Bundesamt
für Sicherheit in der
Informationstechnik

Vorstudie Grid Sicherheits-Infrastruktur (GSI)
Arbeitspaket 4:
Zusammenfassung der Ergebnisse

Version 3.4

Bundesamt für Sicherheit in der Informationstechnik
Postfach 200363
53133 Bonn
Internet: www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung

Das Grid-Computing hat sich aus Bestrebungen heraus entwickelt, die Ressourcen nationaler Supercomputing-Zentren zu verbinden und einfach nutzen zu können. Die „Rechenpower“ sollte so einfach zugreifbar sein, wie der elektrische Strom aus dem Stromnetz (engl. Power Grid). Auf diese Aspekte bezieht sich auch die frühe Definition des Grid-Computing [1] von Ian Foster und Carl Kesselman:

“A computational grid is a hardware and software infrastructure that provides dependable, consistent, pervasive, and inexpensive access to high-end computational capabilities.”

In dieser Definition steht der Aspekt einer technischen Infrastruktur im Vordergrund. Diese sollte eine zuverlässige, konsistente und kostengünstige Nutzung von Höchstleistungsrechnern quasi von „überall“ ermöglichen. Obwohl in dieser Definition nicht explizit genannt, ist die Überwindung der Domänengrenzen, zwischen technisch und rechtlich autonomer Organisationen, bereits ein wichtiges Thema.

Das BSI hat eine Vorstudie „Grid Security Infrastructure/ Grid Sicherheits-Infrastruktur (GSI)“ zu Status und Entwicklung der Grid-Technologie unter den Aspekten Sicherheit und Wirtschaftlichkeit durch SRC Security Research & Consulting GmbH unter maßgeblicher Mitwirkung von Experten der FH Köln sowie der LMU München erstellen lassen.

Das Ziel der Vorstudie war es, unter Verwendung von fünf ausgewählten Szenarien

- die Nutzbarkeit und Praktikabilität der Grid-Technologie über geschlossene Benutzergruppen in Unternehmen und Forschungseinrichtungen hinaus unter Sicherheitsaspekten zu bewerten,
- die Möglichkeiten und Grenzen der Bearbeitung und Speicherung kritischer Daten in Grid-Systemen zu ermitteln,
- einen Maßnahmenkatalog zu entwickeln, der das Sicherheitsniveau für die betrachteten Einsatzszenarien, die nicht über eine geschlossene vertrauenswürdige Benutzergruppe verfügen oder bei denen besonders kritische Daten bearbeitet oder gespeichert werden, verbessert und
- künftige Entwicklungen von Grid-Systemen bei der Implementierung der Sicherheitsmechanismen zu unterstützen.

Um diese Ergebnisse zu erarbeiten, wurden

- notwendige Mechanismen zum Schutz vertrauenswürdiger Daten in verteilten heterogenen Systemen (Grid-Systemen) analysiert,
- Vorgehensweisen zur Durchsetzung von Sicherheitspolitiken beim Einsatz von Grid-Systemen erarbeitet und
- Maßnahmen zum Schutz der Grid-Infrastruktur selbst abgeleitet. Die Maßnahmen wurden im Rahmen der Vorstudie so dargestellt, dass sie unabhängig von einer konkreten technischen Implementierung der Grid-Infrastruktur zu verstehen sind.

Die Erstellung der Risikoanalyse sowie die Definition von Maßnahmen zum Schutz der Grid-Infrastruktur stellte den Mittelpunkt der Studie dar.

Die Ergebnisse der Vorstudie wurden in drei Dokumenten (Arbeitspaketen) niedergelegt:

- ***Arbeitspaket 1: „Relevante Grid-Szenarien und ihr Schutzbedarf“, (vgl. [2])***

  Das Dokument gliedert sich in zwei Teile. Im ersten Teil wird ein Überblick über den aktuellen Stand der Grid-Technologie gegeben, die aktuell gebräuchlichsten Grid-Middleware Lösungen und vorhandene Sicherheitsmechanismen werden detailliert dargestellt. Der zweite Teil des Dokuments ist die beispielhafte Beschreibung

teilweise fiktiver Anwendungsszenarien für Grids (vgl. nachfolgendes Kapitel 2) und die Feststellung des im jeweiligen Szenario relevanten Schutzbedarfs.

- ***Arbeitspaket 2: „Risikoanalyse“, (vgl. [3])***

  Ergebnis dieses Arbeitspaketes ist die Beschreibung potenzieller Bedrohungen und Risiken zu den im vorangegangenen Arbeitspaket definierten Szenarien. Auf Risiken wird hier unter Angabe ihrer in [3] zugeordneten Nummer (Rx.y) Bezug genommen.

- ***Arbeitspaket 3: „Sicherheitsmechanismen“, (vgl. [4])***

  Auf der Basis der Ergebnisse der Risikoanalyse [3] werden im letzten Dokument Maßnahmen erarbeitet, die gegen die als besonders kritisch identifizierten Risiken wirken. Auf Maßnahmen wird hier unter Angabe ihrer in [4] zugeordneten Nummer (Mx.y) Bezug genommen.

Nachfolgend werden die Ergebnisse der einzelnen Arbeitspakete kurz zusammengefasst.

2 Darstellung der Szenarien

Im Rahmen der Studie wurden fünf beispielhafte Anwendungsszenarien der Grid-Technologie, die in [2] ausführlich beschrieben sind, definiert und bildeten die Grundlage für die Risikoanalyse und der Definition der Maßnahmen. Die gewählten Szenarien und deren charakteristische Merkmale werden nachfolgend kurz zusammengefasst.

2.1 Szenario 1: Unternehmensinternes Grid

Szenario 1 stellt ein derzeit vermutlich besonders häufig vorzufindendes Einsatzszenario für Grid-Technologien in Unternehmen dar. Unternehmensinterne Grids haben sich wegen des Erreichens der Leistungsfähigkeitsgrenze von Einzelkomponenten, besonders aber wegen der Forderung nach Optimierung der Ressourcenauslastung entwickelt und verbreitet. Bei Unternehmen, die im wesentlichen auf einen Standort konzentriert sind, lassen sich zwar häufig noch konventionelle IT-Infrastrukturen und entsprechende Prozesse nutzen. Größere Unternehmen und Konzerne, die an verschiedenen Standorten agieren und in ihrem Bereich vorhandenen Ressourcen standortunabhängig und/oder abteilungsübergreifend effizient nutzbar machen wollen, setzen hier aber zunehmend auf „*Service Oriented Architecture*“ und in diesem Zusammenhang auf Grid-Lösungen. Neben dem Zugriff auf zuvor nicht nutzbare oder nicht ausgelastete Rechnerressourcen (z. B. Arbeitsplatz-PCs der Mitarbeiter) kann damit auch der unternehmensweite und standortübergreifende Zugriff auf Anwendungen und Daten von Bedeutung sein.

Der Begriff „Unternehmen“ kann an dieser Stelle auch allgemeiner, etwa im Sinne von „Organisation“ oder auch „Business Unit“, aufgefasst werden, da das Szenario z. B. auch für organisatorisch selbständige Einheiten innerhalb eines Konzernverbunds zutreffen kann. Wichtig ist dabei, dass alle beteiligten Grid-Komponenten in Domänen mit verträglichen Policies oder sogar in der gleichen Domäne angesiedelt sind. Aus diesem Grund kann man hier von einem „Grid mit einheitlicher Policy“ sprechen, im Rahmen der Studie wird die Bezeichnung „unternehmensinternes Grid“ genutzt.

Vorteile dieses Szenarios sind unter anderem:

1. Die Mitwirkung Externer (also nicht zur Domäne oder zum Unternehmen Gehöriger) ist bei einem unternehmensinternen Grid nicht oder nur in relativ geringem Umfang (etwa bei der Bereitstellung sicherer Netze zwischen Standorten) erforderlich, wodurch die Gefahr der Weitergabe geschäftskritischer Daten minimiert wird.
2. Die Einrichtung eines unternehmensinternen Grids ist hinsichtlich der organisatorischen Umsetzung einfacher als bei (domänen- bzw.) unternehmensübergreifenden Lösungen.
3. Die in vielen Fällen vorhandene gesicherte Netzinfrastruktur über Unternehmensstandorte hinweg sowie eine gemeinsame Administration erleichtert die Einrichtung sowie Betrieb und Nutzung eines unternehmensinternen Grids.

Als charakteristisches Merkmal wurde in diesem Szenario die Nutzung nicht-Grid-spezifischer Komponenten (z. B. Arbeitsplatz-PCs) als Grid-Ressourcen identifiziert. Insbesondere bei der in diesem Szenario angenommenen Berechnung geschäftlich sensibler Daten ergeben sich Risiken bzgl. der Vertraulichkeit und Integrität dieser Daten, da hierfür ggf. nicht kontrollierbare Grid-Ressourcen genutzt werden. Es ergeben sich besondere Risiken aus der Betreuung der IT-Infrastruktur durch unterschiedliche Administratoren (z. B. durch Verletzung von definierten Policies), die durch organisatorische Maßnahmen reduziert werden können. Hervorzuheben ist in diesem Szenario, dass die relevanten Risiken nicht spezifisch für Grid-Umgebungen sind und sich durch die konsequente Umsetzung von z. B. Maßnahmen aus dem IT-Grundschutzhandbuch reduzieren lassen.

2.2 Szenario 2: Grid für den unternehmensübergreifenden industriellen Einsatz

Szenario 2 stellt eine Erweiterung von Szenario 1 dar, bei der die eigenen Ressourcen der Organisation durch Ressourcen eines Dienstleisters erweitert werden. Im Gegensatz zu Szenario 1 werden hier also insbesondere Domänen unterschiedlicher Unternehmen zu einem Grid zusammenfügt. Aus dem Blickwinkel der Risikoanalyse ergibt sich hier das Problem, dass der Nutzer des Dienstleisters keinerlei organisatorischen Durchgriff auf die Mitarbeiter des Dienstleisters hat und somit alle Sicherheitsanforderungen im Rahmen der Vertragsverhandlungen fixiert werden müssen. Sicherheitsanforderungen müssen hier somit vor Vertragsformulierung ermittelt worden sein.

Dieses Szenario des „unternehmensübergreifenden Einsatz von Grid-Technologien“ ist besonders für miteinander kooperierende Unternehmen von zunehmendem Interesse, also z. B. bei der Zusammenarbeit zwischen einem großen Konzern und seinen Zulieferern im Rahmen der gemeinsamen Entwicklung von Produkten oder deren Komponenten. Ein weiterer Anwendungsfall ist das Abfangen von Lastspitzen in Unternehmen, indem dann Ressourcen von Dritten angemietet und in das Grid integriert werden. Fasst man den Begriff „Unternehmen“ allgemeiner (im Sinne von „Organisation“ oder auch „Business Unit“), so kann das hier beschriebene Szenario auch z. B. für die Kooperation organisatorisch selbständiger Einheiten innerhalb eines Konzernverbunds zutreffen. Wesentliches Kennzeichen ist dabei, dass die beteiligten Domänen nicht mit einheitlichen Policies betrieben werden. Im Rahmen der Studie wird die Bezeichnung „unternehmensübergreifendes Grid“ verwendet.

Mehrere Unternehmen verbinden dabei über Grid-Technologien Teile ihrer IT-Infrastruktur. Dazu müssen natürlich Domänen und Policies geeignet definiert und realisiert werden. Einen Ansatz dazu bietet z. B. IBM mit dem „Computing-on-demand-Modell“.

Das Szenario ist dadurch charakterisiert, dass Grid-Ressourcen (insbesondere die durch den Dienstleister zur Verfügung gestellten) von im Wettbewerb zueinander stehenden Unternehmen genutzt werden. Allerdings besteht die Möglichkeit, konkrete vertragliche Vereinbarungen im Rahmen eines Service Level Agreements zu treffen und somit die Umsetzung von Sicherheitsmaßnahmen vorab zu vereinbaren. Hierüber lässt sich dann z. B. ein zu erreichendes Sicherheitsniveau definieren. In diesem Szenario stellt sich die Innentäterproblematik als besonders kritisch dar, da ein Innentäter im Bereich des Dienstleisters mit geringem Aufwand großen Schaden verursachen kann und der Kunde des Dienstleisters keine Kontrolle über die Mitarbeiter des Dienstleisters hat. Neben der sorgfältigen Formulierung von Sicherheitsanforderungen in Verträgen kommen möglicherweise die zukünftigen Technologien des Trusted Computing als wirksame Maßnahme gegen die identifizierten Risiken in Frage.

2.3 Szenario 3: Offenes e-Science Grid

Die Entwicklung von Grid-Technologien wurde zunächst vor allem durch den Bedarf verschiedener Wissenschaftsbereiche nach besseren Kooperationsmöglichkeiten und nach besserer Nutzung teurer Ressourcen (insbesondere von Höchstleistungsrechnern) vorangetrieben. Bei den Kooperationsmöglichkeiten stand (und steht) die effiziente gemeinsame wissenschaftliche Arbeit eines Teams im Vordergrund, welches an entfernt voneinander angesiedelten Standorten an einer gemeinsamen Aufgabenstellung arbeitet. Sicherheitsfragen spielen bisher eine untergeordnete Rolle. Zur besseren Ausnutzung teurer und knapper Ressourcen wurde stets die transparente Einbindung „externer“ Ressourcen in die jeweils eigene Infrastruktur angestrebt – zunächst durch standort- bzw. organisationsübergreifend gebildete „Cluster“, dann durch Ressourcen-Verbünde und schließlich durch die Bildung von Grids.

Ein Beispiel für ein offenes e-Science Grid ist das Large Hadron Collider (LHC) Computing Grid, dessen Ausbau und Entwicklung im Europäischen Projekt „EGEE1“ (Enabling Grids for E-sciencE, 01.04.2004 bis 31.03.2006; seit 01.04.2006 gefolgt von „EGEE2“) vorangetrieben wird. Eine Folge dieser Entwicklung ist, dass die wissenschaftliche Nutzung von offenen Computing-Grids nach wie vor eines der am weitesten verbreiteten Anwendungsszenarien ist. Aus diesem Bereich stammen auch zahlreiche Entwicklungen von Grid-Technologien.

Anders als bei einer wirtschaftlichen Nutzung in Unternehmen steht bei der wissenschaftlichen Nutzung nicht die Sicherheit von kritischen Daten im Vordergrund (wenngleich natürlich Forschungsergebnisse bis zu ihrer Veröffentlichung oft vertraulich gehalten werden müssen), sondern die effiziente Nutzung benötigter, oft weltweit verteilter Ressourcen. Ein besonderes Merkmal der wissenschaftlichen Nutzung ist die Notwendigkeit, den Nutzern

das Einbringen selbst entwickelter Software zu ermöglichen. Dadurch erhöht sich das Risiko, dass schädliche Programmcodes in das Grid gelangen und schnell verbreitet werden.

Bei der wissenschaftlichen Arbeit sind insbesondere die vom Benutzer selbst entwickelten Programme häufig ein wesentlicher Bestandteil. Sehr restriktive Regelungen für das Einbringen der zugehörigen ausführbaren Codes in ein Grid sind in diesem Umfeld oft nicht praktikabel und werden daher meist nicht akzeptiert.

Gleichzeitig muss dem allgemein vorhandenen Schutzbedarf der Daten und Benutzerprogramme Rechnung getragen werden. Es ist daher von wichtig, dass die Benutzerverwaltung und die Abgrenzung der Benutzer (Mandantenfähigkeit) untereinander durchgesetzt wird.

Ein Hauptmerkmal dieses Szenarios ist somit der Kompromiss zwischen der einerseits möglichst unkomplizierten Bereitstellung hoch performanter Ressourcen für eine sehr große Zahl häufig wechselnder Nutzer und andererseits dem Bedürfnis, nicht autorisierte Zugriffe auf Ressourcen und die Manipulation wissenschaftlicher Daten im erforderlichen Umfang zu verhindern. Ein besonderes Risiko geht in diesem Szenario von der Phase der Bildung des Grid aus, bei dem die Partner sorgfältig ausgewählt und verbindliche Policies vereinbart werden müssen, und der teilweise sehr komplizierten Benutzerverwaltung. Wie bereits erwähnt ist ein weiteres Risiko das mögliche Auftreten maliziöser Software. In einem Forschungs-Grid ist es ein übliches Szenario, dass Forscher Software für andere Nutzer zur Verfügung stellen. Um jedoch das Know-how zu schützen, werden vielfach nicht die Softwarequellen selbst, sondern Binärdateien verwendet. Hier ist es dem Nutzer nicht mehr möglich, einen maliziösen Charakter zu erkennen. Wie in Szenario 1 ist auch hier hervorzuheben, dass die relevanten Risiken nicht spezifisch für Grid Umgebungen sind und sich durch die konsequente Umsetzung von z. B. Maßnahmen aus dem IT-Grundschutzhandbuch reduzieren lassen.

2.4 Szenario 4: Grids mit personenbezogenen bzw. personenbeziehbaren Daten (z. B. MammoGrid)

In diesem Szenario stehen die Speicherung und Verarbeitung personenbezogener Daten im Grid sowie die daraus resultierenden Risiken im Mittelpunkt. Personenbezogene Daten genießen aufgrund von Gesetzen, Verordnungen, Datenschutzrichtlinien etc. einen besonderen Schutz durch den Gesetzgeber. So ist z. B. beim Umgang mit Patientendaten im Strafrecht §203 StGB die ärztliche Schweigepflicht und das Patientengeheimnis streng geregelt: "Wer unbefugt ein fremdes Geheimnis,....offenbart,... wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft." Dies muss selbstverständlich auch bei Nutzung von Grid-Technologie umgesetzt werden.

Daraus ergeben sich insbesondere Anforderungen an die Vertraulichkeit dieser Daten, die Sicherstellung eines definierten Zugriffsschutzes sowie dessen Protokollierung.

Das Gesundheitswesen und die biomedizinische Forschung können hier als typisches Beispiel für die Verarbeitung personenbezogener Daten dienen. Problematisch kann die Nutzung solcher Daten vor allem in der Forschung werden, da hier bei anderen Szenarien ein nur überwiegend geringer Schutzbedarf bzgl. der Vertraulichkeit der verarbeiteten und gespeicherten Daten festgestellt wurde. Durch geeignete Schutzmaßnahmen muss man den scheinbaren Widerspruch zwischen möglichst großer Offenheit der e-Science-Grids und den hohen Schutzanforderungen an die Daten überwinden. Bewährte Maßnahmen sind z. B. Anonymisierung oder Pseudonymisierung der Personendaten.

Bei medizinischen Studien muss den teilnehmenden Patienten ein jederzeitiges und auch teilweises Widerrufsrecht eingeräumt werden. Wünscht ein Patient sich nicht weiter zu beteiligen, so sind die zu seinem Fall angelegten Daten nachvollziehbar zu löschen. Derzeit sind in virtualisierten Speicherressourcen (mit automatischer Replikation zur Ausfallsicherheit) keine Mechanismen bekannt, die dieses zuverlässig umsetzen. Falls der Patientenwunsch sogar so weit geht, dass er die Verarbeitung „seiner“ Daten auf Rechnern eines bestimmten Rechenzentrums nicht möchte, so kann dies derzeit im Rahmen der verfügbaren Grid-Technologie nicht geleistet werden. In diesem Szenario ist somit die Personenbezogenheit der Daten ein Kernproblem und die Gewährleistung von Vertraulichkeit und Integrität dieser Daten steht im Mittelpunkt. Daher wird hier besonderer Wert auf entsprechende Verpflichtungen der Administratoren, auf wirksame Authentisierungsmechanismen und auf entsprechende Auditing-Funktionen gelegt.

2.5 Szenario 5: Sicherheitskritisches national wichtiges Grid / Katastrophenschutz (K-Grid)

Das fünfte Szenario fällt im Vergleich zu den anderen betrachteten Szenarien aus dem Rahmen, da eine Grid-Infrastruktur („K-Grid“) zu analysieren war, die im Krisenfall („K-Fall“: Umweltkatastrophen, Verteidigungsfall, terroristische Anschläge etc.) in der Lage sein soll, umfangreiche Ressourcen (Rechen-, Daten-, Kommunikationsressourcen usw.) kurzfristig und zuverlässig verfügbar zu machen. Die Ressourcen stehen dabei nicht notwendig bereit, sondern müssen bei Bedarf sehr kurzfristig verfügbar gemacht werden. Hieraus resultiert für dieses Szenario insbesondere die Notwendigkeit einer intensiven Planungs-/Konzeptphase.

Die Ressourcen können also im Normalfall zu sehr unterschiedlichen Einrichtungen und damit Domänen mit im allgemeinen wenig koordinierten Policies gehören und nicht als Grid bzw. in einem gemeinsamen Grid betrieben werden. Erst im Krisenfall muss das K-Grid seine Funktionsfähigkeit erhalten, dann jedoch sehr kurzfristig seinen definierten Zustand (d. h. sowohl technisch als auch organisatorisch) erreichen.

Bezogen auf die Schutzbedarfsfeststellung ist hierbei die genaue Ausrichtung des Grid relevant. Dem gegenüber steht der derzeit noch eher fiktive Charakter dieses Szenarios. K-Grids sind derzeit nur in Teilaspekten in der Praxis zu finden, so dass für die vorliegende Studie Annahmen getroffen werden mussten, um ein solches Szenario mit Zukunftspotenzial überhaupt untersuchen zu können. Ausgehend von den Annahmen können sich sehr unterschiedliche Schutzbedarfsprofile ergeben. Sind bei einem Grid bspw. für die Verarbeitung von Umweltdaten (im Fall von Umweltkatastrophen) die Eingangsdaten lediglich hinsichtlich ihrer Integrität schützenswert und die Ergebnisdaten hinsichtlich ihrer (kurzfristigen) Verfügbarkeit, so sind Eingabedaten im Verteidigungsfall auch bezogen auf ihre Vertraulichkeit mit einem hohen Schutzbedarf zu belegen, da diese Daten ggf. strategische Informationen beinhalten.

Im Rahmen der Vorstudie wurde das Szenario „Umweltkatastrophe“ zugrunde gelegt. Ziel der Nutzung des Grid ist z. B. die Berechnung des Verlaufes von Hochwasser an Flüssen und die damit verbundene Koordinierung von Einsatzkräften zur Katastrophenbekämpfung und dem Bevölkerungsschutz. Insbesondere die Ergebnisdaten und die zur Ermittlung dieser Daten erforderlichen Eingabe- und Basisdaten genießen in diesem Szenario einen besonderen Schutz. Das eigentliche Hauptrisiko des Verlustes der Verfügbarkeit wurde in der Risikoanalyse nicht betrachtet, da die Verfügbarkeit im Bedarfsfall durch entsprechende Maßnahmen in der Konzeptionsphase und regelmäßige Krisenübungen gewährleistet werden muss. Die wesentlichen Gefahren resultieren in diesem Szenario aus der Verletzung der Vertraulichkeit und Integrität von Gefahrmeldungsdaten. Ursache einer Verletzung der Vertraulichkeit sind hier z. B. eine nichtberechtigte Weitergabe dieser Daten durch Einsatzkräfte oder das Versagen von vorhandenen Authentikationsmechanismen. Aus diesem Szenario lässt sich somit insbesondere die Notwendigkeit verlässlicher starker Authentikationsmechanismen ableiten. Es ist hervorzuheben, dass sich die Maßnahmen bei diesem Szenario stark im Bereich von Gesetzen/Verordnungen/Verträgen, im regelmäßigen Üben des Herstellens der Grid-Funktionalität auf Basis von sonst eher eigenständig eingesetzten Ressourcen und im Sicherstellen der Datenintegrität bewegen. Daneben ist unbedingt sicherzustellen, dass die als Administratoren eingesetzten Personen die nötige Eignung und Verlässlichkeit besitzen.

3 Risiken, Bedrohungen und Maßnahmen

3.1 Szenario 1: Unternehmensinternes Grid

Die wesentlichen Risiken im Szenario 1 gehen von Innentätern mit krimineller Intention aus. Sind neben den „üblichen“ Sicherheitsmechanismen keine zusätzlichen Maßnahmen gegen Innentäter getroffen, geht insbesondere von Personen mit besonderen Rechten (Administratoren) eine erhöhte Gefahr aus. Auch sind hierunter Risiken, die aus Nach- oder Fahrlässigkeit sowie Vorsatz entstehen, zu behandeln. Für diese Situationen müssen zusätzliche Maßnahmen, wie sie derzeit im Grid-Umfeld noch nicht verfügbar sind, umgesetzt werden.

Insbesondere der in diesem Szenario angenommene Einsatz „normaler“ Büro-Arbeitsplatz-Systeme (PC) als Grid-Ressource (Computing-Ressource) ist hier für die Sicherheitsbetrachtung interessant. Da Arbeitsplatz-Systeme inzwischen Multi-User fähig sind und geeignete Rechteverwaltungen besitzen, ist bei sorgfältiger Konfiguration nicht von einem erfolgreichen lokalen Angriff über das System selbst auszugehen. Erfolgversprechender für einen gezielten Angriff sind in diesem Szenario vielmehr Angriffe auf die Netzwerkinfrastruktur (z. B. Netzwerkdosen innerhalb der Büros). Sofern physikalischer Zugang zur Netzwerkinfrastruktur erlangt werden kann, ist der Aufwand für das gezielte Abhören sensibler Daten mit geringem Aufwand möglich (vgl. R1.2[3]). Der Schutz der physikalischen Netzwerkinfrastruktur ist daher ein wesentliches Ziel, welches sich auch in anderen Szenarien wiederfindet.

Aus der Kombination fehlender physikalischer Absicherung und dem Angriff auf die IT-Infrastruktur (vgl. z. B. R1.3[3]) können in diesem Szenario Schäden entstehen. Zusätzlich zu Risiken, die auf den physikalischen Gegebenheiten aufbauen sind Innentäter mit weitreichenden Rechten (Administratoren) in diesem Szenario als potenzielle Angreifer zu nennen (vgl. z. B. R1.7[3]). Lokale Nutzer, deren Arbeitsplatz-System als Grid-Ressource genutzt wird, kommen hingegen primär nicht als Angreifer in Betracht (vgl. z. B. R1.2, R1.10[3]). Lediglich das Abhören der Kommunikationsverbindung ist diesem Personenkreis mit einfachen Mitteln möglich, da sie ggf. Zugang zur Netzwerkinfrastruktur besitzen und daher mit geringem Aufwand die Kommunikation zu und von ihrem Arbeitsplatz-System abhören können (vgl. R1.2[3]).

Bei der Betrachtung von Maßnahmen liegt der Schwerpunkt bei den organisatorischen Maßnahmen (z. B. Verpflichtung der Mitarbeiter auf Einhaltung von Security-Policies, Einrichtung einer übergeordneten Administration [„Super-Administrator“]). Mögliche technische Maßnahmen in diesem Bereich stammen aus dem Umfeld zukünftiger Methoden des Trusted Computing, wobei hier jedoch derzeit nicht abschätzbar ist, inwieweit solche Mechanismen in Zukunft auch im Bereich des Grid-Umfelds einsetzbar sind.

3.2 Szenario 2: Grid für den unternehmensübergreifenden industriellen Einsatz

Von besonderem Interesse in Szenario 2 ist der Schutz von Unternehmensdaten, da diese Daten innerhalb der Domäne des Dienstleisters verarbeitet und dort prinzipiell – z. B. durch Mitarbeiter des Dienstleisters – kompromittiert werden können. Durch die im Szenario vorausgesetzte Annahme, dass „State-of-the-Art“ Sicherheitsmaßnahmen ergriffen wurden, reduziert sich dieses Risiko im wesentlichen auf die Ausnutzung von Schwachstellen innerhalb der angenommenen Grid-Middleware oder des eingesetzten Betriebssystems. Auch in diesem Szenario müssen gezielte Angriffe durch Personen mit besonderen Zugriffsrechten angenommen werden (vgl. R2.4[3]).

Neben den durch Innentäter verursachten Risiken wird in diesem Szenario insbesondere der Prozess der Bildung des Grid relevant (vgl. z.B. R2.1[3]). Fehler im Auswahlprozess eines Dienstleisters können schwerwiegende Folgen für die Vertrauenswürdigkeit des Grid haben, so dass Vertraulichkeit, Integrität und Verfügbarkeit der Daten und des Grid ggf. nicht gewährleistet werden können. Im Rahmen des Prozesses der „VO-Bildung“ (Bildung einer Virtuellen-Organisation) wird der Grundstein der Sicherheit des Grid gelegt. Nur durch eine sorgfältige VO-Bildung kann davon ausgegangen werden, dass das Grid als „vertrauenswürdig“ angesehen werden kann. Selbst wenn davon ausgegangen wird, dass ein geeigneter Dienstleister ausgewählt wurde, müssen Maßnahmen ergriffen

werden, welche die Einhaltung des vertraglich vereinbarten Sicherheitsniveaus über die Zeit sicherstellen. Defizite lassen sich insbesondere im Bereich der Organisation und der Überwachung des Grid – und der Einhaltung des SLA – finden (vgl. z. B. R2.1). Aus diesem Szenario wurde die Anforderung abgeleitet, ein zentrales Sicherheitsmanagement zu etablieren und so das Grid einer regelmäßigen und kontinuierlichen Überwachung zu unterziehen.

Die Analyse des Szenarios hat ergeben, dass die Wirksamkeit der umgesetzten Sicherheitsmechanismen maßgeblich von der Auswahl eines geeigneten Dienstleisters (vgl. z. B. R2.1) und der sorgfältigen Administration aller Komponenten/Ressourcen (vgl. z. B. R2.9) abhängt. Auch die Tatsache, dass die lokal wirkenden Administratoren ohne großen Aufwand jeden denkbaren Angriff durchführen können (vgl. z. B. R2.7), ist im Kontext des Szenarios als kritisch anzusehen. Dies ist jedoch ein – auch außerhalb des Grid-Kontextes – bekanntes und derzeit mit technischen Mitteln nur schwer zu lösendes Problem. An dieser Stelle sind organisatorische Maßnahmen und erweiterte technische Maßnahmen (z. B. Nutzung von HSM – Hardware-Sicherheits-Modulen) zur Risikoeindämmung erforderlich.

Neben der sorgfältigen Auswahl von Dienstleistern und der hiermit verbundenen vertraglichen Vereinbarung zur Einhaltung von Sicherheitsmechanismen und Vertraulichkeit zeigt sich in diesem Szenario insbesondere die Relevanz der Notwendigkeit verbindlicher Vereinbarungen zwischen den einzelnen Domänen eines Grid (organisatorische Maßnahme) und der Erfordernis, technischer Maßnahmen zur wirkungsvollen Unterstützung dieser Vereinbarungen einzusetzen. Die zu ergreifenden technischen Maßnahmen müssen gegen Innentäter (hier insbesondere Administratoren des Dienstleisters) wirken und können wie im vorangegangenen Szenario 1 aus dem Umfeld des Trusted Computing stammen.

An diesem Szenario wird ein Grundproblem des Grid-Computing besonders deutlich. „Rechenleistung aus der Steckdose“ bedingt den Transport von Eingabedaten zu den Rechenknoten, ebenso die Erzeugung und Speicherung der Ergebnisdaten auf den Rechenknoten, die nicht notwendigerweise unter der Kontrolle des Nutzers stehen. Zwischen den Rechenknoten können entsprechend dem Grid-Paradigma beliebige räumliche Distanzen liegen und es muss davon ausgegangen werden, dass diese unter fremder administrativer Kontrolle stehen. Besitzen diese Daten einen erhöhten Schutzbedarf (etwa vertrauliche Forschungs- oder Entwicklungsdaten), so sind derzeit keine technischen Lösungen verfügbar, die eine unbefugte Manipulation in der fremden Domäne zuverlässig verhindern. Prinzipbedingt hat der Administrator eines Systems Zugriff auf alle Ressourcen des Systems, und zwar auf allen Ebenen. Dies schließt im Allgemeinen auch sämtliche Daten auf dem System ein.

Maßnahmen zur Erhöhung des Aufwands einer Manipulation sind denkbar, z. B. indem Eingabedaten verschlüsselt übertragen und auf der Grid-Ressource ebenfalls verschlüsselt gespeichert werden. Erfolgt die Entschlüsselung erst im Hauptspeicher der Grid-Ressource unter Zuhilfenahme von Hardware-Sicherheitsmodulen (HSM), kann das Risiko für die Manipulation kritischer Daten durch einen lokalen Administrator etwas verringert werden. Eine darüber hinaus gehende wirksame Maßnahme auf technischer Ebene ist derzeit noch nicht verfügbar, könnte aber im Rahmen zukünftig verfügbarer Mechanismen aus dem Umfeld des Trusted Computing stammen.

3.3 Szenario 3: Offenes e-Science Grid

In diesem Szenario steht der angenommene relativ geringe Schutzbedarf der betrachteten Objekte im Vordergrund, so dass nur wenige kritische Risiken identifiziert werden konnten. Risiken, die aus gezielten Angriffen von Personen ohne Zugriffsberechtigung hervorgehen, werden durch vorhandene und etablierte Sicherheitsmechanismen (Authentikation, bauliche Sicherheit, Zugriffsschutz) stark eingeschränkt. Die Insider-Problematik stellt sich wie in den übrigen Szenarien als kritisch dar.

In diesem Szenario tritt in der Betrachtung der Risiken, insbesondere der Prozess der Organisation des Grid, in den Mittelpunkt, also die Phase, während der das Grid gebildet wird. Wie bereits in Szenario 2 lassen sich Defizite und Risiken im Bereich der Organisation des Grid, innerhalb des Prozesses der Bildung virtueller Organisationen (VO), finden (vgl. z. B. R2.1 und R3.1). Bei der Betrachtung der Sicherheitsmechanismen fällt in diesem Szenario auf, dass kein Domänen-übergeordnetes Sicherheitsmanagement implementiert ist und wichtige Sicherheitsprozesse (z. B. regelmäßiges Audit der Grid-Infrastruktur und der etablierten Sicherheitsmaßnahmen) fehlen. Vor dem Hin-

tergrund der „Offenheit“ und „Virtualität“ eines Grid im universitären Umfeld erscheint dieses Defizit plausibel und nachvollziehbar. Innerhalb des betrachteten Grid fehlt die Rolle eines übergeordneten Verantwortlichen und damit fehlen die in einem Sicherheitsmanagement etablierten – und strengen – Prozesse und Mechanismen, mit denen ein definiertes Sicherheitsniveau erst erreicht und aufrecht erhalten werden kann. Dieses Defizit gilt grundsätzlich für alle betrachteten Szenarien und ist kein Problem, welches für ein einzelnes Szenario spezifisch ist. In diesem Szenario jedoch wird das Defizit besonders deutlich. Als ein in den übrigen Szenarien nicht vorhandenes Risiko sind Schäden durch maliziöse Software zu erwähnen (vgl. R3.19), welche durch Angreifer in das Grid eingeschleust wird.

Eine grundsätzlich wirksame Maßnahme in diesem Szenario wäre die Einführung übergeordneter Managementstrukturen in Teilbereichen der Organisation. Neben dem bereits in Szenario 2 erwähnten übergeordneten Sicherheitsmanagement kommen in Szenario 3 auch Anforderungen an ein übergeordnetes IT-Management zum Tragen.

Insbesondere ein übergeordnetes Benutzer-Management stellt sich als potenzielles Risiko dar (vgl. z. B. R3.17). Innerhalb der Grid-Middleware existieren Mechanismen zur Benutzerberechtigung, die für jede Ressource auf lokale Berechtigungen abgebildet („gemappt“) werden müssen. Eine Grid-Benutzerkennung *USER123* kann z. B. auf der Ressource „Datenbank“ auf eine Sammel-/Gruppenkennung *DBUSER987* abgebildet werden, so dass hier potenziell die Möglichkeit besteht, dass auch ein Grid-Benutzer *USER987* auf den Benutzer *DBUSER987* abgebildet wird und somit auf der Ressource Zugriff auf Daten des Nutzers *USER123* besitzt. Dieses Risiko lässt sich hier durch eine (teilweise) übergeordnete Rechteverwaltung (z. B. durch Einsatz des *Community Authorization Service*, CAS) reduzieren (vgl. M3.5). Das auch in diesem Szenario vorhandene Risiko der Innentäter kann insbesondere hier durch entsprechende Verpflichtungserklärungen der Administratoren und den Einsatz zukünftiger Methoden aus dem Umfeld des Trusted Computing (vgl. z. B. M3.1b, M3.4) reduziert werden. Der durch Signierung unterstützte Einsatz lediglich freigegebener Software (vgl. M3.6) schützt in diesem Szenario vor maliziöser Software.

3.4 Szenario 4: Grids mit personenbezogenen bzw. personenbeziehbaren Daten (z. B. MammoGrid)

Die Verarbeitung personenbezogener und personenbeziehbarer Daten im medizinischen Umfeld zeichnet dieses Szenario aus. Insbesondere Risiken, welche die „informationelle Selbstbestimmung“ gefährden, werden hier betrachtet. Die hohen Eintrittswahrscheinlichkeiten für Risiken, als deren Verursacher Personen mit besonderen Rechten (Administratoren, z. B. R4.3 und R4.7) in Frage kommen, sind in diesem Szenario hervorzuheben, da hier eine Häufung vorliegt. Das Schadensausmaß und die Eintrittswahrscheinlichkeit von Risiken aus diesem Bereich hängt sehr stark von der Intention und der Vertrauenswürdigkeit der Verursacher ab. Stammt ein Angreifer z. B. aus dem Bereich der Administratoren, versagen die üblichen technischen Maßnahmen, da Administratoren unbeschränkten physischen und logischen Zugriff auf Ressourcen haben. Wie bereits in den vorangegangenen Szenarien erläutert, sind in diesem Bereich organisatorische Maßnahmen zu ergreifen, mit denen sichergestellt werden kann, dass mit hoher Wahrscheinlichkeit kein Angriff von diesem Personenkreis ausgeht.

Das bereits in Szenario 3 angerissene Risiko das „Identity-Mapping“ lässt sich aufgrund des hohen Schutzbedarfs für personenbezogene Daten in diesem Szenario als relevant und kritisch identifizieren, da hierdurch ein unberechtigter Zugriff auf schützenswerte Daten möglich ist. Eine in diesem Szenario spezifische Bedrohung geht z. B. vom Schutz sog. Pseudonymisierungstabellen aus. Häufig wird der Personenbezug zu relevanten Daten (Krankheitsbild, Anamnese, etc) durch ein Pseudonym ersetzt. Eine Wiederherstellung des Personenbezugs kann durch sog. Pseudonymisierungstabellen erfolgen, die eine eindeutige Abbildung zwischen Person und Pseudonym erlauben, woraus sich ein erhöhter Schutzbedarf für diese Tabellen ergibt. Das Risiko der Kompromittierung dieser Pseudonymisierungstabellen (vgl. z.B. R4.8) wird im Szenario untersucht, wobei insbesondere Innentäter potenziell sowohl Zugriff auf die Pseudonymisierungstabellen wie auch die pseudonymisierten Daten haben (z. B. Administratoren).

Es wird deutlich, dass in diesem Szenario dem Datenschutz besondere Aufmerksamkeit gewidmet werden muss. Daher wird hier besonderer Wert auf entsprechende Verpflichtungen der Administratoren, wirksame Authentisie-

rungsmechanismen und auf entsprechende Auditing-Funktionen gelegt, so dass den Ansprüchen des Datenschutzes Rechnung getragen werden kann. Daneben kann das Risiko mangelhafter Rechteverwaltungen durch den Einsatz von CAS verringert werden.

Eine wirksame Maßnahme, um auf technischer Ebene Schutz gegen unbefugten Zugriff durch Administratoren zu gewährleisten, ist derzeit auch in diesem Umfeld noch nicht verfügbar. Auch hier sind zukünftig verfügbare Mechanismen aus dem Umfeld des Trusted Computing denkbar.

3.5 Szenario 5: Sicherheitskritisches national wichtiges Grid / Katastrophenschutz (K-Grid)

Der hohe Schutzbedarf bezüglich Vertraulichkeit und Integrität der Ergebnisdaten hat weit reichende Folgen und stellt in diesem Szenario den Schwerpunkt der Untersuchungen dar. Nur durch integere Ergebnisdaten können durch die Einsatzkräfte wirksame Maßnahmen getroffen werden, und nur wenn die Ergebnisdaten verfügbar sind, kann über die zu ergreifenden Maßnahmen entschieden werden. Im Umkehrschluss bedeutet dies, dass alle Bedrohungen, die die Integrität oder Verfügbarkeit der Ergebnisdaten oder der Grid-Infrastruktur beeinträchtigen, ein hohes bis sehr hohes Schadenspotenzial haben. Aufgrund der Relevanz der Ergebnisdaten können bereits kleine und leicht durchzuführende Manipulationen gravierende Auswirkungen haben und den Schutz z. B. der Bevölkerung gefährden.

Das Vorhandensein wirksamer starker Authentikationsmechanismen wird in diesem Szenario zwar angenommen, jedoch ist diese Annahme bei genauerer Betrachtung zu hinterfragen. Für den Feldeinsatz oder den Einsatz unter Stress ist die Nutzung derzeit verfügbarer starker Authentikationsmechanismen fraglich und ggf. separat zu analysieren. Im Rahmen dieser Risikoanalyse wurden solche Aspekte dahingehend betrachtet, dass deaktivierte Authentikationsmechanismen die unberechtigte Nutzung von Endgeräten (z. B. durch Passanten) und Weitergabe von vertraulichen Ergebnisdaten zur Folge hat.

Durch in der Praxis übliche redundante Auslegung von IT-Systemen und Kommunikationsstrecken kann die erforderliche technische Verfügbarkeit des Grid sichergestellt werden. Aufgrund ebenfalls üblicher Katastrophenübungen kann zudem sichergestellt werden, dass die Bildung des Grid im Bedarfsfall wie geplant erfolgen kann (*Proof of Concept*). In diesem Szenario muss jedoch explizit die (technische) Bildung des Grid in solche Katastrophenübungen einbezogen werden.

Ein wesentliches Ziel des Szenarios ist es, die betroffene Bevölkerung zu schützen, bzw. den Schaden zu reduzieren. Hierzu ist es – wie bereits erläutert – erforderlich, dass die für die Entscheidungen relevanten Ergebnisdaten, verfügbar und integer sind. Aufgrund des auf Innentäter zurückzuführenden hohen Schadenspotenzials müssen insbesondere Maßnahmen gefunden werden, die die Innentäterproblematik auch unter den erschwerten Bedingungen eines Katastrophenszenarios reduzieren. Es sind damit insbesondere Maßnahmen erforderlich, die vorsätzliche Handlungen verhindern. Organisatorisch lässt sich das Vier-Augen-Prinzip für kritische Operationen anführen.

Die Innentäterproblematik und Relevanz der Ergebnisdaten spitzen sich im hochkritischen Risiko der unberechtigten Weitergabe von Ereignisdaten zu. Dieses Risiko stellt z. B. den Fall einer unberechtigten oder ungewollten Weitergabe von Ergebnisdaten durch die Leitstelle und einer daraus resultierenden Panik innerhalb der betroffenen Bevölkerungsteile dar. Die Erreichung des Hauptziels „Schutz der Bevölkerung“ ist damit stark gefährdet.

Die erforderlichen Maßnahmen zur Eindämmung der identifizierten Risiken bewegen sich hier stark im Bereich von zu erstellenden Gesetzen/Verordnungen/Verträgen, im regelmäßigen Üben des Herstellens der Grid-Funktionalität auf Basis von sonst eher eigenständig eingesetzten Ressourcen einschließlich entsprechender Sicherstellung der Verfügbarkeit und des „sicheren“ Grid-Abbaus und im Sicherstellen der Datenintegrität, u. a. durch Gewährleistung der Authentizität der zugreifenden Personen. Daneben ist es unabdingbar sicherzustellen, dass die agierenden Personen die nötige Eignung und Verlässlichkeit besitzen.

4 Fazit

Innerhalb eines Grid gibt es unterschiedliche Sicherheitsziele: Nutzer der virtuellen IT-Ressource Grid haben Anforderungen an die Vertraulichkeit und Integrität der Daten und der Verfügbarkeit des Grid selbst. Ressourcenprovider hingegen haben Anforderungen an die Vertraulichkeit, Integrität und Verfügbarkeit der von Ihnen zur Verfügung gestellten Grid-Ressourcen. Neben der Vereinbarung der technischen Rahmenbedingungen, die für die Funktionsfähigkeit des Grid erforderlich sind, besteht im Rahmen der Bildung der virtuellen Organisation die Möglichkeit, das zu erreichende Sicherheitsniveau zu definieren und verbindliche technische und organisatorische Policies zwischen allen beteiligten Partnern zu vereinbaren. Gelingt es, im Rahmen dieses Bildungsprozesses einen Sicherheitsprozess zu etablieren, sind die Voraussetzungen für ein vertrauenswürdiges Grid gegeben.

Ein vertrauenswürdiges Grid ist erforderlich, da einerseits ein Grid Nutzer Ressourcen verwendet, die Dritte zur Verfügung stellen, andererseits Ressourcenprovider ihre Ressourcen einem für sie „unbekannten Personenkreis“ überlassen. Vom Grad der Vertrauenswürdigkeit des Grid sind die vom Nutzer zu treffenden Sicherheitsmechanismen für die in das Grid einzustellenden Daten abhängig. Die Aufgabe der Ressourcenprovider ist es hierbei, einen möglichst hohen Grad an Vertrauenswürdigkeit mit technischen und organisatorischen Maßnahmen sicherzustellen, wobei die technische Absicherung im Vordergrund steht. Eine Vielzahl technischer Maßnahmen ist bereits Bestandteil existierender Grid-Middleware. Auf die Nutzung organisatorischer Maßnahmen soll zurückgegriffen werden, falls technische Maßnahmen nicht ausreichen, nicht implementierbar oder unwirtschaftlich sind. Die organisatorischen Maßnahmen werden hierbei ebenfalls bereits während der Phase der Bildung des Grid zwischen allen Beteiligten verbindlich vereinbart.

Im Rahmen der Vorstudie standen Risiken im Mittelpunkt, die die Vertrauenswürdigkeit des Grid reduzieren. Insbesondere wurden Risiken betrachtet, die durch Personen mit Zugang zu Grid-Ressourcen (Innentäter) verursacht werden. Die Innentäterproblematik stellt sich als Kernproblem innerhalb eines Grid dar, da aus Sicht eines Grid-Nutzers auch Personen außerhalb der eigenen Domäne zum Personenkreis der „Innentätern“ gehören. Dies ist mit der Virtualität eines Grid zu begründen, da aus Nutzersicht nicht direkt zu erkennen ist, in welcher Domäne und welche Grid-Ressourcen genutzt, auf welchen Ressourcen somit die eigenen (ggf. kritischen) Daten verarbeitet werden.

Die Ergebnisse der Vorstudie zeigen, dass drei Arten von Sicherheitsmechanismen genutzt werden können, um die identifizierten Risiken zu kontrollieren:

1. ***Organisatorische Maßnahmen im Rahmen der Bildung des Grid***

   Gegen bestimmte Risiken können derzeit keine technischen Maßnahmen ergriffen werden. Daher ist es erforderlich, im Rahmen der Bildung des Grid (oder der virtuellen Organisation) Domänen-übergreifend organisatorische Maßnahmen zu definieren, die während des gesamten Lebenszyklus gültig sind. Insbesondere die Definition und Etablierung eines geeigneten Sicherheitsprozesses sowie die Definition eines für die gesamte virtuelle Organisation gültigen Sicherheitsmanagement-Teams lässt sich als geeignete Maßnahme hervorheben. Zusätzlich sind die in anderen Bereichen üblichen Freigabemaßnahmen für Änderungen, Vier-Augen Prinzipien für kritische Aktionen oder unabhängige Audits als wirkungsvolle organisatorische Maßnahmen anzusehen, die die Sicherheit innerhalb eines Grid stärken.

2. ***Standard-Sicherheitsmaßnahmen***

   Standard-Sicherheitsmaßnahmen besitzen im Rahmen des Grid-Kontextes besondere Bedeutung. Aufgrund der anzunehmenden geografischen Verteilung der Grid-Ressourcen und der erforderlichen Datenkommunikation sind von Grid-Nutzern Risiken zu betrachten, die durch bewährte Mechanismen (z. B. VPN) ausgeschlossen werden können. Ebenso verhält es sich mit Maßnahmen, die üblicherweise für einen IT-Betrieb ergriffen werden. Durch einen geregelten IT-Betrieb kann das Vorhandensein technischer Schwachstellen verhindert (z. B.

durch das regelmäßige Aktualisieren der Systeme mit Hersteller-Patches) oder die Funktionsfähigkeit der Ressourcen (z. B. durch Systemüberwachungswerkzeuge) sichergestellt werden.

3. Grid-Middleware und Einsatzszenario-spezifische Sicherheitsmaßnahmen

Verschiedene Risiken resultieren aus den spezifischen Eigenschaften der eingesetzten Middleware. Gegen solche Risiken müssen dementsprechend spezielle Maßnahmen ergriffen werden, wie z. B. der Einsatz des Community Authorization Service (CAS) zur übergeordneten Verwaltung von Benutzerrechten. Ebenso verhält es sich mit Risiken, die aus dem jeweiligen Einsatzszenario resultieren (und als Maßnahme die Einbeziehung der betroffenen Mitarbeiter, deren Systeme als Grid-Ressource genutzt werden).

Es ist daher erforderlich, die in jedem Einsatzszenario auftretenden Risiken zu ermitteln und spezifische Maßnahmen zu definieren.

Insgesamt lässt sich als Ergebnis der Vorstudie feststellen, dass Sicherheitsaspekte im Grid-Umfeld – zumindest in der derzeitigen Praxis – noch nicht im Mittelpunkt stehen, sondern vielmehr funktionale Aspekte und Sicherheitsaspekte in einigen Einzelaspekten wie z.B. bei der Verschlüsselung mittels GridFTP berücksichtigt werden. Die derzeit im Einsatz befindlichen Grid-Systeme entstanden ursprünglich durch soziale Netzwerke, bei denen sich die einzelnen Beteiligten kennen oder vertrauen. Es ist davon auszugehen, dass zukünftig die Anzahl der Ressourcenprovider und die räumliche Distanz zwischen diesen zunehmen wird. Daher werden dringend Konzepte benötigt, mit denen das Sicherheitsniveau eines Grid definiert, erreicht, gemessen und nachgewiesen werden kann.

5 Identifizierter Handlungsbedarf

Definition von übergeordneten Organisationsstrukturen

Ein wichtiges Ergebnis der Vorstudie – insbesondere als Resultat der Analyse der Szenarien 2 und 5 – ist die Erkenntnis, dass der Prozess der Bildung einer virtuellen Domäne (eines Grid) die wesentliche Grundlage für die spätere Sicherheit des Grid bildet. Da bisherige Grids im wesentlichen durch soziale Netzwerke entstanden sind, existieren derzeit keine Organisationsstrukturen, die eine sichere Definition oder den sicheren Betrieb eines Grid gewährleisten. Vergleichbares gilt nicht nur für die Bildung, sondern auch für die Änderung oder auch Auflösung einer virtuellen Domäne (Was passiert z. B. mit den Daten, die auf nicht mehr benötigten Grid-Ressourcen gelagert sind? Was passiert mit Replikaten von Daten?). Bei einer künftig stärkeren Nutzung von Grid Technologie besteht daher dringender Handlungsbedarf hinsichtlich einer Definition von Organisationsstrukturen innerhalb des Grid-Kontextes.

Konfiguration von Grid-Middleware Systemen

Insbesondere die Analyse des Szenario 2 hat gezeigt, dass Grid-Middleware – wie jede IT-Komponente/Software – spezifische Schwachstellen besitzt. Im Falle eines konkreten Einsatzes einer speziellen Grid-Middleware ist es erforderlich, Sicherheitskonzepte für die einzelnen Grid-Middleware-Systeme zu erstellen. Wünschenswert sind an dieser Stelle Konfigurationshinweise, z. B. auf der Basis von zu erstellenden IT-Grundschutzbausteinen, mit denen – unabhängig vom Einsatzzweck – ein „sicheres Grid“ betrieben werden kann. Auch die Integration entsprechender Mechanismen in die Grid-Middleware kann so vorangetrieben werden.

Grid-spezifische Managementprozesse

Aus den Ergebnissen der Szenarien 2, 3 und 5 resultiert, dass derzeit keine ausreichenden Managementstrukturen und –prozesse im Grid-Umfeld vorhanden sind, und dass die außerhalb des Grid-Umfelds etablierten Managementsysteme nicht direkt auf ein Grid übertragen werden können. Da für das Grid-Umfeld organisationsübergreifende Managementprozesse erforderlich sind, müssen Aspekte des (Sicherheits- und IT-) Managements eines Grid genauer analysiert werden. Heute verfügbare Systemmanagement-Werkzeuge bieten keine Unterstützung für das Management virtueller Grid-Ressourcen oder die Überwachung und das Grid-weite Management der Middleware selbst. Ähnliches gilt für das Sicherheitsmanagement im Grid-Kontext, da derzeitige Konzepte zum Sicherheitsmanagement lediglich innerhalb *einer* einzelnen Organisation Anwendung finden und organisationsübergreifende Aspekte lediglich über formale Verpflichtungserklärungen (z.B. Verträge) berücksichtigt werden.

Nutzung künftiger Sicherheitstechnologien

In den Szenarien 2 und 5 werden „Trusted Computing“-Mechanismen als mögliche Sicherheitsmaßnahme identifiziert, um die Risiken durch Innentäter (Administratoren) zu reduzieren. Aufgrund der abstrakten Betrachtungsweise dieser Vorstudie ist konkret die Frage zu beantworten, wie und in welchem Umfang „Trusted Computing“-Mechanismen zu mehr Sicherheit im Grid beitragen können. Auf solche Mechanismen wurde zwar in dieser Vorstudie hingewiesen, aber die detaillierte Beantwortung der Frage, welche konkreten Anforderungen an „Trusted Computing“-Mechanismen gestellt werden müssen und welche Risiken dadurch wirksam gesenkt werden können, erfordert eine weitere spezifische Betrachtung.

Abschließend sei betont, dass im Rahmen der Studie lediglich eine abstrakte Betrachtung der Szenarien erfolgt ist, und die Ergebnisse nur bedingt auf reale Szenarien anwendbar sind. Die Arbeit an der Studie hat deutlich gemacht, dass bereits leicht veränderte Annahmen Auswirkungen auf Risiken und Maßnahmen haben können. Die Erstellung

eines Sicherheitskonzeptes für den Einsatz eines Grid ist erforderlich, um die realen Risken zu identifizieren und wirksame Maßnahmen zu definieren.

Anhang A Referenzen

[1] FOSTER, I. und C. KESSELMANN (Herausgeber): The Grid: Blueprint for a New Computing Infrastructure. Morgan Kaufmann Publishers, 2 Auflage, 2004

[2] Vorstudie Grid Sicherheits-Infrastruktur (GSI) Ergebnisse des Arbeitspakets 1: „Relevante Grid-Szenarien und ihr Schutzbedarf“

[3] Vorstudie Grid Sicherheits-Infrastruktur (GSI), Ergebnisse des Arbeitspakets 2: „Risikoanalyse“

[4] Vorstudie Grid Sicherheits-Infrastruktur (GSI), Ergebnisse des Arbeitspakets 3: „Sicherheitsmechanismen“