Bundesamt
für Sicherheit in der
Informationstechnik

Vorstudie Grid Sicherheits-Infrastruktur (GSI)

Ergebnisse des Arbeitspakets 2: Risikoanalyse

Version: 4.0

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

Inhaltsverzeichnis

1 Einleitung

Dieses Teildokument „**AP2: Bedrohungs- und Risikoanalyse**“ enthält unter anderem folgende wesentliche Ergebnisse:

- eine Identifikation potentieller Schwachstellen innerhalb von GRID-Umgebungen auf konzeptioneller Ebene,
- eine Analyse der Ausnutzbarkeit der identifizierten Schwachstellen auf konzeptioneller Ebene,
- eine Analyse des Schadenspotentials beim Eintritt der vorgenannten Bedrohungsszenarien,
- eine Identifikation der implementierten Sicherheitsmechanismen auf konzeptioneller Ebene,
- eine Bewertung der Wirksamkeit der Sicherheitsmechanismen auf konzeptioneller Ebene sowie
- ein Votum über den Stand der IT-Sicherheitstechnologie im Grid-Computing.

In Abschnitt 1.1 wird zunächst die Vorgehensweise bei der Bedrohungs- und Risikoanalyse erläutert. In Kapitel 2 werden die Bedrohungen und Risiken der einzelnen in [3] definierten Szenarien beschrieben. Jedes Szenario schließt hierbei mit einem für das Szenario spezifischen Fazit und einer Zusammenfassung ab.

1.1 Erläuterung zur Vorgehensweise der Risikoanalyse

Die Vorgehensweise zur Erstellung der Risikoanalyse ist an die in Kapitel 5 von [1] beschriebenen Vorgehensweise zur „*Bedrohungs- und Risikoanalyse*“ angelehnt und besteht aus den Schritten:

Schritt 1: Ermittlung der Schutzbedürftigkeit

Dieser Schritt erfolgte bereits im Ergebnisdokument zu „*AP1: Relevante Grid-Szenarien und ihr Schutzbedarf*“ [3]. Bezugnehmend auf die drei Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität wird die Schutzbedürftigkeit der innerhalb der Grid-Infrastruktur auftretenden Objekte (Daten und Systeme) definiert. Die Ergebnisse der in [3] durchgeführten Schutzbedarfsfeststellung werden als Grundlage für die Definition von Sicherheitsanforderungen und die Risikoanalyse verwandt.

Schritt 2: Definition von Sicherheitsanforderungen

Ausgehend von in [3] definierten Sicherheitsanforderungen und Zugriffsberechtigungen für das jeweilige Szenario, werden für die Risikoanalyse abstrakte Sicherheitsanforderungen (*SA*) definiert. Diese abstrakten Sicherheitsanforderungen stellen eine für das Szenario spezifische Sicherheitspolitik dar.

Schritt 3: Definition von Bedrohungen

Aus den Sicherheitsanforderungen werden abstrakte Bedrohungen (*AB*) abgeleitet, welche die Erreichung der Sicherheitsanforderungen (*SA*) verhindern. Anschließend werden konkrete Bedrohungen (*B*) beschrieben, die die abstrakten Bedrohungen konkretisieren und als Grundlage für die anschließende Risikoanalyse dienen.

Das Ziel der Bedrohungsanalyse ist die Ermittlung möglicher Bedrohungen, die eine Erreichung der Sicherheitsanforderungen verhindern. Sofern dies für die jeweilige Bedrohung möglich ist, werden Akteure und bedrohte Objekte bereits im Rahmen der Bedrohungsanalyse beschrieben. Bei Bedrohungen, die von verschiedenen Akteuren verursacht werden kann, wird der Akteur erst im Rahmen der Definition des Risikos beschrieben.

Im Rahmen der Bedrohungsanalyse wird ausgehend von den drei Grundbedrohungen

- **Verlust der Verfügbarkeit**

  Unter dem Verlust der Verfügbarkeit wird im Allgemeinen verstanden, dass ein Objekt nicht zum erforderlichen Zeitpunkt mit den erwarteten Eigenschaften zur Verfügung steht. Nichtverfügbarkeit von Ergebnisdaten bedeutet demnach z. B. dass diese nicht zum erwarteten Zeitpunkt zur Verfügung stehen.

- **Verlust der Vertraulichkeit**

  Als Verlust der Vertraulichkeit kann im Allgemeinen die Bekanntgabe von Informationen an einen unberechtigten Personenkreis verstanden werden. Im Kontext dieses Dokuments ist dies z. B. das Bekanntwerden von Eingabedaten oder Programmcode an Unberechtigte.

und

- **Verlust der Integrität**

  Der Verlust der Integrität bedeutet eine unerlaubte Veränderung mindestens einer Eigenschaft eines Objektes. Dies kann bedeuten, dass das Objekt unerlaubt verändert wurde, Angaben zum Ursprung verfälscht wurden (Authentizität) oder der Zeitpunkt der Erstellung manipuliert wurde

auf konzeptioneller Ebene ermittelt, welchen konkreten Bedrohungen die Erreichung der Sicherheitsanforderungen widerspricht und welche Auswirkung die jeweilige Bedrohung innerhalb des Szenarios hat. Zu betrachtende Bedrohungen können dabei aus den Bereichen „Höhere Gewalt“, „Organisatorische Mängel“, „Menschliche Fehlhandlungen“, „Technisches Versagen“ oder „Vorsätzliche Handlungen“ stammen. Hierbei werden insbesondere auch die Bedrohungen bei der Verarbeitung und Speicherung in Grid-Systemen beachtet.

Um eine Fokussierung auf relevante Bedrohungen und Risiken zu erreichen, werden im Gegensatz zur formal korrekten Vorgehensweise nicht alle potenziellen Bedrohungen betrachtet. Vielmehr werden anhand des in [3] beschriebenen Ablaufes und Datenflusses mögliche Akteure und die von diesen ausgehenden Bedrohungen ermittelt. Des Weiteren werden übergeordnet Bedrohungen identifiziert, die ohne spezielle Akteure eintreten, aber für das betrachtete Szenario relevant sein können. Bedrohungen, die wenig spezifisch für das betrachtete Szenario sind oder eher allgemeinen Charakter haben, werden nicht aufgeführt.

Die gewählte Vorgehensweise hat gegenüber den standardisierten Vorgehensweisen den Vorteil, dass eine Fokussierung auf für das jeweilige Szenario relevante Bedrohungen/Risiken stattfinden kann. Bedrohungen und Risiken, die für das Szenario nicht spezifisch sind, werden bei dieser Vorgehensweise nicht betrachtet, da hierbei davon ausgegangen wird, dass diese bekannt sind.

Schritt 4: Risikoanalyse

Im Rahmen der Risikoanalyse werden die zuvor in Schritt 3 definierten Bedrohungsszenarien für jedes Szenario bewertet. Zu den Bedrohungen wird – abhängig vom Szenario – ermittelt, welche Sicherheitsmechanismen vorhanden sind. Anschließend werden – sofern noch nicht im Rahmen der Definition der Bedrohung geschehen – die möglichen Akteure identifiziert und die zu erwartenden Eintrittshäufigkeit sowie die Höhe des zu erwartenden Schadens bewertet. Das Produkt aus Eintrittshäufigkeit und Höhe des zu erwartenden Schadens ergibt somit das Risiko einer einzelnen Bedrohung. Die Ergebnisse der Risikoanalyse sind damit die Grundlage für die anschließend in „***AP3 Sicherheitsmechanismen***“ stattfindende Auswahl von Sicherheitsmaßnahmen und deren Priorisierung.

Bei einem Angriff innerhalb eines Risikos wird immer ein ***Worst-Case-Szenario*** verwandt. Konkret bedeutet dies z. B., dass eine kriminelle Intention des Akteurs vorausgesetzt wird. Teilweise ergeben sich aus dieser Vorgehensweise realitätsverzerrende Annahmen, so dass in diesem Fall neben einem Worst-Case-Risiko ein weiteres Risiko abgeschätzt wird. In diesem Fall wird das Worst-Case-Risiko entsprechend hervorgehoben.

2 Bedrohungs- und Risikoanalyse

Ausgehend von den in [3] identifizierten Objekten und deren Schutzbedürftigkeiten wird nachfolgend für jedes Szenario eine separate Bedrohungs- und Risikoanalyse durchgeführt. Im ersten Schritt werden hierbei die Sicherheitsanforderungen für das Szenario abgeleitet. Anschließend werden die auf die Objekte wirkenden Bedrohungen identifiziert und abschließend die Eintrittswahrscheinlichkeit und das Schadensausmaß abgeschätzt.

Durch die Eintrittswahrscheinlichkeit wird eine Aussage über die Wahrscheinlichkeit des Eintretens eines Ereignisses getroffen. In der Risikomanagement-Praxis wird die Eintrittswahrscheinlichkeit mit einem Wert zwischen 0 und 1 angegeben, also konkret abgeschätzt. Eine solche Abschätzung ist jedoch nur bei Ereignissen möglich, bei denen auf statistische Erfahrungswerte zurückgegriffen werden kann (z. B. Ereignisse aus dem Bereich der Versicherungswirtschaft). Zu Ereignissen aus der modernen Informationstechnik fehlen solche konkreten Erfahrungswerte, so dass sich eine qualitative Abschätzung der Eintrittswahrscheinlichkeit in Kategorien etabliert hat. Ebenso wird bei der Abschätzung des Schadensausmaßes verfahren.

Die Einstufung der Eintrittswahrscheinlichkeit und des Schadensausmaßes erfolgt hierbei wie bereits in [3] für den Schutzbedarf qualitativ anhand der Kategorien *niedrig*, *mittel*, *hoch* und *sehr hoch*. Die Kategorien werden zunächst konkretisiert.

Bei der Abschätzung der Eintrittswahrscheinlichkeit und dem Schadensausmaß wird von der grundsätzlichen Wirksamkeit der im jeweiligen Szenario vorhandenen Sicherheitsmechanismen ausgegangen. Ist ein Mechanismus jedoch besonders komplex, aufwändig zu handhaben oder anderweitig fehleranfällig, so wird die daraus mögliche Erhöhung eines Risikos berücksichtigt und geht mit in die Abschätzung des Risikos ein. Eine Zusammenfassung der vorhandenen Sicherheitsmechanismen im Grid findet sich in den einzelnen Kapiteln zur Risikoanalyse des Szenarios (z. B. Abschnitt 2.1.3).

Definition von Eintrittswahrscheinlichkeiten

In die Eintrittswahrscheinlichkeiten (oft auch als Schadenswahrscheinlichkeit oder Schadenshäufigkeit bezeichnet) gehen neben der Abschätzung der Häufigkeit des Eintritts eines Ereignisses auch der durch einen Angreifer zu erbringende Aufwand für die erfolgreiche Durchführung eines Angriffs ein. Diese zwei Aspekte werden hier gemeinsam betrachtet, da neben Schadensereignissen die von einem bewussten Angriff eines Angreifers ausgehen, auch Schadensereignisse aus z. B. dem Bereich „Höhere Gewalt“ oder der Fahrlässigkeit eines Akteurs berücksichtigt werden müssen.

Die Bezeichnung als „Eintrittswahrscheinlichkeit“ ist auch bei einem Angriff als konsistent anzusehen, da ein Angriff, der mit geringem Aufwand durchgeführt werden kann, als wahrscheinlicher anzusehen ist, als ein Angriff dessen Durchführung einen hohen Aufwand bedeutet. In die Abschätzung des Aufwandes für einen Angriff gehen Aspekte wie finanzieller Aufwand und Hintergrundwissen mit ein. Ein Angriff, der auf der Basis von allgemein zugänglichem Wissen durchgeführt werden kann, muss hierbei als wahrscheinlicher angesehen werden, als ein Angriff, für dessen Durchführung detailliertes Know-how oder Insiderwissen erforderlich ist. Eine solche Annahme ist in der Praxis üblich, da z. B. die Wahrscheinlichkeit der Ausnutzung einer Schwachstelle in einem IT-System, zu dem Angriffswerkzeuge (Exploits) frei zugänglich sind, deutlich höher festzustellen ist, als ein Angriff bei dem kein solches Werkzeug existiert.

Tabelle 1: Definition von Eintrittswahrscheinlichkeiten

Kategorie	Eintrittswahrscheinlichkeit
niedrig	Der Eintritt des Ereignisses ist sehr unwahrscheinlich, es ist ein sehr hoher Aufwand erforderlich, um einen erfolgreichen Angriff durchzuführen.
mittel	Der Eintritt des Ereignisses ist unwahrscheinlich, es ist ein hoher Aufwand erforderlich, um einen erfolgreichen Angriff durchzuführen.
hoch	Der Eintritt des Ereignisses ist wahrscheinlich, es ist ein mittelhoher Aufwand erforderlich, um einen erfolgreichen Angriff durchzuführen.
sehr hoch	Der Eintritt des Ereignisses ist sehr wahrscheinlich, es ist nur ein geringer Aufwand erforderlich, um einen Angriff durchzuführen.

Definition von Schadensausmaßen

Durch das Schadensausmaß werden die Auswirkungen eines Schadens auf die betroffene Organisation/Person abgeschätzt. Bei dieser Abschätzung geht unter anderem der Aufwand für die Beseitigung und die Erfordernis präventiver Maßnahmen mit ein. Da wie bereits bei der Eintrittswahrscheinlichkeit keine quantitative Aussage getroffen werden kann, wird die nachfolgende Kategorisierung verwandt.

Tabelle 2: Definition von Schadensausmaßen

Kategorie	Schadensausmaß
niedrig	Die Auswirkung des Schadens ist tragbar. Schäden dieser Kategorie haben auf die Organisation keine oder nur geringe Auswirkungen. Eine Beseitigung des Schadens ist entweder nicht erforderlich oder mit einfachen Mitteln möglich.
mittel	Die Auswirkung des Schadens ist überschaubar. Schäden dieser Kategorie können von der Organisation einfach und mit geringem Aufwand behoben werden. Eine Behebung des Schadens ist erforderlich, aber nicht zeitkritisch.
hoch	Die Auswirkung des Schadens ist erheblich Schäden dieser Kategorie sind von der Organisation nur mit erheblichen Aufwand zu beseitigen und haben erhebliche Konsequenzen in verschiedenen Bereichen. Eine Behebung des Schadens ist unmittelbar erforderlich, präventive Maßnahmen sind sinnvoll und müssen getroffen werden
sehr hoch	Die Auswirkung des Schadens ist nicht tragbar. Schäden dieser Kategorie bedrohen die Existenz der Organisation, gefährden Leib und Leben oder haben massive Verstöße gegen Gesetze und Verträge zur Folge. Eine Behebung des Schadens ist (sofern möglich) unmittelbar erforderlich, präventive Maßnahmen sind zwingend erforderlich.

Angenommene Standard-Sicherheitsmaßnahmen

Sofern dies nicht anders angegeben ist, wird im Rahmen der Risikoanalyse das Vorhandensein von Standard-Sicherheitsmaßnahmen, wie sie derzeit auf IT-Systemen und im IT-Betrieb üblich sind, vorausgesetzt. Des Weiteren wird angenommen, dass sich die IT-Komponenten innerhalb eines geregelten IT-Betriebs befinden. Durch die-

se Annahmen soll sichergestellt werden, dass realistische Ergebnisse erzielt werden und die Betrachtung keinen zu theoretischen Charakter bekommt.

Die im Rahmen der Risikoanalyse angenommenen Standard-Sicherheitsmaßnahmen umfassen:

- *Organisatorische Maßnahmen*

  Zu solchen Maßnahmen gehören z. B. der Einsatz geschulter Mitarbeiter (Administratoren), um Fehler durch menschliche Fehlhandlungen oder Inkompetenz zu vermeiden, und geregelte Abläufe bei der Wartung und Pflege der Grid-Ressourcen. Es wird angenommen, dass es sich in allen Bereichen um einen geregelten IT-Betrieb handelt (z. B. ITIL).

  Explizit nicht angenommen, da dies im Grid-Umfeld derzeit unüblich ist, wird das Vorhandensein eines Domänen-übergreifenden Sicherheitsmanagement. Auch wenn diese Maßnahme in anderen Bereichen als üblich anzunehmen ist, ist sie im Grid-Kontext lediglich innerhalb einer Domäne zu finden.

- *Technische Maßnahmen*

  Die technischen Maßnahmen sind vielfältig und umfassen neben den physikalischen Gegebenheiten (z. B. Zugangs- und Zutrittsschutz) insbesondere auch Maßnahmen auf den einzelnen IT-Komponenten.

  Wie im geregelten IT-Betrieb üblich, wird angenommen, dass alle IT-Komponenten überwacht werden, so dass Fehlfunktionen schnell erkannt und entsprechende Gegenmaßnahmen getroffen werden können. Des Weiteren wird angenommen, dass die einzelnen IT-Komponenten angemessen gehärtet sind, also z. B. unnötige Software entfernt und Dienste deaktiviert sind. Des Weiteren wird die regelmäßige Aktualisierung angenommen, so dass vorhandene technische Schwachstellen schnell beseitigt werden.

  Auf der Seite der Kommunikationssicherheit wird angenommen, dass die einzelnen Domänen mittels Firewall-Technologien abgesichert sind und eine Datenverschlüsselung vorgenommen wird, sofern Grid-Ressourcen über öffentliche Netze miteinander kommunizieren. Durch solche Maßnahmen können Angriffe durch Externe weitgehend ausgeschlossen werden (z. B. Angriff über das Internet).

Die genannten Maßnahmen sollen lediglich beispielhaft die angenommenen Maßnahmen darstellen. In der Risikoanalyse wird grundsätzlich von „üblichen Maßnahmen“, wie sie derzeit im IT-Betrieb zu finden sind, ausgegangen. In den einzelnen Szenarien werden die konkret angenommenen und für das Szenario relevanten Sicherheitsmaßnahmen separat aufgeführt.

2.1 Bedrohungs- und Risikoanalyse Szenario 1

Zur Optimierung der Ressourcenauslastung und des unternehmensweiten und standortortübergreifenden Zugriffs auf Anwendungen und Daten innerhalb eines Unternehmens bzw. einer Organisation ist die Einrichtung eines unternehmensinternen Grid weit verbreitet. Insbesondere die inzwischen hohe Rechenleistung von Arbeitsplatz-Systemen kann durch Grid-Systeme effizient – besonders bei Batch-Jobs – genutzt werden. Das Szenario 1 zeichnet sich insbesondere durch die Nutzung von Arbeitsplatz-Systemen als Computing-Ressorcen aus.

2.1.1 Sicherheitsanforderungen

In [3] wurden Sicherheitsanforderungen und Zugriffsberechtigungen für das Szenario 1 definiert, für die Risikoanalyse werden diese konkretisiert.

SA1.I: Die Vertraulichkeit und Integrität geschäftskritischer oder zugriffsbeschränkter Daten (DA-zz, DA-z) ist sicherzustellen.

SA1.II: Nur berechtigte Personen (P-u) dürfen Grid Ressourcen nutzen.

SA1.III: Die Verfügbarkeit der Grid-Ressourcen (SRV, SW, HW) zum erforderlichen Zeitpunkt muss sichergestellt sein.

SA1.IV: Lokale Benutzer einer Grid-Ressorce (z. B Arbeitsplatz-PC als HW-Ressource) dürfen durch Grid-Jobs nicht beeinträchtigt werden.

2.1.2 Abstrakte Bedrohungen

Aus den o. g. Sicherheitsanforderungen werden abstrakte Bedrohungen abgeleitet, die anschließend verfeinert und für die Risikoanalyse genutzt werden:

AB1.I: Geschäftskritische oder zugriffsbeschränkter Daten (DA-zz, DA-z) werden einem nicht berechtigten Personenkreis (P-x) bekannt oder unbemerkt verändert.

AB1.II: Grid-Ressourcen (SRV, HW, SW) stehen zum erforderlichen Zeitpunkt nicht zur Verfügung.

AB1.III: Aufgrund der Nutzung der Ressource (HW) im Grid-Kontext, kann der lokale Benutzer die Ressource nicht nutzen.

AB1.IV: Eine nicht berechtigte Person (P-x) nutzt eine Grid-Ressource.

2.1.3 Annahmen zu Sicherheitsmaßnahmen

Die angenommenen Sicherheitsmaßnahmen leiten sich aus üblicherweise in Unternehmensnetzen umgesetzten Mechanismen ab, hierunter fallen nachfolgend angenommene Sicherheitsmechanismen:

- Der Zutritt zu Räume, in denen sich Grid Ressourcen befinden, ist durch entsprechende bauliche Sicherheitsmaßnahmen (z. B. Alarmanlage, Schließkreise, Zutrittsberechtigungssystem) abgesichert.
- Die Grid-Ressourcen besitzen eine Anti-Viren Lösung und aktuelle Sicherheitsupdates werden regelmäßig eingespielt.
- Die lokalen Benutzer der Grid-Ressourcen (Arbeitsplatz-PCs) besitzen keine administrativen Rechte auf den Komponenten.
- Die verfügbaren starken Authentikationsmechanismen innerhalb der Grid-Middleware werden genutzt.
- Die innerhalb des Unternehmensnetzes befindlichen Grid-Ressourcen sind durch geeignete Firewallmechanismen vor netzwerkbasierten Angriffen abgesichert.

- Die Kommunikation zwischen Unternehmensstandorten (DO-UA und DO-UB) ist durch ein verschlüsseltes VPN abgesichert.

2.1.4 Bedrohungsanalyse

Ausgehend von den abstrakten Bedrohungen AB1 werden nachfolgende konkrete Bedrohungen aufgestellt. Die Bedrohungen resultieren hierbei aus den in Tabelle 9 aus [3] geschilderten Abläufen.

Tabelle 3: Bedrohungsanalyse Szenario 1

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB1.I: Geschäftskritische oder zugriffsbeschränkte Daten (DA-zz) werden einem nicht berechtigten Personenkreis (P-x) bekannt oder unbemerkt verändert. Bedrohungen dieser Kategorie können direkt finanzielle Auswirkungen haben (DA-zz), da sie u. a. mögliche Wettbewerbsvorteile gegenüber Mitbewerbern betreffen. In dieser Kategorie sind insbesondere bewusste Angriffe (Industriespionage) anzusiedeln.			
B1.1	DA-zz DA-z	Vertraulichkeit	Die Vertraulichkeit der Daten DA-zz oder DA-z wird durch das Abhören unternehmensinterner Kommunikationsstrecken durch einen Administrator (P-lad) oder einen Innentäter (P-x) verletzt.
B1.2	DA-zz DA-z	Vertraulichkeit	Die Vertraulichkeit der Daten DA-zz oder DA-z wird durch das Abhören externer Kommunikationsstrecken (WAN) zwischen DO-UA und DO-UB durch einen Angreifer (P-x) verletzt.
B1.3	DA-zz DA-z	Vertraulichkeit Integrität	Die Vertraulichkeit oder Integrität der Daten DA-zz oder DA-z wird durch einen gezielten Angriff auf die Speicherressource (z. B. Datenbank) durch einen Administrator (P-lad) oder einen Innentäter (P-x) verletzt.
B1.4	DA-zz DA-z	Vertraulichkeit Integrität	Die Vertraulichkeit oder Integrität der Daten DA-zz oder DA-z wird durch einen gezielten Angriff auf die Hardware (HW) oder Software (SW) Ressourcen durch einen Administrator (P-lad), einen Innentäter (P-x) oder einen lokalen Benutzer (P-u) verletzt.
AB1.II: Grid-Ressourcen (SRV, HW, SW) stehen zum erforderlichen Zeitpunkt nicht zur Verfügung. Bedrohungen dieser Kategorie bedeuten insbesondere, dass erforderliche Daten den Folgeprozessen nicht rechtzeitig zur Verfügung stehen. Hierdurch können sich Produktionsprozesse verzögern und ggf. Umsatzausfälle die Folge sein.			
B1.5	HW	Verfügbarkeit	Ein als Grid-Ressource (HW) genutzter Arbeitsplatz-PC wird vom lokalen Benutzer (P-u) abgeschaltet, während ein Job berechnet wird.
B1.6	HW SW SRV	Verfügbarkeit	Die Nutzung einer Grid-Ressource (HW, SW, SRV) wird durch einen gezielten Angriff eines Administrators (P-lad) oder eines Innentäters (P-x) verhindert.

Bedro-hung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB1.III: Aufgrund der Nutzung der Ressource (HW) im Grid-Kontext, kann der lokale Benutzer die Ressource nicht nutzen. Diese Bedrohung beschreibt das Szenario, bei dem verfügbare Arbeitsplatz-PCs als Grid-Ressource (HW, „Computing Ressource“) genutzt werden. Durch die Verarbeitung eines Jobs kann der lokale Nutzer des Arbeitsplatz-PCs seinen Tätigkeiten nicht nachkommen, ein Verlust an Arbeitszeit ist die Folge.			
B1.7	HW	Verfügbarkeit	Die Nutzung der Grid-Ressource als Arbeitsplatz-PC wird durch eine fehlerhafte Grid-Anwendung (SW) verhindert.
B1.8	HW	Verfügbarkeit	Durch eine gezielt entwickelte Grid-Anwendung (SW) eines Nutzers (P-u) wird die Nutzung der Grid-Ressource als Arbeitsplatz-PC verhindert.
AB1.IV: Eine nicht berechtigte Person (P-x) nutzt eine Grid-Ressource. Die Bedrohungen dieser Kategorie können weitreichende Folgen haben. Neben dem Zugriff auf Daten (vgl. AB1.I) ist die Manipulation der Ressource selbst eine mögliche Folge.			
B1.9	HW	Vertraulichkeit	Durch einen gezielten Angriff gelingt einem Angreifer (P-x) der unberechtigte Zugriff auf Grid-Ressourcen, um etwa Daten eines laufenden Jobs zu lesen oder einen eigenen Job an das Grid zu übergeben.

2.1.5 Risikoanalyse

Im Folgenden werden die Schadenshöhe und Eintrittswahrscheinlichkeiten der im vorigen Kapitel aufgeführten Bedrohungen abgeschätzt. Die Ursache für das Eintreten der jeweiligen Bedrohung kann vielfältig sein. Um die Abschätzung nachvollziehen zu können, wird auf die möglichen Ursachen im Rahmen der Bemerkung Bezug genommen.

Tabelle 4: Risikoanalyse Szenario 1

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R1.1	B1.1	hoch	hoch	Wird von einem gezielten Angriff mit krimineller Intention (z. B. Industriespionage) gegen die Netzwerkinfrastruktur durch einen lokalen Administrator (P-lad) ausgegangen, ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein lokaler Administrator mit einem geringen Aufwand Zugang zur Netzwerkinfrastruktur erhält und im internen Netz üblicherweise keine Verschlüsselung der Daten DA-zz/DA-z (hier z. B. Simulationsparameter und Konstruktionsdaten) stattfindet. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an dritte). Insbesondere bei der Weitergabe der DA-zz ist ein hoher Schaden zu erwarten.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R1.2	B1.1	hoch	hoch	Wird der Angriff durch einen Innentäter (P-x) durchgeführt, dessen Arbeitsplatz-System als Grid-Ressource eingesetzt wird, wird die Eintrittswahrscheinlichkeit mit hoch abgeschätzt. Es wird davon ausgegangen, dass mit geringem Aufwand die Kommunikation abgehört und ein erfolgreicher Angriff gegen die DA-zz/DA-z (hier z. B. Simulationsparameter und Konstruktionsdaten) durchgeführt werden kann. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an Dritte). Insbesondere bei der Weitergabe der Konstruktionsdaten (DA-zz) ist ein hoher Schaden zu erwarten.
R1.3	B1.1	hoch	hoch	Wird der Angriff durch einen Innentäter (P-x) ohne Zugriff auf die Netzwerkkomponenten der Grid Infrastruktur (z. B. Switches oder Router) durchgeführt (z. B. normaler Mitarbeiter des Unternehmens ohne Zugang zu Grid-Ressourcen), wird die Eintrittswahrscheinlichkeit mit mittel abgeschätzt. Es wird davon ausgegangen, dass mit mittlerem Aufwand Zugang zu strategisch günstigen Räumlichkeiten (z. B. Räume mit Netzwerkinfrastruktur oder Grid-Ressourcen) erlangt werden und ein erfolgreicher Angriff gegen DA-zz/DA-z (hier z. B. Simulationsparameter und Konstruktionsdaten) durchgeführt werden kann. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an Dritte). Insbesondere bei der Weitergabe der DA-zz ist ein hoher Schaden zu erwarten.
R1.4	B1.2	hoch	niedrig	Das Abhören der Kommunikationsverbindung durch einen Angreifer P-x (z. B. Mitarbeiter eines Telekommunikationsunternehmens) zwischen den Standorten der DO-UA und DO-UB wird mit niedrig abgeschätzt, da von einer verschlüsselten Kommunikation ausgegangen wird und somit sehr hoher Aufwand für einen erfolgreichen Angriff gegen DA-zz/DA-z (hier z. B. Simulationsparameter und Konstruktionsdaten) erforderlich ist. Bei einer kriminellen Intention ist davon auszugehen, dass durch Weitergabe der Daten (z. B. der Konstruktionsdaten DA-zz) ein hoher Schaden verursacht wird.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R1.5	B1.3	hoch	hoch	Wird von einem gezielten Angriff mit krimineller Intention (z. B. Industriespionage) ausgegangen, der durch einen lokalen Administrator (P-lad) durchgeführt, ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein lokaler Administrator (z. B. Datenbank-Administrator) mit einem geringen Aufwand Zugang zu Speicherressourcen, z. B. einer Datenbank erhält und Daten DA-zz/DA-z (hier z. B. Simulationsparameter und Konstruktionsdaten) lesen oder verändern kann. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an Dritte). Insbesondere bei der Weitergabe oder Veränderung der Konstruktionsdaten (DA-zz) ist ein hoher Schaden zu erwarten.
R1.6	B1.3	hoch	niedrig	Wird der Angriff durch einen Innentäter (P-x) ohne Zugriff zur Datenbank durchgeführt (z. B. normaler Mitarbeiter des Unternehmens), wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt. Es wird davon ausgegangen, dass ein Zugang zur Datenbank – und damit zu DA-zz/DA-z (hier z. B. Simulationsparameter,, Konstruktionsdaten oder Grid-interne Daten) – nur mit hohem Aufwand möglich ist. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an Dritte). Insbesondere bei der Weitergabe oder Veränderung der Konstruktionsdaten (DA-zz) ist ein hoher Schaden zu erwarten.
R1.7	B1.4	hoch	hoch	Wird von einem gezielten Angriff mit krimineller Intention (z. B. Industriespionage) gegen durch einen lokalen Administrator (P-lad) einer Ressource durchgeführt, ist eine hohe Eintrittswahrscheinlichkeit anzunehmen. Da ein lokaler Administrator für die Wartung und Pflege der Ressourcen (HW, SW) verantwortlich ist, ist der Zugang und die Durchführung eines Angriffs gegen DA-zz/DA-z mit einem geringen Aufwand möglich. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an dritte). Insbesondere bei der Weitergabe oder Veränderung der DA-zz ist ein hoher Schaden zu erwarten.

Risiko Nr.	Bedrohung	Schadenshöhe	Eintrittswahrscheinlichkeit	Bemerkung
R1.8	B1.4	hoch	niedrig	Wird der Angriff durch einen Innentäter (P-x) ohne regulären Zugriff zur Ressource durchgeführt(z. B. normaler Mitarbeiter des Unternehmens), wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt. Es wird davon ausgegangen, dass ein Zugang zur Datenbank – und damit zu DA-zz/DA-z – für diesen Personenkreis nur mit hohem Aufwand möglich ist. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an Dritte). Insbesondere bei der Weitergabe oder Veränderung der Konstruktionsdaten (DA-zz) ist ein hoher Schaden zu erwarten.
R1.9	B1.4	hoch	niedrig	Wird der Angriff auf einem als Grid-Ressource (HW) genutzten Arbeitsplatz-System durch den lokalen Benutzer (P-u) durchgeführt, hängt die Eintrittswahrscheinlichkeit wesentlich von den Rechten des Benutzers auf diesem System ab. Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da auch auf dem Arbeitsplatz-System geeignete Mechanismen zur Rechteverwaltung und Benutzerseparierung angenommen werden. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an dritte). Insbesondere bei der Weitergabe oder Veränderung der Konstruktionsdaten (DA-zz) ist ein hoher Schaden zu erwarten.
R1.10	B1.5	niedrig	mittel	Wird davon ausgegangen, dass auch lokale Arbeitsplatz-PCs als Grid-Ressource genutzt werden, ist die Wahrscheinlichkeit dieses Ereignisses mit mittel anzusehen. Es ist anzunehmen, dass die betroffenen Mitarbeiter (P-u) in diesem Fall über die Nutzung der Arbeitsplatz-PCs als Grid-Ressource informiert wurden. Das Schadensausmaß wird mit niedrig abgeschätzt da davon ausgegangen wird, dass das Job-Management der Middleware entsprechende Mechanismen besitzt Jobs anderweitig zu verteilen, wenn diese nicht fristgerecht fertiggestellt werden.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R1.11	B1.6	hoch	hoch	Wird von einem gezielten Angriff mit krimineller Intention durch einen lokalen Administrator (P-lad) einer Ressource durchgeführt, ist eine hohe Eintrittswahrscheinlichkeit anzunehmen, da ein lokaler Administrator mit geringem Aufwand eine Grid-Ressource kompromittieren und damit die Verfügbarkeit dieser Ressource negativ beeinflussen kann. Bei einer kriminellen Intention ist davon auszugehen, dass ein hoher Schaden verursacht wird. Im wort-case kann das Grid nicht genutzt werden, Ergebnisdaten stehen nicht rechtzeitig zur Verfügung und eine Beseitigung des Schadens ist aufwändig.
R1.12	B1.6	mittel	niedrig	Wird der Angriff durch einen Innentäter (P-x) ohne regulären Zugriff zur Ressource durchgeführt (z. B. normaler Mitarbeiter des Unternehmens), wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt. Es wird davon ausgegangen, dass ein hoher Aufwand für die wirksame Kompromittierung erforderlich ist. Bei einer kriminellen Intention ist davon auszugehen, dass ein gezielter Schaden verursacht wird, das Schadensmaß wird mit mittel abgeschätzt. Im Worst-Case kann das Grid nicht genutzt werden, Ergebnisdaten stehen nicht rechtzeitig zur Verfügung.
R1.13	B1.7	mittel	niedrig	Wird davon ausgegangen, dass das genutzte Betriebssystem ein stabiles Task-Management besitzt, ist die Wahrscheinlichkeit mit der Fehlfunktion einer jeden Softwarekomponente gleichzusetzen und wird daher mit niedrig abgeschätzt. Tritt die Bedrohung an mehreren Ressourcen auf und können die lokalen Nutzer längere Zeit ihrer Arbeit nicht nachkommen, ist mit einem mittleren Schaden aufgrund von Arbeitszeitverlusten zu rechnen.
R1.14	B1.8	mittel	mittel	Gestaltet der Grid-Nutzer (P-u) gezielt eine Anwendung mit dem Ziel die Nutzung der Grid-Ressource durch den lokalen Nutzer zu verhindern, ist von einer mittleren Wahrscheinlichkeit auszugehen. Tritt die Bedrohung an mehreren Ressourcen auf und können die lokalen Nutzer längere Zeit ihrer Arbeit nicht nachkommen, ist mit einem mittleren Schaden aufgrund von Arbeitszeitverlusten zu rechnen.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R1.15	B1.9	hoch	niedrig	Die Bedrohung ist mit einem „Identity-Theft“ durch einen Angreifer P-x gleichzusetzen. Die Eintrittswahrscheinlichkeit wird aus diesem Grund mit niedrig abgeschätzt. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an Dritte). Insbesondere bei der Weitergabe oder Veränderung der Konstruktionsdaten (DA-zz) ist ein hoher Schaden zu erwarten.
R1.16	B1.9	hoch	niedrig	Wird die Bedrohung mit dem Szenario des direkten Angriffs durch eine Person ohne Zugriffsrechte (P-x) betrachtet, ist eine Kompromittierung des Job Submission Systems (JSS) erforderlich. Der Aufwand wird mit hoch abgeschätzt, da starke Mechanismen zur Benutzerauthentikation vorhanden sind. Bei einer kriminellen Intention ist davon auszugehen, dass ein Schaden verursacht wird (z. B. durch Weitergabe der Daten an dritte). Insbesondere bei der Weitergabe oder Veränderung der Konstruktionsdaten (DA-zz) ist ein hoher Schaden zu erwarten.

In der nachfolgenden Risikomatrix sind sowohl die Eintrittswahrscheinlichkeit (x-Achse) als auch die Schadenshöhe (y-Achse) des jeweiligen Risikos aus Tabelle 4 dargestellt.

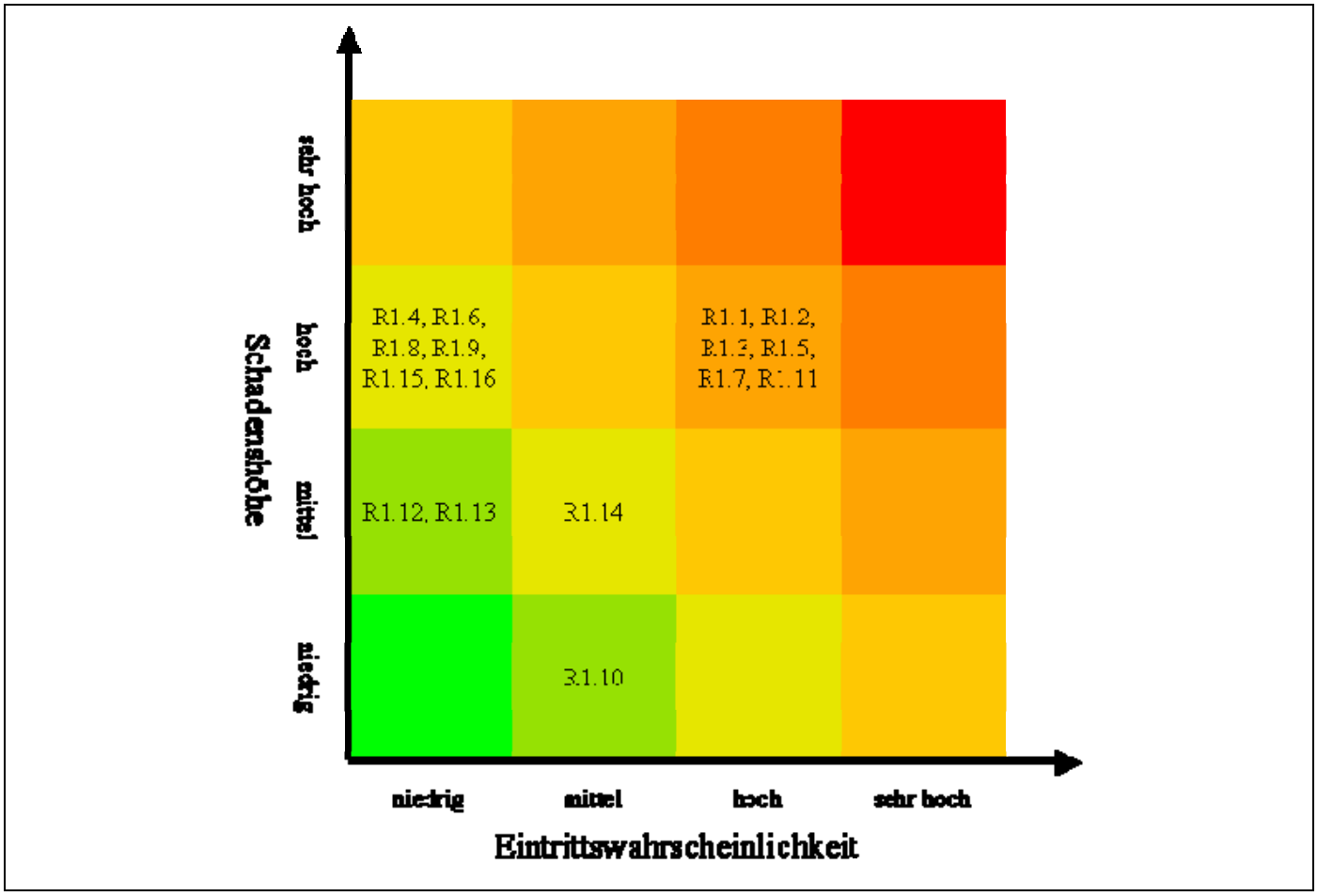

Abbildung 1: Risikomatrix Szenario 1

2.1.6 Fazit der Risikoanalyse

Im Folgenden werden die Erkenntnisse, die im Rahmen der Erstellung der Risikoanalyse für dieses Szenario gewonnen wurden, zusammengefasst.

Innentäter als größte Gefahr

Die wesentlichsten Risiken gehen von Innentätern mit krimineller Intention aus. Sind neben den „üblichen“ Sicherheitsmechanismen keine Maßnahmen gegen Innentäter getroffen, geht insbesondere von Personen mit besonderen Rechten (Administratoren) eine erhöhte Gefahr aus. Für diese Situationen müssen zusätzliche Maßnahmen, wie sie derzeit im Grid-Umfeld noch nicht verfügbar sind, umgesetzt werden. Auch sind hierunter Risiken, die aus Nach- oder Fahrlässigkeit sowie Vorsatz entstehet zu behandeln. Die Risiken der Kategorie „Gefährdungen durch Innentäter“ sind jedoch nicht spezifisch für Grid-Szenarien, sondern ergeben sich vielmehr in allen Bereichen der Informationstechnik.

In diesem Szenario ist insbesondere der Einsatz „normaler“ Arbeitsplatz-Systeme als Grid-Ressource (Computing-Ressource) interessant für eine Sicherheitsbetrachtung. Da Arbeitsplatz-Systeme inzwischen Multi-User fähig sind und geeignete Rechteverwaltungen besitzen, ist nicht von einem erfolgreichen lokalen Angriff auszugehen. Erfolgversprechender für einen gezielten Angriff sind in diesem Szenario Angriffe auf die Netzwerkinfrastruktur. Sofern physikalischer Zugang zur Netzwerkinfrastruktur erlangt werden kann, ist der Aufwand für das gezielte Abhören

sensibler Daten mit geringem Aufwand möglich. Ziel muss daher vor allem der Schutz der physikalischen Netzwerkinfrastruktur sein.

Fazit

Die angenommenen Sicherheitsmechanismen innerhalb des Grid wirken gegen potenzielle Risiken auf IT-technischer Ebene. Unbetrachtet in der Analyse sind Risiken, die sich aus der physischen Infrastruktur ergeben, da diese Risiken nicht Grid spezifisch sind. Insbesondere aus der Kombination fehlender physikalischer Absicherung und Angriff auf die IT Infrastruktur (vgl. R1.3) sind Schäden möglich. 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). Lokale Nutzer, deren Arbeitsplatz-System als Grid-Ressource genutzt wird, kommen hingegen nicht primär als Angreifer in Betracht (vgl. z.B. R1.2, R1.10). 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. In R1.2 hat dieses Risikoszenario den Verlust der Vertraulichkeit sensibler Daten zur Folge.

2.2 Bedrohungs- und Risikoanalyse Szenario 2

Szenario 2 ist die Erweiterung von Szenario 1, bei dem die unternehmenseigene Domäne um eine z. B. zu einem kooperierenden Unternehmen (RZ-Dienstleister) gehörende Domäne erweitert wird. Hierbei dient das Grid dem Abfangen von Lastspitzen oder einer organisationsübergreifenden Kooperation (z. B. zur gemeinsamen Produktentwicklung. Charakteristisch für das in [3] beschriebene Szenario 2 ist, dass kritische Unternehmensdaten in eine Domäne transferiert werden, auf die ggf. auch Mitbewerber Zugriff haben.

Da im Rahmen einer Risikoanalyse vorhandene Sicherheitsmechanismen mit berücksichtigt werden müssen, wird zunächst die im Szenario 2 zugrunde gelegte Sun Grid Engine vorgestellt. Die Sun Grid Engine versteht sich als „Campus Grid“ und besteht aus den drei Stufen:

- **Access Tier**

  Die Stufe „Access Tier“ stellt den Zugang für die Nutzer zum Grid dar, sie bildet somit das Grid-Front End. Insbesondere die „Job Submission“ Funktionalität wird innerhalb dieser Stufe realisiert und über den *QMON Browser* (GUI) gesteuert.

- **Management Tier**

  Innerhalb der Stufe „Management Tier“ sind insbesondere die Funktionalitäten für das *Distributed Resource Management* (DRM) und des *Job Management System* (JMS) realisiert. Insbesondere der „Master Host“ ist innerhalb dieser Stufe angesiedelt, er ist für die gesamte Steuerung der Abläufe und der Benutzerberechtigungen zuständig.

- **Compute Tier**

  Innerhalb der Stufe „Compute Tier“ wird die Rechenkapazitäten zur Verfügung gestellt. Im Compute Tier sind z. B. die Computing Ressourcen angesiedelt.

Die Einstufung als „Campus Grid“ bedeutet in diesem Zusammenhang, dass die Sun Grid Engine für ein Grid, welches innerhalb einer Organisation (z. B. innerhalb eines Unternehmens) betrieben wird, als geeignet bezeichnet wird. Hieraus resultieren insbesondere implementierte Sicherheitsmechanismen, da das Konzept bereits davon ausgeht, dass alle Komponenten unter der Hoheit einer Organisation stehen. Eine wesentliche Folge ist, dass keine Mechanismen vorhanden sind, die eine Nutzung verschiedener Organisationen zulassen (Klientenfähigkeit).

Im beschriebenen Szenario 2 wird davon ausgegangen, dass lediglich Teile des Compute Tier innerhalb der Domäne DO-UB angesiedelt ist und insbesondere die Access- und Management-Komponente weiterhin in der Domäne DO-UA liegen, somit insbesondere nur Personen aus dieser Domäne Zugriff auf diese Teile besitzen.

2.2.1 Sicherheitsanforderungen

In [3] wurden Sicherheitsanforderungen und Zugriffsberechtigungen für das Szenario 2 definiert, für die Risikoanalyse werden diese konkretisiert.

SA2.I: Es muss sichergestellt sein, dass ein vertrauenswürdiger Rechenzentrums-Dienstleister ausgewählt wird.

SA2.II: Der Zugriff auf die geschäftskritischen Daten DA-zz durch Personen außerhalb des Personenkreises P-uzz (insbesondere Personen innerhalb DO-UX und DO-UB) muss verhindert werden.

SA2.III: Der Zugriff auf die für die Verschlüsselung von DA-zz verwendeten Schlüssel außerhalb der Domäne DO-UB ist zu verhindern.

SA2.IV: Der Zugriff auf Grid-Ressourcen darf nur berechtigten Personen möglich sein.

SA2.V: Die Integrität der für die Verarbeitung der Daten DA-zz erforderliche Software (SW) innerhalb der Domäne DO-UB ist gewährleistet.

2.2.2 Abstrakte Bedrohungen

Aus den o. g. Sicherheitsanforderungen werden abstrakte Bedrohungen abgeleitet, die anschließend verfeinert und für die Risikoanalyse genutzt werden:

AB2.I: Durch einen fehlerhaften Auswahlprozess wird ein nicht geeigneter Dienstleister ausgewählt.

AB2.II: Unberechtigte erlangen Zugriff auf Daten DA-zz oder DA-z aus DO-UA.

AB2.III: Die für die Verschlüsselung der DA-zz benötigten Schlüssel werden kompromittiert.

AB2.IV: Grid-Ressourcen werden unberechtigt genutzt.

AB2.V: Unberechtigte erhalten Zugriff auf die für die Verarbeitung der Daten DA-zz erforderliche Software (SW) innerhalb der Domäne DO-UB.

2.2.3 Annahmen zu Sicherheitsmaßnahmen

Die angenommenen Sicherheitsmaßnahmen leiten sich direkt aus vorhandenen Mechanismen innerhalb der Sun Grid Engine ab, hierunter fallen nachfolgend angenommene Sicherheitsmechanismen:

- Die Datenkommunikation zwischen DO-UA und DO-UB ist durch Verschlüsselung (VPN) bei der Übertragung vor unberechtigter Einsichtnahme und Veränderung geschützt (z. B. *Certificate Security Protocol* (*CSP*) der Sun Grid Engine).
- Auf den einzelnen Grid-Ressourcen innerhalb DO-UA und DO-UB sind derzeit übliche (Best-Practice oder Grundschutz) Sicherheitsmaßnahmen umgesetzt, hierzu gehören beispielsweise:
  - Unsichere Services (telnet, rsh, etc.) werden nicht genutzt.
  - Geeignete Authentikationsmechanismen sichern den Zugriff auf die in der Domäne DO-UB enthaltenen Daten und Ressourcen (z. B. *Certificate Security Protocol* (*CSP*) der Sun Grid Engine).
  - Die einzelnen Komponenten innerhalb der Domäne DO-UB sind gehärtet (z. B. unnötige Dienste/Software wurde entfernt, aktuelle Patches sind eingespielt).
  - Der Zutritt zu Räumen und Zugriff auf Ressourcen ist durch geeignete Maßnahmen abgesichert. Insbesondere trifft dies auf die Grid-Ressourcen innerhalb der Domäne DO-UB des Dienstleisters zu.
- Die Grid-Ressourcen innerhalb der Domäne DO-UB sind durch geeignete Firewallmechanismen vor netzwerkbasierten Angriffen abgesichert.
- Insbesondere die Bestandteile der Stufe „Management Tier“ (Management Nodes) innerhalb der Domäne DO-UA sind durch geeignete Firewallmechanismen vor netzwerkbasierten Angriffen abgesichert.
- Der Rechenzentrums-Dienstleister sichert die Sicherheitsmaßnahmen durch ein entsprechendes SLA zu.

2.2.4 Bedrohungsanalyse

Ausgehend von den abstrakten Bedrohungen AB2 werden nachfolgende konkrete Bedrohungen aufgestellt. Die Bedrohungen resultieren hierbei aus den in Tabelle 15 aus [3] geschilderten Abläufen.

Tabelle 5: Bedrohungsanalyse Szenario 2

Bedro-hung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB2.I: Durch einen fehlerhaften Auswahlprozess wird ein nicht geeigneter Dienstleister ausgewählt. Die Bedrohungen dieser Gruppe haben vielfältige Auswirkungen auf die gesamte Nutzung des Grid. Bedrohungen dieser Art sind im Grid-Kontext innerhalb des Prozesses der VO-Bildung, also des Policy-Abgleichs zwischen den einzelnen Domänen, angesiedelt und können ein nicht vertrauenswürdiges Grid zur Folge haben.			
B2.1	SLA	Integrität	Aufgrund der Auswahl eines nicht geeigneten Dienstleisters durch den P-l kommt es im Service Level Agreement zwischen DO-UA und DO-UB zu einem fehlerhaften Policy-Abgleich oder das SLA wird in der DO-UB unbemerkt falsch umgesetzt.
AB2.II: Unberechtigte erlangen Zugriff auf Daten DA-zz oder DA-z aus DO-UA. Hierunter fallen insbesondere Bedrohungen, bei denen z. B. P-u aus der Domäne DO-UB oder DO-UX Zugriff auf DA-z oder DA-zz erhalten. Hierbei wird insbesondere berücksichtigt, dass diese Daten innerhalb der Domäne DO-UA lediglich in verschlüsselter Form vorliegen und ein Zugriff nur in Kombination mit einer Situation aus AB2.III möglich ist.			
B2.2	DA-zz DA-z	Vertraulichkeit	Ein Grid-Nutzer P-u aus DO-UX erhält innerhalb der Domäne DO-UB unberechtigten Zugriff auf DA-zz bzw. DA-z aus DO-UA.
B2.3	DA-zz DA-z	Vertraulichkeit	Ein lokaler Administrator P-lad aus DO-UB erhält innerhalb der Domäne DO-UB unberechtigten Zugriff auf DA-zz bzw. DA-z aus DO-UA.
B2.4	DA-zz DA-z	Vertraulichkeit	Ein Angreifer P-u aus DO-UX erhält unberechtigten Zugriff auf DA-zz bzw. DA-z aus DO-UA.
B2.5	SW SRV HW	Integrität	Der lokale Administrator P-lad aus DO-UB manipuliert die angebotenen Grid-Ressourcen, so dass Zugriff oder Einsicht für Unberechtigte auf verarbeitete Daten möglich wird.
B2.6	SW SRV HW	Integrität	Durch fehlerhafte Konfiguration von Sicherheitsfunktionen auf Grid-Ressourcen durch den P-lad innerhalb der Domäne DO-UB erhalten unberechtigte Zugriff auf Grid-Ressourcen.
AB2.III: Die für die Verschlüsselung der DA-zz benötigten Schlüssel werden kompromittiert. Diese Bedrohung ist als katastrophale Bedrohung anzusehen, da hierdurch der wesentliche Sicherheitsmechanismus zum Schutz der DA-z und DA-zz innerhalb der Domäne DO-UB gefährdet ist. Diese Bedrohung kann weitreichende Ursachen haben, neben einem mangelhaften Schlüsselmanagement ist ein unbeabsichtigtes bekannt werden des Schlüssels (z. B. durch einen Core-Dump) möglich.			
B2.7	DA-zz	Vertraulichkeit	Einem Angreifer P-x gelingt es, die zur Verschlüsselung der DA-zz benötigten Schlüssel zu kompromittieren.
B2.8	DA-zz	Vertraulichkeit	Dem lokalen Administrator P-lad von DO-UB gelingt es, die zur Verschlüsselung der DA-zz benötigten Schlüssel zu kompromittieren.

Bedro-hung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB2.IV: Grid-Ressourcen werden unberechtigt genutzt. Wird davon ausgegangen, dass DO-UB seine Ressourcen kostenpflichtig zur Verfügung stellt, kann durch eine unberechtigte Nutzung direkter finanzieller Schaden für DO-UA abgeleitet werden.			
B2.9	SW SRV HW	Verfügbarkeit	Ein Angreifer P-x erlangt unberechtigten Zugriff auf die Grid-Ressourcen in DO-UB.
B2.10	SW SRV HW	Vertraulichkeit	Ein Nutzer P-u verwendet die Grid-Ressourcen in DO-UB unberechtigt.
AB2.V: Unberechtigte erhalten Zugriff auf die für die Verarbeitung der Daten DA-zz erforderliche Software (SW) innerhalb der Domäne DO-UB. Die Bedrohung bedeutet, dass Personen außerhalb der Personengruppe P-lad Zugriff auf die für die Berechnung benötigte Software erhalten und diese manipulieren können.			
B2.11	SW	Integrität	Ein Grid-Nutzer P-uzz oder P-u erhält unberechtigten Zugriff auf die SW in DO-UB und kann diese manipulieren.
B2.12	SW	Integrität	Ein Angreifer P-x erhält unberechtigten Zugriff auf die SW in DO-UB und kann diese manipulieren.
B2.13	DA-zz,	Vertraulichkeit	Ein Grid-Nutzer P-u erhält durch den unberechtigten Zugriff auf die SW in DO-UB Einsicht in die Daten DA-zz.
B2.14	DA-zz,	Vertraulichkeit	Ein Angreifer P-x erhält durch den unberechtigten Zugriff auf die SW in DO-UB Einsicht in die Daten DA-zz.

2.2.5 Risikoanalyse

Im Folgenden werden die Schadenshöhe und Eintrittswahrscheinlichkeiten der im vorigen Kapitel aufgeführten Bedrohungen abgeschätzt. Die Ursache für das Eintreten der jeweiligen Bedrohung kann vielfältig sein. Um die Abschätzung nachvollziehen zu können, wird auf die möglichen Ursachen im Rahmen der Bemerkung Bezug genommen.

Tabelle 6: Risikoanalyse Szenario 2

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R2.1	B2.1	sehr hoch	niedrig	Die Auswirkungen der Auswahl eines nicht vertrauenswürdigen Dienstleisters durch den verantwortlichen P-l sind mannigfaltig und können gravierende finanzielle und ggf. auch rechtliche Auswirkungen haben. Ist der Dienstleister z. B. nicht in der Lage, die Sicherheitsanforderungen ausreichend zu gewährleisten, sind DA-zz (seismische Basisdaten und geologische Informationen) bedroht, wenn sie innerhalb DO-UB verarbeitet werden. Die Eintrittswahrscheinlichkeit wird als niedrig eingestuft, da eine gewissenhafte Auswahl eines Dienstleisters durch P-l vorauszusetzen ist.
R2.2	B2.2	hoch	niedrig	Ein unberechtigter Zugriff auf geschäftskritische (DA-zz) oder zugriffsbeschränkte (DA-z) Daten in der Domäne DO-UB durch einen P-u aus DO-UX ist nur bei nicht vertrauenswürdiger Grid-Software oder durch Kompromittierung der Verschlüsselungsschlüssel möglich. Wird eine vertrauenswürdige Grid-Software vorausgesetzt, kann die Eintrittswahrscheinlichkeit einer Kompromittierung der Schlüssel durch einen Grid-Nutzer mit niedrig bewertet werden. Die Schadenshöhe bei Kompromittierung von geschäftskritischen (DA-zz) oder zugriffsbeschränkten (DA-z) Daten wird als hoch eingestuft.
R2.3	B2.2	hoch	mittel	**Worst-Case-Abschätzung** Ein unberechtigter Zugriff auf geschäftskritische (DA-zz) oder zugriffsbeschränkte (DA-z) Daten in der Domäne DO-UB durch einen P-u aus DO-UX ist nur bei nicht vertrauenswürdiger Grid-Software oder durch Kompromittierung der Verschlüsselungsschlüssel möglich. Die Vertrauenswürdigkeit kann nicht unbedingt vorausgesetzt werden (vgl. [6]), daher wird die Eintrittswahrscheinlichkeit als mittel eingestuft. Die Schadenshöhe bei Kompromittierung von geschäftskritischen (DA-zz) oder zugriffsbeschränkten (DA-z) Daten wird als hoch eingestuft.
R2.4	B2.3	hoch	mittel	Ein unberechtigter Zugriff auf geschäftskritische Daten DA-zz (seismische Basisdaten und geologische Informationen) in der Domäne DO-UB durch einen P-lad dieser Domäne ist nur durch Kompromittierung der Grid-Software oder der Verschlüsselungsschlüssel möglich. Obwohl der P-lad in DO-UB mit geringem Aufwand die Grid-Software umgehen kann, muss von vertrauenswürdigem Personal ausgegangen werden. Daher wird die Eintrittswahrscheinlichkeit mit mittel abgeschätzt. Die Schadenshöhe bei Kompromittierung von geschäftskritischen Daten wird als hoch eingestuft.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R2.5	B2.4	hoch	niedrig	Ein unberechtigter Zugriff durch einen P-u aus DO-UX auf geschäftskritische Daten DA-zz (seismische Basisdaten und geologische Informationen) in der Domäne DO-UB ist nur durch Kompromittierung der Grid-Software oder der Verschlüsselungsschlüssel möglich. Da davon ausgegangen werden muss, dass ein P-u nur mit sehr hohem Aufwand oder durch Ausnutzung vorhandener Schwachstellen diesen Angriff durchführen kann wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt. Es wird dabei davon ausgegangen, dass Schwachstellen (vgl. [6]) unverzüglich durch den P-lad beseitigt werden. Die Schadenshöhe bei Kompromittierung von geschäftskritischen Daten (DA-zz) Daten wird als hoch eingestuft.
R2.6	B2.5	hoch	niedrig	Eine unbemerkte Manipulation der Grid-Ressourcen durch den P-lad in DO-UB kann weitreichende finanzielle Auswirkungen und ggf. rechtliche Konsequenzen haben. Insbesondere sind Szenarien denkbar, bei denen die Vertraulichkeit der DA-zz und DA-z verletzt wird, denkbar. Die Schadenshöhe wird daher mit hoch bewertet. Die Eintrittswahrscheinlichkeit einer Manipulation der Grid-Ressourcen durch den lokalen Administrator P-lad aus DO-UB wird als niedrig eingestuft, da von vertrauenswürdigem Personal ausgegangen werden muss.
R2.7	B2.5	hoch	sehr hoch	**Worst-Case-Abschätzung** Eine unbemerkte Manipulation der Grid-Ressourcen durch den P-lad aus DO-UB kann weit reichende finanzielle Auswirkungen und ggf. rechtliche Konsequenzen haben. Insbesondere sind Szenarien denkbar, bei denen die Vertraulichkeit der DA-zz und DA-z verletzt wird. Die Schadenshöhe mit daher mit hoch bewertet. Wird die Eintrittswahrscheinlichkeit vor dem Hintergrund einer geplanten Kompromittierung durch den P-lad aus DO-UB betrachtet, ist die Wahrscheinlichkeit mit hoch abzuschätzen, da der P-lad nur geringen Aufwand betreiben muss, um einen erfolgreichen Angriff durchzuführen.
R2.8	B2.6	mittel	mittel	Die Eintrittswahrscheinlichkeit wird mit mittel abgeschätzt, da dieses Ereignis mit einer menschlichen Fehlhandlung des P-lad in DO-UB gleichzusetzen ist und – obwohl von einer sorgfältigen Konfiguration ausgegangen werden muss – Fehler unvermeidlich sind. Die Schadenshöhe wird mit mittel abgeschätzt, da nicht unbedingt von einem kritischen Schaden ausgegangen werden muss.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R2.9	B2.7	sehr hoch	niedrig	Die Kompromittierung der Verschlüsselungsschlüssel durch einen Angreifer P-x innerhalb der Domäne DO-UB setzt den Hauptsicherheitsmechanismus des Grid außer Kraft. Der Schaden wird als sehr hoch eingestuft, da dann insbesondere Zugriff auf DA-zz und DA-z möglich ist. Die Eintrittswahrscheinlichkeit dieses Ereignisses ist durch vorgeschaltete Sicherheitsmechanismen (z. B. Zugriffsbeschränkungen, Hardware-Sicherheitsmechanismen) für einen Angreifer P-x ohne Zugriff auf Grid-Ressourcen als niedrig zu bewerten. Der Aufwand eines gezielten Angriffs wird als hoch angesehen, da hierfür insbesondere die Kompromittierung der Grid-Software (SW) erforderlich ist. *Anmerkung:* Bereits ein kleiner Fehler bei der Rechtevergabe für Dateien kann die Vertraulichkeit aller DA-zz gefährden.
R2.10	B2.8	sehr hoch	mittel	Die Kompromittierung der Verschlüsselungsschlüssel durch einen P-lad aus DO-UB setzt den Hauptsicherheitsmechanismus des Grid außer Kraft. Der Schaden wird als sehr hoch eingestuft, da dann insbesondere Zugriff auf DA-zz möglich ist. Die Eintrittswahrscheinlichkeit diese Ereignisses ist trotz vorgeschalteter Sicherheitsmechanismen (z. B. Zugriffsbeschränkungen, Hardware-Sicherheitsmechanismen) für einen lokalen Administrator P-lad aus DO-UB mit Insider-Kenntnissen als mittel zu bewerten. Insbesondere, wenn innerhalb des Key-Managements keine Hardware-Sicherheitsmodule (HSM) für die sichere Schlüsselaufbewahrung eingesetzt werden (was in diesem Szenario der Fall ist).
R2.11	B2.9	hoch	niedrig	Der Schaden durch entgangenen Nutzen einer kostenpflichtigen Grid-Ressource kann im Extremfall erheblich sein, z. B. wenn die erforderlichen Ergebnisse nicht fristgerecht zur Verfügung stehen und sich nachfolgende Geschäftsprozesse verzögern. Daher wird die Schadenshöhe mit hoch bewertet. Die Eintrittswahrscheinlichkeit wird als niedrig eingestuft, da geeignete Zugriffsbeschränkungen auf den Grid-Ressourcen vorhanden sind und erheblicher Aufwand betrieben werden muss, um diese zu umgehen.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R2.12	B2.9	sehr hoch	niedrig	Erlangt ein Unberechtigter P-x Zugriff auf einzelne Grid-Ressourcen, ist von einer kriminellen Intention und damit von einer Ausnutzung der Ressource auszugehen. Daher wird das Schadenspotenzial mit sehr hoch abgeschätzt. Die Eintrittswahrscheinlichkeit wird als niedrig angesehen, da durch geeignete technische Maßnahmen (Rechenzentrum, Zutrittsschutz, etc.) erheblicher Aufwand betrieben werden muss, um diese zu umgehen.
R2.13	B2.10	hoch	niedrig	Der durch die unberechtigte Nutzung durch einen P-u verursachte Schaden durch entgangenen Nutzen einer kostenpflichtigen Grid-Ressource kann im Extremfall erheblich sein, z. B. wenn die erforderlichen Ergebnisse nicht fristgerecht zur Verfügung stehen und sich nachfolgende Geschäftsprozesse verzögern. Daher wird die Schadenshöhe mit hoch bewertet. Die Eintrittswahrscheinlichkeit wird als niedrig eingestuft, da geeignete Zugriffsbeschränkungen auf den Grid-Ressourcen vorhanden sind und davon ausgegangen werden muss, dass berechtigte Nutzer P-u gewissenhaft mit den Ressourcen umgehen.
R2.14	B2.11	sehr hoch	niedrig	Der mögliche Schaden durch unbemerkt manipulierte Software im Grid durch einen P-u oder P-uzz ist erheblich und wird daher als sehr hoch eingestuft. Insbesondere sind hier Folgen wie der Zugriff auf die Schlüssel oder DA-zz und DA-z zu berücksichtigen. Die Wahrscheinlichkeit der Manipulation der Software durch einen Grid-Nutzer P-uzz oder P-u allerdings wird als niedrig angesehen.
R2.15	B2.12	sehr hoch	niedrig	Der Schaden durch unbemerkt manipulierte Software im Grid durch einen Angreifer P-x ist erheblich und wird daher als sehr hoch eingestuft. Die Wahrscheinlichkeit der Manipulation der Software durch einen externen Angreifer P-x ohne Insider-Kenntnisse allerdings wird als niedrig angesehen.
R2.16	B2.13	hoch	niedrig	Die Schadenshöhe bei Kompromittierung von geschäftskritischen (DA-zz) oder zugriffsbeschränkten (DA-z) Daten durch einen P-u wird als hoch eingestuft. Die Wahrscheinlichkeit der Manipulation der Software durch einen Grid-Nutzer P-u ohne erweiterte Zugriffsrechte allerdings wird als niedrig angesehen.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R2.17	B2.14	sehr hoch	niedrig	Die Schadenshöhe bei Kompromittierung von geschäftskritischen (DA-zz) oder zugriffsbeschränkten (DA-z) Daten durch einen Angreifer P-x wird als sehr hoch eingestuft, da kriminelle Intention vorausgesetzt wird. Die Wahrscheinlichkeit wird als niedrig angesehen, da geeignete Maßnahmen vorhanden sind, derartige gezielte Angriffe durch Personen ohne Zugriffsrechte P-x abzuwehren.

In der nachfolgenden Risikomatrix sind sowohl die Eintrittswahrscheinlichkeit (x-Achse) als auch die Schadenshöhe (y-Achse) des jeweiligen Risikos aus Tabelle 6 dargestellt.

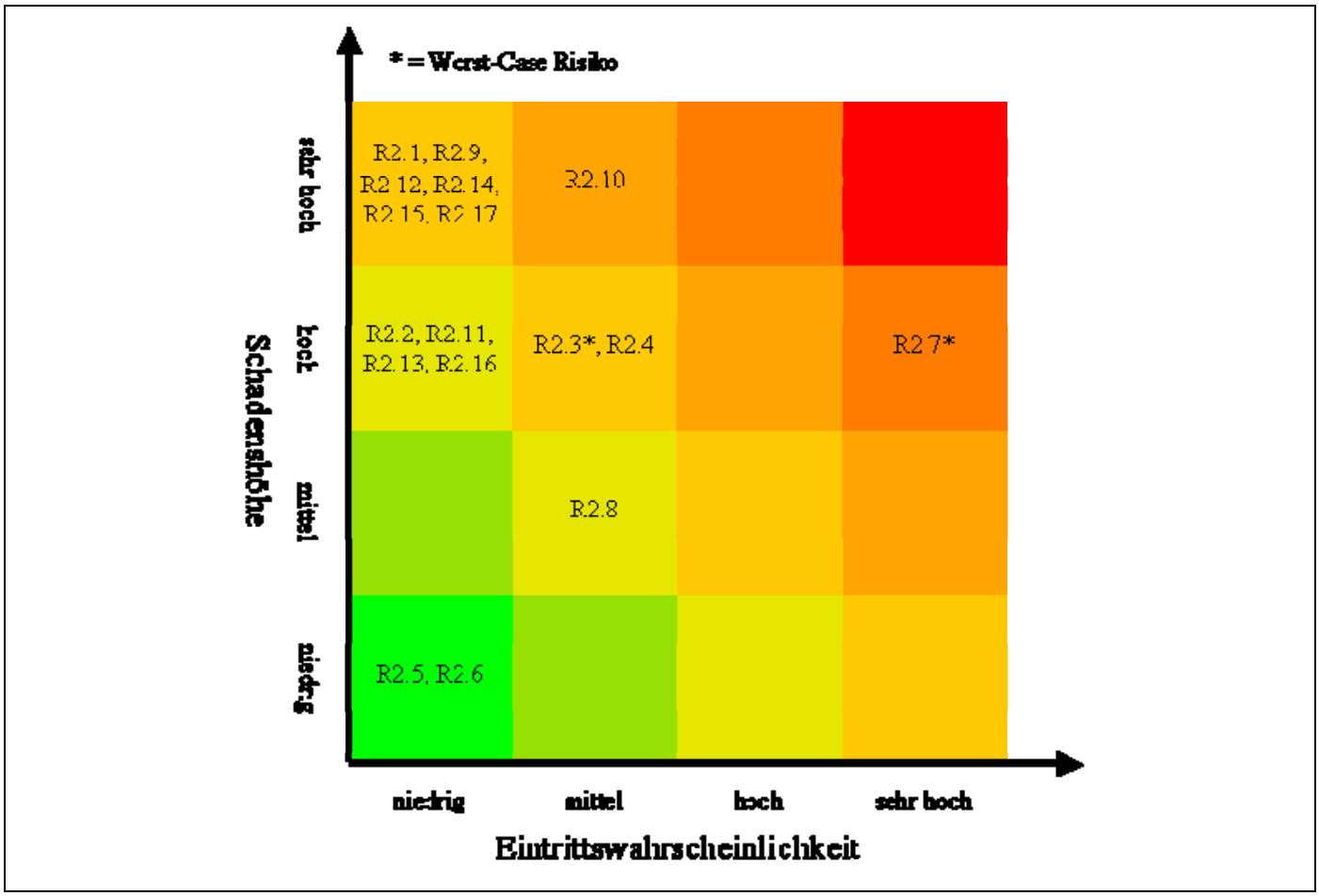

Abbildung 2: Risikomatrix Szenario 2

2.2.6 Fazit der Risikoanalyse

Im Folgenden werden die Erkenntnisse, die im Rahmen der Erstellung der Risikoanalyse für dieses Szenario gewonnen wurden, zusammengefasst.

Etablierte Sicherheitsmechanismen auf Unix-Basis

Die Sun Grid Engine ist hauptsächlich als Erweiterung von Unix-Betriebssystemen zu verstehen und nutzt intensiv etablierte Sicherheitsmechanismen der jeweiligen Betriebssysteme. Innerhalb des Szenario 2 ist insbesondere der Fall von Interesse, bei dem DA-zz oder DA-z innerhalb der Domäne DO-UB durch Personen außerhalb der Domäne DO-UA kompromittiert werden können. Dieser Fall reduziert sich im wesentlichen auf Schwachstellen in der Sun Grid Engine (vgl. [6] und R2.3) oder des Solaris Betriebssystems, gezielte Angriffe (vgl. R2.12) oder Angriffe durch Personen mit besonderen Zugriffsrechten (vgl. R2.4).

Da die Grid-Nutzer P-u keinen direkten Zugriff auf Ressourcen innerhalb der Stufe „Compute Tier“ benötigen, entfällt das Mapping-Problem von Globus (vgl. Abschnitt 2.4), bei dem jede Grid-Nutzerkennung auf eine lokale Nutzerkennung auf der durch P-u zu nutzenden Ressource gemappt werden muss. Hierdurch reduziert sich die Angreifbarkeit der Komponenten innerhalb von „Compute Tier“ deutlich.

Potenzielle Risiken

Insbesondere das in R2.1 dargestellte Risiko muss vordergründig betrachtet werden, da Fehler im Auswahlprozess eines Dienstleisters schwerwiegende Folgen haben kann. 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. Auch wenn davon ausgegangen werden muss, dass ein geeigneter Dienstleister ausgewählt wird, müssen Maßnahmen ergriffen werden, welche die Einhaltung des vertraglich vereinbarten Sicherheitsniveaus sicherstellen. Mögliche Maßnahmen werden in [4] dargestellt.

Die weiteren erhöhten Risiken sind nicht spezifisch für ein Grid oder die eingesetzte Software Sun Grid Engine. Durch die Nutzung etablierter Mechanismen (z. B. VPN zur Absicherung der Kommunikation, Zertifikate zur Benutzerauthentikation) beschränken sich die Risiken auf solche, die auch außerhalb des Grid-Kontextes auf Unix-Komponenten oder in einem Outsourcing-Szenario auftreten können.

Fazit

Die technischen Sicherheitsmechanismen (z.B. Verschlüsselung zwischen den Domänen) entsprechen dem Stand der Technik und wirken angemessen gegen verschiedene Risiken des Szenarios (vgl. z.B. R2.11, R2.12). Bedenklich ist jedoch, dass die Wirksamkeit dieser 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) abhängig ist. Auch die Tatsache dass die lokal wirkenden Administratoren (P-lad) ohne großen Aufwand jeden denkbaren Angriff durchführen können (vgl. z.B. R2.7), ist im Kontext des „Shell“-Grid als kritisch anzusehen. Dies ist jedoch ein – auch außerhalb des Grid-Kontextes – bekanntes und derzeit mit technischen Mitteln nur schwer zu lösendes Problem. Hier sind organisatorische Maßnahmen und erweiterte technische Maßnahmen (z.B Nutzung von HSMs – Hardware Sicherheits Modulen) zur Risikoeindämmung erforderlich.

Besonders in diesem Szenario ist die Bildung des Grid (VO-Bildung), also die Auswahl eines geeigneten Dienstleisters und die verbindliche Vereinbarung eines Sicherheitsniveaus und umzusetzender Sicherheitsmechanismen, eine wesentliche Grundlage für die Gesamtsicherheit und Vertrauenswürdigkeit des Grid. Wie bereits erwähnt entsprechen die implementierten Sicherheitsmechanismen dem Stand der Technik und müssen als angemessen angesehen werden. Defizite lassen sich insbesondere im Bereich der Organisation und der Überwachung des Grid – und der Einhaltung des SLA – finden (vgl. z.B. R2.1). In diesem Szenario sollte überlegt werden ein Sicherheitsmanagement zu etablieren und hierbei das Grid einer regelmäßigen und kontinuierlichen Überwachung zu unterziehen.

2.3 Bedrohungs- und Risikoanalyse Szenario 3

Das offene e-Science-Grid dient in Wissenschaft und Forschung der Kooperation insbesondere bei der gemeinschaftlichen Nutzung knapper und teuerer Ressourcen. In der Regel stellen eine Vielzahl von wissenschaftlichen Einrichtungen ihre Ressourcen einem Grid zur Verfügung. Das offene e-Science-Grid wird von einer hohen Zahl wechselnder Nutzer verwendet. Aus diesem Grund ähnelt das Szenario 3 stark dem Szenario 2, da in beiden Szenarien Grid-Ressourcen von unterschiedlichen Parteien genutzt werden. Bezogen auf die Risikoanalyse bedeutet dies, dass die in Szenario 2 identifizierten Risiken auch auf Szenario 3 anwendbar sind.

Wie bereits in [3] beschrieben, wird im Rahmen der Risikoanalyse Globus als Middleware angenommen. Die Risikoanalyse betrachtet hierbei das Szenario der Nutzung der DO-VO1, bei der sowohl P-u aus DO-P1 wie auch P-u aus DO-P2 Ressourcen innerhalb der virtuellen Domäne DO-VO1 nutzen können. Im Fokus der Risikobetrachtung stehen Szenarien, bei denen Nutzer aus DO-VO2 die virtuelle Domäne DO-VO1 (insbesondere Ressourcen innerhalb DO-P2) kompromittieren. Hierdurch soll die Klientenfähigkeit eines Grid beleuchtet werden.

2.3.1 Sicherheitsanforderungen

In [3] wurden Sicherheitsanforderungen und Zugriffsberechtigungen für das Szenario 3 definiert, für die Risikoanalyse werden diese konkretisiert.

SA3.I: Im Rahmen der Bildung der virtuellen Organisation muss sichergestellt werden, dass nur mit vertrauenswürdigen Partnern kooperiert wird.

SA3.II: Die Integrität der Daten DA-nz und DA-z innerhalb der virtuellen Domäne DO-VO1 muss sichergestellt werden.

SA3.III: Die Vertraulichkeit und Integrität der für die Verarbeitung der Daten DA-nz und DA-z erforderliche Software (SW) innerhalb der Domäne DO-VO1 ist gewährleistet.

SA3.IV: Aus den Domänen DO-P1 oder DO-P2 kommende Daten DA-nz und DA-z dürfen die Domäne DO-VO1 nicht verlassen.

SA3.V: Der Zugriff auf Grid-Ressourcen darf nur berechtigten Personen möglich sein.

2.3.2 Abstrakte Bedrohungen

Aus den o. g. Sicherheitsanforderungen werden abstrakte Bedrohungen abgeleitet, die anschließend verfeinert und für die Risikoanalyse genutzt werden:

AB3.I: Durch einen fehlerhaften Auswahlprozess wird ein nicht geeigneter Partner zur Bildung einer virtuellen Organisation ausgewählt.

AB3.II: Durch unberechtigte Zugriffe werden DA-nz oder DA-z auf Ressourcen innerhalb der Domäne DO-VO1 manipuliert.

AB3.III: Durch unberechtigte Zugriffe wird die für die Verarbeitung der Daten DA-nz und DA-z erforderliche Software (SW) auf Ressourcen innerhalb der Domäne DO-VO1 manipuliert.

AB3.IV: Daten DA-nz oder DA-z verlassen die Domäne DO-VO1.

AB3.V: Die angebotenen Grid-Ressourcen aus DO-VO1 werden unberechtigt genutzt.

2.3.3 Annahmen zu Sicherheitsmaßnahmen

Die derzeit im Einsatz befindlichen Grids in diesem Umfeld besitzen bereits Sicherheitsmechanismen, deren Vorhandensein und Wirksamkeit im Rahmen der Risikoanalyse angenommen wird. Nachfolgend sind die wesentlichsten Sicherheitsmechanismen zusammengefasst:

- Daten DA-nz und DA-z sind durch Verschlüsselung (VPN) bei der Übertragung zwischen den Domänen DO-P1 und DO-P2 vor unberechtigter Einsichtnahme und Veränderung geschützt.
- Die einzelnen Domänen DO-P1 und DO-P2 sind mittels Firewalltechniken vor Angriffen aus öffentlichen Netzen (z. B. Internet) abgesichert.
- Auf den einzelnen Grid-Ressourcen sind derzeit übliche (Best-Practice oder Grundschutz) Sicherheitsmaßnahmen umgesetzt, hierzu gehören beispielsweise:
    - Geeignete Authentikationsmechanismen sichern den Zugriff auf die in der Domäne DO-VO1 enthaltenen Daten DA-nz und DA-z ab.
    - Der Zutritt zu Räumen und Zugriff auf Ressourcen innerhalb der Domäne DO-VO1 ist durch geeignete Maßnahmen abgesichert.
    - Die von Globus zur Verfügung gestellten Sicherheitsmechanismen werden genutzt.
- Die Vertrauenswürdigkeit der Administratoren P-lad ist durch entsprechende Maßnahmen beim Einstellungsprozess sichergestellt.

2.3.4 Bedrohungsanalyse

Ausgehend von den abstrakten Bedrohungen AB3 werden nachfolgende konkrete Bedrohungen aufgestellt. Die Bedrohungen resultieren hierbei aus den in Tabelle 21 aus [3] geschilderten Abläufen.

Tabelle 7: Bedrohungsanalyse Szenario 3

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB3.I: Durch einen fehlerhaften Auswahlprozess wird ein nicht geeigneter Partner zur Bildung einer virtuellen Organisation ausgewählt. Diese Bedrohung umfasst insbesondere organisatorische Fehler im Prozess der Bildung der Domäne DO-VO1, bei dem z. B. ein mangelhafter Anforderungskatalog für den Kooperationspartner erstellt wurde. Die Folgen können vielfältig sein, da je nach Ausprägung Integrität oder Vertraulichkeit der innerhalb des Grid verarbeiteten Daten nicht gewährleistet werden kann.			
B3.1	DO-VO1	Integrität	Durch Auswahl eines nicht geeigneten Kooperationspartners kommt es zwischen DO-P1 und DO-P2 zu einem fehlerhaften Policy-Abgleich.
AB3.II: Durch unberechtigte Zugriffe werden DA-nz oder DA-z auf Ressourcen innerhalb der Domäne DO-VO1 manipuliert. Die Bedrohungen dieser Gruppe betreffen die Integrität der DA-nz und DA-z. Neben einem gezielten Angriff eines P-x (z. B. ein P-u aus der Domäne DO-P2/DO-VO2) sind hierbei insbesondere die Rollen des lokalen Administrators P-lad aus den Domänen DO-P1 und DO-P2 berücksichtigt. Festgestellte Manipulationen werden nicht betrachtet, da diese durch vorhandene Datensicherungen beseitigt werden können.			
B3.2	DA-z	Integrität	Daten DA-z (hier problembezogene Ausgabedaten) werden innerhalb der Domäne DO-VO1 durch den lokalen Administrator P-lad aus DO-P1 oder DO-P2 unberechtigt manipuliert.
B3.3	DA-nz	Integrität	Daten DA-nz werden innerhalb der Domäne DO-VO1 durch den lokalen Administrator P-lad aus DO-P1 oder DO-P2 manipuliert.

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
B3.4	DA-z	Integrität	Daten DA-z (hier problembezogene Ausgabedaten und Grid-Interne Daten) aus der Domäne DO-VO1 werden innerhalb der Domäne DO-P2 durch einen Benutzer P-u aus der Domäne DO-VO2 manipuliert.
B3.5	DA-nz	Integrität	Daten DA-nz aus der Domäne DO-VO1 werden innerhalb der Domäne DO-P2 durch einen Benutzer P-u aus der Domäne DO-VO2 manipuliert.
B3.6	DA-nz DA-z	Integrität	Daten DA-nz und DA-z (hier problembezogene Ausgabedaten und Grid-Interne Daten) aus der Domäne DO-VO1 werden innerhalb der Domäne DO-VO1 durch einen Angreifer P-x manipuliert.
B3.7	DA-nz DA-z	Integrität	Durch die Kompromittierung des „Third-Party"-Mechanismus bei GridFTP gelingt es einem Benutzer P-u aus der Domäne DO-VO2 (in diesem Fall als P-x agierend) Daten DA-nz oder DA-z (hier problembezogene Ausgabedaten und Grid-Interne Daten) aus DO-VO2 zu manipulieren.
AB3.III: Durch unberechtigte Zugriffe wird die für die Verarbeitung der Daten DA-nz und DA-z erforderliche Software (SW) auf Ressourcen innerhalb der Domäne DO-VO1 manipuliert. Die Bedrohung bedeutet, dass Personen außerhalb der Personengruppe P-lad aus DO-P1 bzw. DO-P2 Zugriff auf die für die Berechnung benötigte Software erhalten und diese manipulieren können. Des weiteren sind fortgeschrittene Bedrohungen, z. B. der durch die Manipulation mögliche Zugriff auf Daten DA-nz oder DA-z, möglich.			
B3.8	SW	Integrität	Ein Grid-Nutzer P-u erhält unberechtigten Zugriff auf die SW in DO-VO1 und kann diese manipulieren.
B3.9	SW	Integrität	Ein Angreifer P-x erhält unberechtigten Zugriff auf die SW in DO-VO1 und kann diese manipulieren.
B3.10	DA-z, DA-nz	Vertraulichkeit	Ein Grid-Nutzer P-u aus DO-P3 erhält durch den unberechtigten Zugriff auf die SW in DO-VO1 Einsicht in die Daten DA-z bzw. DA-nz.
B3.11	DA-z, DA-nz	Vertraulichkeit	Ein Angreifer P-x erhält durch den unberechtigten Zugriff auf die SW in DO-VO1 Einsicht in die Daten DA-z (hier problembezogene Ausgabedaten und Grid-Interne Daten) bzw. DA-nz.
AB3.IV: Daten DA-nz oder DA-z verlassen die Domäne DO-VO1. Bedrohungen dieser Klasse bedeuten insbesondere, dass durch z. B. fehlerhafte Konfiguration des *Grid Ressource and Allocation Management (GRAM)* Ressourcen außerhalb der Domäne DO-VO1 für die Verarbeitung von Daten DA-z oder DA-nz aus DO-VO1 verwandt werden und somit Daten in der Domäne DO-P3 verarbeitet werden.			
B3.12	DA-z, DA-nz, SW	Vertraulichkeit	Durch eine fehlerhafte Konfiguration des GRAM durch den P-lad aus DO-P2 gelangen Daten DA-nz, DA-z oder SW aus DO-VO1 in die Domäne DO-P3.
B3.13	DA-nz DA-z SW	Vertraulichkeit	Durch die Kompromittierung des „Third-Party"-Mechanismus bei GridFTP gelingt es einem Benutzer P-u aus der Domäne DO-VO2 Daten DA-nz oder DA-z aus DO-VO1 nach DO-VO2 zu übertragen.

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB3.V: Die angebotenen Grid-Ressourcen aus DO-VO1 werden unberechtigt genutzt. Diese Bedrohung ist mit dem Szenario gleichzusetzen, dass eine Person (P-x), die nicht aus der Domäne DO-VO1 stammt, eine Ressource aus DO-VO1 nutzt.			
B3.14	DO-VO1	Vertraulichkeit	Durch eine Kompromittierung der „GRAM Job Control“ in der Domäne DO-P2 durch einen P-u aus Domäne DO-VO2 können Ressourcen innerhalb DO-VO1 unberechtigt genutzt werden.
B3.15	DO-VO1	Vertraulichkeit	Durch eine fehlerhafte Gestaltung des „Grid Map File“ in der Domäne DO-P2 erhält ein P-u aus DO-VO2 Zugriff auf Daten aus DO-VO1.
B3.16	DO-VO1	Vertraulichkeit	Durch die Veröffentlichung einer maliziösen Software (z. B. Trojanisches-Pferd) eines Forschers (P-x) und die Nutzung durch einen P-u innerhalb der Domäne DO-VO1 erlangt P-x unberechtigt Zugriff auf Ressourcen innerhalb DO-VO1.

2.3.5 Risikoanalyse

Im Folgenden werden die Schadenshöhe und Eintrittswahrscheinlichkeiten der im vorigen Kapitel aufgeführten Bedrohungen abgeschätzt. Die Ursache für das Eintreten der jeweiligen Bedrohung kann vielfältig sein. Um die Abschätzung nachvollziehen zu können, wird auf die möglichen Ursachen im Rahmen der Bemerkung Bezug genommen.

Tabelle 8: Risikoanalyse Szenario 3

Risiko Nr.	Bedrohung	Schadenshöhe	Eintrittswahrscheinlichkeit	Bemerkung
R3.1	B3.1	sehr hoch	niedrig	Die Auswirkungen der Auswahl eines nicht vertrauenswürdigen Kooperationspartners sind vielfältig und können gravierende finanzielle und ggf. auch rechtliche Auswirkungen haben. Ist der jeweilige Partner z. B. nicht in der Lage, die Sicherheitsanforderungen ausreichend zu gewährleisten, sind die Daten DA-z und DA-nz bedroht, wenn sie innerhalb DO-VO1 verarbeitet werden. Die Eintrittswahrscheinlichkeit wird als niedrig eingestuft, da eine gewissenhafte Auswahl eines Kooperationspartners angenommen wird. Siehe auch R2.1

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R3.2	B3.2	hoch	sehr hoch	**Worst-Case-Abschätzung** Das Schadenspotenzial der Manipulation von DA-z (hier problembezogene Ausgabedaten und Grid-Interne Daten) wird mit hoch abgeschätzt, da z. B. Konfigurationsdaten für die Funktionsfähigkeit des Grid fundamental sind. Die Eintrittswahrscheinlichkeit wird mit sehr hoch abgeschätzt, wenn von einer vorsätzlichen Handlung ausgegangen wird und der P-lad die DA-z innerhalb seiner Domäne manipuliert. Bei einer vorsätzlichen Handlung ist vom lokalen Administrator P-lad nur geringer Aufwand erforderlich, um jegliche Manipulationen durchzuführen. Spezielle Sicherheitsmaßnahmen, die gegen nicht-vertrauenswürdige Administratoren wirken, sind nicht vorhanden.
R3.3	B3.2	hoch	niedrig	Das Schadenspotenzial der Manipulation von DA-z (hier problembezogene Ausgabedaten und Grid-Interne Daten) wird mit hoch abgeschätzt, da z. B. Konfigurationsdaten für die Funktionsfähigkeit des Grid fundamental sind. Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, wenn das Szenario betrachtet wird, dass der P-lad aus DO-P2 versucht DA-z in DO-P1 zu manipulieren. In diesem Fall besitzt der P-lad keinerlei Rechte in DO-P1 und ist als nicht zur Domäne gehörende Person (P-x aus der Sicht von DO-P1) anzusehen, der zu betreibende Aufwand für die Durchführung eines erfolgreichen Angriffs wird als erheblich angesehen, da etablierte Sicherheitsmechanismen vorhanden sind.
R3.4	B3.3	hoch	sehr hoch	Das Schadenspotenzial der Manipulation von DA-nz wird mit hoch abgeschätzt, da die auf die DA-nz aufbauenden Ergebnisse ggf. falsch und damit unbrauchbar sind. Die Eintrittswahrscheinlichkeit wird mit sehr hoch abgeschätzt, wenn von einer vorsätzlichen Handlung ausgegangen wird und der P-lad die DA-z innerhalb seiner Domäne manipuliert. Bei einer vorsätzlichen Handlung ist vom lokalen Administrator P-lad nur geringer Aufwand erforderlich, um jegliche Manipulationen durchzuführen. Spezielle Sicherheitsmaßnahmen, die gegen nicht-vertrauenswürdige Administratoren wirken, sind nicht vorhanden.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R3.5	B3.3	hoch	niedrig	Das Schadenspotenzial der Manipulation von DA-nz wird mit hoch abgeschätzt, da die auf die DA-nz aufbauenden Ergebnisse ggf. falsch und damit unbrauchbar sind. Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, wenn das Szenario betrachtet wird, dass der P-lad aus DO-P2 versucht DA-nz in DO-P1 zu manipulieren. In diesem Fall besitzt der P-lad keinerlei Rechte in DO-P1 und ist als nicht zur Domäne gehörende Person (P-x aus der Sicht von DO-P1) anzusehen. Der durch den P-lad zu betreibende Aufwand für die Durchführung eines erfolgreichen Angriffs wird als erheblich angesehen, da etablierte Sicherheitsmechanismen vorhanden sind.
R3.6	B3.4	hoch	niedrig	Das Schadenspotenzial der Manipulation von DA-z (hier problembezogene Ausgabedaten und Grid-Interne Daten) wird mit hoch abgeschätzt, da z. B. Konfigurationsdaten für die Funktionsfähigkeit des Grid fundamental sind. Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da davon ausgegangen wird, dass Benutzerberechtigungen in allen Domänen durch den zuständigen P-lad sorgfältig gepflegt und etablierte Sicherheitsmechanismen (vgl. 2.3.4) umgesetzt sind. Der durch einen P-u aus DO-VO2 zu betreibenden Aufwand für einen erfolgreichen Angriff auf DA-z aus DO-VO1 wird als sehr hoch eingestuft, die Eintrittswahrscheinlichkeit für die Bedrohung daher als niedrig.
R3.7	B3.5	hoch	niedrig	Das Schadenspotenzial der Manipulation von DA-nz wird mit hoch abgeschätzt, da die auf die DA-nz aufbauenden Ergebnisse ggf. falsch und damit unbrauchbar sind. Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da davon ausgegangen wird, dass Benutzerberechtigungen durch den P-lad sorgfältig gepflegt und etablierte Sicherheitsmechanismen (vgl. 2.3.4) umgesetzt sind. Der durch einen P-u aus DO-VO2 zu betreibenden Aufwand für einen erfolgreichen Angriff auf DA-z aus DO-VO1 wird als sehr hoch eingestuft, die Eintrittswahrscheinlichkeit für die Bedrohung daher als niedrig.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R3.8	B3.6	hoch	niedrig	Das Schadenspotenzial der Manipulation von DA-nz wird mit hoch abgeschätzt, da sowohl die auf die DA-nz aufbauenden Ergebnisse ggf. falsch und damit unbrauchbar sind als auch die Funktionsfähigkeit durch eine Manipulation gefährdet ist. Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da davon ausgegangen wird, dass etablierte Sicherheitsmechanismen (vgl. 2.3.4, z. B. Firewallmechanismen) umgesetzt sind. Der durch einen P-x (ohne Zugriff auf DO-VO1 oder DO-VO2) zu betreibenden Aufwand für einen erfolgreichen Angriff wird als sehr hoch eingestuft, die Eintrittswahrscheinlichkeit für die Bedrohung daher als niedrig.
R3.9	B3.7	hoch	niedrig	Das Schadenspotenzial der Manipulation von DA-nz wird mit hoch abgeschätzt, da sowohl die auf die DA-nz aufbauenden Ergebnisse ggf. falsch und damit unbrauchbar sind als auch die Funktionsfähigkeit durch eine Manipulation gefährdet ist. Die Bedrohung kann lediglich durch eine fehlerhafte Konfiguration (der Benutzerberechtigung durch einen P-lad) oder durch eine direkte Manipulation der auf den Third-Party Ressourcen installierten GridFTP-Server eintreten. Die Wahrscheinlichkeit wird mit niedrig abgeschätzt, da keine direkten Angriffspfade für eine Kompromittierung bekannt sind und von einer sorgfältigen Konfiguration auszugehen ist.
R3.10	B3.8	hoch	niedrig	Durch die Manipulation der Software (SW) durch einen P-u auf einer Grid-Ressource können erhebliche Schäden entstehen, da in diesem Fall von einer fehlerhaften Funktion des Grid ausgegangen wird, die Ergebnisse somit verfälscht sein könnten. Das Schadenspotenzial wird daher als hoch eingeschätzt. Die Eintrittswahrscheinlichkeit wird als niedrig eingestuft, da eine sorgfältige Konfiguration der Komponenten, insbesondere der Benutzerrechte, angenommen wird. Somit ist für einen Benutzer mit lokalen Rechten (P-u) ein erheblicher Aufwand zu betreiben, unberechtigte Manipulationen an SW vorzunehmen.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R3.11	B3.9	hoch	niedrig	Durch die Manipulation der Software (SW) durch einen P-x auf einer Grid-Ressource können erhebliche Schäden entstehen, da in diesem Fall von einer fehlerhaften Funktion des Grid ausgegangen wird, die Ergebnisse somit verfälscht sein könnten. Das Schadenspotenzial wird daher als hoch eingeschätzt. Die Eintrittswahrscheinlichkeit wird als niedrig eingestuft, da eine sorgfältige Konfiguration der Komponenten, insbesondere der Benutzerrechte, angenommen wird. Somit ist insbesondere für einen Benutzer ohne lokalen Rechten (P-x) ein erheblicher Aufwand zu betreiben, unberechtigte Manipulationen an SW vorzunehmen.
R3.12	B3.10	mittel	mittel	Die Schadenshöhe wird mit mittel eingestuft, da an die Vertraulichkeit sowohl von DA-z als auch von DA-nz keine besonders hohen Anforderungen gestellt werden. Die Eintrittswahrscheinlichkeit wird mit mittel eingestuft, da insbesondere der Fall, bei dem ein P-u aus DO-P3 innerhalb der Domäne DO-P2 auf lokale SW eines P-u aus DO-P1 lesende Zugriffsrechte besitzt als wahrscheinlich angesehen wird. Insbesondere wenn die P-u z. B. auf einer unter Unix betriebenen Grid-Ressource derselben Benutzergruppe angehören.
R3.13	B3.11	mittel	niedrig	Die Schadenshöhe wird mit mittel eingestuft, da an die Vertraulichkeit sowohl von DA-z als auch von DA-nz keine besonders hohen Anforderungen gestellt werden. Die Eintrittswahrscheinlichkeit wird mit niedrig eingestuft, da vom Vorhandensein etablierter Sicherheitsmechanismen ausgegangen wird und somit ein hoher Aufwand durch einen externe Angreifer P-x zu betreiben ist.
R3.14	B3.12	hoch	niedrig	Insbesondere aufgrund der hohen Anforderungen an die Vertraulichkeit der SW wird die Schadenshöhe hier mit hoch eingestuft. Gelangt ein SW aus DO-P1 in DO-P3 ist die Vertraulichkeit gefährdet. Die Eintrittswahrscheinlichkeit wird im Falle eines fahrlässigen Konfigurationsfehlers (z. B. durch einen P-lad) innerhalb des GRAM mit niedrig abgeschätzt, da von einer sorgfältigen Konfiguration ausgegangen wird.

Risiko Nr.	Bedrohung	Schadenshöhe	Eintrittswahrscheinlichkeit	Bemerkung
R3.15	B3.13	hoch	niedrig	Insbesondere aufgrund der hohen Anforderungen an die Vertraulichkeit der SW wird die Schadenshöhe hier mit hoch eingestuft. Gelangt ein P-u aus DO-P3 an die SW aus DO-P1 ist die Vertraulichkeit gefährdet. Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da keine Schwachstellen im GridFTP bekannt sind und der Aufwand für eine erfolgreiche Kompromittierung durch einen P-u aus DO-VO2 daher mit hoch abgeschätzt wird.
R3.16	B3.14	niedrig	niedrig	Das direkte Schadenspotenzial wird mit niedrig abgeschätzt, da in diesem Fall zwar von einer unberechtigten Nutzung der Ressourcen innerhalb DO-VO1 auszugehen ist, die Folge aber lediglich eine Verzögerte Abwicklung der Jobs berechtigter P-u aus DO-VO1. Erst durch kombinierte Bedrohungen, z. B. wenn es einem P-u aus DO-P3 durch einen fortgeschrittenen Angriff zusätzlich gelingt eine Benutzerberechtigung innerhalb DO-P1 zu kompromittieren, erhöht sich die Schadenshöhe. Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da zum einen keine Angriffe gegen das GRAM bekannt sind, zum anderen eine sorgfältige Konfiguration der Ressourcen durch den P-lad angenommen wird. Somit ist für den P-u aus DO-VO3 ein hoher Aufwand für den Angriff zu betreiben.
R3.17	B3.15	hoch	mittel	Insbesondere aufgrund der hohen Anforderungen an die Vertraulichkeit der SW wird die Schadenshöhe hier mit hoch eingestuft. Gelangt ein P-u auf SW aus DO-VO1 ist die Vertraulichkeit gefährdet. Die Eintrittswahrscheinlichkeit wird mit mittel abgeschätzt, da sich in der Praxis fehlerhaftes Berechtigungsmanagement immer als Fehlerquelle herausstellt. Es wird daher – trotz einer sorgfältigen Konfiguration des Grid Map File – von einer mittleren Wahrscheinlichkeit ausgegangen (siehe auch R3.12), dass ein P-u aus DO-VO2 auf Daten aus DO-VO1 zugreifen kann.
R3.18	B3.16	hoch	niedrig	Gelingt es einem P-x, maliziöse Software in die Domäne DO-VO1 einzuschleusen und durch einen P-u ausführen zu lassen, sind Daten und Ressourcen der Domäne gefährdet und P-x kann sämtliche Ressourcen und Daten nutzen. Der mögliche Schaden wird mit hoch abgeschätzt. Im Fall, dass die Software im Quelltext vorliegt, wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt. In diesem Fall ist davon auszugehen, dass der P-u die Software im Rahmen seiner Sorgfaltspflichten prüft.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R3.19	B3.16	hoch	hoch	Gelingt es einem P-x, maliziöse Software in die Domäne DO-VO1 einzuschleusen und durch einen P-u ausführen zu lassen, sind Daten und Ressourcen der Domäne gefährdet und P-x kann sämtliche Ressourcen und Daten nutzen. Der mögliche Schaden wird mit hoch abgeschätzt. Im Fall, dass es sich bei der Software um Binärcode (compilierte Software) handelt, wird die Eintrittswahrscheinlichkeit mit hoch abgeschätzt. In diesem Fall hat P-u keine Möglichkeit die Software umfassend auf Schadfunktionen zu prüfen .

In der nachfolgenden Risikomatrix sind sowohl die Eintrittswahrscheinlichkeit (x-Achse) als auch die Schadenshöhe (y-Achse) des jeweiligen Risikos aus Tabelle 8 dargestellt.

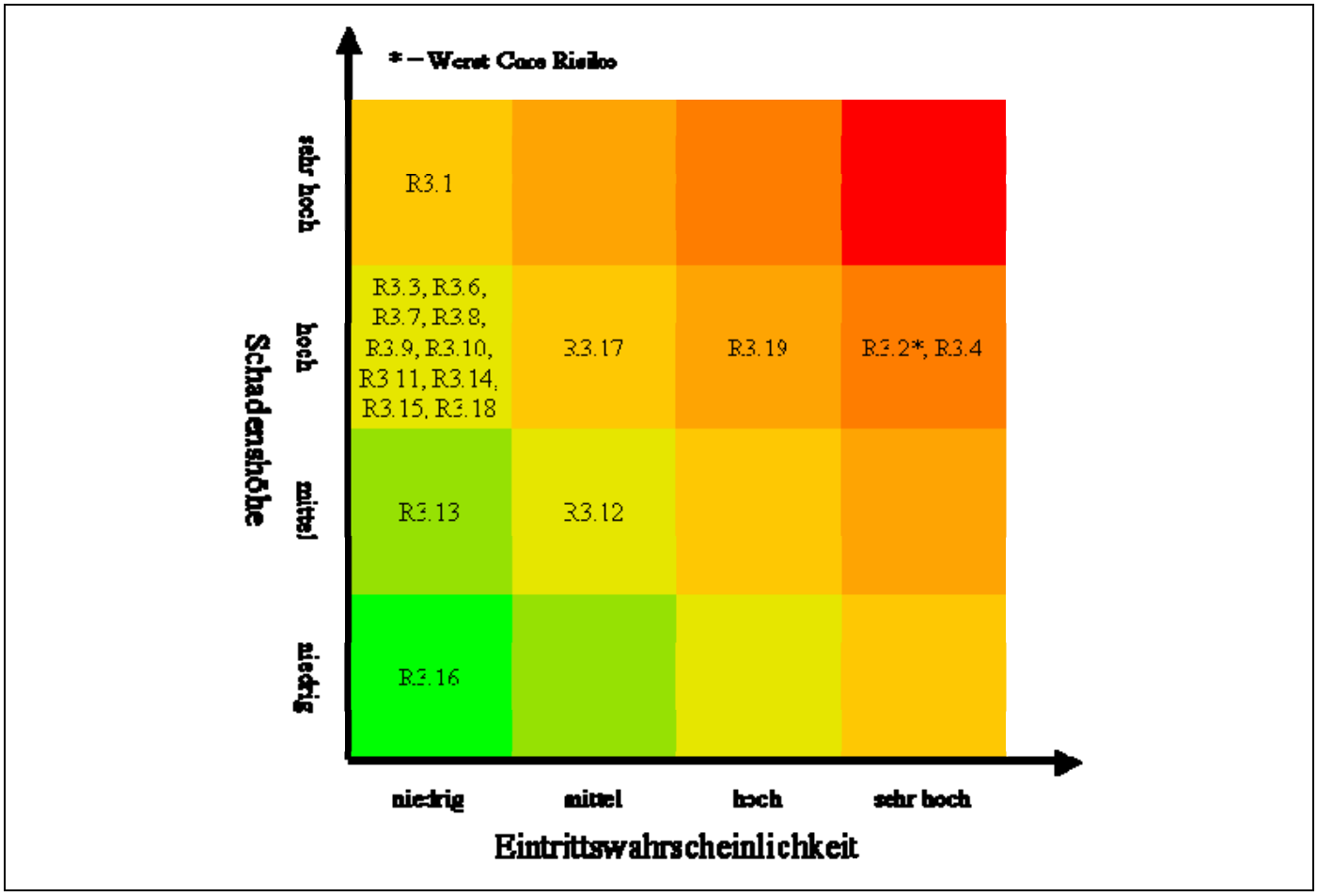

Abbildung 3: Risikomatrix Szenario 3

2.3.6 Fazit der Risikoanalyse

Im Folgenden werden die Erkenntnisse, die im Rahmen der Erstellung der Risikoanalyse für dieses Szenario gewonnen wurden, zusammengefasst.

Etablierte Sicherheitsmechanismen

Sicherheitsmechanismen, die sich auch außerhalb des Grid-Kontextes etabliert haben, erweisen sich auch in diesem Beispielszenario als Wirkungsvoll gegen Risiken, die in diesem Szenario relevant sind. Insbesondere die auch in den übrigen Szenarien als wirkungsvolle Maßnahme vorhandene Verschlüsselung der Kommunikation, wie auch die Authentikation schränken in diesem Szenario die relevanten Risiken stark ein. Hinzu kommt der relativ geringe Schutzbedarf der betrachteten Objekte, so dass lediglich vier kritische Risiken (R3.1, R3.2, R3.4 und R3.17) identifiziert werden konnten. Risiken, die aus gezielten Angriffen von Personen ohne Zugriffsberechtigung ausgehen werden durch vorhandene und etablierte Sicherheitsmechanismen (Authentikation, bauliche Sicherheit) stark eingeschränkt. Lediglich die Insider-Problematik stellt sich auch in diesem Szenario als kritisch dar und ist noch nicht durch technische Maßnahmen lösbar. Die Insider-Problematik ist zwar nicht spezifisch für den Grid-Kontext, entwickelt hier jedoch besondere Brisanz, da hochsensible Daten in eine fremde Domäne transferiert werden.

Potenzielle Risiken

Aufgrund des als gering eingestuften Schutzbedarfs der Objekte in diesem Szenario sind lediglich die Risiken R3.1, R3.2, R3.4 und R3.17 hervorzuheben. Insbesondere das Risiko R3.1 (Versäumnisse im Rahmen der VO-Bildung) ist in diesem Szenario von besonderer Bedeutung, da in diesem Prozess die Grundlage für die Vertrauenswürdigkeit der gebildeten Virtuellen-Organisation (Domäne DO-VOx) gelegt wird. Wie bereits im Fazit zu Szenario 2 erläutert sind Fehler, die in diesem Prozess begangen werden, nicht oder nur schwer durch technische Maßnahmen bei der Nutzung / dem Betrieb des Grid zu kompensieren

Fazit

Die in diesem Szenario angenommenen technischen und organisatorischen Sicherheitsmechanismen entsprechen dem Stand der Technik und werden als angemessen angesehen. Auch hier ist bedenklich, dass die Wirksamkeit der vorhandenen Sicherheitsmechanismen maßgeblich von der sorgfältigen Administration aller Komponenten/Ressourcen abhängig (vgl. z.B. R3.6). Die lokal wirkenden Administratoren (P-lad) können ohne großen Aufwand jeden denkbaren Angriff durchführen (vgl. z.B. R3.4), wenn ausreichende kriminelle Energie und damit ausreichende Mittel vorausgesetzt werden. Wie auch in den anderen Szenarien erläutert, ist dies ein – auch außerhalb des Grid-Kontextes – bekanntes und derzeit mit technischen Mitteln schwer zu lösendes Problem. Hier sind organisatorische Maßnahmen zur Risikoeindämmung erforderlich.

An dieser Stelle tritt in der Betrachtung des Risikos insbesondere die Organisation des Grid in den Mittelpunkt, also die Phase während derer das Grid gebildet wird. Defizite und Risiken lassen sich insbesondere im Bereich der Organisation des Grid, also innerhalb des Prozesses der Bildung virtueller Organisationen (VO), finden (vgl. z.B. R3.1). Bei der Betrachtung der Sicherheitsmechanismen fällt auf, dass kein Domänen-übergeordnetes Sicherheitsmanagement implementiert ist und wichtige Sicherheitsprozesse (z. B. regelmäßiges Audit der Grid-Infrastruktur) fehlen. Vor dem Hintergrund der „Offenheit“ und „Virtualität“ eines Grid erscheint dieses Defizit plausibel und nachvollziehbar, denn innerhalb eines Grid fehlt die Rolle eines übergeordneten Verantwortlichen, eines übergeordneten Management und damit fehlen die im Sicherheitsmanagement etablierten – und strengen – Prozesse und Mechanismen. Dies gilt für alle betrachteten Szenarien und ist kein Problem, welches für ein einzelnes Szenario spezifisch ist.

2.4 Bedrohungs- und Risikoanalyse Szenario 4

Grids mit personenbezogenen bzw. personenbeziehbaren Daten sind durch hohe Anforderungen an die Vertraulichkeit der verarbeiteten Daten gekennzeichnet. Insbesondere in der (medizinischen) Forschung steht dieser hohe Vertraulichkeitsanspruch im Widerspruch zur „Offenheit“ der dort etablierten offenen e-Science-Grids (vgl. Szenario 3). Insbesondere aus der Sicht der Ressourcen-Provider, die personenbeziehbare Daten in das Grid einbringen, stellt sich die Frage nach der Gewährleistung ihrer Schutzansprüche.

Ausgehend von aktuellen Diskussionen im MammoGRID-Umfeld konzentriert sich die Risikoanalyse des Szenarios 4 auf die Fragestellung der möglichen Kompromittierung der personenbezogenen bzw. personenbeziehbaren Daten (DA-zpp und DA-zp) sowie der Frage nach der Protokollierung der Zugriffe auf diese Daten.

2.4.1 Sicherheitsanforderungen

In [3] wurden Sicherheitsanforderungen und Zugriffsberechtigungen für das Szenario 4 definiert, für die Risikoanalyse werden diese konkretisiert.

SA4.I: Die gesetzlichen Ansprüchen an die ärztliche Schweigepflicht sowie den Datenschutz werden erfüllt.

SA4.II: Die persönliche Unversehrtheit des Patienten P-p wird gewährleistet.

SA4.III: Nur der Arzt und dessen medizinisches Fachpersonal kann einen Personenbezug bei erfassten Daten herstellen.

SA4.IV: Eine unberechtigte Nutzung/Veränderung von DA-zpp, DA-zp und DA-z wird verhindert.

SA4.V: Zugriffe auf DA-zpp und DA-zp sowie deren Datenfluss sind rekonstruierbar (d. h. nachvollziehbar).

SA4.VI: Die angebotenen Grid-Ressourcen aus DO-srvp, DO-swp, DO-hwp und DO-dap stehen nur berechtigten Personen zur Verfügung.

2.4.2 Abstrakte Bedrohungen

Aus den o. g. Sicherheitsanforderungen werden abstrakte Bedrohungen abgeleitet, die anschließend verfeinert und für die Risikoanalyse genutzt werden:

AB4.I: Durch unberechtigte Handlungen werden die ärztliche Schweigepflicht oder der Datenschutz verletzt.

AB4.II: Ein Personenbezug kann durch andere Personen als den Arzt und dessen medizinisches Fachpersonal hergestellt werden.

AB4.III: Unberechtigte erhalten Einblick auf DA-zpp, DA-zp oder DA-z.

AB4.IV: DA-zpp, DA-zp, DA-z oder DA-nz werden unberechtigt und unbemerkt verändert.

AB4.V: Erfolgte Zugriffe auf DA-zpp oder DA-zp oder deren Fluss durch die Komponenten des Grid können nicht nachvollzogen werden.

AB4.VI: Die angebotenen Grid-Ressourcen aus DO-srvp, DO-swp, DO-hwp und DO-dap werden unberechtigt genutzt.

AB4.VII: Die persönliche Unversehrtheit der Patienten P-p ist gefährdet.

2.4.3 Annahmen zu Sicherheitsmaßnahmen

Die derzeit im Einsatz befindlichen Grids in diesem Umfeld (z. B. MammoGRID) besitzen bereits Sicherheitsmechanismen, deren Vorhandensein und Wirksamkeit im Rahmen der Risikoanalyse angenommen wird. Nachfolgend sind die wesentlichen Sicherheitsmechanismen zusammengefasst:

- DA-zpp, DA-zp und DA-z sind durch Verschlüsselung (VPN) bei der Übertragung vor unberechtigter Einsichtnahme und Veränderung geschützt.
- Auf den einzelnen Grid-Ressourcen sind derzeit übliche (Best-Practice oder Grundschutz) Sicherheitsmaßnahmen umgesetzt, hierzu gehören beispielsweise:
  - Geeignete Authentikationsmechanismen sichern den Zugriff auf die in der Domäne DO-dap enthaltenen Daten DA-zp und DA-z ab.
  - Backupdatenträger in der Domäne DO-e werden geschützt aufbewahrt und sicher entsorgt.
  - Der Zutritt zu Räumen und Zugriff auf Ressourcen ist durch geeignete Maßnahmen abgesichert.
- Die Vertrauenswürdigkeit der Administratoren P-ad und P-lad sowie der Ressourcen-Provider P-srvp, P-swp, P-hwp und P-dap ist durch entsprechende Maßnahmen beim Einstellungsprozess sichergestellt.

2.4.4 Bedrohungsanalyse

Ausgehend von den Abstrakten Bedrohungen AB4 werden nachfolgende konkrete Bedrohungen aufgestellt. Die Bedrohungen resultieren hierbei aus den in Tabelle 27 aus [3] geschilderten Abläufen.

Tabelle 9: Bedrohungsanalyse Szenario 4

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB4.I: Durch unberechtigte Handlungen wird die ärztliche Schweigepflicht oder der Datenschutz verletzt. Diese Bedrohungsgruppe ist mit einem Verlust der Vertraulichkeit der Personendaten DA-zpp gleichzusetzen. Es werden die konkreten Bedrohungen aufgeführt, die zur o. g. abstrakten Bedrohung führen können.			
B4.1	DA-zpp	Vertraulichkeit	Der lokale Administrator P-lad in der Domäne DO-e erhält unberechtigt Einsicht auf DA-zpp (Personendaten).
B4.2	DA-zpp	Vertraulichkeit	Ein Patient P-p innerhalb der Domäne DO-e erhält unberechtigt Zugriff auf DA-zpp (Personendaten) eines anderen P-p.
B4.3	DA-zpp	Vertraulichkeit	Ein Angreifer P-x erlangt gezielt Zugriff auf die DA-zpp (Personendaten).
B4.4	DA-zpp	Vertraulichkeit	Eine Person außerhalb der Domäne DO-e erhält unberechtigt Zugriff auf DA-zpp (Personendaten).
AB4.II: Ein Personenbezug kann durch andere Personen als den Arzt und dessen medizinisches Fachpersonal hergestellt werden. An dieser Stelle werden lediglich Bedrohungen betrachtet, die noch nicht durch AB4.I abgedeckt sind. Ein Personenbezug kann nur dann hergestellt werden, wenn die Pseudonymisierung/Anonymisierung fehlerhaft ist oder manipuliert wurde.			
B4.5	SW	Verfügbarkeit	Die für die Pseudonymisierung/Anonymisierung der Personendaten DA-zpp verwandte Software arbeitet fehlerhaft.

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
B4.6	SW	Integrität	Die für die Pseudonymisierung/Anonymisierung der Personendaten DA-zpp verwandte Software oder Funktionalität wird durch den P-lad manipuliert.
B4.7	DA-z	Vertraulichkeit	Die für die Wiederherstellung des Personenbezugs benötigten Pseudonyme werden einem Nutzer der pseudonymisierten Daten (P-up) bekannt.
AB4.III: Unberechtigte erhalten Einblick auf DA-zp oder DA-z Diese Bedrohungen decken das Szenario ab, bei dem Personen, die lokale Berechtigungen auf den Grid-Ressourcen besitzen, unberechtigt Einblick in zugriffsgeschützte Daten (personenbeziehbare Daten DA-zp und zugriffsbeschränkte Daten DA-z) erhalten. Hierbei muss zwischen Personen mit besonderen Rechten (Administratoren und Providern) und lokalen Benutzern unterschieden werden.			
B4.8	DA-zp DA-z	Vertraulichkeit	Lokale Benutzer P-x der Grid-Ressourcen innerhalb der Domäne DO-hw erhalten unberechtigt Zugriff auf DA-zp und DA-z.
B4.9	DA-zp DA-z	Vertraulichkeit	Ein Grid-Nutzer P-u mit Berechtigung auf Grid-Ressourcen innerhalb der Domäne DO-hw erhält unberechtigt Zugriff auf DA-zp und DA-z.
B4.10	DA-zp DA-z	Vertraulichkeit	Lokale Administratoren P-lad der Grid-Ressourcen innerhalb der Domäne DO-hw erhalten unberechtigt Zugriff auf DA-zp (personenbeziehbare Daten) und DA-z (hier z. B. anonymisierte Patientinnendaten).
B4.11	DA-zp DA-z	Vertraulichkeit	Ressourcenprovider der Grid-Ressourcen (P-svp, P-swp, P-hwp, P-dap) innerhalb der Domäne DO-hw erhalten unberechtigt Zugriff auf DA-zp (personenbeziehbare Daten) und DA-z (hier z. B. anonymisierte Patientinnendaten).
B4.12	DA-zp DA-z	Vertraulichkeit	DA-zp/DA-z werden bei der Übertragung einem Unberechtigten bekannt.
AB4.IV: DA-zpp, DA-zp, DA-z oder DA-nz werden unberechtigt und unbemerkt verändert. Diese Bedrohungen betreffen die Integrität der jeweiligen Daten. Schwerpunkt der Betrachtung ist die unbemerkte Manipulation, da festgestellte Manipulationen durch eine vorhandene Datensicherung wiederhergestellt werden können.			
B4.13	DA-zpp	Integrität	Patientendaten (DA-zpp) werden innerhalb der Domäne DO-e durch den P-lad manipuliert.
B4.14	DA-zpp	Integrität	Patientendaten (DA-zpp) werden innerhalb der Domäne DO-e durch einen P-p manipuliert.
B4.15	DA-zp	Integrität	Die in der Domäne DO-dap befindlichen DA-zp werden durch den lokalen Administrator P-lad manipuliert.
B4.16	DA-zp	Integrität	Die in der Domäne DO-dap befindlichen DA-zp werden durch einen P-up manipuliert.
B4.17	DA-zp	Integrität	Die in der Domäne DO-dap befindlichen DA-zp werden durch einen lokalen Benutzer P-x der Domäne DO-dap manipuliert.
B4.18	DA-z	Integrität	Die Auditingdaten (DA-z) werden durch einen lokalen Administrator P-lad in der Domäne DO-hw manipuliert.

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
B4.19	DA-nz	Integrität	Frei zugängliche Daten DA-nz werden durch einen lokalen Administrator P-lad der Domäne DO-hw manipuliert.
B4.20	DA-nz	Integrität	Frei zugängliche Daten DA-nz in der Domäne DO-dap werden durch einen P-u der Domäne DO-u manipuliert.
AB4.V: Erfolgte Zugriffe auf DA-zpp oder DA-zp oder deren Fluss durch die Komponenten des Grid können nicht nachvollzogen werden. Ursache kann das Manipulieren/Löschen der Auditingdaten oder die Deaktivierung/Manipulation der Auditingfunktion der Datenbank in der Domäne DO-dap sein. Des weiteren ist hier das Fehlen einer geeigneten Auditing Funktionalität in der eingesetzten Software zu berücksichtigen.			
B4.21	DA-z	Integrität	Die Auditingdaten (DA-z) wurden manipuliert/gelöscht (s.o)
B4.22	SW	Integrität	Die Auditingfunktionalität innerhalb der Domäne DO-dap wurde manipuliert/deaktiviert.
B4.23	SW	Verfügbarkeit	Die innerhalb der Domäne DO-hw eingesetzte Software besitzt keine ausreichende Auditingfunktionalität.
AB4.VI: Die angebotenen Grid-Ressourcen aus DO-srvp, DO-swp, DO-hwp und DO-dap werden unberechtigt genutzt. Diese Bedrohung ist mit dem Szenario gleichzusetzen, dass eine Person (P-x), die nicht aus der Domäne DO-u stammt, eine Ressource aus DO-hw nutzt.			
B4.24	SW SRV HW	Vertraulichkeit	Eine unberechtigte Person P-x erlangt Zugriff auf eine Grid-Ressource innerhalb der Domäne DO-hw.
AB4.VII: Die persönliche Unversehrtheit der Patienten P-p ist gefährdet.			
B4.25	DA-zpp	Verfügbarkeit	Durch Diebstahl, Löschung, Brand oder Ereignisse gehen die Patientendaten (DA-zpp) verloren.

Die in Tabelle 9 aufgeführten Bedrohungen haben generischen Charakter und sind auch für Szenarien außerhalb des Grid-Kontextes gültig. Da im betrachteten Szenario existierende Komponenten von Grid-Middleware genutzt werden (z. B. Globus), werden in der nachfolgenden Tabelle 10 zusätzliche konkrete Grid-spezifische Bedrohungen (BK) dargestellt. Jede dieser spezifischen Bedrohungen einer oder mehreren abstrakten Bedrohungen zugeordnet werden, die in der letzten Spalte der Tabelle angegeben werden. In der nachfolgenden Risikoanalyse werden diese Bedrohungen BK ebenfalls berücksichtigt.

Tabelle 10: Grid-spezifische Konkretisierung von Bedrohungen

Konkretisierung Nr.	Konkretisierung von Risiken	Beschreibung	Zugehörige abstrakte Bedrohung
BK4.1	Kompromittierung des „Third-Party"-Mechanismus bei GridFTP	Der Datentransfer bei Nutzung von Globus als Grid-Middleware erfolgt auf Basis von GridFTP. Dabei werden unter Kontrolle einer Leitinstanz Datentransfers zwischen zwei anderen Systemen (Folgeinstanzen) durchgeführt. Hier ist sowohl die Authentizität der Leit- als auch der Folgeinstanzen zu wahren, damit weder von einer unberechtigten Leitinstanz Dateiübertragungen beauftragt noch von einer anderen als der jeweils berechtigten Folgeinstanz gesendet bzw. entgegengenommen werden.	AB4.IV, AB4.V
BK4.2	Kompromittierung der „GRAM Job Control"	Die Globus-Komponente „GRAM" steuert u. a. die Ausführung von Aufträgen auf anderen Systemen des Grid. Hier ist ggf. sowohl die Authentizität der initiierenden als auch der Adapterinstanzen zu wahren, damit nicht eine unbefugte Instanz einen Auftrag erteilt bzw. ein solcher nicht an eine andere als die dazu bestimmte Instanz erteilt wird.	AB4.VI
BK4.3	Kompromittierung des „Grid Map File"	Die Globus-Komponente „GRAM" steuert u. a. die Ausführung von Aufträgen auf anderen Systemen des Grid. Dabei werden globale Grid-ID's auf lokale abgebildet (unter Verwendung lokaler GRAM-Adapter und des Grid Map File). Beim Grid Map File stellt fehlende Integrität eine Bedrohung dar, da evtl. Aufträge mit falschen Benutzerrechten ausgeführt und damit andere Sicherheitsmechanismen unterlaufen werden.	AB4.VI
BK4.4	Unzureichende Job-Abschottung auf einzelnen Rechnern des Grid	Anhand typischer Systemkennwerte (Beobachtung der Prozessaktivitäten anderer Benutzer, etwa mit den Unix-/Linux-Kommandos `ps`, `finger`, `who` u. ä.) lassen sich ggf. unter Anwendung branchentypischen Fachwissens Rückschlüsse auf Aktivitäten von Konkurrenten ziehen. So könnte bspw. ein Automobilhersteller einen Mitbewerber „beobachten" und anhand des Verhaltens von dessen Aufträgen (Laufzeit, CPU-Last, Anzahl der Aufträge etc.) Rückschlüsse auf den Entwicklungsstand eines neuen Modells ziehen.	AB4.III
BK4.5	Fehlerhafte Authentisierung der Client-Systeme bzw. der dortigen Benutzer	Client-Systeme werden dazu verwendet, Aufträge und Daten ins Grid zu füllen. Hier ist die Authentizität der Client-Systeme und der dortigen Benutzer sicher zu stellen. Beim Daten- und Dateitransfer vom und zum Client-System müssen Integrität und Vertraulichkeit erhalten bleiben, damit nicht von einem unberechtigten Benutzer und/oder einem unberechtigten Client aus auf Grid-Ressourcen zugegriffen werden kann.	AB4.III, AB4.IV, AB4.V

Konkretisierung Nr.	Konkretisierung von Risiken	Beschreibung	Zugehörige abstrakte Bedrohung
BK4.6	Unberechtigter Zugriff auf „Proxy Certification Files“	„Proxy Certification Files“ enthalten u. a. einen in der Lebensdauer beschränkten privaten temporären Schlüssel („Temporary Private Key“). Dessen Bekanntwerden erlaubt zumindest bis zum Ende der Nutzungszeit des Schlüssels oder des zugehörigen Zertifikats, den echten „User Proxy“ durch einen gefälschten zu ersetzen. Integrität und Vertraulichkeit des „Proxy Certification Files“ müssen daher gewahrt bleiben.	AB4.III, AB4.IV, AB4.VI

2.4.5 Risikoanalyse

Im Folgenden werden die Schadenshöhe und Eintrittswahrscheinlichkeiten der im vorigen Kapitel aufgeführten Bedrohungen abgeschätzt. Die Ursache für das Eintreten der jeweiligen Bedrohung kann vielfältig sein. Um die Abschätzung nachvollziehen zu können, wird auf die möglichen Ursachen im Rahmen der Bemerkung Bezug genommen.

Zusätzlich werden auch die spezifischen Bedrohungen BK aus Tabelle 10 berücksichtigt. Zur besseren Unterscheidung werden die Risiken, die auf diese Bedrohungen zurückzuführen sind mit RK bezeichnet und mit einer eigenen Nummerierung versehen.

Tabelle 11: Risikoanalyse Szenario 4

Risiko Nr.	Bedrohung	Schadenshöhe	Eintrittswahrscheinlichkeit	Bemerkung
R4.1	B4.1	niedrig	hoch	Aufgrund seiner weitreichenden Rechte innerhalb der Domäne muss davon ausgegangen werden, dass der lokale Administrator (P-lad) mit hoher Wahrscheinlichkeit Zugriff auf personenbezogene Daten (DA-zpp) erhalten kann. Es ist jedoch nur von einem geringen Schaden auszugehen, da Mitarbeiter per Gesetz zur Verschwiegenheit verpflichtet sind.
R4.2	B4.2	hoch	mittel	Durch geeignete Maßnahmen (Zutritts- und Zugriffsschutz) innerhalb der Domäne DO-e wird der Zugriff auf Patientendaten (DA-zpp) für unberechtigte P-p verhindert. Es wird eine mittlere Eintrittswahrscheinlichkeit angesetzt, da davon auszugehen ist, dass dieses Ereignis z. B. durch Unachtsamkeit (z. B. fehlender Bildschirmschoner) eintreten kann. Der resultierende Schaden wird als hoch eingeschätzt, da der Arzt (P-e/P-upp) neben einem Imageschaden mit empfindlichen rechtliche Konsequenzen rechnen muss.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R4.3	B4.3	sehr hoch	hoch	Bei einem gezielten Angriff durch einen P-x muss kriminelles Potenzial vorausgesetzt werden. Die Eintrittswahrscheinlichkeit des Zugriffs auf die DA-zpp ist hierbei abhängig vom Angreifer P-x und dessen Motivation. Sie wird mit hoch abgeschätzt, wenn der Angreifer aus dem Umfeld der Domäne stammt (z. B. P-lad). In diesem Fall ist von einer hohen Eintrittswahrscheinlichkeit auszugehen. Der resultierende Schaden wird als sehr hoch eingeschätzt, da der Arzt (P-e/P-upp) neben einem Imageschaden mit empfindlichen rechtliche Konsequenzen rechnen muss. Insbesondere ist hier zu berücksichtigen, dass das Ziel eines Angreifers die Verursachung eines Schadens ist.
R4.4	B4.3	sehr hoch	niedrig	Die Eintrittswahrscheinlichkeit eines gezielten Angriffs auf die DA-zpp durch einen P-x ist hierbei abhängig vom Angreifer und dessen Motivation, sie wird mit niedrig abgeschätzt, wenn der Angreifer nicht aus dem Umfeld berechtigter Personen stammt. In diesem Fall ist von einer geringen Eintrittswahrscheinlichkeit auszugehen. Der resultierende Schaden wird als sehr hoch eingeschätzt, da der Arzt (P-e/P-upp) neben einem Imageschaden mit empfindlichen rechtliche Konsequenzen rechnen muss. Insbesondere ist hier zu berücksichtigen, dass das Ziel eines Angreifers die Verursachung eines Schadens ist.
R4.5	B4.4	hoch	niedrig	Dieses Ereignis tritt ein, wenn die DA-zpp die Domäne DO-e verlassen und eine nicht berechtigte Person P-x hierdurch Zugriff auf DA-zpp erhält. Ursache kann eine menschliche Fehlhandlung sein. Ein Versagen der Pseudonymisierung wird in B4.5 betrachtet. Die Eintrittswahrscheinlichkeit wird daher als niedrig eingeschätzt. Der resultierende Schaden wird als hoch eingeschätzt, da der Arzt (P-e/P-upp) neben einem Imageschaden mit empfindlichen rechtliche Konsequenzen rechnen muss. Im Gegensatz zu R4.4 wird der Schaden nur mit „hoch“ abgeschätzt, da nicht von einem gezielten Angriff auszugehen ist.

Risiko Nr.	Bedrohung	Schadenshöhe	Eintrittswahrscheinlichkeit	Bemerkung
R4.6	B4.5	hoch	niedrig	Ein Versagen der Pseudonymisierung oder Anonymisierung hat zur Folge, dass ungewollt personenbezogene Daten einem großen Personenkreis bekannt werden können (z. B. P-dap, P-up, P-uz, P-u). Die Eintrittswahrscheinlichkeit wird mit niedrig eingeschätzt, da in diesem Bereich von einem geeigneten Softwareentwicklungsprozess ausgegangen werden kann. Der resultierende Schaden wird als hoch eingeschätzt, da der Arzt (P-e/P-upp) neben einem Imageschaden mit empfindlichen rechtliche Konsequenzen rechnen muss. Im Gegensatz zu R4.4 wird der Schaden nur mit „hoch“ abgeschätzt, da nicht von einem gezielten Angriff auszugehen ist.
R4.7	B4.6	hoch	sehr hoch	Wird von einem gezielten Angriff durch einen P-lad ausgegangen ist die Eintrittswahrscheinlichkeit als sehr hoch anzusehen, da lediglich die Protokollierungsfunktion deaktiviert werden müsste. Der durch einen P-lad zu betreibenden Aufwand ist sehr gering. Das Schadensausmaß wird ebenfalls unter dem Aspekt des gezielten Angriffs abgeschätzt. Es wird ein hohes Schadensmaß angesetzt, da davon auszugehen ist, dass die Deaktivierung einen Angriff auf DA-zpp oder DA-zp zur Folge hat.
R4.8	B4.7	mittel	mittel	Die Pseudonymisierungstabellen befinden sich ausschließlich in der Domäne DO-e, in der (außer dem lokalen Administrator P-lad) sich ausschließlich Personen mit Zugriffsberechtigung auf DA-zpp befinden. Tritt dieses Szenario ein, müssen die Pseudonymisierungstabellen die Domänengrenze verlassen. Die Eintrittswahrscheinlichkeit hierfür wird mit niedrig abgeschätzt, da dies entweder einem gezielten Angriff oder einer massiven menschlichen Fehlhandlung (Weitergabe) gleich kommt. Der Schaden wird mit mittel abgeschätzt, da der Personenkreis P-up zwar keine Berechtigung für DA-zpp besitzt jedoch nicht von einer zu einem Schaden führenden Ausnutzung auszugehen ist.
R4.9	B4.8	mittel	niedrig	Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da durch geeignete Maßnahmen (Zugriffsschutz auf Datenbanken und auf Dateisystemen) entsprechende Zugriffsrechte gesetzt werden und ein P-x hohen Aufwand für den Zugriff auf DA-zp/DA-z betreiben müssten. Der Schaden wird mit mittel abgeschätzt, da der Personenkreis P-x zwar keine Berechtigung für DA-zp/DA-z besitzt jedoch nicht von einer zu einem Schaden führenden Ausnutzung auszugehen ist.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R4.10	B4.9	mittel	niedrig	Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da durch geeignete Maßnahmen (Zugriffsschutz auf Datenbanken und auf Dateisystemen) entsprechende Zugriffsrechte gesetzt werden und der Aufwand für die Umgehung durch einen P-u sehr hoch ist. Der Schaden wird mit mittel abgeschätzt, da der Personenkreis P-u zwar keine Berechtigung für DA-zp/DA-z aber für die Grid-Nutzung besitzt jedoch nicht von einer zu einem Schaden führenden Ausnutzung auszugehen ist.
R4.11	B4.10	niedrig	sehr hoch	Aufgrund der weitreichenden Rechte des P-lad innerhalb der Domäne muss davon ausgegangen werden, dass dieser mit hoher Wahrscheinlichkeit und geringem Aufwand ein Zugriff auf DA-zp (personenbeziehbare Daten) und DA-z (hier z. B. anonymisierte Patientinnendaten) erhalten kann. Es ist jedoch nur von einer niedrigen Schadenshöhe auszugehen.
R4.12	B4.11	niedrig	sehr hoch	Wie in B4.8 ist auch hier von weitreichenden Rechten der Ressourcenprovider (P-svp, P-swp, P-hwp, P-dap) auszugehen, so dass diese mit geringem Aufwand und daher sehr hoher Wahrscheinlichkeit ein Zugriff auf DA-zp/DA-z erhalten können. Es ist jedoch nur von einem niedrigen Schadenspotenzial auszugehen, da die Ressourcenprovider (P-svp, P-swp, P-hwp, P-dap) ein sehr hohes Interesse an einem positiven Image haben und nicht von einer Ausnutzung auszugehen ist.
RK4.1	BK4.4	niedrig	hoch	Die Eintrittswahrscheinlichkeit wird mit hoch abgeschätzt, da einem Grid-User P-u üblicherweise alle lokal verfügbaren Systemwerkzeuge zur Verfügung stehen und diese genutzt werden können. Von einer gehärteten Umgebung (restricted shell) kann nicht ausgegangen werden, so dass geringer Aufwand erforderlich ist. Das Schadenspotenzial wird in diesem Szenario mit niedrig abgeschätzt, da nicht davon ausgegangen werden kann, dass Rückschlüsse auf verarbeitete Daten und insbesondere auf Personendaten (DA-zpp) möglich sind.
RK4.2	BK4.5	hoch	niedrig	Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da von funktionierenden Mechanismen zur Benutzerauthentikation (Zertifikate) und damit einem hohen Aufwand zur Durchführung des Angriffs ausgegangen werden kann. Das Schadenspotenzial wird als hoch eingeschätzt, da bei eintreten der Bedrohung unberechtigte Zugriff auf schützenswerte Daten erlangen können (z. B. DA-zp, DA-z).

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R4.13	B4.12	mittel	niedrig	Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da die Übertragungswege innerhalb des Grid durch VPN vor einer Abhörung abgesichert sind und somit hoher Aufwand für einen Angriff erforderlich ist. Das Schadenspotenzial wird mit mittel abgeschätzt, da nicht von einer Ausnutzung auszugehen ist.
RK4.3	BK4.1	mittel	niedrig	Da GridFTP bereits Mechanismen zur Wahrung von Vertraulichkeit und Integrität besitzt (data channel protection mode), ist eine Kompromittierung der Daten während des Dateitransfers zwischen den Folgeinstanzen (z. B. Zwischenergebnisse) sehr unwahrscheinlich. Der Aufwand für einen gezielten Angriff ist sehr hoch, da kryptografische Verfahren gebrochen werden müssten. Das Schadenspotenzial wird mit mittel abgeschätzt, da nicht von einer Ausnutzung auszugehen ist. Siehe auch Risiko R4.13
R4.14	B4.13	sehr hoch	niedrig	Auch wenn der lokale Administrator P-lad mit sehr hoher Wahrscheinlichkeit die Möglichkeit der Manipulation hat, wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt, da hier eine vorsätzliche Handlung anzunehmen wäre. Das Schadenspotenzial wird als sehr hoch eingeschätzt, da eine Manipulation zu fehlerhaften Diagnosen oder Behandlungen führen könnte und somit die persönliche Unversehrtheit des Patienten P-p gefährdet ist.
R4.15	B4.14	sehr hoch	niedrig	Wie auch bei B4.11 wirkt sich hier Vorsatz abschwächend auf die Abschätzung der Eintrittswahrscheinlichkeit aus. Zusätzlich ist es erforderlich, dass der P-p in der Bedienung möglicher Front-End Systeme eingewiesen sein müsste, um fachlich in der Lage zu sein die Manipulation durchzuführen. Das Schadenspotenzial wird als sehr hoch eingeschätzt, da eine Manipulation zu fehlerhaften Diagnosen oder Behandlungen führen könnte und somit die persönliche Unversehrtheit des Patienten P-p gefährdet ist.
R4.16	B4.15	hoch	niedrig	Auch wenn der lokale Administrator P-lad mit sehr hoher Wahrscheinlichkeit die Möglichkeit der Manipulation hat, wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt, da hier eine vorsätzliche Handlung anzunehmen wäre. Das Schadenspotenzial wird mit hoch abgeschätzt, da auf die DA-zp aufbauenden Forschungsergebnisse ggf. falsch und damit unbrauchbar sind.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R4.17	B4.16	hoch	niedrig	Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da das Vorhandensein eines geeigneten Zugriffsschutz vorausgesetzt wird und ein P-up somit hohen Aufwand betreiben müsste. Das Schadenspotenzial wird mit hoch abgeschätzt, da auf die DA-zp aufbauenden Forschungsergebnisse ggf. falsch und damit unbrauchbar sind.
R4.18	B4.17	hoch	niedrig	Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da das Vorhandensein eines geeigneten Zugriffsschutz vorausgesetzt wird und ein P-x somit hohen Aufwand betreiben müsste. Das Schadenspotenzial wird mit hoch abgeschätzt, da auf die DA-zp aufbauenden Forschungsergebnisse ggf. falsch und damit unbrauchbar sind.
R4.19	B4.18 B4.21	mittel	niedrig	Auch wenn der lokale Administrator P-lad mit sehr hoher Wahrscheinlichkeit und geringem Aufwand die Möglichkeit der Manipulation hat, wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt, da hier eine vorsätzliche Handlung anzunehmen wäre. Das Schadenspotenzial wird mit mittel abgeschätzt, da zwar der Nachweispflicht nicht nachgekommen werden kann, die resultierenden Konsequenzen jedoch gering sind.
R4.20	B4.19	hoch	niedrig	Auch wenn der lokale Administrator P-lad mit sehr hoher Wahrscheinlichkeit und geringem Aufwand die Möglichkeit der Manipulation hat, wird die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt, da hier eine vorsätzliche Handlung anzunehmen wäre. Das Schadenspotenzial wird mit hoch abgeschätzt, da auf die DA-nz aufbauenden Forschungsergebnisse ggf. falsch und damit unbrauchbar sind.
R4.21	B4.20	hoch	niedrig	Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da das Vorhandensein eines geeigneten Zugriffsschutz vorausgesetzt wird und damit der durch einen P-u zu betreibende Aufwand groß ist. Das Schadenspotenzial wird mit hoch abgeschätzt, da auf die DA-nz aufbauenden Forschungsergebnisse ggf. falsch und damit unbrauchbar sind.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R4.22	B4.21	mittel	niedrig	Eine bewusste Manipulation oder Löschung durch einen P-lad wird bezüglich der Eintrittswahrscheinlichkeit mit niedrig abgeschätzt, da Vorsatz oder mangelnde Sorgfalt die Ursache wären und in diesem Szenario davon nicht ausgegangen werden kann. Das Schadenspotenzial wird mit mittel abgeschätzt, zwar kann der Nachweispflicht nicht nachgekommen werden kann, die resultierenden Konsequenzen jedoch gering sind.
R4.23	B4.22	mittel	niedrig	Eine bewusste Manipulation durch einen P-lad oder ungewollte Fehlfunktion wird bezüglich der Eintrittswahrscheinlichkeit mit niedrig abgeschätzt, da Vorsatz oder mangelnde Sorgfalt die Ursache wären und in diesem Szenario davon nicht ausgegangen werden kann. Das Schadenspotenzial wird mit mittel abgeschätzt, zwar kann der Nachweispflicht nicht nachgekommen werden kann, die resultierenden Konsequenzen jedoch gering sind.
R4.24	B4.23	mittel	hoch	Die Standard-Softwarekomponenten besitzen heute selten weitreichende Auditingfunktionen, so dass mit hoher Wahrscheinlichkeit davon ausgegangen werden kann, dass die Auditingfunktionen nicht ausreichen. Das Schadenspotenzial wird mit mittel abgeschätzt, zwar kann der Nachweispflicht nicht nachgekommen werden , die resultierenden Konsequenzen sind jedoch gering.
R4.25	B4.24	niedrig	niedrig	Durch den Zugriff auf eine Grid-Ressource innerhalb DO-hw durch einen P-x ist zwar eine unberechtigte Nutzung anzunehmen, jedoch wird die Wahrscheinlichkeit mit niedrig abgeschätzt, da geeigneter Zugriffsschutz vorausgesetzt wird und somit hoher Aufwand zu betreiben wäre. Das Schadenspotenzial wird ebenfalls mit gering eingeschätzt, da bei der Nutzung einer Grid-Ressource noch nicht von einem Schaden ausgegangen werden kann. Im schlimmsten Fall wird ein berechtigter Nutzer P-u durch die unberechtigte Nutzung behindert.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
RK4.4	BK4.2	hoch	niedrig	Die Kompromittierung des Globus Resource Allocation Manager Prozesses ist identisch mit der Manipulation einer Softwarekomponente auf einer Grid Ressource. Eine solche Manipulation kann lediglich durch berechtigte Personen (P-lad) erfolgen, der Aufwand für den Angriff ist zwar gering, jedoch muss davon ausgegangen werden, dass vertrauenswürdiges Personal eingesetzt wird. Die Eintrittswahrscheinlichkeit wird daher mit niedrig abgeschätzt. Das Schadensausmaß wird mit hoch abgeschätzt, da neben den verarbeiteten Daten (z. B. DA-zpp, DA-z) auch die Grid Ressource bezüglich ihrer Integrität und Verfügbarkeit gefährdet ist.
RK4.5	BK4.3	hoch	hoch	Die Eintrittswahrscheinlichkeit wird mit hoch abgeschätzt, da das referenzierte Grid Map File manuell erstellt wird und hier menschliches Versagen eine häufige Ursache für Fehler sind. Des weiteren ist nicht immer gewährleistet, dass eine 1-zu-1 Beziehung zwischen Grid-ID und lokaler User-ID gegeben ist, d. h. es ist möglich dass mehrere Grid-IDs durch Gruppenbildung auf eine lokale User-ID gemappt werden. Die potenzielle Schadenshöhe wird mit hoch abgeschätzt, da aufgrund der fehlenden Separierung lokaler User-IDs die Möglichkeit besteht auf Daten (z. B. DA-zpp, DA-z) anderer Grid-User zuzugreifen. Integrität und Vertraulichkeit sind somit stark gefährdet.
RK4.6	BK4.6	hoch	niedrig	Die Kompromittierung des Proxy Certification Files ist identisch mit der Manipulation einer Softwarekomponente auf einer Grid Ressource. Eine solche Manipulation kann lediglich durch berechtigte Personen (P-lad) erfolgen, der Aufwand für den Angriff ist zwar gering, jedoch muss davon ausgegangen werden, dass vertrauenswürdiges Personal eingesetzt wird. Die Eintrittswahrscheinlichkeit wird daher mit niedrig abgeschätzt. Das Schadensausmaß wird mit hoch abgeschätzt, da neben den verarbeiteten Daten (z. B. DA-zpp, DA-z) auch die Grid Ressource bezüglich ihrer Integrität und Verfügbarkeit gefährdet ist.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R4.26	B4.25	sehr hoch	niedrig	Im Falle einer menschlichen Fehlhandlung (Löschung, Zerstörung) wird von einer niedrigen Eintrittswahrscheinlichkeit ausgegangen, da das Vorhandensein einer geeigneten Datensicherung angenommen wurde und damit ein Verlust der Patientendaten durch unerwartete Ereignisse verhindert werden kann. Durch das Vorhandensein einer Datensicherung ist die Wiederherstellung verloren gegangener Patientendaten (DA-zpp) in kurzer Zeit möglich. Der Schaden wird als sehr hoch eingeschätzt, da bei einem Verlust der Patientendaten eine nicht fristgerechte Behandlung des Patienten (P-p) zu befürchten und somit die persönliche Unversehrtheit gefährdet ist.
R4.27	B4.25	sehr hoch	hoch	Tritt die Bedrohung als Folge höherer Gewalt (z. B. Brand, Wasser etc.) ein, ist davon auszugehen, dass sowohl die Daten als auch die Datensicherung zerstört wurde, da üblicherweise keine externe Aufbewahrung der Daten stattfindet. Daher wird die Eintrittswahrscheinlichkeit mit hoch bewertet. Der Schaden wird als sehr hoch eingeschätzt, da bei einem Verlust der Patientendaten eine nicht fristgerechte Behandlung des Patienten (P-p) zu befürchten und somit die persönliche Unversehrtheit gefährdet ist.

In der nachfolgenden Risikomatrix sind sowohl die Eintrittswahrscheinlichkeit (x-Achse) als auch die Schadenshöhe (y-Achse) des jeweiligen Risikos aus Tabelle 11 dargestellt.

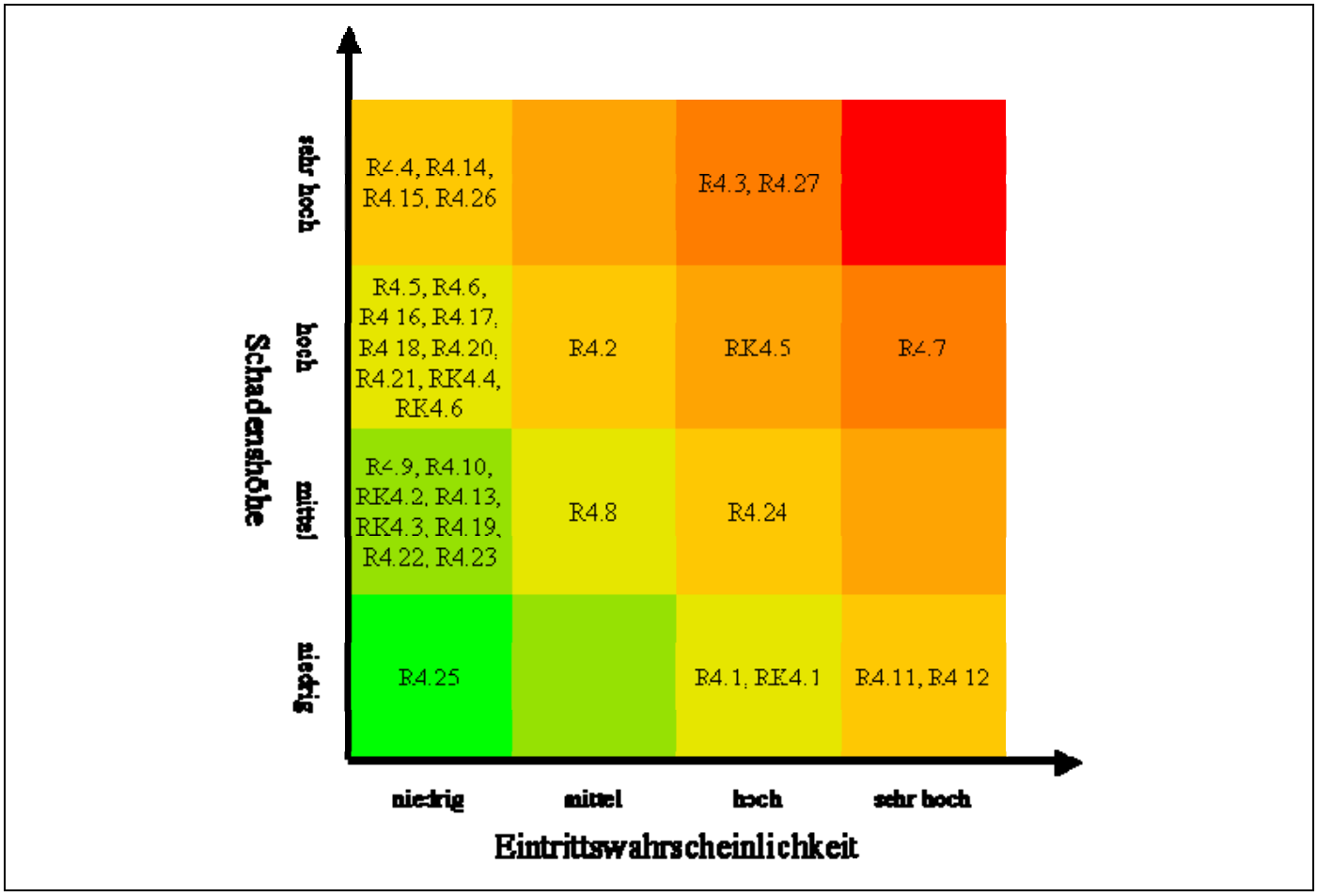

Abbildung 4: Risikomatrix Szenario 4

2.4.6 Fazit der Risikoanalyse

Im Folgenden werden die Erkenntnisse, die im Rahmen der Erstellung der Risikoanalyse für dieses Szenario gewonnen wurden, zusammengefasst.

Etablierte Sicherheitsmechanismen

Insbesondere das Vorhandensein außerhalb des Grid-Kontextes etablierter Sicherheitsmechanismen (Verschlüsselung, Authentikation, Datensicherung) schränken in diesem Szenario die relevanten Risiken auf vorsätzliche Handlungen durch Angreifer und höhere Gewalt ein. Wird von der Wirksamkeit der Sicherheitsmechanismen ausgegangen, also dass Zugriffsrechte in Datenbanken und auf Dateisystemen sorgfältig gepflegt sind, beschränkt sich der Personenkreis der „Angreifer“ auf Personen mit krimineller Intention oder Personen mit besonderen Rechten (Administratoren).

Potenzielle Risiken

Insbesondere die hohen Eintrittswahrscheinlichkeiten für Risiken, deren Verursacher Personen mit besonderen Rechten (z. B. R4.3 und R4.7) sind, 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 Admi-

nistratoren, versagen die üblichen technischen Maßnahmen, da Administratoren unbeschränkten physischen und logischen Zugriff auf Ressourcen haben. In diesem Bereich sind organisatorische Maßnahmen zu ergreifen, mit denen sichergestellt werden kann, dass mit hoher Wahrscheinlichkeit kein Angriff von diesem Personenkreis ausgeht.

Insbesondere im MammoGRID lässt sich aktuell als Risiko das „Identity-Mapping“ als relevant und kritisch identifizieren. 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 in DO-swp auf eine Sammel-/Gruppenkennung gemappt werden, so dass hier potenziell die Möglichkeit besteht, dass ein Grid-Benutzer *USER987* in DO-swp auf denselben Benutzer gemappt wird und somit auf der Ressource Zugriff auf Daten des Nutzers *USER123* besitzt.

Fazit

Die Wirksamkeit der im Grid vorhandenen Sicherheitsmechanismen hängt maßgeblich von der sorgfältigen Administration aller Komponenten/Ressourcen ab. Die lokal wirkenden Administratoren (P-lad) können ohne großen Aufwand jeden denkbaren Angriff durchführen (vgl. z.B. R4.1, R4.7). Dies ist jedoch ein – auch außerhalb des Grid-Kontextes – bekanntes und derzeit mit technischen Mitteln schwer zu lösendes Problem. Hier sind organisatorische Maßnahmen zur Risikoeindämmung zwingend erforderlich.

2.5 Bedrohungs- und Risikoanalyse Szenario 5

Im fünften Szenario geht es um eine Grid-Infrastruktur („K-Grid“), die bei großen krisenhaften Ereignissen („K-Fall“: Umweltkatastrophen, Verteidigungsfall, sonstige Krisenfälle, terroristische Anschläge etc.) in der Lage ist, umfangreiche Ressourcen (Rechen-, Daten-, Kommunikationsressourcen usw.) kurzfristig und zuverlässig verfügbar zu machen. Die Ressourcen stehen dabei nicht notwenig bereit, sondern müssen bei Bedarf sehr kurzfristig verfügbar gemacht werden.

Die Ressourcen können also im Normalfall zu sehr unterschiedlichen Einrichtungen und damit Domains 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 erreichen, dann muss es jedoch sehr kurzfristig seinen zuvor definierten Zustand (d. h. technisch und organisatorisch) erreichen.

Bezogen auf die Schutzbedarfsfeststellung ist hierbei die genaue Ausrichtung des Grid relevant. Dem gegenüber steht der 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 müssen, um ein solches Szenario mit Zukunftspotential 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, sind Eingabedaten im Verteidigungsfall auch bezogen auf ihre Vertraulichkeit mit einem hohen Schutzbedarf zu belegen.

2.5.1 Sicherheitsanforderungen

In [3] wurden Sicherheitsanforderungen und Zugriffsberechtigungen für das Szenario 5 definiert, für die Risikoanalyse werden diese konkretisiert.

SA5.0: Die persönliche Unversehrtheit der beteiligten Personen ist sichergestellt.

SA5.I: Die Verfügbarkeit des Grid muss im Bedarfsfall in kurzer Zeit gewährleistet sein.

SA5.II: Die Integrität/Authentizität der gelieferten Basisdaten und Eingabedaten (DA-z) ist sichergestellt.

SA5.III: Die Integrität/Authentizität der Ergebnisdaten (DA-zz) ist sichergestellt.

SA5.IV: Die Vertraulichkeit der Ergebnisdaten (DA-zz) ist sichergestellt.

Die SA5.0 ist in diesem Szenario ein übergeordnetes und primäres Ziel. Die SA5.I-SA5.IV sind streng genommen Sicherheitsziele, die die Erreichung des SA5.0 gewährleisten oder unterstützen. Bedrohungen, die auf SA5.I-SA5.IV wirken haben im Worst-Case Auswirkung auf SA5.0, daher wird zu SA5.0 keine abstrakte Bedrohung definiert.

2.5.2 Abstrakte Bedrohungen

Aus den o. g. Sicherheitsanforderungen werden abstrakte Bedrohungen abgeleitet, die anschließend verfeinert und für die Risikoanalyse genutzt werden:

AB5.I: Durch einen fehlerhaften Auswahlprozess werden Partner ausgewählt, die Grid-Ressourcen im Bedarfsfall nicht schnell genug oder nicht während der erforderlichen Zeit zur Verfügung stellen können.

AB5.II: Die Datenprovider (P-dap) liefern nicht authentische Basis- oder Eingabedaten (DA-z).

AB5.III: Basisdaten (DA-z) werden verändert.

AB5.IV: Die Ergebnisdaten (DA-zz) werden verändert.

AB5.V: Ergebnisdaten (DA-zz) werden einem nicht berechtigten Personenkreis bekannt.

2.5.3 Annahmen zu Sicherheitsmaßnahmen

Die derzeit im Einsatz befindlichen Grids besitzen bereits Sicherheitsmechanismen, deren Vorhandensein und Wirksamkeit im Rahmen der Risikoanalyse angenommen wird. Nachfolgend sind die wesentlichsten Sicherheitsmechanismen zusammengefasst:

- Die Kommunikation zwischen den einzelnen Domänen erfolgt verschlüsselt, so sind die Daten bei der Übertragung vor unberechtigter Einsichtnahme und Veränderung geschützt.
- Auf den einzelnen Grid-Ressourcen sind derzeit übliche (Best-Practice oder Grundschutz) Sicherheitsmaßnahmen umgesetzt, hierzu gehören beispielsweise:
  - Geeignete Authentikationsmechanismen sichern den Zugriff auf die Ressourcen und Daten ab.
  - Der Zutritt zu Räumen und Zugriff auf Ressourcen ist durch geeignete physikalische Maßnahmen abgesichert.

2.5.4 Bedrohungsanalyse

Ausgehend von den abstrakten Bedrohungen AB5 werden nachfolgende konkrete Bedrohungen aufgestellt. Die Bedrohungen resultieren hierbei aus den in Tabelle 33 aus [3] geschilderten Abläufen.

Tabelle 12: Bedrohungsanalyse Szenario 5

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB5.I: Durch einen fehlerhaften Auswahlprozess werden Partner ausgewählt, die Grid-Ressourcen im Bedarfsfall nicht schnell genug oder nicht während der erforderlichen Zeit zur Verfügung stellen können. Die Auswirkungen können weitreichend sein, im Worst-Case-Szenario stehen die für die Koordinierung der Einsatzkräfte erforderlichen Ergebnisdaten nicht rechtzeitig zur Verfügung, um betroffene Personen aus der Gefahrenzone zu evakuieren. Die persönliche Unversehrtheit ist damit gefährdet.			
B5.1	DA-zz	Verfügbarkeit	Aufgrund der Auswahl nicht geeigneter Partner (hier durch die DO-BBK) ist das Grid im Bedarfsfall nicht Einsatzfähig. In der Folge können die Ergebnisdaten (DA-zz) nicht in erforderlicher Zeit zur Verfügung gestellt werden.
B5.2	SW SRV HW	Verfügbarkeit	Erforderliche Grid-Ressourcen fallen während der Nutzung aus und in der Folge können Ergebnisdaten (DA-zz) nicht in erforderlicher Zeit zur Verfügung gestellt werden.
AB5.II: Die Datenprovider (P-dap) liefern nicht authentische Basis- oder Eingabedaten. Die Auswirkungen aufgrund nicht authentischer und damit fehlerhafter Basis- oder Eingabedaten können ebenso weitreichend sein, wie die Folgen von AB5.II. Im Worst-Case-Szenario sind die Ergebnisdaten unbrauchbar, werden unnötige und unwirksame Maßnahmen durch die Einsatzkräfte ergriffen, so dass real gefährdete Personen nicht geschützt werden können. Auch hier ist die persönliche Unversehrtheit gefährdet.			
B5.3	DA-z	Integrität	Aufgrund menschlichem Versagens liefern die Einsatzkräfte (P-dap) in der Domäne DO-FW falsche Eingabedaten (DA-z).
B5.4	DA-z	Integrität	Aufgrund menschlichem Versagens liefern die Datenprovider (P-dap) in den unterschiedlichen Domänen (DO-BAM, DO-AWA) falsche Basisdaten (DA-z).

Bedrohung Nr.	Bedrohtes Objekt	Verletzter Grundwert	Bedrohungsszenario
AB5.III: Basisdaten (DA-z) werden verändert. Auch diese Bedrohung kann zur falschen Koordinierung von Einsatzkräften infolge unbrauchbarer Ergebnisdaten (DA-zz) führen und somit zu Gefahr für Leib und Leben der betroffenen Personen führen. Die Veränderung in dieser Bedrohung werden im Gegensatz zu in AB5.II unter dem Szenario der mutwilligen Änderung betrachtet.			
B5.5	DA-z	Integrität	Basisdaten (DA-z) werden durch Datenprovider (P-dap) in den Domänen der Datenprovider (DO-BAM, DO-AWA) unberechtigt verändert.
B5.6	DA-z	Integrität	Basisdaten (DA-z) werden während der Verarbeitung in den Domänen der Hardware-Provider (DO-GRZ1, DO-GRZ2) durch die lokalen Administratoren (P-lad) verändert.
AB5.IV: Die Ergebnisdaten (DA-zz) werden verändert. Eine Manipulation von Ergebnisdaten (DA-zz) oder von Teilergebnissen (diese werden auch als DA-zz aufgefasst) kann gravierende Folgen haben. Die Situation der Katastrophe kann falsch aufgefasst und in der Folge Einsatzkräfte fälschlich koordiniert werden. In letzter Konsequenz kann dies Leib und Leben der betroffenen Bevölkerung gefährden, somit gegen die Erreichung von SA5.0 wirken.			
B5.7	DA-zz	Integrität	Ergebnisdaten (DA-zz) werden durch einen lokalen Administrator (P-lad) in den Domänen der Hardware-Provider (DO-GRZ1, DO-GRZ2) manipuliert.
B5.8	DA-zz	Integrität	Ergebnisdaten (DA-zz) werden durch einen lokalen Administrator (P-lad) in DO-BBK manipuliert.
B5.9	DA-zz	Integrität	Ergebnisdaten (DA-zz) werden durch einen Datenprovider (P-dap) in DO-BBK manipuliert.
AB5.V: Ergebnisdaten (DA-zz) werden einem nicht berechtigten Personenkreis bekannt. Als unberechtigter Personenkreis können im K-Fall z. B. die Medien aufgefasst werden, die Auswirkungen des Ereignis veröffentlichen. In der Folge kann es zu Panik unter der Bevölkerung oder zum Katastrophentourismus kommen, so dass die erfolgreiche Arbeit der Einsatzkräfte erschwert oder behindert wird. Finanzielle Schäden sind durch den erhöhten Bedarf an Einsatzkräften zwar denkbar, jedoch insbesondere die erschwerte Erreichung des SA5.0 in diesem Fall eine relevante Auswirkung.			
B5.10	DA-zz	Vertraulichkeit	Ein lokaler Administrator (P-lad) aus den Domänen der Hardware-Provider (DO-GRZ1, DO-GRZ2) greift unberechtigt auf Ergebnisdaten DA-zz (oder Teilergebnisse, die ebenfalls als DA-zz aufgefasst werden) zu und gibt diese an Außenstehende weiter.
B5.11	DA-zz	Vertraulichkeit	Innerhalb der Domäne DO-BBK greift ein P-lad oder P-dap unberechtigt auf Ergebnisdaten (DA-zz) zu und gibt diese an Außenstehende weiter.
B5.12	DA-zz	Vertraulichkeit	Ein P-uz aus DO-BBK oder DO-FW gibt die Ergebnisdaten (DA-zz) unberechtigt an Außenstehende weiter.
B5.13	DA-zz	Vertraulichkeit	Eine außenstehende Person (P-x) nutzt unberechtigt Ressourcen innerhalb der Domäne DO-FW und gibt Ergebnisdaten (DA-zz) an Außenstehende weiter.

2.5.5 Risikoanalyse

Im folgenden werden die Schadenshöhe und Eintrittswahrscheinlichkeiten der im vorigen Kapitel aufgeführten Bedrohungen abgeschätzt. Die Ursache für das Eintreten der jeweiligen Bedrohung kann vielfältig sein. Um die Abschätzung nachvollziehen zu können, wird auf die möglichen Ursachen im Rahmen der Bemerkung Bezug genommen.

Tabelle 13: Risikoanalyse Szenario 5

Risiko Nr.	Bedrohung	Schadenshöhe	Eintrittswahrscheinlichkeit	Bemerkung
R5.1	B5.1	sehr hoch	niedrig	Die Auswirkungen der Auswahl nicht geeigneter Partner in der Phase der Bildung des Grid (hier durch die DO-BBK) können gravierende Auswirkungen haben. Kann das Grid in der Folge im Bedarfsfall nicht genutzt werden, sind Leib und Leben der betroffenen Bevölkerung und der Einsatzkräfte bedroht. Die Eintrittswahrscheinlichkeit wird als niedrig eingestuft, da eine gewissenhafte Auswahl der Partner vorauszusetzen ist. ***Anmerkung:*** In diesem Szenario wird davon ausgegangen, dass die Funktionsfähigkeit des Grid regelmäßig in Form von Katastrophenübungen überprüft und damit die Eintrittswahrscheinlichkeit signifikant reduziert wird.
R5.2	B5.2	sehr hoch	niedrig	Die Auswirkungen des Ausfalls einzelner Grid-Ressourcen sind vergleichbar mit den Auswirkungen von R5.1. Der mögliche Schaden wird daher ebenfalls mit sehr hoch abgeschätzt. Der Ausfall von kompletten Ressourcen ist durch redundante Auslegung relevanter IT-Komponenten nicht anzunehmen, die Eintrittswahrscheinlichkeit wird daher mit niedrig abgeschätzt. ***Anmerkung:*** Insbesondere hier muss während der Konzeptphase auf ausreichende Redundanz der einzelnen Komponenten geachtet werden. Hierzu zählen aufgrund der verteilten Standorte auch die Redundanz der Kommunikationsstrecken zwischen den einzelnen Domänen.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R5.3	B5.2	sehr hoch	niedrig	Die Auswirkungen des Ausfalls einzelner Grid-Ressourcen sind vergleichbar mit den Auswirkungen von R5.1. Der mögliche Schaden wird daher ebenfalls mit sehr hoch abgeschätzt. Wird die Verfügbarkeit einzelner oder mehrerer Komponenten des Grid mittels eines Distributed Denial of Service (DDoS) Angriffs (vgl. [7]) beeinträchtigt, sind spezielle Maßnahmen zum Schutz erforderlich, die bereits während der Erstellung des Sicherheitskonzepts berücksichtigt werden müssen, da hierbei auch die Betreiber der Kommunikationsstrecken mit einbezogen werden müssen (vgl. [8]). Die Eintrittswahrscheinlichkeit wird mit niedrig abgeschätzt, da es sich bei der DDoS-Problematik um ein bekanntes Problem handelt und davon ausgegangen werden kann, dass diese Problematik bei der Erstellung des Sicherheitskonzepts berücksichtigt und entsprechende Maßnahmen umgesetzt wurden. ***Anmerkung:*** Dieses Risiko ist nur für den Fall relevant, dass die Kommunikationsinfrastruktur des Grid auf der Basis des öffentlichen Internet und nicht auf privaten Netzen wie z.B. TESTA, IVBB oder IVBV realisiert ist.
R5.4	B5.3	hoch	mittel - hoch	Durch die Einsatzkräfte gelieferte, leicht fehlerhafte Eingangsdaten (DA-z) können gravierende Auswirkungen auf Ergebnisdaten (DA-zz) haben. Die Schadenshöhe wird daher mit hoch abgeschätzt. Die Eintrittswahrscheinlichkeit wird mit mittel bis hoch abgeschätzt, da insbesondere im Umfeld der Einsatzkräfte durch Stress und äußere Einflüsse Fehlerquellen angenommen werden müssen.
R5.5	B5.4	hoch	niedrig	Wie in R5.4 können auch leicht fehlerhafte Basisdaten (DA-z) gravierende Auswirkungen auf Ergebnisdaten (DA-zz) haben. Die Schadenshöhe wird daher mit hoch abgeschätzt. Im Unterschied zu R5.4 kann hier davon ausgegangen werden, dass die Fehlerhäufigkeit deutlich geringer liegt, das die Daten unter anderen Umständen erfasst wurden. Die Eintrittswahrscheinlichkeit wird daher mit niedrig abgeschätzt.
R5.6	B5.5	hoch	niedrig	Wie in R5.4 können auch leicht veränderte Basisdaten (DA-z) gravierende Auswirkungen auf Ergebnisdaten (DA-zz) haben. Die Schadenshöhe der Manipulation durch einen P-dap in DO-BAM, DO-AWA oder DO-BBK wird daher mit hoch abgeschätzt. Wird vom Normalfall ausgegangen, kann die Eintrittswahrscheinlichkeit mit niedrig abgeschätzt werden, da vorsätzliche Manipulation ausgeschlossen werden kann.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R5.7	B5.5	hoch	hoch	**Worst-Case-Abschätzung** Wie in R5.4 können auch leicht veränderte Basisdaten (DA-z) gravierende Auswirkungen auf Ergebnisdaten (DA-zz) haben. Die Schadenshöhe der Manipulation durch einen P-dap in DO-BAM, DO-AWA oder DO-BBK wird daher mit hoch abgeschätzt. Wird im Worst-Case-Szenario angenommen, dass ein P-dap bewusst Änderungen vornimmt, also vorsätzlich handelt, kann die Abschätzung der Eintrittswahrscheinlichkeit lediglich über den Aufwand erfolgen. Der Aufwand wird als niedrig angesehen, da P-dap Schreibrechte besitzen. Die Wahrscheinlichkeit wäre damit hoch.
R5.8	B5.6	hoch	niedrig	Wie in R5.4 können auch hier leicht veränderte Basisdaten (DA-z) gravierende Auswirkungen auf Ergebnisdaten (DA-zz) haben. Die Schadenshöhe der Manipulation durch einen P-lad in DO-GRZ1 oder DO-GRZ2 wird daher mit hoch abgeschätzt. Die Eintrittswahrscheinlichkeit wird für den Normalfall mit niedrig abgeschätzt, da auch hier von vertrauenswürdigen P-lad ausgegangen wird.
R5.9	B5.6	hoch	hoch	**Worst-Case-Abschätzung** Wie in R5.4 können auch hier leicht veränderte Basisdaten (DA-z) gravierende Auswirkungen auf Ergebnisdaten (DA-zz) haben. Die Schadenshöhe der Manipulation durch einen P-lad in DO-GRZ1 oder DO-GRZ2 wird daher mit hoch abgeschätzt. Wird im Worst-Case-Szenario angenommen, dass ein P-lad bewusst Änderungen vornimmt, also vorsätzlich handelt, kann die Abschätzung der Eintrittswahrscheinlichkeit lediglich über den Aufwand erfolgen. Der Aufwand wird als niedrig angesehen, da P-lad volle administrative Rechte auf den Hardwareressourcen (HW) besitzt. Die Wahrscheinlichkeit wäre damit hoch.
R5.10	B5.7	sehr hoch	niedrig	Eine Manipulation von Ergebnisdaten (DA-zz) oder von Teilergebnissen (diese werden auch als DA-zz aufgefasst) durch einen P-lad in DO-GRZ1 oder DO-GRZ2 kann gravierende Folgen haben. Die Situation der Katastrophe kann falsch aufgefasst und in der Folge Einsatzkräfte fälschlich koordiniert werden. In letzter Konsequenz kann dies Leib und Leben der betroffenen Bevölkerung gefährden, somit gegen die Erreichung von SA5.0 wirken. Die Eintrittswahrscheinlichkeit wird für den Normalfall mit niedrig abgeschätzt, da auch hier von vertrauenswürdigen P-lad ausgegangen wird.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R5.11	B5.7	sehr hoch	hoch	**Worst-Case-Abschätzung** Eine Manipulation von Ergebnisdaten (DA-zz) oder von Teilergebnissen (diese werden auch als DA-zz aufgefasst) durch einen P-lad in DO-GRZ1 oder DO-GRZ2 kann gravierende Folgen haben. Die Situation der Katastrophe kann falsch aufgefasst und in der Folge Einsatzkräfte fälschlich koordiniert werden. In letzter Konsequenz kann dies Leib und Leben der betroffenen Bevölkerung gefährden, somit gegen die Erreichung von SA5.0 wirken. Wird im Worst-Case-Szenario angenommen, dass ein P-lad bewusst Änderungen vornimmt, also vorsätzlich handelt, kann die Abschätzung der Eintrittswahrscheinlichkeit lediglich über den Aufwand erfolgen. Der Aufwand wird als niedrig angesehen, da P-lad volle administrative Rechte auf den Hardwareressourcen (HW) besitzt. Die Wahrscheinlichkeit wäre damit hoch.
R5.12	B5.8	sehr hoch	niedrig	Eine Manipulation von Ergebnisdaten (DA-zz) durch einen P-lad in DO-BBK kann gravierende Folgen haben. Die Situation der Katastrophe kann falsch aufgefasst und in der Folge Einsatzkräfte fälschlich koordiniert werden. In letzter Konsequenz kann dies Leib und Leben der betroffenen Bevölkerung gefährden, somit gegen die Erreichung von SA5.0 wirken. Die Eintrittswahrscheinlichkeit wird für den Normalfall mit niedrig abgeschätzt, da auch hier von vertrauenswürdigen P-lad ausgegangen wird.
R5.13	B5.8	sehr hoch	hoch	**Worst-Case-Abschätzung** Eine Manipulation von Ergebnisdaten (DA-zz) durch einen P-lad in DO-BBK kann gravierende Folgen haben. Die Situation der Katastrophe kann falsch aufgefasst und in der Folge Einsatzkräfte fälschlich koordiniert werden. In letzter Konsequenz kann dies Leib und Leben der betroffenen Bevölkerung gefährden, somit gegen die Erreichung von SA5.0 wirken. Wird im Worst-Case-Szenario angenommen, dass ein P-lad bewusst Änderungen vornimmt, also vorsätzlich handelt, kann die Abschätzung der Eintrittswahrscheinlichkeit lediglich über den Aufwand erfolgen. Der Aufwand wird als niedrig angesehen, da P-lad volle administrative Rechte auf den Ressourcen innerhalb DO-BBK besitzt. Die Wahrscheinlichkeit wäre damit hoch.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R5.14	B5.9	sehr hoch	niedrig	Eine Manipulation von Ergebnisdaten (DA-zz) durch einen P-uz in DO-BBK kann gravierende Folgen haben. Die Situation der Katastrophe kann falsch aufgefasst und in der Folge Einsatzkräfte fälschlich koordiniert werden. In letzter Konsequenz kann dies Leib und Leben der betroffenen Bevölkerung gefährden, somit gegen die Erreichung von SA5.0 wirken. Die Eintrittswahrscheinlichkeit wird für den Normalfall mit niedrig abgeschätzt, da auch hier von vertrauenswürdigen P-uz ausgegangen wird.
R5.15	B5.9	sehr hoch	hoch	**Worst-Case-Abschätzung** Eine Manipulation von Ergebnisdaten (DA-zz) durch einen P-dap in DO-BBK kann gravierende Folgen haben. Die Situation der Katastrophe kann falsch aufgefasst und in der Folge Einsatzkräfte fälschlich koordiniert werden. In letzter Konsequenz kann dies Leib und Leben der betroffenen Bevölkerung gefährden, somit gegen die Erreichung von SA5.0 wirken. Wird im Worst-Case-Szenario angenommen, dass ein P-dap bewusst Änderungen vornimmt, also vorsätzlich handelt, kann die Abschätzung der Eintrittswahrscheinlichkeit lediglich über den Aufwand erfolgen. Der Aufwand wird als niedrig angesehen, da P-dap Schreibrechte auf DA-zz innerhalb DO-BBK besitzt. Die Wahrscheinlichkeit wäre damit hoch.
R5.16	B5.10 B5.11	hoch	niedrig	Die unberechtigte Weitergabe von Ereignisdaten kann die Arbeit der Einsatzkräfte erschweren oder behindern. Insbesondere die hieraus als mögliche Folge resultierende Gefährdung von Leib und Leben. Die Schadenshöhe wird daher mit hoch abgeschätzt. Die Eintrittswahrscheinlichkeit wird für den Normalfall mit niedrig abgeschätzt, da von vertrauenswürdigen P-lad aus DO-GRZ1, DO-GRZ2 oder DO-BBK ausgegangen wird.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R5.17	B5.10 B5.11	hoch	hoch	**Worst-Case-Abschätzung** Die unberechtigte Weitergabe von Ereignisdaten kann die Arbeit der Einsatzkräfte erschweren oder behindern. Insbesondere die hieraus als mögliche Folge resultierende Gefährdung von Leib und Leben. Die Schadenshöhe wird daher mit hoch abgeschätzt. Wird im Worst-Case-Szenario angenommen, dass ein P-lad bewusst Ergebnisdaten (DA-zz) weitergibt, kann die Abschätzung der Eintrittswahrscheinlichkeit lediglich über den Aufwand erfolgen. Der Aufwand wird als niedrig angesehen, da P-lad administrative Rechte auf den Ressourcen innerhalb DO-GRZ1, DO-GRZ2 oder DO-BBK besitzt. Die Wahrscheinlichkeit wäre damit hoch.
R5.18	B5.12	sehr hoch	niedrig	Die unberechtigte Weitergabe von Ereignisdaten kann die Arbeit der Einsatzkräfte erschweren oder behindern. Insbesondere die hieraus als mögliche Folge resultierende Gefährdung von Leib und Leben. Die Schadenshöhe wird hier im Gegensatz zu R5.16/R5.17 mit sehr hoch abgeschätzt, da hier davon ausgegangen wird, das die Daten beim Empfänger als authentischer angenommen wird. Die Eintrittswahrscheinlichkeit wird für den Normalfall mit niedrig abgeschätzt, da von vertrauenswürdigen P-uz aus DO-BBK oder DO-FW ausgegangen wird.
R5.19	B5.12	sehr hoch	sehr hoch	**Worst-Case-Abschätzung** Die unberechtigte Weitergabe von Ereignisdaten kann die Arbeit der Einsatzkräfte erschweren oder behindern. Insbesondere die hieraus als mögliche Folge resultierende Gefährdung von Leib und Leben. Die Schadenshöhe wird hier im Gegensatz zu R5.16/R5.17 mit sehr hoch abgeschätzt, da hier davon ausgegangen wird, das die Daten in der Öffentlichkeit als authentischer angesehen werden. Wird im Worst-Case-Szenario angenommen, dass ein P-uz bewusst Ergebnisdaten (DA-zz) weitergibt, kann die Abschätzung der Eintrittswahrscheinlichkeit lediglich über den Aufwand erfolgen. Der Aufwand wird als niedrig angesehen, da P-uz aus DO-BBK / DO-FW Zugriffsrechte auf DA-zz besitzt.

Risiko Nr.	Bedro-hung	Scha-denshöhe	Eintritts-wahrschein-lichkeit	Bemerkung
R5.20	B5.13	hoch	mittel	Die unberechtigte Weitergabe von Ereignisdaten kann die Arbeit der Einsatzkräfte erschweren oder behindern. Insbesondere die hieraus als mögliche Folge resultierende Gefährdung von Leib und Leben. Die Schadenshöhe wird daher mit hoch abgeschätzt. Werden die derzeit üblichen Authentikationsmechanismen angenommen, kann davon ausgegangen werden, dass diese im Feldeinsatz wenig geeignet sind und ggf. deaktiviert werden. Der Aufwand, an DA-zz zu gelangen wird daher als mittel abgeschätzt.

In der nachfolgenden Risikomatrix sind sowohl die Eintrittswahrscheinlichkeit (x-Achse) als auch die Schadenshöhe (y-Achse) des jeweiligen Risikos aus Tabelle 13 dargestellt.

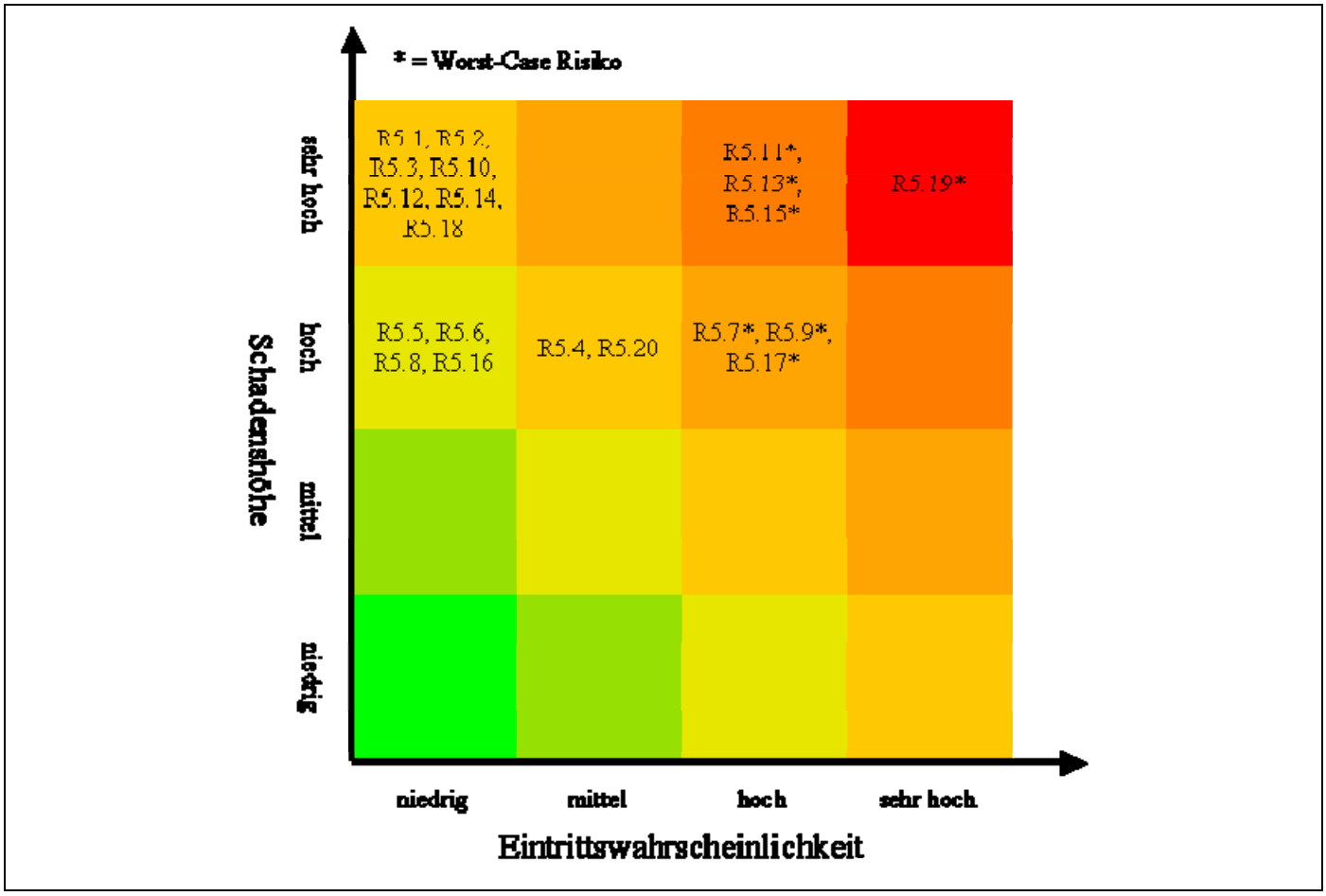

Abbildung 5: Risikomatrix Szenario 5

2.5.6 Fazit der Risikoanalyse

Im Folgenden werden die Erkenntnisse, die im Rahmen der Erstellung der Risikoanalyse für dieses Szenario gewonnen wurden, zusammengefasst.

Großes Schadenspotenzial

Der hohe Schutzbedarf bezüglich Vertraulichkeit und Integrität der Ergebnisdaten hat weitreichende Folgen und stellt in diesem Szenario den Schwerpunkt dar. Nur durch integre 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 beeinträchtigen ein hohes bis sehr hohes Schadenspotenzial haben. Die Folge ist, dass insbesondere in diesem Szenario eine Häufung von Risiken mit hohem oder sehr hohem Schadenspotenzial gegeben ist. Aufgrund der Relevanz der Ergebnisdaten können bereits kleine und leicht durchzuführende Manipulationen gravierende Auswirkungen haben (z. B. R5.9).

Wirksame Standard-Sicherheitsmaßnahmen

Durch technische Maßnahmen lassen sich die in diesem Szenario relevanten „Technik-Risiken“ gut reduzieren. Insbesondere das Vorhandensein geeigneter Authentikationsmechanismen ist bei Betrachtung der Risiken jedoch 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 lediglich in R5.20 betrachtet, so dass insbesondere Risiken, die durch unberechtigte Nutzung von Endgeräten (z. B. durch Passanten) nicht weiter analysiert wurden.

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 das 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.

Vertrauenswürdigkeit der Akteure maßgeblich für Risiko

Ein wesentliches Ziel des Szenarios ist die betroffene Bevölkerung zu schützen, bzw. den Schaden zu reduzieren (vgl. SA5.0). Hierzu ist es – wie bereits erläutert – erforderlich, dass die für die Entscheidungen relevanten Ergebnisdaten, verfügbar und integer sind. Aufgrund des durch Innentäter hervorgehenden hohen Schadenspotenzials (vgl. z.B. R5.7, R5.9, R5.15) müssen insbesondere Maßnahmen gefunden werden, die die Innentäterproblematik reduzieren. Es sind damit insbesondere Maßnahmen erforderlich, die vorsätzliche Handlungen verhindern. Organisatorisch lassen sich hier das vier-Augen-Prinzip für kritische Operationen anführen.

Die Innentäterproblematik und Relevanz der Ergebnisdaten spitzen sich im hochkritischen Risiko R5.19 zu. Dieses Risiko stellt z. B. den Fall einer unberechtigten 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.

Anhang A Referenzen

[1] Handbuch für die sichere Anwendung der Informationstechnik (IT) IT – Sicherheitshandbuch, BSI 7105, BSI, Version 1.0 - März 1992

[2] IT-Grundschutzhandbuch, BSI, November 2004

[3] Vorstudie Grid Sicherheits-Infrastruktur (GSI) Ergebnisse des Arbeitspakets 1: „Relevante Grid-Szenarien und ihr Schutzbedarf“, Version 9.3

[4] Vorstudie Grid Sicherheits-Infrastruktur (GSI), Ergebnisse des Arbeitspakets 3: „Sicherheitsmechanismen“, Version 4.1

[5] BSI-Studie "Grid Security Infrastructure / Grid Sicherheits-Infrastruktur (GSI)" - Abschlussbericht zu AP2, Version 3.0 – 22. November 2005

[6] Schwachstelle in der Sun Grid Engine, “Sun Grid Engine Local Privilege Escalation Vulnerability”, 24. Januar 2006, http://www.securityfocus.com/bid/16366

[7] (D)DoS-Angriffe, http://www.bsi.bund.de/fachthem/sinet/gefahr/gefahr_ddos.htm

[8] Empfehlungen zum Schutz vor verteilten Denial of Service-Angriffen im Internet, Version 1.1a vom 20.06.2000, http://www.bsi.bund.de/fachthem/sinet/gefahr/ddos.htm