Elektronische Archive in virtuellen Organisationen: Gestaltung im Spannungsfeld von Kooperation und Konkurrenz

Gunnar Stevens[1] und Volker Wulf[2,3]

[1]ProSEC - Informatik III, Universität Bonn, Römerstr. 164, 53117 Bonn

[2] Fraunhofer Institut FIT, Schloß Birlinghoven, 53754 Sankt Augustin

[3] IISI - Internationales Institut für Sozio-Informatik, Heerstr. 148, 53111 Bonn

Virtuelle Organisationen stellen ein relativ neues Anwendungsfeld der Informatik dar. Aus den Besonderheiten dieses Organisationstypus ergeben sich neue Gestaltungsaufgaben. In diesem Aufsatz wird an Hand einer Fallstudie aus der Stahlindustrie gezeigt, in welch komplexer Weise Kooperation und Konkurrenz in virtuellen Organisationen miteinander verwoben sein kann. Daraus ergeben sich Konsequenzen für die Gestaltung der Zugriffskontrolle auf elektronische Archive, wenn diese für die organisationsübergreifende Kooperation in einer virtuellen Organisation genutzt werden. Basierend auf diesen Erkenntnissen stellt der in der nächsten Ausgabe des Informatik-Spektrum erscheinende zweite Teil des Aufsatzes eine komponenten-basierte Anwendung zur Zugriffskontrolle in virtuellen Organisationen vor.

Der Begriff der virtuellen Organisation (VO) ist in der Literatur bisher nicht eindeutig bestimmt. Im allgemeinen werden unter diesem Begriff Phänomene erfasst, die mit bisherigen Beschreibungen organisatorischer Modelle nur unzureichend abgedeckt werden. Eine weitgehend akzeptierte Definition beschreibt virtuelle Organisationen als eine Kooperation von rechtlich unabhängigen Firmen oder Einzelpersonen, die ihre Kernkompetenzen in vertikaler oder horizontaler Weise miteinander vernetzen. Die Literatur betont außerdem das Faktum, dass Hierarchien in virtuellen Organisationen flach und zentrale Koordinations- und Kontrollfunktionen nicht etabliert sind. Die meisten Autoren geben an, dass die virtuelle Organisation nur für eine begrenzte Zeit errichtet wird, und dass die Mitglieder einer virtuellen Organisation gewöhnlich geographisch verteilt arbeiten. Die räumlich Distanz soll dabei durch Einsatz von Informations- und Kommunikationstechniken (I.u.K.-Techniken) überwunden

werden (vgl. Davidow and Malone 1992; Arnold und Härtling 1995; Travica 1997; Strausak 1998; Mertens, Griese und Ehrenberg 1998; Sieber 1998; Rittenbruch, Kahler und Cremers 1999; Nett, Fuchs-Frohnhofen und Wulf 2000; Rohde, Rittenbruch und Wulf 2001).

Mit der Auflösung der organisatorischen und räumlichen Grenzen erwächst die besondere Flexibilität, die man den VOs zuschreibt. Diese Flexibilität stellt einen entscheidenden Wettbewerbsvorteil in sich dynamisch wandelnden Märkten dar. Aus der Kooperation aus rechtlich selbstständigen und räumlich verteilten Partnern ergeben sich aber auch neuartige Unsicherheitsmomente. Diese ergeben sich häufig aus der widersprüchlichen Einheit von gemeinsamen und unterschiedlichen Interessenlagen der Kooperationspartner[1]. In klassischen Organisationen können Konflikte, die sich aus divergierende Interessenlagen zwischen Individuen oder einzelnen Organisationseinheiten ergeben, durch Weisung entlang der Organisationshierarchien (zumindestends prinzipiell) geregelt werden. Solche Regelungsmöglichkeiten bestehen in virtuellen Organisationen typischerweise nicht.

Die widersprüchliche Einheit von Kooperation und Konkurrenz führt auch zu neuen Herausforderungen für die Informatik, weil in der Diskussion um virtuelle Organisationen im allgemeinen davon ausgegangen wird, dass die Effiziens einer organisatorischen Kopplung durch informatorische Integration erhöht werden kann. Aus den unterschiedlichen Interessenlage der Akteure kann sich dann ein Zielkonflikt zwischen wirtschaftlicher Autonomie und informatorischer Kopplung ergeben. Schüppler (1998, S. 67) geht beispielsweise davon aus, dass mit der informatorischen Integration die „*Offenlegung von unternehmensinternen Sachverhalten mit dem Risiko der Preisgabe von Kernkompetenzen (Typebene) und sensiblen Daten (Ausprägungsebene) einhergeht*."

Will die Informatik Arbeitsprozesse innerhalb virtueller Organisationen durch informatorische Integration fördern, so muß sie sich mit den neuartigen Kooperationbedingungen innerhalb dieser Organisationsform beschäftigen. Dies ist zunächst eine empirische Fragestellung, die die Grundlage für eine angemessenen Technikgestaltung und –konfiguration bietet. Im folgenden soll das Problem des Zugangs zu elektronischen Archiven in virtuellen Organisationen näher untersucht werden. Dazu wird zunächst die zwischenbetriebliche Kooperation in einem Konstruktionsnetzwerk der Stahlindustrie genauer untersuchen. Aus den Ergebnissen der Fallstudie ergeben sich neue

[1] So verwundert es nicht, dass in der VO-Diskussion das Thema Vertrauen einen besonderen Stellenwert hat. Picot und Neuberger (1997) sprechen gar von einem „Vertrauensdilemma", dem „zum einen ist Vertrauen eine notwendige Voraussetzung [für VOs], zum anderen ist diese Voraussetzung jedoch nur sehr schwierig herzustellen" (zit. nach Schüppler 1998). Auf den Zusammenhang von Vertrauen und Kontrolle weist Sydow et al. (1995 S.55 ff.) hin.

Anforderungen an die Gestaltung der Zugriffskontrolle für gemeinsame Archive. In der in der nächsten Ausgabe des Informatik-Spektrums folgenden Fortsetzung des Beitrags wird ein komponenten-basierter Ansatz zur flexibilisierter Gestaltung der Zugriffskontrolle in virtuellen Organisationen vorgestellt.

Fallstudie

Die hier dargestellte Untersuchung fand im Rahmen des OrgTech-Projektes statt. Im Projekt wurde in zwei unterschiedlichen Anwendungsfeldern untersucht, wie sich die Wettbewerbsbedingungen kleiner und mittelständischer Ingenieurbüros durch innovative zwischenbetriebliche Kooperationsprozesse verbessern lassen. Als Vorgehensmodell wurde der Ansatz *"Integrierter Organisations- und Technikentwicklung (OTE)"* verwandt *(vgl.* Wulf und Rohde 1995 und Wulf et al. 1999).

Im folgenden werden wir Ergebnisse aus einem der beiden Anwendungsfelder der OrgTech-Projektes presentieren. In diesem Anwendungsfeld wurde die Zusammenarbeit zwischen dem Stahlwerk „Bausig" und den beiden Ingenieurbüros „Schmidt & Partner" und „Lange"[2], die für das Stahlwerk Konstruktionsaufträge erledigen, untersucht (vgl. Iacucci et al. 1998 und Fuchs-Frohnhofen, Nett, Wulf 2001). Zu Beginn des Projektes wurde dazu ein Workshop unter der Beteiligung von Vertretern Bausigs und den Büros Schmidt & Partner und Lange veranstaltet. Nach einer Vorstellung der Projektziele wurde per Kartenabfrage Probleme in der zwischenbetrieblichen Kooperation von den Teilnehmern genannt und gemeinsam geordnet. Basierend auf den im Workshop genannten Problemfeldern wurde ein Interviewleitfaden eintwickelt und etwa 20 semistrukturierte Interviews mit Mitarbeitern der drei Organisationen geführt. Dabei wurde von Seiten der Ingenieurbüros u.a. die unzureichenden Vorgaben bei der Auftragsvergabe durch Bausig und das Fehlen eines einfachen Datenaustauschs zwischen ihnen und dem Stahlwerk bemängelt. Sie regten an, das elektronische Zeichnungsarchiv von Bausig für die Kooperation zu öffnen. Auf dem sich an die Interviewphase anschließenden Auswertungsworkshop zeigten sich die Mitarbeiter von Bausig ambivalent hinsichtlich einer elektronischen Öffnung ihres Archives. Einerseits würde eine solche Öffnung des Archives die Kooperation mit den externen und damit auch ihre persönliche Arbeit erleichtern, andererseits befürchteten sie eine mißbräuchliche Nutzung des Archivzugangs. Diese Haltung lässt sich am Besten mit dem Satz charakterisieren:

[2] Zur Anonymisierung sind die Namen des Stahlwerkes und der Ingenieurbüros geändert worden.

„Die Fremddienstleister sollen zwar selbständig arbeiten können, aber die Kontrolle muss bei Bausig bleiben."

Sydow et al. (1995, S. 62) sprechen in diesen Sinne bei interorganisatorischer Kooperation auch von *kontrollierter Autonomie*, wenn *„den Akteuren bewußt ein gewisses Maß an Autonomie zugestanden wird, die Einhaltung der Autonomiespielräume aber gezielt kontrolliert werden"*.

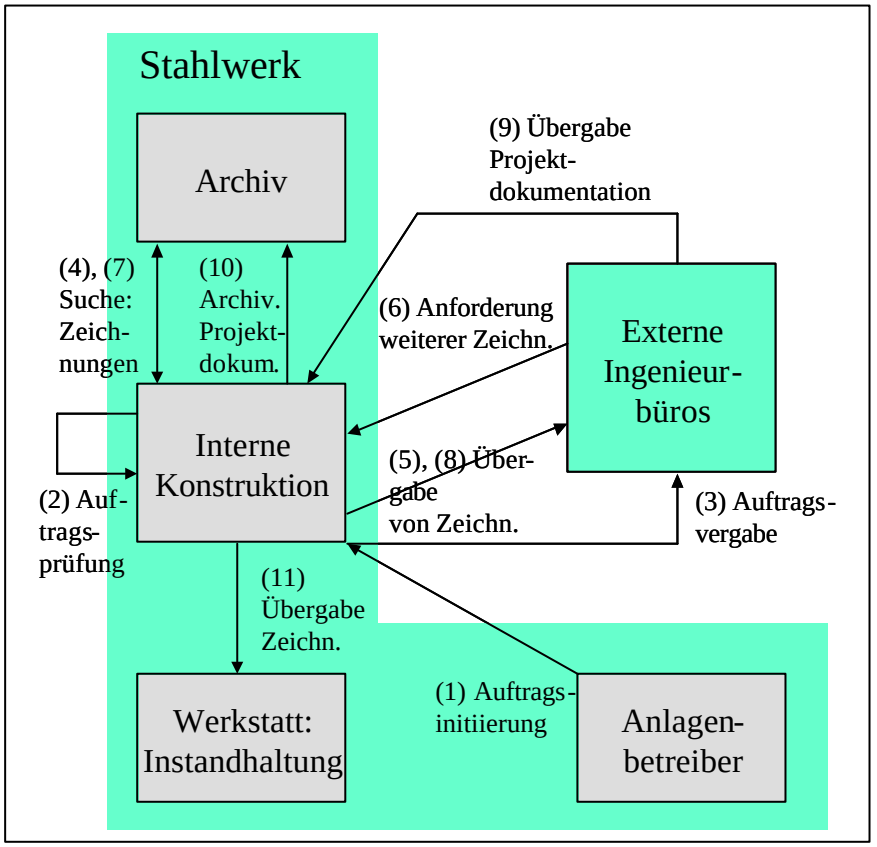

Abb. 1: Ablaufdiagramm der Auftragsbearbeitung

Im weiteren betrachten wir den in Abb. 1 schematisch dargestellten Arbeitsablauf wie er aus der Sicht eines Mitarbeiters der internen Konstruktion und eines

Mitarbeiters eines Ingenieurbüro geschildert wird[3]. Abb. 1 stellt dabei den vom Stahlwerk zentral vorgegebenen Prozeßverlauf dar.

Arbeitsablauf

Ein Mitarbeiter der internen Konstruktionsabteilung beschreibt den Arbeitsablauf wie folgt.

> *„Der Ablauf sieht so aus, dass wir zunächst einen Konstruktionsauftrag erhalten.[...] Wir prüfen zunächst das Anliegen der Endkunden formal und inhaltlich. Dann müssen wir Kapazitäten und Kompetenzen für die Konstruktion überprüfen, z.B. einen passenden Fremddienstleister suchen. Die Externen erhalten offiziell erst nach dieser internen Prozedur den Konstruktionsauftrag. Bei Eile wird jedoch direkt hin und her telefoniert und ein mündlicher Auftrag erteilt, so dass sich die formale und die tatsächliche Struktur überschneiden. Offiziell dürfen wir keinen Auftrag erteilen ohne offizielle Genehmigung als Ende des offiziellen Wegs. Aber niemand kann verantworten, dass z.B. die Produktion wochenlang stillsteht. ‚Dazwischen spielt sich die Wahrheit ab'.[...]"*

Kontrastiv dazu sei hier die Sicht eines Mitarbeiters eines Ingenieurbüro auf die Auftragsbearbeitung dargestellt.

> *„In der Kooperation mit Bausig gibt es den formalen und den informalen Ablauf. Formell werden die Aufträge von der zentralen Konstruktionsabteilung an die Büros vergeben. Dazu sollte sich der Anlagenbetreiber nach der Morgenbesprechung an den Instandhalter vor Ort wenden. Dieser dokumentiert den Wunsch und vergibt den Auftrag an den kostengünstigeren. Er ist formal auch für die Überwachung und die Abrechnung des Konstruktionsauftrages verantwortlich. Die Ingenieure erhalten je nach Anzahl der Zeichnungen einen bestimmten, für 3 Jahre ausgehandelten Fixsatz. Insofern ist formal der Auftraggeber von Partner & Lange immer die Konstruktion. De facto werden die Aufträge aber ganz anders vergeben: Die Anlagenbetreiber – als die tatsächlichen Endkunden – wenden sich häufig direkt an die Konstruktionsbüros (telefonisch nach der alltäglichen Morgenbesprechung) und machen Termine aus, um anstehende Aufträge zu besprechen."*

Aus diesen beiden Darstellungen lassen sich zwei Feststellungen treffen, die im weiteren genauer erläutert werden.

[3] Die Zitate beruhen auf Gedächnisprotokollen, die nach den Einzelinterviews bzw. nach Workshops erstellt worden sind. Zu den Problemen, editierte Protokolle zu analysieren, sei hier auf Oevermann (1997) verwiesen.

- ❖ Die interne Konstruktionsabteilung und die externen Büros stehen in einem dialektischen Verhältnis von Konkurrenz und Kooperation.
- ❖ Der vorgeschriebene Weg und die tatsächliche Arbeitspraxis bei der Auftragsbearbeitung klaffen (zeitweilig) auseinander.

Die interne Konstruktionsabteilung und externen Büros stehen in einem dialektischen Verhältnis von Konkurrenz und Kooperation

Zu Beginn des Projektes befand sich das Stahlwerk in einem längerwährenden Umstrukturierungsprozeß, der zur Einführung ergebnisorientierter Teileinheiten, so genannten Cost- und Profitcenter, beinhaltete. Die Umstrukturierungsmaßnahmen beinhalteten auch das Outsourcing[4] von Unternehmensteilen. Umstrukturierungsmaßnahmen sind meist mit einer Verunsicherung der Betroffenen verbunden (vgl. Peltzer 1998, S. 174). Dies trifft insbesondere dann zu, wenn wie im Falle der Instandhaltungskonstruktion die eigene Abteilung zugunsten externer Dienstleister abgebaut wird.

Durch diese Umstrukturierungsmaßnahmen hat sich die Funktion der internen Konstruktionsabteilung gewandelt. Gegenüber den externen Büros nimmt sie unterschiedliche Rollen ein, die sich im Widerstreit zueinander befinden. Im Kontext unserer Untersuchung sind vor allem die Rollen des Auftragebers, des eigenständigen Marktteilnehmers und des Werkschutzes[5] zu nennen. Geklammert werden die verschiedenen Rollen durch das übergeordnete Ziel, im Sinne Bausigs zu handeln. Dementsprechend ist der Externe aus Sicht der internen Konstruktion sowohl ein Auftragnehmer, ein Konkurrent bzw. ein potentieller Spion. Aus dieser Konstellation ergeben sich die Unwägbarkeiten in der Beziehung. Das strukturelle Dilemma der internen Konstruktionsabteilung hat ein Bausig-Mitarbeiter so beschrieben: *„Wenn der Fremddienstleister direkt die Betreiber kontaktiert, wird die interne Konstruktionsabteilung zwar entlastet, aber bei Problemen trägt sie die Verantwortung ohne beteiligt worden zu sein. [...] Weiterhin geht der Überblick für die interne Abteilung verloren, wenn Dienstleister und Betreiber*

---

[4] Outsourcing wird im Wirtschaftslexikon wie folgt beschrieben:
„1. Verlagerung von Wertschöpfungsaktivitäten des Unternehmens auf Zulieferer. O. stellt eine Verkürzung der Wertschöpfungskette bzw. der Leistungstiefe des Unternehmens dar. [...]
2. *O. von Dienstleistungen (z.B. Datenverarbeitung), aber auch der Teileproduktion oder ganzer Komponenten und damit die kostenorientierte Verkürzung der Wertschöpfungstiefe, hat strategisch in den letzten Jahren an Bedeutung gewonnen. Der Einsatz moderner Produktions- und Logistikkonzepte (z.B. Just-in-time) setzt erfolgreiches O. voraus, da die Zulieferer konzeptionell in der Wertschöpfungskette mit eingebunden sind."* (o.V., Wirtschaftslexikon 1997)

[5] Auf den ersten Blick könnte man die Rolle des Werkschutzes als ein Bestandteil der Rolle des eigenständigen Marktteilnehmers ansehen. Bei der ersteren hat man jedoch die Aufgabe Bausig zu schützen, in der letzteren seine eigene Position.

direkt miteinander (ohne interne Konstruktion) kommunizieren, da die interne Konstruktion u.U. gar nicht erfährt, dass etwas geändert wurde." Das Wünschenswerte, Fremddienstleister und Endkunden agieren direkt miteinander, hat umkehrseitig das zu Vermeidende zur Folge, nämlich, dass die interne Konstruktion außen vor bleibt.

Somit sind bei der Zusammenarbeit zwischen Internen und Externen immer gleichgerichtete als auch divergierende Interessen vorhanden. Hierin unterscheiden sich unsere Beobachtungen beim Outsourcing einzelner Arbeitsprozesse von den Ergebnissen von Harms (1973), der traditionellere, weniger integrierte Formen zwischenbetrieblicher Kooperation untersucht hat und dabei die Beziehungen in kooperierende und konkurrierende Aspekte einteilen konnte. Wie wir im weiteren sehen werden, hat diese Gleichzeitigkeit von Kooperation und Konkurrenz Auswirkungen auf die Gestaltung der Zugriffskontrolle.

Die offiziell vorgeschriebene und die tatsächliche Arbeitspraxis bei der Auftragsbearbeitung klaffen (zeitweilig) auseinander

Dieser Sachverhalt wurde in den Zitaten offen angesprochen, und dürfte jedem Praktiker bekannt sein. Dieser Tatbestand ist auch schon häufiger in mikrosoziologischen bzw. ethnographischen Studien untersucht worden (vgl. Bensman und Gerver 1963; Boland und Pondy 1983; Mambrey und Robinson 1997).

Bei genauerem Hinsehen wirft dieses Faktum für die Software-Entwicklung jedoch ein grundsätzliches Problem auf. Dies kann hier nur verkürzt dargestellt werden und dient vor allem zur Motivation für unseren gewählten Weg der Softwaregestaltung. Auf die Frage, was ein Computersystem sei, bekommt man von Informatikern häufig die Antwort, es sei ein Modell der Wirklichkeit[6]. Diese Auffassung mag bei der Softwareentwicklung auch in einigen Fällen, wie z.B. der Wettersimulation, sinnvoll sein. Bei der Gestaltung von Computersystemen gerade im CSCW-Bereich ist sie jedoch nur bedingt tauglich. Denn die Tatsache, dass sowohl die offizielle als auch die de facto Struktur gleichermaßen real sind, stellt den Softwarehersteller vor das Problem, entscheiden zu müssen, welche Realität zur Modellierung herangezogen werden soll, ohne das ihm durch die *Isomorphie-Maxime* eine Entscheidungshilfe angeboten wird. Dem sich auftuenden Entscheidungszwang versucht man dadurch zu entfliehen, dass man die offizielle Struktur als ein Soll-Zustand definiert und jede Abweichung in der Praxis als eine Störung ansieht, die es zu vermeiden gilt. Damit besteht aber die

[6] So schreibt Schefe (1998) in seiner Einleitung *„Die Isomorphie von Realität und ihrer softwaretechnischen Rekonstruktion (vgl. Everling, 1995) scheint eine Basis-Auffassung der Softwaretechnik zu sein"*.

Gefahr, dass die Bedürfnisse der Betroffenen und die Notwendigkeiten der Praxis ausgeblendet werden.

Demgegenüber soll hier ein Computersystem als ein Artefakt angesehen werden, dass ein Teil der (zukünftigen) Praxis ist. Dabei wird die Forderung nach einem, wie auch immer gearteten, Morphismus zwischen dem Computersystem und der Wirklichkeit fallen gelassen. Damit verändert sich aber die Art der Anforderungsanalyse und damit auch die Fragestellung bei der „Feldforschung". Die aufgestellten Modelle bzw. Theorien über die Praxis dienen den Softwareentwickler nicht dazu, diese in ein ablauffähiges Computerprogramm umzuwandeln, sondern die zukünftige Nutzung schon bei der Gestaltung zu antizipieren. Die Frage, die es somit zu beantworten gilt, ist nicht mehr allein die, was automatisierbar ist, sondern auch (und vielleicht vor allem) die, wie sich das Computersystem in die Arbeitspraxis einfügen wird.

Vor diesem Hintergrund kann man das in der Forschung zur angewandten Informatik diskutierte Konzept der Anpassbarkeit (vgl. Wulf 2000; Kahler 2001; Stiemerling 2000) als einen Versuch ansehen, den Unwägbarkeiten Rechnung zu tragen, die dadurch entstehen, dass es nicht mehr die eine objektiv erfaßbare Realität gibt, die modelliert werden kann. Stattdessen soll hier die Systemgestaltung dahingehend offen gelassen werden, dass die „politischen" Aushandlungen, die mit den technischen Gestaltungsentscheidungen verwoben sind[7], möglichst wieder in die Praxis zurück verlagert werden.

Zugriff auf das elektronische Archiv

Die Untersuchungen der Auftragvergabe hat die Ambivalenz von Kooperation und Konkurrenz im Zusammenwirken zwischen internen und externen Organisationseinheiten virtueller Organisationen verdeutlicht. Diese Ambivalenz kennzeichnet aber nicht nur die Auftragsvergabe sondern auch die weitere Auftragsbearbeitung. Im folgenden wollen wir insbesondere die zur Auftragsbearbeitung notwendigen Zugriffe aufs elektronische Zeichnungsarchiv betrachten.

Bei dem Zugriff der Externen auf das Archiv müssen wir ebenfalls zwischen der offiziellen und der tatsächlichen Struktur unterscheiden. Die von Bausig beabsichtige Arbeitsteilung kann grob so skizziert werden: Der interne Sachbe-

[7] So sehen Weltz/Lullies/Ortmann (1991) die Softwareentwicklung als *"ein Doppelprozeß von technischer Entwicklung und "politischer" Verarbeitung (Interessenaushandlung). Beide Prozesse sind auf vielfältige und meist schwer durchschaubare Weise miteinander verwoben."* Sie kommen dabei zu dem Schluß, *dass "ein Symptom des Doppelcharakters der Software-Entwicklungsprozesse, das die Auseinandersetzungen über die Systemgestaltung zweifellos erschwert, ist der Umstand, dass häufig auf der technischen Ebene argumentiert wird, selbst wo es auch oder primär um 'politische' Aspekte geht".*

arbeiter sucht alle notwendigen Zeichnungen für den Externen heraus und übergibt sie ihm. Dieser überarbeitet sie dann und gibt sie anschließend wieder zurück. Abschließend wird sie von Bausig noch einer Qualitätskontrolle unterzogen. Ein Mitarbeiter beschreibt dies wie folgt: *„Der externe Dienstleister bekommt von uns in der Regel die komplette Dokumentation, zum Teil auch die Problemlösung übergeben. Er verbleibt nach dieser Vorklärung aber ausführendes Organ. Nachher müssen wir neben inhaltlicher und geographischer Prüfung auch noch die Strukturprüfung vornehmen."*

In einem solchen Idealfall besteht nicht das Problem eines externen Zugriffs auf das Archiv. In der Praxis kommt es aber immer wieder vor, dass, wie in Abb. 1 dargestellt, Unterlagen nachgefordert werden. Dies kann auf verschiedenen Wegen geschehen. Die Zeichnung kann über Telephon, Fax und neuerdings auch E-Mail angefordert werden. Oder aber der externe Ingenieur fährt auf das Werksgelände und sucht dort zusammen mit einem Mitarbeiter von Bausig oder auch alleine mittels eines guest-account im elektronischen Archiv nach der Zeichnung.

Im Archivzugriff reproduziert sich dabei der oben beschriebene Grundkonflikt zwischen den Internen und Externen. Die interne Konstruktion beschränkt sich bei der Dokumentenübergabe auf das Notwendigste. Demgegenüber gehört es mit zur Aufgabe der Konstruktion, zu beurteilen, ob eine Zeichnung für das Problem relevant bzw. **nicht** relevant ist.

So kann das Dilemma für die interne Konstruktionabteilung wie folgt umschrieben werden: Wenn der Fremddienstleister also direkt das Archiv kontaktiert, wird sie zwar entlastet. Aber bei Problemen trägt sie die Verantwortung ohne beteiligt worden zu sein. Weiterhin geht der Überblick für sie verloren, wenn der Dienstleister, ohne sie zu kontaktieren, sich direkt die Zeichnung beschafft, da sie u.U. gar nicht erfährt, dass etwas geändert wurde.

Dabei scheint auf den ersten Blick der guest-account mittels dessen die Externen selbstständig im elektronischen Archiv suchen können im Widerspruch zur obigen Kontroll-Hypothese zu stehen. Doch um ihn nutzen zu können, muss sich der Externe zu Bausig begeben und sich dafür vorher angemeldet haben. Damit stellt aber das Werkstor, als eine räumliche Begrenzung des Zugangs, und das ist hier offenbar entscheidend, eine für das Sicherheitsbedürfnis von Bausig ausreichende Kontrolle dar. Der guest-account kann als ein Indiz dafür gesehen werden, dass nicht die Zeichungen an sich das eigentlich Sensible darstellen, sondern der unkontrollierte Zugang dazu.

Da die Kontrolle des Zugriffs eine zentrale Rolle für die Akzeptanz des externen Zugriffs auf das elektronische Zeichnungsarchiv spielt, soll im folgenden ein kurzer Abriss über den Stand der Forschung im Bereich Zugriffskontrolle gegeben werden. Dabei soll insbesondere auf neuere Ansätze eingegangen werden, die den Kontrollbedürfnissen der Akteure im Anwendungsfeld besser gerecht werden.

Zugriffskontrolle

Die Aufgabe eines Sicherheitssystems ist es sicherzustellen, dass keine unerlaubten Aktionen auf zu schützenden Daten ausgeführt werden. Neuere Ansätze gehen bei der Kommunikation erschiedener Akteure von mehrseitiger Sicherheitsanforderungen aus (vgl. Pfitzmann und Müller 1997). Sicherheitssysteme können in verschiedene Teilsysteme wie Authentifizierung, Verschlüsselung und Zugriffskontrolle unterteilt werden. Die Authentifizierung und die Verschlüsselung sind für zwischenbetriebliche Anwendungen, die über offene Netze kommunizieren, von besonderer Bedeutung (vgl. Coulouris 1998; Coulouris, Dollimore und Roberts 1998; Schneiders 1998 und 1999). Unsere Untersuchung konzentriert sich hier aber ausschließlich auf den Bereich der Zugriffskontrolle.

Die Aufgabe eines Zugriffskontrollsystems besteht darin, einem Subjekt s in einer bestimmten Situation t eine Operation r auf ein Objekt o ausführen zu lassen bzw. zu verweigern. Die Systeme kann man danach unterscheiden, wie Trägermengen für die Parameter s, t, r und o aussehen, und die der Zugriff durch sie geregelt werden kann. Eine Übersicht von klassischen Modellen und deren Einordnung bzgl. ihrer Einstellmöglichkeiten, findet sich bei Eckert (1996).

Neben dieser technischen Sichtweise, stellen andere Studien zu diesem Thema den Nutzer in den Vordergrund ihrer Betrachtung. Zum einem interessieren sie sich dafür, welche Parameter überhaupt in der Praxis relevant sind. So haben Stiemerling, Won und Wulf (2000) im Verwaltungsbereich empirisch die Faktoren ermittelt, die für den Anwender wichtig sind. Zum anderen wurden die Systeme unter softwareergonomischen Gesichtspunkten untersucht. Bei der Handhabung der Einstellmöglichkeiten der Zugriffsrechte, hat sich vor allem das Zugriffsmatrix-Modell als zu unflexibel erwiesen (vgl. Shen und Dewan 1992). Das Problem der Zugriffsmatrix besteht in seiner Flachheit, d.h. dass für jedes einzelne Feld der Objekt-Subjekt-Matrix die Zugriffsart festgelegt werden muss. Entsprechend erweiterte Modelle beinhalten die Möglichkeit der Hierarchisierung, was sowohl Subjekt, Objekt als auch die Operationen betrifft (vgl. Shen und Dewan 1992; Stimmerling 1996; Sikkel 1997). Zur Spezifikation der Zugriffsstrategie sind bei diesen Modellen auch negative Rechte erlaubt. Die einzelnen Modelle unterscheiden sich darin, wie komplex die Hierarchie werden kann und wie sie für den Anwender gehandhabt werden.[8]

[8] Der einfachste Fall einer Hierarchisierung ist z.B. die Gruppenbildung bei Subjekten. Komplexer sind schon Modelle, bei denen man die Möglichkeit hat, Baumstrukturen, wie z.B. Dateisysteme, zu spezifizieren. Noch komplizierter sind azyklische Graphen, wie z.B. im Modell von Shen und Dewan (1992). In dem Fall, in den beliebige Graphen definiert werden können, kann man eigentlich schon nicht mehr von einer Hierarchie sprechen.

Ellis, Gibb und Rein (1991) haben darauf aufmerksam gemacht, dass solche Modelle für den Anwender recht kompliziert zu handhaben sind. Dies hängt unter anderem damit zusammen, dass sich in diesen Modellen widersprüchliche Regeln definieren lassen, die dann in Konflikt zu einander geraten können. Deshalb stellen einige dieser Modell automatische Konfliktlösungs-Mechanismen zur Verfügung, die jedoch nicht immer für den Benutzer auf den ersten Blick durchschaubar sind.

Zeitpunkt der Kontrolle

Den oben beschriebenen Zugriffsmodellen liegt die Annahme zu Grunde, dass *vor dem Zugriff* bestimmt werden kann, was erlaubt bzw. verboten ist. Folgt man dieser Prämisse, gibt es eine exakte Abgrenzung zwischen beiden Punkten. Erweist sich ein Zugriffssystem in der Praxis als unzureichend, kann der Grund für den Mangel nur darin bestehen, dass der Grenzverlauf zwischen dem Erlaubten und dem Verbotenen nicht genau genug gezogen werden kann. Dies kann entweder daran liegen, dass die Einstellmöglichkeiten zu grobkörnig oder dass sie zu kompliziert zu bedienen sind.

Im Gegensatz dazu wollen wir Aufgrund der obigen Untersuchung diese Prämisse fallenlassen. Wir gehen stattdessen davon aus, dass eine Abgrenzung in legitimen und nicht legitimen Zugriff situationsabhängig ist. Deshalb ist eine exakte Festlegung im vorherein nicht immer möglich. Dies soll als Motivation dafür dienen, nach qualitativ anderen Kontrollmechanismen zu suchen.

Um Kontrollmechanismen zu klassifizieren, kann man den Zeitpunkt, an dem die Legitimation des Zugriff festgelegt wird, heranziehen. Es lassen sich dabei drei Zeitpunkte unterscheiden:

1. *Eine **ex-ante** Kontrolle liegt dann vor, wenn vor dem Zugriff festgelegt wird, ob er legitim bzw. illegitim ist.*
2. *Eine **uno-tempore** Kontrolle liegt dann vor, wenn während des Zugriffs festgelegt wird, ob er legitim bzw. illegitim ist.*
3. *Eine **ex-post** Kontrolle liegt dann vor, wenn nach dem Zugriff festgelegt wird, ob er legitim bzw. illegitim ist.*

Die traditionellen Zugriffskontrollen fallen damit in die Kategorie der ex-ante Mechanismen. Ein Beispiel einer uno-tempore Kontrolle findet sich bei Kindern wieder, die grundsätzlich darauf bestehen, dass man nachfragt, bevor man irgendeins ihrer Spielzeuge leihen möchte. Andere Beispiele für diese Kontrollmechanismen finden sich bei Wulf (1995b, 1997).

Ein Beispiel einer ex-post Kontrolle findet sich in dem Ausspruch: „Der Missbrauch wird bestraft“ wieder. Die Kontrollstrategie die dahintersteht, beruht darauf, dass drei Voraussetzungen erfüllt sind:

1. Es gibt einen Gebrauch, denn sonst gäbe es umkehrseitig auch kein Missbrauch.
2. Ein Missbrauch ist erkennbar.
3. Ein Missbrauch kann bestraft werden.

Im folgenden sollen hier zwei Arbeiten vorgestellt werden, die sich kritisch mit den tradionellen Zugriffkontroll-Systemen auseinandersetzen.

Optimistic Security: A New Access Control Paradigm"

Die Idee der optimistischen Sicherheit, wie von Povey (1999a) beschrieben, entspringt auf folgender Beobachtung:

"*Legitimate and optimistic access control takes the approach of assuming that most accesses will relys* on controls external to the system *to ensure that the organisations security policy is maintained". [Hervorhebung im Orginal] (Povey 1999a).*

Den Kernpunkt der Funktionsweise seines Ansatzes beschreibt er folgend:

"In an optimistic system, enforcement of the security policy is retrospective, and relies on administrators to detect unreasonable access and take steps to compensate for the action. Such steps might include: Undoing illegitimate modifications, taking punitive action (e.g. firing, or prosecuting individuals) or removing privileges" (Povey 1999a).

Der Ansatz beruht dabei auf fünf Vorraussetzungen: kontrollierten Einstiegspunkten (Constrained entry points), die Zurechenbarkeit (Accountability), die Aufzeichenbarkeit (Auditability), die Wiederherstellbarkeit (Recoverability) und die Androhbarkeit (Deterrents).

Die Unterschiede, die sich gegenüber den traditionellen Zugriffsmechanismens, die er pessimistisch nennt, sind in Tab. 1 zusammengefasst. Insgesamt stellt Poveys Ansatz eine technische Umsetzung eines ex-post Kontroll Mechanismus dar.

ATTRIBUTE	PESSIMISTIC	OPTIMISTIC
Access Decision	Prospective	Retrospective
Access Enforcement	Deny	Recover/Deter
Cost of Violation	None	Some
Flexibility	None	Some

Tab. 1: Eigenschaften der pessimistischen vs. der optimistischen Sicherheitsstrategie (Povey 1999b)

Between 'Yes or No' – Extending Access Control in Groupware with Awareness and Negotiation"

Stiemerling und Wulf (2000) plädieren ebenfalls für eine andere Sichtweise. Im Gegensatz zu Povey, der eher technisch argumentiert, haben Stiemerling und Wulf (2000) in der Arbeitspraxis anzutreffende Kontrollmechanismen empirisch untersucht. Die Autoren haben dabei Formen der Regelung des Zugriffs auf physische und elektronische Materialien in mehreren Organisationen des Büro- und Verwaltungsbereichs untersucht. Die Ergebnisse wurden an Hand von drei Fallstudien präsentiert. Diese sollen im folgenden kurz referiert werden.

Im ersten Fall wurden die Passwörter der Benutzer versiegelt in einem verschlossenen Kasten aufbewahrt. Die Schlüssel zu ihm besaßen nur zwei Vertrauenspersonen. In dringenden Fällen konnte so auf den Computer eines kranken oder verreisten Kollegen zugegriffen werden. In einem anderen Fall hatte eine vertrauenswürdige Person Zugriff auf alle Dokumente. Kollegen konnten in dringenden Fällen über diese Person auf die notwendigen Dokumente zugreifen. Der dritte Fall beschreibt, wie die Zugriffskontrolle mit Hilfe von offenen Postfächern gelöst wurde. Diese stehen im Haupteingangsbereich einer Zeitungsredaktion, so dass Kollegen Informationen für den Betreffenden hinterlassen können. Hier schränkte die soziale Kontrolle den (illegitimen) Zugriff auf die Postfächer ein.

Ihre Beobachtungen fassen sie wie folgt zusammen:

- „Trusted third persons play an important role in the three scenarios"
- „Access can be subject to negotiation at the time of access"
- „Awareness can be used to control access"

Mit dem „Gewahr werden" (awareness) wird jedoch nur eine Seite des Kontrollmechanismus erfasst. Diese ist zwar eine notwendige, aber nicht hinreichende Bedingung, dass eine ex-post Kontrolle funktionieren kann. Hinzu kommt, dass ein Missbrauch, wie oben angedeutet wurde, bestraft und/oder, wie beim „Optimistic Security"-Ansatz, rückgängig gemacht werden kann. Wichtig sind bei ex-post Mechanismen immer der (soziale) Kontext, in dem diese angewandt werden.

Die Arbeit von Stiemerling und Wulf (2000) ist auch in der Hinsicht interessant, dass sie zeigen, dass bei den einzelnen Kontrollmechanismen nicht ein „entweder-oder", sondern ein „sowohl-als-auch" praktiziert wird. Im ersten Fall wird zum Beispiel die Zugriffskontrolle im voraus an Dritte delegiert, die sie dann aktuell aushandeln. Dadurch, dass der Betroffene von dem Zugriff erfährt, kann dieser ihn nachträglich auf seine Richtigkeit überprüfen.

Zwischenfazit: Folgerungen aus der Fallstudie

Aus den Geschäftszielen und dem Aufbau eines Unternehmens ergibt sich dessen Kerngeschäft und das seiner Organisationseinheiten. Angelegenheiten der zwischenbetrieblichen Kooperation, die in diesen Bereich fallen, werden dementsprechend kritischer beurteilt als die, die eher im Randbereich liegen. Beim Stahlwerk Bausig stellt die Regelung des Zugriff aufs elektronische Archiv, ein Privileg der internen Konstruktionsabteilung dar, insbesondere auch im Wettbewerb mit den externen Dienstleistern. Bedroht die Einführung eines externen Zugriffs auf das elektronische Archiv diesen „Wettbewerbsvorteil", wie dies in unserer Fallstudie der Fall ist, kann dies zu besonderen Spannungen führen.

Durch die Einführung von Telekooperationssystemen fallen physische Zugriffskontroll-Mechanismen weg, im Falle Bausig beispielsweise das Werkstor bei externem Zugriff auf das elektronische Archiv. Der Wegfall dieser Kontrollmechanismen hat zur Folge, dass interorganisatorische Spannungen virulent werden und dies sogar die Einführung von I.u.K.-Systemen verhindern kann. Sydow et al. (1995, S. 219) beschreibt einen solchen Fall aus der Versicherungsbranche: *„Es spricht einiges dafür, dass vor allem die großen Versicherer den unabhängigen Vermittlern den Zugriff auf bestehende Außendienst- bzw. Agentur-Informationssysteme weniger aus technischen als vielmehr aus* strategischen *Gründen auch weiterhin verleiden bzw. verweigern" [Hervorhebung im Orginal],* um so ihrem eigenen Außendienst einem Wettbewerbsvorteil zu erhalten. Um eine solche Entwicklung zu verhindern, muss die Gestaltung von Telekooperationssystemen die Gleichzeitigkeit von Kooperation und Konkurrenz ebenso in Rechnung stellen wie von organisationalen Vorgaben abweichende Arbeitspraxis.

Für die Implementierung eines Zugriffskontrollsystems für elektronische Archive in virtuellen Organisationen ergeben sich daraus u. E. zwei Konsequenzen. Zum einen muss ein solches Zugriffskontrollsystem den einzelnen Akteuren die Möglichkeit geben, eigenständig Zugriffspolitiken für einzelne Zuständigkeitsbereiche des elektronischen Archivs zu definieren. Dies erfordert eine mächtiges, aber intuitiv nutzbares Konfigurationswerkzeug. Zum anderen kann die Flexibilität des Zugriffskontrollsystems durch „uno-tempore" und „ex-post"-Mechanismen weiter erhöht werden. In der Fortsetzung dieses Beitrags wird eine komponenten-basierte Lösung vorgestellt, die dieser Anforderungen erfüllt.