agiert, um so einen transparenten Zugang mit einem unmodifizierten SSH-Client auf einem unmodifizierten SSH-Server zu ermöglichen. Es kommt das pam_python Modul zum Einsatz und die AuthN wird über ein Python Script realisiert. Das Script richtet eine PAOS-Anfrage (Reverse SOAP[7]) an einen Shibboleth SP, der für die ECP Nutzung konfiguriert ist. Auf diese Anfrage antwortet der SP mit einer SOAP-Anfrage, die das Script an den zuständigen ECP-Endpunkt des IdP schickt. Dabei kommt ein Suffix ähnlich einem Radius-Realm zum Einsatz. Dieses Suffix muss in einer Mapping-Tabelle mit einem dazugehörenden ECP-Endpunkt vorhanden sein. Aktuell unterstützt der Shibboleth IdP nur die ECP-Variante mit HTTP Basic Authentifikation. Bei dieser Variante wird der ECP-Endpunkt beim IdP mittels HTTP Basic geschützt. Es ist also Aufgabe des Scripts die vom Nutzer übermittelten Zugangsdaten mit der SOAP Anfrage an den ECP-Endpunkt zu übermitteln. Ist der Login erfolgreich, antwortet der IdP mit einer Assertion, die das Script wiederum an den SP weiterleitet.

[7] http://www.w3.org/TR/soap/

An dieser Stelle können nun vom SP evtl. notwendige AuthZ-Merkmale entgegengenommen und überprüft werden. Für diesen PoC musste lediglich ein PAM sowie eine Web-Anwendung implementiert werden. SSH-Clients und -Server, NSS sowie Shibboleth IdP und SP können ohne Anpassung des jeweiligen Programmcodes in die vorgeschlagene Infrastruktur aufgenommen werden. Dies unterstreicht die Betriebsfähigkeit des Ansatzes.

5.4 Deprovisionierung: Aufstellen von Regeln (dienstabhängig)

Die Provisionierung von permanenten Nutzerkonten bringt jedoch auch Probleme mit sich. Insbesondere ist zunächst unklar, wie zu verfahren ist, wenn ein Nutzer das Zugangsrecht zum Dienst verliert, sei es etwa durch Ausscheiden aus der Hochschule oder beispielsweise aufgrund der Sperrung seines Accounts aus Sicherheitsgründen. Ist ein permanentes Nutzerkonto eingerichtet, das es zum Beispiels erlaubt, sich mit Hilfe von SSH-Schlüsseln zu authentifizieren, so ist es dem Dienst nicht ohne weiteres möglich, von entsprechenden Änderungen des Shibboleth-Nutzerprofils Kenntnis zu erlangen, da in diesem Fall keine AuthN gegenüber dem Shibboleth IdP erfolgt. Wie der Dienst möglichst zeitnah über Änderungen informiert wird, ist noch unklar und wird derzeit in weiterführenden Untersuchungen adressiert. Denkbar wäre einerseits ein Push-Ansatz, bei dem der IdP alle ihm bekannten Dienste aktiv mit Änderungsmeldungen versorgt; ein derartiger Ansatz scheint jedoch bereits aus Komplexitätsgründen nicht ratsam, würde aber jedenfalls das lose gekoppelte föderale Konzept brechen, da jeder IdP doch wieder Informationen an alle Dienste verteilen müsste. Alternativ wird im Projekt bwIDM derzeit ein Pull-Ansatz evaluiert, bei dem jeder Dienst beim Login der Nutzer oder auch regelmäßig beim IdP anfragt, um Änderungen an den für ihn relevanten Identitäten zu erfahren. Hierbei wird insbesondere untersucht, ob Shibboleth/ECP bereits alle notwendigen technischen Mittel bereitstellt.

6 Zusammenfassung und Ausblick

Nach der Integration zahlreicher webbasierter IT-Dienste in föderative Verbünde wächst der Wunsch nach betriebsfähigen Integrationslösungen für nicht-webbasierte Dienste. Im vorliegenden Papier wurden Anforderungen an föderative Verfahren aufgestellt, die erfüllt werden müssen, um auch diese Dienste einbinden zu können. Moonshot, als ein derzeit entstehender, Radius-basierter Ansatz, und ein Ansatz zur Dienstintegration via PAM und ECP wurden vorgestellt und bewertet. Kontrastierend zu den zuvor aufgestellten Anforderungen wurden notwendige Erweiterungen für den für die Integrationsvorhaben vielversprechenderen zweiten Ansatz (PAM/ECP) identifiziert. Die technische Ausgestaltung dieser Erweiterungen wurde im Folgenden diskutiert und die Umsetzbarkeit in einem Proof-of-Concept (PoC) belegt. Das so skizzierte bwIDM-Konzept passt mit der bisherigen Planung und prototypischen Umsetzung auf die obligatorischen Anforderungen.

Auch wenn die Anforderungen durch das skizzierte PAM/ECP-Konzept mit den diskutierten Erweiterungen weitestgehend erfüllt werden können, sind weitere Schritte in Rich-

tung einer betriebsfähigen Lösung zu gehen. Neben der zu führenden Diskussion über die Deprovisionierung (Push- oder Pull-Ansätze), sind Richtlinien zur Nutzung der bwIDM-Föderation zu definieren. Ferner ist der derzeit auf SSH-Zugänge beschränkte PoC auf die in Kapitel 1 genannten CIFS und NFS zu erweitern. Abschließend sollte diskutiert werden, wie dem SAML-Paradigma Rechnung getragen werden kann, so dass einem SP der Zugriff auf die Credentials eines Nutzers stets verwehrt werden kann.

7 Weitere Autoren und Danksagung

An der Entstehung dieses Papiers waren neben den oben genannten Personen folgende Autoren beteiligt: Tobias Dussa und Sebastian Labitzke (Editor) vom Karlsruher Institut für Technologie (KIT), Jacob Becker, Markus Grandpre, Michael Längle und Daniel Scharon von der Universität Konstanz, Harald Däubler und Vladimir Nikolov von der Universität Ulm sowie Markus Klein von der Universität Freiburg. Ein besonderer Dank gebührt dem Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK), dem Projektverantwortlichen Prof. Dr. Hannes Hartenstein sowie allen Projektteilnehmern aller Landesuniversitäten in Baden-Württemberg.

Literatur

[ABV+04] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson und H. Levkowetz. Extensible Authentication Protocol (EAP) - RfC 3748, 2004.

[DW98] J. Danielsson und A. Westerlund. Heimdal: an independent implementation of Kerberos 5. In *Proceedings of the annual conference on USENIX Annual Technical Conference*, ATEC '98, pages 34–34, Berkeley, CA, USA, 1998. USENIX.

[Eck09] C. Eckert. *IT-Sicherheit - Konzepte, Verfahren, Protokolle (6.A.)*. Oldenbourg, 2009.

[HCH+05] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, P. Mishra, R. Philpott und E. Maler. Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0, 2005.

[HVS10] J. Howlett, Nordh V. und W. Singer. Deliverable DS3.3.1: eduGAIN service definition and policy Initial Draft. Technical report, GÉANT, 2010.

[Lin93] J. Linn. Generic Security Service Application Program Interface - RfC 1508, 1993.

[Lin96] J. Linn. The Kerberos Version 5 GSS-API Mechanism - RfC 1964, 1996.

[MRW+08] M. Milinovic, J. Rauschenbach, S. Winter, L. Florio, D. Simonsen und J. Howlett. Deliverable DS5.1.1: eduroam Service Definition and Implementation Plan. Technical report, GÉANT2, 2008.

[NYHR05] C. Neuman, T. Yu, S. Hartman und K. Raeburn. The Kerberos Network Authentication Service (V5) - RfC 4120, 2005.

[RWRS00] C. Rigney, S. Willens, A. Rubens und W. Simpson. Remote Authentication Dial In User Service (RADIUS) - RfC, 2000.

[Sam96] V. Samar. Unified login with pluggable authentication modules (PAM). In *Proceedings of the 3rd ACM conference on Computer and communications security*, CCS '96, pages 1–10, New York, NY, USA, 1996. ACM.

[WMVW11] S. Winter, M. McCauley, S. Venaas und K. Wierenga. TLS encryption for RADIUS - draft-ietf-radext-radsec-09, 2011.

Die OCTAVE-Risikoanalysemethode als selbstgesteuerter Einstieg ins Informationssicherheitsmanagement

Christian Paulsen
DFN-CERT Services GmbH
Sachsenstraße 5
20097 Hamburg
paulsen@dfn-cert.de

Abstract: In diesem Beitrag wird die Risikoanalysemethode OCTAVE vorgestellt, die einen einfachen Einstieg in das komplexe Thema Informationssicherheitsmanagement ermöglicht. Dieser selbstgesteuerte Analyseansatz konzentriert sich auf die kritischen Werte einer Organisation und auf eine Auswahl von geeigneten Schutzmaßnahmen. Die Methode ist vollständig kompatibel zum Informationssicherheitsstandard ISO 27001.

1 Einleitung

Grundlage für jede aktive und angemessene Sicherheitsstrategie ist eine Risiko- und Bedrohungsanalyse, in der systematisch die betriebswirtschaftlichen Risiken mit Schwachstellen und Gefährdungen in Beziehung gesetzt werden, um daraus Maßnahmen zur Risikoverminderung bzw. -vermeidung abzuleiten. Dies gilt ganz besonders für den Teilaspekt der Informationssicherheit[1], der heute immer stärker Einfluss – direkt und indirekt – auf alle anderen Risiken einer Organisation nimmt. Viele Unternehmen, Hochschulen und andere Organisationen stehen jedoch vor dem Problem, den Einstieg in dieses komplexe Thema mit begrenzten zeitlichen und finanziellen Ressourcen zu bewältigen. Die für eine Bewertung der Informationssicherheit zur Verfügung stehenden Standards bieten wenig Unterstützung bei der Fragestellung, wie eine Risikoanalyse sinnvoll und angemessen durchgeführt werden kann, da die Umsetzung von Maßnahmen nicht Gegenstand von Normen ist. Mit dem Ziel, diese Lücke zu schließen, bietet das DFN-CERT die Risikoanalysemethode OCTAVE an, die in diesem Beitrag zusammenfassend und praxisorientiert vorgestellt wird.

[1] In der Fachliteratur wird zunehmend der Begriff IT-Sicherheit durch Informationssicherheit ersetzt, um den ganzheitlichen Ansatz hervorzuheben.

2 Nachteile gängiger Risikoanalyseverfahren und -standards

Jede Organisation bzw. jedes Unternehmen, das eine IT-Infrastruktur besitzt, setzt bereits mehr oder weniger umfangreiche Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit der verwendeten Daten und Systeme ein. Es ist jedoch für die verantwortlichen Mitarbeiter und deren Vorgesetzte in der Regel sehr schwierig zu evaluieren, ob die gewählten Maßnahmen ausreichend sind oder nicht. Dies kann erst durch eine individuelle Risikoanalyse in Erfahrung gebracht werden. Gängige Standards zur Informationssicherheit bieten jedoch wenig Unterstützung bei der Fragestellung, wie eine Risikoanalyse sinnvoll und angemessen durchgeführt werden kann. Lediglich das BSI bietet eine Methode zur Risikoanalyse an. Diese kann jedoch nur dann zur Anwendung kommen, wenn eine Organisation bereits den IT-Grundschutz (weitgehend) umgesetzt hat.

Inzwischen haben viele IT-Sicherheitsdienstleister die Durchführung einer Risiko- und Bedrohungsanalyse in ihrem Angebot. Die angewandten Methoden sind jedoch häufig nicht transparent und die zur Anwendung kommenden Maßstäbe unterscheiden sich in der Praxis sehr. Somit ist eine Reproduzierbarkeit oder auch nur Vergleichbarkeit in der Regel nicht gegeben. Des weiteren ist es häufig so, dass Unternehmen / Organisationen auf die Einbeziehung einer externen Expertise angewiesen sind und somit das Know-How – dabei vor allem der Erfahrungsschatz aus der praktischen Arbeit in anderen, vergleichbaren Organisationen – herein geholt werden soll. Die Vergleichbarkeit ist auch dann ausschlaggebend, wenn intern die Ergebnisse verschiedener eigener Risikoanalysen (z. B. aus den Vorjahren) mit einem aktuellen Ergebnis verglichen werden sollen.

Damit für eine Organisation durch die Risikoanalyse und Sicherheitsbewertung ein qualifiziertes Ergebnis erzielt werden kann, müssen alle Beteiligten ihre Stärken in den Sicherheitsprozess mit einbringen. Erwartet wird ja gerade die zielgerichtete Umsetzung von Maßnahmen zur Absicherung kritischer Geschäftsprozesse, Vermeidung von Fehlinvestitionen und insgesamt eine tragfähige Umsetzung einschließlich Budgetplanung. Dies kann nicht allein durch die IT-Sicherheitsverantwortlichen und technischen Administratoren geleistet werden. In manchen Fällen führen die Diskussionen vor und während der Risikoanalyse auch zu einem grundlegenden Wandel in der Einschätzung von Informationssicherheit (Stichwort „Awareness“). Ausgelöst wird dann gewissermaßen ein Paradigmenwechsel, durch den die Verantwortung für Informationssicherheit insgesamt neu geregelt wird. Der Fokus der Analyse darf also nicht nur auf technische Aspekte beschränkt sein.

Ein weiterer wichtiger Punkt, der oft unterschätzt wird, ist die Nachhaltigkeit. Die reine Erfassung der aktuellen Situation oder die einmalige Durchführung einer Risikoanalyse ist nicht zielführend. Stattdessen müssen Ergebnisse kontinuierlich umgesetzt und Maßnahmen überwacht oder angepasst werden. Informationssicherheit ist kein statischer Zustand, sondern ein Prozess, der auch als solcher verstanden sein muss.

3 Erfolgsfaktoren für nachhaltige Risikoanalysen

Aus den im vorigen Abschnitt genannten Aspekten resultieren die folgenden Erfolgsfaktoren für die Durchführung einer nachhaltigen Risikoanalyse:

- Anwendung einer einheitlichen und transparenten Methode, mit der durch ein Team Risiken und Bedrohungen analysiert werden können, um zu reproduzierbaren und vergleichbaren Ergebnissen zu gelangen.
- Maßgebliche Beteiligung durch Einforderung einer konkreten inhaltlichen Mitarbeit (Eigenanteil) aller Verantwortlichen, ihren jeweiligen Rollen entsprechend, um Kosten zu senken und die Akzeptanz der Ergebnisse zu erhöhen.
- Beteiligung aller Entscheidungsebenen in einer Organisation (Management, Vertreter der Fachabteilungen, IT-Sicherheitsverantwortliche und Administratoren).
- Einbeziehung externer Expertise mit den Schwerpunkten Technologie, Qualitätssicherung und Moderation, falls dies notwendig ist.
- Pragmatische Umsetzung der Ergebnisse, nicht nur ein Festhalten an der erfolgten Dokumentation des Ist-Zustands. Hierbei sollte klar zwischen Ad-hoc-Maßnahmen, die sofort umgesetzt werden müssen, wenn ein kritischer Punkt identifiziert wurde, und den kontinuierlichen Maßnahmen unterschieden werden.
- Etablierung von kontinuierlichen Prozessen zur Sicherstellung der Informationssicherheit, d. h. Informationssicherheit als Prozess.

4 Die OCTAVE-Methode

Die Risikoanalysemethode OCTAVE vereint die eben aufgeführten Merkmale in sich. OCTAVE steht für „Operationally Critical Threat, Asset, and Vulnerability Evaluation“, was man am besten frei als „Bewertung operativ kritischer Werte, Bedrohungen und Schwachstellen“ übersetzen kann. Dieses Verfahren wurde an der Carnegie Mellon Universität in Zusammenarbeit mit dem CERT/CC entwickelt und unterstützt den Anwender mit Formblättern, Checklisten und Moderationsplänen bei der Durchführung einer Sicherheitsevaluation. Das DFN-CERT hat die umfangreichen Arbeitsblätter ins Deutsche übersetzt, gekürzt, an ISO 27001[2] angepasst und ein Software-Tool entwickelt.

Die OCTAVE Methode liefert als Ergebnis eine strategische Beurteilung und Planung für Informationssicherheit auf Basis einer Risikoanalyse. Dabei wird der Schwerpunkt auf eine betriebswirtschaftliche Analyse der Risiken und Sicherheitsprozesse gelegt, nicht auf eine technologische Basis.

OCTAVE ist grundsätzlich ein selbst gesteuerter Ansatz, mit dem die eigenen Mitarbeiter einer Organisation den Bedürfnissen für Informationssicherheit Rechnung tragen können.

[2] Internationaler Standard für die Etablierung eines Informationssicherheitsmanagementsystems (ISMS).

Die Umsetzung erfolgt durch ein bereichsübergreifendes Team, das allerdings überschaubar bleiben soll. Um eine wirksame Umsetzung zu realisieren, muss das Team eine gute Kenntnis von den Geschäfts- und Sicherheitsprozessen der Organisation besitzen. Das Team ist für die Durchführung verantwortlich und erhält hierfür ein explizites Mandat des Managements. Letztendlich wird basierend auf den spezifischen betriebswirtschaftlichen Risiken der Organisation eine Sicherheitsstrategie entwickelt.

5 Vorgehensweise bei der OCTAVE Methode

Bei der OCTAVE Methode werden die folgenden Phasen unterschieden (siehe auch Abbildung 1):

1. Vorbereitungsphase für die Teambildung und Zeitplanung
2. Ermittlung von Bedrohungsprofilen für Werte, die an Informationsverarbeitung und IT festzumachen sind
3. Identifizierung von Schwachstellen in der IT-Infrastruktur
4. Entwicklung der IT-Sicherheitsstrategie und deren Umsetzung

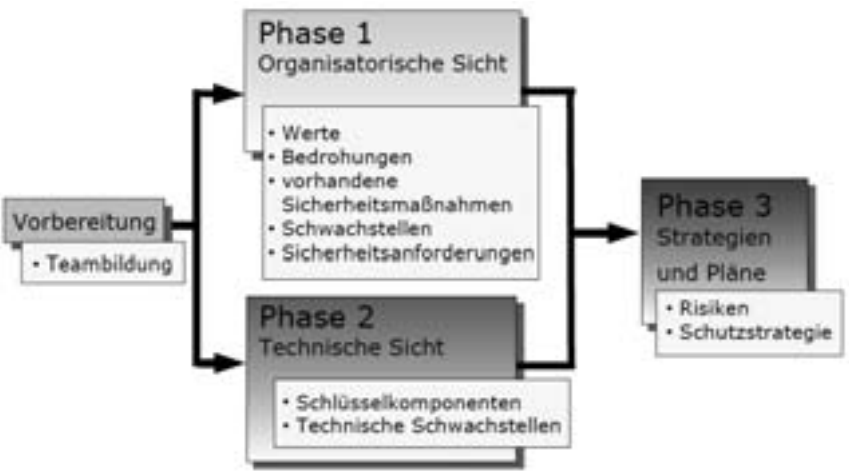


Abbildung 1: Überblick über die Phasen einer OCTAVE-Analyse

Diese Prozesse untergliedern sich, je nach Größe der Organisation, in fünf bis acht Schritte und weitere, nachgeordnete Aktivitäten. Dabei werden wichtige Werte[3] zu Objekten zu-

[3]Unter Werte werden hier nicht nur materielle Werte wie z. B. das Anlagevermögen verstanden, sondern ebenso immaterielle Werte wie Informationen und das Know-How der Mitarbeiter, welche neben den Produktionsmitteln ebenso Voraussetzung zur Erzeugung von Produkten oder zur Erbringung von Dienstleistungen sind.

sammengefasst. Ein Objekt kann dabei ein komplexes IT-System sein, wobei die technischen Einzelheiten (u. a. Server, Netzwerk, Arbeitsplätze) zunächst nicht im Vordergrund stehen. Allerdings werden auch Geschäftsprozesse, Verfahren oder Anweisungen als Objekte angesehen und behandelt, es geht also insgesamt um eine ganzheitliche Betrachtung.

5.1 Phase 1: Ermittlung von Bedrohungsprofilen für Werte, die an Informationsverarbeitung und IT festzumachen sind

Der Schwerpunkt der ersten Phase liegt in der Auswertung der organisatorischen Aspekte. Zunächst definiert das Team die Bewertungskriterien, die später verwendet werden, um Risiken zu beurteilen. Anschließend werden die wichtigen Werte identifiziert, in Objekten zusammengefasst und die aktuellen Sicherheitsmaßnahmen evaluiert.

Die Aufgaben werden allein vom Analyseteam durchgeführt, zusätzliche Informationen werden nur eingeholt, wenn es erforderlich ist. Aus den wichtigen Werten bzw. Geschäftsprozessen werden dann hinsichtlich ihrer Bedeutung für die Organisation drei bis fünf ausgewählt und dann im Detail analysiert. Zuletzt definiert das Team die Sicherheitsanforderungen und definiert ein Bedrohungsprofil für jeden kritischen Wert.

Die OCTAVE Methode wurde entwickelt, um den Einstieg in eine strategische Beurteilung und Planung von Informationssicherheit zu unterstützen. Dabei wird bewusst darauf verzichtet, bei der ersten Anwendung von OCTAVE alle Werte zu analysieren, dies muss im Rahmen des kontinuierlichen Sicherheitsprozesses nachgezogen werden. Wichtige Fragestellungen in dieser Phase sind:

- Welches sind die kritischen Werte?
- In welcher Beziehung stehen die Werte zueinander?
- Was sind die spezifischen Bedrohungen?
- Was wird bereits unternommen, um diese Werte zu schützen?

5.2 Phase 2: Identifizierung von Schwachstellen in der IT-Infrastruktur

Während dieser Phase erfasst das Analyseteam die IT-Infrastruktur, die in Bezug zu den kritischen Werten steht. Der Schwerpunkt liegt dabei auf den Sicherheitsmaßnahmen, die durch die Betreiber der Infrastruktur getroffen worden sind.

Das Analyseteam ermittelt zuerst, wie die Mitarbeiter die IT-Infrastruktur nutzen, wenn auf kritische Werte zugegriffen wird. Dies beinhaltet die Identifizierung der Schlüsselkomponenten und die für die Konfiguration und Betrieb verantwortlichen Personen. Abschließend wird analysiert, ob durch die verantwortlichen Personen Sicherheitsmaßnahmen technisch umgesetzt wurden.

- Wichtige Fragestellungen in dieser Phase sind:
- Wie greifen die Mitarbeiter auf die kritischen Werte zu?
- Welche Komponenten der technischen Infrastruktur sind den kritischen Werten zuzuordnen?
- Was sind die technischen Schwachstellen?

5.3 Phase 3: Entwicklung der Sicherheitsstrategie und deren Umsetzung

In der dritten Phase erfolgt eine Risikoanalyse auf Grundlage der vorangegangen Phase. Es werden die Schadenswirkungen und Eintrittswahrscheinlichkeiten der identifizierten Bedrohungen abgeschätzt. Darauf aufbauend wird eine Schutzstrategie für die kritischen Werte entwickelt. Anschließend werden geeignete Sicherheitsmaßnahmen ausgewählt und ein Umsetzungsplan erstellt. Wichtige Fragestellungen in dieser Phase sind:

- Was sind die Auswirkungen im Schadensfall?
- Welche Maßnahmen werden benötigt, um den Bedrohungen entgegenzuwirken?
- Welche Maßnahmen müssen unverzüglich / mittelfristig / langfristig ergriffen werden?
- Welche Veränderungen sind im Sicherheitsmanagement erforderlich, um die Informationssicherheit kontinuierlich sicher zu stellen?

Auch wenn OCTAVE lediglich zum Zweck der Risikoanalyse eingesetzt wird, erhält man durch die ermittelten und bewerteten Risiken eine übersichtliche Informationsbasis, mit der Fehlinvestitionen vermieden und Maßnahmen zielgerichtet umgesetzt werden können. In der letzten OCTAVE Phase wird zudem eine Strategie zur Unterstützung des zukünftigen Risikomanagements ausgearbeitet. Hiermit wird die wichtigste Grundlage für die Etablierung eines strategisch ausgerichteten Informationssicherheitsmanagements bereitgestellt.

GI-Edition Lecture Notes in Informatics

P-1 Gregor Engels, Andreas Oberweis, Albert Zündorf (Hrsg.): Modellierung 2001.

P-2 Mikhail Godlevsky, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications, ISTA'2001.

P-3 Ana M. Moreno, Reind P. van de Riet (Hrsg.): Applications of Natural Lan-guage to Information Systems, NLDB'2001.

P-4 H. Wörn, J. Mühling, C. Vahl, H.-P. Meinzer (Hrsg.): Rechner- und sensorgestützte Chirurgie; Workshop des SFB 414.

P-5 Andy Schürr (Hg.): OMER – Object-Oriented Modeling of Embedded Real-Time Systems.

P-6 Hans-Jürgen Appelrath, Rolf Beyer, Uwe Marquardt, Heinrich C. Mayr, Claudia Steinberger (Hrsg.): Unternehmen Hochschule, UH'2001.

P-7 Andy Evans, Robert France, Ana Moreira, Bernhard Rumpe (Hrsg.): Practical UML-Based Rigorous Development Methods – Countering or Integrating the extremists, pUML'2001.

P-8 Reinhard Keil-Slawik, Johannes Magenheim (Hrsg.): Informatikunterricht und Medienbildung, INFOS'2001.

P-9 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Innovative Anwendungen in Kommunikationsnetzen, 15. DFN Arbeitstagung.

P-10 Mirjam Minor, Steffen Staab (Hrsg.): 1st German Workshop on Experience Management: Sharing Experiences about the Sharing Experience.

P-11 Michael Weber, Frank Kargl (Hrsg.): Mobile Ad-Hoc Netzwerke, WMAN 2002.

P-12 Martin Glinz, Günther Müller-Luschnat (Hrsg.): Modellierung 2002.

P-13 Jan von Knop, Peter Schirmbacher and Viljan Mahni_ (Hrsg.): The Changing Universities – The Role of Technology.

P-14 Robert Tolksdorf, Rainer Eckstein (Hrsg.): XML-Technologien für das Semantic Web – XSW 2002.

P-15 Hans-Bernd Bludau, Andreas Koop (Hrsg.): Mobile Computing in Medicine.

P-16 J. Felix Hampe, Gerhard Schwabe (Hrsg.): Mobile and Collaborative Business 2002.

P-17 Jan von Knop, Wilhelm Haverkamp (Hrsg.): Zukunft der Netze –Die Verletzbarkeit meistern, 16. DFN Arbeitstagung.

P-18 Elmar J. Sinz, Markus Plaha (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2002.

P-19 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund.

P-20 Sigrid Schubert, Bernd Reusch, Norbert Jesse (Hrsg.): Informatik bewegt – Informatik 2002 – 32. Jahrestagung der Gesellschaft für Informatik e.V. (GI) 30.Sept.-3. Okt. 2002 in Dortmund (Ergänzungsband).

P-21 Jörg Desel, Mathias Weske (Hrsg.): Promise 2002: Prozessorientierte Methoden und Werkzeuge für die Entwicklung von Informationssystemen.

P-22 Sigrid Schubert, Johannes Magenheim, Peter Hubwieser, Torsten Brinda (Hrsg.): Forschungsbeiträge zur "Didaktik der Informatik" – Theorie, Praxis, Evaluation.

P-23 Thorsten Spitta, Jens Borchers, Harry M. Sneed (Hrsg.): Software Management 2002 – Fortschritt durch Beständigkeit

P-24 Rainer Eckstein, Robert Tolksdorf (Hrsg.): XMIDX 2003 – XML-Technologien für Middleware – Middleware für XML-Anwendungen

P-25 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Commerce – Anwendungen und Perspektiven – 3. Workshop Mobile Commerce, Universität Augsburg, 04.02.2003

P-26 Gerhard Weikum, Harald Schöning, Erhard Rahm (Hrsg.): BTW 2003: Datenbanksysteme für Business, Technologie und Web

P-27 Michael Kroll, Hans-Gerd Lipinski, Kay Melzer (Hrsg.): Mobiles Computing in der Medizin

P-28 Ulrich Reimer, Andreas Abecker, Steffen Staab, Gerd Stumme (Hrsg.): WM 2003: Professionelles Wissensmanagement – Er-fahrungen und Visionen

P-29 Antje Düsterhöft, Bernhard Thalheim (Eds.): NLDB'2003: Natural Language Processing and Information Systems

P-30 Mikhail Godlevsky, Stephen Liddle, Heinrich C. Mayr (Eds.): Information Systems Technology and its Applications

P-31 Arslan Brömme, Christoph Busch (Eds.): BIOSIG 2003: Biometrics and Electronic Signatures

P-32 Peter Hubwieser (Hrsg.): Informatische Fachkonzepte im Unterricht – INFOS 2003

P-33 Andreas Geyer-Schulz, Alfred Taudes (Hrsg.): Informationswirtschaft: Ein Sektor mit Zukunft

P-34 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 1)

P-35 Klaus Dittrich, Wolfgang König, Andreas Oberweis, Kai Rannenberg, Wolfgang Wahlster (Hrsg.): Informatik 2003 – Innovative Informatikanwendungen (Band 2)

P-36 Rüdiger Grimm, Hubert B. Keller, Kai Rannenberg (Hrsg.): Informatik 2003 – Mit Sicherheit Informatik

P-37 Arndt Bode, Jörg Desel, Sabine Rathmayer, Martin Wessner (Hrsg.): DeLFI 2003: e-Learning Fachtagung Informatik

P-38 E.J. Sinz, M. Plaha, P. Neckel (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2003

P-39 Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.): IT-Incident Management & IT-Forensics – IMF 2003

P-40 Michael Rebstock (Hrsg.): Modellierung betrieblicher Informationssysteme – MobIS 2004

P-41 Uwe Brinkschulte, Jürgen Becker, Dietmar Fey, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle, Thomas Runkler (Edts.): ARCS 2004 – Organic and Pervasive Computing

P-42 Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Economy – Transaktionen und Prozesse, Anwendungen und Dienste

P-43 Birgitta König-Ries, Michael Klein, Philipp Obreiter (Hrsg.): Persistance, Scalability, Transactions – Database Mechanisms for Mobile Applications

P-44 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): Security, E-Learning. E-Services

P-45 Bernhard Rumpe, Wofgang Hesse (Hrsg.): Modellierung 2004

P-46 Ulrich Flegel, Michael Meier (Hrsg.): Detection of Intrusions of Malware & Vulnerability Assessment

P-47 Alexander Prosser, Robert Krimmer (Hrsg.): Electronic Voting in Europe – Technology, Law, Politics and Society

P-48 Anatoly Doroshenko, Terry Halpin, Stephen W. Liddle, Heinrich C. Mayr (Hrsg.): Information Systems Technology and its Applications

P-49 G. Schiefer, P. Wagner, M. Morgenstern, U. Rickert (Hrsg.): Integration und Datensicherheit – Anforderungen, Konflikte und Perspektiven

P-50 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 1) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-51 Peter Dadam, Manfred Reichert (Hrsg.): INFORMATIK 2004 – Informatik verbindet (Band 2) Beiträge der 34. Jahrestagung der Gesellschaft für Informatik e.V. (GI), 20.-24. September 2004 in Ulm

P-52 Gregor Engels, Silke Seehusen (Hrsg.): DELFI 2004 – Tagungsband der 2. e-Learning Fachtagung Informatik

P-53 Robert Giegerich, Jens Stoye (Hrsg.): German Conference on Bioinformatics – GCB 2004

P-54 Jens Borchers, Ralf Kneuper (Hrsg.): Softwaremanagement 2004 – Outsourcing und Integration

P-55 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): E-Science und Grid Adhoc-Netze Medienintegration

P-56 Fernand Feltz, Andreas Oberweis, Benoit Otjacques (Hrsg.): EMISA 2004 – Informationssysteme im E-Business und E-Government

P-57 Klaus Turowski (Hrsg.): Architekturen, Komponenten, Anwendungen

P-58 Sami Beydeda, Volker Gruhn, Johannes Mayer, Ralf Reussner, Franz Schweiggert (Hrsg.): Testing of Component-Based Systems and Software Quality

P-59 J. Felix Hampe, Franz Lehner, Key Pousttchi, Kai Ranneberg, Klaus Turowski (Hrsg.): Mobile Business – Processes, Platforms, Payments

P-60 Steffen Friedrich (Hrsg.): Unterrichtskonzepte für inforrmatische Bildung

P-61 Paul Müller, Reinhard Gotzhein, Jens B. Schmitt (Hrsg.): Kommunikation in verteilten Systemen

P-62 Federrath, Hannes (Hrsg.): „Sicherheit 2005“ – Sicherheit – Schutz und Zuverlässigkeit

P-63 Roland Kaschek, Heinrich C. Mayr, Stephen Liddle (Hrsg.): Information Systems – Technology and ist Applications

P-64 Peter Liggesmeyer, Klaus Pohl, Michael Goedicke (Hrsg.): Software Engineering 2005

P-65 Gottfried Vossen, Frank Leymann, Peter Lockemann, Wolffried Stucky (Hrsg.): Datenbanksysteme in Business, Technologie und Web

P-66 Jörg M. Haake, Ulrike Lucke, Djamshid Tavangarian (Hrsg.): DeLFI 2005: 3. deutsche e-Learning Fachtagung Informatik

P-67 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 1)

P-68 Armin B. Cremers, Rainer Manthey, Peter Martini, Volker Steinhage (Hrsg.): INFORMATIK 2005 – Informatik LIVE (Band 2)

P-69 Robert Hirschfeld, Ryszard Kowalcyk, Andreas Polze, Matthias Weske (Hrsg.): NODe 2005, GSEM 2005

P-70 Klaus Turowski, Johannes-Maria Zaha (Hrsg.): Component-oriented Enterprise Application (COAE 2005)

P-71 Andrew Torda, Stefan Kurz, Matthias Rarey (Hrsg.): German Conference on Bioinformatics 2005

P-72 Klaus P. Jantke, Klaus-Peter Fähnrich, Wolfgang S. Wittig (Hrsg.): Marktplatz Internet: Von e-Learning bis e-Payment

P-73 Jan von Knop, Wilhelm Haverkamp, Eike Jessen (Hrsg.): “Heute schon das Morgen sehen“

P-74 Christopher Wolf, Stefan Lucks, Po-Wah Yau (Hrsg.): WEWoRC 2005 – Western European Workshop on Research in Cryptology

P-75 Jörg Desel, Ulrich Frank (Hrsg.): Enterprise Modelling and Information Systems Architecture

P-76 Thomas Kirste, Birgitta König-Riess, Key Pousttchi, Klaus Turowski (Hrsg.): Mobile Informationssysteme – Potentiale, Hindernisse, Einsatz

P-77 Jana Dittmann (Hrsg.): SICHERHEIT 2006

P-78 K.-O. Wenkel, P. Wagner, M. Morgenstern, K. Luzi, P. Eisermann (Hrsg.): Land- und Ernährungswirtschaft im Wandel

P-79 Bettina Biel, Matthias Book, Volker Gruhn (Hrsg.): Softwareengineering 2006

P-80 Mareike Schoop, Christian Huemer, Michael Rebstock, Martin Bichler (Hrsg.): Service-Oriented Electronic Commerce

P-81 Wolfgang Karl, Jürgen Becker, Karl-Erwin Großpietsch, Christian Hochberger, Erik Maehle (Hrsg.): ARCS´06

P-82 Heinrich C. Mayr, Ruth Breu (Hrsg.): Modellierung 2006

P-83 Daniel Huson, Oliver Kohlbacher, Andrei Lupas, Kay Nieselt and Andreas Zell (eds.): German Conference on Bioinformatics

P-84 Dimitris Karagiannis, Heinrich C. Mayr, (Hrsg.): Information Systems Technology and its Applications

P-85 Witold Abramowicz, Heinrich C. Mayr, (Hrsg.): Business Information Systems

P-86 Robert Krimmer (Ed.): Electronic Voting 2006

P-87 Max Mühlhäuser, Guido Rößling, Ralf Steinmetz (Hrsg.): DELFI 2006: 4. e-Learning Fachtagung Informatik

P-88 Robert Hirschfeld, Andreas Polze, Ryszard Kowalczyk (Hrsg.): NODe 2006, GSEM 2006

P-90 Joachim Schelp, Robert Winter, Ulrich Frank, Bodo Rieger, Klaus Turowski (Hrsg.): Integration, Informationslogistik und Architektur

P-91 Henrik Stormer, Andreas Meier, Michael Schumacher (Eds.): European Conference on eHealth 2006

P-92 Fernand Feltz, Benoît Otjacques, Andreas Oberweis, Nicolas Poussing (Eds.): AIM 2006

P-93 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 1

P-94 Christian Hochberger, Rüdiger Liskowsky (Eds.): INFORMATIK 2006 – Informatik für Menschen, Band 2

P-95 Matthias Weske, Markus Nüttgens (Eds.): EMISA 2005: Methoden, Konzepte und Technologien für die Entwicklung von dienstbasierten Informationssystemen

P-96 Saartje Brockmans, Jürgen Jung, York Sure (Eds.): Meta-Modelling and Ontologies

P-97 Oliver Göbel, Dirk Schadt, Sandra Frings, Hardo Hase, Detlef Günther, Jens Nedon (Eds.): IT-Incident Mangament & IT-Forensics – IMF 2006

P-98 Hans Brandt-Pook, Werner Simonsmeier und Thorsten Spitta (Hrsg.): Beratung in der Softwareentwicklung – Modelle, Methoden, Best Practices

P-99 Andreas Schwill, Carsten Schulte, Marco Thomas (Hrsg.): Didaktik der Informatik

P-100 Peter Forbrig, Günter Siegel, Markus Schneider (Hrsg.): HDI 2006: Hochschuldidaktik der Informatik

P-101 Stefan Böttinger, Ludwig Theuvsen, Susanne Rank, Marlies Morgenstern (Hrsg.): Agrarinformatik im Spannungsfeld zwischen Regionalisierung und globalen Wertschöpfungsketten

P-102 Otto Spaniol (Eds.): Mobile Services and Personalized Environments

P-103 Alfons Kemper, Harald Schöning, Thomas Rose, Matthias Jarke, Thomas Seidl, Christoph Quix, Christoph Brochhaus (Hrsg.): Datenbanksysteme in Business, Technologie und Web (BTW 2007)

P-104 Birgitta König-Ries, Franz Lehner, Rainer Malaka, Can Türker (Hrsg.) MMS 2007: Mobilität und mobile Informationssysteme

P-105 Wolf-Gideon Bleek, Jörg Raasch, Heinz Züllighoven (Hrsg.) Software Engineering 2007

P-106 Wolf-Gideon Bleek, Henning Schwentner, Heinz Züllighoven (Hrsg.) Software Engineering 2007 – Beiträge zu den Workshops

P-107 Heinrich C. Mayr, Dimitris Karagiannis (eds.) Information Systems Technology and its Applications

P-108 Arslan Brömme, Christoph Busch, Detlef Hühnlein (eds.) BIOSIG 2007: Biometrics and Electronic Signatures

P-109 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 1

P-110 Rainer Koschke, Otthein Herzog, Karl-Heinz Rödiger, Marc Ronthaler (Hrsg.) INFORMATIK 2007 Informatik trifft Logistik Band 2

P-111 Christian Eibl, Johannes Magenheim, Sigrid Schubert, Martin Wessner (Hrsg.) DeLFI 2007: 5. e-Learning Fachtagung Informatik

P-112 Sigrid Schubert (Hrsg.) Didaktik der Informatik in Theorie und Praxis

P-113 Sören Auer, Christian Bizer, Claudia Müller, Anna V. Zhdanova (Eds.) The Social Semantic Web 2007 Proceedings of the 1st Conference on Social Semantic Web (CSSW)

P-114 Sandra Frings, Oliver Göbel, Detlef Günther, Hardo G. Hase, Jens Nedon, Dirk Schadt, Arslan Brömme (Eds.) IMF2007 IT-incident management & IT-forensics Proceedings of the 3rd International Conference on IT-Incident Management & IT-Forensics

P-115 Claudia Falter, Alexander Schliep, Joachim Selbig, Martin Vingron and Dirk Walther (Eds.) German conference on bioinformatics GCB 2007

P-116 Witold Abramowicz, Leszek Maciszek (Eds.) Business Process and Services Computing 1st International Working Conference on Business Process and Services Computing BPSC 2007

P-117 Ryszard Kowalczyk (Ed.) Grid service engineering and manegement The 4th International Conference on Grid Service Engineering and Management GSEM 2007

P-118 Andreas Hein, Wilfried Thoben, Hans-Jürgen Appelrath, Peter Jensch (Eds.) European Conference on ehealth 2007

P-119 Manfred Reichert, Stefan Strecker, Klaus Turowski (Eds.) Enterprise Modelling and Information Systems Architectures Concepts and Applications

P-120 Adam Pawlak, Kurt Sandkuhl, Wojciech Cholewa, Leandro Soares Indrusiak (Eds.) Coordination of Collaborative Engineering - State of the Art and Future Challenges

P-121 Korbinian Herrmann, Bernd Bruegge (Hrsg.) Software Engineering 2008 Fachtagung des GI-Fachbereichs Softwaretechnik

P-122 Walid Maalej, Bernd Bruegge (Hrsg.) Software Engineering 2008 - Workshopband Fachtagung des GI-Fachbereichs Softwaretechnik

P-123 Michael H. Breitner, Martin Breunig, Elgar Fleisch, Ley Pousttchi, Klaus Turowski (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Technologien, Prozesse, Marktfähigkeit
Proceedings zur 3. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2008)

P-124 Wolfgang E. Nagel, Rolf Hoffmann, Andreas Koch (Eds.)
9th Workshop on Parallel Systems and Algorithms (PASA)
Workshop of the GI/ITG Speciel Interest Groups PARS and PARVA

P-125 Rolf A.E. Müller, Hans-H. Sundermeier, Ludwig Theuvsen, Stephanie Schütze, Marlies Morgenstern (Hrsg.)
Unternehmens-IT:
Führungsinstrument oder Verwaltungsbürde
Referate der 28. GIL Jahrestagung

P-126 Rainer Gimnich, Uwe Kaiser, Jochen Quante, Andreas Winter (Hrsg.)
10th Workshop Software Reengineering (WSR 2008)

P-127 Thomas Kühne, Wolfgang Reisig, Friedrich Steimann (Hrsg.)
Modellierung 2008

P-128 Ammar Alkassar, Jörg Siekmann (Hrsg.)
Sicherheit 2008
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 4. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)
2.-4. April 2008
Saarbrücken, Germany

P-129 Wolfgang Hesse, Andreas Oberweis (Eds.)
Sigsand-Europe 2008
Proceedings of the Third AIS SIGSAND European Symposium on Analysis, Design, Use and Societal Impact of Information Systems

P-130 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
1. DFN-Forum Kommunikations-technologien Beiträge der Fachtagung

P-131 Robert Krimmer, Rüdiger Grimm (Eds.)
3rd International Conference on Electronic Voting 2008
Co-organized by Council of Europe, Gesellschaft für Informatik and E-Voting. CC

P-132 Silke Seehusen, Ulrike Lucke, Stefan Fischer (Hrsg.)
DeLFI 2008:
Die 6. e-Learning Fachtagung Informatik

P-133 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 1

P-134 Heinz-Gerd Hegering, Axel Lehmann, Hans Jürgen Ohlbach, Christian Scheideler (Hrsg.)
INFORMATIK 2008
Beherrschbare Systeme – dank Informatik
Band 2

P-135 Torsten Brinda, Michael Fothe, Peter Hubwieser, Kirsten Schlüter (Hrsg.)
Didaktik der Informatik –
Aktuelle Forschungsergebnisse

P-136 Andreas Beyer, Michael Schroeder (Eds.)
German Conference on Bioinformatics GCB 2008

P-137 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2008: Biometrics and Electronic Signatures

P-138 Barbara Dinter, Robert Winter, Peter Chamoni, Norbert Gronau, Klaus Turowski (Hrsg.)
Synergien durch Integration und Informationslogistik
Proceedings zur DW2008

P-139 Georg Herzwurm, Martin Mikusz (Hrsg.)
Industrialisierung des Software-Managements
Fachtagung des GI-Fachausschusses Management der Anwendungsentwick-lung und -wartung im Fachbereich Wirtschaftsinformatik

P-140 Oliver Göbel, Sandra Frings, Detlef Günther, Jens Nedon, Dirk Schadt (Eds.)
IMF 2008 - IT Incident Management & IT Forensics

P-141 Peter Loos, Markus Nüttgens, Klaus Turowski, Dirk Werth (Hrsg.)
Modellierung betrieblicher Informations-systeme (MobIS 2008)
Modellierung zwischen SOA und Compliance Management

P-142 R. Bill, P. Korduan, L. Theuvsen, M. Morgenstern (Hrsg.)
Anforderungen an die Agrarinformatik durch Globalisierung und Klimaveränderung

P-143 Peter Liggesmeyer, Gregor Engels, Jürgen Münch, Jörg Dörr, Norman Riegel (Hrsg.)
Software Engineering 2009
Fachtagung des GI-Fachbereichs Softwaretechnik

P-144 Johann-Christoph Freytag, Thomas Ruf, Wolfgang Lehner, Gottfried Vossen (Hrsg.)
Datenbanksysteme in Business, Technologie und Web (BTW)

P-145 Knut Hinkelmann, Holger Wache (Eds.)
WM2009: 5th Conference on Professional Knowledge Management

P-146 Markus Bick, Martin Breunig, Hagen Höpfner (Hrsg.)
Mobile und Ubiquitäre Informationssysteme – Entwicklung, Implementierung und Anwendung
4. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2009)

P-147 Witold Abramowicz, Leszek Maciaszek, Ryszard Kowalczyk, Andreas Speck (Eds.)
Business Process, Services Computing and Intelligent Service Management
BPSC 2009 · ISM 2009 · YRW-MBP 2009

P-148 Christian Erfurth, Gerald Eichler, Volkmar Schau (Eds.)
9th International Conference on Innovative Internet Community Systems
I^{2}CS 2009

P-149 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
2. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-150 Jürgen Münch, Peter Liggesmeyer (Hrsg.)
Software Engineering
2009 - Workshopband

P-151 Armin Heinzl, Peter Dadam, Stefan Kirn, Peter Lockemann (Eds.)
PRIMIUM
Process Innovation for Enterprise Software

P-152 Jan Mendling, Stefanie Rinderle-Ma, Werner Esswein (Eds.)
Enterprise Modelling and Information Systems Architectures
Proceedings of the 3rd Int'l Workshop EMISA 2009

P-153 Andreas Schwill, Nicolas Apostolopoulos (Hrsg.)
Lernen im Digitalen Zeitalter
DeLFI 2009 – Die 7. E-Learning Fachtagung Informatik

P-154 Stefan Fischer, Erik Maehle Rüdiger Reischuk (Hrsg.)
INFORMATIK 2009
Im Focus das Leben

P-155 Arslan Brömme, Christoph Busch, Detlef Hühnlein (Eds.)
BIOSIG 2009:
Biometrics and Electronic Signatures
Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-156 Bernhard Koerber (Hrsg.)
Zukunft braucht Herkunft
25 Jahre »INFOS – Informatik und Schule«

P-157 Ivo Grosse, Steffen Neumann, Stefan Posch, Falk Schreiber, Peter Stadler (Eds.)
German Conference on Bioinformatics 2009

P-158 W. Claupein, L. Theuvsen, A. Kämpf, M. Morgenstern (Hrsg.)
Precision Agriculture Reloaded – Informationsgestützte Landwirtschaft

P-159 Gregor Engels, Markus Luckey, Wilhelm Schäfer (Hrsg.)
Software Engineering 2010

P-160 Gregor Engels, Markus Luckey, Alexander Pretschner, Ralf Reussner (Hrsg.)
Software Engineering 2010 – Workshopband
(inkl. Doktorandensymposium)

P-161 Gregor Engels, Dimitris Karagiannis Heinrich C. Mayr (Hrsg.)
Modellierung 2010

P-162 Maria A. Wimmer, Uwe Brinkhoff, Siegfried Kaiser, Dagmar Lück-Schneider, Erich Schweighofer, Andreas Wiebe (Hrsg.)
Vernetzte IT für einen effektiven Staat
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2010

P-163 Markus Bick, Stefan Eulgem, Elgar Fleisch, J. Felix Hampe, Birgitta König-Ries, Franz Lehner, Key Pousttchi, Kai Rannenberg (Hrsg.)
Mobile und Ubiquitäre Informationssysteme
Technologien, Anwendungen und Dienste zur Unterstützung von mobiler Kollaboration

P-164 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2010: Biometrics and Electronic Signatures Proceedings of the Special Interest Group on Biometrics and Electronic Signatures

P-165 Gerald Eichler, Peter Kropf, Ulrike Lechner, Phayung Meesad, Herwig Unger (Eds.)
10th International Conference on Innovative Internet Community Systems (I^2CS) – Jubilee Edition 2010 –

P-166 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
3. DFN-Forum Kommunikationstechnologien
Beiträge der Fachtagung

P-167 Robert Krimmer, Rüdiger Grimm (Eds.)
4th International Conference on Electronic Voting 2010
co-organized by the Council of Europe, Gesellschaft für Informatik and E-Voting.CC

P-168 Ira Diethelm, Christina Dörge, Claudia Hildebrandt, Carsten Schulte (Hrsg.)
Didaktik der Informatik
Möglichkeiten empirischer Forschungsmethoden und Perspektiven der Fachdidaktik

P-169 Michael Kerres, Nadine Ojstersek Ulrik Schroeder, Ulrich Hoppe (Hrsg.)
DeLFI 2010 - 8. Tagung der Fachgruppe E-Learning der Gesellschaft für Informatik e.V.

P-170 Felix C. Freiling (Hrsg.)
Sicherheit 2010
Sicherheit, Schutz und Zuverlässigkeit

P-171 Werner Esswein, Klaus Turowski, Martin Juhrisch (Hrsg.)
Modellierung betrieblicher Informationssysteme (MobIS 2010)
Modellgestütztes Management

P-172 Stefan Klink, Agnes Koschmider Marco Mevius, Andreas Oberweis (Hrsg.)
EMISA 2010
Einflussfaktoren auf die Entwicklung flexibler, integrierter Informationssysteme
Beiträge des Workshops der GI-Fachgruppe EMISA (Entwicklungsmethoden für Informationssysteme und deren Anwendung)

P-173 Dietmar Schomburg, Andreas Grote (Eds.)
German Conference on Bioinformatics 2010

P-174 Arslan Brömme, Torsten Eymann, Detlef Hühnlein, Heiko Roßnagel, Paul Schmücker (Hrsg.)
perspeGKtive 2010
Workshop „Innovative und sichere Informationstechnologie für das Gesundheitswesen von morgen“

P-175 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 1

P-176 Klaus-Peter Fähnrich, Bogdan Franczyk (Hrsg.)
INFORMATIK 2010
Service Science – Neue Perspektiven für die Informatik
Band 2

P-177 Witold Abramowicz, Rainer Alt, Klaus-Peter Fähnrich, Bogdan Franczyk, Leszek A. Maciaszek (Eds.)
INFORMATIK 2010
Business Process and Service Science – Proceedings of ISSS and BPSC

P-178 Wolfram Pietsch, Benedikt Krams (Hrsg.)
Vom Projekt zum Produkt
Fachtagung des GI-Fachausschusses Management der Anwendungsentwicklung und -wartung im Fachbereich Wirtschafts-informatik (WI-MAW), Aachen, 2010

P-179 Stefan Gruner, Bernhard Rumpe (Eds.)
FM+AM`2010
Second International Workshop on Formal Methods and Agile Methods

P-180 Theo Härder, Wolfgang Lehner, Bernhard Mitschang, Harald Schöning, Holger Schwarz (Hrsg.)
Datenbanksysteme für Business, Technologie und Web (BTW)
14. Fachtagung des GI-Fachbereichs „Datenbanken und Informationssysteme“ (DBIS)

P-181 Michael Clasen, Otto Schätzel, Brigitte Theuvsen (Hrsg.)
Qualität und Effizienz durch informationsgestützte Landwirtschaft, Fokus: Moderne Weinwirtschaft

P-182 Ronald Maier (Hrsg.)
6th Conference on Professional Knowledge Management
From Knowledge to Action

P-183 Ralf Reussner, Matthias Grund, Andreas Oberweis, Walter Tichy (Hrsg.)
Software Engineering 2011
Fachtagung des GI-Fachbereichs Softwaretechnik

P-184 Ralf Reussner, Alexander Pretschner, Stefan Jähnichen (Hrsg.)
Software Engineering 2011
Workshopband
(inkl. Doktorandensymposium)

P-185 Hagen Höpfner, Günther Specht, Thomas Ritz, Christian Bunse (Hrsg.)
MMS 2011: Mobile und ubiquitäre Informationssysteme Proceedings zur 6. Konferenz Mobile und Ubiquitäre Informationssysteme (MMS 2011)

P-186 Gerald Eichler, Axel Küpper, Volkmar Schau, Hacène Fouchal, Herwig Unger (Eds.)
11th International Conference on Innovative Internet Community Systems (I^2CS)

P-187 Paul Müller, Bernhard Neumair, Gabi Dreo Rodosek (Hrsg.)
4. DFN-Forum Kommunikations-technologien, Beiträge der Fachtagung 20. Juni bis 21. Juni 2011 Bonn

P-188 Holger Rohland, Andrea Kienle, Steffen Friedrich (Hrsg.)
DeLFI 2011 – Die 9. e-Learning Fachtagung Informatik
der Gesellschaft für Informatik e.V. 5.–8. September 2011, Dresden

P-189 Thomas, Marco (Hrsg.)
Informatik in Bildung und Beruf
INFOS 2011
14. GI-Fachtagung Informatik und Schule

P-190 Markus Nüttgens, Oliver Thomas, Barbara Weber (Eds.)
Enterprise Modelling and Information Systems Architectures (EMISA 2011)

P-191 Arslan Brömme, Christoph Busch (Eds.)
BIOSIG 2011
International Conference of the Biometrics Special Interest Group

P-192 Hans-Ulrich Heiß, Peter Pepper, Holger Schlingloff, Jörg Schneider (Hrsg.)
INFORMATIK 2011
Informatik schafft Communities

P-193 Wolfgang Lehner, Gunther Piller (Hrsg.)
IMDM 2011

P-194 M. Clasen, G. Fröhlich, H. Bernhardt, K. Hildebrand, B. Theuvsen (Hrsg.)
Informationstechnologie für eine nachhaltige Landbewirtschaftung
Fokus Forstwirtschaft

P-195 Neeraj Suri, Michael Waidner (Hrsg.)
Sicherheit 2012
Sicherheit, Schutz und Zuverlässigkeit
Beiträge der 6. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI)

P-197 Jörn von Lucke, Christian P. Geiger, Siegfried Kaiser, Erich Schweighofer, Maria A. Wimmer (Hrsg.)
Auf dem Weg zu einer offenen, smarten und vernetzten Verwaltungskultur
Gemeinsame Fachtagung Verwaltungsinformatik (FTVI) und Fachtagung Rechtsinformatik (FTRI) 2012

P-198 Stefan Jähnichen, Axel Küpper, Sahin Albayrak (Hrsg.)
Software Engineering 2012
Fachtagung des GI-Fachbereichs Softwaretechnik

P-199 Stefan Jähnichen, Bernhard Rumpe, Holger Schlingloff (Hrsg.)
Software Engineering 2012
Workshopband

P-200 Gero Mühl, Jan Richling, Andreas Herkersdorf (Hrsg.)
ARCS 2012 Workshops

P-201 Elmar J. Sinz Andy Schürr (Hrsg.)
Modellierung 2012

P-202 Andrea Back, Markus Bick, Martin Breunig, Key Pousttchi, Frédéric Thiesse (Hrsg.)
MMS 2012:Mobile und Ubiquitäre Informationssysteme

P-203 Paul Müller, Bernhard Neumair, Helmut Reiser, Gabi Dreo Rodosek (Hrsg.)
5. DFN-Forum Kommunikations-technologien
Beiträge der Fachtagung

The titles can be purchased at:

Köllen Druck + Verlag GmbH
Ernst-Robert-Curtius-Str. 14 · D-53117 Bonn
Fax: +49 (0)228/9898222
E-Mail: druckverlag@koellen.de