Jens Nedon, Sandra Frings, Oliver Göbel (Hrsg.)

IT-Incident Management & IT-Forensics

Erste Tagung der Fachgruppe SIDAR der Gesellschaft für Informatik

24. – 25. November 2003 in Stuttgart, Deutschland

Gesellschaft für Informatik 2003

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

Volume P-39

ISBN 3-88579-368-7
ISSN 1617-5468

Volume Editors
Jens Nedon
ConSecur GmbH
Schulze-Delitzsch-Strasse 2, D-49716 Meppen
Nedon@consecur.de
Sandra Frings
Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO
Nobelstraße 12, D-70569 Stuttgart
Sandra.Frings@iao.fhg.de
Oliver Göbel
RUS-CERT (Universität Stuttgart)
Breitscheidstr. 2, D-70174 Stuttgart
Goebel@CERT.Uni-Stuttgart.DE

printed by Köllen Druck+Verlag GmbH, Bonn

Informationslogistische Ansätze für CERTs

Caroline Neufert[1], Dr. Christoph Thiel[2]

[1)] BearingPoint GmbH
Kurfürstendamm 207-208
D-10719 Berlin
Caroline.Neufert@bearingpoint.com

[2)] Abteilungsleiter Sicherheits-Management
Fraunhofer Institut für Software- und Systemtechnik
Mollstraße 1
D-10178 Berlin
Christoph.Thiel@isst.fhg.de

Abstract: Die Informationslogistik erforscht intelligente Systeme zur bedarfsgerechten Informationsversorgung. Die Anwender erwarten die richtigen Informationen zur richtigen Zeit am richtigen Ort in einer geeigneten Präsentation. In diesem Papier beschreiben wir ein informationslogistisches Framework, mit dessen Hilfe informationslogistische Anwendungen und insbesondere die Informationsversorgung eines CERT effektiv modelliert und implementiert werden können.

1 Einleitung

So unterschiedlich Naturkatastrophen oder Angriffe gegen IT-Infrastrukturen auch erscheinen und so verschieden ihre direkten oder indirekten Auswirkungen sein können, so offensichtlich haben sie auch vieles gemeinsam: So kann man durch Vorsorgemaßnahmen weder ihr Eintreten noch mögliche Schäden vollständig verhindern. Zudem lassen sich diese Ereignisse, ihre Größenordnung, Intensität und Schadenshöhe - wenn überhaupt - nur sehr ungenau und kurzfristig vorhersagen. Ferner können mögliche Betroffene und Helfer nur dann Schaden von sich und anderen abwehren, wenn sie möglichst frühzeitig über alle für sie relevanten Informationen zu drohenden oder eingetretenen Gefahren verfügen und so eine größtmögliche Vorbereitungszeit und Handlungsfreiräume gewinnen.

Fragestellungen, die sich bezüglich der dazu notwendigen Informationsversorgung ergeben, wurden in den letzten Jahren intensiv untersucht. Schwerpunkte dieser Arbeiten waren die Auswahl des richtigen Informationsinhalts ([OSE95, Y00]), die rechtzeitige Bereitstellung von Informationen ([K99]), die Quality-of-Service von Informationsdienstleistungen ([HB99]), die Ortsabhängigkeit von Informationen ([JD99, 11]) oder die Kombination von Inhaltsauswahl und Ortsabhängigkeit ([L91]) oder von Inhaltsauswahl und rechtzeitiger Informationsbereitstellung ([B96]).

Aus unserer Sicht müssen in den meisten Szenarien alle zuvor genannten Schwerpunkte gemeinsam berücksichtigt werden, d.h. die Informationsversorgung muss durch eine zielgerichtete Bereitstellung und bedarfsgerechte Zustellung von Informationen dahingehend optimiert sein, dass die inhaltlich richtigen Informationen zum Zeitpunkt des Bedarfs und an dem Ort, wo sie benötigt werden, vorliegen. Die Entwicklung und die Untersuchung entsprechender Konzepte und Lösungen sind Gegenstand der *Informationslogistik* ([DL01]).

Im Folgenden untersuchen wir Anforderungen an die Informationsversorgung durch *Warn- und Frühwarnzentralen*, insbesondere durch *Computer Emergency Response Teams (CERTs)*. Wir beschreiben zunächst ein ideales Anwendungsszenario, erklären wie solche Anforderungen in informationslogistischen Systemen umgesetzt werden können und skizzieren eine komponentenbasierte Systemarchitektur, die eine effiziente und kostengünstige Realisierung CERT ermöglicht. Dabei nutzen wir insbesondere Erfahrungen, die wir bei der Konzeption und dem Aufbau von Warn- und Frühwarnzentralen aus den Bereichen Unwetter- und Hochwasserschutz gewonnen haben ([JPTS03]).

2 Informationslogistische Komponenten eines CERT

Zur Erläuterung der idealen Nutzung und Arbeitsweise eines CERT beschreiben wir zunächst ein idealtypisches Anwendungsbeispiel eines CERT: In der Firma Klein & Mittel GmbH wird der für den Internet-Zugang verantwortliche IT-Administrator durch eine SMS des von ihm genutzten CERTs auf seinem Mobiltelefon über eine Sicherheitslücke in einem bestimmten Betriebssystem informiert. Da dies unter anderem einen im Internet exponierten Server betrifft und die Lücke von außen kompromittiert werden kann, ist der Alarm hoch priorisiert. Die Wartung dieses Servers ist an einen Dienstleister vergeben, der ebenfalls direkt informiert wurde. Vom Dienstleister wird entsprechend dem vereinbarten Service Level Agreement (SLA) kurz darauf die Behebung der Schwachstelle bestätigt. Der IT-Administrator installiert inzwischen nach der Anleitung aus der per E-Mail zugestellten Alarm-Meldung schon die notwendige Software auf seinen lokalen Servern, wobei hier durch den Schutz der Firewall die Dringlichkeit nicht so hoch ist. Dabei werden zusätzlich auch Sicherheitssysteme wie die Firewall und das Intrusion Detection System so angepasst, dass ein Angriff auf diese Schwachstelle verhindert und bemerkt wird. Kurz darauf klingelt bei ihm das Telefon. Der für IT-Sicherheit zuständige stellvertretende Geschäftsführer fragt auf Grund seiner Kurzinformation des CERT über eine sein Unternehmen betreffende kritische Schwachstelle nach dem Stand. Er bekommt vom IT- Administrator bereits die Behebung mitgeteilt.

Durch Nutzung der Dienstleistungen des CERTs werden Alarme nur ausgelöst, wenn sie wirklich auf das eigene Unternehmen zutreffen. Somit gibt es keine störende Informationsüberflutung, aber auch keine Unterversorgung.

Da im Unternehmen überwiegend Systeme eingeführt wurden, die in der Vergangenheit wenig Angriffspotential aufwiesen – was sich anhand der Meldungen des CERT zeigte - konnte der Pflegeaufwand stark reduziert werden.

Auf Grundlage dieses Beispiels lassen sich große Teile eines CERTs als informationslogistisches System auffassen, dessen Leistungsfähigkeit von der Quantität und der Qua-

lität der ihm zur Verfügung stehenden sicherheitsrelevanten Informationen, der von ihm genutzten Daten über die Bedürfnisse und Präferenzen der einzelnen Nutzer und insbesondere von der Integration folgender Komponenten abhängt:

- **Nutzerspezifisches Content Management**

  Jeder einzelne Adressat des CERTs (IT-Administrator oder Geschäftsführer eines Unternehmens, externer Dienstleister) muss auf Grundlage seines individuellen Informationsbedarfs unterstützt werden. Es muss daher möglich sein, diesen Bedarf Adressat-bezogen zu modellieren und entweder explizit durch vorgegebene Anforderungen des Adressaten oder implizit durch Ableitung aus nutzerspezifischen Informationen zu definieren. So könnte beispielsweise ein Nutzer explizit bestimmte Sicherheitsmeldungen anfordern oder nur eine allgemeine Beschreibung der IT-Infrastruktur eines Unternehmens und seiner Position in diesem Unternehmen (z.B. Geschäftsführer) angeben, um implizit damit diejenigen Warnmeldungen zu definieren, die für ihn interessant sind. Auf Grundlage aller Nachfragemuster aller Nutzer muss der Zugang des CERT zu den entsprechenden Informationsquellen sichergestellt werden.

- **Communication Management**

  Der aktuelle Informationsbedarf eines Nutzers hängt sehr von seinem Standort (zuhause oder im Unternehmen) ab und noch mehr von der jeweiligen Situation. Dazu gehört seine spezielle aber auch die allgemeine Situation des Unternehmens wie zum Beispiel die aktuelle Verfügbarkeit von IT-Mitarbeitern am Wochenende. Es muss also möglich sein, nicht nur die Position eines Benutzers wahrzunehmen sondern auch seinen Kontext zu identifizieren. Auf dieser Grundlage kann bestimmt werden, ob eine Kommunikation mit dem Benutzer (d.h. Informationslieferung) stattfinden sollte, welche Informationen gegebenenfalls zu liefern sind und welches Kommunikationsmedium gewählt werden soll (z.B. Mobiltelefon, Fax, PDA, etc.).

- **Time Management**

  Eine rechtzeitige Bereitstellung oder Lieferung von Informationen und Warnungen bedeutet auch, dass das CERT in der Lage sein muss, den Zeitraum oder -punkt zu bestimmen, an dem eine Warnung für einen Benutzer von Bedeutung ist. Dies hängt nicht nur vom Kontext des Adressaten ab, sondern auch von der Häufigkeit, mit der in CERT eingehende Informationen und ausgehende Warnungen aktualisiert werden können. Die Angabe von Software-Patches oder Sicherheitsmaßnahmen zur Behebung einer Sicherheitslücke, die am vorherigen Abend bekannt wurde, ist zum Beispiel dann für den IT-Administrator bedeutungslos geworden, wenn bereits eine neue Lücke innerhalb des Patches bekannt ist. Beim Versenden sind insbesondere die Art und Dauer der Informationsübertragung sowie mögliche Verzögerungen zu berücksichtigen.

Ein informationslogistisches System eines CERT kombiniert zudem eine passive (d.h. der Nutzer fordert spezielle Informationen an) und eine aktive (Informationen werden ohne Zutun des Nutzers an diesen weitergeleitet) Informationsversorgung auf Grundlage der Nutzerprofile und der Kenntnis über die Kommunikations- und Informationsinfrastruktur.

3 Ein informationslogistisches Framework

Es gibt eine Vielzahl unterschiedlicher Anwendungen informationslogistischer Systeme, die von Verkehrsleitsystemen bis zu Steuerungssystemen militärischer Operationszentren reichen. Im vorliegenden Papier erklären wir unsere grundlegenden Konzepte für die Implementierung informationslogistischer Anwendungen anhand der Warn- und Frühwarnfunktionen eines CERTs entsprechend des oben beschriebenen Beispiels der Firma Klein & Mittel GmbH.

Die Zielsetzung ist die Entwicklung eines informationslogistischen Systems zur intelligenten Versorgung seiner Nutzer mit IT-sicherheitsrelevanten Informationen. Die Informationen sollten bedarfsgerecht und an speziell festgelegte Orte weitergeleitet oder an den jeweiligen Aufenthaltsort des Adressaten transferiert werden. In unserer Lösung ist der einzelne Nutzer in der Lage, in einem Web-basierten Front-End über WAP- oder Web-Browser ein Profil anzulegen, das seinen persönlichen Informationsbedarf modelliert. Der Nutzer erhält dann automatisch (nur) die für ihn relevanten Informationen über die von ihm gewählten Endgeräte (Mobiltelefone mit SMS oder WAP, FAX, Sprachtelephonie, etc.).

Möchte man eine informationslogistische Anwendung implementieren, so gibt es zunächst die Möglichkeit, eine einfache Lösung auf Basis eines bereits existierenden Content Management Systems, einer Unified Messaging Infrastruktur o. ä. zu realisieren. Dieser „Quick-and-dirty“-Ansatz stößt jedoch i. a. bei der von uns postulierten Integration von Content-, Communication- und Time Management schnell an seine Grenzen, insbesondere dann, wenn das einmal entwickelte System erweitert oder an andere Gegebenheiten angepasst werden soll. In den meisten Fällen muss die Lösung dann von Grund auf neu entwickelt werden, da sogar aus Anwendersicht geringfügige Änderungen nur mit großem Aufwand oder gar nicht realisierbar sind.

Um diese Probleme zu vermeiden, haben wir ein Baukastensystem oder Framework entwickelt, das aus einzelnen, miteinander kombinierbaren Komponenten besteht, die für den effizienten und kostengünstigen Aufbau informationslogistischer Anwendungen und insbesondere von CERTs eingesetzt werden können. Besondere Schwerpunkte bei der Konzeption und Umsetzung dieser Komponenten waren die Anpassbarkeit, Modifizierbarkeit und Konfigurierbarkeit der einzelnen Komponenten und des gesamten Frameworks.

3.1 Modellierung nutzerspezifischer Informationsbedarfe

Die Warn- und Frühwarnkomponente eines CERT benötigt wie jede andere informationslogistische Anwendung sehr viele unterschiedliche nutzerspezifische Informationen. Wir verfolgen den Ansatz, dass dieser individuelle Informationsbedarf, der von den Informationszielen, der Situation und der Umgebung des Nutzers abhängt, durch *Subscriptions* beschrieben wird. Die für die Kommunikation relevanten Informationen wie z.B. die zur Verfügung stehenden Kommunikationsgeräte oder die Nutzerpräferenzen, die z. B. angeben, wann und über welches Kommunikationsgerät der Nutzer informiert werden möchte, werden in individuellen *Nutzerprofilen* gespeichert.

Die dynamische Natur des informationslogistischen Szenarios eines CERT zeigt sich darin, dass eine Vielzahl unterschiedlicher Ereignisse die persönliche Situation und damit den aktuellen Informationsbedarf aber auch die verfügbaren Informationen insgesamt verändern können. Da das CERT die Informationsversorgung des Nutzers (bezüglich sicherheitsrelevanter Informationen) optimieren soll, muss es in der Lage sein, diese verändernden Ereignisse wahrzunehmen, auszuwerten und entsprechend zu reagieren. Wir benutzen zur Modellierung eines solchen Verhaltens das *Event-Condition-Action Modell* (ECA): Beim Eintreffen eines Ereignisses und bei Erfüllung der Bedingung wird die spezifizierte Aktion ausgeführt ([H00]).

3.2 Architektur des Frameworks

Nachdem wir die Grundidee der Informationsversorgung auf Basis von Nutzerbedarfen, die mittels Subscriptions und Profilen beschrieben und in Regeln nach dem ECA-Modell umgesetzt werden, dargestellt haben, beschreiben wir nun die Architektur des Framework für eine bedarfsgerechte Informationsversorgung.

Das System erlaubt die Eingabe und Erfassung des Bedarfs mittels einer graphischen Nutzerschnittstelle (GUI). Wichtige Hilfsdienste sind dafür vor allem Datenbanken zur Speicherung der Profile und des Bedarfs der Anwender. Das GUI kann Web- und WAP-basiert oder eine beliebig andere Anwendung sein. Ferner ist das informationslogistische System in der Lage, verschiedenste Informationsquellen zu integrieren.

Das Kernsystem versucht, aus den eingespeisten Informationen die auf bestimmte Profile und Subscriptions passenden Informationen zu extrahieren und diese zu übermitteln.

Die Funktionalität der Komponenten des Frameworks ist ausschlaggebend dafür, wie viele Dimensionen des durch Ort, Zeit und Bedarf des Nutzers und der Bereitstellung der Informationen aufgespannten Zustandsraumes bei der Auswahl und Zustellung der Informationen berücksichtigt werden.

Die folgende Darstellung (Abbildung 3.1) veranschaulicht die Architektur des Frameworks.

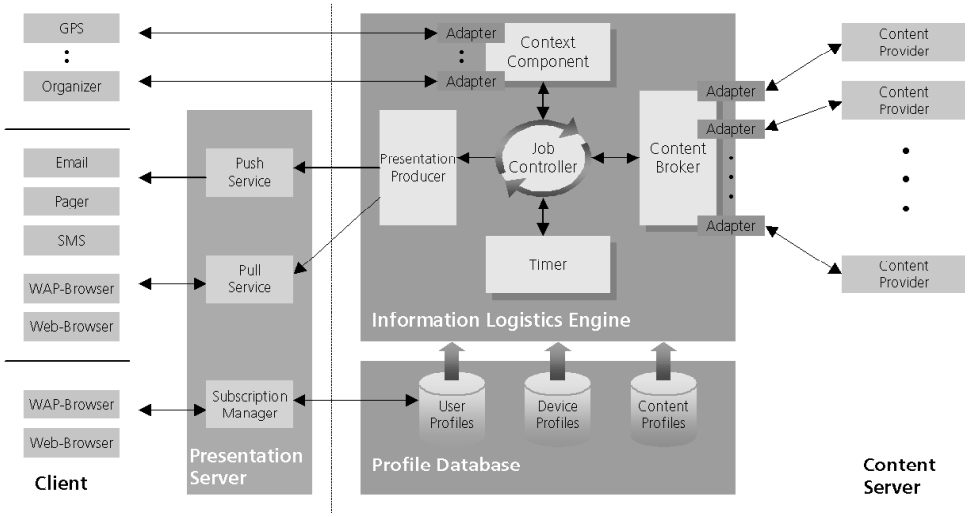

Abbildung 3.1: Architektur des informationslogistischen Frameworks für CERTs

- Die Komponente *ContentBroker* kann verschiedene Informationsquellen mit speziellen Adaptern integrieren. Sie stellt Anfragefunktionen zur Verfügung, mit denen einerseits passiv Informationen für den angegebenen Bedarf abgefragt, und andererseits aktiv aktuell eintreffende Informationen, die zum angegebenen Bedarf passen, an den jeweiligen Interessenten gemeldet werden können.

- Die Komponente *PresentationProducer* erzeugt aus Beschreibungen von Inhalten die Präsentation der Inhalte in Abhängigkeit von der Art des Übermittlungskanals zum Empfänger sowie der Darstellungsmöglichkeiten beim Empfänger.

- Die Komponente *Sender* versendet Dokumente auf verschiedenen Kanälen, zum Beispiel Fax, Email, Pager und SMS, an die angegebene Adresse. Zusätzlich stellt die Komponente ein Transaktionsprotokoll für die asynchron übermittelten Zustellungsergebnisse bereit. Der Sender besteht aus einem Pull- und einem Push-Dienst und unterstützt damit eine passive und eine aktive Informationsversorgung.

- Die Komponente *Timer* stellt Dienste zur Verfügung, die zum einen passiv Auskunft über die aktuelle Zeit geben und zum anderen aktiv als Melder, zum Beispiel wenn ein spezieller Zeitpunkt erreicht ist, agieren. Zudem ist der Timer verantwortlich für die Überwachung zeitlicher Aspekte von Nutzerbedarfen.

- Die Komponente *Locator* als Teil der *ContextComponent* kann spezifische Adaptoren verwalten, die den Zugang zu verschiedenen Systemen zur Ortung von Personen und Sachen ermöglichen. Solche Systeme sind zum Beispiel Infrarot-Baken, GPS-Ortungssysteme oder einfach ein Empfangskanal (Email oder SMS), an den eine formatierte Nachricht, die neben der Identifikation des Nutzers das KFZ-Kennzeichen, die Postleitzahl oder GPS-Koordinate enthält, geschickt wird. Die Komponente stellt aktive und passive Dienste zur Ortung bereit.

Abbildung 3.1 zeigt weitere Komponenten, wie z.B. den *Subscription Manager,* der für die Verwaltung der Subscriptions zuständig ist, und Datenbanken für unterschiedliche Profiltypen, die notwendig, aber für das vorliegende Papier nicht von besonderem Interesse sind. Jede Komponente benutzt einen Plug-in-Mechanismus, um einem Entwickler die Integration eigener Anwendungs-spezifischer Funktionalitäten zu ermöglichen.

Die von jeder Komponente exportierten Dienste müssen in geeigneter Weise koordiniert und kontrolliert werden, damit ihr Zusammenwirken die Semantik der Anwendung, d.h. eines CERTs, erfüllt. Die Koordination und Kontrolle wird von der Auftrags- und Ereignisverwaltung, im Framework *JobController* genannt, übernommen. Die Auftrags- und Ereignisverwaltung etabliert Kommunikationsverbindungen zu den einzelnen Komponenten und nutzt deren Dienste. Sie verwaltet Aufträge (Jobs) und Events, die ihr vom System übergeben werden. Dabei sind die Aufträge das Ergebnis konkreter Ausprägungen eines Bedarfs, der zum Beispiel über die Web-basierte Oberfläche definiert und dem System wie oben erwähnt als Subscriptions übergeben wird. Diese Subscriptions werden vom SubscriptionManager in ausführbare Aufträge (Jobs) umgewandelt. Der JobController ist der Motor des gesamten Systems und übernimmt die komplette Steuerung der anderen Komponenten ([MP01]). Der Auftrag enthält die dazu notwendigen konkreten Anweisungen in Form von Event-Condition-Action-Regeln. Die Struktur und Arbeitsweise eines Auftrags können sehr individuell ausfallen. Die einzige Integrationsbedingung für Aufträge und Ereignisse ist die Erfüllung einer generischen Schnittstelle.

Um die notwendige Flexibilität für verschiedene Anwendungsszenarien sicherzustellen, wurden auch die Komponenten unabhängig voneinander und mit möglichst wenigen Annahmen über ihr Zusammenspiel entworfen. Zudem wurden alle Funktionalitäten einer Komponente, die wahrscheinlich nicht von allen informationslogistischen Anwendungen genutzt werden, in spezifische Plug-ins ausgelagert. Jede Komponente hat somit die Gestalt eines Dispatchers, der Funktionsaufrufe an diese Plug-ins weiterleitet. So nutzt der ContentBroker z. B. eine Vielzahl von Content Service Plug-ins, die die existierenden Informationsquellen wie Datenbanken, Newsgroups und Web-Services ansteuern und abfragen.

Mithilfe dieses modularen Konzepts kann nahezu jeder Typ von Informationsquellen an den ContentBroker angeschlossen und in einer beliebigen informationslogistischen Anwendung, speziell einem CERT, auf Basis unseres Frameworks genutzt werden. Dabei stellt der ContentBroker selbst einen Single-Point-of-Access zu allen integrierten Informationsquellen dar.

Die Funktionalität der Plug-ins ist nur über den Weg der entsprechenden Komponenten nutzbar, so dass die Komponente vor der Implementierung eines Plug-ins gekapselt ist.

Andererseits muss sich der Plug-in-Entwickler nicht um die Kommunikation der Komponenten untereinander kümmern. Die APIs der Komponenten definieren Schnittstellen zur Integration eines Moduls. Ein Modul muss nur diese Schnittstelle unterstützen und kann dann durch Konfigurieren der Komponente integriert werden.

Ein Anwendungsentwickler ist nicht darauf beschränkt, die kleine Anzahl existierender Komponenten zu erweitern oder zu konfigurieren. Natürlich gibt es eine weitere Möglichkeit, Anwendungs-spezifische Komponenten in CERTs, zu integrieren. Die Einbindung einer solchen Komponente in eine Anwendung erfordert nur die sorgfältige Konfiguration des JobControllers und die Definition geeigneter Aufträge, die diese Komponente nutzen.

3.3 Praktische Erfahrungen

Die bisher auf Basis des Frameworks realisierten informationslogistischen Anwendungen, speziell die Unwetterwarnzentrale WIND ([JPTS03]), zeigen den Nutzen des Frameworks. Etwa 70% des Codes dieser Anwendungen basiert direkt auf dem Framework, nur 30% mussten angepasst werden. Dabei handelte es sich um Anwendungs-spezifische Teile des Subscription-Interface, spezifische Datenstrukturen für Subscriptions und Content Objekte und die Anwendungslogik in Form eines speziellen Auftragstyps.

Die gewonnenen Erfahrungen auf dem Gebiet der Informationslogistik ermöglichen den Aufbau von CERTs, die effizient und damit kostengünstig Informationen und Services bereitstellen können.

4 Zusammenfassung

Das vorgestellte Framework ermöglicht die einfache und effektive Entwicklung von informationslogistischen Anwendungen, speziell im Umfeld der Informationsversorgung durch ein CERT. Die im Framework vorhandenen Komponenten können durch weitere Komponenten erweitert werden, die für den Betrieb eines CERT sinnvoll erscheinen.

5 Literaturverzeichnis

[B96] Barker, P. (1996), *Towards real information on demand*. In: Raitt, D.-I.; Jeapes, B., *Online-Information-96-Proceedings*. Learned Inf. (Europe), Oxford, UK.

[DL01] Deiters, W; Lienemann, C. (Ed.) (2001), *Informationslogistik - Informationsversorgung Just-in-Time.* Symposion Verlag, Dusseldorf, Germany.

[H00] Dr. Winfried Heicking: »Analyse bestehender Ereignis- und Auftragsverwaltungssysteme«. Projektbericht. Fraunhofer ISST, August 2000.

[HB99] Hafid, A.; Bochmann, G. (1999), *An approach to quality of service management in distributed multimedia application: design and an implementation*. Multimedia Tools and Applications, 9(2).

[JD99] Jose, R.; Davies, N. (1999), *Scalable and flexible location-based services for ubiquitous information access.* HUC 99 Proc., Lecture Notes in Computer Science, Vol. 1707, Springer Verlag, Germany.

[JPTS03] Jaksch, S.; Pfennigschmidt, S.; Thiel, C.; Sandkuhl, K, (2003), *Information Logistic Applications for Information-on-Demand Scenarios: Lessons from WIND Project.* Proceedings of Euromicro 2003.

[K99] Knowles, C. (1999), *Just-in-time information.* Proc. 2nd International Conf. On Practical Application of Knowledge Management, Practical Application Company, Blackpool, UK.

[L91] Liebesny, J.-P. (1991), *An advanced traveller information system providing real-time, location-specific on-demand traffic information.* VNIS-91 Proceedings, Soc. Automotive Eng., Warrendale, PA, USA.

[MP01] Ulrich Meissen, Stefan Pfennigschmidt (2001), *»Lernen aus »Lothar« - Sturmwarnungen mit @ptus-weather«*. In W. Deiters, C. Lienemann: »Report Informationslogistik«, 1. Auflage.

[OSE95] Ozsu, M.-T.; Szafron, El-Medani, G.; Vittal, C. (1995), *An object-oriented multimedia database system for a news-on-demand application*. Multimedia Systems, 3(5-6).

[Y00] Yin Fu Hang et al. (2000), *The design and implementation of an interactive news-on-demand system*. Journal of the Chinese Institute of Engineers, 23(5).